WINTER– 16 EXAMINATION
Model Answer

Subject Code: 17429

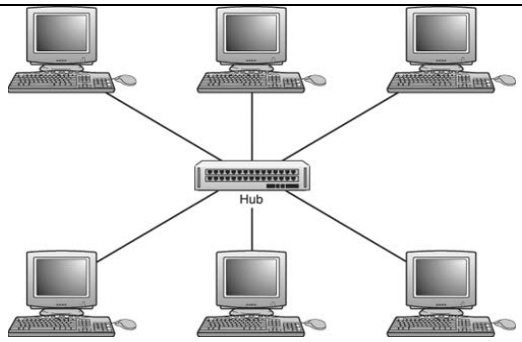
Important Instructions to examiners:

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 Marks**
	(i)	**State the need of computer network.**	**2M**
	Ans:	**Need for computer network:** • File/Folder Sharing • Hardware Sharing (Resource sharing) • Application sharing • User Communication (Email, Remote Access)	**(Any two Each 1 mark)**
	(ii)	**Name any two types of server.**	**2M**
	Ans:	**Types of Servers:** • File and print Servers • Application Servers • Email servers • Networking Servers like DHCP, VPN etc. • Internet Servers like web, internet email, Proxy Server etc. • Remote Access Servers	**(Any two server names Each: 1 mark)**
	(iii)	**Give two criteria for selection of network topologies.**	**2M**

	Ans:	**Selection criteria for selecting network topology:** • Size of the network & number of devices or nodes being connected. • Ease of configuration & installing. • The ease of adding new device in an existing network. • The ease of fault indication & reflection. • Number of physical links required to be used for connecting the devices. • Need of network connecting devices such as repeaters, switches, hubs etc. • Costs of the network. • Based on the security requirement • Need of network administration.	**(Any two criteria Each: 1 mark)**
	(iv)	**State the function of:** **1) Hub** 2) **Router**	**2M**
	Ans:	**Functions of Hub:** • Hub connects all nodes in star topology. Hub is broadcasting device. • It sends packets to all nodes in the network. • It works at Physical Layer of OSI model **Functions of Router:** • Router chooses the best path for packet forwarding. • Router read complex network address in packet. • It works at Network Layer of OSI model • Efficiently direct packets from one network to another, reducing excessive traffic. • Join neighbouring or distant network • Connect dissimilar networks. • Prevent network bottlenecks by isolating portions of a network.	**(Any one function of each device: 1 mark)**
	(v)	**State the frequency band used in cellular telephony for transmission and reception.**	**2M**
	Ans:	• A quad-band GSM phone could use GSM service in the 850-MHz, 900-MHz, 1800-MHz or 1900-MHz band. • GSM operates in the 900-MHz and 1800-MHz bands in Europe and Asia and in the 850-MHz and 1900-MHz band in the United States. • CDMA mobiles operate in **800 MHz** band • In Advanced Mobile Phone System (AMPS) The band between 824 and 849 MHz carries reverse communication; the band between 869 and 894 MHz carrie forward communication	**(Any one Correct frequency band: 2 marks)**

		• A dual-band TDMA phone could use TDMA services in either an 800-MHz or a 1900-MHz system.	
	(vi)	**State four applications of satellite communication.**	**2M**
	Ans:	**Applications of Satellite communications:** • Communication between any points on Earth. • Global Positioning System (GPS) satellites provide time and location information for vehicles and ships. • Used in voice and data communications for handheld terminals. • Used in universal broadband Internet access. • Used in data transmission to remote locations	**(Any four applications: $\frac{1}{2}$ mark)**
	(vii)	**Define Protocol. State the need for the same.**	**2M**
	Ans:	**Protocol** : There are certain rules that must be followed to ensure proper communication & a set of such rules and regulation is known as protocol. **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** Protocol is a system of digital message formats and rules for exchanging those messages in or between computing systems. **Need**: The computers can be physically connected through networking transmission medium and connectivity devices. The communication between two devices or computer can take place only if the two ends agree upon common set of rules and conventions. Hence protocol is essential for communication between two computers or devices.	**(Definition: 1 mark, Need: 1 mark)**
	(viii)	**State two features of IPV6.**	**2M**
	Ans:	**Features of IPv6:** • 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 • It gives greater flexibility in address allocation. • There are three types of addresses in IPv6: unicast, anycast, and multicast.	**(Any two features each: 1 mark)**

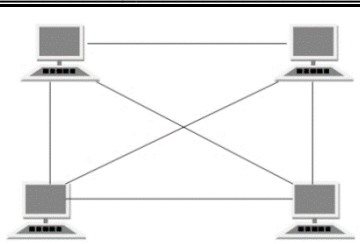
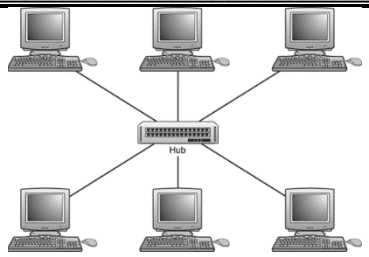
		• In an IPv6 address, the variable type prefix field defines the address type or purpose.	
	b)	**Attempt any TWO of the following:**	**8 Marks**
	(i)	**Name any four resources that can be shared in a computer network.**	**4M**
	Ans:	• Files • Folders or directories • Devices like Printers, modems, Fax cards etc. • Application software	**(Each Resource: 1 mark)**
	(ii)	**Draw a neat diagram and describe the working of star topology.**	**4M**
	Ans:	 **Star Topology:** • In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. • The devices are not directly linked to one another. • A star topology does not allow direct traffic between devices. • The controller acts as an exchange. • If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device. • A star topology is less expensive than a mesh topology. • In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.	**(Diagram: 1 mark, Description: 3 marks)**

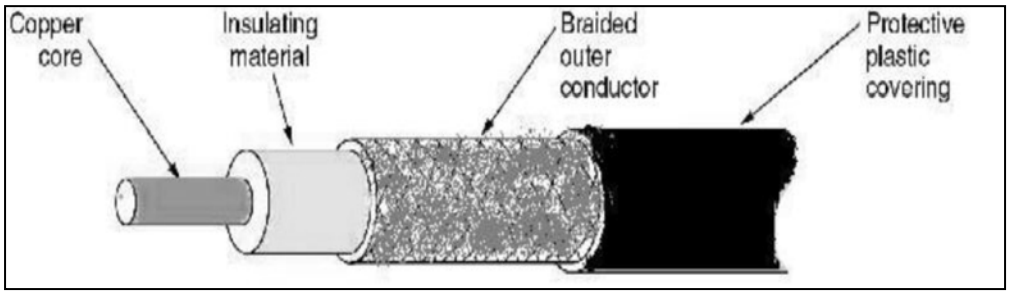
- Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation.
- As long as the hub is working, it can be used to monitor link problems and bypass defective links.
- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub.
- The star topology is used in local-area networks (LANs). High-speed LANs often use a star topology with a central hub.

