



SUMMER – 19 EXAMINATION

Subject Name: Computer Network

Model Answer

Subject Code: 17429

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 M
	a	Enlist different types of computer networks on the basis of their geography.	2 M
	Ans	Classification of networks based on geography LAN - Local Area Network MAN - Metropolitan Area Network WAN - Wide Area Network CAN - Campus Area Network PAN - Personal Area Network	Listing of any 4 networks : ½ M each
	b	Enlist different types of servers.	2 M
	Ans	Different types of servers are: Definition of server: The central computer which is more powerful than the clients which allows the clients to access its software, database is called as the server. Types of server: 1. File server 2. Print server 3. Application server 4. Mail server	Listing of any 4 servers : ½ M each
	c	State features of any one network control devices.	2 M
	Ans	A hardware device that are used to connect computers, printers, fax machine and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks.	Any two features : 1M each



	<p>Network Control devices are:</p> <ol style="list-style-type: none">1. Repeater2. Hub3. Switch4. Bridge5. Router6. Gateway7. Modem <p>Features of network control device:</p> <p>Repeater:</p> <ul style="list-style-type: none">• It is used to take the distorted, weak and corrupt input signal and regenerate this signal at its output.• It ensures that the signals are not distorted or weak before it reaches the destination.• It recreates the bit pattern of the signal, and puts this regenerated signal back on to the transmission medium• It works in the physical layer with no intelligent function. <p>Hub:</p> <ul style="list-style-type: none">• It is also known as multiport repeater.• It is normally used for connecting stations in a physical star topology.• It is the broadcasting device.• It sends packets to all nodes in the network. <p>Switch:</p> <ul style="list-style-type: none">• It is used to connect multiple computers in which it can direct a transmission to its specific destination. (Unicast the signals).• It is a unicasting device.• It avoids unnecessary network traffic.• It operates in both the physical and the data link layer. <p>Bridge:</p> <ul style="list-style-type: none">• It is a device which connects two or more segment of a network.• A bridge filters data traffic at a network boundary.• Bridges reduces the amount of traffic on a LAN by dividing it into two segments.• It inspects incoming traffic and decides whether to forward or discard it.• It sends packets between two networks of same type.• A bridge operates in both the physical and the data link layer. <p>Gateway:</p> <ul style="list-style-type: none">• It is a node in a computer network, a key stopping point for data on its way to or from other networks.• Gateway is protocol converter.• Gateway enables communication between different network architecture and environments.• It works at all layers of OSI model. <p>Router:</p>	
--	--	--



	<ul style="list-style-type: none"> • It is a device that helps in determining the best and shortest path out of the available paths, for a particular transmission. • Routers use logical and physical addressing to connect two or more logically separate networks. • Router read complex network address in packet and efficiently direct packets from one network to another, reducing excessive traffic • It works at Physical, Data-Link and Network Layer of OSI model • It Connect dissimilar networks. <p>Modem:</p> <ul style="list-style-type: none"> • Modem works as modulator as well as demodulator. • It is the device used to converts digital signals generated by the computer into analog signals which can be transmitted over a telephone or cable line transforms incoming analog signals into their digital equivalents. • A two way communication is established. 		
	d	State two advantages of Mesh topology.	2 M
	Ans	<p>Network Topology refers to layout of a network. Network topology specifically refers to the physical layout of the network especially the locations of the computers & how the cable is run between them.</p> <p>Types of Network Topology</p> <p>Mesh Topology Bus Topology Star Topology Ring Topology Tree Topology Hybrid Topology</p> <p>Advantages of Mesh topology</p> <ul style="list-style-type: none"> • Dedicated Links: Dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices • It is robust. If one link becomes unusable, it does not incapacitate the entire system • It is Secure. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages • Point to Point Connection: Point-to-point links make fault identification and fault isolation easy. 	Any 2 advantages : 1M each
	e	State the reason for keeping uplink and downlink frequency different in satellite communication.	2 M
	Ans	<p>Uplink frequency is used for transmission of signals from earth station transmitter to satellite. Downlink frequency is used for transmission of signals from satellite to earth station receiver.</p> <p>Satellite takes uplink signal coming from sender, processes it and converts to</p>	Definition of uplink and downlink : 1M and any



		downlink frequency and transmit it towards earth. Both the frequencies are different because: 1. The satellite transmitter generates a signal that would jam its own receiver if both uplink and downlink shared same frequency. 2. Trying to receive and transmit an amplified version of the same uplink waveform at same satellite will cause unwanted feedback or ring around from downlink antenna back to the receiver. 3. Frequency band separation allows the same antenna to be used for both receiving and transmitting simplifying satellite hardware.	three reasons why to use the frequency : 3M
	f	State the frequency band used for Infrared communication and FM radio.	2 M
	Ans	The section of the electromagnetic spectrum defined as radio communication is divided into eight ranges, called bands, each regulated by government authorities. Frequency Band used for: Infrared Communication: 300 GHz to 400 THz FM radio: 30 to 300 MHz	Each frequency : 1M each
	g	Define Protocol and Encapsulation.	2 M
	Ans	i. Protocol: Protocol is defines as the set of rules and regulations to communicate between layers in networking. OR It is set of rules and conventions sender and receiver in data communication must agree on common set of rules before they can communicate with each other. OR There are certain rules that must be followed to ensure proper communication & a set of such rules and regulation is known as protocol. ii. Encapsulation: In computer networking, the term encapsulation is used to refer to the process of each layer at the sending computer adding its own header information, in the form of metadata to the actual payload (data) OR Encapsulation is the process of taking data from one protocol and translating it into another protocol, so the data can continue across a network. For example, a TCP/IP packet contained within an ATM frame is a form of encapsulation. OR Encapsulation is the process of adding the headers and footers to the data.	Definition : 1M each
	h	Give two features of IPv6.	2 M
	Ans	Two features of IPv6 are: <ul style="list-style-type: none">• An IPv6 address consists of 16 bytes (octets)• It is 128 bits long.• IPv6 specifies hexadecimal colon notation.• Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon• IPv6 has a much larger address space	Any two features : 2M



	<ul style="list-style-type: none">• It gives greater flexibility in address allocation.• There are three types of addresses in IPv6: unicast, anycast, and multicast.• In an IPv6 address, the variable type prefix field defines the address type or purpose.	
B	Attempt any TWO :	8 M
a	Explain four features of computer networks.	4 M
Ans	<p>A computer network is interconnection of two or more computers connected to each other so that they can exchange information such as e-mail, messages or documents, or share resources such as disk storage or printer.</p> <p>Features of computer network: Network features:</p> <p>Following are the features of network:</p> <ol style="list-style-type: none">1. File Sharing2. Printer Sharing3. Application Services4. E-Mail5. Remote Access. <p><u>File sharing:</u></p> <ul style="list-style-type: none">• File sharing is the primary reason to have a network.• Before networking, computers become a popular way of sharing files, if you want to transfer a file from one computer to another; you would save the file to a floppy disk & walk it over to the other computer.• File sharing requires a shared directory or disk drive to which many users can access over the network.• When many users are accessing the same file on network, more than one person can make changes to a file at the same time.• Additionally, Network operating systems that perform file sharing also administer the security of these shared files.• Advantages:<ol style="list-style-type: none">1. Easily share information on network.2. User needs regular access of word processing files, spreadsheets so they access easily.• Disadvantages:<ol style="list-style-type: none">1. Conflicting problem arises.2. Less secure if permission not set proper. <p><u>Printer sharing:</u></p> <ul style="list-style-type: none">• Printer sharing enables you to reduce the number of printer s you need & also enables you to offer much higher quality printer.• Printer sharing can be done in several different ways on network.	Any 4 features : 1M each



- The most common way is to use printer queues on server.
- The printer queue holds print job until any currently running print jobs are finished and then automatically send the waiting job to the printer.
- Another way to share printer on network is that each workstation accesses the printer directly (Network Printer), but each must wait its turn.
- network printer that use printer queue always have a print server that handles the job of sending each print job to the printer in turn
- the print server function can be filed in a number of ways:-
 - By a file server with a printer connected directly to it.
 - By computer connected to the network with the printer connected to that computer.
- Advantages:
 1. Reduce number of printer.
 2. Reduce cost.
- Disadvantages:
 1. Reduce server performance if printer connected to server.
 2. Each user must wait its turn.

