S.Y. Diploma : Sem. IV
[CO/CM/IF/CW]

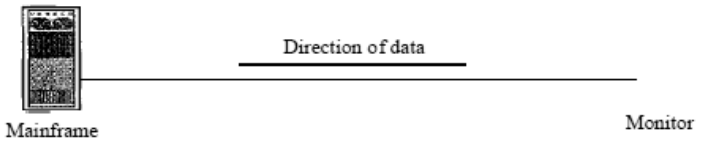
Data Communication & Computer Network

Time: 3 Hrs.] Prelim Question Paper Solution **[Marks : 70**

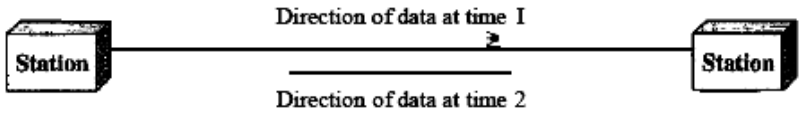
Q.1 Attempt any FIVE of the following : **[10]**

Q.1(a) List modes of Communication. **[2]**

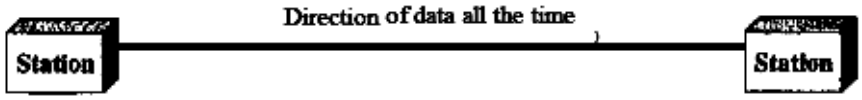
Ans.: Communication between two devices can be simplex, half-duplex, or full-duplex as shown:



(a) Simplex



(b) Half-duplex.



(c) Full duplex.

- **Simplex:** 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. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.
- **Half-Duplex:** 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.
- **Full-Duplex:** In full duplex, both stations can transmit and receive simultaneously. In this sharing can occur in two ways.

Q.1(b) Define Guided & Unguided Transmission Medium. **[2]**

Ans.: **Guided Media :**

Also called as bounded or wired media. Point to point connection i.e. signal travelling is directed. Transport signal in electric current or light/beam. Unidirection, not broadcast. Installation is costly and time consuming. Wired media leads to discrete network topologies. Attenuation depends exponentially on the distance. Example: Twisted pair cable, Coaxial cable, Fiber optic cable.

Unguided media :

Also called as unbounded or wireless media. Used for radio broadcasting in all directions i.e. signal travelling is undirected. Transport signal in the form of electromagnetic waves. It is Broadcast. Installation needs less time and money. Wireless media leads to continuous network topologies. Attenuation is proportional to square of the distance. Example: radio, Infrared light, Microwave.

Q.1(c) List any four Networking Connecting Devices. **[2]**

Ans.: (i) Gateways and Hosts
(ii) Routers
(iii) Bridges
(iv) Repeaters

Q.1(d) Define computer network. **[2]**

Ans.: A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

Q.1(e) Write any two specifications of switch. **[2]**

Ans.: A network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive.

Environmental Specifications

Environment		Specification
Temperature	Ambient operating	32 to 104°F (0 to 40°C)
	Ambient non operating	-40 to 158°F (-40 to 70°C)
Relative humidity	Ambient (non condensing) operating	8 to 80%
	Ambient (non condensing) non operating	5 to 90%

Q.1(f) What is hub? Give types of hub. **[2]**

Ans.: **HUB:** Hub is a connecting device; it is also known as multiport repeater. It is normally used for connecting stations in a physical star topology All networks require a central location to bring media segments together. These central locations are called hubs. A hub organizes the cables and relays signals to the other media segments.

There are three main types of hubs:
1. Passive Hub
2. Active Hub
3. Intelligent Hub

Q.1(g) State any two advantages of coaxial cable. **[2]**

Ans.:
1. Transmits digital signals at a very high speed of 10 Mbps
2. Greater channel capacity.
3. Greater bandwidth
4. Lower error rates.
5. Data Transmission without distortion.
6. Greater spacing between amplifier

Q.2 Attempt any THREE of the following : **[12]**

Q.2(a) Define computer network & state need of computer. **[4]**

Ans.: **Define Compute Network**

A computer network is a set of connected computers. Computers on a network are called nodes. The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. Connected computers can share resources, like access to the Internet, printers, file servers, and others.