(iii) **Compare Mesh topology with Star topology.** **4M**

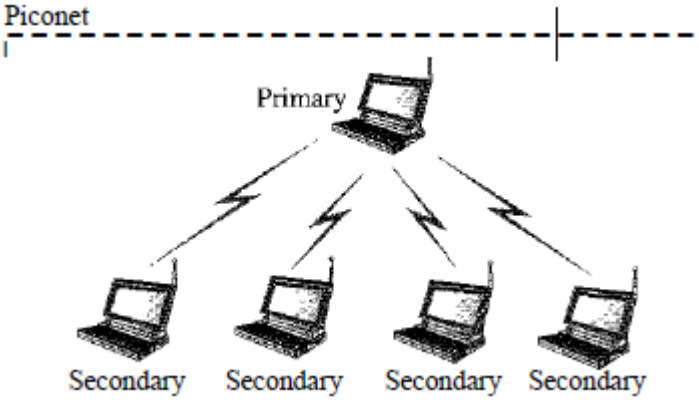
Ans: **(Any 4 Each: 1 mark)**

Mesh Topology	Star Topology
In a mesh topology, every device has a dedicated point-to-point link to every other device.	In star topology, each device has a dedicated point-to-point link only to a central controller.
More expensive than star	Less expensive than Mesh
More cabling and I/O ports required	Less cabling and less I/O ports required
Fault identification and fault isolation easier	Fault identification and fault isolation slightly less easier
More privacy and security	Less privacy and security
Because every device must be connected to every other device, installation and reconnection are difficult.	Installation and reconnection are easier.

		 	
2.		**Attempt any FOUR of the following:**	**16 Marks**
	a)	**Describe the working of peer-to-peer network.**	**4M**
	Ans:	**Peer to peer network:** • A peer to peer network is the one in which computers on the network communicate with each other as equals. • Each computer is responsible for making its own resources available to other computers on the network. These resources may be files, directories or folders, devices or applications. • Each computer is responsible for accessing the network resources it needs from other peer to peer computers. • In this each machine has same power. • Uses less expensive computer hardware. • Easy to setup & administrator. • Less secure as all peers are able to access the resources. • Network Operating System is not required • It support small Network.	**(Any four points each: 1 mark)**
	b)	**State four features of LAN and WAN.**	**4M**
	Ans:	**Features of LAN and WAN** **LAN (Local Area Network):** • **Covers :** Local areas only (e.g. homes, offices, schools) • **Definition :** LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, school, or group of buildings. • **Speed :** High speed (1000 mbps) • **Data transfer rates :** LANs have a high data transfer rate. • **Example :** The network in an office building can be a LAN. • **Set-up costs:** If there is a need to set-up a couple of extra devices on the network, it is not • **Connection :** One LAN can be connected to other LANs over any distance via telephone lines and radio waves. • **Data Transmission Error :** Experiences fewer data transmission errors	**(Any four features from each, Each: $\frac{1}{2}$ mark)**

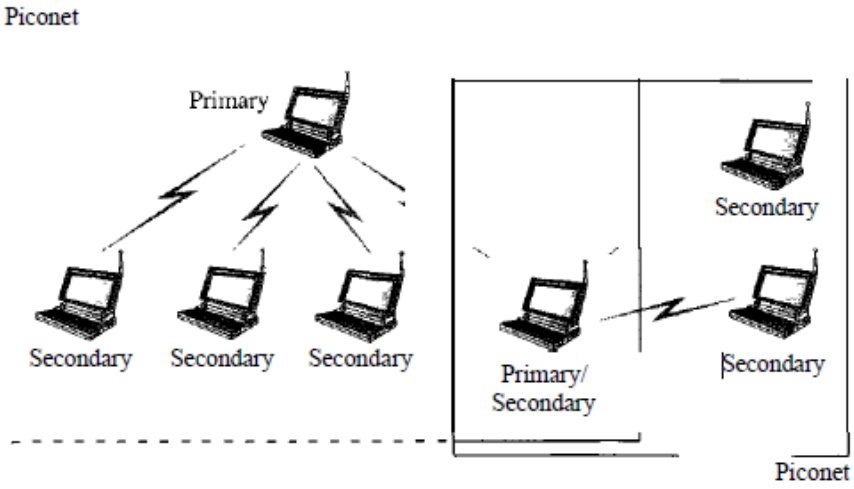
		• **Ownership :** Typically owned, controlled, and managed by a single person or organization. **WAN (Wide Area Network):** • **Covers:** Large geographic areas(e.g. cities, states, nations) • **Definition :** WAN (Wide Area Network) is a computer network that covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries over a long distance). • **Speed :** Less speed (150 mbps) • **Data transfer rates :** WANs have a lower data transfer rate compared to LANs. • **Example :** Internet is a good example of a WAN • **Set-up costs:** Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. • **Connection :** Experiences more data transmission errors as compared to LAN • **Data Transmission Error :** WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management over long distances. • **Ownership :** For WANs since networks in remote areas have to be connected	
	c)	**Draw a neat sketch and describe the construction of co-axial cable.**	**4M**
	Ans:	 **Fig: Construction of Co-axial cable** • Coaxial cable, commonly called coax, has two conductors that share the same axis. • A solid copper wire or standard wire runs down the center of the cable, rounded by a second conductor, a wire mesh tube, metallic foil, or both. • The wire mesh protects the wire from EMI. It is often called the shield. • A tough plastic jacket forms the cover of the cable, providing protection and insulation.	**(Neat labelled Diagram: 2 marks, Description: 2 marks)**
	d)	**Give two applications of:**	**4M**

		(i) Modems **(ii) Routers**	
	Ans:	**Applications of Modem and Router** **Modems:** • Used in connecting computers to communicate either wired or wireless • Used in remote management. • Used in broadband connectivity • Used in Point of Sale machines **Routers :** • Used in Connecting multiple LANs • Used in connecting similar and dissimilar networks • Used in connecting WAN (Internet) to LAN.	**(Any two from each Each: 1 mark)**
	e)	**State four benefits of network used for centralized management.**	**4M**
	Ans:	**Four benefits of centralized managed network** • Centralised administration for higher security. • Better performance for large number of user. • Centralized backup can be taken. • Easy to manage resources. • Reduces the cost by sharing high cost devices • Increased Reliability	**(Each Benefit: 1 mark)**
	f)	**Describe the architecture of bluetooth technology.**	**4M**
	Ans:	**Architecture of Bluetooth Technology** Bluetooth defines two types of networks: piconet and scatternet. *Piconets* A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.	**(Each architecture: 2 marks)**



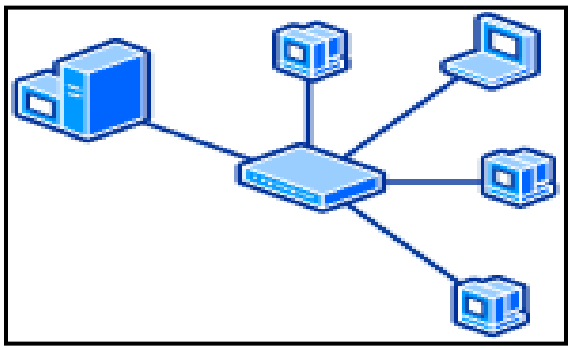
Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the *parked state.* A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

