WINTER – 19 EXAMINATION
Subject Name: Data Communication and Network

Model Answer

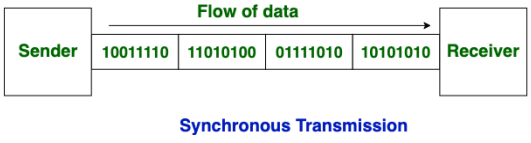
Subject Code: 22414

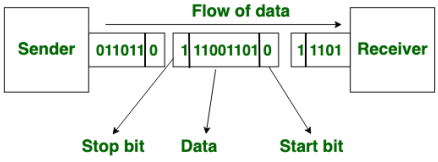
Important Instructions to examiners:

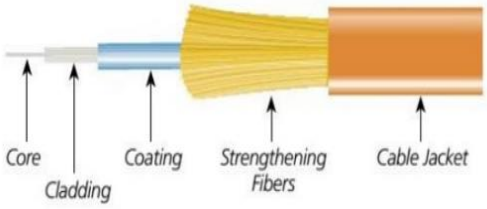
1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling 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.		**Attempt any Five of the following:**	**10M**
	a	**Define bit rate and baud rate.**	**2M**
	Ans	Bit Rate: Bit rate is simply the number of bits (i.e., 0's and 1's) transmitted per unit time. Baud Rate: Baud rate is the number of signal units transmitted per unit time that is needed to represent those bits.	1M-Bit rate 1M-Baud Rate
	b	**List different characteristics of data communication system.(Any two)**	**2M**
	Ans	1. Delivery 2. Accuracy 3. Timeliness 4. Jitter	1 M for 1 characteristic
	c	**Define guided and unguided communication media.**	**2M**
	Ans	**Guided communication media:** Guided transmission media are known as the **wired communication**. The electromagnetic signals travel between the communicating devices through a physical medium/conductor. **Unguided communication media:** The unguided media is also called **wireless communication**. It does not require any physical medium to transmit electromagnetic signals. In unguided media, the electromagnetic signals are broadcasted through air to everyone.	1M-Guided media 1M-Unguided media

<table>
<tr><td></td><td>d</td><td>Classify mobile generations.</td><td>2M</td></tr>
<tr><td></td><td>Ans</td><td>First Generation (1G)
Second Generation (2G)
Third Generation (3G)
Fourth Generation (4G) or LTE
Fifth Generation (5G)</td><td>All generations to be mentioned-2M</td></tr>
<tr><td></td><td>e</td><td>Compare LRC and CRC(Any two points each)</td><td>2M</td></tr>
<tr><td></td><td>Ans</td><td><table><tr><th>LRC</th><th>CRC</th></tr><tr><td>Longitudinal Redundancy Check (LRC)is a method in which a block of bits is organized in table(rows and columns)calculate the parity bit for each column and the set of this parity bit is also sending with original data. From the block of parity we can check the redundancy</td><td>Cyclic Redundancy Check (CRC) is one of the most common and powerful error detecting codes in which a sequence of redundant bits, called the CRC is appended to the end of the unit so that the resulting data unit become exactly divisible by a second, predetermined binary number.</td></tr><tr><td>LRC of n bits can easily detect</td><td>CRC is more powerful than</td></tr><tr><td>Burst error of n bits.</td><td>VRC and LRC in detecting errors.</td></tr><tr><td>A longitudinal redundancy check (LRC) is an error-detection method based on binary addition</td><td>CRC is based on binary division.</td></tr></table></td><td>2 M for any relevant 2 points</td></tr>
<tr><td></td><td>f</td><td>State different types of Network topologies.</td><td>2M</td></tr>
<tr><td></td><td>Ans</td><td>1. Mesh Topology
2. Star Topology
3. Bus Topology
4. Ring Topology
5. Hybrid Topology</td><td>Mention of all Topologies-2M</td></tr>
<tr><td></td><td>g</td><td>List classes of IP addressing with their IP address range.</td><td>2M</td></tr>
<tr><td></td><td>Ans</td><td>An IP address is an address used to uniquely identify a device on an IP network.
Classes and range:
Class A- 1.0.0.1 to 126.255.255.254
Class B - 128.1.0.1 to 191.255.255.254
Class C - 192.0.1.1 to 223.255.254.254
Class D- 224.0.0.0 to 239.255.255.255
Class E - 240.0.0.0 to 254.255.255.254</td><td>List1M,correct range 1M</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