Need of computer network

(i) 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.

(ii) 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.

(iii) 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.

(iv) 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.

(v) 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.

Q.2(b) Draw & explain TCP/IP protocol suite. [4]

Ans.: Overview of TCP/IP Architecture

The TCPIP network architecture is a set of protocols that allows communication across multiple diverse networks. The architecture evolved out of research that had the original objective of transferring packets across three different packet networks: the ARPANET packet-switching network, a packet radio network, and a packet satellite network.

Figure 1(a) shows the TCP/IP network architecture, which consist of four layers. The application layer provides services that can be used by other applications. For examples, protocols have been developed for remote login, for e-mail, for file transfer, and for network management. The TCP/IP application layer incorporates the functions of the top three OSI layers.

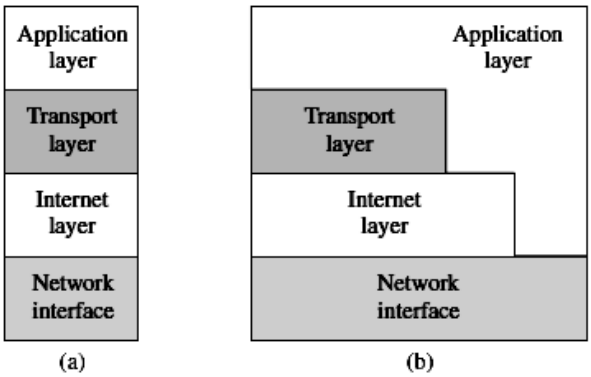


Fig. 1 : TCP/IP network architecture

The application layer programs are intended to run directly over the transport layer. Two basic types of services are offered in the transport layer. The first service consists of reliable connection-oreinted transfer of a byte stream, which is provided by the Transmission Control Protocol (TCP). The second service consists of best-effort connectionless transfer of individual messages, which is provided by the User Datagram Protocol (UDP). This service provides no mechanisms for error recovery or flow control. UDP is used for applications that require quick but necessarily reliable delivery.

The TCP/IP model not require strict layring, as shown in figure 1(b). In other words, the application layer has the option of bypassing intermediate layers. For example, an application layer may run directly over the internet layer.

The internet layer handles the transfer of information across multiple networks through the use off gateways or routers, as shown in figure 2. The internet layer corresponds to the part of the OSI network layer that is concerned with the transfer of packets between machines that are connected to different networks. It must therefore deal with the routing of packets across these networks as well as with the control of congestion. A key aspect of the internet layer is the definition of globally unique addresses for machines that are attached to the Internet.

The internet layer provides a single service, namely, best-effort connectionless packet transfer. IP packets are exchanged between routers without a connection setup; the packets are routed indedpendently, and so they may traverse different paths. For this reason, IP packets are also called datagrams. The connectionless approach makes the system robust; that is, if failures occur in the network, the packets are routed around the points of failure; there is no need to set up the conncetions. The gateways that interconnect the intermediate networks may discard packets when congestion occurs. The responsibility for recovery from these losses is passed on the the transport layer.

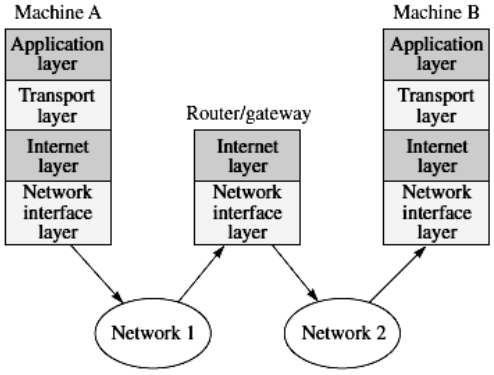


Fig. 2 : The internet layer and network interface layers

Finally, the network interface layer is concerned with the network-specific aspects of the transfer of packets. As such, it must deal with part of the OSI network layer and data link layer. Various interfaces are available for connection end computer systems to specific networks such as X.25, ATM, frame relay, Ethernet and token ring.

