Royal Education Society's

## College of Computer Science and Information Technology, Latur.

# Department of Computer Science

**Academic Year** (2022-23) **Class/Semester:** B.Sc.(CS) SY SEM-III

**Name of Paper:** Computer Network (**BCS-302**) **Prepared by:** Mr. S. S. Shaikh

## Question Paper (75 Marks)

**Q.1 Attempt any FIVE of the following (3 Marks each)** **15**

a) Define Application of computer network.
b) Short Note on Signal.
c) Short Note on PBX.
d) Short Note on RING Topology.
e) Internet Service Provider
f) Define 10Base2 and 10BaseT
g) Short Note on ISDN

**Q. 2 Attempt any Three of the following (5 Marks each)** **15**

a) Explain LAN, MAN and WAN in detail.
b) Explain BUS, STAR & MESH with diagram.
c) Describe Data Transmission Media with diagram.
d) Explain design issues for layers.
e) Explain service primitives.

**Q. 3 Answer any Three of the following (5 Marks each)** **15**

a) Explain ISO/OSI in detail.
b) Define TCP/IP Model.
c) Explain Connection Oriented and connection less service.
d) What is protocol hierarchies? explain in detail.
e) Explain concept of addressing in detail.

**Q. 4 Attempt any Three of the following (5 Marks each)** **15**

a) What is error control? explain in detail.
b) Explain HUB, Switch and Router?
c) What is Flow control? explain in detail with diagram.
d) Explain Multiplexing with types in detail.
e) Difference between parallel & serial data transmission.

**Q .5 Attempt any Three of the following (5 Marks each)** **15**

a) Explain Ethernet, fast Ethernet and gigabit Ethernet in detail.
b) Explain FDDI in detail with example.
c) Explain Sliding window protocol in detail.
d) Explain Network Protocols- IP, PPP & FTP.
e) Explain Internet verses Intranet.

# Model Answer Paper

## Q.1. Attempt any Five of the following (3 Marks each) 15

## a) Define Application of computer network.

**Ans:**

***Definition & Applications of Computer Network:***

**Definition**: *"Computer network is a group of two or more computers or other electronic devices that are interconnected either by a cable or a wireless connection for the purpose of exchanging data and sharing resources (like software or printer)."*

**Applications of Computer Network:**

**1. Resource Sharing:** Resource sharing is an application of a computer network. Resource sharing means you can share Hardware (printers, scanner etc.) and Software applications among multiple users in a network.

**2. Information Sharing:** Using a Computer network, we can share Information over the network, and it provides Search capabilities such as WWW. Over the network, single information can be shared among the many users over the internet.

**3. Communication:** Communication includes email, calls, message broadcast, electronic funds transfer system etc.

**4. Online Education:** In lockdown period of pandemic we use zoom, Google meet etc. applications to continue our study this is make possible only with computer and mobile networks.

**5. Entertainment Industry:** In Entertainment industry also uses computer networks widely. Some of the Entertainment industries are movie theatre, Video on demand, Multi-player games, cable or dish tv, etc.

**6. Access to Remote Databases:** Computer networks allow us to access the Remote Database of the various applications by the end-users. Some applications are Reservation for Hotels, Airplane Booking, Home Banking, Automated Newspaper, Automated Library etc.

**7. Home applications:** For example, managing bank accounts, transferring money to some other banks, paying bills electronically. A computer network arranges a robust connection mechanism between users.

**8. Business work:** The cloud computing manages all resource sharing. And the purpose of resource sharing is that without moving to the physical location of the resource, all the data, plans, and tools can be shared to any network user. Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network. Even most of the IT companies are allocating and submitting their work online to employees with work from home concept.

**9. Mobile users:** The rapidly growing sectors in computer applications are mobile devices like notebook computers and PDAs (personal digital assistants). Here mobile users/device means portable device. The computer network is widely used in new-age technology like smart watches, wearable devices, tablets to make online transactions, purchasing or selling products online, etc.

**10. Social media:** Social media is also a great example of a computer network application. It helps people to share and receive any information related to political, ethical, and social issues.

## b) Short note on Signal.

**Ans:**

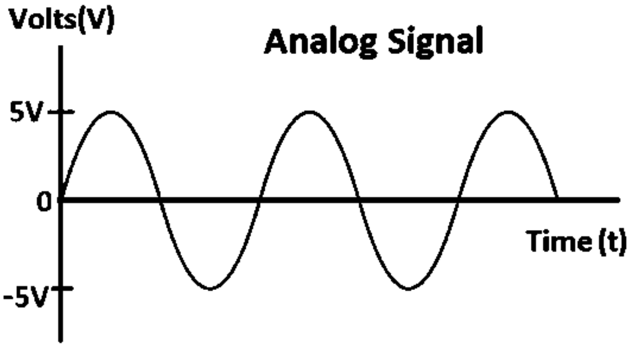
**Basic Concepts Signals, Types — *Analog and Digital Signals:***

***Signals:*** *"A signal is an electrical or electromagnetic current that is used for carrying data from one device or network to another"*

In electronics, a signal is an electrical pulse that is used as a method of transmitting data. Typically, a signal is created when a command or data is sent to a device.

- **Types of Signals:**

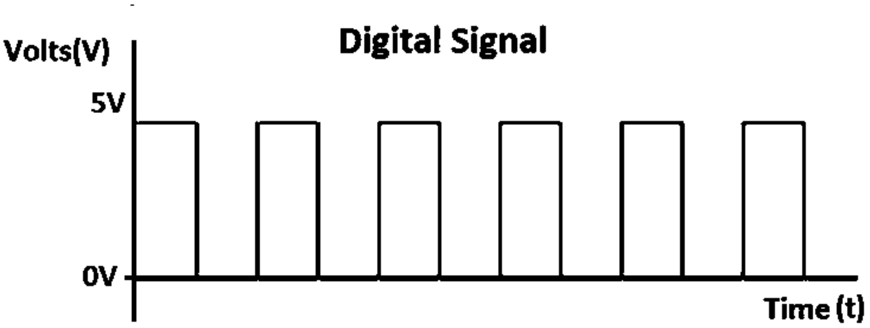
1. **Analog Signals-**



- ✓ Analog signals are continuous signals which represented by sine waves.
- ✓ Analog signals are more accurate than digital signals.
- ✓ It records the information as it is.
- ✓ Analog signals are older than Digital signals.
- ✓ These kind of signals works with physical values and natural phenomena such as recording of human voice, natural sound, set frequency, monitoring earthquake, volcano, speed of wind, weight, thunder lighting, etc.
- ✓ These signals are used in analog devices.

- ✓ Analog signals produce too much noise.
  Examples of Analog signals are old black & white tv antenna signals, Radio broadcasting stations, land line phone etc.

**1. Digital Signals-**



- ✓ Digital signals are not continuous, they are individually separate and distinct signals.
- ✓ We can represent digital signals in the form of square waves.
- ✓ Converts the information into binary form.
- ✓ Now a days Digital signals are much more in use than Analog signals.
- ✓ Digital signals can be easily stored.
- ✓ Digital signals do not produce noise.
- ✓ Examples of digital signals are computers, smartphones, smartwatch, tablet PC, Digital electronic devices etc. use these signals.

## c) Short note on PBX.

## Ans:

**PBX:**

A PBX is an acronym for Private Branch Exchange, which is a private telephone network that allows users can talk to each other. Different hardware components work in tandem to provide connectivity to the telephone network.

A PBX operates a company’s internal telephone network. A PBX system manages the routing and advanced calling features for inbound and outbound calls.

Setting up a PBX is no small task. A company enlists the help of one or more systems administrators with decades of telecom experience. You would also need the physical space to place the PBX system in the office, like a closet or server room.

**PBX System Benefits for Businesses:**

1. **Manage and complete calls** on a specific, pre-programmed schedule. You can choose the direction of the “branching out” and set your own rules in the PBX network tree. Operators can restrict or permit international dialing as needed to avoid high costs.

2. **Transfer calls between users** and departments with ease. Establish and maintain connections without dropping calls. You can transfer calls effectively through a warm transfer or cold transfer. Either way, you can transfer calls reliably.

3. **Customize greetings** with recorded messages, including the choice of music for your business. This feature is a fantastic way to alert customers about a sale or service issues.

4. **Operate a call center** to help you manage a sales team or customer support department. While costly, a PBX can hold **inbound and outbound calls** in a queue based on its physical limitations. A cloud-based PBX can handle a higher volume of calls and distribute them to the desired people or teams.

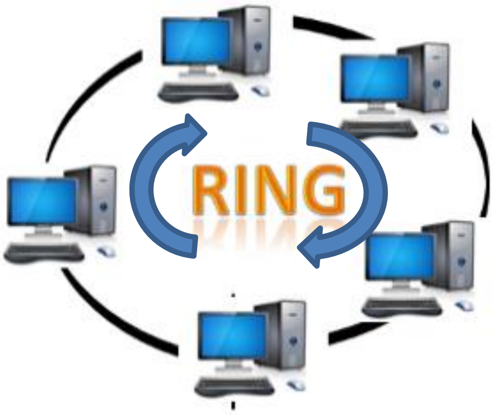
5. **Connect multiple office locations** with the same phone system so employees can talk to each other. Instead of managing separate phone systems, you would use a PBX to handle this call routing.

## d) Short note on RING Topology.

## Ans:

1. **RING Topology:**

- **Ring:** Ring topology is like a bus topology, but with circle shape. The node that receives the message from the previous computer will retransmit to the next node. It has no termination (end) point like bus topology.



- **Types:** The data flows in one direction on one cable, i.e., it is single Ring architecture. The data flows in both direction in two cable, it is dual Ring architecture.
- **Token:** The data in a ring topology flow in a clockwise direction. The most common access method of the ring topology is token passing. Token is a signal which rotates across the ring, 'Who has token only those computer can send or receive data.'

## e) Short note on ISP.

## Ans:

### Internet Service Providers:

ISP stands for Internet Service Provider. It is a company that provides connection of access to the internet. For example, when you connect to the Internet, the connection between your Internet-enabled device and the internet is executed through a specific transmission technology that involves the transfer of information packets through an Internet Protocol route.

**Types of Services offered by ISP:**

**Dial-up Internet access:** It is the oldest technology to provide Internet access by modem to modem connection using telephone lines. In this method, the user's computer is connected to a modem with a telephone line. This method has become outdated today due to slow connection speed.

