ARULMIGU PALANIANDAVR ARTS COLLEGE FOR WOMEN
(Autonomous)
(Re-Accredited with 'B++' Grade by NAAC 3rd Cycle)
Run by Arulmigu Dhandayuthapani Swamy Thirukoil, H.R & C.E Dept. Government of Tamil Nadu
A Government Aided College - Affiliated to Mother Teresa Women's University, Kodaikanal
CHINNAKALAYAMPUTHUR(PO), PALANI - 624615

DEPARTMENT OF COMPUTER SCIENCE

AND

COMPUTER APPLICATION

LEARNING RESOURCE

Data Communications

The fundamental purpose of a communication system is the exchange of data between two communicable devices. So to make the communication possible, the devices need to be connected through some form of transmission medium such as a wire cable.

For data communications to occur, the communicating devices must be part of acommunication system made up of a combination of hardware (physical equipment) and software (programs).

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy:** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness:** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. **Jitter:** Jitter refers to the variation in the packet arrival time. It is the uneven delay in thedelivery of audio or video packets. For example, let us assume that video packets are sent every 30ms. If some of the packets arrive with 30ms delay and others with 40ms delay, an uneven quality in the video is the result.

Components of a data communications system

A data communications system has five components

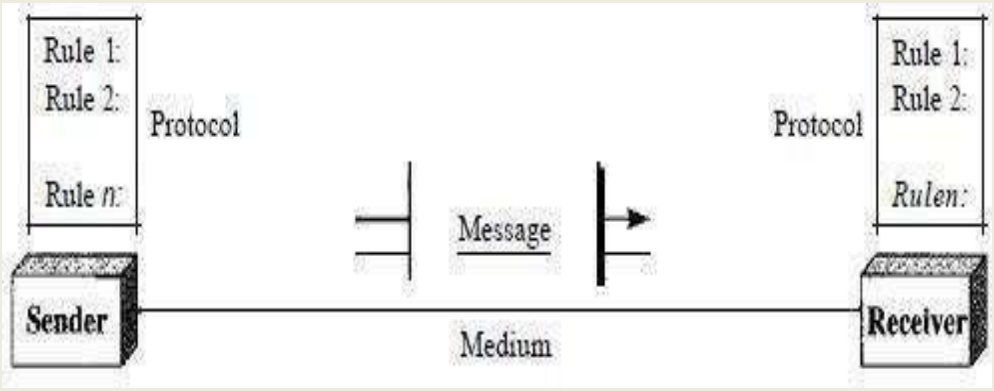
Message: The message is the information(data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

Sender: The sender is the device that sends the data message.It can be a computer, workstation, telephone handset, video camera, and so on.

Receiver: The receiver is the device that receives the message.It can be a computer, workstation, telephone handset, television, and so on.

Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver.Some examples of transmission media include twisted-pairwire, coaxial cable, fiber-optic cable, and radio waves.

Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.



Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (Os or Is). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers:

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution.* For example, an image can be divided into 1000 pixels or 10,000

pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image. After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only blackand- white dots (e.g., a chessboard), a I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: *red*, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

ANALOG AND DIGITAL SIGNALS

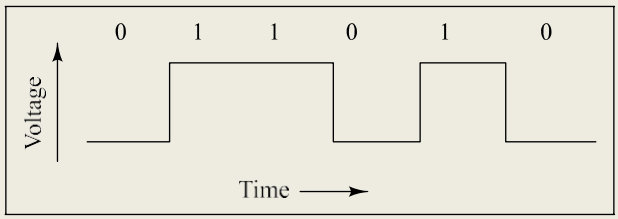


Fig.1.7 Digital Signal

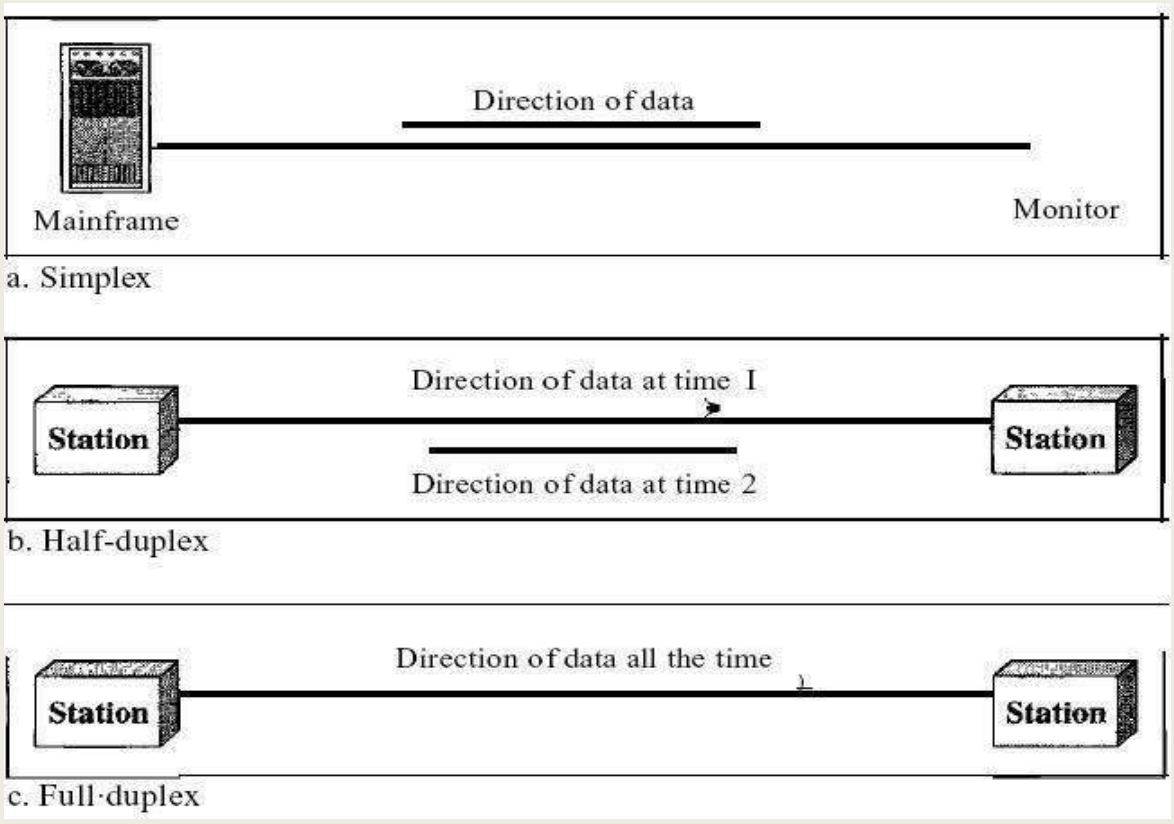
The term *analog* is very common and has been used for decades in the field of telephony. The human voice generates an analog (i.e.,continuously varying) signal, which is transmitted as an analog signal over the medium. On the way, the signal suffers attenuation. Amplifiers are used to overcome this problem,but then amplifiers amplify noise along with the original signal.The problem with this type of combination is that if the signal gets distorted, it cannot be reconstructed at all. It is a permanent loss. At the destination, it is very difficult to imagine, from the received distorted signal, what the signal *should have been*. This is thereas on why this type is not used where highlevel of accuracy is desired. However, in human communications, as light distortion does no tnormally matter to the gist or the content of the conversation. Therefore, this has played a major role in telephony in so many past decades. Figure 2.1 shows this.

DIGITAL SIGNAL,DIGITALTRANSMISSION

We know that the information coming out of a computer is in the form of digital signals. We also know that a digital signal has an infinite bandwidth, where as any medium has only a limited bandwidth. Therefore, as the signal is generated, and enters any medium at that point itself, only limited frequencies are permissible on the medium depending upon its *bandwidth* (this has nothing to do with the noise). If we add all the frequencies admitted on the medium, the resultant signal would not be the same as a digital signal.Therefore, the signal is distorted from the original digital signal to begin with. As it traverses over the medium, noise adds further distortion. Beyond a certain distance, the signal becomes unrecognizable from the original one. Therefore hardware equipment called regenerative repeater or repeater is used to regenerate the digital signal as shown in Fig.2.2. We show three points on the path,viz.,*A*,*B* and*C*.At point*A*,the signal is in itsoriginal digital form. It gets distorted at point *B*. However, you can still recognize the signal as 0100101. The repeater *recognizes* the bits and outputs the signal in its original form at point *C*.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure



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 (see Figure a). 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 The half-duplex mode is like a one-lane road with traffic allowed in both directions.

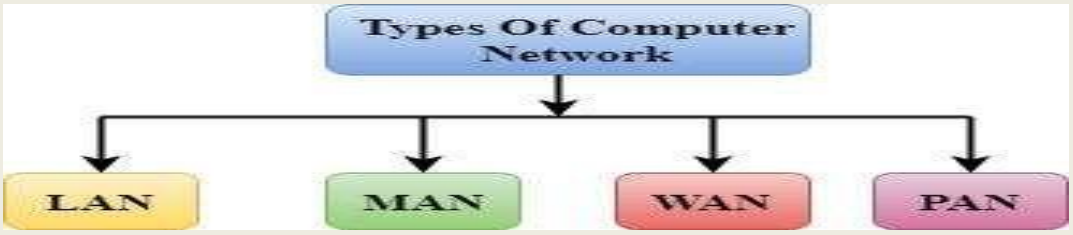
When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously (see Figure c). The full-duplex mode is like a tW<D-way street with traffic flowing in both directions at the same time. In full-duplex mode, si~nals going in one direction share the capacity of the link: with signals going in the other din~c~on. This sharing can occur in two ways: Either the link must contain two physically separate t:nmsmissiIDn paths, one for sending and the other for receiving; or the capacity is divided between signals traveling in both directions. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

Types of Computer Networks:

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.



5

1. **Local Area Network (LAN).**
2. **Metropolitan Area Network (MAN).**
3. **Wide Area Network(WAN).**
4. **Personal Area Network.** A **Personal Area Network (PAN)** is the most basic type, usually used for homes or home offices. ...

Local Area Network (LAN) :

- Local Area Network is a group of computers connected to each other in a small area such as building,office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

Metropolitan Area Network(MAN) :

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.

* 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.
* In MAN, various LANs are connected to each other through a telephone exchange line.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, etc.
*It has a higher range than Local Area Network (LAN).