Q.2(c) Differentiate between TCP and UDP [Any four points]. [4]

Ans.:

	TCP	**UDP**
Acronym for	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.

Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control
Error Checking	TCP does error checking.	UDP does error checking, but no recovery options.

Q.2(d) With neat diagram, explain satellite communication system. [4]

Ans.: Satellite Communication: In satellite communication, signal transferring between the sender and receiver is done with the help of satellite. In this process, the signal which is basically a beam of modulated microwaves is sent towards the satellite called UPLINK (6Ghz). Then the satellite amplifies the signal and sent it back to the receiver's antenna present on the earth's surface called as DOWNLINK (4Ghz), as shown in the diagram given

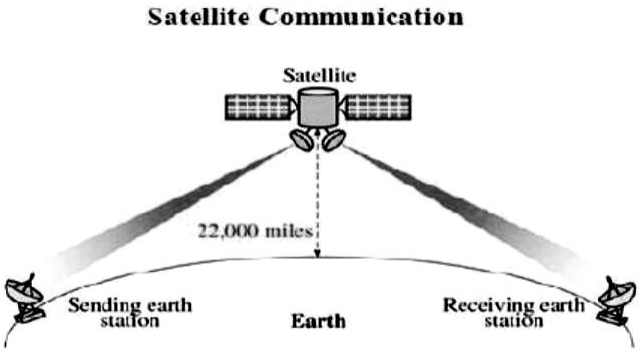


Fig: Satellite Communication

As the entire signal transferring is happening in space. Thus this type of communication is known as space communication. The satellite does the functions of an antenna and the repeater together. If the earth along with its ground stations is revolving and the satellite is stationery, the sending and receiving earth stations and the satellite can be out of sync over time. Therefore Geosynchronous satellites are used which move at same RPM as that of the earth in the same direction. So the relative position of the ground station with respect to the satellite never changes.

Q.3 Attempt any THREE of the following : [12]

Q.3(a) Describe the role of transmission medium in the process of data communication. [4]

Ans.: Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

- **Cost and 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.
- **Type of cable:** Coaxial cable, Twisted Pair Cable, Fiber Optic Cable
- **No of conductors/connectors**
  RJ- 45, BNC, LC and ST
- **Noise:** It leads to distortion of a signal. Noise immunity of transmission media is considered at the time of selecting particular network.
- **Bandwidth:** Higher bandwidth transmission media support higher data rate.
- **Radiation:** It is leakage of signal from media caused by undesirable characteristics of media.
- **Durability:** Life span of media.
- **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)
- **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.

Q.3(b) With suitable diagram describe star topology and ring topology. [4]

Ans.:

- **Star Topology**

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure).

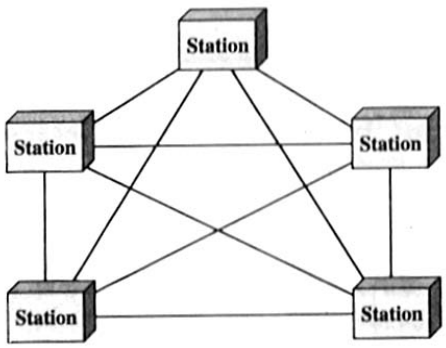


Fig.: A star topology connecting four

Advantages of star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed,

and additions, moves, and deletions involve only one connection: between that device and the hub.

Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

One big **disadvantage** of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

The star topology is used in local-area networks (LANs).

- **Ring Topology :**
  In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Figure).

