



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 judgment 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.

1. a) Attempt any SIX of the following:

Marks 12

i) List any two applications of computer network.

(Listing of any 2 applications- 1 Mark each)

Ans: Applications of Computer Network

- 1) Banking
- 2) Video conferencing
- 3) Marketing
- 4) School
- 5) Radio
- 6) Television
- 7) E-mail

ii) List any four types of computer network by considering geography.

(Listing of any 4 networks - 1/2 Mark each)

Ans: LAN - Local Area Network

MAN - Metropolitan Area Network

WAN - Wide Area Network

CAN - Campus Area Network

HAN - Home Area Network

PAN - Personal Area Network



iii) Give two advantages of mesh topology.

(Any 2 advantages - 1 Mark each)

Ans: Advantages of Mesh topology:

- Dedicated Links: Dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices
- It is robust. If one link becomes unusable, it does not incapacitate the entire system
- It is Secure. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages
- Point to Point Connection: Point-to-point links make fault identification and fault isolation easy

iv) Give the names of various N/W connecting devices (Any two).

(Listing of any 2 control devices -1 Mark each)

Ans: N/W connecting device:

- Repeater
- Hub
- Switch
- Bridge
- Router
- Gateway
- Modem

v) List any two advantages of optical fiber cable.

(Any two advantages- 1 Mark each)

Ans: Advantages of optical fiber cable:

- 1) Higher bandwidth
- 2) Less signal attenuation
- 3) Immunity to electromagnetic interference
- 4) Resistance to corrosive materials

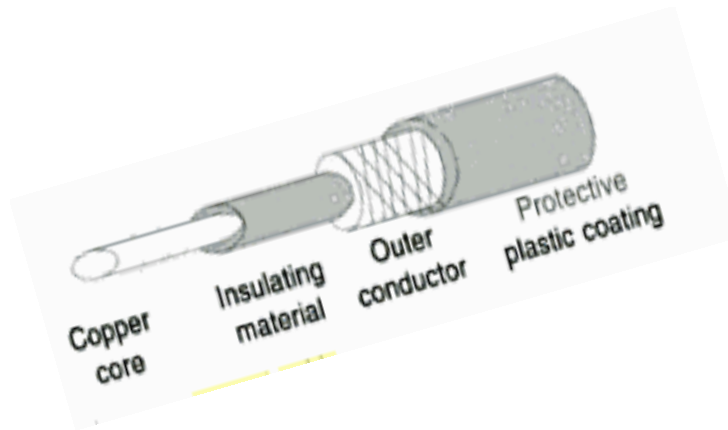


- 5) Light weight
- 6) Greater immunity to tapping
- 7) Easily available

vi) Draw the sketch of co-axial cable (cross-sectional view)

(Diagram-1 Mark, Labeling- 1 Mark)

Ans:



vii) Define 'Protocol' with reference to computer network. What is the function of IP?

(Definition of protocol - 1 Mark, Function of IP - 1 Mark)

Ans: **Protocol:** - Protocol 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.

Protocol defines.

- a) Syntax (what is to be communicated)
- b) Semantics (how is it to be communicated)
- c) Timing (When it should be communicated)

Function of IP:

- a. Addressing
- b. Routing
- c. Data encapsulation
- d. Fragmentation & reassembly



viii) List any two components which works at physical layer of OSI model.

(Listing of any 2 components – 1 Mark each)

Ans: Repeater

- 1) Hub
- 2) Network Interface card (NIC)
- 3) Cables
- 4) Connectors

b) Attempt ant TWO of the following:

Marks 08

i) Describe four advantages of computer network.

(Any 4 advantages – 1 Mark each)

Ans: Advantages of computer network:

1. **Access to remote information:** -Access to remote information comes in many forms. It can be surfing the World Wide Web for information or just for fun. Information available includes the arts, business, cooking, government, health, history, hobbies, recreation, science, sports, travel, and many others.
2. **Resource Sharing:** Programs, data equipment are made available to every node on the network.
Example: Printer sharing, LAN
3. **Saving Money:** Reducing equipment cost by sharing data resources, software's etc.
4. **High Reliability:** All files are copied on no of computers, if one of the computer becomes unavailable then the file can be read from other available system
5. **Providing powerful communication Medium:** Using network it is easy for two or more people, who live far apart can write report together.
6. **Person-to-person communication:** Email, chats is already widely used by millions of people to routinely share audio, video and text documents.
7. **Interactive entertainment:** Real-time streaming is possible because of network
8. **Electronic commerce:** E-commerce is trading in products or services conducted via computer networks such as the Internet. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange.



ii) Compare Bus topology and Ring topology (four points).

(Any 4 points – 1 Mark each)

Ans:

	Factors	BUS	RING
1.	Configuration	Moderate	Difficult
2.	Type	It is passive Topology	It is Active Topology
3.	Troubleshooting	Difficult	More Difficult
4.	Media Failure	Entire N/W collapse	Entire network collapse
5.	Failure of Node	Partially affected	Entire N/W Collapse
6.	Addition of a node	Bit difficult as entire N/W has to shut down and then a node can be added	Very difficult as entire N/W has to shutdown and then node can be added and entire N/W has to reconfigure
7.	Cables and connectors used	T- Connector, BNC Connector, Terminator, Co-axial cable	T-Connector, BNC connector, Co-axial Cable OR Fiber optic connector and fiber optic cable
8.	LAN Card used	Ethernet	Ethernet OR Fiber Optic Card
9.	Reliability	Lower	Moderate

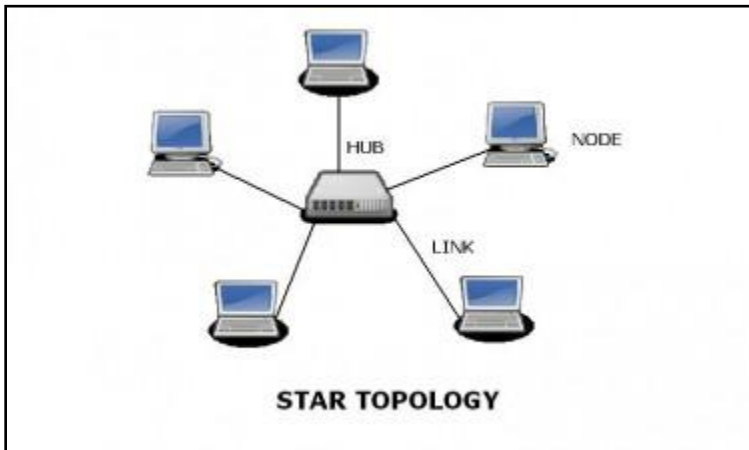


iii) Suppose you are going to implement a computer network in a small business mall. Which topology will you use? Why?

(Determining the topology -2 Marks, Justification - 2 Marks)

Ans: Which topology will you use? Why?

STAR Topology



In star topology, each computer or node is connected to a central hub. This is more reliable than a classical ring topology because a node failing will not bring down entire network. A bus topology arguably is more reliable but it has poor performance.

Advantages:

- 1.Highly reliable
- 2.Adding new node is very easy
- 3.Failure of any node does not affect the network
- 4.Troubleshooting is very easy



2. Attempt any **FOUR** of the following:

Marks 16

a) Name the types of server used in server-based network.

Describe the working of such a network.

(Listing of servers - 2 Marks, Brief Explanation- 2 Marks)

Ans: Types:

1. Application Server
2. Message Server
3. Database Server
4. Web server

DESCRIPTION:

Application Servers: The application server often serves to connect database servers with the end-user, thus acting as a kind of "middleware" that releases stored information requested by said user. The server is usually responsible for properly decoding and recoding data and providing security over connections.

Message Servers: These servers provide instant, real-time communication between users, regardless of where a user may be. Message servers allow a wide variety of communication methods, from simple forms such as text to more complex forms such as video, audio and graphics.

Database Servers: These servers manage the database that is stored in that server using the SQL database management system. A client request is sent in the form of an SQL query to the server. That server in turn searches through the database for the requested information and sends the results to the client.