Application services:

- Just as file sharing, applications can also be shared on network.
- You can share copy of application & keeping it on the network server, from where it is also run.
- When a workstation wants to run the program, it loads the file from the network into its own memory.
- Keeping application centralized reduces the amount of disk space needed on each workstation. It is easier to administer the application.
- Advantage:
 1. Reduces the amount of disk space needed on each workstation.
 2. Centralized administration, so more security and reliability.
 3. Installation of software on each workstation without CD-ROM.
 4. Installing application on workstation is much faster and more convenient.
 5. Reduce cost.
- Disadvantage:
 1. It increases network traffic on network.
 2. If server fail or crash, then workstation is useless on network.
 3. Requires network license copy for application software or business software.

E-mail:

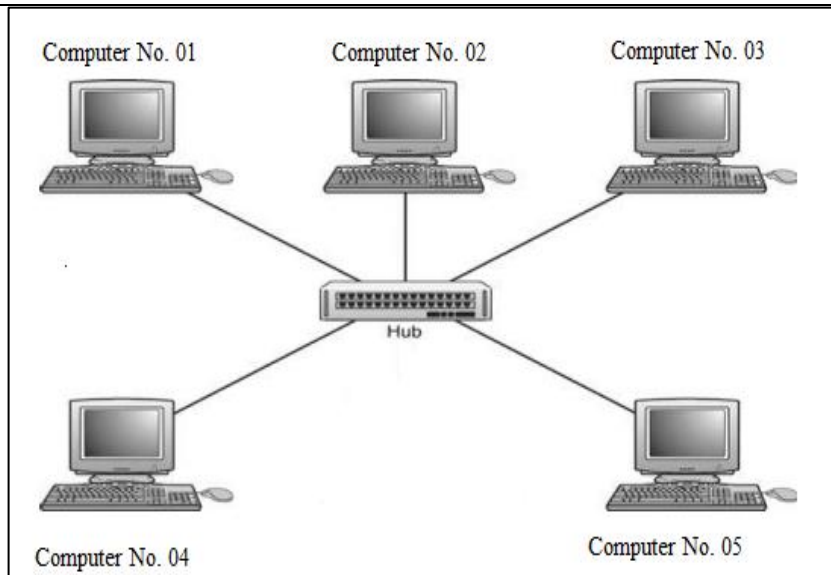
- E-mail is extremely valuable and important feature for communication within organization or outside the people in word.
- E-mail service can be used by user in two different ways:



	<p>a. File based b. Client server.</p> <ul style="list-style-type: none">● File based e-mail system is consists of a set of files kept in a shared location on a server.● File based e-mail system requires gateway server for connecting or handling the e-mail interface between the two system using gateway software that is part of the file based e-mail system.● In a Client-server e-mail system, an e-mail server contains the message and handles all incoming and outgoing mail.● Client-server e-mail systems are more secure and powerful than File based e-mail system.● Advantage:<ol style="list-style-type: none">1. Helpful for communication within a company or outside a company.2. Faster communication.● Disadvantage:<ol style="list-style-type: none">1. Network becomes unreliable due to viruses.2. Require more security mechanism. <p>Remote access:</p> <ul style="list-style-type: none">● Another important service for most networks is remote access to the network users' use this feature to access their files & e-mail.● When they are traveling or working from a remote location such as their homes.● Using this feature user can access their files and e-mail, when they are travelling or working on remote location.● Some of the methods to provide remote access feature can be implemented as follows :<ol style="list-style-type: none">1. Using modem2. Using dial-up mechanism3. Setting up VPN● Advantages:<ol style="list-style-type: none">1. User access their files and e-mails from remote location.2. It enables user's access to centralized application, stored private or shared files on LAN.● Disadvantages:<ol style="list-style-type: none">1. Require more security.2. More hardware or complex hardware required.● Technologies:<ol style="list-style-type: none">1. Public Switched Telephone Network (PSTN).2. Leased line.3. Integrated Services Digital Network (ISDN).4. Cable TV.	
--	--	--



5. Digital Subscriber Line (DSL).		
b	State the functions of i. Repeater ii. Switch iii. Gateway iv. Bridges	4 M
Ans	i) Repeater: Repeaters are used to take the distorted, weak and corrupt input signal and regenerate this signal at its output. It ensures that the signals are not distorted or weak before it reaches the destination. It increases the signal strength. ii) Switch: A switch is a small hardware device that joins multiple computers together within one Local Area Network (LAN). Network switches operate at Data Link Layer of the OSI model. A switch is device that provides a central connection point for cables from workstations, servers and peripherals. iii) Gateway: It is a device which connects two different dissimilar networks which has similar function of communication. It is also called as protocol convertor. It works in all layers of OSI model. iv) Bridge: A bridge device filters data traffic at a network boundary. Bridges reduces the amount of traffic on a LAN by dividing it into two segments. It inspects incoming traffic and decides whether to forward or discard it. It sends packets between two networks of same type.	2 Functions of each component : ½ M each
c	It is desired to connect five computers that are joined at a single point called central node. i) Draw the setup. ii) Name the topology. iii) State two advantages and disadvantages of this topology.	4 M
Ans	i. Setup:	Draw setup : 1M, Name of topology : 1 M, any 2 Advantages and disadvantages : 1/2 M each



ii. Name of topology: Star topology

iii. Advantages of Star Topology

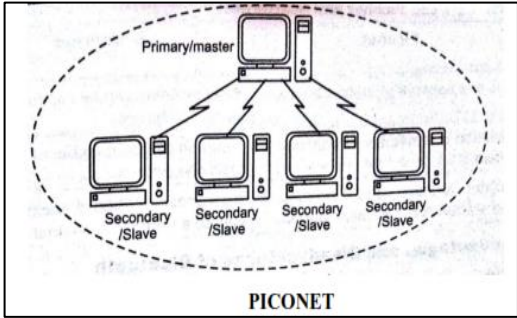
- 1) As compared to Bus topology it gives far much better performance, signals don't necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.
- 2) Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.
- 3) Centralized management. It helps in monitoring the network.
- 4) Failure of one node or link doesn't affect the rest of network. At the same time, it is easy to detect the failure and troubleshoot it.

Disadvantages of Star Topology

- 1) Too much dependency on central device has its own drawbacks. If it fails whole network goes down.
- 2) The use of hub, a router or a switch as central device increases the overall cost of the network.
- 3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.