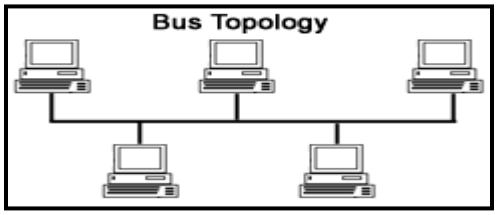
Scatternet

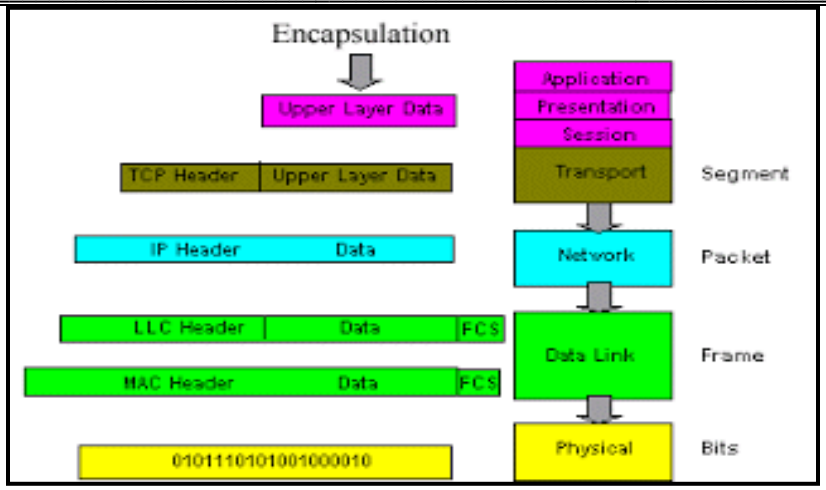


Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

3.		**Attempt any FOUR of the following:**	**16 Marks**
	a)	**Describe the working of server based networks. Where is it used?**	**4M**

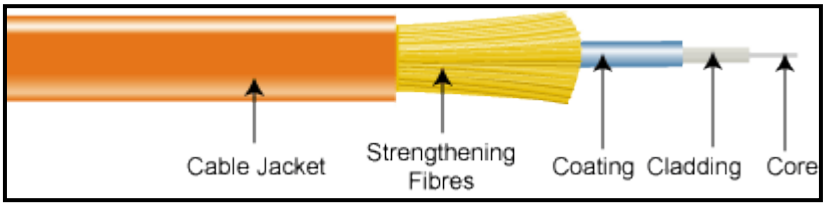
	Ans:	**Server-based network** In a server-based network, the server is the central location where users share and access network resources. This dedicated computer controls the level of access that users have to share resources. Shared data is in one location, making it easy to back up critical business information. Each computer that connects to the network is called a client computer. In a server-based network, users have one user account and password to log on to the server and to access shared resources. Server operating systems are designed to handle the load when multiple client computers access server-based resources.  **Fig: Server-based network** Server based network are used for 1. **Centralization:** Servers help in administering the whole set-up. Access rights and resource allocation is done by Servers. 2. **Proper Management:** All the files are stored at the same place. Also it becomes easier to find files. 3. **Back-up and Recovery possible:** As all the data is stored on server it's easy to make a back-up of it. 4. **Up-gradation and Scalability in Client-server set-up:** Changes can be made easily by just upgrading the server. Also new resources and systems can be added by making necessary changes in server. 5. **Accessibility:** From various platforms in the network, server can be accessed remotely. 6. **Security:** Rules defining security and access rights can be defined at the time of set-up of server.	**(Working: 2 marks, Uses: 2 marks)**
	b)	**Draw a neat sketch of Bus topology and describe its working. Give its advantages.**	**4M**
	Ans:	**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. This central cable is the backbone of the network and is known as Bus. Every workstation communicates with the other device through this Bus. A signal from the source is broadcasted and it travels to all workstations connected to bus cable. Although the	**(Diagram: 1 mark, Working: 2 marks,**

		message is broadcasted but only the intended recipient, whose MAC address or IP address matches, accepts it. If the MAC /IP address of machine doesn't match with the intended address, machine discards the signal. A terminator is added at ends of the central cable, to prevent bouncing of signals. A barrel connector can be used to extend it.  **Fig: Bus Topology** **Advantages of Bus topology** a. It is easy to set-up and extend bus network. b. Cable length required for this topology is the least compared to other networks. c. Bus topology costs very less. d. Linear Bus network is mostly used in small networks which are good for LAN.	**Advantages: 1 mark)**
	c)	**Describe the concept of encapsulation.**	**4M**
	Ans:	**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. The physical layer is responsible for physical transmission of the data. Link encapsulation allows local area networking and Internet Protocol (IP) provides global addressing of individual computers; Transmission Control Protocol (TCP) adds application or process selection. During encapsulation, each layer builds a protocol data unit (PDU) by adding a header (and sometimes trailer) containing control information to the PDU from the layer above. For example, in the Internet protocol suite, the contents of a web page are encapsulated with an HTTP header, then by a TCP header, an IP header, and, finally, by a frame header and trailer. The frame is forwarded to the destination node as a stream of bits, where it is de-capsulated (or de-encapsulated) into the respective PDUs and interpreted at each layer by the receiving node. Encapsulation, the more abstract layer is often called the upper layer protocol while the more specific layer is called the lower layer protocol. Sometimes, however, the terms upper layer protocols and lower layer protocols are used to describe the layers above and below IP	**(Description: 4 marks)**

			
	d)	**Name the protocols used in:** **(i) Data Link layer** **(ii) Network layer** **(iii) Transport layer** (iv) **Presentation layer**	**4M**
	Ans:	**1.Data Link layer:** • Ethernet • FDDI Fibre Distributed Data Interface • Frame Relay • L2TP Layer 2 Tunnelling Protocol • PPP Point-to-Point Protocol • SLIP Serial Line Internet Protocol • Token ring **2. Network layer** • ICMP Internet Control Message Protocol • IGMP Internet Group Management Protocol • IGRP Interior Gateway Routing Protocol • IPv4 Internet Protocol version 4 • IPv6 Internet Protocol version 6 • IPSec Internet Protocol Security **3. Transport layer** • AHAH Authentication Header over IP or IPSec • TCP Transmission Control Protocol • UDP User Datagram Protocol **4. Presentation layer** • Network Data Representation • Netware Core Protocol • MIDI (Musical Instrument Digital Interface)	**Any 2 Protocols in Each Layer: ½ mark Each)**

<table>
<tr><td></td><td></td><td>• Telnet (a remote terminal access protocol)
• X.25 Packet Assembler/Disassembler Protocol (PAD)</td><td></td></tr>
<tr><td></td><td>e)</td><td>State the reasons for having a layered architecture in OSI reference model.</td><td>4M</td></tr>
<tr><td></td><td>Ans:</td><td>The reasons of having a layered architecture in OSI reference model are as follows:
1. It simplifies the design process as the functions of each layers and their interactions are well defined.
2. The layered architecture provides flexibility to modify and develop network services.
3. The number of layers, name of layers and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers certain services to its upper layer.
4. The concept of layered architecture redefines the way of convincing networks. This leads to a considerable cost savings and managerial benefits.
5. Addition of new services and management of network infrastructure become easy.
6. Due to segmentation, it is possible to break complex problems into smaller and more manageable pieces.
7. Logical segmentation helps development taking place by different terms.</td><td>(Any 4 reasons: 1 mark Each)</td></tr>
<tr><td></td><td>f)</td><td>Compare TCP and UDP.</td><td>4M</td></tr>
<tr><td></td><td>Ans:</td><td><table><tr><th>TCP</th><th>UDP</th></tr><tr><td>TCP is connection oriented protocol</td><td>UDP is connectionless protocol.</td></tr><tr><td>TCP is more reliable than UDP</td><td>UDP is less reliable than TCP</td></tr><tr><td>TCP is slower for data sending than TCP.</td><td>UDP is faster for data sending than TCP</td></tr><tr><td>TCP makes checks for errors and reporting.</td><td>UDP makes error checking but no repor</td></tr><tr><td>TCP gives guarantee that the order of data at receiving end is same as on sending end</td><td>UDP has no such guarantee.</td></tr><tr><td>TCP is 20 bytes</td><td>Header size of UDP is 8 bytes.</td></tr><tr><td>TCP is heavy weight as it needs three packets to setup a connection</td><td>UDP is light weight.</td></tr><tr><td>TCP has acknowledgement segments</td><td>UDP has no acknowledgement</td></tr><tr><td>TCP is used for application that require high reliability but less time critical</td><td>UDP is used for application that are tim sensitive but require less reliability</td></tr></table></td><td>(Any 4 differentiation : 1 mark Each)</td></tr>
<tr><td>4.</td><td></td><td>Attempt any <u>FOUR</u> of the following:</td><td>16 Marks</td></tr>
<tr><td></td><td>a)</td><td>Differentiate IPV4 and IPV6.</td><td>4M</td></tr>
<tr><td></td><td>Ans:</td><td><table><tr><th>IPv4</th><th>IPv6</th></tr></table></td><td>(Any 4 differentiation : 1 mark Each)</td></tr>
</table>

		Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length. For more information.	
		Uses broadcast addresses to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, multicast scoped addresses are used.	
		Fragmentation is supported at originating hosts and intermediate routers.	Fragmentation is not supported at routers. It is only supported at the originating host.	
		IP header includes a checksum.	IP header does not include a checksum.	
		IP header includes options.	All optional data is moved to IPv6 extension headers.	
		IPsec support is optional.	IPsec support is required in a full IPv6 implementation.	
		No identification of payload for **QoS** handling by routers is present within the IPv4 header.	Payload identification for **QoS** handling by routers is included in the IPv6 header using the Flow Label field.	
		Addresses must be configured either manually or through DHCP.	Addresses can be automatically assigned using stateless address auto configuration, assigned using DHCPv6, or manually configured.	
		Uses host address (**A**) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (**AAAA**) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.	
	b)	**Explain the protocols ARP and RARP.**		**4M**
	Ans:	**ARP (Address Resolution Protocol):** ARP is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. **RARP (Reverse Address Resolution Protocol):** RARP is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area networks gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.	**(ARP: 2 marks, RARP: 2 marks)**

	c)	**Draw a sketch indicating the construction of fibre optic cable. State four advantages over electrical cables.**	**4M**
	Ans:	 **Core**: This is the physical medium that transports optical data signals from an attached light source to a receiving device. The core is a single continuous strand of glass or plastic that's measured in microns (µ) by the size of its outer diameter. The larger the core, the more light the cable can carry. **Cladding**: This is the thin layer that surrounds the fibre core and serves as a boundary that contains the light waves and causes the refraction, enabling data to travel throughout the length of the fibre segment. **Coating**: This is a layer of plastic that surrounds the core and cladding to reinforce and protect the fibre core. Coatings are measured in microns and can range from 250 to 900 microns. **Strengthening fibres**: These components help protect the core against crushing forces and excessive tension during installation. The materials can range from Kevlar® to wire strands to gel-filled sleeves. **Cable jacket**: This is the outer layer of any cable. Most fibre optic cables have an orange jacket, although some types can have black or yellow jackets. **Advantages of optical fibre:** 1. Extremely High Bandwidth. 2. Optical Fibre Transmission Distance 3. Easy to Accommodate Increasing Bandwidth 4. Resistance to Electromagnetic Interference 5. Secure Transmissions.	**(Diagram: 2 marks, Four advantages: ½ marks each)**
	d)	**Describe the various IP address classes with suitable example.**	**4M**
	Ans:	An IP address is 32-bit address that uniquely and universally defines the connection off a device (for example, a computer or a router) to the Internet **IP addresses are classified into 5 classes** 1) Class A 2) Class B	**(List: 1 mark, Explanation: 3 marks)**

3) Class C
4) Class D
5) Class E

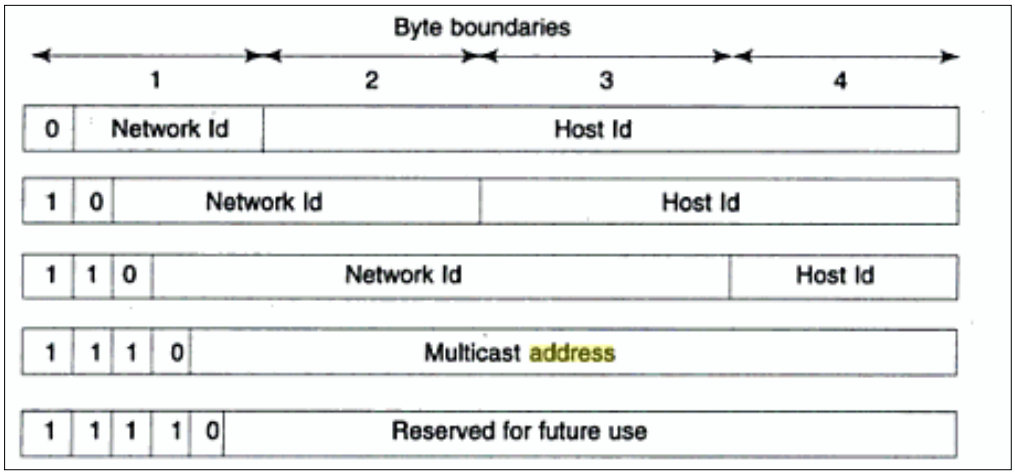
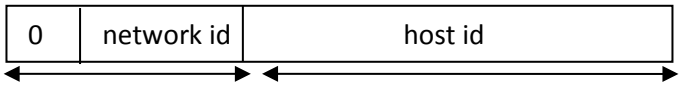


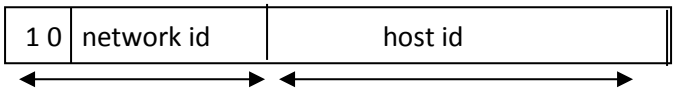
Fig: Classes of IP address

Class A format:



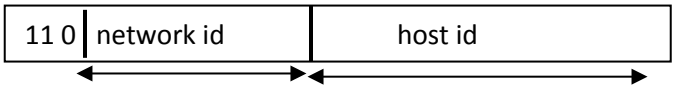
(For first byte)In the first field the first bit '0' indicates that it is class A network address. The next 7 bits are used indicate network id. Rest of the 3 bytes are used to indicate host id Class A: Minimum value is 0.0.0.0 and maximum value 127.255.255.255

Class B format:

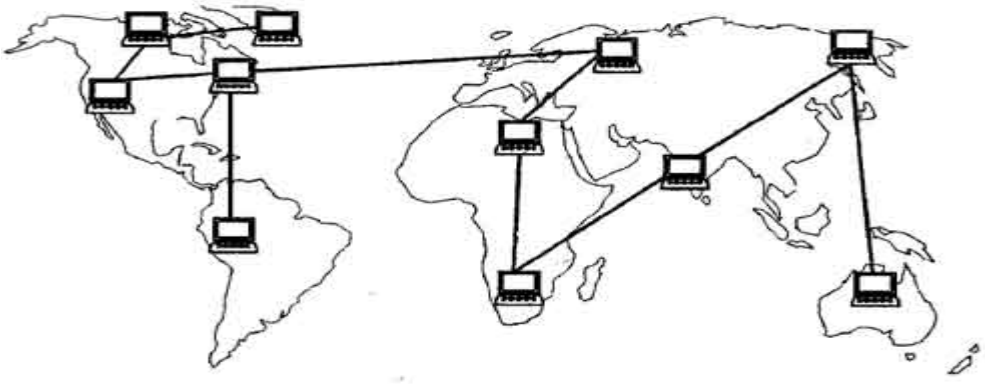


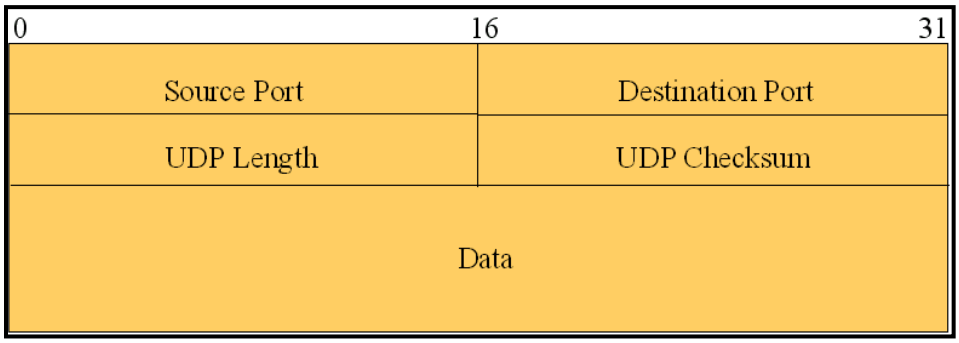
Minimum value is 128.0.0.0 to maximum value 191.255.255.255

Class C format:



		21bits 8 bits (4th byte) Minimum value 192.0.0.0 to maximum value 223.255.255.255 **Class D format:** 111 0 | multi cast address If first 4 bits are 1110 the IP address belongs to class D The IPv4 networking standard defines **Class D** addresses as reserved for **multicast**. Multicast is a mechanism for defining groups of nodes and sending IP messages to that group rather than to every node on the LAN (broadcast) or just one other node (**unicast**). Multicast is mainly used on research networks. As with Class E, Class D addresses should not be used by ordinary nodes on the Internet. For class D minimum value for multi cast address is 224.0.0.0 and maximum multi class address is 239.255.255.255 **Class E format:** 11110 | reserved For class E minimum value for reserved address is 240.0.0.0 to 255.255.255.255	
	e)	**Explain the services provided by the transport layer of the OSI model.**	**4M**
	Ans:	**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: I. Connectionless Transport Layer: Each segment is considered as an independent packet and delivered to the transport layer at the destination machine. II. Connection Oriented Transport Layer: Before delivering packets, connection is made with transport layer at the destination machine.	**(Any 4 Services: 1 mark Each)**

		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. 6. **Data Integrity:** Using checksums, the data integrity across all the delivery layers can be ensured. These checksums guarantee that the data transmitted is the same as the data received through repeated attempts made by other layers to have missing data resent.	
	f)	**Draw a neat diagram and describe a wide area network. What are the three phases of communication in a WAN.**	**4M**
	Ans:	 **Wide area network** **Wide Area Network (WAN)** Wide Area Network is a computer network that covers relatively larger geographical area such as a state, province or country. It provides a solution to companies or organizations operating from distant geographical locations who want to communicate with each other for sharing and managing central data or for general communication. WAN is made up of two or more Local Area Networks (LANs) or Metropolitan Area Networks (MANs) that are interconnected with each other, thus users and computers in one location can communicate with users and computers in other locations.	**(Diagram: 1 mark, Description of WAN: 1 mark, Explanation of Three phases: 2 marks)**

		In Wide Area Network, Computers are connected through public networks, such as the telephone systems, fibre-optic cables, and satellite links or leased lines. The Internet is the largest WAN in a world. WANs are mostly private and are built for a particular organization by Internet Service Providers (ISPs) which connects the LAN of the organization to the internet. WANs are frequently built using expensive leased lines where with each end of the leased line a router is connected to extend the network capability across sites. The three phases of communication in WAN 1. **Circuit establishment:** The establishment phase involves creating the virtual circuit between the source and destination devices. 2. **Data transfer:** Data transfer involves transmitting data between the devices over the virtual circuit 3. **Circuit termination:** Circuit-termination phase involves tearing down the virtual circuit between the source and destination devices.	
	5.	**Attempt any FOUR of the following:**	**16 Marks**
	a)	**Explain the various fields in the frame format of UDP with a neat diagram.**	**4M**
	Ans:	 **Fig:Frame Format of UDP**: **Source port number:** This field identifies the sender's port when meaningful and should be assumed to be the port to reply to if needed. If not used, then it should be zero. If the source host is the client, the port number is likely to be an ephemeral port number. If the source host is the server, the port number is likely to be a well-known port number. **Destination port number:** This field identifies the receiver's port and is required. Similar to source port number, if the client is the destination host then the port number will likely be an ephemeral	**(Diagram: 2 marks, Explanation of the field: 2 marks)**

port number and if the destination host is the server then the port number will likely be a well-known port number.[4]

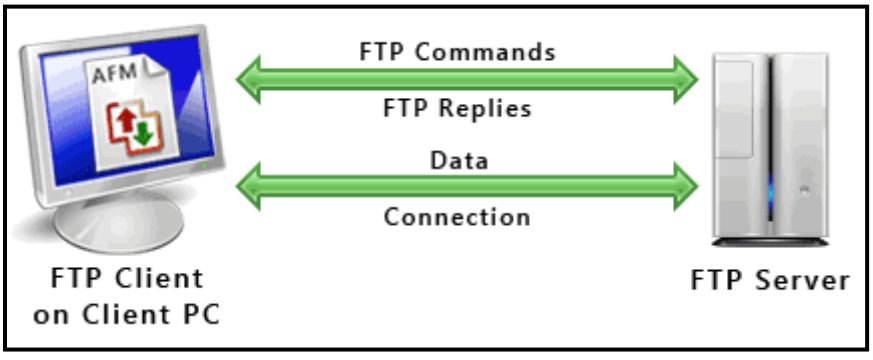
Length:

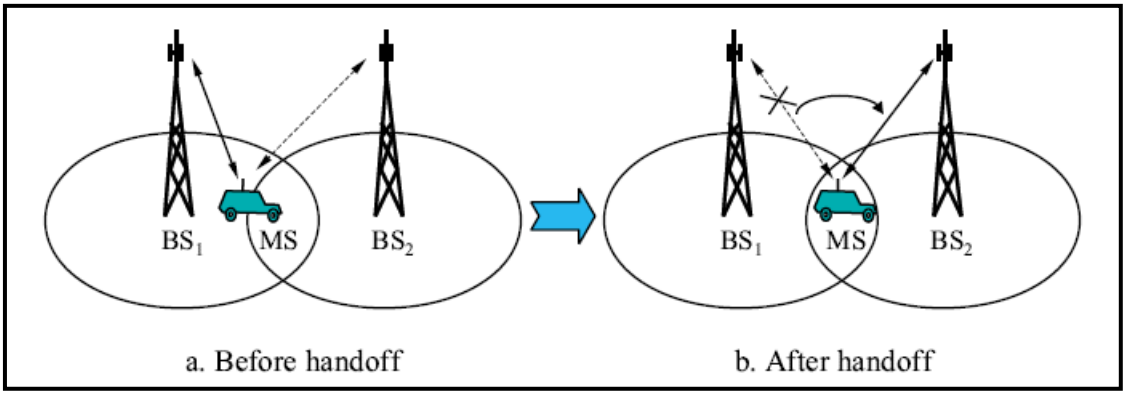
A field that specifies the length in bytes of the UDP header and UDP data. The minimum length is 8 bytes because that is the length of the header. The field size sets a theoretical limit of 65,535 bytes (8 byte header + 65,527 bytes of data) for a UDP datagram. The practical limit for the data length which is imposed by the underlying IPv4 protocol is 65,507 bytes (65,535 − 8 byte UDP header − 20 byte IP header).