Web Servers: Web servers provide access to the Internet through the HyperText Transfer Protocol (HTTP). Files in a web server use HyperText Markup Language (HTML) to display content on web browsers. A web server usually receives requests from a web browser and sends back the requested HTML file and related graphic files.

b) Explain any four benefits of computer network.

(Any 4 benefits – 1 Mark each)

Ans: Benefits of computer network:

1. **File sharing:** -files can be centrally stored and used by multiple users. Shared directory or disk drive is used. If many users access same file on network and make changes at same time and conflict occurs. Network operating system performs file sharing and provides security to share files.
2. **Printer sharing:** Printer connected in a network can be shared in many ways. Use printer queues on server. Here printer is connected to server. Each work station can access printer directly. Printer can be connected to server. Connect a printer to a computer in a network and run special print server software. Use built in print server. Use dedicated print server. By printer sharing reduces no. of printers needed. Share costly and high quality printers.
3. **Application services:** Share application on a network. When applications are centralized, amount of memory required on disk of work station is reduced. It is easier to administer an application. It is more secure and reliable. It is faster and convenient.
4. **E-mail services.** Two types of email systems are available:
 - 1) File based system: Files are stored in shared location on server. Server provides access to file. Gate way server connects from file based email system to internet.
 - 2) Client server e-mail system: E-mail server contains message and handles e-mail interconnections. E-mail client functions (also consider other e-mail functions): read mail, send, compose, forward, delete.
E-mail protocols: SMTP, POP etc.
5. **Remote access:** Set up remote access service on network operating system. Setup VPN (virtual private network) on internet terminal services (TELNET). User can access files from remote location. User can access centralized application or share files on LAN.



c) Describe various factors to be considered while selecting transmission media.

(Any 4 factors - 1 Mark each)

Ans:

1. Cost & Ease of installation: Costing is an important factor, when we select a media. Because absolute cost and ease of installation data are difficult to provide without referring to specific implementations, one can make relative judgments by comparing each medium to the others.

2. Type of cable: Coaxial cable, Twisted Pair Cable, Fiber Optic Cable

3. No of conductors/connectors: RJ-45, BNC, LC & ST

4. Noise: It leads to distortion of a signal. Noise immunity of transmission media is considered at the time of selecting particular network.

5. Bandwidth: Higher bandwidth transmission media support higher data rate.

6. Radiation: It is leakage of signal from media caused by undesirable characteristics of media.

7. Durability: Life span of media

8. Interference: interference occurs when undesirable electromagnetic waves affect the signal. Interference can be caused by many factors, including

- Electromagnetic Interference (EMI)
- Radio wave interference (RFI)

9. Attenuation: Attenuation refers to the tendency of electromagnetic waves to weaken or become distorted during transmission. It is loss of energy as the signals propagates outwards. Attenuation increases with distance, as a wave passes through a medium, some of its energy is absorbed or scattered by the medium's physical properties.

d) Describe two application of

i) twisted pair cable

ii) co-axial cable

(Any 2 applications of each – 1 Mark each)

Ans: i) Twisted pair cable

1. Telephone lines.
2. Local area Network
3. DSL Lines



ii) Co-axial cable

1. Television Systems
2. Connecting VCRs to television
3. Ethernet LANs

e) What are the various components of computer network.

Describe any one.

(Listing of Components - 2 Marks, Explanation (any one) - 2 Marks)

Ans: Components of Computer networks:

1. Computers (two or more)
2. Network Operating System software.
3. Network Interface card (on each Computer)
4. Cables that connects the computers to each other (coaxial cable, Fiber optic cable or twisted pair cable)
5. Network devices such as routers, gateways, switch, hub, bridges, connectors.

Description:

1. Computers: Set of Computers with latest configuration.

Example: Intel Processor core i3/i5/i7 or latest with motherboard cheapest 41/61 with 4 USB, 1 Serial port, 4GB RAM DDR III, 500 GB Hard disk.

2. Network Operating System refers to software that implements an operating system of some kind that is oriented to computer networking. For example, one that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions

Example: Windows Server 2003/08/12, UNIX SERVER.

3. NIC (Network interface card / network adapter): It physically makes the connection, works as interface between computer and network cable.

Functions of NIC:

1. Provide physical link or connectivity between computer and the network physical medium.
2. Prepare data from computer for network cable.
3. Send data to another node in network.
4. Control flow of data between computer and physical medium



4. Cables:

1. Co-axial Cable: It is made of two conductors that share a common axis. The center of the cable is stiff solid copper wire or stranded wire encased in insulating plastic foam. The foam is surrounded by the second conductor, a wire mesh tube which serves as a shield from EMI. A tough insulating plastic tube forms the cover of the cable

2. Twisted Pair Cable: They are formed by twisting of two insulated copper wires. One or more twisted pairs are combined within a common jacket. Twisting the copper wires reduces Crosstalk.

Types:

- i) Unshielded Twisted Pair Cable (UTP)
- ii) Shielded Twisted Pair Cable (STP)

3. Fiber optic cable: It is made of a light-conducting glass or plastic core surrounded by more glass called cladding, and tough outer sheath. The center core provides the light path or wave guide while the cladding is composed of varying layers of reflective glass.

5. Network Connecting Devices:

1. **Repeaters:** A repeater works at the physical layer of the OSI Reference Model to regenerate the network's signals and resend them out on other segments.

2. **Router:** It is a device that attaches two or more network & forward packets according to information found in routing table

3. **Hub:** It is a device used in Star Topology that connects the computers in a LAN. Hubs are Passive, Active or Hybrid. It is a Multicast device

6. Connectors: To connect cables between two computers

Example: RJ-45, BNC



f) Compare guided and unguided media used in computer network.

(Any 4 points – 1 Mark each)

Ans:

GUIDED MEDIA	UNGUIDED MEDIA
Also called as bounded or wired media	Also called as unbounded or wireless media
Point to point connection i.e. signal travelling is directed	Used for radio broadcasting in all directions i.e. signal travelling is undirected
Transport signal in electric current or light/ beam	Transport signal in the form of electromagnetic waves
Unidirection, not broadcast	Broadcast
Installation is costly and time consuming	Installation needs less time and money
Wired media leads to discrete network topologies	Wireless media leads to continuous network topologies
Attenuation depends exponentially on the distance	Attenuation is proportional to square of the distance
Example: Twisted Pair cable, Coaxial cable, Fiber optic cable	Example: Radio, Infrared light, Microwave

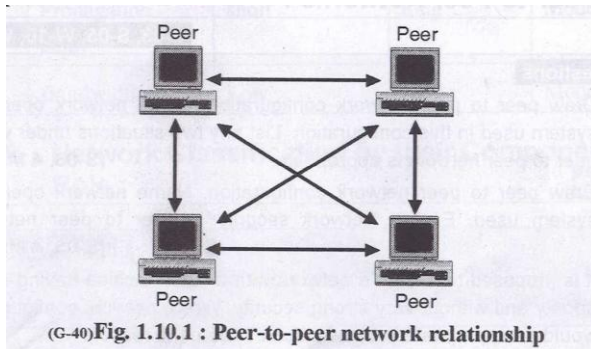
3. Attempt any **FOUR** of the following:

Marks 16

a) Describe the concept of peer-to-peer network. Where it is used?

(Peer to peer concept explanation-2 Marks, Diagram - 1 Marks, Use - 1 Mark)

Ans: Peer to peer (P2P) is an alternative network model to that provided by traditional client-server architecture. P2P networks use a decentralised model in which each machine, referred to as a peer, functions as a client with its own layer of server functionality. A peer plays the role of a client and a server at the same time. That is, the peer can initiate requests to other peers, and at the same time respond to incoming requests from other peers on the network. It differs from the traditional client-server model where a client can only send requests to a server and then wait for the server's response.



1. Peer to Peer networks do not have a central control system. There are no servers in peer networks.
2. In this type of network users simply share disk space and resources, such as printers and faxes.
3. Peer networks are organised into workgroups. Workgroup have very little security. There is no central login process.
4. If the user has logged into one peer on the network he can use any resources on the network that are not controlled by a specific password.
5. Access to individual resource can be controlled if the user who shared the resources requires a password to access it.
6. Since there is on central security, the user will have to know individual password for each secured shared resources he wishes to access.