2	Attempt any FOUR :	16 M
a	State the need for computer networks.	4 M
Ans	Need for computer network: <ul style="list-style-type: none"> • File/Folder Sharing • Hardware Sharing (Resource sharing) • Application sharing • User Communication (Email, Remote Access) 	Any 4 need : 1M each
b	Compare peer to peer network and server based networks.	4 M



Ans	Peer to Peer Network	Server Based Network	Any 4 points : 1M each
	It is a decentralized management	It is centralized management	
	It is easy to set up & no administrator required	It is complex to set up & required professional administrator.	
	Network operating system is not required.	Very reliable dedicated Network operating system is required.	
	It does not give better performance for large number of users.	It gives better performance for large number of users.	
	In this each machine has same power	In this Server has more power & client has less power.	
	Uses less expensive computer hardware.	It is hardware intensive.	
c	Explain the architecture of Bluetooth technology with suitable diagram.		4 M
Ans	<p>Bluetooth is short range wireless technology. Range of Bluetooth is 10 meters. Bluetooth Architecture defines 2 types of networks.</p> <p>1)Piconet 2)Scatternet</p> <p>Piconet: - It is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes. It can have 8 active nodes within the distance of 10 meter. Communication between primary and secondary can be one-to-one or one-to-many. All communication is between master and slave. There can be only one primary or master station in each piconet.</p> <div style="text-align: center;">  <p>PICONET</p> </div> <p>Scatternet: - Scatternet is formed by combining various piconets. Slave in one piconet acts as a master or primary in other piconet. A node can receive messages from master in first piconet and deliver the messages to its slave in other piconet where it is acting as master. This node is called bridge slave. This node cannot be the master of two piconets.</p>		Piconet explanation with diagram : 2M, Scatternet explanation with diagram : 2M



	d	Explain handoff procedure in mobile communication.	4 M
	Ans	<p>Assume that there is a call going on between two parties over a voice channel. When the mobile unit moves out of coverage area of a particular cell site the reception becomes weak. Then the cell site will request a hand off. The system will switch the call to a new cell site without interrupting the call or changing the user. This procedure is called as the hand off procedure or handover procedure.</p> <p>Following are various types of handoffs. Supported by a Mobile Station (MS):</p> <ol style="list-style-type: none"> 1. Hard Hand Off 2. Soft Hand off 3. Queued hand off 4. Delayed hand off 5. Forced hand off <p>1. Hard hand off: A hard handoff is a handoff technique used with cellular networks that requires the user's connection to be entirely broken with an existing base station before being switched to another base station.</p> <p>2. Soft hand off: The hand off is known as soft handoff if the MS starts communication with a new base station without stopping the communication with the older base station.</p> <p>3. Delayed Hand off: In many situations, instead of one level, a two level handoff procedure is used, in order to provide a high opportunity for a successful handoff. A hand off can be delayed if on available cell take the call.</p> <p>4. Forced handoff: A forced handoff is defined as the off which would normally occur but prevented from happening or a handoff that should not occur but is forced to happen.</p> <p>5. Queued handoff: In the queued handoff process, the MTSO arranges the handoff requests in a queue instead of rejecting them, if the new cell sites are busy.</p>	<p>Handoff Procedure : 2M, Types of Handoff : 2M</p>
	e	Compare LAN, WAN and MAN. (four points)	4 M
	Ans		<p>Any 4 points : 1M each</p>



		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%;">BASIS OF COMPARISON</th> <th style="width: 25%;">LAN</th> <th style="width: 25%;">MAN</th> <th style="width: 25%;">WAN</th> </tr> </thead> <tbody> <tr> <td>Expands to</td> <td>Local Area Network</td> <td>Metropolitan Area Network</td> <td>Wide Area Network</td> </tr> <tr> <td>Area</td> <td>A network that connects a group of computers in a small geographical area.</td> <td>It covers relatively large region such as cities, towns.</td> <td>It spans large locality and connects countries together. Example Internet.</td> </tr> <tr> <td>Ownership of Network</td> <td>Private</td> <td>Private or Public</td> <td>Private or Public</td> </tr> <tr> <td>Design and maintenance</td> <td>Easy</td> <td>Difficult</td> <td>Difficult</td> </tr> <tr> <td>Propagation Delay</td> <td>Short</td> <td>Moderate</td> <td>Long</td> </tr> <tr> <td>Speed</td> <td>High, typically 10, 100 and 1000 Mbps</td> <td>High, typically 100 Mbps</td> <td>Slow, about 1.5 Mbps (May vary based on wireless technologies used)</td> </tr> <tr> <td>Fault Tolerance</td> <td>More Tolerant</td> <td>Less Tolerant</td> <td>Less Tolerant</td> </tr> <tr> <td>Congestion</td> <td>Less</td> <td>More</td> <td>More</td> </tr> <tr> <td>Used for</td> <td>College, School, Hospital.</td> <td>Small towns, City.</td> <td>Country/Continent.</td> </tr> </tbody> </table>	BASIS OF COMPARISON	LAN	MAN	WAN	Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network	Area	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.	Ownership of Network	Private	Private or Public	Private or Public	Design and maintenance	Easy	Difficult	Difficult	Propagation Delay	Short	Moderate	Long	Speed	High, typically 10, 100 and 1000 Mbps	High, typically 100 Mbps	Slow, about 1.5 Mbps (May vary based on wireless technologies used)	Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant	Congestion	Less	More	More	Used for	College, School, Hospital.	Small towns, City.	Country/Continent.	
BASIS OF COMPARISON	LAN	MAN	WAN																																								
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network																																								
Area	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.																																								
Ownership of Network	Private	Private or Public	Private or Public																																								
Design and maintenance	Easy	Difficult	Difficult																																								
Propagation Delay	Short	Moderate	Long																																								
Speed	High, typically 10, 100 and 1000 Mbps	High, typically 100 Mbps	Slow, about 1.5 Mbps (May vary based on wireless technologies used)																																								
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant																																								
Congestion	Less	More	More																																								
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.																																								
f	State four features of Wi-Fi.			4 M																																							
Ans	Wi-Fi 1. Wi-Fi stands for wireless fidelity. 2. Wi-Fi typically provides local network access for around a few hundred feet with speeds of up to 54 Mbps. 3. Wi-Fi based on IEEE 802.11 standards. 4. High Capacity Load Balancing 5. Scalability 6. Network Management System			Any 4 Features : 1M each																																							



		7. Role Based Access Control 8. Indoor as well as Outdoor coverage options 9. Ability to Measure Performance 10. Network Access Control Web Content/Application Filtering 11. Mobile Device Management	
3		Attempt any FOUR :	16 M
	a	Explain TELNET.	4 M
	Ans	<p>1. Telnet is the joint abbreviation of Telecommunications and Networks and it is a networking protocol best known for UNIX platform. Telnet uses the port 23 and it was designed specifically for local area networks.</p> <p>2. Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely.</p> <p>3. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.</p> <p>4. Telnet is not a secure communication protocol because it does not use any security mechanism and transfers the data over network/internet in a plain-text form including the passwords and so any one can sniff the packets to get that important information.</p> <p>5. There are no authentication policies & data encryption techniques used in telnet causing huge security threat that is why telnet is no longer used for accessing network devices and servers over public network.</p>	Any relevant answer : 4M
	b	State any four selection criteria of a network topology.	4 M
	Ans	<p>1. Size of network: Size of network varies according to the company requirement and budget.</p> <p>2. Configuration & Installation: This process should be simple & easy.</p> <p>3. Adding new devices: Adding new nodes to the network topology should be easy & it should not affect the other nodes.</p> <p>4. Fault identification: Fault should be easily recognizable and proper remedy should be Available.</p> <p>5. Type of network: for instance hybrid topology is more applicable to larger network like Internet while duo ring topology can be applied in Wide Area Network (WAN).</p> <p>6. Reliability of the topology: hybrid topology seems to be more reliable as</p>	Any 4 correct points : 1M for each



	<p>compared to ring, because in ring topology failure in any of the host leads to stoppage of the whole network topology.</p> <p>7. Geographical span: point to point topology can be applied to network spanning smaller areas like the LAN and PAN while ring topology can be applied to WANs.</p>	
c	Explain Encapsulation.	4 M
Ans	<p>1. In computer networking, the term encapsulation is used to refer to the process of each layer at the sending computer adding its own header information, in the form of metadata to the actual payload (data) To satisfy all the requirements, the protocols operating at the various layers work together to supply a unified quality of service</p> <div style="text-align: center; border: 1px solid black; padding: 10px; margin: 10px auto; width: fit-content;"> </div> <p>2. In a typical transaction, an application layer protocol (which includes presentation and session layer functions) generates a message that is passed down to a transport layer protocol.</p> <p>3. The protocol at the transport layer has its own packet structure, which is known as a protocol data unit (PDU).</p> <p>4. PDU includes specialized header field and a data field that carries the payload.</p> <p>5. The payload is the data received from the application layer protocol.</p> <p>6. The transport layer encapsulates the application layer data and then passes it down to the next layer.</p> <p>7. The network layer protocol then receives the PDU from the transport</p>	<p>Diagram : 2M, Explanation : 2M</p>