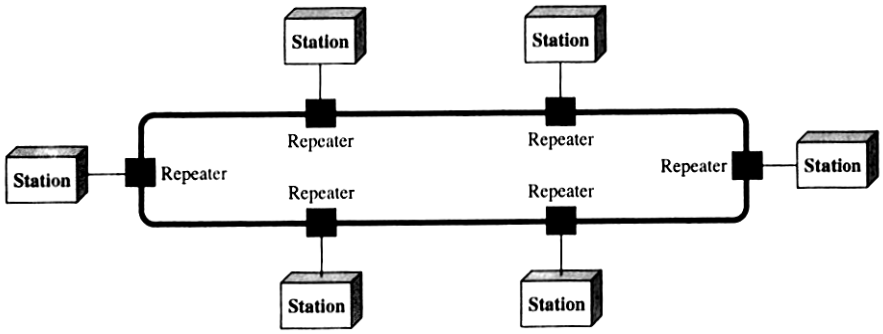


Fig.: A ring topology connecting six stations

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

Q.3(c) Describe major functions of the network layer in TCP/IP protocol suit. [4]

Ans.: ICMP :

- The Internet Control Message Protocol (ICMP) is a network-layer protocol that does not carry user data, although its messages are encapsulated in IP datagrams.
- ICMP files two roles in the TCP/IP suite: it provides error-reporting functions, informing the sending system when a transmission cannot reach its destination, for example, and it carries query and response messages for diagnostic programs.

ARP :

- The Address Resolution Protocol (ARP) occupies an unusual place in the TCP/IP suite because it defies all attempts at categorization.
- Unlike most of the other TCP/IP protocols, ARP messages are not carried within IP datagrams. A separate protocol identifier is defined in the "Assigned Numbers" document that data link-layer protocols use to indicate that they contain ARP messages.
- The function of the ARP protocol is to reconcile the IP addresses used to identify systems at the upper layers with the hardware addresses at the data-link layer.

RARP--Reverse Address Resolution Protocol

What is it for: Diskless clients don't have a place to store there IP number. Rarp translates machines addresses into IP numbers.

How RARP works : The client broadcasts a RARP packet with an ethernet broadcast address, and it's own physical address in the data portion. The server responds by telling the client it's IP address. Note there is no name sent. Also note there is no security. Does not use IP; uses's physical frames.

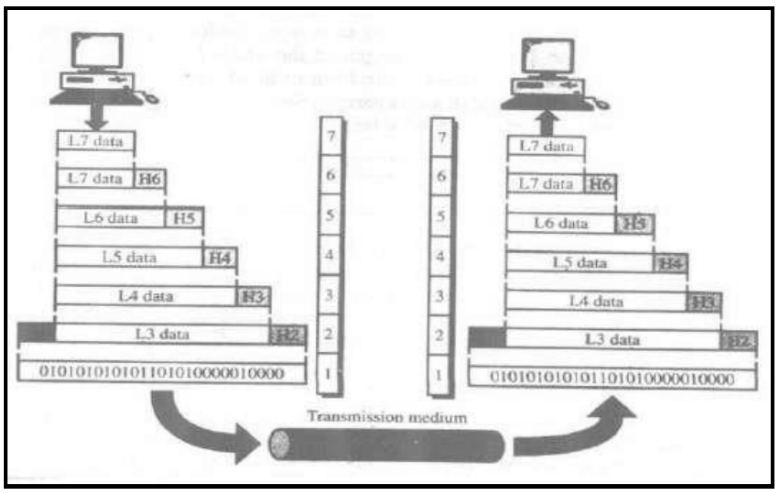
RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

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)
- ARP
- RARP
- IP

Q.3(d) Describe data encapsulation. **[4]**

Ans.:



Explanation:

- The protocols operating at the various layers work together to supply a unified quality of service.
- Each protocol layer provides a service to the layers directly above and below it.
- The process of adding the headers and trailers to the data is called as data encapsulation.

- A packet(header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on. In other words, the data portion of a packet at level N-1 carries the whole packet (data and header and maybe trailer) from level N.

Q.4Attempt any THREE of the following : [12]

Q.4(a) List all layers of OSI model & state its function. [4]

Ans.: The OSI model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

Layered Architecture

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6) and application (layer 7).