The peer to peer networks are suitable/used for the following working conditions.

1. If security is not important.
2. If the number of users is less than 10.
3. If all the users are situated in the same area.
4. If the possibility of future expansion is less.

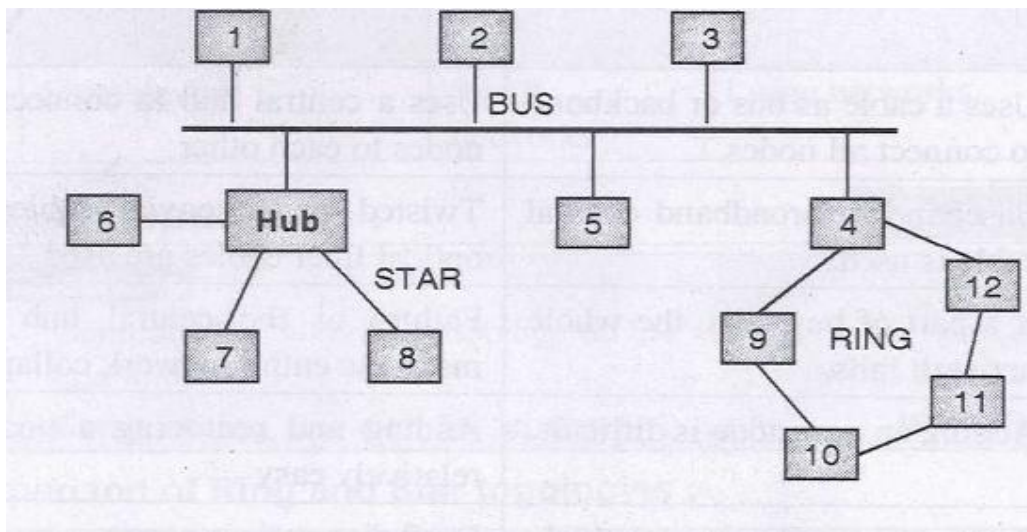
b) Describe with neat sketch “Hybrid topology” Give its applications.

(Hybrid topology explanation-2 Marks, Diagram -1 Mark, Use - 1 Mark)

Ans: A combination of two or more different topologies makes for a hybrid topology. When different topologies are connected to one another, they do not display characteristics of any one specific topology.

WORKING OF Hybrid Topology

The Hybrid topology scheme combines multiple topologies into one large topology. The hybrid network is common in large wide area networks. Because each topology has its own strengths and weaknesses, several different types can be combined for maximum effectiveness.



ADVANTAGES of Hybrid Topology

- 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:** Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while their weaknesses are neutralized.

DISADVANTAGES of Hybrid Topology

1) **Complexity of Design:** One of the biggest drawbacks of hybrid topology is its design. It is not easy to design this type of architecture and it is a tough job for designers. Configuration and installation process needs to be very efficient.

2) **Costly Hub:** The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should function even if a part of network is down.

3) **Costly Infrastructure:** As hybrid architectures are usually larger in scale, they require a lot of cables, cooling systems, sophisticated network devices, etc.

Applications: widely used in WAN.

c) **What is meant by subnet? How to use subnet masking to create two subnets?**

(Explanation of subnet -2 Marks, Subnet masking explanation with any suitable example - 2 Marks)

Ans: A **subnet** is a logical grouping of connected network devices. Nodes on a subnet tend to be located in close physical proximity to each other on a LAN.

Network designers employ subnets as a way to partition networks into logical segments for greater ease of administration. When subnets are properly implemented, both the performance and security of networks can be improved.



In Internet Protocol (IP) networking, devices on a subnet share contiguous ranges of IP address numbers. A mask (known as the *subnet mask* or network mask) defines the boundaries of an IP subnet. The correspondence between subnet masks and IP address ranges follows defined mathematical formulas. IT professionals use *subnet calculators* to map between masks and addresses.

Subnet masking for 2 subnet:

To calculate the number of subnets or nodes, use the formula $(2^n - 2)$ where n = number of bits in either field, and 2^n represents 2 raised to the n th power. Multiplying the number of subnets by the number of nodes available per subnet gives you the total number of nodes available for your class and subnet mask. Also, note that although subnet masks with non-contiguous mask bits are allowed, they are not recommended.

Example:

10001100.10110011.11011100.11001000	140.179.220.200	IP Address
11111111.11111111.11000000.00000000	255.255.192.000	Subnet Mask
10001100.10110011.11000000.00000000	140.179.192.000	Subnet Address

Hence

Subnet number	Address
1	140.179.64.0
2	140.179.128.0

d) Describe horizontal and vertical communication.

(Horizontal Comm.-2 Marks, Vertical Comm.- 2 Marks)

Ans: Horizontal communications

- The horizontal communication between the different layers is logical; there is no direct communication between them. Information included in each protocol header by the transmitting system is message that will be carried to the same protocol in the destination system.



- For two computers to communicate over a network, the protocols used at each layer of the OSI model in the transmitting system must be duplicated at the receiving system.
- The packet travels up through the protocol stack and each successive header is stripped off by the appropriate protocol and processed.
- When the packet arrives at its destination, the process by which the headers are applied at the source is respected in reverse.
- The protocol operating at the various layers communicate horizontally with their counterparts in the other system, as shown in below fig.

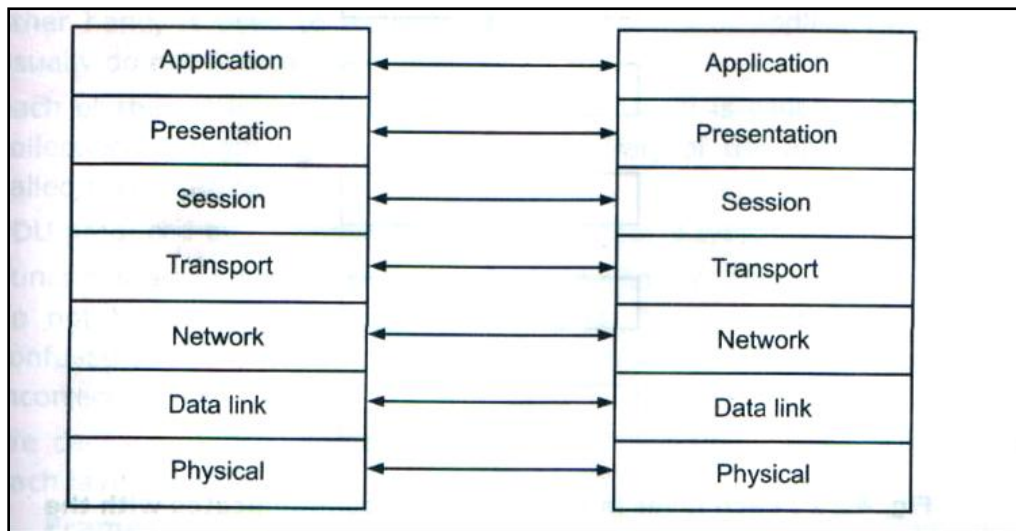


Fig: Horizontal communications

Vertical Communications

- In addition to communicating horizontally with the same protocol in the other system, the header information also enables each layer to communicate with the layer above and below it.
- The headers applied by the different protocols implemented the specific functions carried out by those protocols.
- For Example: When a system receives a packets and passes it up through the protocol stack, the data link layer protocol header includes a field that identifies which network-layer protocol the system should use to process the packet.
- Network –layer protocol header in turn specifies one of the transport-layer protocols and the transport-layer protocol identifies the application for which the data is ultimately destined.



- Vertical communication makes it possible for a computer to support multiple protocols at each of the layers simultaneously.