**DSL:** DSL stands for **'digital subscriber line'** is an advanced version of the dial-up Internet access method. It uses high frequency to execute a connection over the telephone network and allows the internet and the phone connection to run on the same telephone line.

**Wireless Broadband (WiBB):** It is a modern wireless broadband technology for Internet access. It allows high-speed wireless internet within a large area. To use this technology, you are required to place a dish on the top of your house and point it to the transmitter of your Wireless Internet Service Provider (WISP).

**Wi-Fi Internet:** It is the short form for "wireless fidelity," which is a wireless networking technology that provides wireless high-speed Internet connections using radio waves. It is commonly used in public places such as hotels, airports, restaurants to provide internet access to customers.

**Ethernet:** It is a wired LAN (Local Area Network) where computers are connected within a primary physical space.

## f) Short note on 10Base2 and 10BaseT.

## Ans:

## Types of Ethernet:

**10Base2:**

- 10Base2 is a type of standard for implementing Ethernet networks.
- 10Base2 networks are wired together in a **bus topology**, in which individual stations (computers) are connected directly to one long cable.
- 10Base2 is sometimes referred to as **ThinNet** (or "thin coax") because it uses thin coaxial cabling for connecting stations to form a network.
- 10Base2 supports a maximum bandwidth of **10 Mbps**.
- The maximum length of any particular segment of a 10Base2 network is **185 meters**.
- A 10Base2 support maximum **30 stations**.
- Stations are attached to the cable using **BNC connectors**.
- The two ends of a 10Base2 bus must be properly **terminated**. If they are not, signals will bounce and network communications will be impossible.

**10Base5:**

- 10Base2 networks are wired together in a **bus topology**.
- 10Base5 is developed by the Institute of Electrical and Electronic Engineers (**IEEE**).
- 10Base5 is sometimes referred to as **ThickNet** because it uses thick coaxial cabling for connecting stations to form a network. Another name for 10Base5 is Standard Ethernet because it was the first type of Ethernet to be implemented.
- 10Base5 supports a maximum bandwidth of **10 Mbps**.
- The maximum distance of cable length is **50 meters**.
- A 10Base5 segment should have no more than **100 stations**.
- The two ends of a 10Base5 bus must be properly **terminated**.

## f) Short note on ISDN.

## Ans:

## ISDN Architecture:

These are a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. The main feature of ISDN is that it can integrate speech and data on the same lines, which were not available in the classic telephone system. ISDN or Integrated Services Digital Network is a circuit-switched telephone network system that transmits both data and voice over a digital line.

**What are Types of ISDNs?**

There are two types of ISDN networks —

1) **BRI (Basic Rate Interface):**

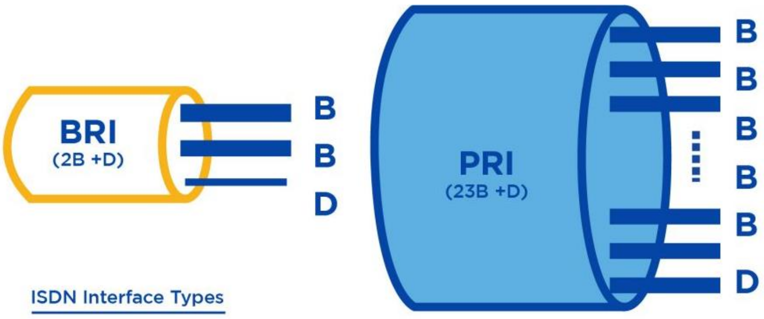
BRI is the lower tier of service. It only provides basic needs at a lower cost.

2) **PRI (Primary Rate Interface):**

PRI is the main service. It provides a better connection, more reliable service, and faster speeds.

The major difference between BRI and PRI is the level of service and reliability.
Both PRI and BRI ISDN use B channels for sending data and D channels for other forms of communication. The difference lies in the number of channels they use to accomplish this.

For instance,
**BRI** uses only two B channels and one D channel. It has a maximum speed of 128 kbps.
**PRI** varies in the number of channels it uses given its location. It can be adjusted for speeds up to 2.94 Mbps.



**What are the advantages of ISDN?**

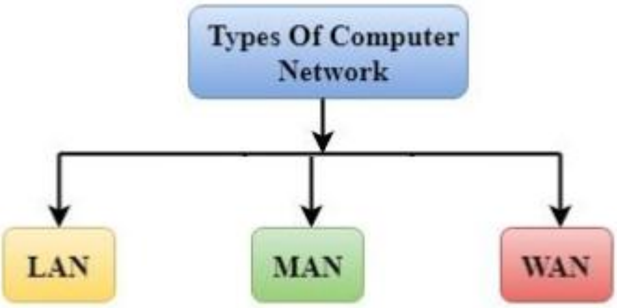
1) Provide digital data signal in to Analog telephone network. It first started as an alternative to your dial-up connection that provided higher internet speeds.
2) ISDN provides a higher data transfer rate with digital signals through telephone lines.
3) Can connect devices and allow them to operate over a single cable. This includes credit card readers, fax machines, and other manifold devices.
4) To access the internet with ISDN, users had to connect through a digital modem.
5) Broadband ISDN, also known as B-ISDN, transmitted data over fiber optic cable. Another attempt was ISDN BRI which attempted to improve voice services.

## Q.2. Attempt any THREE of the following (5 Marks each) 15

## a) Explain LAN, MAN, WAN in detail.

**Ans:**

**Network Types LAN, MAN, WAN :**



### 1) LAN (Local Area Network):

- Local Area Network is a group of computers connected to each other in a small area using small amount of computers such as in room, building, and office.
- LAN is structured and arranged by network topologies such as BUS, RING, STAR, etc
- LAN is used for connecting two or more personal computers through a wired communication medium such as coaxial, twisted pair, Fiber Optic cables.
- LAN can be connecting with the help of wireless media such as Bluetooth, Micro waves, Radio waves, Wi-Fi, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, switch, and cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.
- **Example:** Office, School & College computer laboratories, Cyber café network, Small business network.

### 2) MAN (Metropolitan Area Network):

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- A network which can applied on city level to provide some services all those networks can be considered as MAN.
- It has a larger geographical area than Local Area Network (LAN).
- **Example:** Cable TV Network, Landline Telephone exchange line, Mobile cellular company network, Internet Service Provider, CCTV Camera network by police Department, etc.

### 3) WAN (Wide Area Network):

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is much bigger network than the LAN and MAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- **Example:** The internet that is WWW service is applied on one of the biggest type of network in the world that is WAN.
- A Wide Area Network is widely used in the field of Business, government, and education.

## b) Explain BUS, STAR & MESH Topology with diagram.

## Ans:

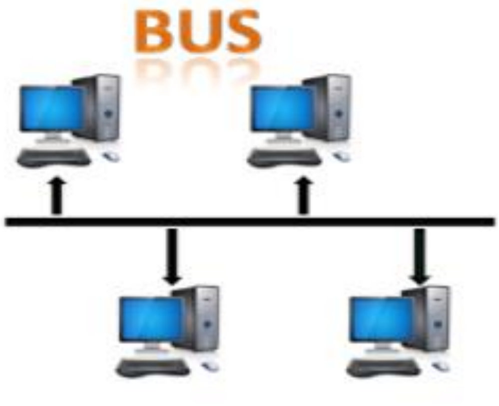
**Network topologies- BUS, STAR, MESH:**

**Network Topology:** *"Network topology is the physical and logical arrangement of nodes and connections in a network" and also called as structure or map of network.*

***Note:*** A node is any physical device within a network that can send, receive, or forward information. **Example-** switches, routers, printers, computers, servers, etc.

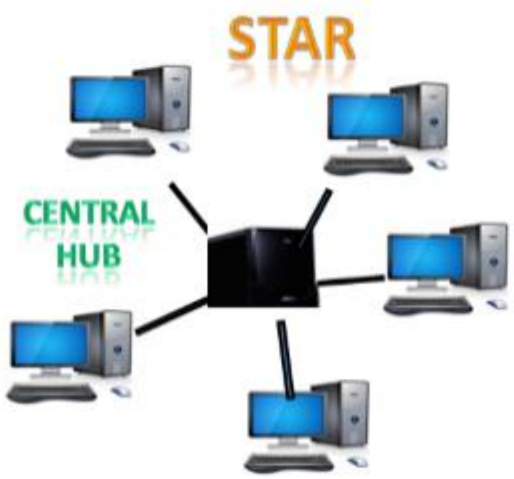
### 1. BUS Topology:

- **First:** This topology is the first topology among all, the bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- **Simple:** The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations. Start and end point of cable terminator devices are used.
- **Problem:** The main problem faced in implementing this topology is the fact that only one communication channel (cable) exists to serve the entire network. As a result, if this channel fails, then the whole network will go out of operation.



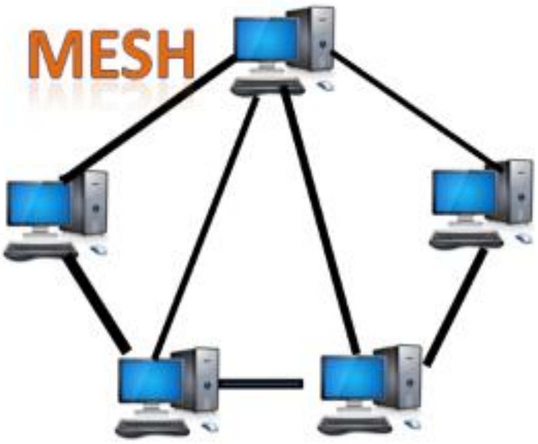
### 2. STAR Topology:

- Star topology is an arrangement of the network in which every node is connected to the central hub or switch networking device.
- **Simple:** It is simple and easy to maintenance
- **Cables:** Coaxial cable or UTP cables are used to connect the computers.
- Star topology is the most popular topology in network implementation.
- **Problem:** The main disadvantage of this is if central device failed suddenly complete network collapse.



### 3. Mesh Topology

- **Mesh**: It is an arrangement of the network in which computers are interconnected with each other through various redundant connections. There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- **Wireless:** Mesh topology is mainly used for wireless networks like satellite network.