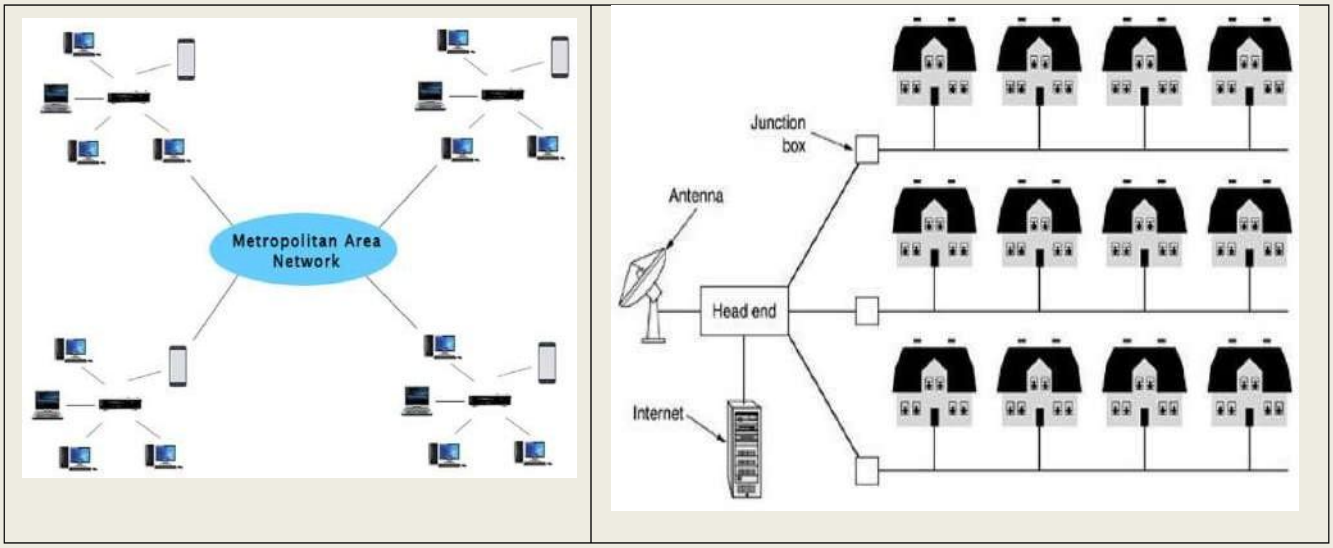


Fig.: Metropolitan area network based on cable TV.

Wide Area Network (WAN) :

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one route to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet.

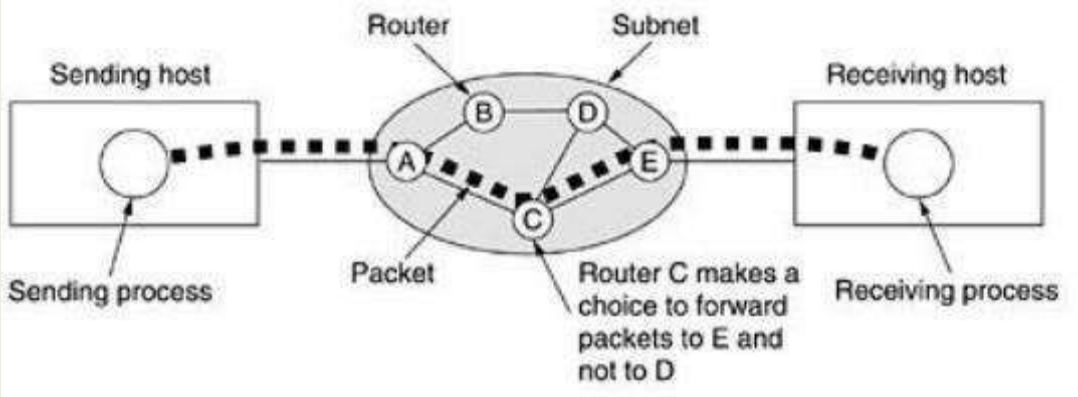
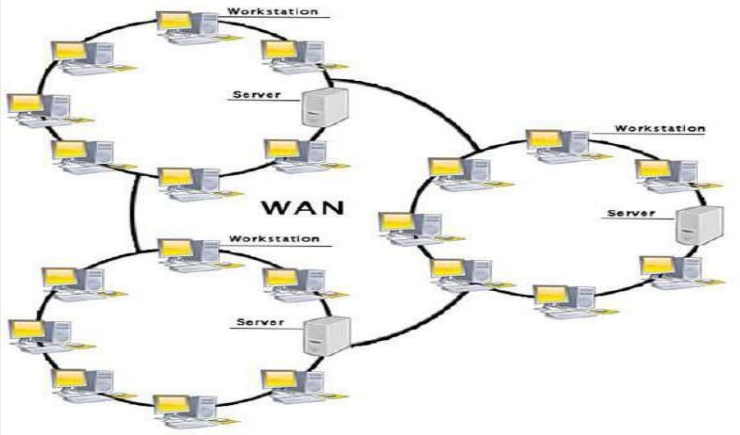


Fig.: A stream of packets from sender to receiver

* A Wide Area Network is a network that extends over a large geographical area such as states or countries.
* A Wide Area Network is quite bigger network than the LAN.
* 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.
* The internet is one of the biggest WAN in the world.
* A Wide Area Network is widely used in the field of Business, government, and education.

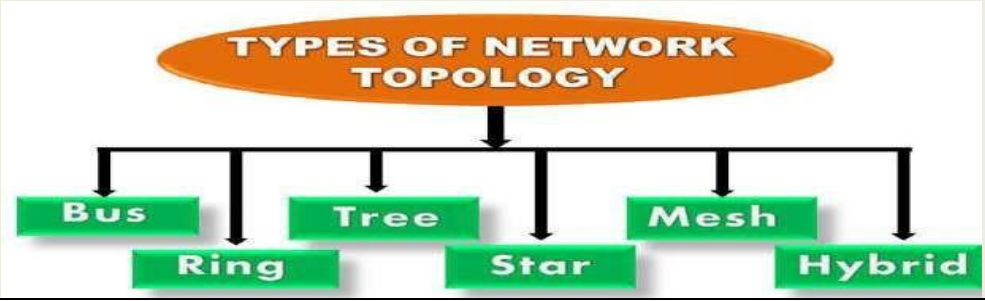


Personal Area Network (PAN):

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Thomas Zimmerman was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of 30 feet.
- Personal computer devices that are used to develop the personal area network are the aptop, mobile phones, media player and play stations.

What is Topology?

- Topology defines the structure of the network of how all the components are interconnected to each other.
- There are two types of topology: **physical and logical topology**.
- Physical topology is the geometric representation of all the nodes in a network.



1. Bus Topology:

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (Ethernet) and 802.4 standard networks.
- 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.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

Advantages of Bus Topology :

- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology :

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.

  It is slower than the ring topology.

2. Ring Topology :

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.

  Token passing: It is a network access method in which token is passed from one node to another node.

  Token: It is a frame that circulates around the network

Working of Token passing :

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology :

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

3. *Star Topology:*

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology :

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology.In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network.

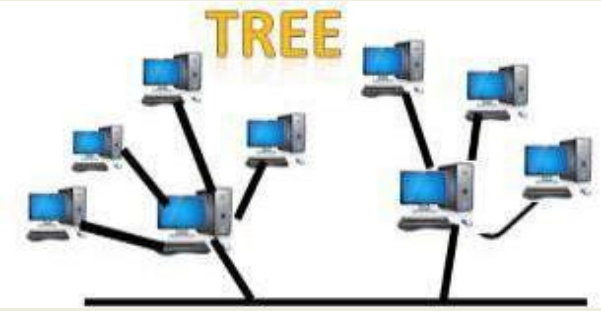
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology :

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

4. Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent -child hierarch



Advantages of Tree topology:

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signalsare sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology iseasily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which canbe easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overallnetwork.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to receive signals

5. *Mesh topology*

- Mesh technology 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.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.

- Mesh topology can be formed by using the formula:

Number of cables = (n(n-1))/2;*

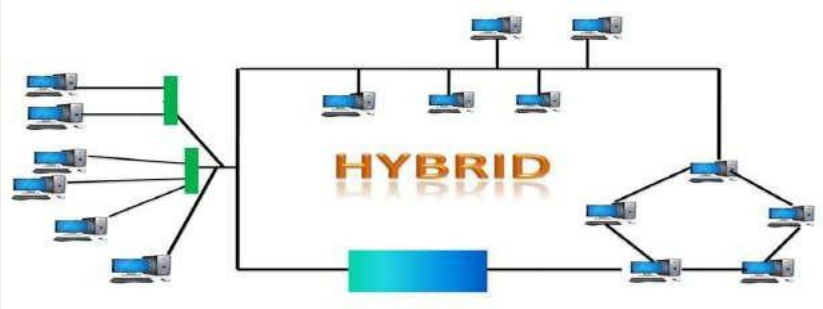
Where n is the number of nodes that represents the network.

Advantages of Mesh topology:

- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other Devices Disadvantages of Mesh topology
- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

6. Hybrid Topology

- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.



THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

A Brief History :

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort. In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.

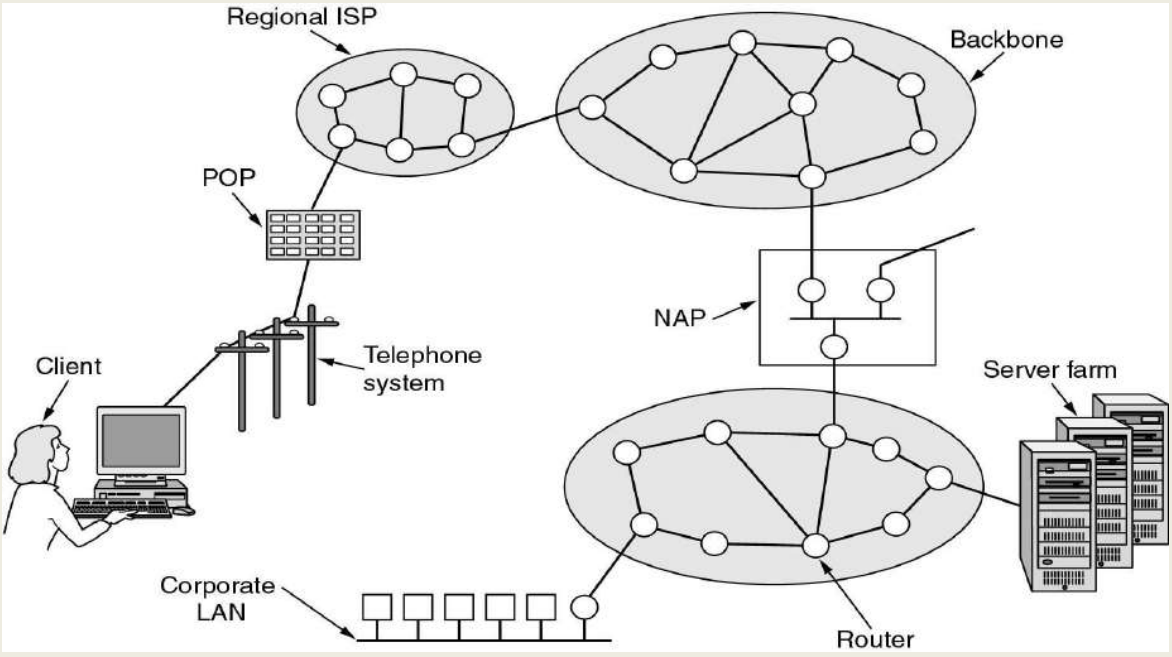
Transmission Control Protocol (TCP) and Internetworking Protocol (lP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.

Internet service provider (ISP), company that provides Internet connections and services to individuals and organizations. In addition to providing access to the Internet, **ISPs** may also provide software packages (such as browsers), e-mail accounts, and a personal Web site or home page.

POP protocol is used in the **application layer protocol**, and it delivers best ability to fetch and receive all email by users.