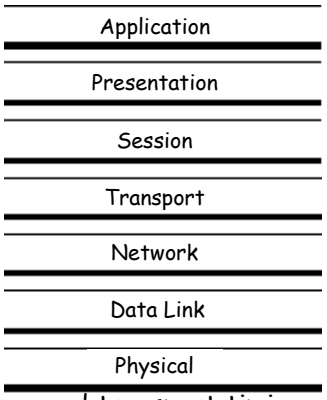
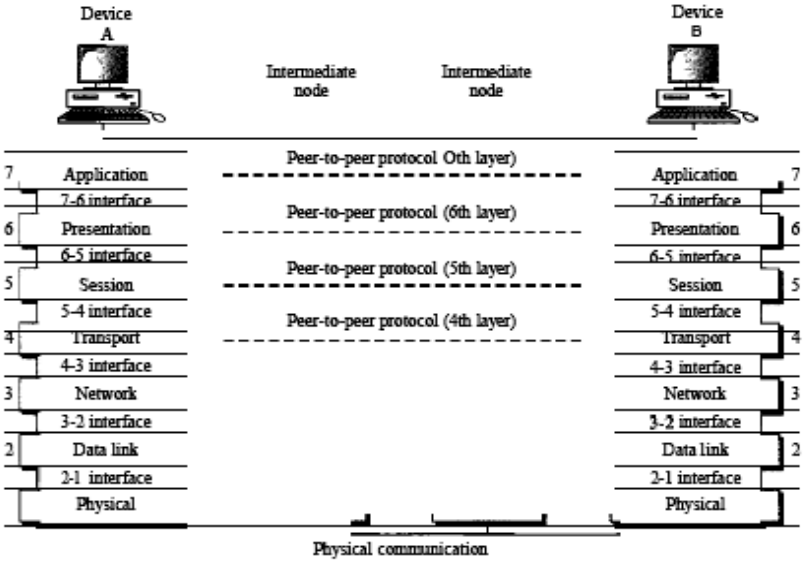


Figure shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

The seven layers can be thought of as belonging to three subgroups. Layers 1, 2, and 3 physical, data link, and network-are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability). Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.

The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.



Q.4(b) Give the names of network layer. Where following protocols are relate/ belong to: [4]
(i) SMTP (ii) TCP-UDP (iii) IP (iv) PPP

Ans.: Names of Network Layer:
(i) Application Layer
(ii) Transport Layer
(iii) Network Layer
(iv) Data-Link Layer

Q.4(c) Describe any 4 classes of IPv4 addresses with its range. [4]

Ans.: Class A - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh

- First bit 0; 7 network bits; 24 host bits
- Initial byte: 0 - 127
- 126 Class As exist (0 and 127 are reserved)
- 16,777,214 hosts on each Class A

In a Class A Network binary address start with 0, therefore the decimal number can be anywhere from 1 to 126. The first 8 bits (the first octet) identify the network and the remaining 24 bits indicate the host within the network. An example of a Class A IP address is 102.168.212.226, where "102" identifies the network and "168.212.226" identifies the host on that network.

Class B - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh

- First two bits 10; 14 network bits; 16 host bits
- Initial byte: 128 - 191
- 16,384 Class Bs exist
- 65,532 hosts on each Class B

In a Class B Network, binary addresses start with 10, therefore the decimal number can be anywhere from 128 to 191. The number 127 is reserved for loopback and is used for internal testing on the local machine. The first 16 bits (the first two octets) identify the network and the remaining 16 bits indicate the host within the network. An example of a Class B IP address is 168.212.226.204 where "168.212" identifies the network and "226.204" identifies the host on that network.

Class C - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh

- First three bits 110; 21 network bits; 8 host bits
- Initial byte: 192 - 223
- 2,097,152 Class Cs exist
- 254 hosts on each Class C

Binary addresses start with 110, therefore the decimal number can be anywhere from 192 to 223. The first 24 bits (the first three octets) identify the network and the remaining 8 bits indicate the host within the network. An example of a Class C IP address is 200.168.212.226 where "200.168.212" identifies the network and "226" identifies the host on that network.