## c) Describe Data Transmission Media with diagram.

## Ans:

**Communication Media:**

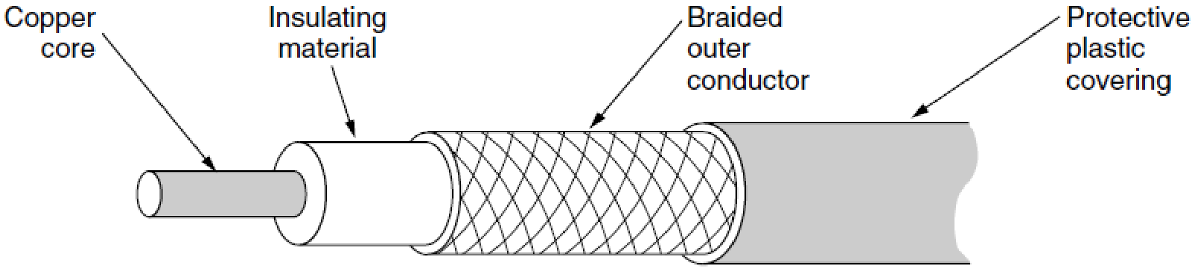
There are a many communication media that are used to interconnect computers and form a computer network.

**Types of communication media:**

1. Coaxial cable
2. Twisted pair cable
3. Fiber-Optic cable
4. Satellite communication

### 1) Coaxial cable:

This cable widely used in digital cable TV network. The outer black hard plastic known as outer jacket, The jacket covers braided outer conductor shield (twisted mesh of wires), Insulating material made up with dielectric material (which is white in colour covered with foil paper), then appears thick copper core wire which carries actual data.

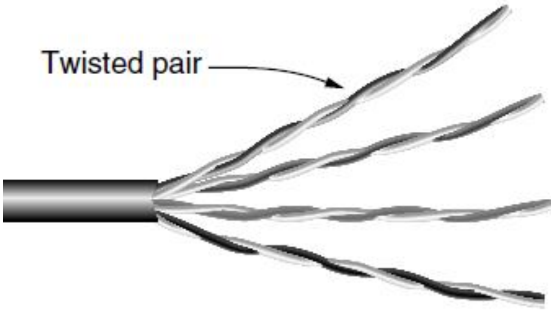


- Coaxial cabling is extremely high resistant to EMI.
- It is complex to install because of its hard to bend capacity.

- It can handle much longer distance in lengths between network devices than the twisted pair cable.
- **Types:** 1) thin coaxial 2) thick coaxial.

### 2) Twisted Pair Cable:

Twisted pair cable is used for Telephone as well as computer LAN networks. Twisted pair cabling is a form of wiring in which pairs of wires are twisted together for the purposes of cancelling out electromagnetic interference (EMI) from other wire pairs and from external sources.



**Types of twisted pair cable:**

**1) Shielded twisted pair (STP):**

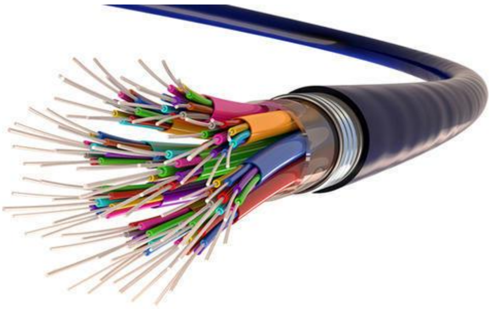
- Extra shied is used to provide more protection from EMI.
- It is costly than UTP cable.

**2) Unshielded twisted pair (UTP):**

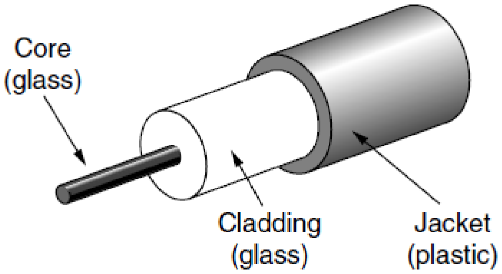
- No extra shied used, only having 4 twisted pair wires with four colors.
- The most popular widely used type is UTP.
- UTP cable include eight copper wires covered by an insulating material.
- The cable size is small, and easy to bend and install.
- The price is less than other type of network cable.
- UTP cable is install using the Registered Jack (RJ 45) connector.
- **Speed:** CAT5 support up to 100Mbps. Where CAT7 supports 10Gbps.

### 3) Fiber optic cable:

Fiber optic cable does not use electric current but use laser light to carry data. This is world’s fastest data transmission cable. It consists of a center glass core surrounded by several layers of protective material. Optical fiber deployment is more expensive than copper but offers higher speed and can cover longer distances.



**Picture**



**Diagram**

This cable consists of core, cladding and jacket. The core is made from the thin strands of glass or plastic that can carry data over the long distance. The core is wrapped in the cladding; and the cladding is wrapped in the jacket.

- Core carries the data signals in the form of the light.
- Cladding reflects light back to the core.
- The jacket protects the cable from physical damage.

Fiber optic cable has no current so that no EMI impact happened. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 km at the speed of 100Gbps.

**Types:** 1) SMF (Single mode Fiber) 2) MMF (Multi mode Fiber).

4) **Satellite Communication:**

- Satellite Communication are high speed wireless network.
- Satellites use a wide range of radio and microwave frequencies
- It covers very large geographical area.
- A communications satellite is an artificial satellite that relays and amplifies signals via a **transponder (Large Dish antenna)** from the earth.
- In telecommunication network satellite perform vital role. TV channel Transponder send signals towards satellite and satellite receives those signals and forward to another satellite or back to **VSAT** (very small aperture terminal) also known as dish TV antenna at consumer home.
- The high frequency radio waves used for telecommunications in mobile network.

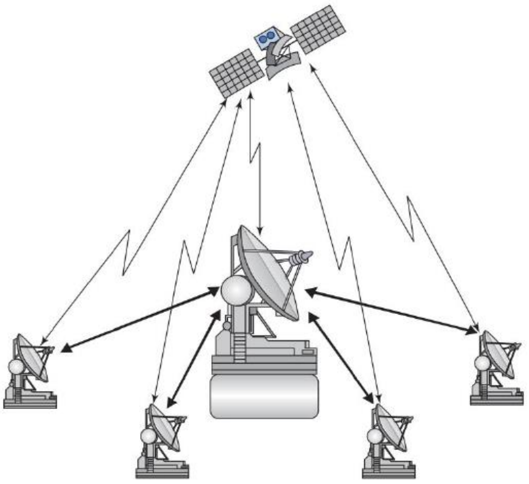


Fig. *A model of satellite communication*

## d) Explain Design Issues for layers.

## Ans:

### ***Design issues for layers:***

A number of design issues exist for the layer to layer approach of computer networks.

Some of the main design issues are as follows −

1) **Reliability:**

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not inaccurate.

2) **Scalability:**

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

3) **Addressing:**

At a particular time, countless messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

4) **Error Control:**

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

5) **Flow Control:**

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

6) **Resource Allocation:**

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

7) **Routing:**

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

8) **Security:**

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

## d) Explain Design Issues for layers.

## Ans:

### ***Design issues for layers:***

A number of design issues exist for the layer to layer approach of computer networks.

Some of the main design issues are as follows −

**9) Reliability:**

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not inaccurate.

**10) Scalability:**

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

**11) Addressing:**

At a particular time, countless messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

**12) Error Control:**

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

**13) Flow Control:**

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

**14) Resource Allocation:**

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

**15) Routing:**

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

**16) Security:**

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

## e) Explain service primitives.

## Ans:

### ***Service Primitives - listen, connect, receive, send, and disconnect:***

A service is formally specified by a set of primitives (operations) available to user processes to access the service.

These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.

The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connectionless service.

| **Primitive** | **Meaning** |
|---|---|
| **1. LISTEN** | Block waiting for an incoming connection |
| **2. CONNECT** | Establish a connection with a waiting peer |
| **3. ACCEPT** | Accept an incoming connection from a peer |
| **4. RECEIVE** | Block waiting for an incoming message |
| **5. SEND** | Send a message to the peer |
| **6. DISCONNECT** | Terminate a connection |

Figure. Six service primitives that provide a simple connection-oriented service.

These primitives might be used for a request-reply interaction in a client-server environment.

First, the server executes **LISTEN** to indicate that it is prepared to accept incoming connections. A common way to implement LISTEN is to make it a blocking system call.

Next, the client process executes **CONNECT** to establish a connection with the server. The CONNECT call needs to specify who to connect to, so it might have a parameter giving the server's address. The operating system then typically sends a packet to the peer asking it to connect, as shown in below Figure.

The client process is suspended until there is a response (1). When the packet arrives at the server, the operating system sees that the packet is requesting a connection. It checks to see if there is a listener, and if so it unblocks the listener. The server process can then establish the connection with the **ACCEPT** call. This sends a response back to the client process to accept (2) the connection.

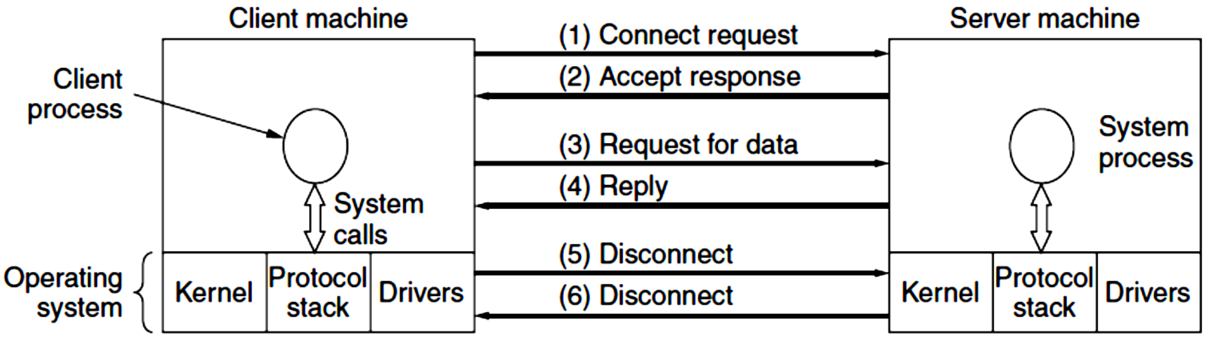


**Fig.** a simple client-server interaction using acknowledged datagrams.

At this point the client and server are both running and they have a connection established.

The next step is for the server to execute **RECEIVE** to prepare to accept the first request. Then the client executes **SEND** to transmit its request (3) followed by the execution of RECEIVE to get the reply. The arrival of the request packet at the server machine unblocks the server so it can handle the request.

After it has done the work, the server uses SEND to return the answer to the client (4). The arrival of this packet unblocks the client, which can now inspect the answer. If the client has additional requests, it can make them now.