In IPv6 jumbogram it is possible to have UDP packets of size greater than 65,535 bytes. RFC 2675 specifies that the length field is set to zero if the length of the UDP header plus UDP data is
greater than 65,535.

Checksum:

The checksum field may be used for error-checking of the header and data. This field is optional in IPv4, and mandatory in IPv6. The field carries all-zeros if unused.

	b)	**Explain the operation of file transfer protocol.**	**4M**
	Ans:	**peration of FTP:**When you want to copy files between two computers that are on the same local network, often you can simply "share" a drive or folder, and copy the files the same way you would copy files from one place to another on your own PC. What if you want to copy files from one computer to another that is halfway around the world? You would probably use your Internet connection. However, for security reasons, it is very uncommon to share folders over the Internet. File transfers over the Internet use special techniques, of which one of the oldest and most widely-used is FTP. **FTP,** short for **"File Transfer Protocol,"** can transfer files between any computers that have an Internet connection, and also works between computers using totally different operating systems. Transferring files from a client computer to a server computer is called **"uploading"** and transferring from a server to a client is **"downloading".**  **Requirements for using FTP**	**(Diagram: 1 mark, Explanation: 3 marks)**

		1. An FTP client like Auto FTP Manager installed on your computer **2.** Certain information about the FTP server you want to connect to: **a**. The **FTP server address.** This looks a lot like the addresses you type to browse web sites. Example : Server address is "ftp.videodesk.net". Sometimes the server address will be given as a numeric address, like "64.185.225.87". **b**. A user name and password. Some FTP servers let you connect to them anonymously. For anonymous connections, you do not need a user name and password. To transfer files, provide your client software (Auto FTP Manager) with the server address, user name, and password. After connecting to the FTP server, you can use Auto FTP Manager's **File Manager** to upload, download and delete files. Using the File Manager is a lot like working with Windows Explorer.	
	c)	**Explain Handoff procedure in mobile communication.**	**4M**
	Ans:	**Hand off procedure in mobile communication: Mobility** is the most important feature of a wireless cellular communication system. Usually, continuous service is achieved by supporting handoff (or handover) from one cell to another. Handoff is the process of changing the channel (frequency, time slot, spreading code, or combination of them) associated with the current connection while a call is in progress. It is often initiated either by crossing a cell boundary or by a deterioration in quality of the signal in the current channel. Handoff is divided into two broad categories— **hard and soft handoffs**. They are also characterized by "**break before make" and "make before break."** In hard handoffs, current resources are released before new resources are used; in soft handoffs, both existing and new resources are used during the handoff process.  a. Before handoff b. After handoff A hard handoff is essentially a "break before make" connection. Under the control of the MSC, the BS hands off the MS's call to another cell and then drops the call. In a hard handoff,	**(Diagram: 2 marks, Explanation: 2 marks)**

		the link to the prior BS is terminated before or as the user is transferred to the new cell's BS; the MS is linked to no more than one BS at any given time. Hard handoff is primarily used in FDMA (frequency division multiple access) and TDMA (time division multiple access), where different frequency ranges are used in adjacent channels in order to minimize channel interference. So when the MS moves from one BS to another BS, it becomes impossible for it to communicate with both BSs (since different frequencies are used). A hard handoff occurs when the old connection is broken before a new connection is activated. The performance evaluation of a hard handoff is based on various initiation criteria	
	d)	**What are the situations under which gateways are used in networks?**	**4M**
	Ans:	**Following are the situations under which Gateways are used in a network :** •Gateways are specifically made to connect dissimilar networks together •A gateway is a node (router) in a computer network, a key *stopping point* for data on its way to or from other networks. The Internet wouldn't be any use to us without gateways (as well as a lot of other hardware and software). •In a workplace, the gateway is the computer that routes traffic from a workstation to the outside network that is serving up the Web pages. For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet. •On the Internet, the node that's a stopping point can be a gateway or a host node. •A computer that controls the traffic your Internet Service Provider (ISP) receives is a node. •If you have a wireless network at home that gives your entire family access to the Internet, your gateway is the modem (or modem-router combo) your ISP provides so you can connect to their network. On the other end, the computer that controls all of the data traffic your Internet Service Provider (ISP) takes and sends out is itself a node. •When a computer-server acts as a gateway, it also operates as a firewall and a proxy server. A firewall keeps out unwanted traffic and outsiders off a private network. A proxy server is software that "sits" between programs on your computer that you use (such as a Web browser) and a computer server—the computer that serves your network. The proxy server's task is to make sure the real server can handle your online data requests.	**(List Any four situation Each: 1 mark)**
	e)	**Compare OSI and TCP/IP network model.**	**4M**
	Ans:	Following are some major differences between OSI Reference Model and TCP/IP Reference Model **OSI** | **TCP/IP**	**(Any four difference: 1 Mark each)**

			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.	7. TCP/IP model does not fit any protocol		
			8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.		
			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		

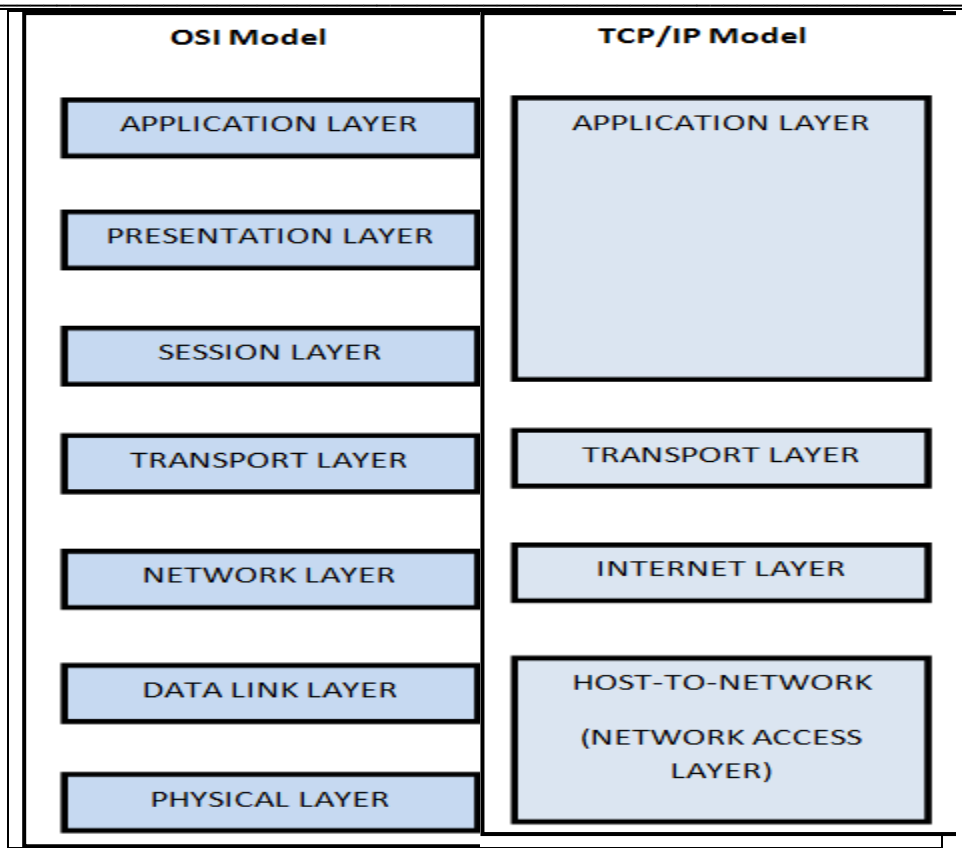


Fig: Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model

	f)	**Name the topology which combines two or more topologies. What are its advantages? Draw a neat diagram of the same.**	**4M**
	Ans:	**Hybrid topology** combines two or more topologies. **Advantages:** **1) Reliable :** Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network. **2) Scalable:** Its easy to increase the size of network by adding new components, without disturbing existing architecture. **3) Flexible:** Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high. **4) Effective:** we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high tolerance capability	**(Topology identification: 1 mark , Advantages: 1 mark , Diagram: 2 marks)**