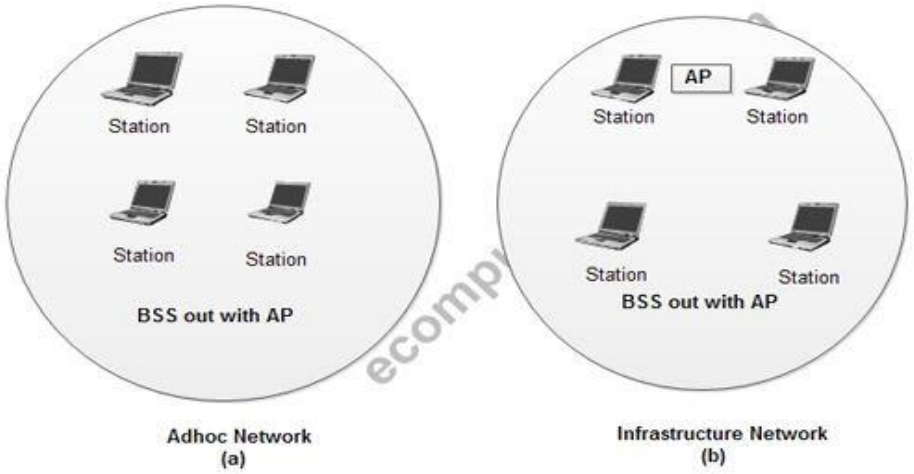
<table>
<tr><td>2.</td><td></td><td>Attempt any Three of the following:</td><td>12M</td></tr>
<tr><td></td><td>a</td><td>Differentiate between synchronous and asynchronous communication.(Any four points)</td><td>4M</td></tr>
<tr><td></td><td>Ans</td><td>
<table>
<tr><th>Synchronous communication</th><th>Asynchronous communication</th></tr>
<tr><td>In Synchronous Transmission, data is sent in form of blocks or frames.</td><td>In Asynchronous Transmission, data is sent in form of byte or character.</td></tr>
<tr><td>Sender and Receiver use the same clock signal</td><td>Does not need clock signal between the sender and the receiver</td></tr>
<tr><td>It is more efficient and more reliable than asynchronous transmission to transfer the large amount of data.</td><td>In this transmission start bits and stop bits are added with data.</td></tr>
<tr><td> 

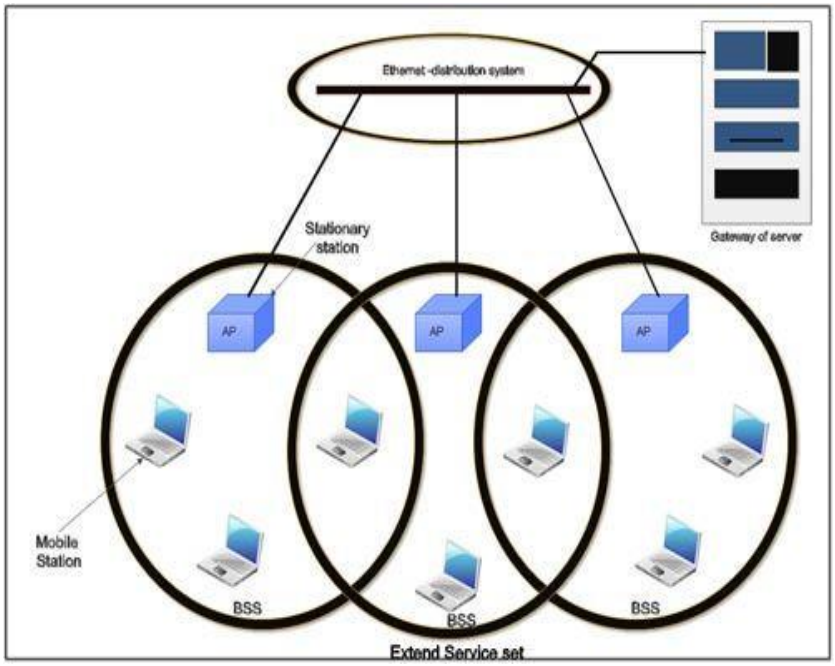
Synchronous Transmission</td><td> 

Asynchronous Transmission</td></tr>
<tr><td>Synchronous transmission is fast.</td><td>Asynchronous transmission is slow.</td></tr>
<tr><td>In Synchronous transmission, time interval of transmission is constant.</td><td>In asynchronous transmission, time interval of transmission is not constant, it is random.</td></tr>
</table>
</td><td>1M for 1 point</td></tr>
<tr><td></td><td>b</td><td>Draw and explain fiber optic cable.</td><td>4M</td></tr>
<tr><td></td><td>Ans</td><td> 