International Internet Service Providers:

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers:

The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points.* These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers:

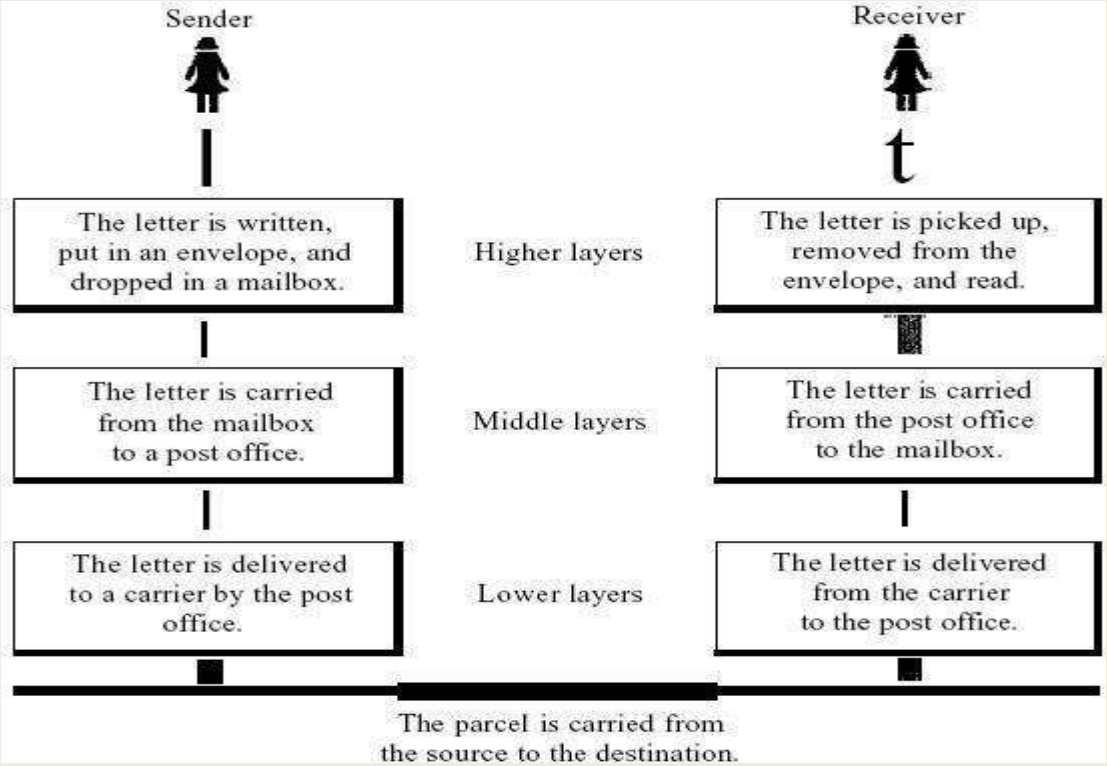
Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

Local Internet Service Providers:

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

LAYERED TASKS

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal maiL The process of sending a letter to a friend would be complex if there were no services available from the post office. Below Figure shows the steps in this task.



Sender, Receiver, and Carrier

In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site

Let us first describe, in order, the activities that take place at the sender site.

- Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.
- Middle layer. The letter is picked up by a letter carrier and delivered to the post office.
- Lower layer. The letter is sorted at the post office; a carrier transports the letter.

0n the Way: The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

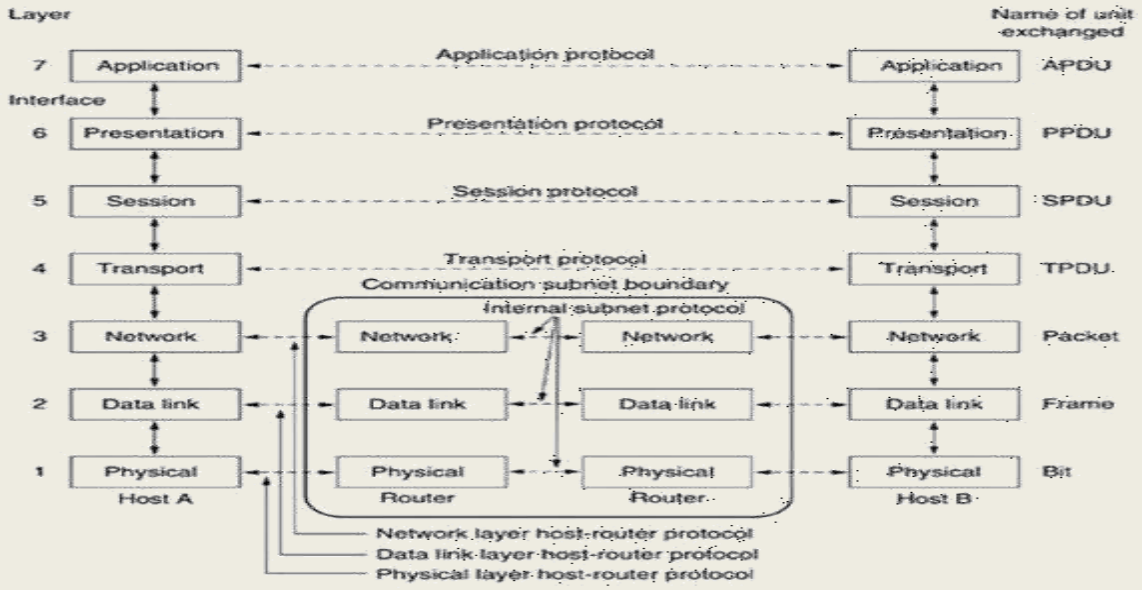
- Lower layer. The carrier transports the letter to the post office.
- Middle layer. The letter is sorted and delivered to the recipient's mailbox.
- Higher layer. The receiver picks up the letter, opens the envelope, and reads it.

The OSI Reference Model:

The OSI model (minus the physical medium) is shown in Fig. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995(Day, 1995). The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

The OSI model has **seven layers**. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.



The Physical Layer:

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

The Data Link Layer:

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmits the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated.

The Network Layer:

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer. More generally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.

When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected. In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The Transport Layer:

The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology. The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent. However, other possible kinds of transport service are the transporting of isolated messages, with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations. The type of service is determined when the connection is established.

The transport layer is a true end-to-end layer, all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages.

The Session Layer:

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

The Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

The Application Layer:

The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

The TCP/IP Reference Model:

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.
2. To survive after partial subnet hardware failures.
3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Host-to-Network Layer
2. Internet Layer

3. Transport Layer
4. Application Layer

Host-to-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

Internet Layer:

This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer. Fig. shows this correspondence.

The Transport Layer:

The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control

to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

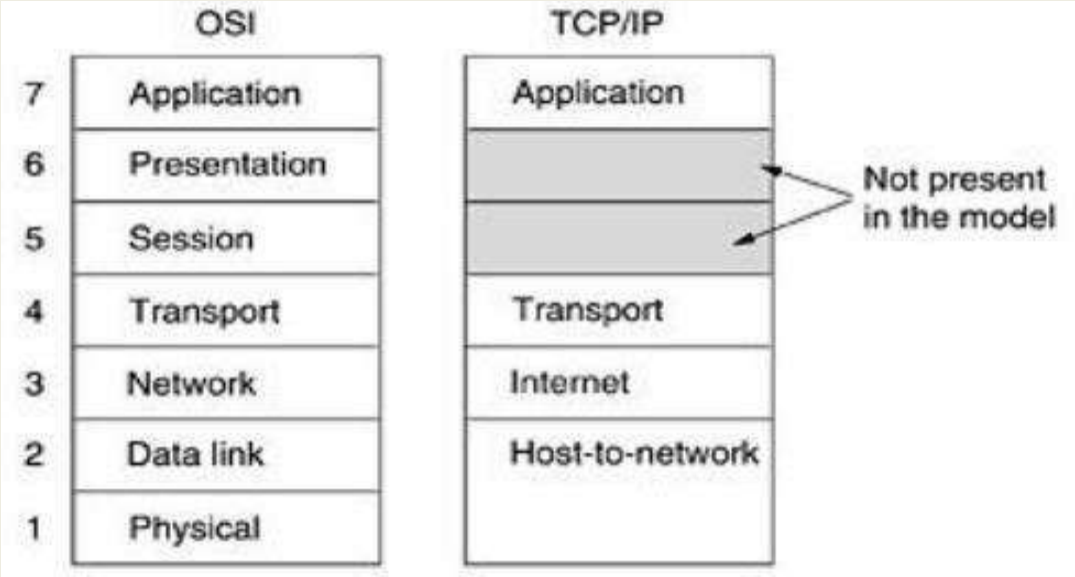


Fig.1: The TCP/IP reference model.

The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig.2. Since the model was developed, IP has been implemented on many other networks.

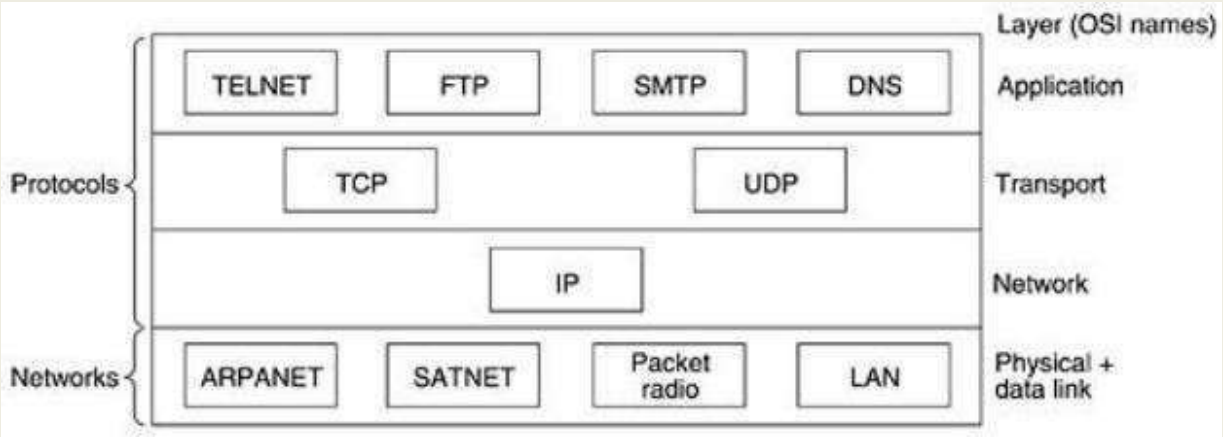


Fig.2: Protocols and networks in the TCP/IP model initially.

The Application Layer:

The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig.6.2. The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, NNTP, the protocol for moving USENET news articles around, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.

Comparison of the OSI and TCP/IP Reference Models:

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols. Also, the functionality of the layers is roughly similar. For example, in both models the layers up through and including the transport layer are there to provide an end-to-end, network-independent transport service to processes wishing to communicate. These layers form the transport provider. Again in both models, the layers above transport are application-oriented users of the transport service. Despite these fundamental similarities, the two models also have many differences Three concepts are central to the OSI model:

1. Services.
2. Interfaces.
3. Protocols.

Probably the biggest contribution of the OSI model is to make the distinction between these three concepts explicit. Each layer performs some services for the layer above it. The service definition tells what the layer does, not how entities above it access it or how the layer works. It defines the layer's semantics.