	<p>layer and encapsulates it within its own PDU by adding a header and using the entire transport layer PDU as its Payload.</p> <p>8. The same process occurs again when the network layer passes its PDU to the data link layer, which adds a header and footer.</p> <p>9. Once it is encapsulated by the data link protocol, the complete packet is then ready to be converted to the appropriate type of signal used by the network medium.</p> <p>10. The final packet consists of original application layer data plus several headers added by the protocol at the succeeding layers.</p>	
d	<p>Name the protocols used in</p> <ol style="list-style-type: none">1.Data link layer2.Network layer3.Transport layer4. Presentation layer.	4 M
Ans	<p>1. The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.</p> <p>Data Link Layer is divided into two sub layers :</p> <ol style="list-style-type: none">1. Logical Link Control (LLC)2. Media Access Control (MAC) <p>The functions of the data Link layer are :</p> <ol style="list-style-type: none">1. Framing.2. Physical addressing:3. Error control4. Flow Control.5. Access control.6. <p>2. Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer.</p>	Each layer : 1M



		<p>The functions of the Network layer are :</p> <ol style="list-style-type: none"> 1. Routing 2. Logical Addressing 3. Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found. <p>The functions of the transport layer are :</p> <ol style="list-style-type: none"> 1. Segmentation and Reassembly 2. Service Point Addressing 4. Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. <p>The functions of the presentation layer are :</p> <ol style="list-style-type: none"> 1. Translation 2. Encryption/ Decryption. 3. Compression 	
	e	Explain network layer of the OSI reference model.	4 M
Ans	<p>The diagram illustrates the Network Layer's role in the OSI model. It shows two vertical paths of data flow. On the left, data flows downwards from 'Data from Transport Layer' through a 'Network Layer' (which handles 'Packets') to 'Data to Data Link Layer'. On the right, data flows upwards from 'Data from Data Link Layer' through a 'Network Layer' (which handles 'Packets') to 'Data to Transport Layer'.</p>		<p>Diagram : 1M, Explanation : 3M</p>
	<p>The network Layer controls the operation of the subnet. The main aim of this layer is to deliver packets from source to destination across multiple links (networks). If two computers (system) are connected on the same link, then there is no need for a network layer. It routes the signal through different channels to the other end and acts as a network controller.</p> <p>It also divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels. In broadcast networks, the routing problem is simple, so the network layer is often thin or even non-existent.</p>		



		Functions of Network Layer		
		<ol style="list-style-type: none"> 1. It translates logical network address into physical address. Concerned with circuit, message or packet switching. 2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination. 3. Connection services are provided including network layer flow control, network layer error control and packet sequence control. 4. Breaks larger packets into small packets. 		
	f	Compare UDP and TCP.		4 M
Ans		Sr.no	TCP	UDP
		1	TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
		2	TCP is reliable as it guarantees delivery of data to the destination router	The delivery of data to the destination cannot be guaranteed in UDP
		3	TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
		4	Sequencing of data is a feature of Transmission Control Protocol (TCP). This means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
		5	TCP is comparatively slower	UDP is faster, simpler and more
				Any 4 correct points :1M each



			than UDP.	efficient than TCP.		
		6	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).		
		7	TCP header size is 20 bytes.	UDP Header size is 8 bytes.		
		8	TCP is heavy-weight.	UDP is lightweight.		
		9	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.		
4		Attempt any FOUR :				16 M
	a	Draw the layered architecture of TCP/IP. Explain each layer's function.				4 M
	Ans	<p style="text-align: center;">Protocols and networks in the TCP/IP model:</p> <p>Overview of TCP/IP reference model</p> <p>TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.</p> <p>The features that stood out during the research, which led to making the TCP/IP reference model were:</p>				<p>Diagram : 2M, Explanation : 2M</p>



- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to (send data packets) another application running on different computer.

Different Layers of TCP/IP Reference Model

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
 - Delivering IP packets
 - Performing routing
 - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.



		<p>6. Transport layer also arrange the packets to be sent, in sequence.</p> <p>Layer 4: Application Layer The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.</p> <ol style="list-style-type: none"> 1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it. 2. FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient. 3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route. 4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network. 5. It allows peer entities to carry conversation. 6. It defines two end-to-end protocols: TCP and UDP <ul style="list-style-type: none"> ○ TCP (Transmission Control Protocol): It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control. ○ UDP (User-Datagram Protocol): It is unreliable connectionless protocols that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service. 	
	b	Explain sub netting and super netting.	4 M
	Ans	<p>1. sub netting</p> <ul style="list-style-type: none"> ● Subnetting is a technique of partitioning an individual physical network into several small-sized logical sub-networks. These subnetworks are known as <i>subnets</i>. ● An IP address is made up of the combination of the network segment and a host segment. A subnet is constructed by accepting the bits from the IP address host portion which are then used to assign a number of small-sized sub-networks in the original network. ● The Subnetting basically converts the host bits into the network bits. As mentioned above the subnetting strategy was initially devised for slowing down the depletion of the IP addresses. ● The subnetting permits the administrator to partition a single class A, class B, class C network into smaller parts. VLSM (Variable Length Subnet Mask) is a technique which partitions IP address space into 	<p>Relevant Explanation : (subnetting : 2M, Supernetting : 2M)</p>



subnets of different sizes and prevent memory wastage.

- Furthermore, when the number of hosts is same in subnets that is known as **FLSM (Fixed Length Subnet Mask)**.
- Example.

Subnetted Address : 172.16.32.0/20				
In binary : 10101100.00010000.00100000.00000000				
1st Subnet	172 . 16 . 0010	0000 . 00	000000	= 172.16.32.0/26
2nd Subnet	172 . 16 . 0010	0000 . 01	000000	= 172.16.32.64/26
3rd Subnet	172 . 16 . 0010	0000 . 10	000000	= 172.16.32.128/26
4th Subnet	172 . 16 . 0010	0000 . 11	000000	= 172.16.32.192/26
5th Subnet	172 . 16 . 0010	0001 . 00	000000	= 172.16.33.0/26

Changing bits

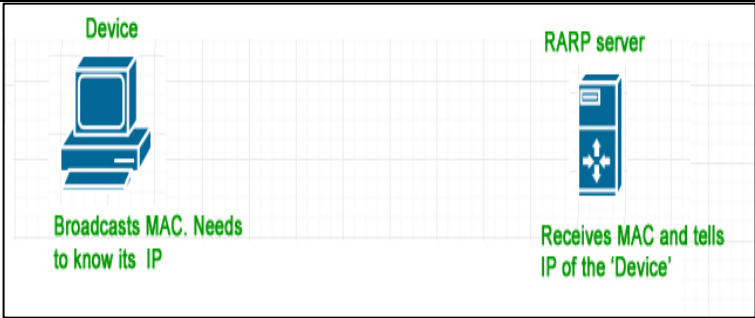
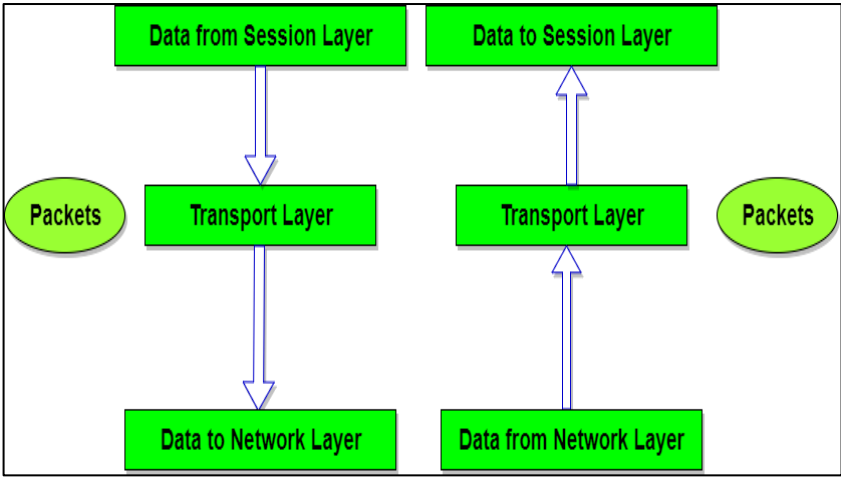
2. Super netting