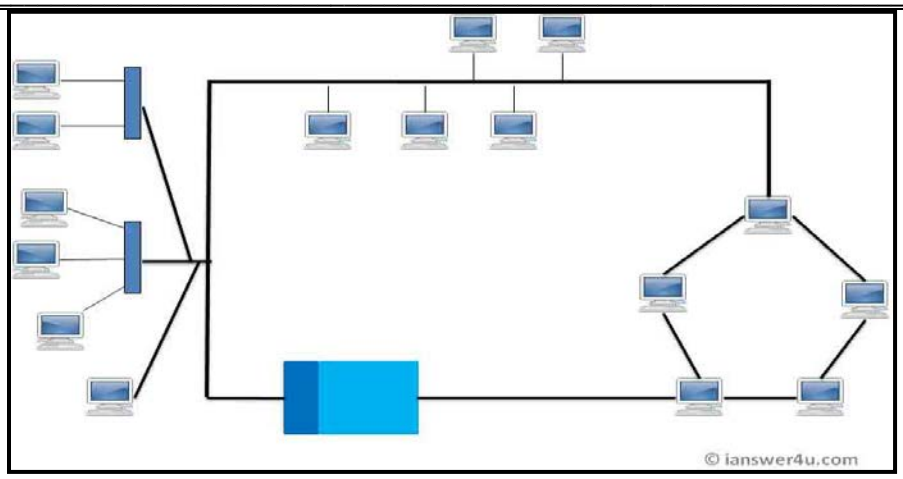
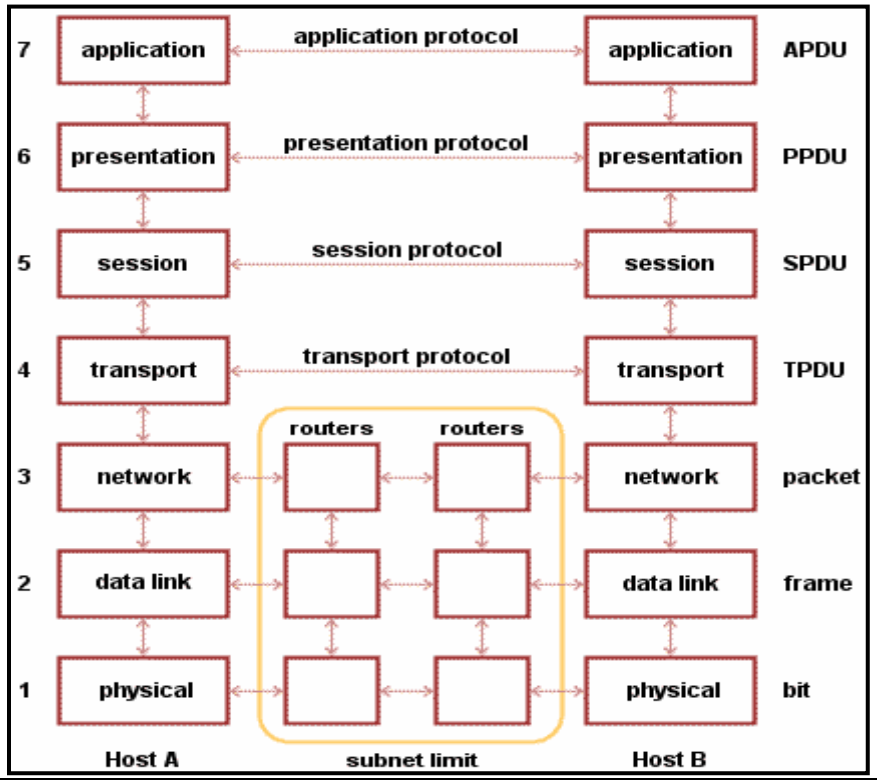


Fig: Hybrid Topology

6.		**Attempt any TWO of the following:**	**16 Marks**
	a)	**Draw a neat diagram showing the layers of OSI model and state the function of each layer.**	**8M**
	Ans:	***The ISO - OSI REFERENCE Model Layers*** 	**(Diagram: 3 marks, Functions: 5 marks)**

The OSI model takes the task of internetworking and divides that up into what is referred to as a *vertical stack* that consists of the following 7 Layers

Physical (Layer 1)
OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. .

Data Link (Layer 2)
At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Network (Layer 3)
Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Transport (Layer 4)
Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer from source to destination.

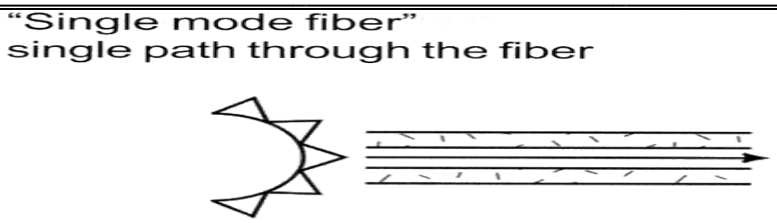
Session (Layer 5)
This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Presentation (Layer 6)
This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax & semantics

Application (Layer 7)
OSI Model, Layer 7, supports application and end-user processes. Everything at this layer is application-specific. This layer provides application services for file

		transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. . All the applications are residing in this layer.	
	b)	**Explain the terms:** **(i) Subnetting** **(ii) Supernetting** **(iii) Masking** **(iv) Classless IP addressing with suitable examples.**	**8M**
	Ans:	**(i) Subnetting: Logically separated network** A subnet short for sub network is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. Without subnets, an organization could get multiple connections to the Internet, one for each of its physically separate subnetworks, . **(ii) Supernetting** : A **supernetwork**, or **supernet**, is an Internet Protocol (IP) network that is formed, for routing purposes, from the combination of two or more networks (or subnets) into a larger network. The new routing prefix for the combined network represents the constituent networks in a single route table entry. The process of forming a supernet is called **supernetting**, **prefix aggregation**, **route aggregation**, or **route summarization** Supernetting within the Internet serves as a preventive strategy to avoid topological fragmentation of the IP address space by using a hierarchical allocation system that delegates control of segments of address space to regional network service providers.[1] This method facilitates regional route aggregation. The benefits of supernetting are conservation of address space and efficiencies gained in routers in terms of memory storage of route information and processing overhead when matching routes. Supernetting, however, has risks. **(iii) Masking :** In computing world **mask** is data that are used for bitwise operations, particularly in a bit field mask, multiple bits in a byte, nibble, word (etc.) can be set either on, off or inverted from on to off (or vice versa) in a single bitwise operation. if you take the example of IP Address masking where in subnet mask of class C 255.255.255.0 will be masking first 3 digits that meanse first three octate can not be changed for keeping yourself the part of the same network. Thus here mask decides host part of an IP address & a network part of an IP address	**(Description of each term: 2 marks)**