Fiber optic cable:

A fiber-optic cable is made up of glass or plastic.
It transmits signals in the form of light.
The outer jacket is made up of PVC or Teflon.
Kevlar strands are placed inside the jacket to strengthen the cable.
Below the Kevlar strands, there is another plastic coating which acts as a cushion.
The fiber is at the center of the cable, and it consists of cladding and glass core.
The density of the cladding is less than that of the core.
</td><td>2 M Labelled Diagram,2 M explanation</td></tr>
</table>

		• Optical fibers use the principle of 'reflection' to pass light through a channel.	
	c	**Explain wireless LAN 802.17 architecture.**	**4M**
	Ans	**Wireless LAN 802.11:** The IEEE 802.11 standard defines the physical layer and media access control (MAC) layer for a wireless local area network. Wireless LANs transmit and receive data over the atmosphere, using radio frequency (RF) or infrared optical technology, thereby; eliminating the need for fixed wired connections. **802.11 Architecture**: The 802.11architecture defines two types of services: 1. Basic services set (BSS) 2. Extended Service Set (ESS) **1. Basic Services Set (BSS)** • The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP). • The use of access point is optional. • If the access point is not present, it is known as stand-alone network. Such a BSS cannot send data to other BSSs. This type of architecture is known as adhoc architecture. • The BSS in which an access point is present is known as an infrastructure network.  **Basic Service Sets** **2. Extend Service Set (ESS)** An extended service set is created by joining two or more basic service sets (BSS) having access points (APs).	**Consider IEEE 802.11 instead of 802.17** BSS diagram 1M, Explanation - 1M- ESS diagram 1M, Explanation - 1M ***Note:** **If student attempted to solve the answer give appropriate marks.**

		These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.  **There are two types of stations in ESS:** **(i) Mobile stations**: These are normal stations inside a BSS. **(ii) Stationary stations**: These are AP stations that are part of a wired LAN.	
	d	**State the functions of any two layers of OSI Model**	**4M**
	Ans	**The functions of the physical layer are :** 1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level. 2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second. 3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology. 4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.	Functions of each layer- 2M

Functions of data link layer:

- **Framing:** Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.
- **Addressing**: Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- **Synchronization:** When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
- **Error Control:** Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- **Flow Control:** Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.
- **Multi-Access:** When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

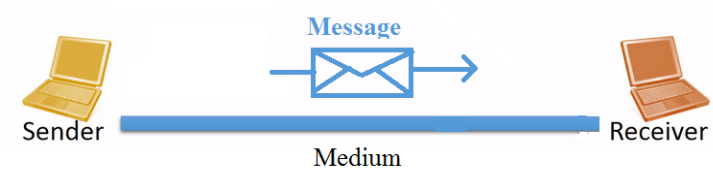
Functions of the Network layer are as follows:

- It is responsible for routing packets from the source host to the destination host. The routes can be based upon static tables that are rarely changed, or they can be automatically updated depending upon network conditions.
- The data link layer assigns the physical address locally. When the data packets are routed to remote locations, a logical addressing scheme is required to differentiate between the source system and the destination system. This is provided by the network layer.
- This layer also provides mechanisms for congestion control.
- The network layer tackles issues like transmission delays, transmission time, avoidance of jitters, etc.

Functions of Transport Layer

- **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.
- **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

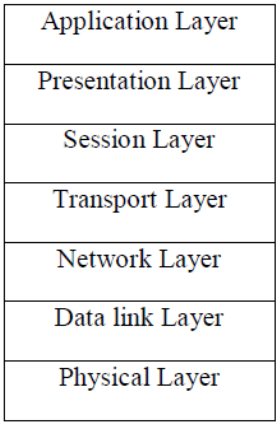
		arrival at the destination and replaces packets which were lost in transmission. • **Connection Control:** It includes 2 types: • **Connectionless Transport Layer**: Each segment is considered as an independent packet and delivered to the transport layer at the destination machine. • **Connection Oriented Transport Layer**: Before delivering packets, connection is made with transport layer at the destination machine. • **Flow Control:** In this layer, flow control is performed end to end. • **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. **The functions of the Session layer are :** 1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection. 2. **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided. 3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex. **The functions of the presentation layer are :** 1. **Translation:** For example, ASCII to EBCDIC. 2. **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data. 3. **Compression:** Reduces the number of bits that need to be transmitted on the network. **The functions of the Application layer are :** 1. Network Virtual Terminal 2. FTAM-File transfer access and management 3. Mail Services 4. Directory Services	
3.		**Attempt any Three of the following:**	**12M**
	a	**State the two advantages and disadvantages of unguided media**	**4M**
	Ans	**Advantages:** 1 .Use for long distance communication.	2 M advantages