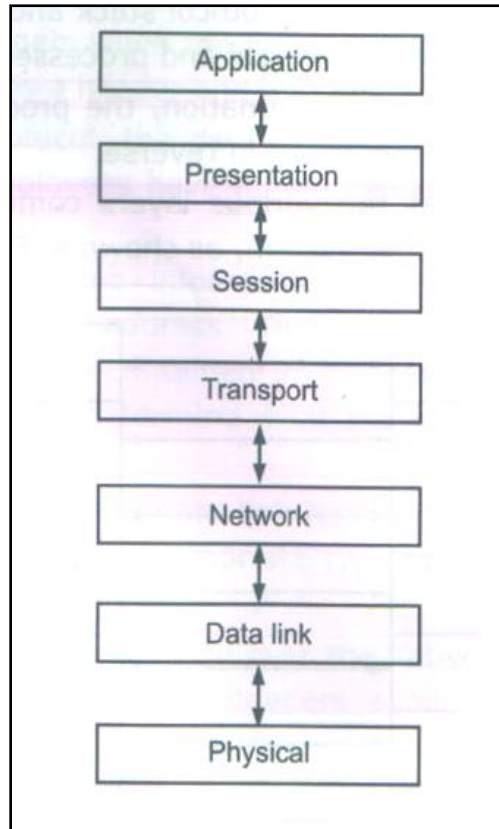


Fig: Vertical communications

e) Describe the importance/role of presentation layer in OSI model.

(Any 4 importance/functions of presentation layer – 1 Mark each)

Ans: Role of presentation layer in OSI model the presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

The form and syntax (language) of the two communicating systems can be different e.g. one system is using the ASCII code for file transfer and the other one user IBM's EBCDIC.

Under such condition the presentation layer provider the “translation” from ASCII to EBCDIC and vice versa.



The presentation layer performs the following function:

1. It translates data between the formats the network requires and the format the computer expects.
2. It does the protocol conversion
3. For security and privacy purpose it carries out encryption at the transmitter and decryption at the receiver.
4. It carries out data compression to reduce the bandwidth of the data to be transmitted.
5. Unlike the session layer, which provides many different functions, the presentation layer has only one function.
6. It basically functions as a pass through device. It receiver primitives from the application layer and issues duplicate primitives to the session layer below it using the Presentation Service Access point (PSAP) and Session Service Access point (SSAP)

f) Explain the working of “File Transfer Protocol” with a neat diagram.

(Working - 3 Marks, Diagram 1 Mark)

Ans: FTP is a stranded mechanism provided by the Internet for copying a file from one host to the other.

1. Some of the problem in transferring files from one system to the other are as follows:
 - Two systems may use different file name conventions.
 - Two systems may represent text data in different types.
 - The directory structure of the two systems may be different.
2. FTP provides a simple solution to all these problems.
3. The basic model of FTP is shown
4. FTP established two connections between the client and server. One is for data transfer and the other is for the control information.
5. The fact that FTP separates control and data makes it very efficient.
6. The control connection uses simple rules of communication. Only one line of command or a line of response is transferred at a time.



7. But the data connection uses more complex rules due to the variety of data types being transferred.
8. FTP uses port 21 for the control connection and port 20 for the data connection.
9. As shown in the figure client has three components namely:
 - i. User interface
 - ii. Control process and
 - iii. Data transfer process.
10. The Server has two components: the control process and data transfer process.
11. The control connection is maintained during the entire interactive FTP session. The data connection is first opened, file is transferred and data connection is closed. This is closed. This is done for transferring each file.

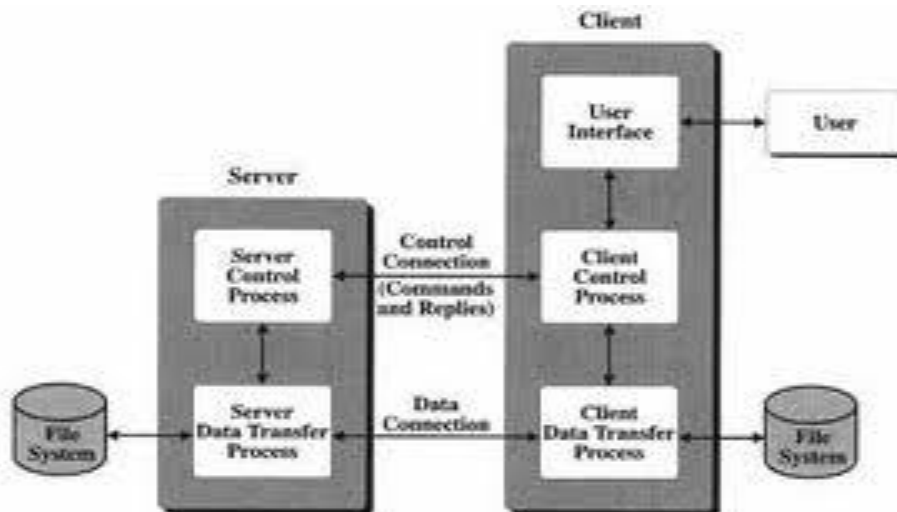


Fig. Basic Model Of FTP

Control connection:

- This connection is created in the same way as the other application programs described earlier.
- Control connection remains alive during the entire process.
- The IP uses minimize delay type services because this is an interactive connection between a user and server.

Data Connection:



- Data connection uses the port 20 at the site. This connection is opened when data to be transferred is ready and it is closed when transfer of data is over.
- The service types used by IP is maximize throughput.

4. Attempt any **FOUR** of the following:

Marks 16

a) Describe TCP used in computer communication.

(Any 4 Services/ Relevant explanation – 1 Mark each)

Ans: Following are some of the services offered by TCP to the process at the application layer:

1. Stream delivery service
2. Sending and receiving buffers
3. Bytes and segments
4. Full duplex service
5. Connection oriented service
6. Reliable service.
7. Process to process communication

1. Stream delivery service:

TCP is a stream oriented protocol. It allows the sending process to deliver data as a stream of bytes and the receiving process to obtain as a stream of bytes.

TCP creates a working environment in such a way that the sending and receiving processes seem to be connected by an imaginary “tube”

This is called as stream delivery service.

2. Sending and receiving buffers:

The sending and receiving process may not produce and receive data at the same speed.

Hence TCP needs buffers for storage. There are two types of buffers used in each direction:

- 1) Sending buffer
- 2) Receiving buffer.

A buffer can be implemented by using a circular array of 1 byte locations as shown

The movement of data in one direction on the sending side the buffer has three types of locations:



1. Empty Locations
2. Location containing the bytes which have been sent but not acknowledgement. These bytes are kept in the buffer till an acknowledgement is received.
3. The locations containing the bytes to be sent by the sending TCP.

3. Bytes and segments:

- Buffering is used to handle the difference between the speed of data transmission and data consumption.
- But only buffering is not enough. We need one more step before sending the data.
- The IP layer, as a service provider for TCP, need to send data in the form of packets and as a stream of bytes.
- At the transport layer, TCP groups a number of bytes together into a packet called a segment.
- A header is added to each segment for the purpose of exercising control.
- The segments are encapsulated in an IP datagram and then transmitted. The entire operation is transparent to the receiving process.
- The segments may be receiver out of order, lost or corrupted when it reaches the receiving end.

4. Full duplex service:

TCP offers full duplex service where the data can flow in both the direction simultaneously. Each TCP will then have a sending buffer and receiving buffer.

The TCP segments are sent both the directions.

5. Connection oriented service:

TCP is a connection oriented protocol. When process -1 wants to communicate (send and receive) with another process (process-2), the sequence of operations is as follows:

TCP of process -1 informs TCP of process -2 and gets its approval.

TCP of process -1 and TCP of process -2 exchange data in both the directions.

After completing the data exchange, when buffers on both sides are empty, the two TCPs destroy their buffers.



1. The type of connection in TCP is not physical, it is virtual. The TCP segment is encapsulated in an IP datagram and can be sent out of order.
2. These segments can get lost or corrupted and have to be resent.
3. Each segment may take a different path to reach the destination.

6. Reliable services:

TCP is a reliable transport protocol. It uses an acknowledgment mechanism for checking the safe and sound arrival of data.

7. Process to process communication:

The TCP user port numbers a transport layer addresses.

Show some well known port number used by TCP.

Note that if an application can use both UDP and TCP, the same port number is assigned to this application.

b) Computer IPv4 and IPv6 (four points).

(Any four points -1 Mark each)

Ans:

IPv4	IPv6
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.

c) **Explain handoff procedure of cellular mobile phone.**

(Handoff Procedure -2 Marks, Types of Handoff – 2 Marks)

Ans: Assume that there is a call going on between two parties over a voice channel.