- **Supernetting** is inverse process of subnetting, in which several networks are merged into a single network. While performing supernetting, the mask bits are moved toward the left of the default mask.
- The supernetting is also known as **router summarization** and **aggregation**. It results in the creation of more host addresses at the expense of network addresses, where basically the network bits are converted into host bits.
- The supernetting is performed by internet service provider rather than the normal users, to achieve the most efficient IP address allocation.
- **CIDR (Classless Inter-Domain Routing)** is scheme used to route the network traffic across the internet. CIDR is a supernetting technique where the several subnets are combined together for the network routing. In simpler words, CIDR allows the IP addresses to be organized in the subnetworks independent of the value of the addresses.
- Example



		<p>Supernetting Address : 172.16.168.0/24 In binary : 10101100.00010000.10101000.00000000</p> <table border="1" style="margin: auto; border-collapse: collapse;"> <tr> <td style="padding: 2px;">172.16.168.0/24</td> <td style="padding: 2px;">172 . 16 . 10101</td> <td style="padding: 2px;">000</td> <td style="padding: 2px;">00000000</td> </tr> <tr> <td style="padding: 2px;">172.16.169.0/24</td> <td style="padding: 2px;">172 . 16 . 10101</td> <td style="padding: 2px;">001</td> <td style="padding: 2px;">00000000</td> </tr> <tr> <td style="padding: 2px;">172.16.170.0/24</td> <td style="padding: 2px;">172 . 16 . 10101</td> <td style="padding: 2px;">010</td> <td style="padding: 2px;">00000000</td> </tr> <tr> <td style="padding: 2px;">172.16.171.0/24</td> <td style="padding: 2px;">172 . 16 . 10101</td> <td style="padding: 2px;">011</td> <td style="padding: 2px;">00000000</td> </tr> <tr> <td style="padding: 2px;">172.16.172.0/24</td> <td style="padding: 2px;">172 . 16 . 10101</td> <td style="padding: 2px;">100</td> <td style="padding: 2px;">00000000</td> </tr> </table> <p style="text-align: center; margin-top: 5px;"> Number of common bits = 21 Non-common bits = 11 </p>	172.16.168.0/24	172 . 16 . 10101	000	00000000	172.16.169.0/24	172 . 16 . 10101	001	00000000	172.16.170.0/24	172 . 16 . 10101	010	00000000	172.16.171.0/24	172 . 16 . 10101	011	00000000	172.16.172.0/24	172 . 16 . 10101	100	00000000	
172.16.168.0/24	172 . 16 . 10101	000	00000000																				
172.16.169.0/24	172 . 16 . 10101	001	00000000																				
172.16.170.0/24	172 . 16 . 10101	010	00000000																				
172.16.171.0/24	172 . 16 . 10101	011	00000000																				
172.16.172.0/24	172 . 16 . 10101	100	00000000																				
c	State the performance Characteristics of coaxial cable and twisted pair cable.	4 M																					
Ans	<p>1.Twisted pair</p> <ol style="list-style-type: none"> 1.Attenuation for twisted pair is a very strong function of frequency 2. Twisted cable has a lower bandwidth up to about 250 kHz 3. Analog signals, amplifiers are required about every 5 to 6 km. 4.digital signals, repeaters are required every 2 or 3 km 5.The medium is quite susceptible to interference and noise 6.data rates of up to 100 Mbps <p>2.Coaxial Cable</p> <ol style="list-style-type: none"> 1. Attenuation is much higher in coaxial cables. 2. coaxial cable has a much higher bandwidth, 3. It has higher frequency and data rate. 4. Coaxial cable is much less susceptible to interference and crosstalk. 5. Requires the frequent use of repeaters. 6. Long-distance transmission of analog signals, amplifiers is needed every few kilometers, with closer spacing required if higher frequencies are used. 7.The usable spectrum for analog signaling extends to about 400 MHz. 	<p>Twisted pair (any 2 point:1M each), Coaxial (any 2 point: 1M each)</p>																					
d	Explain working of ARP and RARP.	4 M																					

Ans	<p>1. Address Resolution Protocol (ARP) –</p> <p>Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.</p> <div style="text-align: center; border: 1px solid black; padding: 10px; margin: 10px auto; width: fit-content;"> </div> <p>In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.</p> <p>Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.</p> <p>2. Reverse Address Resolution Protocol (RARP) –</p> <p>Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.</p> <p>When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.</p>	Any Relevant Diagram : 2M, Explanation : 2M
------------	--	---

		 <p style="text-align: center;">A special host configured inside the local area network, called as RARP-server is responsible to reply for these kinds of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server sends the response packet to the requesting device along with IP address.</p> <ul style="list-style-type: none"> ● LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol. ● RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP (Dynamic Host Configuration Protocol). 	
e	State the services provided by the transport layer of OSI reference model.		4 M
Ans	 <p style="text-align: center;">The basic function of the Transport layer is to accept data from the layer above, split it up into smaller units, pass these data units to the Network layer, and ensure that all the pieces arrive correctly at the other end.</p>		<p>Diagram : 2M, Explanation : 2M</p>



	<p>Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology.</p> <p>The Transport layer also determines what type of service to provide to the Session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent.</p> <p>The Transport layer is a true end-to-end layer, all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages.</p> <p>Functions of Transport Layer</p> <ol style="list-style-type: none">1. Service Point Addressing: Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.2. Segmentation and Reassembling: A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.3. Connection Control: It includes 2 types:<ul style="list-style-type: none">○ Connectionless Transport Layer: Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.○ Connection Oriented Transport Layer: Before delivering packets, connection is made with transport layer at the destination machine.4. Flow Control: In this layer, flow control is performed end to end.5. Error Control: Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.	
f	Explain the various components of computer network.	4 M
Ans	Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), local operating system(LOS), and the network operating system (NOS).	Any 4 components: 1M each



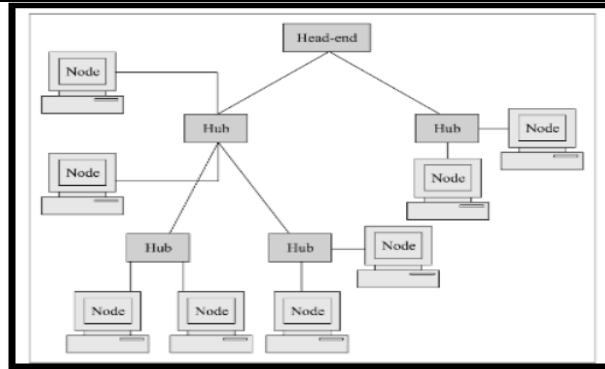
	<ul style="list-style-type: none">● Servers - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers, to name a few.● Clients - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive services from the servers.● Transmission Media - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.● Shared data - Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.● Shared printers and other peripherals - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.● Network Interface Card - Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.● Local Operating System - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, UNIX, Linux, Windows 2000, Windows 98, Windows XP etc.● Network Operating System - The network operating system is a program that runs on computers and servers that allows the computers to communicate over the network.● Hub - Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer requests information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.● Switch - Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or	
--	--	--