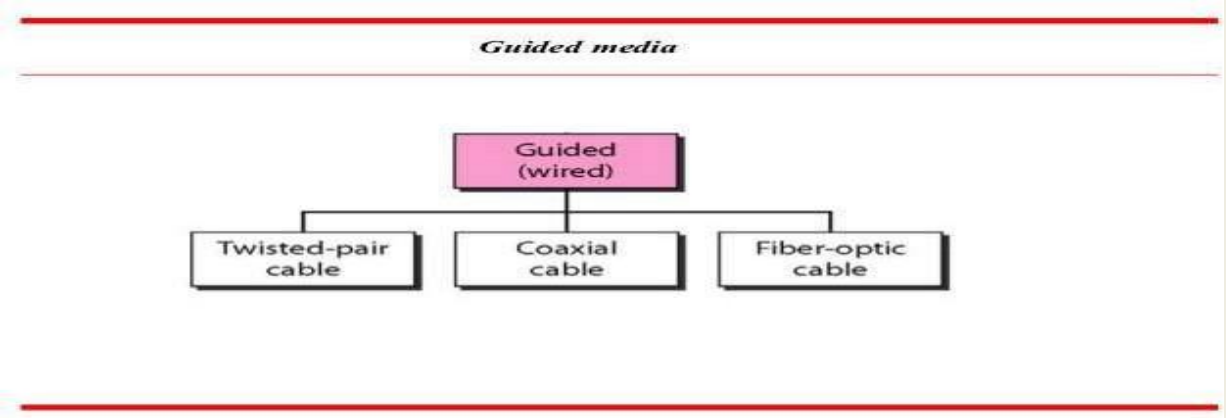
A layer's interface tells the processes above it how to access it. It specifies what the parameters are and what results to expect. It, too, says nothing about how the layer works inside.

Types of Transmission Medias

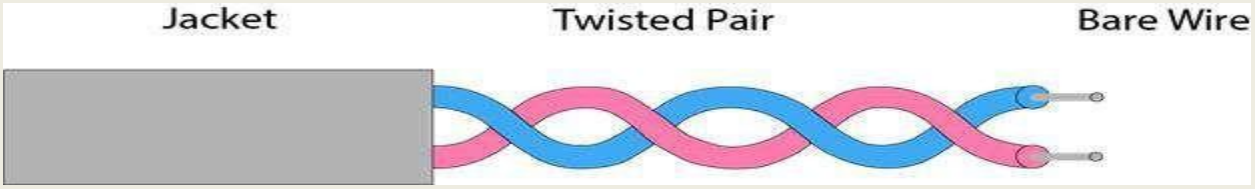
1. **Guided Transmission Media**
2. **Unguided Transmission Media**

Guided Transmission Media :

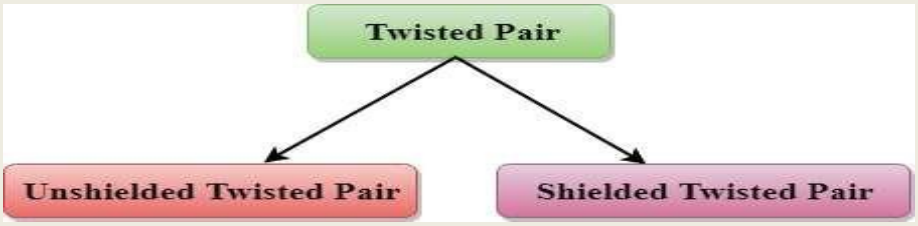
It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.



1. **Twisted Pair Cable :** Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.



Types of Twisted pair:



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

Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks.

Figure 2.1 Unshielded Twisted Pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association / Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Type	Use
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

Table Categories of Unshielded Twisted Pair

Advantages Of Unshielded Twisted Pair:

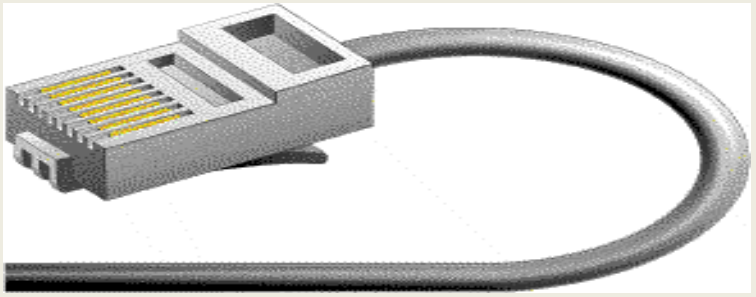
- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Unshielded Twisted Pair Connector

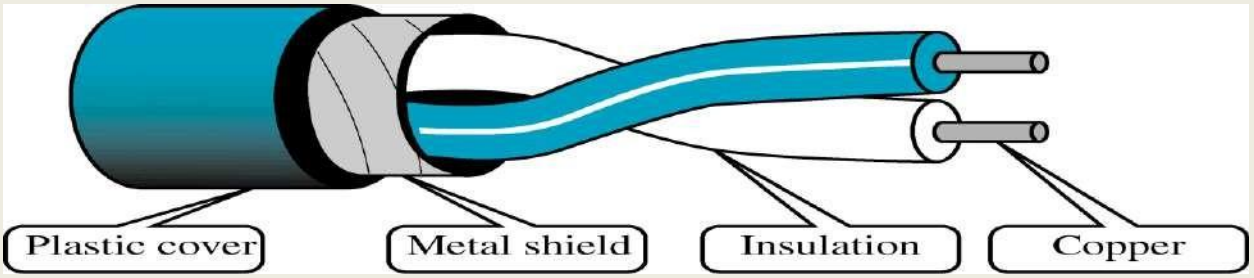
The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2.2). a slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



Shielded Twisted Pair (STP) Cable :

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair |(STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.



Characteristics Of Shielded Twisted Pair:

- **The cost of the shielded twisted pair cable is not very high and not very low.**
- An installation of STP is easy.
- **It has higher capacity as compared to unshielded twisted pair cable.**
- It has a higher attenuation.
- **It is shielded that provides the higher data transmission rate.**

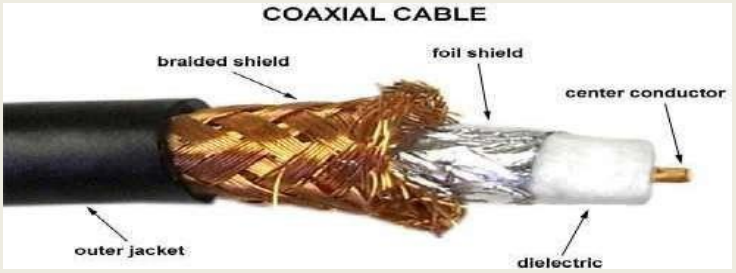
Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- **It has a higher attenuation rate.**

2. *Coaxial Cable*

Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and the braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



Fiber Optic Cable :

- Fiber optic cable is a cable that uses electrical signals for communication.
- Fiber optic is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibers from heat, cold, electromagnetic interference from other types of wiring.

Fiber optics provide faster data transmission than copper wires. Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting. Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over mush longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

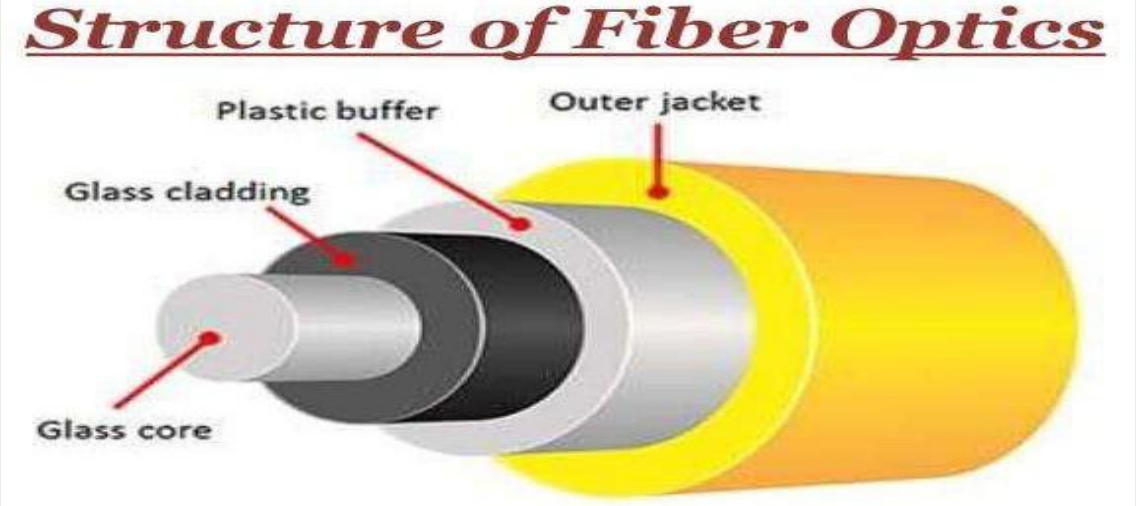


Fig-1. Fiber Optic Cable

Facts about fiber optic cables:

- Outer insulating jacket is made of Teflon or PVC.
- Kevlar fiber helps to strengthen the cable and prevent breakage.
- A plastic coating is used to cushion the fiber center.
- Center (core) is made of glass or plastic fibers.

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

Specification	Cable Type	Maximum length
10BaseT	**Unshielded Twisted Pair**	**100 meters**
10Base2	**Thin Coaxial**	**185 meters**
10Base5	**Thick Coaxial**	**500 meters**
10BaseF	**Fiber Optic**	**2000 meters**
100BaseT	**Unshielded Twisted Pair**	**100 meters**
100BaseTX	**Unshielded Twisted Pair**	**220 meters**

Table : Ethernet Cable Summary

Unguided Transmission Media:

Unguided transmission media is data signals that flow through the air. They are not guided or bound to a channel to follow.

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device receiving them. Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation.

In **ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: *The greater the power, the greater the distance.* Ground waves have carrier frequencies up to 2 MHz. AM radio is an example of ground wave propagation.

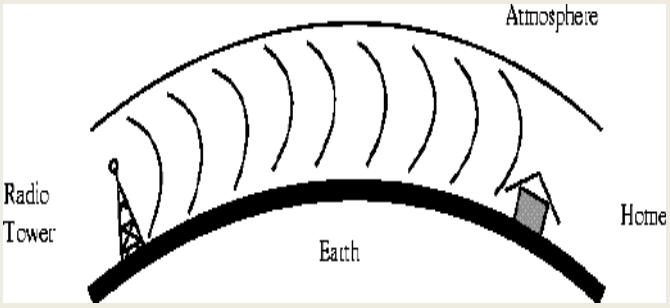


Fig. 2.6 Ground Wave Propagation

In **sky propagation**, higher frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where the particles exist as ions) where they are reflected back to the earth. This type of transmission allows for greater distances with lower output power.

It is sometimes called double hop propagation. It operates in the frequency range of 30 – 85 MHz. Because it depends on the earth's ionosphere, it changes with the weather and time of day. The signal bounces off of the ionosphere and back to the earth. Ham radios operate in this range. Other books called this **Ionospheric propagation**.