Class D - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm

- First four bits 1110; 28 multicast address bits
- Initial byte: 224 - 247

In a Class D Network, binary addresses start with 1110, therefore the decimal number can be anywhere from 224 to 239. Class D networks are used to support multicasting.

Class E - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

- First four bits 1111; 28 reserved address bits
- Initial byte: 248 - 255
- Reserved for experimental use

In a Class E Network, binary addresses start with 1111, therefore the decimal number can be anywhere from 240 to 255. Class E networks are used for experimentation. They have never been documented or utilized in a standard way.

Q.4(d) Compare Client-Server and peer to peer network. [4]

Ans.:

Sr. No.	Client server Network	Peer to peer Network
1	Strong central security	Weak central security.
2	Better performance for large number of user.	Poor performance for large number of user.
3	Centralized backup can be taken.	Each user needs to take his as her own backup.
4	Easy manageability for large number of user.	Difficult to manage more than few (10) user.
5	Very reliable dedicated Network operating system (NOS) required.	No Network OS required, existing machines with stand-alone OS.
6	Expensive dedicated H/W.	No extra dedicated H/W.
7	Requires professional N/W Administrator.	Not required, user can manage.
8	Here server is more powerful than client.	All user are equal in peer to peer.
9	Client always request & server serves the request.	Anybody can be server and anybody can be client.

Q.4(e) Explain OSI reference model with its layered architecture. [4]

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
Physical Layer

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

Physical (Layer 1)

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

Data Link (Layer 2)

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

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

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

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

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

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

Q.5 Attempt any TWO of the following : [12]

Q.5(a) Explain RARP and ICMP. [6]

Ans.: RARP (Reverse Address Resolution Protocol):

- This is used to obtain the IP address of a host based on its physical address.
- This performs the job exactly opposite to that of ARP (Address Resolution Protocol)
- In RARP, a host in LAN can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache.
- A network administrator creates a table in a local area networks gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses.
- When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address.
- Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

The Internet Control Message Protocol (ICMP):

- ICMP is a error reporting protocol.
- This protocol is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
- ICMP can also be used to relay query messages.
- ICMP enables the detection and reporting of problems in the Internet.

Q.5(b) Explain structure of IP frame header. [6]

Ans.: IPv4 header:

The IP datagram contains header and data.
The header consists of around 20 to 60 bytes consists of information about routing and delivery.
The header is like an envelope i.e., it contains information about the data.

The structure of the standard format is as shown below.

<table>
<tr><td>Version
(4 Bits)</td><td>HLEN
(4 bits)</td><td>Service Type
(ToS) (8 Bits)</td><td colspan="2">Total Length (16 bits)</td></tr>
<tr><td colspan="3">Identification (16 bits)</td><td>Flags
(3bits)</td><td>Fragmentation
offset (13 bits)</td></tr>
<tr><td colspan="2">Time to Live
(TTL) (8 bits)</td><td>Protocol
(8 bits)</td><td colspan="2">Header Checksum (16 bits)</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
</table>

The various fields are as described below:

Version: This field identifies the version of IP, which contains a value 4, which indicates IP version 4. It may contain 6 for IPv6

Header length (HLEN): This indicates the size of the header in a multiple of 4 byte words. When the header size is 20 bytes, HLEN = 5, and HLEN = 15 when maximum size (60 bytes).

Service Type (Type of Service): This field is used to define service parameters such as the priority of the datagram and the level of reliability desired.

Total Length: This field contains the total length of the IP datagram. IP datagram cannot be more than 65,536 since this filed size is 2 bytes or 16 (2_{16} = 65,536).

Identification: This field is used in the situations when a datagram is fragmented. The sub datagram are sequenced using identification field so that later it can be used to reconstruct the original datagram.

Flags: This field corresponds to identification field. It indicates whether a datagram can be fragmented and if fragmented, the position of the fragment (first, last or middle).

Fragmentation Offset: If a datagram is fragmented, this field indicates the offset of the data in the original datagram before segmentation. This is used while reconstructing.