		<p>port. Unlike a hub, switch doesn't broadcast the received message to entire network; rather before sending it checks to which system or port should the message be sent. In other words, switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.</p> <ul style="list-style-type: none"> ● Router - When we talk about computer network components, the other device that used to connect a LAN with an internet connection is called Router. When you have two distinct networks (LANs) or want to share a single internet connection to multiple computers, we use a Router. In most cases, recent routers also include a switch which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks. There are two types of Router: wired and wireless. The choice depends on your physical office/home setting, speed and cost. ● LAN Cable A local area Network cable is also known as data cable or Ethernet cable which is a wired cable used to connect a device to the internet or to other devices like other computer, printers, etc. 															
5		Attempt any FOUR :	16 M														
	a	Compare OSI and TCP/IP network model.	4 M														
	Ans	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%; text-align: center;">OSI</th> <th style="width: 50%; text-align: center;">TCP/IP</th> </tr> </thead> <tbody> <tr> <td>1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.</td> <td>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.</td> </tr> <tr> <td>2. In OSI model the transport layer guarantees the delivery of packets.</td> <td>2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.</td> </tr> <tr> <td>3. Follows vertical approach.</td> <td>3. Follows horizontal approach.</td> </tr> <tr> <td>4. OSI model has a separate Presentation layer and Session layer.</td> <td>4. TCP/IP does not have a separate Presentation layer or Session layer.</td> </tr> <tr> <td>5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.</td> <td>5. TCP/IP model is, in a way implementation of the OSI model.</td> </tr> <tr> <td>6. Network layer of OSI model provides both connection oriented and connectionless service.</td> <td>6. The Network layer in TCP/IP model provides connectionless service.</td> </tr> </tbody> </table>	OSI	TCP/IP	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. Still the TCP/IP model is more reliable.	3. Follows vertical approach.	3. Follows horizontal approach.	4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.	5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.	6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.	<p>For any 4 correct points : 1M each</p>
OSI	TCP/IP																
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. Still the TCP/IP model is more reliable.																
3. Follows vertical approach.	3. Follows horizontal approach.																
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.																
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.																
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. 8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	7. TCP/IP model does not fit any protocol. 8. In TCP/IP replacing protocol is not easy.	
	b	Explain Bus topology and Tree topology with a neat sketch.		4 M
Ans	<p><u>BUS TOPOLOGY:-</u> <u>Diagram:-</u></p> <div style="text-align: center;"> <p style="text-align: center;">Bus Topology</p> </div> <p><u>Working:-</u></p> <ol style="list-style-type: none"> 1. Bus topology is a network setup in which each computer and network device are connected to a single cable or backbone by the help of interface connectors. 2. This central cable is the backbone of the network and is known as Bus. 3. Every workstation communicates with the other device through this Bus. 4. A signal from the source is broadcasted and it travels to all workstations connected to bus cable. 5. Although the message is broadcasted but only the intended recipient, whose MAC address or IP address matches, accepts it. 6. If the MAC /IP address of machine doesn't match with the intended address, machine discards the signal. 7. A terminator is added at ends of the central cable, to prevent bouncing of signals. 8. A barrel connector can be used to extend it. <p><u>TREE TOPOLOGY:-</u> <u>Diagram:-</u></p>			Bus Topology Diagram: 1M, Working: 1M, Tree Topology Diagram: 1M, Working: 1M



Working:-

1. A tree topology is cascading of star.
2. As in a star, nodes in a tree are linked to a central hub head end that controls the traffic to a network. However, not every computer plugs into the central hub, majority of them are connected to a secondary hub which in turn is connected to the central hub as shown in fig.
3. The central hub head is either a switch or a router.
4. The central hub contains a repeater, which looks at the incoming bits and 99 regenerates them afresh as full blown signals for 0 or 1 as per case.
5. This allows the digital signals to traverse over longer distances.
6. Therefore, the central hub is also called active hub.
7. The tree topology also contains many secondary hubs, which may be active hubs or passive hubs.

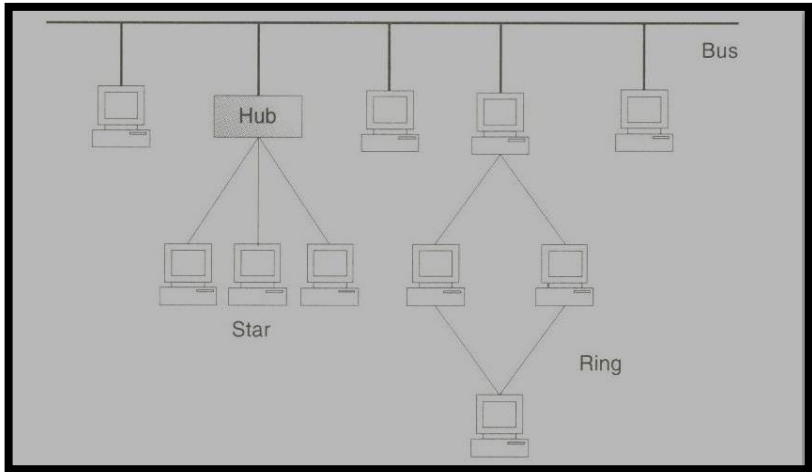
c	Explain the construction of fiber optic cable with suitable diagram.	4 M
Ans		<p>Diagram : 2M, Explanation : 2M</p>

		<p><u>Construction:-</u></p> <ol style="list-style-type: none"> 1. As shown in the figure, at the center is the glass core through which the light propagates. In multimode fibers, the core is typically 50 microns in diameter. 2. In single mode fibers, the core is 8 to 10 microns. 3. The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core. 4. A thin plastic jacket is used to protect the cladding. Fibers are grouped in bundles, protected by an outer sheath. 5. Fibers can be connected in three different ways. First they can terminate in connectors and be plugged into fiber sockets. 6. Connectors lose about 10 to 20 percent of the light, but they make it easy to reconfigure systems. Second they can be spliced mechanically. 7. Mechanical splices just lay the two carefully – cut ends next to each other in a special sleeve and clamp them in place. 8. Alignment can be improved by passing light through the junction and then making small adjustments to maximize the signal. 9. Third, two pieces of fiber can be fused to form a solid connection. 10. A fusion splice is almost as good as a single drawn fiber. 	
	d	State the function of modem. Enlist its types. Where are they used in a computer network?	4 M
Ans		<p><u>Functions:-</u></p> <ol style="list-style-type: none"> 1. Modem works as modulator as well as demodulator. 2. Modem converts analog signal to digital signal and vice versa. 3. In case of networking data has to be transferred from one location to another location. 4. At present to transfer such data whatever the infrastructure (PSTN) is available it is of analog technology but computer sends digital data to transfer this data to another location it is needed to convert into analog format so that it can be transferred by using currently available infrastructure. <div style="text-align: center; border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="font-size: small; text-align: center;">Signal corrupted by noise</p> </div> <p><u>Types of modem:-</u></p> <ul style="list-style-type: none"> • Modems can be of several types and they can be categorized in a number of ways. • Categorization is usually based on the following basic modem 	<p>Functions : 2M, Types : 1M, Used in : 1M, (diagram: optional)</p>