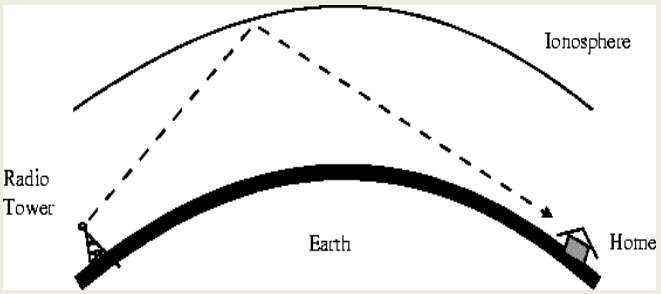
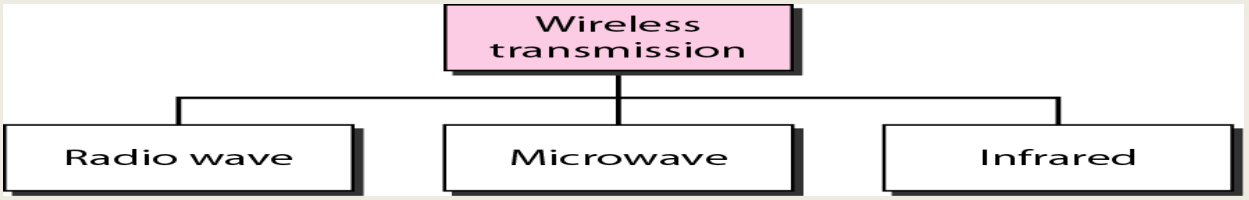


Fig. 2.7 Ionospheric Propagation

In **line-of-sight propagation**, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature the earth. Line-of-sight propagation is tricky because radio transmission cannot be completely focused.

It is sometimes called space waves or tropospheric propagation. It is limited by the curvature of the earth for ground-based stations (100 km, from horizon to horizon). Reflected waves can cause promlems. Axamples are: FM radio, microwave and satellite.

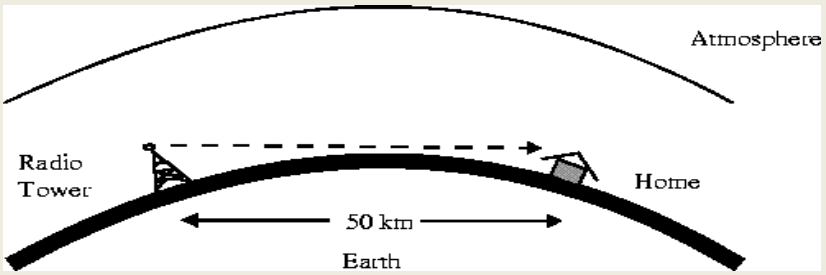
We can divide wireless transmission into **three broad groups**: radio waves, microwaves, and infrared waves.



1. *Radio Waves*

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna.



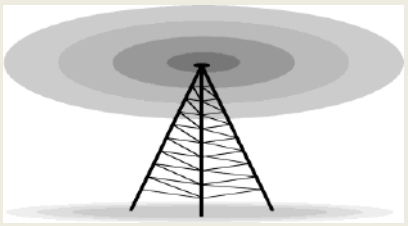


Fig: Omnidirectional antenna

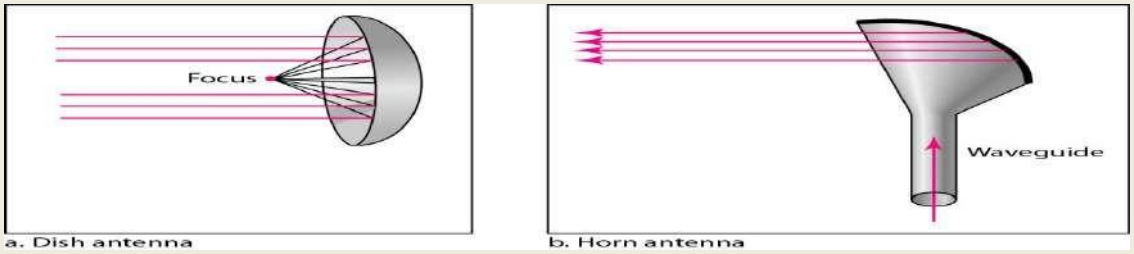
The omnidirectional property has a disadvantage too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

2. *Microwaves*

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. The following describes some characteristics of microwave propagation:



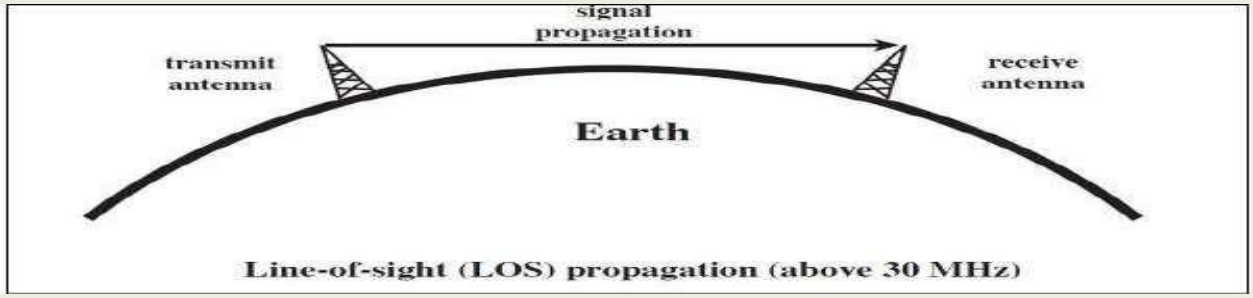
- Microwave propagation is line-of-sight. Since towers with the mounted antennas need to be in direct sight of each other. This also set a limit on the distance between stations depending on the local geography. Towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles does not allow two short towers to communicate by using microwaves. Typically the line of sight due to the Earth's curvature is only 50 km to the horizon. Repeaters are often needed for

long-distance communication.

- Very high frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

3. *Infrared Waves*

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 mm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one



Line-of-sight (LOS) propagation (above 30 MHz)

system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote of our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Satellite

Satellites are transponders (units that receive on one frequency and retransmit on another) that are set in geostationary orbits directly over the equator. These geostationary orbits are 36, 000 km from the Earths's surface. At this point, the gravitational pull of the Earth and the centrifugal force of Earth's rotation are balanced and cancel each other out. Centrifugal force is the rotational force placed on the satellite that wants to fling it out into the space.

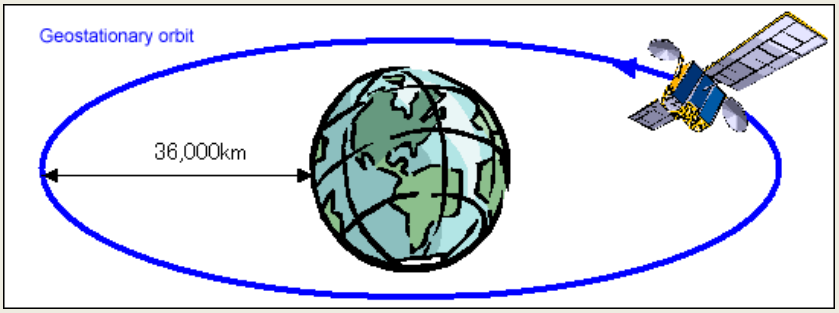


Fig. Satellite Communication

The uplink is the transmitter of data to the satellite. The downlink is the receiver of data. Uplinks and downlinks are also called Earth stations because they are located on the Earth. The footprint is the "shadow" that the satellite can transmit to, the shadow being the area that can receive the satellite's transmitted signal.

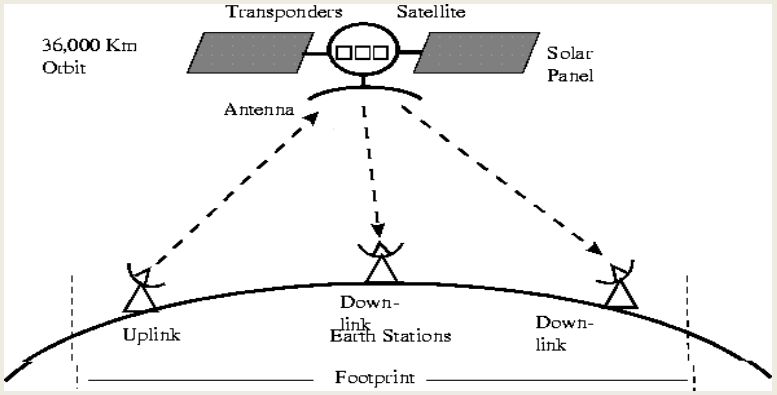
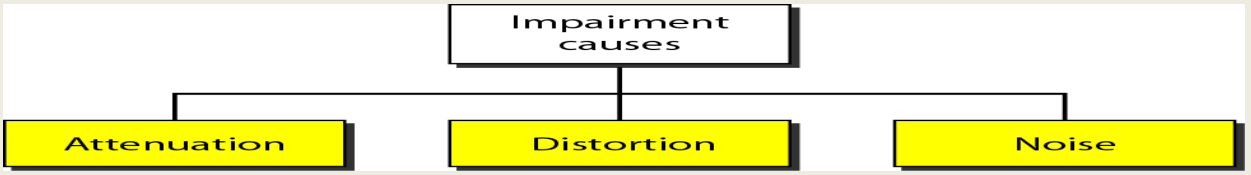


Fig. Uplink and Downlink

Impairments: It means that signals that are transmitted at the beginning of the medium are not the same asthe signals that are received at the end of the medium that is what is sent is not what is received.



Attenuation:

- Means loss of energy -> weaker signal
- When a signal travels through a medium it loses energy overcoming the resistance of the medium
- Amplifiers are used to compensate for this loss of energy by amplifying the signal.

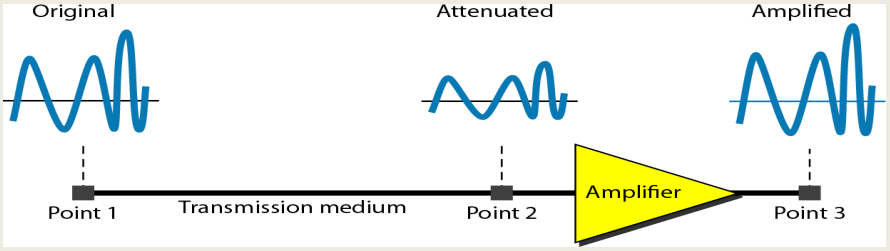


Fig. *Example for Attenuation*

Distortion:

- Means that the signal changes its form or shape
- Distortion occurs in composite signals
- Each frequency component has its own propagation speed traveling through a medium.
- The different components therefore arrive with different delays at the receiver.
- That means that the signals have different phases at the receiver than they did at the source.

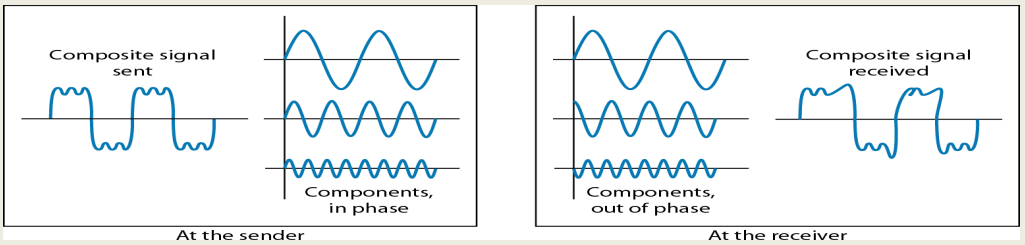
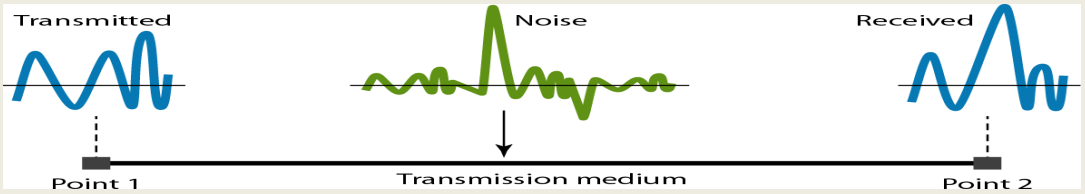


Fig: Distortion

Noise:

- Thermal - random noise of electrons in the wire creates an extra signal
- Crosstalk -Crosstalk is the transmission of signals and noise due to coupling between lines, and is also called interference.
- Impulse - Spikes that result from power lines etc.