When the client is done, it executes **DISCONNECT** (5) to terminate the connection. Usually, an initial DISCONNECT (6) is a blocking call, suspending the client and sending a packet to the server saying that the connection is no longer needed.

## Q.3. Attempt any THREE of the following (5 Marks each) 15

### a) Explain ISO/OSI Model in detail.

**Ans:**

***<u>OSI reference model:</u>***

- The OSI model is developed by the International Standards Organization (ISO).
- The model is called the ISO OSI (Open Systems Interconnection) Reference
- Model, we will just call it the OSI model for short.
- This model formed in year 1983 as a first step toward international standardization of the protocols used in the various layers.
- The OSI model has seven layers.

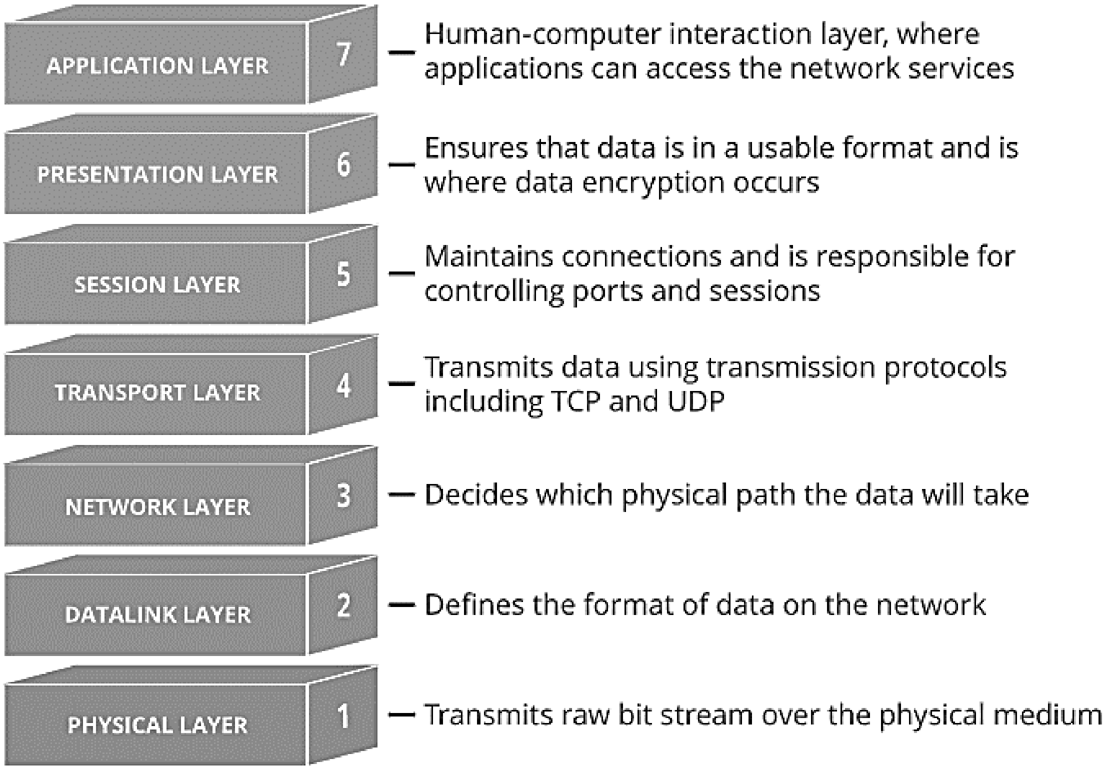

APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATALINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

**Fig.** OSI Reference Model

***7. The Application Layer:***

This is the only layer that directly interacts with data from the user. **Software applications like web browsers and email clients** rely on the application layer to initiate communications. Application layer protocols include **HTTP, FTP** as well as **SMTP** (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

***6. The Presentation Layer:***

This layer is primarily responsible for preparing data so that it can be used by the application layer. The presentation layer is responsible for translation, encryption, and compression of data like **MPEG, JPEG** formats.

- **Translation:** Two communicating devices communicating may be using different encoding methods.
- **Encryption:** it can present the application layer with unencrypted, readable data.
- **Compression:** This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

***5. The Session Layer:***

This is the layer responsible for **opening and closing communication** between the two devices. The time between when the communication is opened and closed is known as the **session**. The session layer also **synchronizes data transfer with checkpoints**.

***4. The Transport Layer:***

- **End-to-end communication** between the two devices.

- **Breaking it up into chunks called segments** before sending it to layer 3.
- **Reassembling the segments** into data the session layer can consume.
- **Flow control and error control**
- **TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)** are used here.

***3. The Network Layer:***

The network layer is responsible for facilitating data transfer between two **different networks**. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer **breaks up segments from the transport layer into smaller units, called packets**, on the sender's device, and reassembling these packets on the receiving device. The network layer also **finds the best physical path** for the data to reach its destination; this is known as routing. **IP protocol** works under this layer

***2. The Data Link Layer***

The data transfer between two devices on the **same network**. The data link layer takes data from the network layer and **breaks them into smaller pieces called frames**. Like the network layer, the data link layer is also responsible for **flow control and error control in intra-network communication** (The transport layer only does flow control and error control for inter-network communications). The **point to point protocol, switch and bridge** networking devices are works under this layer.

***1. The Physical Layer***

This layer includes the physical equipment involved in the data transfer, such as the **cables and switches**. This is also the layer where the **data gets converted into a bit stream**, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

## b) Explain TCP/IP Model in detail.

## Ans:

## TCP/IP Reference Model:

The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.

- The TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s
- It stands for Transmission Control Protocol/Internet Protocol.
- It is based on standard protocols.
- The TCP/IP model is older than the OSI model.
- It contains four layers, unlike seven layers in the OSI model.

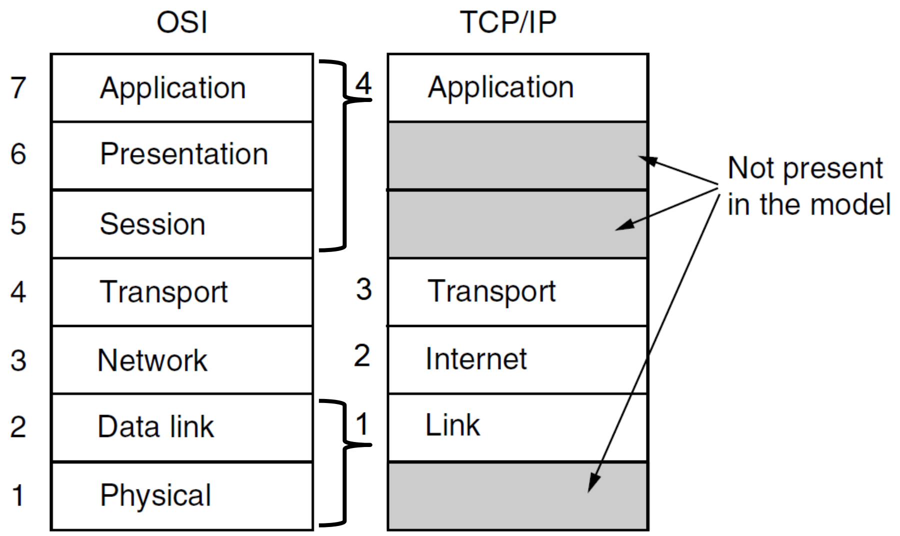


**Fig.** The TCP/IP Reference Model

**1. Link Layer –**

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

**2. Internet Layer –**

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: **IPv4** and **IPv6**. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

**3. Transport Layer –**

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are:

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

**4. Application Layer –**

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, and LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are:

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL (Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

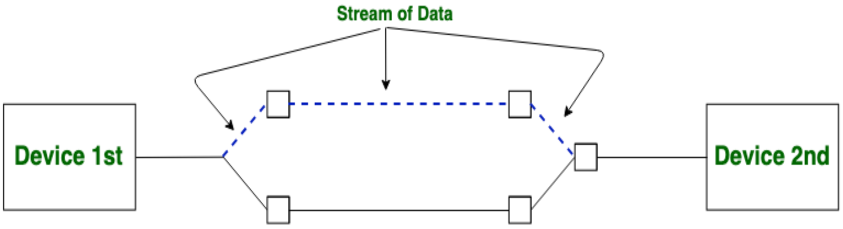
## c) Explain Connection Oriented and Connection less Services

## Ans:

### ***Connection Oriented & Connectionless services:***

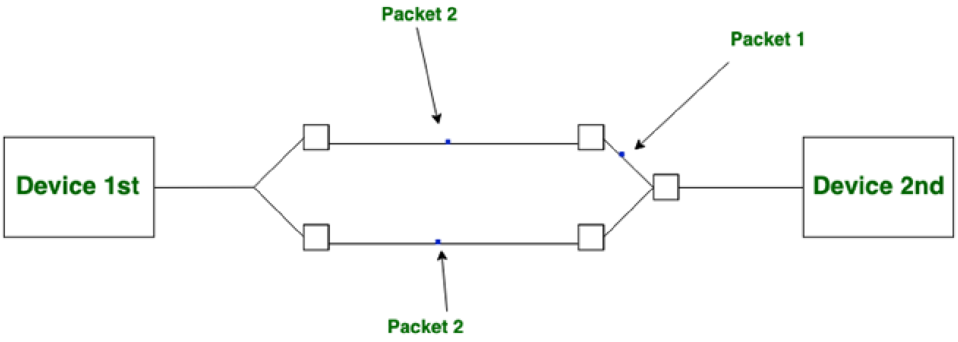
Both Connection-oriented service and Connection-less service are used for the connection establishment between two or more devices.

**Connection-oriented service:** It is modelled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection (A **circuit** is another name for a connection), uses the connection, and then releases the connection. The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end. In most cases the order is preserved so that the bits arrive in the order they were sent.



CONNECTION-ORIENTED SERVICE

**Connectionless service**: It is modelled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages. There are different names for messages in different contexts; a **packet** is a message at the network layer. When the intermediate nodes receive a message in full before sending it on to the next node, this is called **store-and-forward switching**. Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent can be delayed so that the second one arrives first.