When the mobile unit moves out of coverage area of a particular cell site the reception becomes weak.

Then the cell site will request a **hand off**.

The system will switch the call to a new cell site without interrupting the call or changing the user. This procedure is called as the hand off procedure or handover procedure.

Following are various types of handoffs. Supported by a Mobile Station (MS):

1. Hard Hand Off
2. Soft Hand off
3. Queued hand off
4. Delayed hand off
5. Forced hand off

**1. Hard hand off:**

A hard handoff is a handoff technique used with cellular networks that requires the user's connection to be entirely broken with an existing base station before being switched to another base station.

2. Soft hand off:

The hand off is known as soft handoff if the MS starts communication with a new base station without stopping the communication with the older base station.

3. Delayed Hand off:

In many situations, instead of one level, a two level handoff procedure is used, in order to provide a high opportunity for a successful handoff. A hand off can be delayed if on available cell take the call.

4. Forced handoff :

A forced handoff is defined as the off which would normally occur but prevented from happening or a handoff that should not occur but is forced to happen.

5. Queued handoff:

In the queued handoff process, the MTSO arranges the handoff requests in a queue instead of rejecting them, if the new cell sites are busy.

d) Describe meaning and function of:**i) MAC address****ii) IP address**

(MAC address explanation- 1 Mark, Example- 1 Mark)

Ans: i) MAC Address:

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as **hardware** addresses or **physical** addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:



MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer.

Example,

00:A0:C9:14:C8:29

ii) IP Address:

(IP address Explanation -1 Mark, Example – 1 Mark)

An **Internet Protocol address (IP address)** is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

1. The IP address consists of two parts namely a network identifier and a host identifier.
2. All the computers on a particular subnet will have the same network identifier but different host identifiers
3. The internet Assigned Number Authority (IANA) assigns network identifiers to avoid any duplication of addresses.
4. An IPv4 address consists of two parts. The first part of the of the address, called the network number, identifies a network on the internet; the remainder, called the host ID, identifies an individual host on that network.

Classful Addressing:

The IPv4 addresses are classified into 5 types as follows:

1. Class A
2. Class B



3. Class C
4. Class D
5. Class E

e) **What are the services provided by the network layer of OSI model.**
(Any 4 Services – 1 Mark each)

Ans: The services provided by the network layer of OSI model as follows

1. To route the signals through various channels to the other end.
2. To act as the network controller by deciding which route data should take.
3. To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher levels.
4. The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links)
5. **Logical addressing:** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

f) **Describe in brief:**

- i) **Backing up data**
- ii) **File sharing**

Ans: i) Backing up data (Explanation - 2 Marks)

The process of data backup, data from computer system is copied from the disk to some other medium for keeping it safe.

Such backups are important because it protects the data against any unpredictable, Accidental loss of data due to system failure, computer viruses, or human error.

But taking a backup of individual user's data separately is a time consuming and unorganized.

Hence in a network, the users first save their important data on the central server and then the backup can be taken from the server itself.



This reduces the time and stores the backup data at a single place only. This makes the data retrieval easy.

We can have two or three sets of the entire backup data. This helps in the event of one or two sets getting corrupt. The Duplication of backup data becomes easily possible due to centralization storage.

The centralization backup procedures have become easy now a day due to the advanced technology.

There are two basic network backup strategies:

1. Isolated
2. Centralized

The operating system will provide tools required for data backups. For example windows NT provides a tape backup program called as **backup**.

Some backup Policies are as follows:

1. Full Backup.
2. Incremental Backup.
3. Differential Backup.

ii) File sharing:

(Explanation - 2 Marks)

File sharing is the primary feature of network. Due to use of networks the sharing of files becomes easier.

File sharing requires a shared directory or disk drive to which many users can access over the network; more than one person can make changes to a file at the same time. They might both making conflicting change simultaneously.

Hence most of software programs don't have ability to allow multiple changes to a single file at the same time to resolve this type of problem that might arise.



Network operating systems that perform file sharing also administer the security of these shared files and what kind of access they have. For example: Some user might have permission to view only certain shared files, while other have permission to edit or even delete certain shared files.

Advantages:

1. Easily share information on networking.
2. User needs regular access of word processing files. Spreadsheets so they access easily.

Disadvantages:

1. Conflicting problem arises.
2. Less secure if permission not set proper.

5. Attempt any **FOUR** of the following:

Marks 16

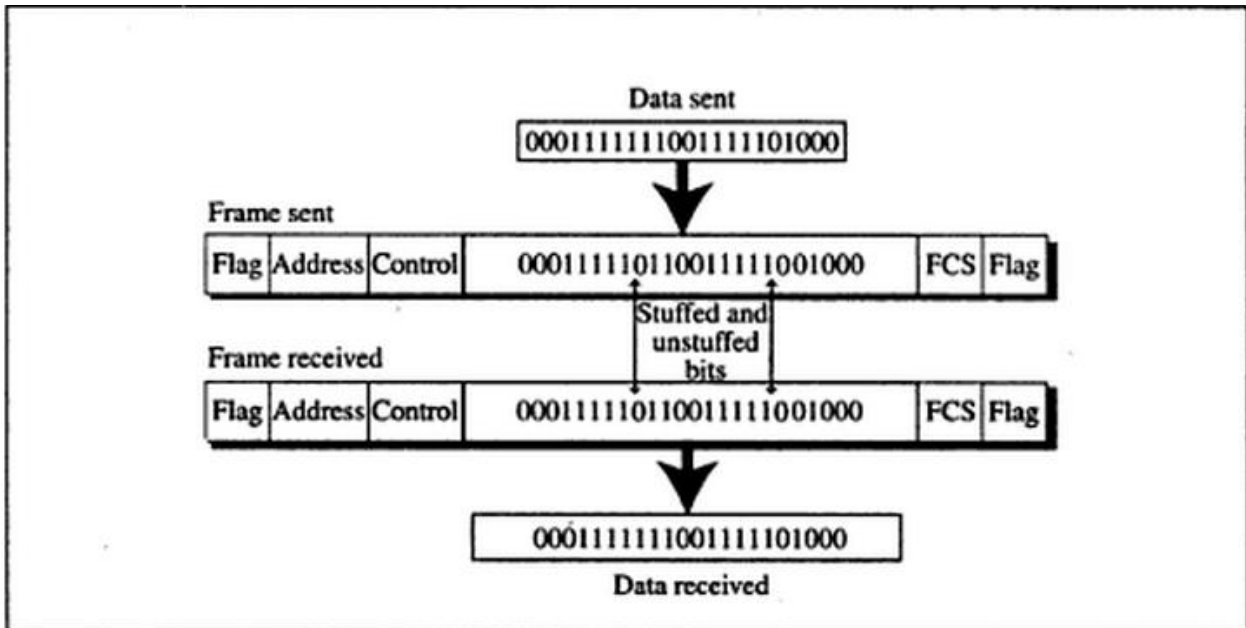
- a) Which layer of OSI model packages raw data bit. Describe bit stuffing with one example.
(Identification of Data link layer - 1 Mark, bit stuffing- 2 Marks, Example- 1 Mark)

Ans: Data link layer of OSI model packages raw data bit.

Bit stuffing:

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1's in the data, so that the receiver does not mistake the pattern 0111110 or a flag.

At sender side the bit is stuffed and at receiver side stuffed bit is removed. As shown in following



For example

Stuffed Bit



Sequence 011111111000 becomes 011111**0**111000.

This extra bit is inserted regardless of sixth bit 0 or 1.

b) In which circumstances star topology is preferred mostly. Name the centralized device used in star topology. Give its two advantages over Hub.

(List of circumstances - 1 Mark, Name of device - 1 Mark, Any Two advantages- 2 Marks)

Ans: star topology is preferred under following circumstances

- 1) When centralized management of nodes is required
- 2) There are more chances of adding or removing nodes in the network.
- 3) When there is a need of robust network. If one link fail only that node is affected.

Switch is the centralized device used in star topology.

Switch has following advantages over HUB

- 1) Switch is point to point networking device because switch send data to only destination node
- 2) Switch is intelligent device because it understands MAC address.