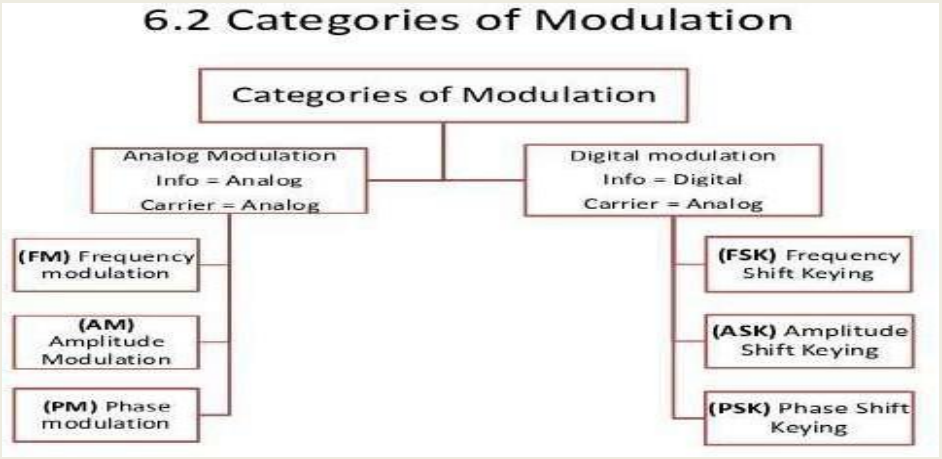


Modulation:

- Modulation is a process of suppressing low frequency information signal on a high frequency carrier signal.

OR

Modulation is a process of modifying the any of the characteristics (amplitude, frequency, phase) of high frequency carrier in accordance with low frequency information signal.



Digital Modulation Techniques :

Digital-to-Analog signals is the next conversion we will discuss in this chapter. These techniques are also called as **Digital Modulation techniques**.

Digital Modulation Digital modulation is defined as the modulation process in which discrete signals are used for modulating carrier waves and it is used for removing noise from the waves.

There are many types of digital modulation techniques and also their combinations, depending upon the need. Of them all, we will discuss the prominent ones.

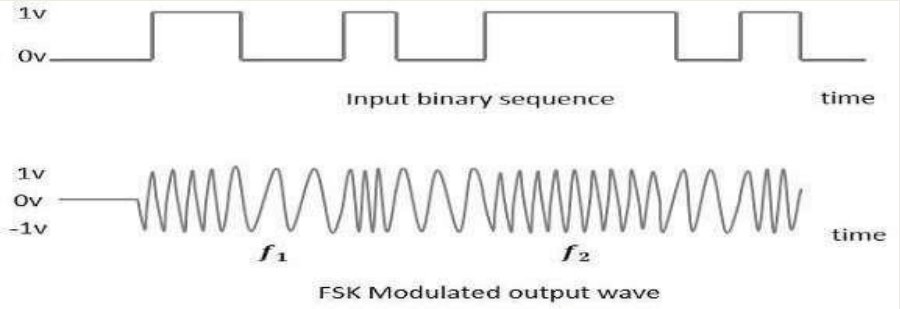
Types of **Digital Modulation**:

There are three types of digital modulation, and they are:

Amplitude shift key (ASK)

Frequency shift key (FSK)

Phase shift key (PSK)



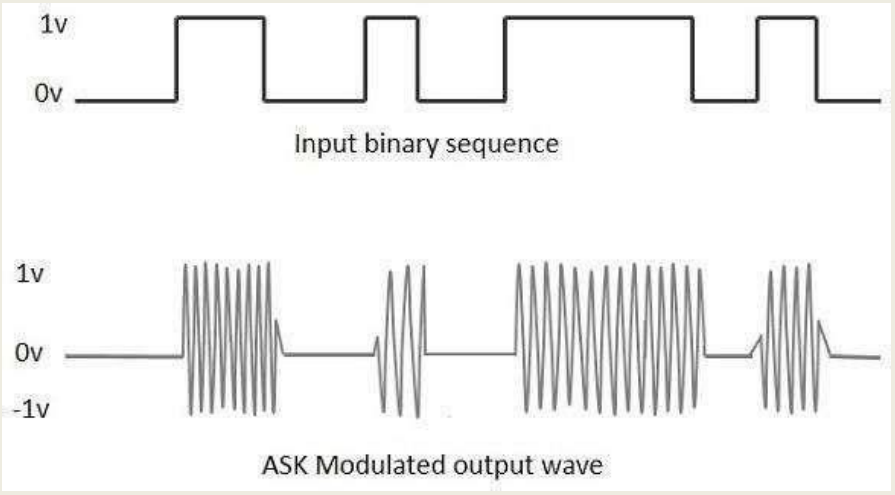
- ASK – Amplitude Shift Keying

The amplitude of the resultant output depends upon the input data whether it should be a zero level or a variation of positive and negative, depending upon the carrier frequency.

Amplitude Shift Keying (ASK) is a type of Amplitude Modulation which represents the binary data in the form of variations in the amplitude of a signal.

- Any modulated signal has a high frequency carrier. The binary signal when ASK modulated, gives a **zero** value for **Low** input while it gives the **carrier output** for **High** input.

- The following figure represents ASK modulated waveform along with its input.



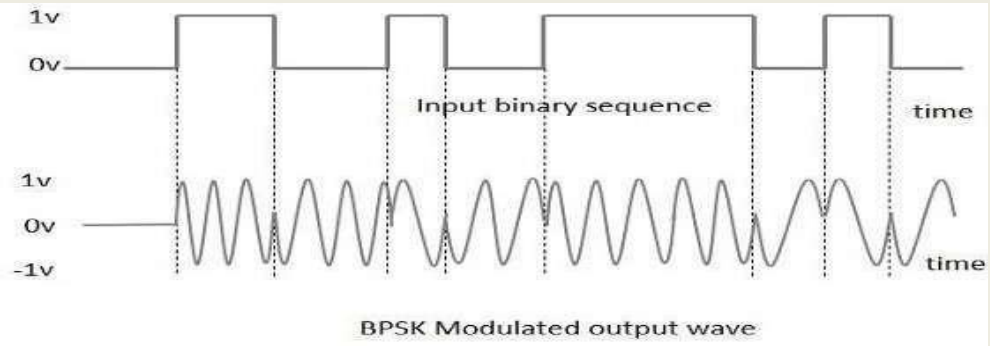
Frequency Shift Keying (FSK) is the digital modulation technique in which the frequency of the carrier signal varies according to the digital signal changes. FSK is a scheme of frequency modulation.

The output of a FSK modulated wave is high in frequency for a binary High input and is low in frequency for a binary Low input. The binary **1s** and **0s** are called Mark and Space frequencies.

The following image is the diagrammatic representation of FSK modulated waveform along with its input.

Phase Shift Keying (PSK) is the digital modulation technique in which the phase of the carrier signal is changed by varying the sine and cosine inputs at a particular time. PSK technique is widely used for wireless LANs, bio-metric, contactless operations, along with RFID and Bluetooth communications.

Following is the diagrammatic representation of BPSK Modulated output wave along with its given input.



Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

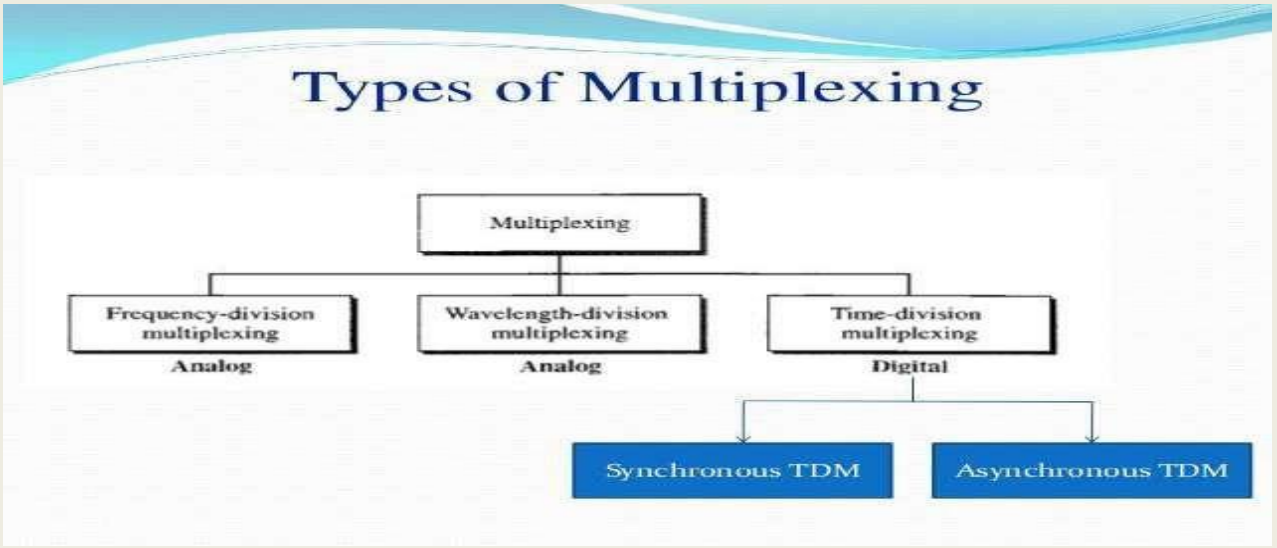
When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

Multiplexing:

- It is the set of techniques that allows the simultaneous transmission of multiple signalsacross a single data link.
- Multiplexing is done using a device called Multiplexer (MUX) that combine *n* input linesto generate one output line i.e. (*many to one).*
- At the receiving end a device called De-multiplexer (DEMUX) is used that separatesignal into its component signals i.e. one input and several outputs *(one to many).*

Advantages of Multiplexing:

- Effective use of the bandwidth of medium
- More than one signals can be sent over single medium or link



1. Frequency Division Multiplexing:

- It is an analog technique.
- Signals of different frequencies are combined into a composite signal and is transmitted on the single link.
- Bandwidth of a link should be greater than the combined bandwidths of the various channels.
- Each signal is having different frequency.
- Channels are separated by the strips of unused bandwidth called *Guard Bands* (to prevent overlapping).