CONNECTIONLESS SERVICE

**Comparison of Connection-oriented vs Connection-Less service:**

| S. No | Comparison Parameter | Connection-oriented Service | Connection Less Service |
|---|---|---|---|
| 1. | **Related System** | It is designed and developed based on the telephone system. | It is service based on the postal system. |
| 2. | **Definition** | It is used to create an end to end connection between the senders to the receiver before transmitting the data over the same or different network. | It is used to transfer the data packets between senders to the receiver without creating any connection. |
| 3. | **Virtual path** | It creates a virtual path as circuit. | It does not create any virtual connection or path. |
| 4. | **Authentication** | It requires authentication before | It does not require |

|  |  |  |  |
|---|---|---|---|
|  |  | transmitting the data packets. | authentication. |
| 5. | **Data Packets Path** | All data packets are received in the same order as those sent by the sender. | Not all data packets are received in the same order as those sent by the sender. |
| 6. | **Bandwidth Requirement** | It requires a higher bandwidth to transfer the data packets. | It requires low bandwidth to transfer the data packets. |
| 7. | **Data Reliability** | It guarantees that data packets can transfer from one end to the other end. | Data packets may or may not be transfer from one end to the other end. |
| 8. | **Congestion** | There is no data traffic jam. | There may be data traffic jam. |
| 9. | **Protocol** | Transmission Control Protocol (TCP) | User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP). |
| 10. | **Example** | Telephone, Mobile, Video Conferencing, Live broadcasting | WWW, Email etc. |

## d) What is Protocol Hierarchies? Explain in detail.

## Ans:

### <u>Protocol Hierarchies:</u>

A **Protocol** is simply defined as a set of rules and regulations for data communication. Rules are basically defined for each and every step and process at time of communication among two or more computers. In a network there are multiple protocols are used to make data communication successfully in between all nodes or computers of a network.

All protocols might be implemented using hardware, software, or combination of both of them. When one computer send data towards another computer data travels from screen of the user to physical cable and receiving from physical cable to appearing on screen of a computer. When data travels, it goes thought various protocols, such as when data appear on screen a particular protocols will take care and when it processes by Operating System and send towards cable there are another some special protocols used. The working category of protocols defined by the layers.

To reduce their design complexity, most networks are organized as a **stack of layers or levels**, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

This concept is actually a familiar one and is used throughout computer science, where it is variously known as information hiding, abstract data types, data encapsulation, and object-oriented programming. The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them. When layer *n* on one machine carries on a conversation with layer *n* on another machine, the rules and conventions used in this conversation are collectively known as the layer *n* protocol.

A set of layers and protocols is called a **network architecture**. The diagram shows communication between Host 1 and Host 2. The data is passed through a number of layers from one host to other. Virtual communication is represented using dotted lines between layers. Physical communication is represented using solid arrows between adjacent layers. Through physical medium, actual communication occurs. The layers at same level are commonly known as peers.

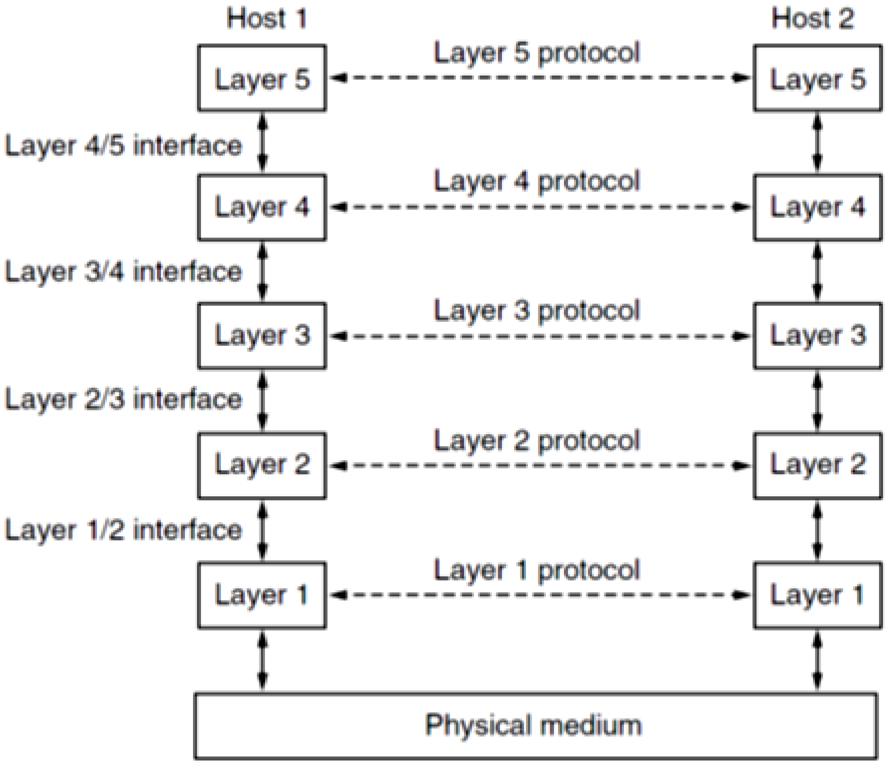


**Figure**-A five-layer network.

The **peers** may be software processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol to talk to each other. The peer basically has a set of communication protocols.

An **interface** is present between each of layers that are used to explain operations and services provided by lower layer to higher layer.

Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the **physical medium** through which actual communication occurs. In above Figure, virtual communication is shown by dotted lines and physical communication by solid lines.

**Advantages:**

- The layers generally reduce complexity of communication between networks
- It increases network lifetime.
- It also uses energy efficiently.
- It does not require overall knowledge and understanding of network.

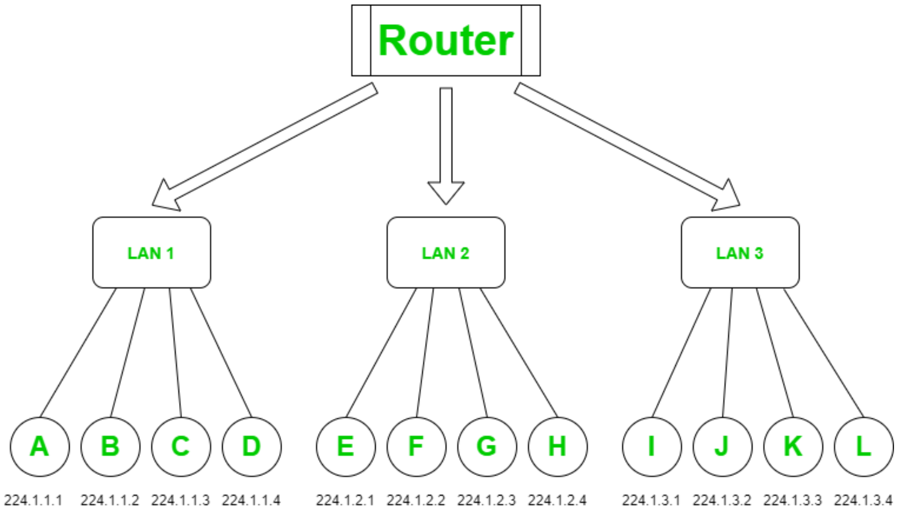
## e) Explain concept of addressing in detail.

## Ans:

### <u>Addressing:</u>

A computer network is a group of some interconnected computers that are sharing a common or different resources provided on or by network nodes. These sharing or communication between the machines is governed by some set of rules or network protocols. These computers or machines are identified by network addresses, and may have hostnames.

A Network Address is a logical or physical address that uniquely identifies a host or a machine in a telecommunication network. A network may also not be unique and can contain some structural and hierarchical information of the node in the network. Internet protocol (IP) address, media access control (MAC) address and telephone numbers are some basic examples of network addresses. It can be of numeric type or symbolic or both in some cases.



### Network Addressing:

It is the prime responsibility of the network layer to assign unique addresses to different nodes in a network. As mentioned earlier they can be physical or logical but primarily they are logical addresses i.e. software-based addresses.

The most widely used network address is an IP address.

## IP Address:

It uniquely identifies a node in an IP network. An IP address is a 32-bit long numeric address represented in a form of dot-decimal notation where each byte is written in a decimal form separated by a period.

**For example** 196.32.216.9 is an IP address where 196 represents first 8 bits, 32 next 8 bits and so on. The first three bytes of an IP address represents the network and the last byte specifies the host in the network.

## IP Address Classes:

An IP address is further divided into sub classes :

| | |
|---|---|
| **Class A:** | An IP address is assigned to those networks that include large number of hosts. |
| **Class B:** | An IP address is assigned to networks range from small sized to large sized. |
| **Class C:** | An IP address is assigned to networks that are small sized. |
| **Class D:** | IP address are reserved for multicast address and does not possess subnetting. |
| **Class E:** | An IP address is used for the future use and for the research and development purposes and does not possess any subnetting. |

**An IP address is divided into two parts:**

1. **Network ID :** represents the number of networks.
2. **Host ID :** represents the number of hosts (computers).

## Q.4. Attempt any THREE of the following (5 Marks each) 15

### a) What is error control? Explain in detail.

### Ans:

## Error Control:

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

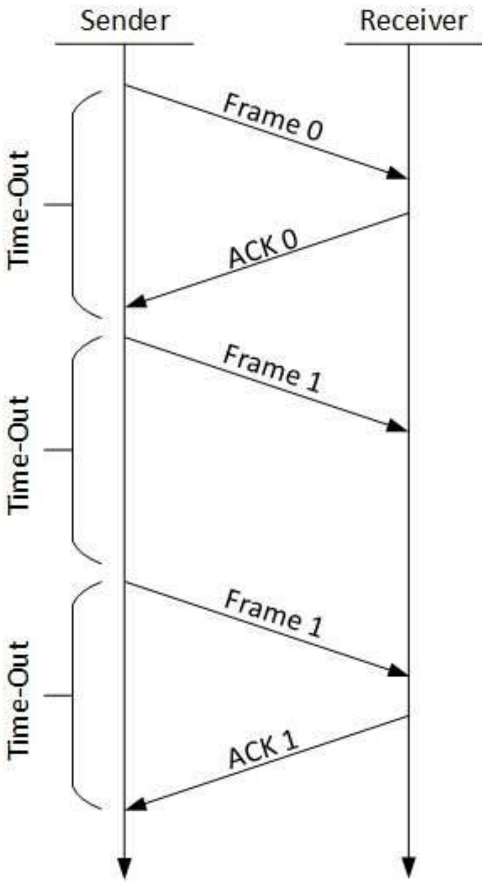
Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

- **Stop-and-wait ARQ**

  The following transition may occur in Stop-and-Wait ARQ:
  - The sender maintains a timeout counter.
  - When a frame is sent, the sender starts the timeout counter.
  - If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
  - If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
  - If a negative acknowledgement is received, the sender retransmits the frame.