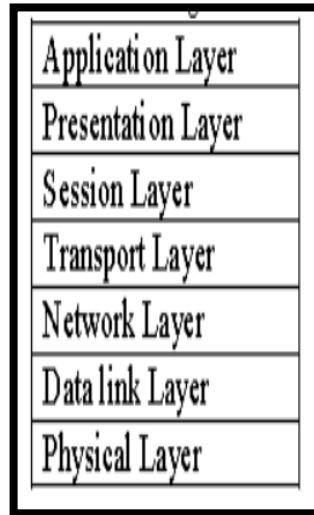


		<p>features:</p> <ol style="list-style-type: none"> 1. Directional capacity: half duplex modem and full duplex modem. 2. Connection to the line: 2-wire modem and 4-wire modem. 3. Transmission mode: asynchronous modem and synchronous modem. <p><u>Situations where modems are used:-</u></p> <ol style="list-style-type: none"> 1. Modems are used when digital signal is sent over analog medium. 2. When the data transmission is over an analog medium such as telephone lines, Modem is used for converting analog signal to digital signal. 3. When a home user need to connect to ISP a modem is used to connect to telephone lines. 4. Or when user wants to connect internet by telephone line. 																										
	e	Draw the sketch of IP packet frame format in IPv4 and explain.	4 M																									
Ans	<p>IPv4 header: The IP datagram contains header and data. The header consists of around 20 to 60bytes consists of information about routing and delivery. The header is like an envelope i.e., it contains information about the data. The structure of the standard format is as shown below.</p> <div style="text-align: center; border: 2px solid black; padding: 10px; margin: 10px auto; width: fit-content;"> <table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="text-align: center;">Version (4 Bits)</td> <td style="text-align: center;">HLEN (4 bits)</td> <td style="text-align: center;">Service Type (ToS) (8 Bits)</td> <td colspan="2" style="text-align: center;">Total Length (16 bits)</td> </tr> <tr> <td colspan="3" style="text-align: center;">Identification (16 bits)</td> <td style="text-align: center;">Flags (3bits)</td> <td style="text-align: center;">Fragmentation offset (13 bits)</td> </tr> <tr> <td style="text-align: center;">Time to Live (TTL) (8 bits)</td> <td style="text-align: center;">Protocol (8 bits)</td> <td colspan="3" style="text-align: center;">Header Checksum (16 bits)</td> </tr> <tr> <td colspan="5" style="text-align: center;">Source IP address (32 bits)</td> </tr> <tr> <td colspan="5" style="text-align: center;">Destination IP address (32 bits)</td> </tr> </table> </div> <p>The various fields are as described below:</p> <ol style="list-style-type: none"> 1. Version: This field identifies the version of IP, which contains a value 4, which indicates IP version 4. It may contain 6 for IPv6 2. Header length (HLEN): This indicates the size of the header in a multiple of 4 byte words. When the header size is 20 bytes, HLEN = 5, and HLEN = 15 when maximum size (60 bytes). 3. Service Type (Type of Service): This field is used to define service parameters such as the priority of the datagram and the level of reliability desired. 4. Total Length: This field contains the total length of the IP datagram. IP datagram cannot be more than 65,536 since this filed size is 2 bytes or 16 (216 = 65,536). 5. Identification: This field is used in the situations when a datagram is 		Version (4 Bits)	HLEN (4 bits)	Service Type (ToS) (8 Bits)	Total Length (16 bits)		Identification (16 bits)			Flags (3bits)	Fragmentation offset (13 bits)	Time to Live (TTL) (8 bits)	Protocol (8 bits)	Header Checksum (16 bits)			Source IP address (32 bits)					Destination IP address (32 bits)					<p>Packet Format : 2M, Explanation: 2M</p>
Version (4 Bits)	HLEN (4 bits)	Service Type (ToS) (8 Bits)	Total Length (16 bits)																									
Identification (16 bits)			Flags (3bits)	Fragmentation offset (13 bits)																								
Time to Live (TTL) (8 bits)	Protocol (8 bits)	Header Checksum (16 bits)																										
Source IP address (32 bits)																												
Destination IP address (32 bits)																												



	<p>fragmented. The sub datagram are sequenced using identification field so that later it can be used to reconstruct the original datagram.</p> <ol style="list-style-type: none">6. Flags: This field corresponds to identification field. It indicates whether a datagram can be fragmented and if fragmented, the position of the fragment (first, last or middle).7. Fragmentation Offset: If a datagram is fragmented, this field indicates the offset of the data in the original datagram before segmentation. This is used while reconstructing.8. Time to Live (TTL): This field is initialized by some value and decremented each time it passes through routers. If the value becomes zero or negative, the data is not forwarded. Thus it decides the lifetime of the data.9. Protocol: This field identifies the transport protocol running on top of IP. The upper layer software piece can be TCP or UDP. This field specifies which piece of software at the destination node the datagram should be passed on to.10. Source address: This field contains the 32 bit IP address of the sender.11. Destination address: This field contains the 32 bit IP address of the final destination.	
f	Draw a diagram of any hybrid topology. Explain.	4 M
Ans	<div style="text-align: center;"></div> <p style="text-align: center;">OR</p>	<p>Diagram : 2M, Explanation : 2M **Note:-any relevant diagram and explanation shall be considered</p>

		<p>Explanation:-</p> <ol style="list-style-type: none"> 1. Hybrid topology is one that uses two or more basic topologies together the above figure depict this. 2. In this case, the bus, star & ring topologies are used to create this hybrid topology. There are multiple ways in which this can be created. 3. The hybrid topology which is to be used for a particular application depends on the requirements of that application. 4. In practice, many networks are quite complex but they can be reduced to some form of hybrid topology. 	
6		Attempt any TWO :	16 M
	a	Draw the seven layered architecture of OSI reference model. State the function of each layer.	8 M
	Ans	<p>OSI model (open system interconnection) model was developed by ISO (international standard organization)</p> <p>Function of OSI model:</p> <ol style="list-style-type: none"> i. It provides way to understand how internetwork operates. ii. It gives guideline for creating network standard. <p>OSI model has 7 layers as shown in the figure.</p> <p>OSI model has following 7 layers as Physical layer, data link layer, Network layer, Transport layer, session layer, presentation layer, application layer.</p>	<p>Diagram : 2M, Functions of layers : 6M</p>



1. Physical layer:

It co-ordinates the functions required to transmit bit stream over physical medium. It deals with mechanical and electrical specifications of interface and transmission medium. For transmission it defines procedures and functions that devices and transmission medium has to perform

- i. Physical characteristics of interfaces and media.
- ii. Representation of bits: Data rate (transmission rate).
- iii. Synchronization of bits.
- iv. Line configuration: Point to point or multipoint configuration should be used.

2. Data link layer: It is responsible for transmitting group of bits between the adjacent nodes. The group of bits is called as frame. The network layer passes a data unit to the data link layer. Header and trailer is added to the data unit by data link layer. This data unit is passed to the physical layer. Data link layer is responsible for moving frames from one node to the next.

Functions of data link layer are:

- i. Framing
- ii. Physical addressing
- iii. Flow control
- iv. Error control
- v. Media access control
- vi. 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 e to destination delivery of individual packets across multiple networks. It ensures that packet is