		2. High speed data transmission. 3. Many receiver stations can receive signals from same sender station **Disadvantages :1.**.Radio waves travel through Lowest portion of atmosphere which can have lot of noise and interfering signals 2. Radio wave communication through unguided media is an insecure communication. 3.Radio wave propagation is susceptible to weather effects like rain, thunder and storm etc.	1 mark for each advantage 2 M Disadvantages 1mark for each disadvantage
	b	**Draw and explain block diagram of communication system.**	**4M**
	Ans	 Considering the communication between two computers , the communication system is as shown in above diagram **It has following five components:** 1. Message 2. Sender 3. Medium 4. Receiver 5. Protocol **Message:** • Message is the information or data which is to be sent from sender to the receiver • A message can be in the form of sound, text, picture, video or combination of them(multimedia) **Sender:** Sender is device such as host, camera, workstation, telephone etc. which sends the message over medium **Medium:** The message originated from sender needs a path over which it can travel to the receiver. Such path is called as medium or channel	1 M diagram. 3M explanation

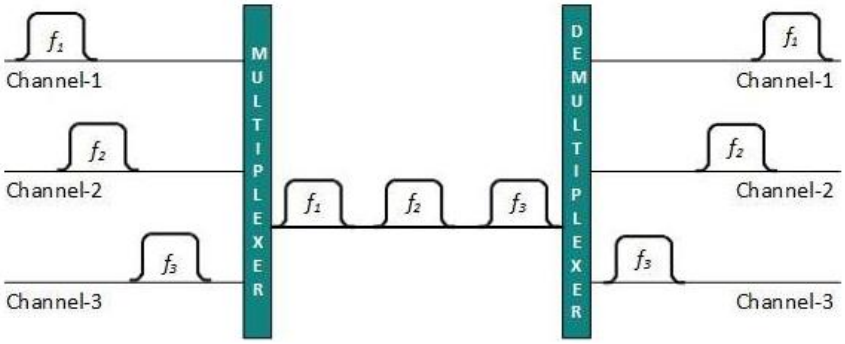
		Receiver: It is the device which receives the message and reproduces it. A receiver can be host, camera, workstation, telephone etc. **Protocol:** A protocol is defined as set of rules agreed by sender and receiver. Protocol governs the exchange of data in true sense.	
	c	**Describe different connecting devices used in computer network.**	**4M**
	Ans	**Network Connecting devices are:** 1. Repeater 2. Hub 3. Switch 4. Bridge 5. Router 6. Gateway 7. Modem **Repeater:** •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. **Hub:** •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. **Switch:** It is used to connect multiple computers in which it can direct a transmission toits specific destination. (Unicast the signals).	Any 4 devices. 1 M each

		•It is a unicasting device. •It avoids unnecessary network traffic. •It operates in both the physical and the data link layer. **Bridge:** •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. **Gateway:** •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. **Router:** •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 directs 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. **Modem:**	

		•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	**Draw and explain OSI reference model.**	**4M**
	Ans	OSI model (Open System Interconnection) model was developed by ISO (international standard organization) which provides way to understand how internetwork operates. It gives guidelines for creating network standard. OSI model has 7 layers as shown in the figure. Application Layer, Presentation Layer ,Session Layer, Transport Layer ,Network Layer ,Data link Layer and Physical Layer **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)** 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	1 M diagram and 3 M explanation

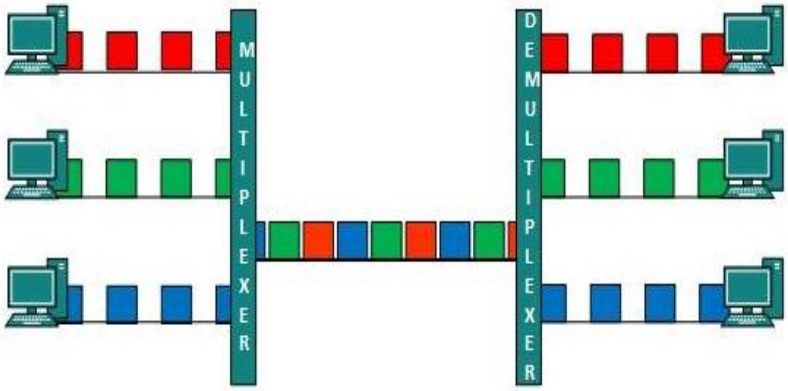
		Presentation (Layer 6) This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats 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.  **OSI Model**	
4.		**Attempt any Three of the following:**	**12M**
	a	**Describe Multiplexing techniques**	**4M**
	Ans	Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams. Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing. When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers. Different multiplexing techniques are 1.Frequency Division multiplexing 2.Time division multiplexing **Frequency Division Multiplexing:** When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier	2 M each technique explanation

bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



Time Division Multiplexing: TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.