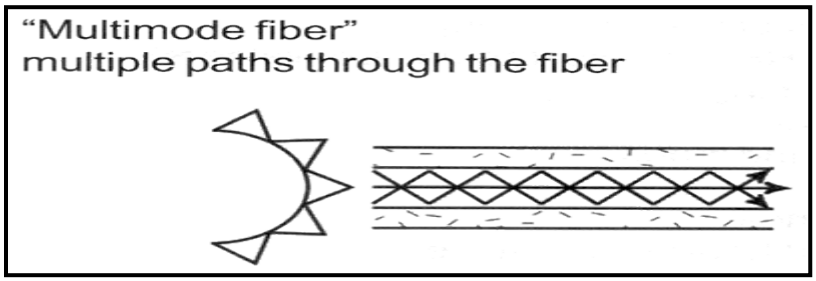
		(iv) Classless IP address : Using a classful IP addressing format worked well when the Internet was relatively small. But as the number of networks on the Internet grew, the limitations of classful addresses became apparent. The Class A address space contains only 125 usable networks in the range 0–127 because networks 0 and 127 are reserved, and network 10 is used for private addressing. Each of these 125 Class A networks could theoretically contain 224 – 2 or 16,777,214 hosts, but it's not realistic to have more than 16 million hosts on the same network. Therefore, the Internet moved away from a classful address space to a classless address space. In other words, the number of bits used for the network portion of an IP address became variable instead of fixed. The network portion of classful IP addresses is fixed. For the network portion of an IP address, Class A addresses use 8 bits, Class B addresses use 16 bits, and Class C addresses use 24 bits. A router could determine the address class by inspecting the first byte of the address. A value of 1–126 is Class A, 128–191 is Class B, and 192–223 is Class C. For classless IP addressing, there is no longer a relationship between the number of bits used in the network portion and the value of the first byte of the address. A different method has to be used to determine the size of the network portion of an IP address. This new method allows you to borrow bits that are normally used for the host portion of an IP address, and use them to extend the network portion of an IP address.	
	c)	**With the help of neat diagram describe:** **(i) Single mode step index** **(ii) Single mode graded index** **(iii)Multimode step index** **(iv)Multimode graded index fibre**	**8M**
	Ans:	**Single Mode cable**: Is a single stand that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate. Single Modem fiber is used in many applications where data is sent at multi-frequency (WDM Wave-Division-Multiplexing) so only one cable is needed - (single-mode on one single fiber) Single-mode fiber gives you a higher transmission rate. Single-mode fiber has a much smaller core than multimode. The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation and the highest transmission speeds of any fiber cable type.	**(Description of each point: 2 marks)**

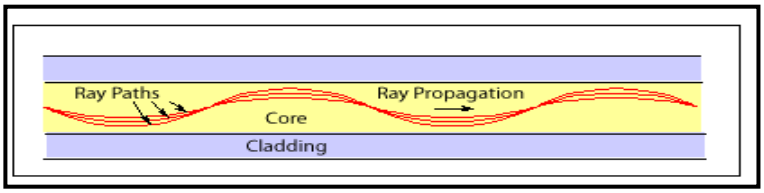


jump to single mode fiber

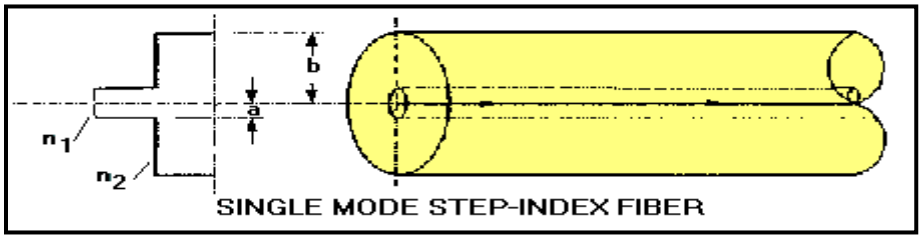
Multi-Mode cable : has a little bit bigger diameter, Multimode fiber gives you high bandwidth . Light waves are dispersed into numerous paths, or modes, as they travel through the cable.

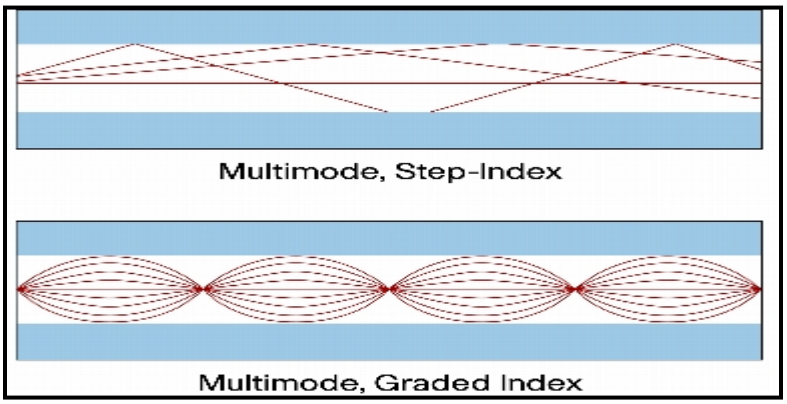
In **Single mode** light takes single path through the fiber core. Step index means sharp step in the index of refraction between core and cladding interface. This indicates that in step index, core and cladding have their own constant index of refractions N1 and N2 respectively.





Single Mode Graded Index





Step-Index Multimode Fiber: has a large core, up to 100 microns in diameter. As a result, some of the light rays that make up the digital pulse may travel a direct route, whereas others zigzag as they bounce off the cladding. These alternative pathways cause the different groupings of light rays, referred to as modes, to arrive separately at a receiving point.

Multimode Graded Index Fiber:

One way to reduce the modal dispersion in multimode fiber is to change the fiber's optical characteristics to compensate for the problem. By modifying the refractive index of the glass through very precise manufacturing techniques, the light can be made to travel more slowly than light that is bouncing around in modes near the outside of the core. The shorter paths are made slower so that they are held back to the pace of the faster (but longer) paths. The light that travels farther travels faster and the light that travels less travels slower. The net effect is that the light pulse stays together and doesn't spread out in the way that it would with non-Graded Index fiber. A graded index fiber typically transmits roughly 800 modes. The core fiber has a varying refractive index. The core is clad with a glass with a lower refractive index, just like non-GI multimode, to cause stray light to bounce back into the cable.

Step index single mode fibers :

- The light energy in a single-mode fiber is concentrated in one mode only.
- This is accomplished by reducing Δ and or the core diameter to a point where the V is less than 2.4.
- In other words, the fiber is designed to have a V number between 0 and 2.4.
- This relatively small value means that the fiber radius and Δ, the relative refractive index difference, must be small.

No intermodal dispersion exists in single mode fibers because only one mode exists

Contd.

		• With careful choice of material, dimensions and λ, the total dispersion can be made extremely small, less than 0.1 ps /(km × nm), making this fiber suitable for use with high data rates. • In a single-mode fiber, a part of the light propagates in the cladding. • The cladding is thick and has low loss. • Typically, for a core diameter of 10 μm, the cladding diameter is about 120 μm. • Handling and manufacturing of single mode step index fiber is more difficult. **Single - Mode Graded Index Fiber:** In fiber optics, a **graded index** is an optical fiber whose core has a refractive index that decreases with increasing radial distance from the optical axis of the fiber . Because parts of the core closer to the fiber axis have a higher refractive index than the parts near the cladding, light rays follow sinusoidal paths down the fiber. The most common refractive index profile for a graded-index fiber is very nearly parabolic. The parabolic profile results in continual refocusing of the rays in the core, and minimizes modal dispersion.	

Q. No.	Sub Q. N.	Answer	Marking Scheme