## b) Explain HUB, Switch and Router.

## Ans:

## Hub:

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices

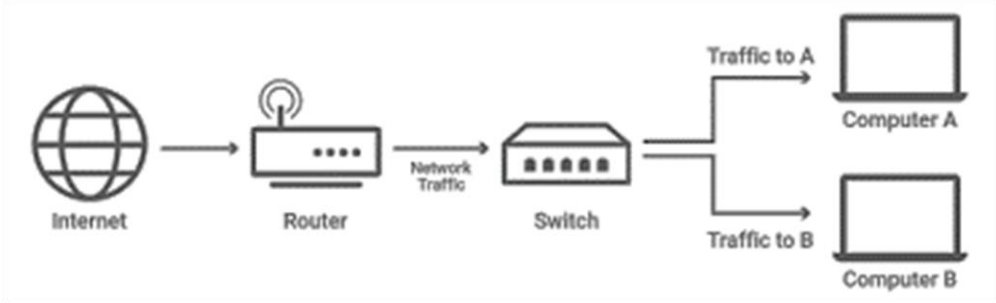
**Types of Hub**

1. **Passive Hub:** The passive hubs are the connection point for wires that helps to make the physical network. It is capable of determining the bugs and faulty hardware. Simply, it accepts the data packet over a port and circulates it to all ports. It includes connectors RJ-45 that can be applied as a standard in your network. This connector is connected to all local area network (LAN) devices.
2. **Active Hub:** As compared to a passive hub, it includes some additional features. It is able to monitor the data sent to the connected devices. It plays an important role between the connected devices with the help of store technology, where it checks the data to be sent and decides which packet to send first. It has the ability to fix the damaged packets when packets are sending, and also able to hold the direction of the rest of the packets and distribute them. It can boost the signal if any connecting device is not working in the network. Therefore, it helps to make the continuity of services in LAN.
3. **Intelligent Hub:** It is a little smarter than passive and active hubs. These hubs have some kinds of management software that help to analyze the problem in the network and resolve them. It is beneficial to expend the business in networking; it offers better performance for the local area network. Furthermore, with any physical device, if any problem is detected, it is able to detect this problem easily.

---

## 3) Switch:

Switch is a network device that connects other devices to networks through twisted pair cables. A switch is a data link layer device. Switch is used in STAR topology. Switch is an upgraded networking device from Hub. It uses packet switching technique to receive, store and forward data packets on the network. The switch maintains a list of network addresses of all the devices connected to it.



The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. On receiving a packet, it checks the destination address and transmits the packet to the correct port.

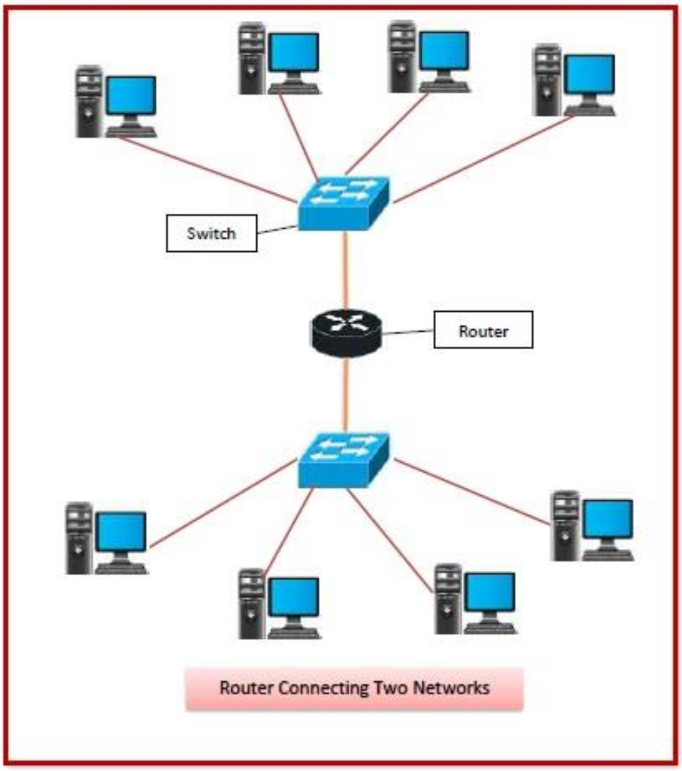
Data transmission speed in switches is double as compared to hubs. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on networks through use of multiple switches.

## Router:

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

### How does a router work?

Think of a router as an air traffic controller and data packets as aircraft headed to different airports (or networks). Just as each plane has a unique destination and follows a unique route, each packet needs to be guided to its destination as efficiently as possible. In the same way that an air traffic controller ensures that planes reach their destinations without getting lost or suffering a major disruption along the way, a router helps direct data packets to their destination IP address.



In order to direct packets effectively, a router uses an internal routing table — a list of paths to various network destinations. The router reads a packet's header to determine where it is going, then consults the routing table to figure out the most efficient path to that destination. It then forwards the packet to the next network in the path.

**Features of Routers**

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs, bridges and switches.

## What is Routing Table?

The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations. The router consults the routing table to determine the optimal route through which the data packets can be sent.

**Routing tables are of two types −**

- **Static Routing Table** − Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.

**Dynamic Routing Table** − Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of

routers.

## c) What is Flow control? Explain in detail with diagram.

## Ans:

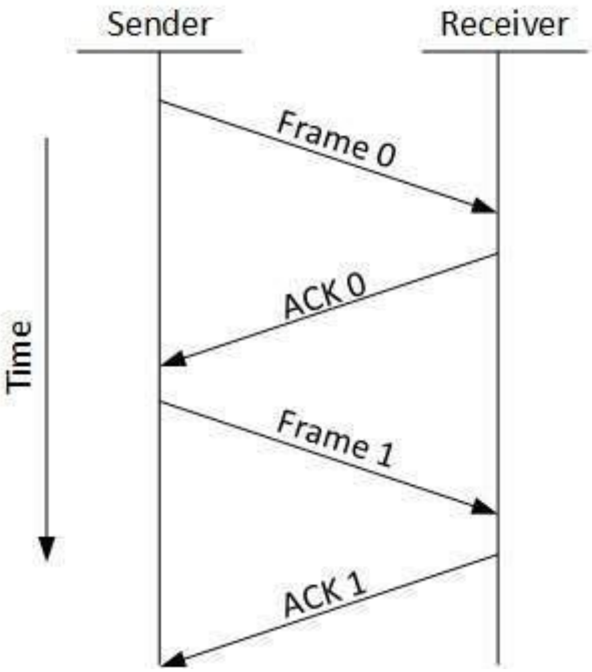
## Flow Control:

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- **Stop and Wait**
  This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.

- **Sliding Window**
  In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.



## d) Explain Multiplexing with all types in detail.

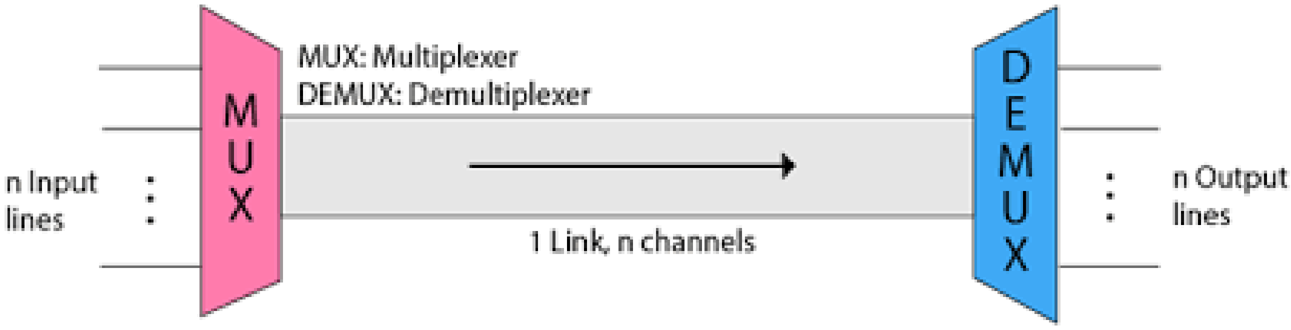
### Ans: Multiplexing & De-Multiplexing:

**Multiplexing** is the process of combining multiple signals into one signal, over a shared medium. If the analog signals are multiplexed, then it is called as **analog multiplexing**. Similarly, if the digital signals are multiplexed, then it is called as **digital multiplexing**.

Multiplexing was first developed in telephone system.

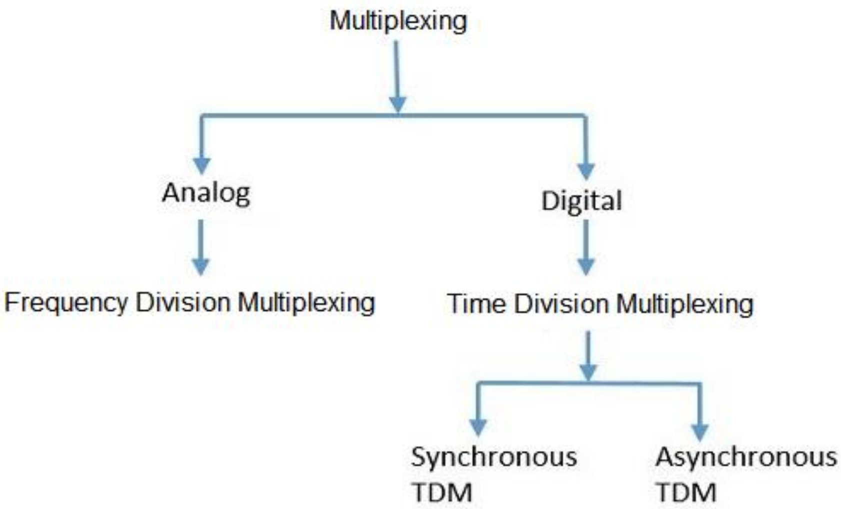
The device that does multiplexing can be called as **Multiplexer** or **MUX**.

The device that does de-multiplexing can be called as **de-multiplexer** or **DEMUX**.



## ③ Types of Multiplexing:

A device is used to multiplexing called Multiplexer, There are mainly two types of multiplexers, namely analog and digital. They are further divided into Frequency Division Multiplexing (FDM), Wavelength Division Multiplexing (WDM), and Time Division Multiplexing (TDM). The following figure gives a detailed idea about this classification.