When channel A transmits its frame at one end, the De-multiplexer provides media to channel A on the other end. As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer

works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner

b **Compare IPV4 and IPV6 (any four point)** **4M**

Ans Any 4 correct points1M each

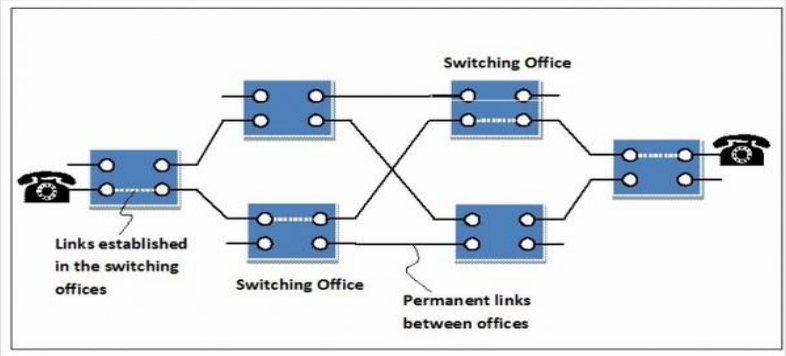
IPV4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128Bits (16 bytes) in length.
No. addresses are limited to number of bits (32 bits)	Larger addressing area
Uses broadcast addresses to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, multicast scoped addresses aroused
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 IPv6extension headers
IPv4 has classful addressing scheme, includes classes like A,B,C,D and E.	Classless addressing scheme.
Uses decimal dotted notation	Uses hexadecimal notation

c **Explain circuit switching networks with neat sketch.** **4M**

Ans Circuit switching is a connection-oriented network switching technique. Here, a dedicated route is established between the source and the destination and the entire message is transferred through it. 1 M for diagram. 3 M for explaination

Phases of Circuit Switch Connection:

- **Circuit Establishment**: In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centers. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.

		• **Data Transfer**: Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate. • **Circuit Disconnection**: When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver.  The diagram represents circuit established between two telephones connected by circuit switched connection. The blue boxes represent the switching offices and their connection with other switching offices. The black lines connecting the switching offices represent the permanent link between the offices.	
	d	**Draw and explain TCP/IP model.**	**4M**
	Ans	TCP/IP that is Transmission Control Protocol and Internet Protocol has following features ●Support for a flexible architecture. Adding more machines to a network was easy. ●The network is robust, and connections remained intact until the source and destination machines were functioning. The main 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:	1 M for diagram. 3 M for explaination

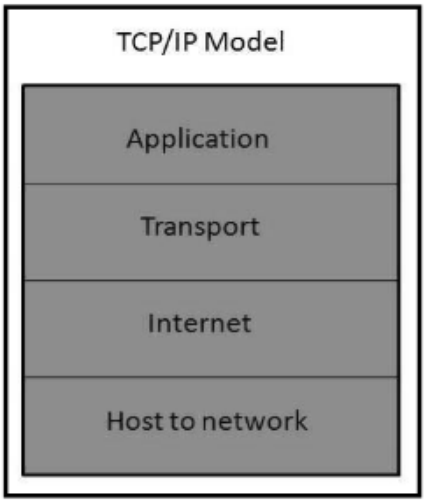


Fig: TCP/IP reference model

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.

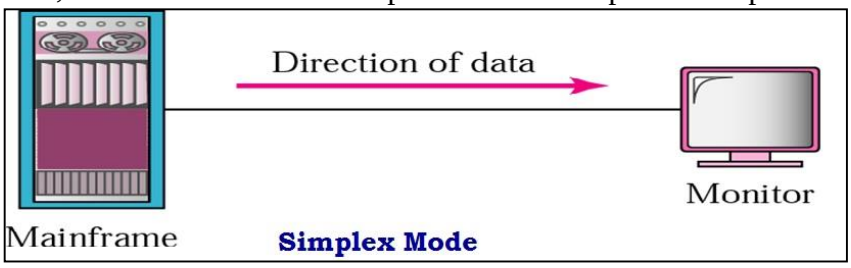
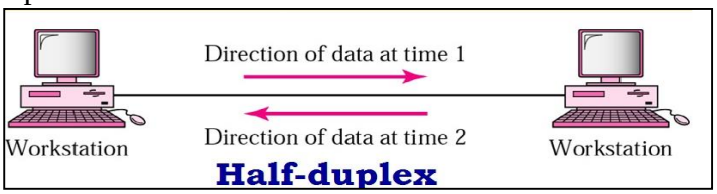
5. IP (Internet Protocol) is used in this layer.