3) Switch works at Data link layer of OSI model, where as Hub works at Physical Layer of OSI model.

4) Switch gives full speed to all connected node, where as Hub Distributes the speed to the all connected nodes.

c) **Describe OSI model with layer structure.**

(Diagram - 1 Mark, Explanation - 3 Marks)

Ans: OSI model (open system interconnection) model was developed by ISO (international standard organization)

Function of OSI model

1) It provides way to understand how internetwork operates.

2) It gives guideline for creating network standard.

OSI model has 7 layers as shown in the figure.

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Datalink Layer
Physical Layer

Fig: OSI Reference model.

OSI model has following 7 layers as Physical layer, data link layer, Network layer, Transport layer, session layer, presentation layer, application layer.

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



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

2) Data link layer:

It is responsible for transmitting group of bits between the adjacent nodes. The group of bits is called as frame. The network layer passes a data unit to the data link layer. Header and trailer is added to the data unit by data link layer. This data unit is passed to the physical layer.

Data link layer is responsible for moving frames from one node to the next.

Functions of data link layer are:

- 1) Framing
- 2) Physical addressing
- 3) Flow control
- 4) Error control
- 5) Media access control
- 6) Node to node delivery

3) Network layer:

It is responsible for routing the packets within the subnet i.e. from source to destination. It is responsible for source to destination delivery of individual packets across multiple networks. It ensures that packet is delivered from point of origin to destination.

Functions of network layer:

- 1) logical addressing
- 2) Routing.
- 3) Congestion control
- 4) Accounting and billing
- 5) Address transformation
- 6) Source host to destination host error free delivery of packet.



4) Transport layer:

Responsibility of process to process delivery of message

Ensure that whole message arrives in order.

- 1) Service point addressing
- 2) Segmentation and reassembly
- 3) Connection control
- 4) Flow control: Flow control is performed end to end
- 5) Error control

5) Session layer:

Establishes, maintains, synchronizes the interaction among communication systems

It is responsible for dialog control and synchronization

- 1) Dialog control
- 2) Synchronization, session and sub session
- 3) Session closure

6) Presentation layer: It is concerned with syntax, semantics of information exchanged between the two systems.

Functions: Translation, encryption, compression

7) Application layer: It enables user to access the network. It provides user interfaces and support for services like email, remote file access.

Functions: network virtual terminal, file transfer access and management, mail services and directory services

d) Explain the working of “TELNET”

(Explanation - 4 Marks)

Ans: TELNET

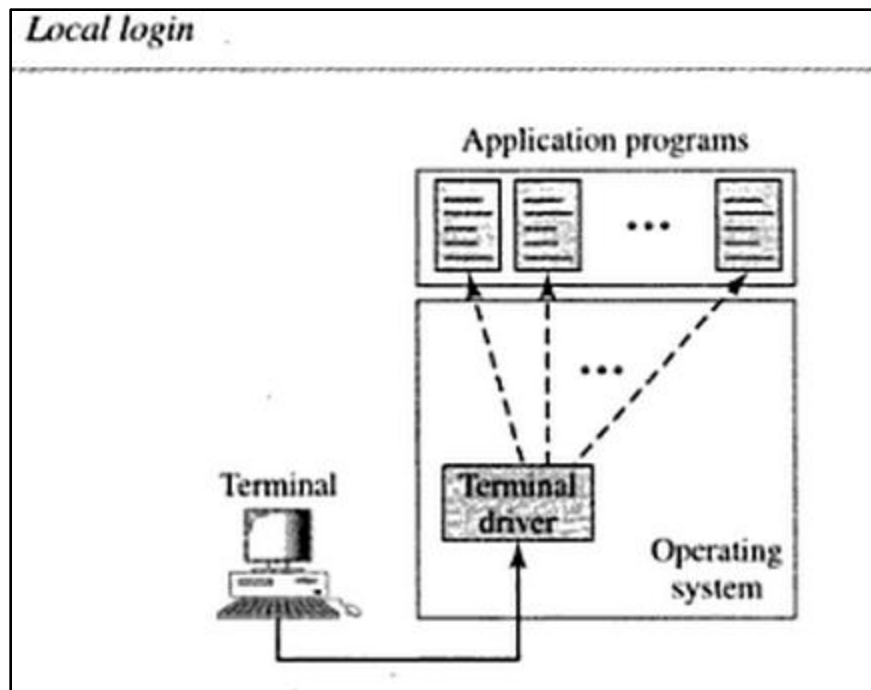
TELNET is abbreviation for Terminal Network. It is standard TCP/IP protocol for virtual terminal services proposed by ISO. TELNET enables establishment of connection to a remote system in such a way that a local terminal appears to be terminal at remote system.

TELNET is general purpose client server application program.



Local Login

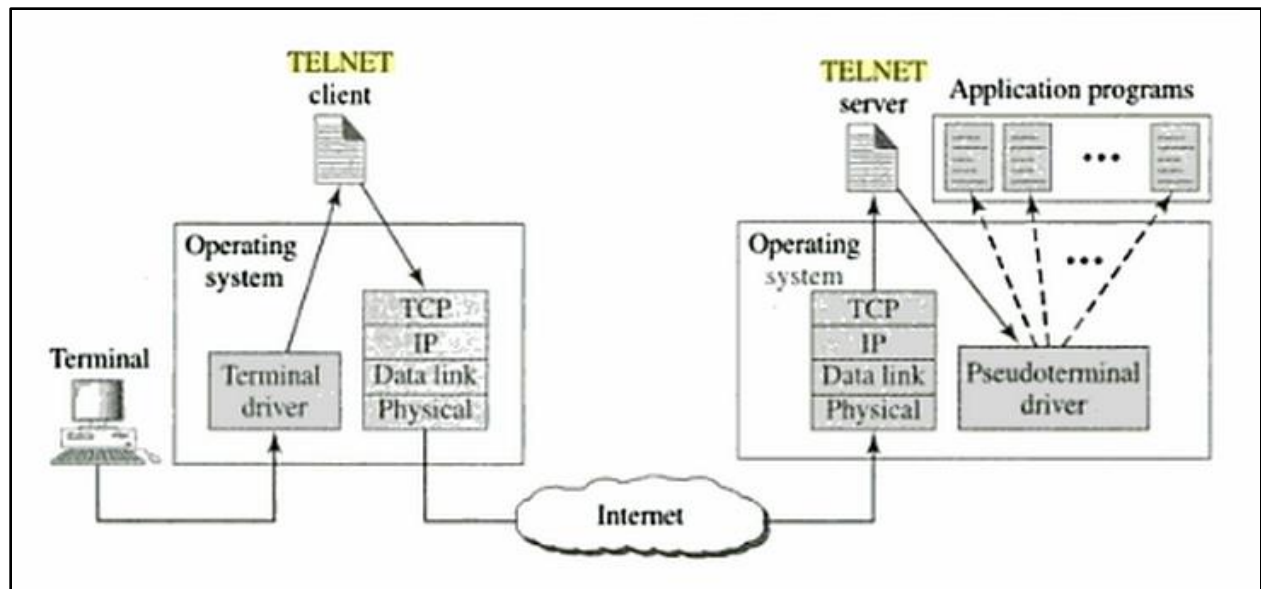
When user log in to local time sharing system it is called local login. The keystrokes accepted by terminal driver. Terminal driver passes the character to the operating system. Operating system, in turn interprets the combination of character and invoke the desired application or utility.



Remote login

When user wants to access the application or utility located at the remote machine, he or she performs remote login. Here the telnet client and server program come into use.

The user sends the keystrokes to local operating system. local operating system accept is, but do not interpret them. The characters are send to TELNET client. TELNET client transform the character to a universal character set called Network Virtual Terminal Character and deliver them to the local TCP/IP stack.