Time to Live (TTL): This filed is initialized by some value and decremented each time it passes through routers. If the value becomes zero or negative, the data is not forwarded. Thus it decides the lifetime of the data.

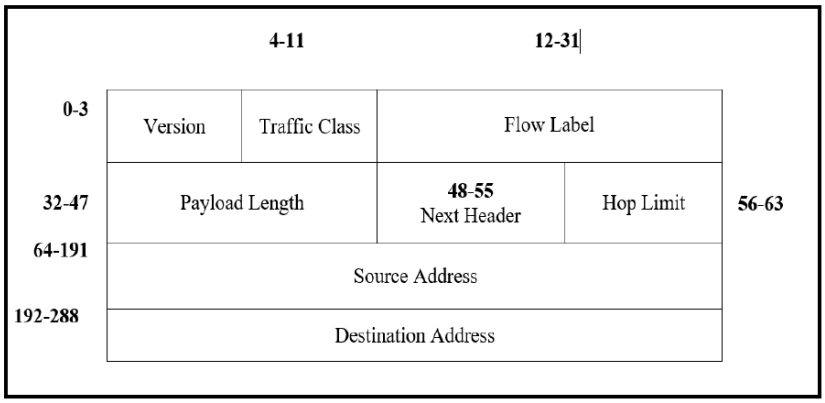
Protocol: This field identifies the transport protocol running on top of IP. The upper layer software piece can be TCP or UDP. This field specifies which piece of software at the destination node the datagram should be passed on to.

Source address: This field contains the 32 bit IP address of the sender.

Destination address: This field contains the 32 bit IP address of the final destination.

OR

IPv6 header:



IPv6 fixed header is 40 bytes long and contains the following information.

- **Version (4 bit):** It represents the version of Internet Protocol, i.e. 0110
- **Traffic Class (8-bits):** These 8 bit are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
- **Flow label (20-bits):** This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re- ordering of data packets. It is designed for streaming/real –time media.
- **Payload Length (16-bits):** This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated, but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
- **Next Header (8-bits):** This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer.
- **Hop Limit (8-bits):** This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPV4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packets is discarded.
- **Source Address (128-bits):** This field indicates the address of originator of the packet.
- **Destination Address (128–bits):** This field provides the address of intended recipient of the packet.

Q.5(c) Compare IPv4 and IPv6. **[6]**

Ans.:

Sr. No.	IPV4	IPV6
1	Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
2	Uses broadcast addresses to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, multicast scoped addresses are used.
3	Fragmentation is supported at originating hosts and intermediate routers.	Fragmentation is not supported at routers. It is only supported at the originating host.
4	IP header includes a checksum.	IP header does not include a checksum
5	IP header includes options.	All optional data is moved to IPv6 extension headers.
6	IPsec support is optional	IPsec support is required in a full IPv6 implementation.
7	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.
8	Address must be configured either manually or through DHCP.	Addresses can be automatically assigned using stateless address auto configuration, assigned using DHCPv6, or manually configured.

Q.6 Attempt any TWO of the following : **[12]**

Q.6(a) Describe Bluetooth architecture technologies. **[6]**

Ans.: BLUETOOTH

The basic unit of a Bluetooth system, is a piconet, which consists of a master node and up to seven active slave nodes within a distance of 10 meters. Multiple piconets can exist in the same (large) room and can even be connected via a bridge node, as shown in figure below. An interconnected collection of piconets is called a scatternet.

In addition to the seven active slave nodes in a piconet, there can be up to 255 parked nodes in the net. These are devices that the master has switched to a low power state to reduce the drain on their batteries. In parked state, a device cannot do anything except respond to an activation or beacon signal from the master.