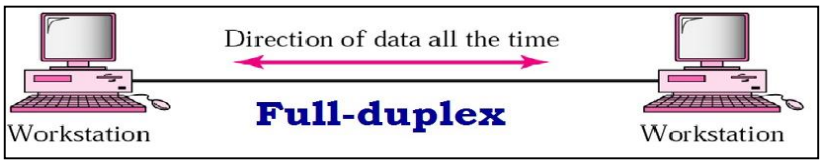
6. **The various functions performed by the Internet Layer are:**

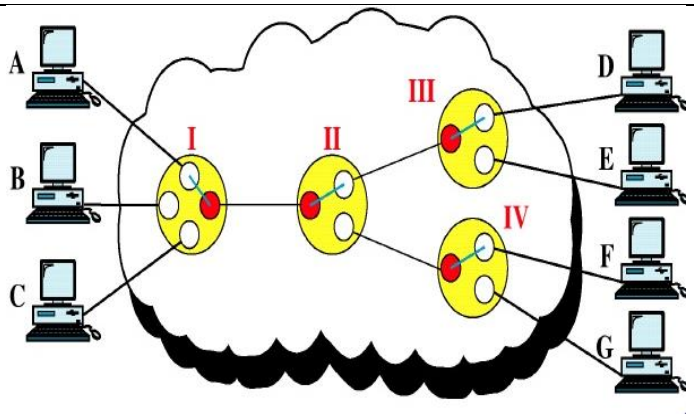
- Delivering IP packets
- Performing routing
- Avoiding congestion

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. 6.Transport layer also arrange the packets to be sent, in sequence **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. 1. Telnets a two-way communication protocol which allows connecting to a remote machine and run applications on it. 2. FTP (File Transfer Protocol) is 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.	
	e	**Explain various IEEE communication standards.**	**4M**
	Ans	A set of network standards developed by the IEEE. They include: • IEEE 802.1: Standards related to network management. • IEEE 802.2: General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sublayers -- the logical link control (LLC) layer and the media access control (MAC) layer. The MAC layer varies for different network types and is defined by standards IEEE 802.3 through IEEE 802.5. • IEEE 802.3: Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard. IEEE 802.4: Defines the MAC layer for bus networks that use a token passing mechanism (token bus networks).	1 M for 1 standard each

		• IEEE 802.5: Defines the MAC layer for token-ring networks. • IEEE 802.6: Standard for Metropolitan Area Networks (MANs). • IEEE 802.11 Wireless Network Standards: 802.11 is the collection of standards setup for wireless networking.	
5.		**Attempt any Two of the following:**	**12M**
	a	**Explain simplex, half duplex and full duplex modes in data communication.**	**6M**
	Ans	Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called Communication Mode. These modes direct the direction of flow of information. There are three types of transmission modes. **They are:** • Simplex Mode • Half duplex Mode • Full duplex Mode **1.** In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction. Keyboards, traditional monitors and printers are examples of simplex devices.  **2.** In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction -for example: Walkie-talkies.  **3**. In full-duplex mode both stations can transmit and receive data simultaneously. The transmission medium sharing can occur in two ways,	for each mode 1M for diagram 1M for explanation

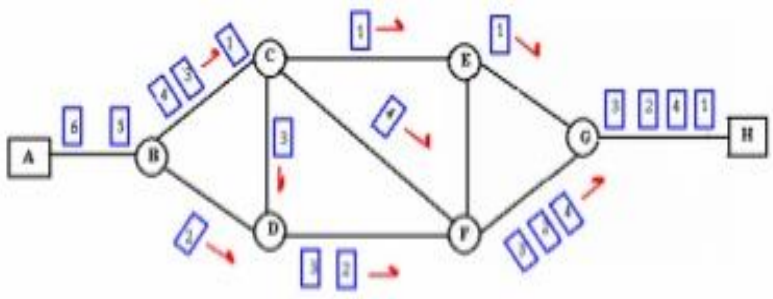
		namely, either the link must contain two physically separate transmission paths or the capacity of the channel is divided between signals traveling in both directions .One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.  	
	b	**Describe the principles of packet switching and circuit switching techniques with neat diagram.**	**6M**
	Ans	**Circuit Switching:** When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place. Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases: ● Establish a circuit ● Transfer the data ● Disconnect the circuit	Circuit switching-3M 1 M –diagram, 2M explanation: Packet switching-3 M 1M- diagram, 2M explanation



Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between callers and called is established over the network.