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

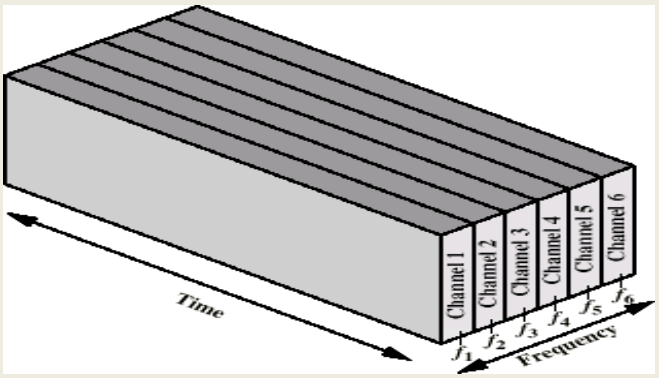
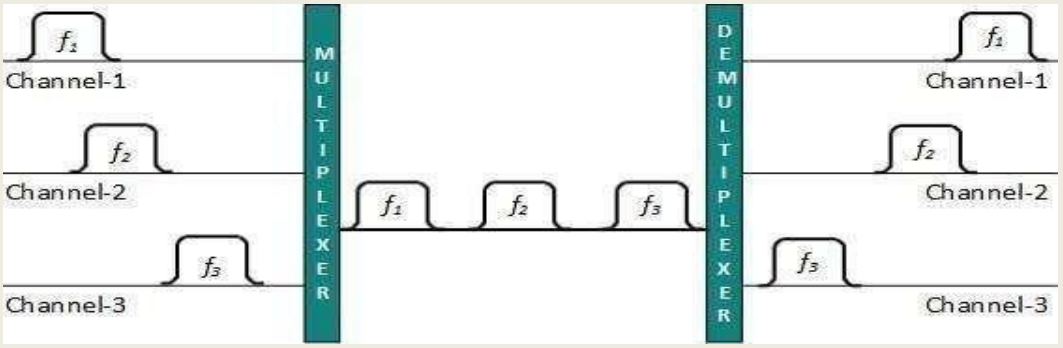
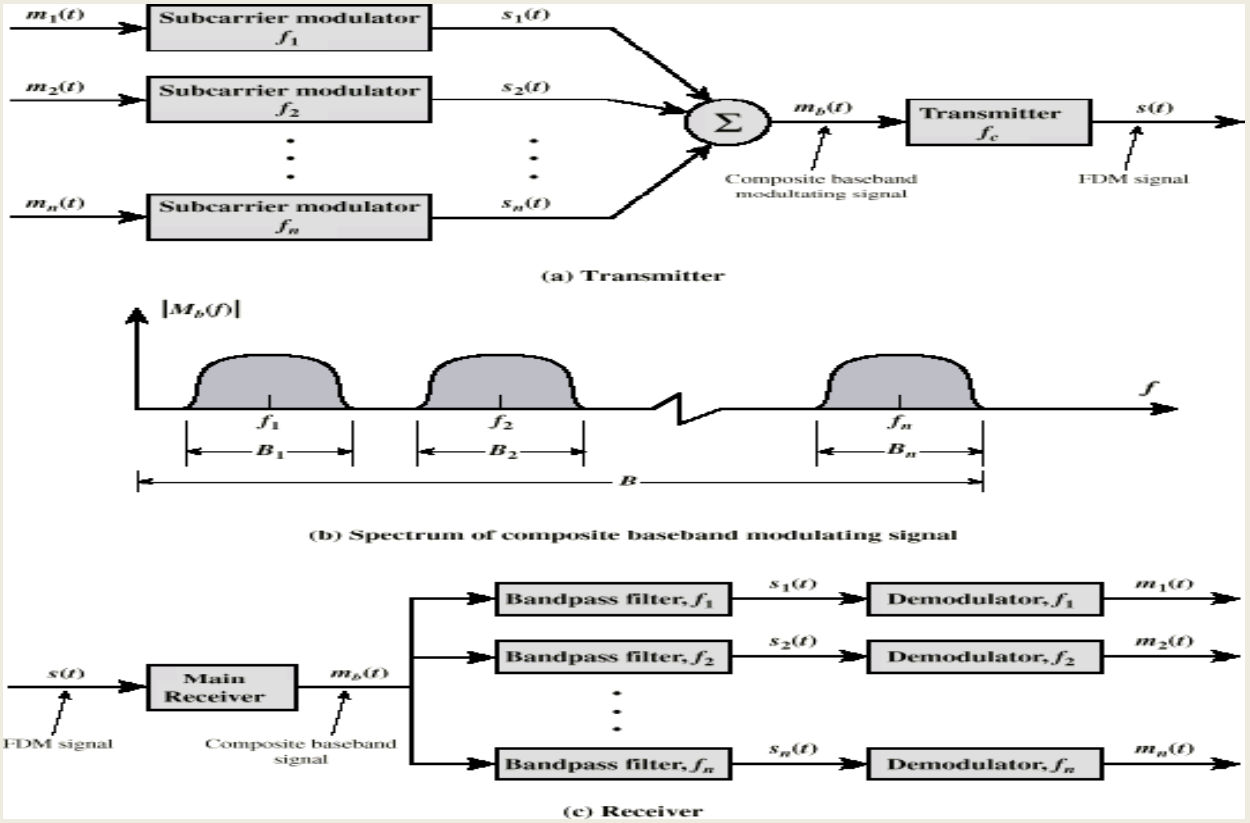


Fig: FDM System





***2.** Wavelength division multiplexing:*

- WDM is an analog multiplexing technique.
- Working is same as FDM.
- In WDM different signals are *optical or light* signals that are transmitted through optical fiber.
- Various light waves from different sources are combined to form a composite light signal that is transmitted across the channel to the receiver.
- At the receiver side, this composite light signal is broken into different light waves by Demultiplexer.
- This Combining and the Splitting of light waves is done by using a PRISM. Prism bends beam of light based on the angle of incidence and the frequency of light wave.

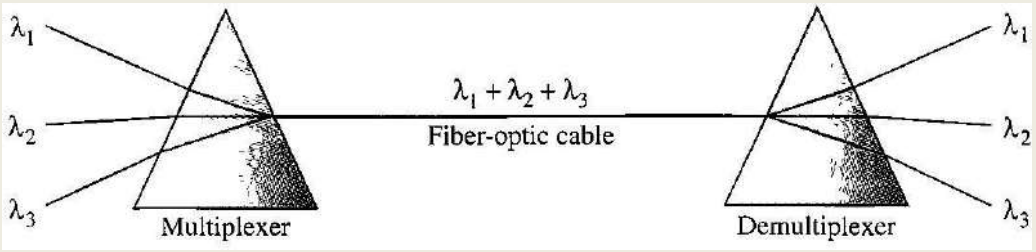


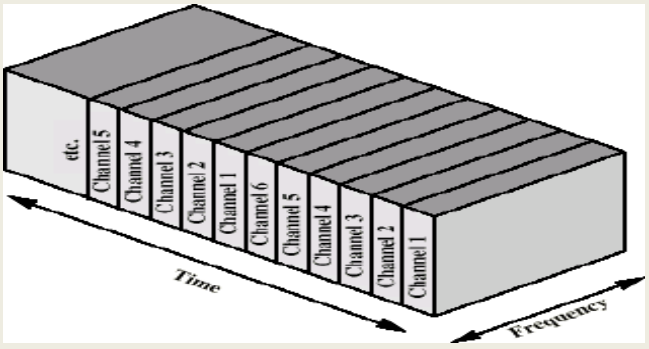
Fig : Wave Division Multiplexing

- Number of sources generating laser beams at different frequencies.
- Multiplexer consolidates sources for transmission over single fiber.
- Optical amplifiers amplify all wavelengths.
  -Typically tens of km apart

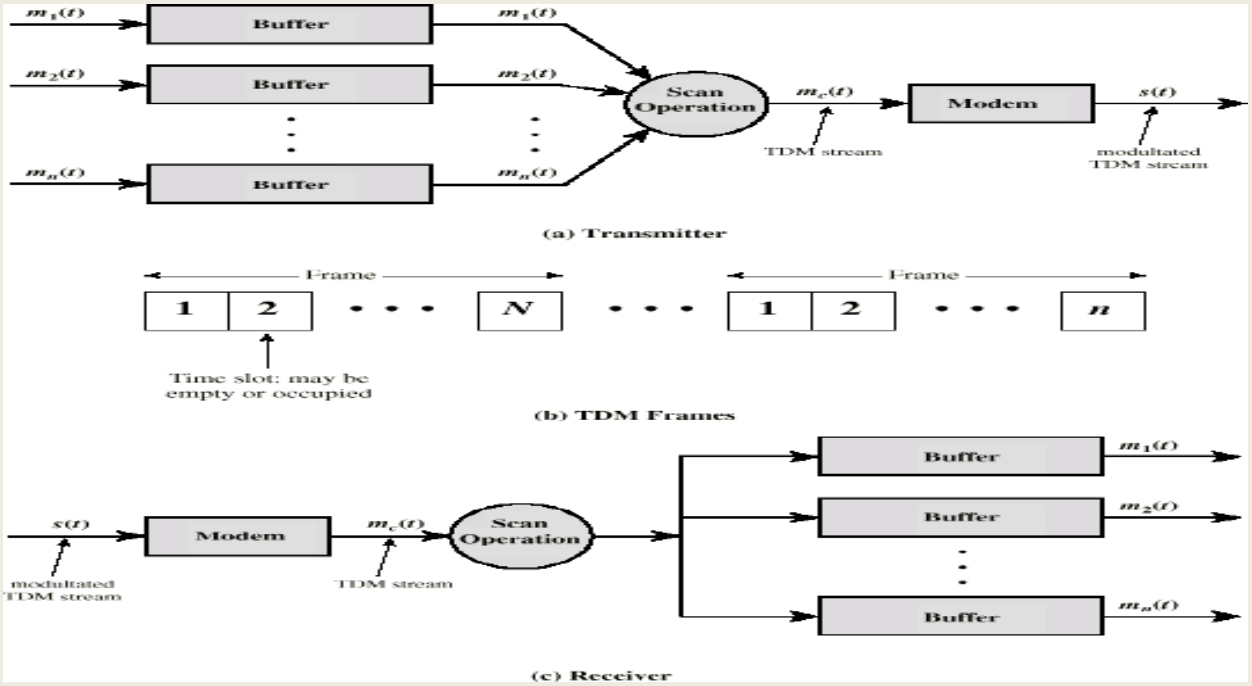
- Demux separates channels at the destination
- Mostly 1550nm wavelength range
- Same general architecture as other FDM
- Was 200MHz per channel
- Now 50GHz

Time Division Multiplexing:

- It is the digital multiplexing technique.
- Channel/Link is not divided on the basis of *frequency* but on the *basis of time.*
- Total time available in the channel is divided between several users.
- Each user is allotted a particular time interval called *time slot* or *slice.*
- In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending of receiving devices



TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.



Types of TDM :

- **Synchronous TDM**
- **Asynchronous TDM**

Synchronous TDM :

- Each device is given same Time Slot to transmit the data over the link, whether thedevice has any data to transmit or not.
- Each device places its data onto the link when its *Time Slot* arrives, each device isgiven the possession of line turn by turn.
- If any device does not have data to send then its time slot remains empty.
- Time slots are organized into *Frames* and each frame consists of one or more timeslots.
- If there are *n* sending devices there will be *n* slots in frame.