As shown in above figure the command/text in NVT form travel through internet, and arrive at TCP/IP stack of remote Machine. Here the characters are delivered to the operating system and Passed to the TELNET server. Which changes the characters to the understandable characters by the remote computer. However characters could not directly pass to the operating system because remote operating system is not designed to receive characters from TELNET server. The solution is to add piece of software called Pseudo- terminal driver, which pretends that characters are coming from terminal. The operating system passes the characters to appropriate application program.

e) **Which different classes are used for IP addressing. Describe each in brief.**

(Listing of classes - 1 Mark, Explanation - 3 Marks)

Ans: IP Address is classified into 5 types as

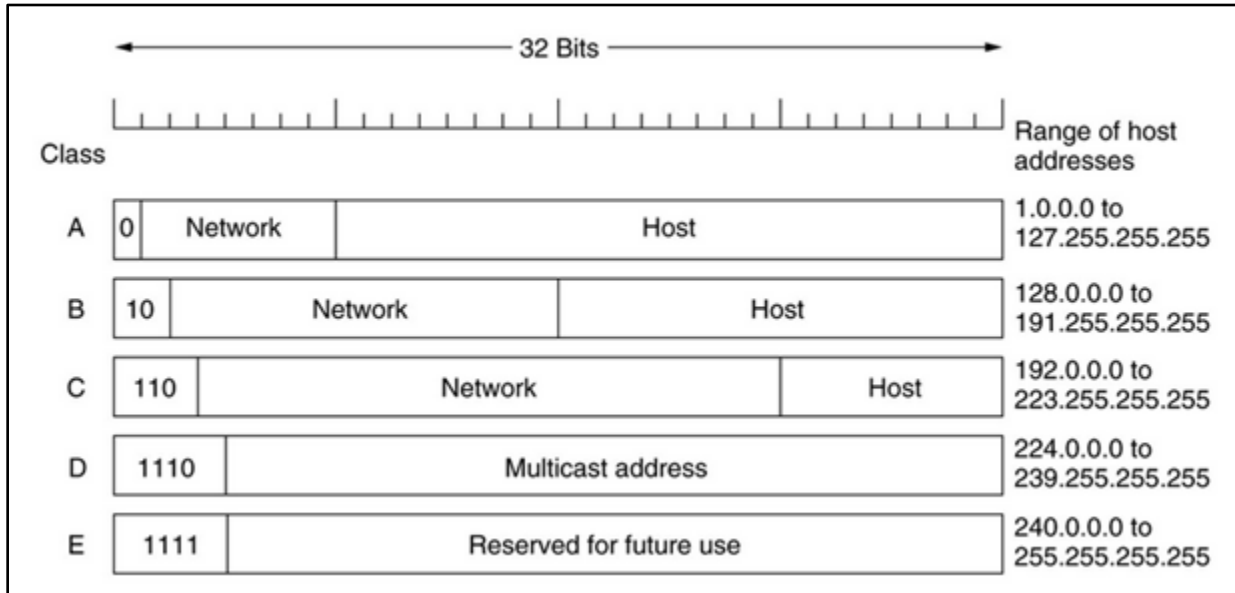
Class A

Class B

Class C

Class D

Class E



Class A format



In this 7bits are used for network field and 24 bits for host field.

Class A IP address range includes 1.0.0.0 to 127.255.255.255

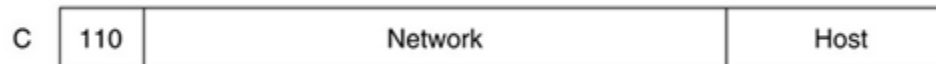
Class B format



In this 14 bits are used for network field and 16 bits for host field.

Class B IP address range includes 128.0.0.0 to 191.255.255.255

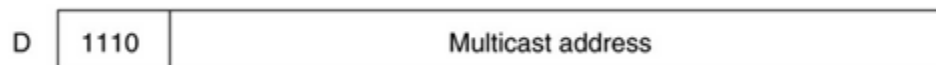
Class C format



In this 21 bits are used for network field and 8 bits for host field.

Class C IP address range includes 192.0.0.0 to 223.255.255.255

Class D format

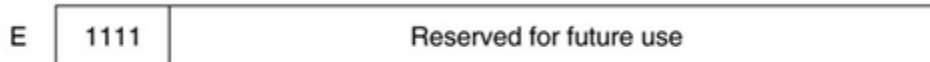




Class D IP address is used for multicasting

Class D IP address range includes 224.0.0.0 to 239.255.255.255

Class E format



Class E IP address are reserved for future use.

Class E IP address range includes 240.0.0.0 to 255.255.255.255

f) Describe the role of following network device used in computer network

i) Gateway

ii) Router

iii) Hub

iv) Switch

(Each -1 Mark)

Ans: 1) Gateway

- Gateway is protocol converter.
- Gateway enables communication between different network architecture and environments.
- Gateway connects two systems that do not use the same protocol, data format, language and architecture.
- It works at all layers of OSI model.
- Convert commonly used protocols (e.g. TCP/IP) to a specialized protocol (for example, an SNA: System Network Architecture).
- Convert message formats from one format to another.
- Translate different addressing schemes

2) 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 neighboring or distant network
- Connect dissimilar networks.
- Prevent network bottlenecks by isolating portions of a network.

3) 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

4) Switch

- Switch connects all nodes in star topology.
- Switch is point to point networking device.
- Switch sends packets only to destination node.
- It works at Data link layer of OSI model

6. Attempt any **TWO** of the following:

Marks 16

a) Describe TCP/IP with neat sketch. Compare TCP/IP and OSI reference model.

(TCP/IP model digram-2 Marks, explanation 2 Marks, Comparison of TCP/IP with OSI model any 4 points - 4 Marks)

Ans:

TCP/IP Model

Application Layer
Transport Layer
Internet Layer
Network access Layer (Host to Network Layer)



TCP/IP Model contains following layer.

1) Network Access Layer

- It defines characteristics of transmission media.
- It also concern with delivery of data when two systems are attached to same network.

2) Internet Layer –

- This layer permits host to inject packets into network and packet travels independently to destination.
- This layer defines packet format and protocol called IP (internet Protocol)

3) Transport Layer -

- It has TCP and UDP
- TCP (transmission control protocol) –it is Reliable & connection oriented protocol.
- UDP (User Datagram Protocol)- it is Unreliable & connectionless protocol.

4) Application Layer -

- It includes virtual Terminal (TELNET), file transfer Protocol (FTP), simple Mail Transfer Protocol (SMTP) and other protocols like HTTP, WWW, DNS.
-

Comparison of TCP/IP model with OSI model.

Sr.No.	TCP/IP MODEL	OSI MODEL
1	It has 4 layers	It has 7 layers
2	Function of presentation layer are performed by application layer	It has separate presentation layer
3	Function of session layer are performed by transport layer	It has separate session layer
4	Transport layer supports both connection oriented and connection less services.	Transport layer support only connection oriented services.
5	It is difficult to add a new protocol in existing protocol stack.	Adding a new protocol is easy.



6	Network layer supports only connectionless service	Network layer support both connection oriented and connection less service
7	It is used as internet standard . It describe protocols widely used around internet.	It is generic protocol independent standard. It describes general protocols
8	TCP/IP model not clearly distinguish between services, interface and protocols	OSI model clearly distinguish between services, interface and protocol.
9	Diagram of TCP/IP Model <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">Application Layer</p> <hr/> <p style="text-align: center;">Transport Layer</p> <hr/> <p style="text-align: center;">Internet Layer</p> <hr/> <p style="text-align: center;">Network access Layer (Host to Network Layer)</p> </div>	Diagram of OSI model <div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">Application Layer</p> <hr/> <p style="text-align: center;">Presentation Layer</p> <hr/> <p style="text-align: center;">Session Layer</p> <hr/> <p style="text-align: center;">Transport Layer</p> <hr/> <p style="text-align: center;">Network Layer</p> <hr/> <p style="text-align: center;">Datalink Layer</p> <hr/> <p style="text-align: center;">Physical Layer</p> </div>

b) Describe any two connectionless and connection oriented protocols.