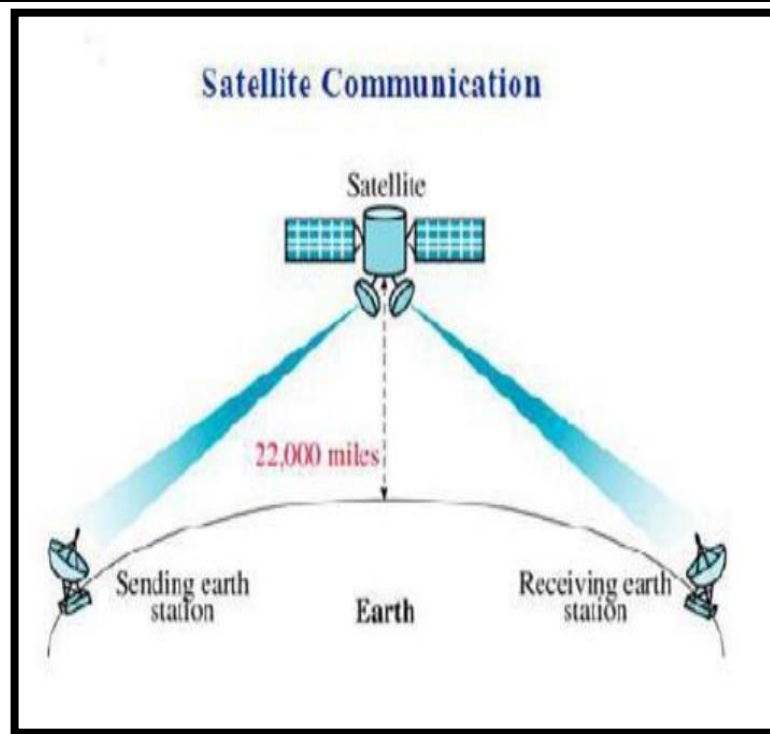


	<p>delivered from point of origin to destination.</p> <p>Functions of network layer:</p> <ol style="list-style-type: none">i. logical addressingii. Routing.iii. Congestion controliv. Accounting and billingv. Address transformationvi. Source host to destination host error free delivery of packet. <p>4. Transport layer: Responsibility of process to process delivery of message Ensure that whole message arrives in order.</p> <p>Functions of Transport layer:</p> <ol style="list-style-type: none">i. Service point addressingii. Segmentation and reassemblyiii. Connection controliv. Flow control: Flow control is performed end to endv. Error control <p>5. Session layer: Establishes, maintains, and synchronizes the interaction among communication systems It is responsible for dialog control and synchronization.</p> <p>Functions of Session layer:</p> <ol style="list-style-type: none">i. Dialog controlii. Synchronization, session and sub sessioniii. Session closure <p>6. Presentation layer: It is concerned with syntax, semantics of information exchanged between the two systems.</p> <p>Functions of Presentation layer:</p> <ol style="list-style-type: none">i. Translation: presentation layer is responsible for converting various formats into required format of the recipientii. Encryption: Data encryption and decryption is done by presentation layer for security.iii. Compression and Decompression: data to be transform compressed while sending and decompress while receiving for reducing time of transmission. <p>7. Application layer: It enables user to access the network. It provides user interfaces and support for services like email, remote file access.</p> <p>Functions of Application layer:</p>	
--	---	--

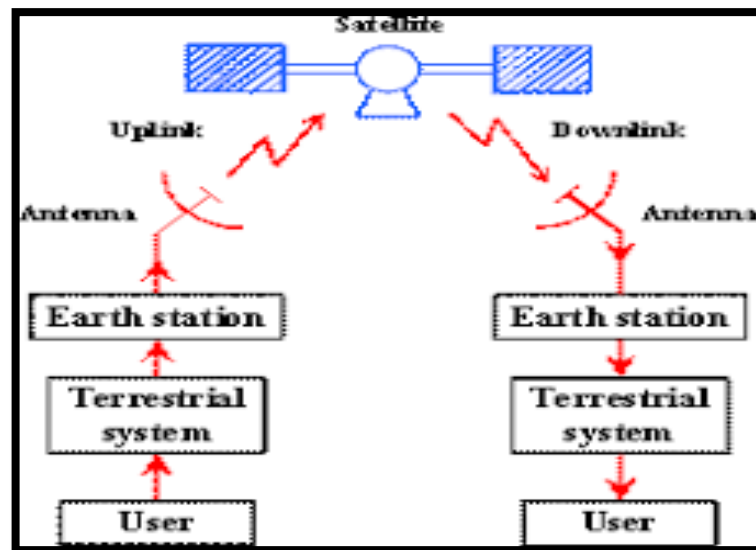
		i. Network virtual terminal ii. file transfer access and management iii. mail services and directory services	
b	Explain the application layer protocols with block diagram : i. FTP ii. SMTP		8 M
Ans	i) FTP <u>Diagram:-</u> <div style="text-align: center;"> </div> <u>Explanation:-</u> <ol style="list-style-type: none"> 1. File Transfer Protocol (FTP) is the standard mechanism provided by <i>TCP/IP</i> for copying a file from one host to another. Figure shows the basic model of FTP. 2. The client has three components: user interface, client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. 3. The control connection is made between the control processes. The data connection is made between the data transfer processes. 4. The control connection remains connected during the entire interactive FTP session. 5. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred. 6. Separation of commands and data transfer makes FTP more efficient. FTP uses the services of TCP. It needs two TCP connections. 7. FTP uses two well-known TCP ports: Port 21 and Port 20. ii) SMTP <u>Diagram:-</u>		FTP :- Explanation : 2M, Diagram : 2M; SMTP:- Explanation : 2M, Diagram : 2M



	<div style="text-align: center;"> </div> <p>Explanation:-</p> <ol style="list-style-type: none"> 1. It is Simple Mail transfer Protocol. 2. It is connection oriented text based protocol in which sender communicates with receiver using a command and supplying data over reliable TCP connection. 3. SMTP is standard application layer protocol for delivery of email over TCP/IP network. 4. SMTP establish a TCP connection between Sender And port number 25 of receiver. 5. It is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP that let the user save messages in a server mailbox and download them periodically from the server. 	
c	<p>Draw the block diagram of satellite communication system and explain in brief. State any four frequency bands used for satellite communication.</p>	8 M
Ans	<p>SATELLITE COMMUNICATION:</p> <ol style="list-style-type: none"> 1. In satellite communication, signal transferring between the sender and receiver is done with the help of satellite. 2. In this process, the signal which is basically a beam of modulated microwaves is sent towards the satellite called UPLINK (6 GHz). 3. Then the satellite amplifies the signal and sent it back to the receiver's antenna present on the earth's surface called as DOWNLINK (4Ghz), as shown in the diagram given 	<p>Explanation : 4M, any relevant diagram : 2M, frequency bands : 2M</p>

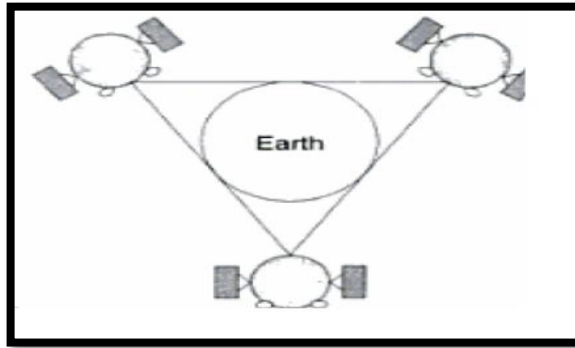


OR

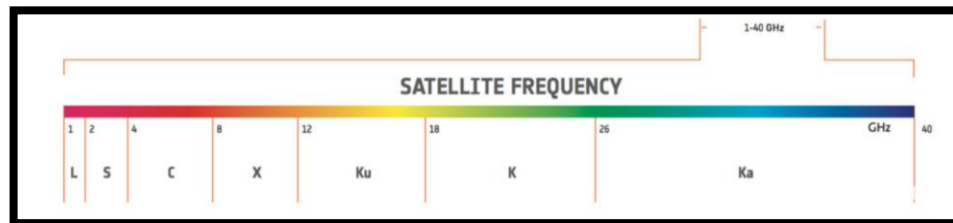


4. As the entire signal transferring is happening in space. Thus this type of communication is known as space communication. The satellite does the functions of an antenna and the repeater together. If the earth along with its ground stations is revolving and the satellite is stationary, the sending and receiving earth stations and the satellite can be out of sync over time.
5. Therefore Geosynchronous satellites are used which move at same RPM

- as that of the earth in the same direction.
6. So the relative position of the ground station with respect to the satellite never changes.
 7. However 3 satellites are needed to cover earth's surface entirely.



Frequency band used in satellite communication:



Band	Frequency
L	1-2 GHz
C	4-8 GHz
X	8-12 GHz
Ku	12-18 GHz
Ka	26-40 GHz