Packet Switching: The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

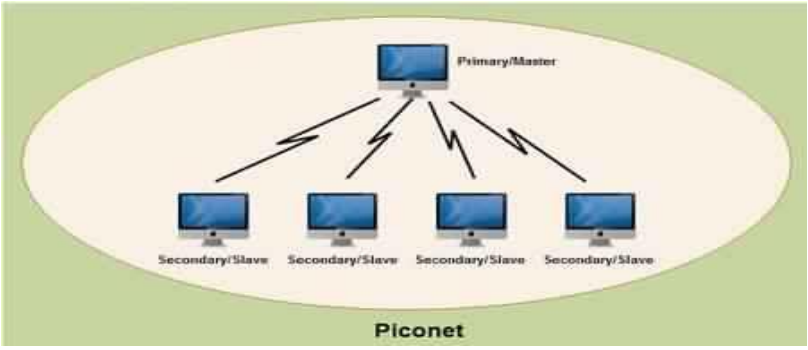
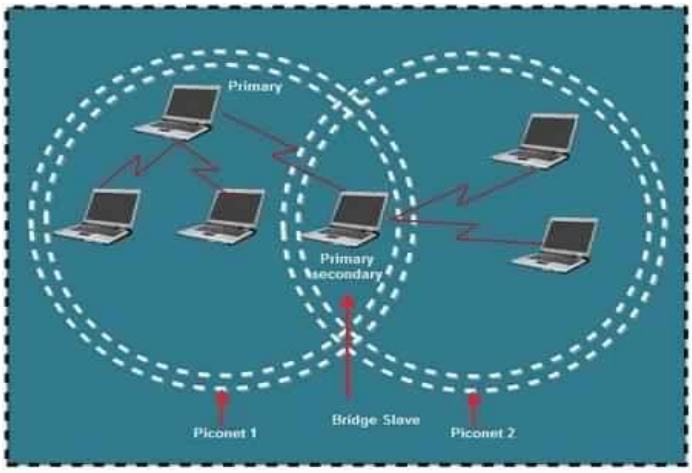
It is easier for intermediate networking devices to store small size packets and they do not take much resource either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

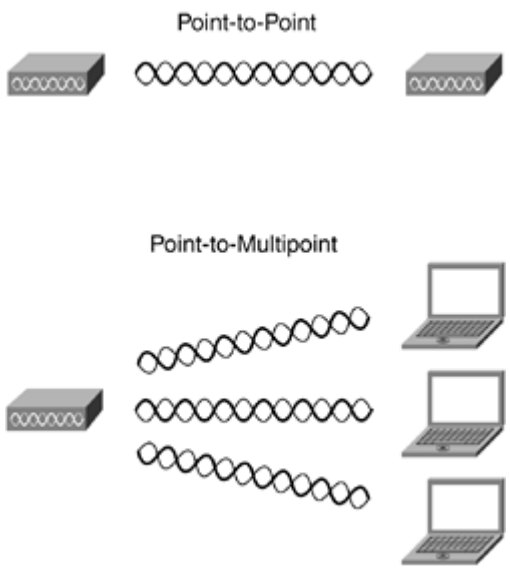
	c	**Explain configuration of TCP/IP protocol in network.**	**6M**
	Ans	Before beginning configuration procedure, the following are the prerequisites. ● Network hardware is installed and cabled. . ● TCP/IP software is installed. To configure your TCP/IP network, the following steps are followed: ● Read TCP/IP protocols for the basic organization of TCP/IP.	Step by step procedure -6M