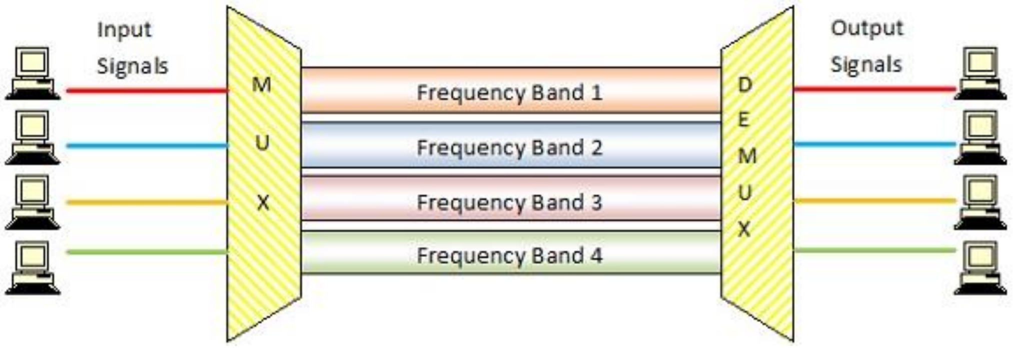


## 1. Analog Multiplexing:-

The signals used in analog multiplexing techniques are analog in nature. The analog signals are multiplexed according to their frequency (FDM) or wavelength (WDM).

### 1.1 Frequency Division Multiplexing:

In analog multiplexing, the most used technique is Frequency Division Multiplexing (FDM). This technique uses various frequencies to combine streams of data, for sending them on a communication medium, as a single signal.



**Example** – A traditional television transmitter, which sends a number of channels through a single cable uses FDM. In Telephone networks. It can also be used in cellular networks, wireless networks and for satellite communications.

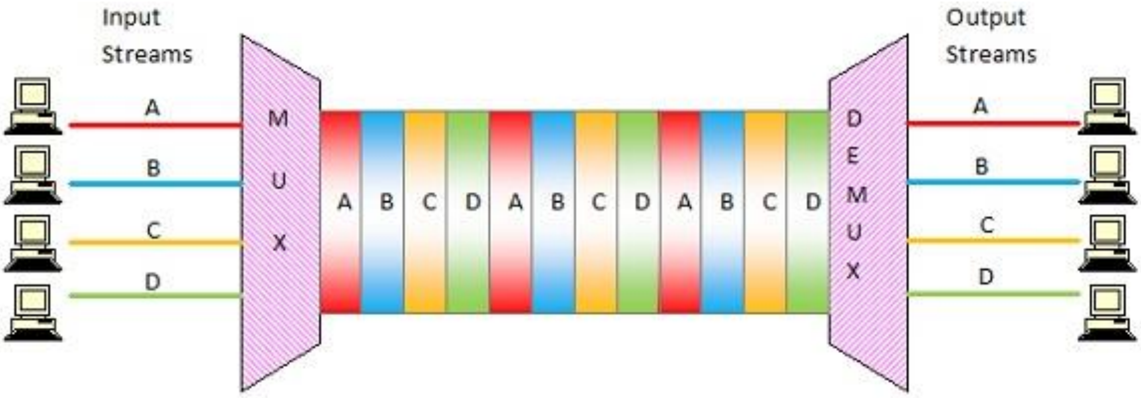
## 2. Digital Multiplexing:-

The term digital represents the discrete bits of information. Hence, the available data is in the form of frames or packets, which are discrete.

### 2.1 Time Division Multiplexing:

In Time Division Multiplexing (TDM), the time frame is divided into slots. This technique is used to transmit a signal over a single communication channel, by allotting one slot for each message.

Time Division Multiplexing (TDM) can be classified into Synchronous TDM and Asynchronous TDM.



### 2.1.1 Synchronous TDM

In Synchronous TDM, the input is connected to a frame. If there are 'n' number of connections, then the frame is divided into 'n' time slots. One slot is allocated for each input line. The MUX allocates the **same slot** to each device at all times.

### 2.1.2 Asynchronous TDM

In Asynchronous TDM, the sampling rate is different for each of the signals and a common clock is not required. If the allotted device for a time slot transmits nothing and sits idle, then that slot can be **allotted to another** device, unlike synchronous

This type of TDM is used in Asynchronous transfer mode networks.

## e) Difference between parallel & serial data transmission mode.

## Ans:

### ➢ Serial and Parallel Data Transmission:

The process of sending data between two or more digital devices is known as *data transmission*. Data is transmitted between digital devices using one of the two methods – *serial transmission* or *parallel transmission*.

### What is Serial Transmission?

In serial transmission, data bits are sent one after the other across a single channel. A serial transmission transfers data one bit at a time, consecutively, via a communication channel or computer bus in telecommunication and data transmission. On the other hand, parallel communication delivers multiple bits as a single unit through a network with many similar channels.

- 8-bits are conveyed at a time in serial transmission, with a start bit and a stop bit.
- All long-distance communication and most computer networks employ serial communication.
- Serial computer buses are becoming more common, even across shorter distances, since newer serial technologies' greater signal integrity and transmission speeds have begun to outperform the parallel bus's simplicity advantage.
- The majority of communication systems use serial mode. Serial networks may be extended over vast distances for far less money since fewer physical wires are required.

### What is Parallel Transmission?

Parallel data transmission distributes numerous data bits through various channels at the same time. Parallel communication is a means of transmitting multiple binary digits (bits) simultaneously in data transmission. It differs from serial communication, which sends only one bit at a time; this distinction is one method to classify a communication channel.

- A parallel interface comprises parallel wires that individually contain data and other cables that allow the transmitter and receiver to communicate. Therefore, the wires for a similar transmission system are put in a single physical thread to simplify installation and troubleshooting.
- A large amount of data must be delivered across connection lines at high speeds that match the underlying hardware.
- The data stream must be transmitted through "n" communication lines, which necessitates using many wires. This is an expensive mode of transportation; hence it is usually limited to shorter distances.

## Difference between Serial and Parallel Transmission

The following table highlights the major differences between Serial and Parallel Transmission –

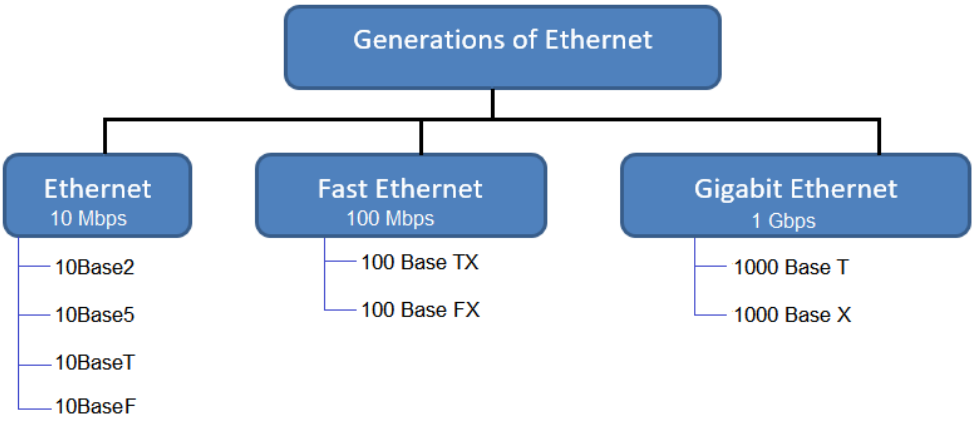
| Key | Serial Transmission | Parallel Transmission |
|---|---|---|
| **Definition** | Serial Transmission is the type of transmission in which a single communication link is used to transfer the data from one end to another. | Parallel Transmission is the mode of transmission in which multiple parallel links are used that transmit each bit of data simultaneously. |
| **Bit transmission** | In case of Serial Transmission, only one bit is transferred at one clock pulse. | In case of Parallel Transmission, 8-bits transferred at one clock pulse. |
| **Cost Efficiency** | As single link is used in Serial Transmission, it can be implemented easily without having to spend a huge amount. It is cost efficient. | Multiple links need to be implemented in case of Parallel Transmission, hence it is not cost efficient. |
| **Performance** | As single bit gets transmitted per clock in case of Serial Transmission, its performance is comparatively lower as compared to Parallel Transmission. | 8-bits get transferred per clock in case of Parallel transmission, hence it is more efficient in performance. |
| **Preference** | Serial Transmission is preferred for long distance transmission. | Parallel Transmission is preferred only for short distance. |
| **Complexity** | Serial Transmission is less complex as compared to that of Parallel Transmission. | Parallel Transmission is more complex as compared to that of Serial Transmission. |

## Q.5. Attempt any THREE of the following (5 Marks each) 15

## a) Explain Ethernet, Fast Ethernet, and Gigabit Ethernet in detail.

**Ans:**

## Network Standards:



### A) Ethernet:

Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN within buildings, homes, and even small neighborhoods.

### Types of Ethernet:

**10Base2:**

- 10Base2 is sometimes referred to as **ThinNet** (or "thin coax") because it uses thin coaxial cabling for connecting stations to form a network.
- 10Base2 supports a maximum bandwidth of **10 Mbps**.

**10Base5:**

- 10Base5 is sometimes referred to as **ThickNet** because it uses thick coaxial cabling for connecting stations to form a network. Another name for 10Base5 is Standard Ethernet because it was the first type of Ethernet to be implemented.
- 10Base5 supports a maximum bandwidth of **10 Mbps**.

**10BaseT:**

- 10BaseT is the most popular form of 10-Mbps Ethernet, using **unshielded twisted-pair (UTP) cabling** for connecting stations, and using hubs to form a network.
- 10BaseT supports a maximum bandwidth of **10 Mbps**.

**10BaseF:**

- 10BaseF is different from other 10-Mbps Ethernet technologies because it uses **fiber-optic cabling** instead of copper unshielded twisted-pair (UTP) cabling.

## B) Fast Ethernet:

- Fast Ethernet is a version of Ethernet standards, initiated in 1995 as IEEE 802.3u.
- Fast Ethernet focused on increased network and network appliance speed over standard Ethernet and Ethernet devices.
- Fast Ethernet provided uniform operability for data transmission at over 100 megabits per second.
- It is designed for 100 Base T networks and is also compatible with 10 Base T networks, allowing users to benefit from faster Ethernet speeds (with the use of compatible switches) without having to completely upgrade their network systems.
- **Unshielded Twisted Pair (UTP)** cabling such as Category 5 and higher rated cables can run on Fast Ethernet devices. However, the maximum length and effectiveness of UTP cabling is 100 meters and bandwidth can be limited.
  - **100BaseTX:** This is a twisted pair cable and offer a speed of 100 Mbps.
- **Fiber optic** transmission allows for longer distance and greater bandwidth capacity over UTP cabling, permitting Fast Ethernet network appliances and devices to deliver at full potential.
  - **100Base FX:** Fiber optic protocol which offers a speed of 100 Mbps.