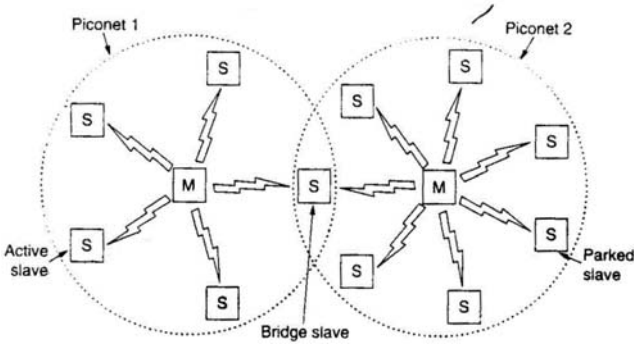
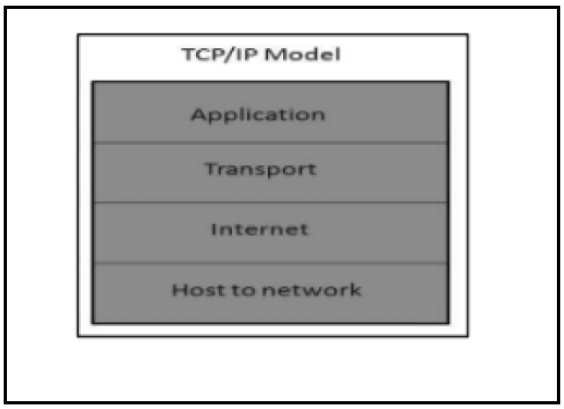


Fig.: Two piconets can be connected to form a scatternet.

The reason for the master / slave design is that the designers intended to facilitate the implementation of complete Bluetooth chips for under $5. At its heart, a piconet is a centralized TDM system, with the master controlling the clock and determining which device gets to communicate in which time slot.

Q.6(b) Describe TCP/IP model with suitable diagram. **[6]**

Ans.:



TCP/IP Reference Model: TCP/IP means transmission control protocol and internet protocol.

Overview of TCP/IP reference model

TCP/IP that is transmission control protocol and the internet protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) under the project of network interconnection.

Most widely used protocol for interconnecting computers and it is the protocol of the internet. It has 4 layers as given below.

Layer 1: Host-to-network Layer

1. Protocol is used to connect the host, so that the packets can be sent over it.
2. Varies 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 internet layer.
2. It the layer which holds the whole architecture together.
3. It allows the host to insert the packets.
4. It helps the packet to travel independently to the destination.
5. Order in which packets are received is different from the way they are sent.
6. IP (internet protocol) is used in this layer.

Layer 3: Transport Layer

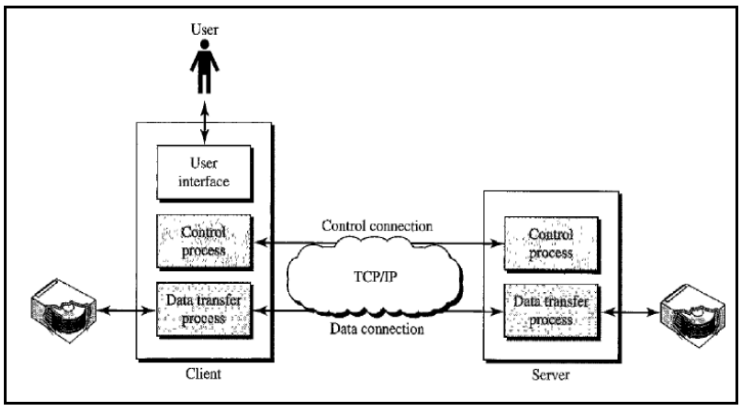
1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer.
3. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
4. Functions of the transport layer are same as the OSI model.
5. Transport layer also arrange the packets sent in sequence.

Layer 4: Application Layer

1. Protocols used in this layer are high level protocols such as TELNET, FTP (file transfer protocol etc.

Q.6(c) Explain the principle of FTP. **[6]**

Ans.: FTP Diagram:



Explanation:

File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Figure shows the basic model of FTP.

- The client has three components: user interface, client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process.
- The control connection is made between the control processes. The data connection is made between the data transfer processes.
- The control connection remains connected during the entire interactive FTP session.
- The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.
- Separation of commands and data transfer makes FTP more efficient. FTP uses the services of TCP. It needs two TCP connections.
- FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

❑ ❑ ❑ ❑ ❑