(Any 2 Connectionless protocol- 4 Marks, Any 2 connection oriented protocols - 4 Marks)

Ans: Connectionless protocols:

- 1) IP
- 2) ICMP
- 3) UDP

IP

- IP is internet Protocol.
- It is unreliable protocol because it does not provide any error control and flow control.
- Packets in IP are called “Datagram”



- Datagram is variable length packet with two parts –header and data

ICMP

- It is internet control message protocol.
- It reports error and sends control messages.
- Error reporting messages include – destination unreachable, source quench , time exceed, parameter problem , redirection etc.
- Query message includes –echo request and reply, time stamp request and reply, router solicitation and advertisement. etc

UDP

- UDP is user datagram protocol.
- It is connectionless protocol because data is sent without establishing a connection between sender and receiver before sending the data.
- UDP is unreliable because data is delivered without acknowledgement.
- UDP does not perform Auto retransmission.
- UDP does not use flow control .
- UDP has high transmission speed.

Connection oriented protocol:

- 1) TCP
- 2) SLIP
- 3) PPP
- 4) SMTP

TCP

- TCP is transmission control protocol.
- It is connection oriented protocol because connection must be establish prior to transmission of data.
- TCP is reliable protocol because data is delivered with acknowledgement.
- TCP perform Auto Retransmission if the data is lost.
- TCP use flow control.



- TCP has low speed of transmission.

SLIP

- SLIP is serial line internet protocol
- SLIP does not perform error detection and correction.
- SLIP does not provide any authentication.
- SLIP is not approved internet standard.
- SLIP supports only Internet protocol (IP)
- SLIP supports static IP address assignment

PPP

- PPP is point to point protocol.
- PPP perform error detection
- PPP provides authentication and security.
- PPP is approved internet standard.
- PPP supports IP and other protocols.
- PPP supports Dynamic IP address assignment

SMTP

- SMTP is simple mail transfer protocol.
- It is connection oriented text based protocol in which sender communicates with receiver using a command and supplying data over reliable TCP connection.
- SMTP is standard application layer protocol for delivery of email over TCP/IP network.
- SMTP establish a TCP connection between Sender And port number 25 of receiver



c) Explain following wireless technologies used in computer communication:

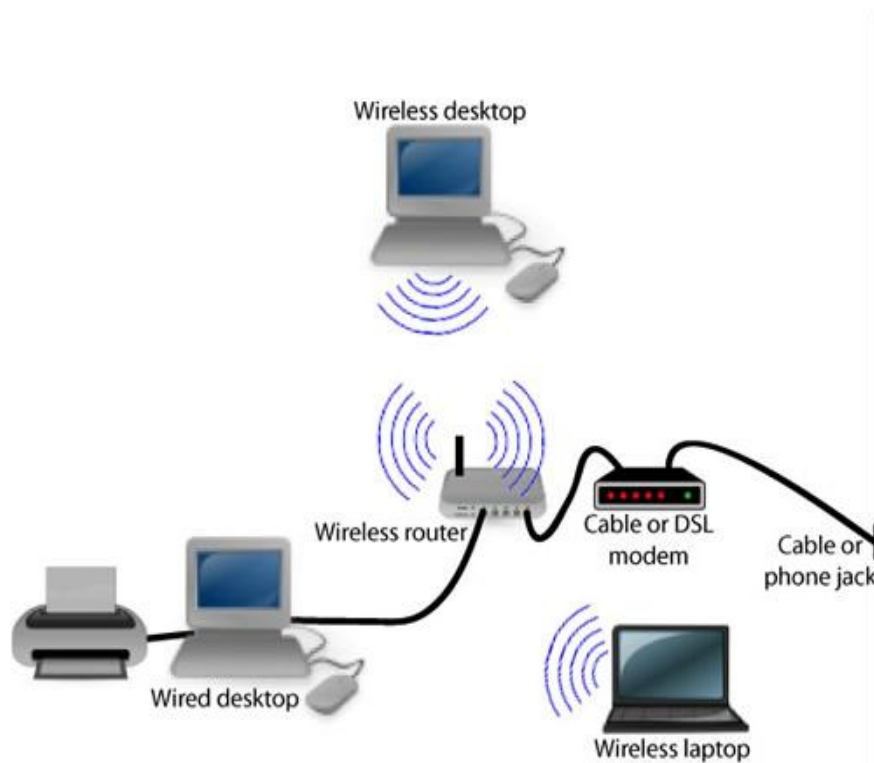
i) Wi-Fi

ii) Bluetooth

(WiFi diagram - 1 Mark, Explanation- 3 Marks, Bluetooth diagram – 2 Marks, Explanation 2 Marks)

Ans: i) **Wi-Fi**

- Wi-Fi stands for wireless fidelity.
- Wi-Fi provide data rate of 54 Mbps.
- Wi-Fi based on IEEE 802.11 standard.



Advantages

- 1) Easy to use.
- 2) Easy and simple to expandability.
- 3) Easy to install and setup.
- 4) No requirement of wires

Disadvantage

- 1) The range of Wi-Fi is limited
- 2) Security is less in Wi-Fi connections as compared with others.
- 3) Wi-Fi connections are highly suspect able interruption by other devices which are operating in close proximity.

ii) Bluetooth

- Bluetooth is short range wireless technology.
- Range of bluetooth is 10 meters.

Bluetooth Architecture define 2 types of networks.

1) piconet 2) scatternet

Piconet

- It consist of 1 master node and 7 slave nodes.
- Piconet have 8 active nodes(7+1) in the range of 10 meters.
- There can be only 1 master station in each piconet.
- Communication is between master and slave
- Slave-slave communication is not possible.
- Piconet can have 255 parked nodes, that can not take part in communication
- There will be 7 slaves in active state and 255 nodes in parked state.

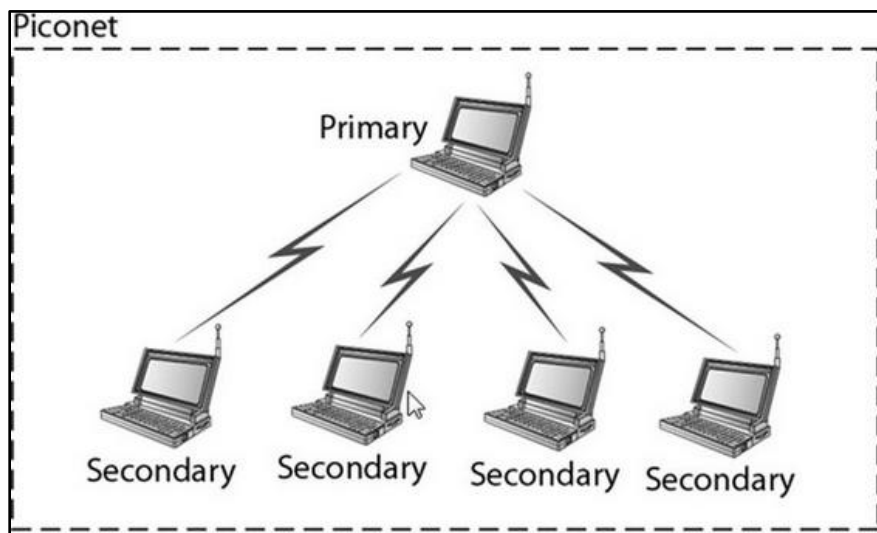


Fig :piconet

Scatter net

- It is formed by combining various piconets.
- Slave in one piconet can act as master in other piconet.
- Such a node can receive message from the master in the first piconet and deliver the message in second piconet.
- Station can be member of two piconets.
- Station can not be master of two piconet.

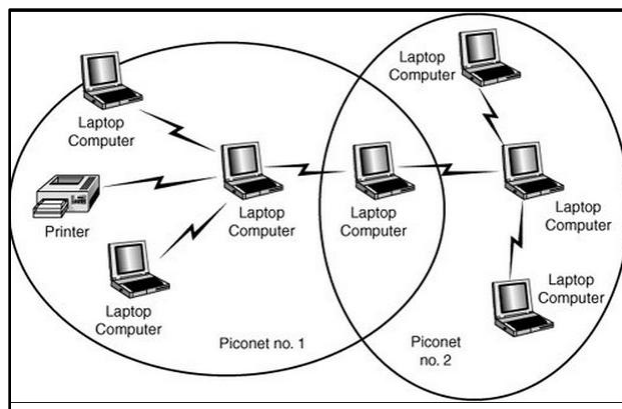


Fig: Scatternet