## C) Gigabit Ethernet

- Gigabit Ethernet is the **latest version of Ethernet standards**, initiated in **1999** as **IEEE 802.3ab** and in **2004** as **IEEE 802.3ah**. Gigabit Ethernet provided uniform standards for **1000 megabits per second**, or **1 gigabit per second**, network transmission.
- **Standard IEEE 802.3ab**: It defined Gigabit Ethernet's applicability for 1000 Base T networks and allowed use of existing UTP cabling. The IEEE 802.3ab standard certified Gigabit Ethernet applicability for both industry and desktop users working with the existing Category 5 cables.
- **Standard IEEE 802.3ah:** It certified for fiber optic transmissions.
  - **1000Base SX:** Fiber optic protocol which used for multimode networks.
  - **1000Base LX:** Fiber optic protocol which used for singlemode networks.

  Gigabit Ethernet network appliances and devices can transfer data packets at rates much faster than Fast Ethernet. A Fast Ethernet switch can transfer data packets at a rate of 10 to 100 megabits per second where a Gigabit Ethernet switch can transfers data packets at relatively higher speeds of one gigabit per second.
- In comparison, a Gigabit Ethernet switch can transfer data packets at around 100 times faster than a Fast Ethernet switch. Gigabit Ethernet can meet increasingly complex network demands such as connecting multiple bandwidth-intensive devices and broadband internet connections for video streaming.
- Gigabit Ethernet applications include gigabit switches that can manage data transfer between multiple IP security cameras and network appliances, and gigabit switches that support video and other high-quality signal transfer between home servers and high-definition televisions and monitors.

## b) Explain FDDI in detail with example.

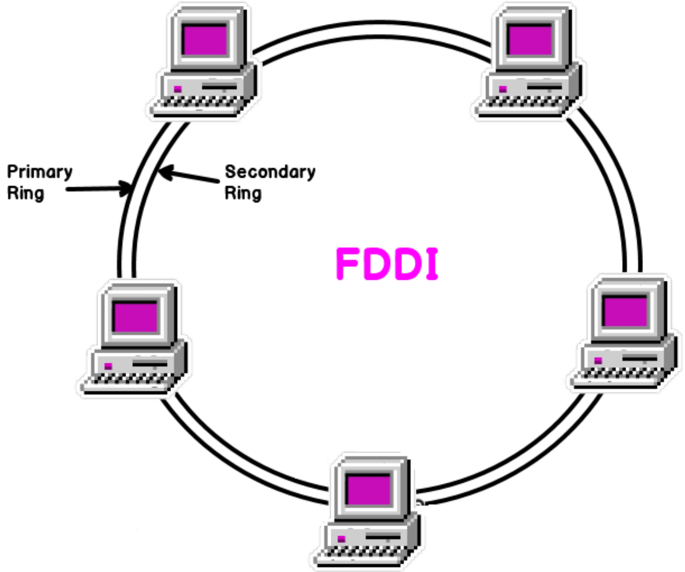
## Ans:

**FDDI:**

Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables.

FDDI was created in 1986 by ANSI. It is applicable in large LANs that can extend up to 200 kilometers in diameter. The cable used in FFDI is fiber optic to make ring of the network. Two rings (cables) are used to prevent sudden network down problem. It is in fact a pair of rings (one is called "primary", the other, allowing to catch up the errors of the first, is called "secondary").

The **FDDI topology** is used the token ring topology. This is called a bi-connected system. Fiber Distributed Data Interface (FDDI) is a type of LAN or MAN computer network that allows multiple LANs to be interconnected at a speed of 100 Mbit/s over fiber optics (which allows it to reach a maximum distance of 200 km).



A signal which rotates continuously on the ring is called as token. The token circulates between the machines at a very high speed. If the token does not arrive after a certain time, the machine considers that an error has occurred on the network. This technology works under a basic principal "who has token those can send and receive data", it means if any computer wants to send data it first catch the rotating token and engage it then data attach with this token and send on the cable then token along with data will rotate and reached towards other computers, each computer who has not a token checks the destination address of the data and if that matched with itself then it take token with data from the ring and release token from data and again empty token send on the ring to be rotate again.

**Features**

- FDDI uses optical fiber as its physical medium.
- It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
- It provides high data rate of 100 Mbps and can support thousands of users.
- It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
- It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
- FDDI technology can also be used as a backbone for a wide area network (WAN).

**Advantages of FDDI Topology:**

The FDDI is much more advantageous than the token ring because if one of the rings is defective, the network continues to function. In fact, one of the rings can catch and correct the errors of the other and vice versa.

## c) Explain Sliding Window Protocol in detail.

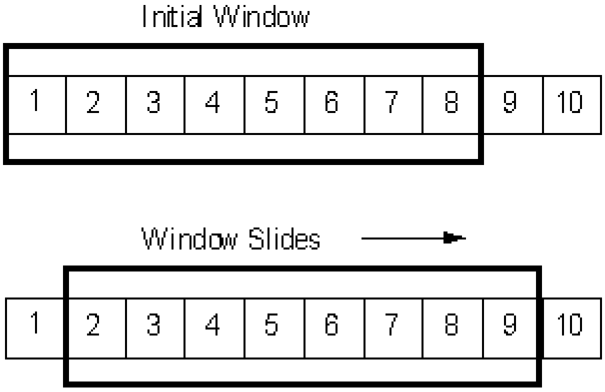
## Ans:

### Sliding Window Protocol:

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end.

The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.



**Types of Sliding Window Protocol:**

1. **Go – Back – *N* ARQ**
   Go – Back – *N* ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

2. **Selective Repeat ARQ**
   This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

**Differences:**

| Go-Back-N ARQ | Selective Repeat ARQ |
|---|---|
| If a frame is corrupted or lost in it,all subsequent frames have to be sent again. | In this, only the frame is sent again, which is corrupted or lost. |
| If it has a high error rate,it wastes a lot of bandwidth. | There is a loss of low bandwidth. |
| It is less complex. | It is more complex because it has to do sorting and searching as well. And it also requires more storage. |
| It does not require sorting. | In this, sorting is done to get the frames in the correct order. |
| It does not require searching. | The search operation is performed in it. |
| It is used more. | It is used less because it is more complex. |

## d) Explain Network protocols- IP, PPP & FTP.

## Ans:

**1) Internet Protocol (IP):**

- Internet Protocol is **connectionless** and **unreliable** protocol. It ensures no guarantee of successfully transmission of data.
- In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

- Internet protocol transmits the data in form of a **datagram**. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.
- The first major version of IP, Internet Protocol Version 4 (**IPv4**), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (**IPv6**), which has been in increasing deployment on the public Internet since c. 2006.

**Points to remember:**

- The length of datagram is variable.
- The Datagram is divided into two parts: **header** and **data.**
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.

**2) PPP Protocol:**

- The PPP stands for **Point-to-Point protocol**.
- It is the most commonly used protocol for point-to-point access.
- It is a data **link layer protocol** that resides in the layer 2 of the OSI model.
- The main feature of the PPP protocol is the **encapsulation**. It defines how network layer data and information in the payload are encapsulated in the data link frame.
- It defines the **authentication** process between the two devices. The authentication between the two devices, handshaking and how the password will be exchanged between two devices are decided by the PPP protocol.
- The PPP protocol can be used on synchronous link like **ISDN** as well as asynchronous link like **dial-up**. It is mainly used for the communication between the two devices.
- It can be used over many types of physical networks such as **serial cable, phone line, trunk line, cellular telephone, fiber optic links such as SONET**.
- As the data link layer protocol is used to identify from where the transmission starts and ends, so ISP (Internet Service Provider) use the PPP protocol to provide the dial-up access to the internet.

**Services provided by PPP**

- It defines the format of frames through which the transmission occurs.
- It defines the link establishment process. If user establishes a link with a server, then "how this link establishes" is done by the PPP protocol.
- It defines data exchange process, i.e., how data will be exchanged, the rate of the exchange.

**3) FTP Protocol:**

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is also used for downloading the files to computer from other servers.
- It provides the sharing of files.

- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

**Advantages of FTP:**

1. **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
2. **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
3. **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
4. **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

## e) Explain Internet verses Intranet.

## Ans:

### Internet versus Intranet:

| Attributes | Internet | Intranet |
|---|---|---|
| **Definition** | Internet is a WWW service of computer network applied on WAN network. | An Intranet is a private network of computers designed for a certain group of people and owned by a particular firm or organization. |
| **Users** | The Internet is a globally connected network; number of users are comparatively much higher than Intranet. | Because of a limited range, the total numbers of users on Intranet are limited. When compared to the Internet, Intranet has very few users. |

| | | |
|---|---|---|
| **Accessibility** | Anyone can access and use it on worldwide basis. | Only certain people are authorized to use Intranet because it is a company's internal network, so accessible by the employees or admin who have login credentials. |
| **Type of Network** | The Internet is a type of public network (Wide Area Network). | The intranet is a type of private network installed mainly for any organization operations. It can include several local area networks and also uses high speed internet connection in the wide-area network. |
| **Security** | Because the internet is a public network, it is a considerably less secure network. Cybercriminals usually target people using the Internet. | Due to limited access, there is no such possibility or very less possibility of cyber threats in Intranet, making it more secure compared to that of the Internet. |
| **Information and Data** | Due to a wider range, the availability of information and the data is unlimited. People are free to use the Internet and their knowledge. That is why more and more data is being added to different fields on the Internet regularly. | The intranet is limited to group-specific information. That means the Intranet information and data are limited to any specific company's records, operations, inventory, etc. In this case, only certain people with admin privileges are allowed to add or modify the information. |
| **Traffic** | Due to a higher number of users and a public network, the total visitor's traffic very high. It is almost uncountable. | Intranet has limited users, and so visitor's traffic is limited and comparatively less than the Internet. In the case of Intranet, traffic is countable. |
| **Characteristic** | The Internet includes several intranets. | The intranet is like a subset of the Internet. Intranet can only be used using the Internet but with certain restrictions and security practices. |