		● Minimally configure each host machine on the network. This means adding a network adapter, assigning an IP address, and assigning a host name to each host, as well as defining a default route to your network. For background information on these tasks, refer to TCP/IP network interfaces, TCP/IP addressing, and Naming hosts on your network. ● Configure and start the intend daemon on each host machine on the network. Read TCP/IP daemons and then follow the instructions in Configuring the intend daemon. ● Configure each host machine to perform either local name resolution or to use a name server. If a hierarchical Domain Name networks being set up, configure at least one host to function as a name server. ● If the network needs to communicate with any remote networks, configure at least one host to function as a gateway. The gateway can use static routes or a routing daemon to perform inters network routing. ● Decide which services each host machine on the network will use. By default, all services are available. Follow the instructions in Client network services if you wish to make a particular service unavailable. ● Decide which hosts on the network will be servers, and which services a particular server will provide.Follow the instructions in Server network services to start the server daemons you wish to run. ● Configure any remote print servers that are needed. ● Optional: If desired, configure a host to use or to serve as the master time server for the network.	
6.		**Attempt any Three of the following:**	**12M**
	a	**Describe Bluetooth architecture technologies.**	**6M**
	Ans	Bluetooth Architecture Bluetooth architecture defines two types of networks: 1. Piconet 2. Scatternet **1. Piconet** • Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes. • Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters. • There can be only one primary or master station in each piconet.	Piconet 3M (1M diagram, 2M for explanation); Scatternet-3M(1M diagram, 2M for explanation

		• The communication between the primary and the secondary can be one-to-one or one-to-many.  • All communication is between master and a slave. Salve-slave communication is not possible. • In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state. **2. Scatternet** • Scattemet is formed by combining various piconets. • A slave in one piconet can act as a master or primary in other piconet. • Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave. • Thus a station can be a member of two piconets. • A station cannot be a master in two piconets.  	
	b	**Explain the process of DHCP server configuration.**	**6M**

	Ans	**Configuring the DHCP Server** To configure the DHCP server: **1. From the Control Panel, go to Administrative Tools >> Computer Management >> Services and Application >> DHCP.** **2. From the Action menu, select New Scope.** The New Scope wizard is displayed. **3. Enter the following information as prompted:** ▪ Scope name and description: ▪ IP address range (for example, 192.168.0.170 to 192.168.0.171) ▪ Subnet mask (for example, 255.255.255.0) ▪ Add exclusions (do not exclude any IP addresses) ▪ Lease duration (accept the default of 8 days) ▪ Router (default gateway) of your subnet (for example, 192.168.0.1) ▪ Domain name, WINS server (these are not needed) ▪ Activate Scope? (select "Yes, I want to activate this scope now") **4. Click Finish to exit the wizard.** The contents of the DHCP server are listed. **5. Right-click Scope [**iPad dress**] scope-name and select Properties.** **6. In the Scope Properties box, click the Advanced tab.** **7. Select BOOTP only, set the lease duration to Unlimited, and click OK.** **8. Right-click Reservations.** The Controller A Properties box is displayed. **9. Enter the IP address and the MAC address for Controller A. Click Add.** The Controller B Properties box is displayed.	Step by step procedure- 6M

		10. Enter the IP address and the MAC address for Controller B. Click Add. The controllers are added to the right of the Reservations listing. **11. Right-click Scope [**iPad dress**] scope-name to disable the scope.** **12. Click Yes to confirm disabling of the scope.** **13. Right-click Scope and select Activate.**	
	c	**Describe wireless infrastructure components in detail.**	**6M**
	Ans	**Wireless Network Infrastructures** The infrastructure of a wireless network interconnects wireless users and end systems. The infrastructure might consist of base stations, access controllers, application connectivity software, and a distribution system. These components enhance wireless communications and fulfill important functions necessary for specific applications. **1. Base Stations** The base station is a common infrastructure component that interfaces the wireless communications signals traveling through the air medium to a wired network? Often referred to as a distribution system. Therefore, a base station enables users to access a wide range of network services, such as web browsing, e-mail access, and database applications. A base station often contains a wireless NIC that implements the same technology in operation by the user's wireless NIC. Residential gateways and routers are more advanced forms of base stations that enable additional network functions. As show in Figure a base station might support point-to-point or point-to-multipoint communications.	4 components-11/2M each



Base Stations Support Different Configurations

Access Controllers

In the absence of adequate security, quality of service (QoS), and roaming mechanisms in wireless network standards, companies offer access-control solutions to strengthen wireless systems. The key component to these solutions is an access controller, which is typically hardware that resides on the wired portion of the network between the access points and the protected side of the network. Access controllers provide centralized intelligence behind the access points to regulate traffic between the open wireless network and important resources. In some cases, the access point contains the access control function.

Application Connectivity Software

Web surfing and e-mail generally perform well over wireless networks. All it takes is a browser and e-mail software on the client device. Users might lose a wireless connection from time to time, but the protocols in use for these relatively simple applications are resilient under most conditions.

Special application connectivity software is necessary as an interface between a user's computer device and the end system hosting the application's software or database.

		Distribution System A wireless network is seldom entirely free of wires. The distribution system, which often includes wiring, is generally necessary to tie together the access points, access controllers, and servers. In most cases, the common Ethernet comprises the distribution system.	