Asynchronous TDM (or) Statistical TDM:
The channel capacity cannot be fully utilized. Some of the slots go empty in certain frames

Statistical TDM:

- In Synchronous TDM many slots are wasted
- Statistical TDM allocates time slots dynamically based on demand
- Multiplexer scans input lines and collects data until frame full
- Data rate on line lower than aggregate rates of input lines

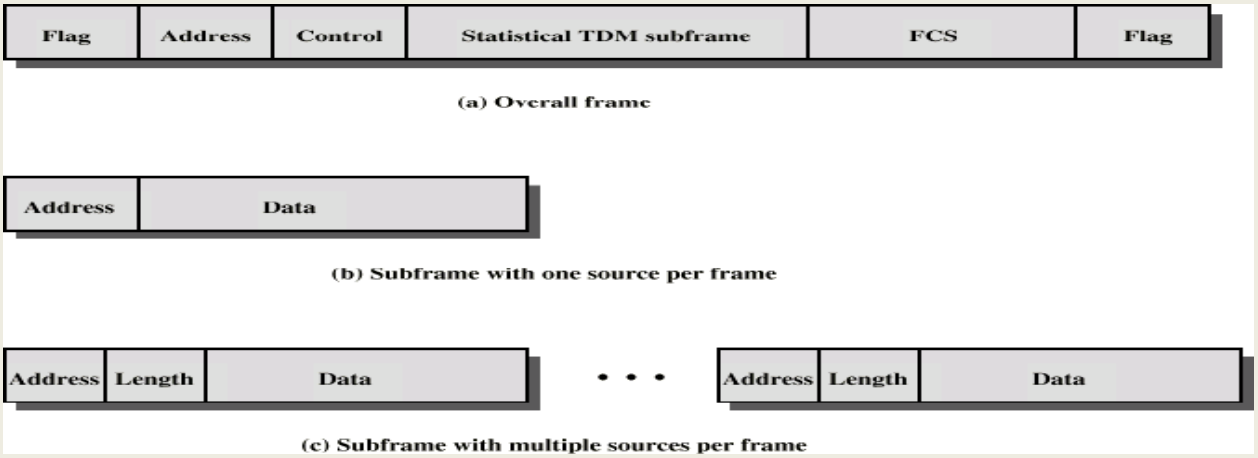
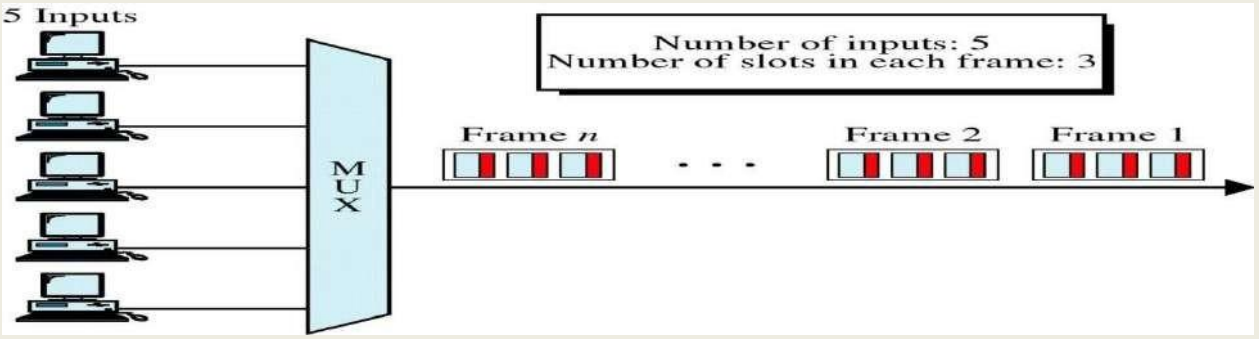


Fig: Statistical TDM Frame Formats



Asynchronous TDM

- Also known as Statistical Time Division *multiplexing*
- In Asynchronous TDM time slots are not *Fixed* i.e. slots are Flexible.
- Total speed of the input lines can be greater than the capacity of the path.
- In ASTDM we have *n* input lines and *m* slots i.e. *m* less than *n* (*m*<*n*).
- Slots are not predefined rather slots are allocated to any of the device that has data to send.

TRANSPORT PROTOCOLS - UDP

The Internet has two main protocols in the transport layer, **a connectionless protocol** and a **connection- oriented** one. The protocols complement each other. The connectionless protocol is **UDP.** It does almost nothing beyond sending packets between applications, letting applications build their own protocols on top as needed.

The connection-oriented protocol is **TCP.** It does almost everything. It makes connections and adds reliability with retransmissions, along with flow control and congestion control, all on behalf of the

applications that use it. Since UDP is a transport layer protocol that typically runs in the operating system andprotocols that use UDP typically run in user s pace, these uses might be considered applications.

INTROUCTION TO UDP

- The Internet protocol suite supports a connectionless transport protocol called UDP

(User Datagram Protocol). UDP provides a way for applications to send encapsulated IP datagrams without having to establish a connection.

- UDP transmits segments consisting of an 8-byte header followed by the pay-load. The two ports serve to identify the end-points within the source and destination machines.
- When a UDP packet arrives, its payload is handed to the process attached to the destination port. This attachment occurs when the BIND primitive. Without the port fields, the transport layer would not know what to do with each incoming packet. With them, it delivers the embedded segment to the correct application.

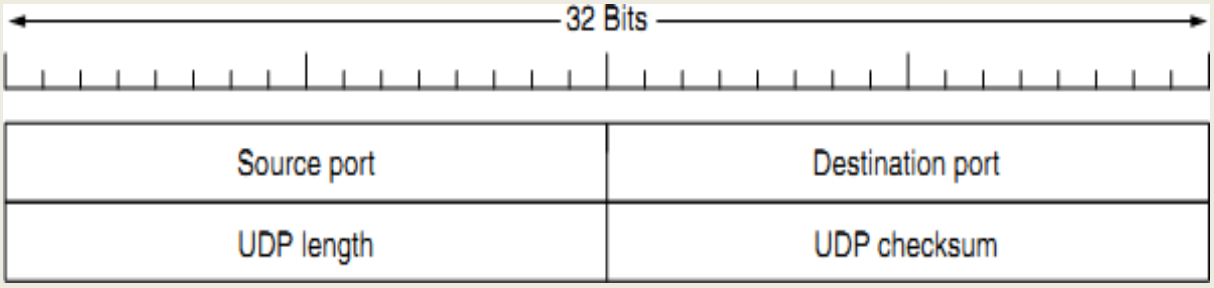


Fig 4.9: The UDP header

Source port, destination port: Identifies the end points within the source and destination machines.

UDP length: Includes 8-byte header and the data

UDP checksum: Includes the UDP header, the UDP data padded out to an even number of bytes if need be. Itis an optional field

TCP (TRANSMISSION CONTROL PROTOCOL)

It was specifically designed to provide a reliable end-to end byte stream over an unreliable network. It was designed to adapt dynamically to properties of the inter network and to be robust in the face of many kinds of failures.

Each machine supporting TCP has a TCP transport entity, which accepts user data streams from local processes, breaks them up into pieces not exceeding 64kbytes and sends each piece as a separate IP datagram. When these datagrams arrive at a machine, they are given to TCP entity, which reconstructs the original byte streams. It is up to TCP to time out and retransmits them as needed, also to reassemble datagrams into messagesin proper sequence.

The different issues to be considered are:

1. The TCP Service Model
2. The TCP Protocol
3. The TCP Segment Header
4. The Connection Management
5. TCP Transmission Policy
6. TCP Congestion Control
7. TCP Timer Management.

Choose the best answer:

1. The fundamental basis of data communications is _____.

(a) light (b) electricity

(c) voltage (d) signal propagation

Ans: (d) signal propagation

2. _____ signals are continuous in nature.

(a) Analog (b) Digital

(c) Mixed (d) None of the above

Ans: (a) Analog

3. _____ signals are on-off in nature.

(a) Analog (b) Digital

(c) Mixed (d) None of the above

Ans: (b) Digital

4. The strength of a signal at any point of time is called as its _____.

(a) amplitude (b) frequency

(c) period (d) phase

Ans: (a) amplitude

5. The time required for the completion of one signal cycle is its _____.

(a) amplitude (b) frequency

(c) period (d) phase

Ans: (d) period

6. The number of cycles completed by a signal in one second is its _____.

(a) amplitude (b) frequency

(c) period (d) phase

Ans: (b) frequency

7. The unit used to measure frequency is _____.

(a) hertz (b) volts

(c) ampere (d) seconds

Ans: (a) hertz

8. An amplifier amplifies _____.

(a) only the original signal (b) the original signal and noise

(c) only the noise (d) the original signal but not noise

Ans: (c) only the noise

9. A _____ is used to send digital data over analog telephone lines.

(a) multiplexer (b) repeater

(c) amplifier (d) modem

Ans: (a) multiplexer

10. In _____, we transmit all the 8 bits at a time.

(a) serial transmission (b) parallel transmission

(c) synchronous communication (d) mixed transmission

Ans: (b) parallel transmission

11. In _____, the whole block of data bits is transferred at once, instead of a character at a time.

(a) serial transmission (b) synchronous transmission

(c) asynchronous transmission (d) isochronous transmission

Ans: (b) synchronous transmission

12. _____ is used when large amount of data is to be sent from one place to the other.

(a) Parallel transmission (b) Synchronous transmission

(c) Asynchronous transmission (d) Isochronous transmission

Ans: (d) Isochronous transmission

13. In _____, the idle period between the two characters cannot be random.

(a) parallel transmission (b) synchronous transmission

(c) asynchronous transmission (d) isochronous transmission

Ans: (b) synchronous transmission

14. In half-duplex communication, _____.

(a) only one party can transmit data

(b) both parties can transmit data, but not at the same time

(c) both parties can transmit data at the same time

(d) no party can transmit

Ans: (a) only one party can transmit data

15. Multiplexing _____.

(a) divides one line into multiple channels

(b) combines many channels into one line

(c) is same as modulating

(d) is same as demodulating

Ans: (a) divides one line into multiple channels

16. _____ is caused because the signals at different frequencies travel at different speeds along the medium.

(a) Noise (b) Delay distortion

(c) Attenuation (d) Retransmission

Ans: (b) Delay distortion

17. Some electromagnetic energy can get inserted somewhere during transmission, which is normally called _____.

(a) noise (b) delay distortion

(c) attenuation (d) retransmission

Ans: (c) attenuation

18. In _____, the sender sends one frame and waits for an acknowledgement from the receiver before sending the next frame.

(a) stop-and-wait (b) Go-back-n

(c) sliding window (d) CRC

Ans: (b) Go-back-n

19. The two wires inside a UTP are twisted around each other to reduce _____.

(a) noise (b) crosstalk

(c) error (d) voltage

Ans: (b) crosstalk

20. _____ is generally used for cable television transmissions.

(a) Optical fiber (b) Coaxial cable

(c) UTP (d) STP

Ans: (b) Coaxial cable

21. Optical fibers use _____ for data transmission.

(a) voltage (b) current

(c) light (d) sound

Ans: (c) light

22. Optical fibers use _____ to guide the light through the optical fiber.

(a) refraction (b) critical angle

(c) reflection (d) waves

Ans: (a) refraction

23. Out of all the guided media, _____ has the highest data transmission rates.

(a) optical fiber (b) coaxial cable

(c) UTP (d) STP

Ans: (a) optical fiber

24. Geosynchronous satellites move at _____ RPM as that of the earth.

(a) same (b) half

(c) double (d) thrice

Ans: (a) same

25. _____ transmits each signal on a different frequency.

(a) TDMA (b) CDMA

(c) TDM (d) FDMA

Ans: (d) FDMA

26. _____ allows any transmitter to transmit in any frequency, and at any time.

(a) TDMA (b) CDMA

(c) FDM (d) FDMA

Ans: (b) CDMA

27. A _____ controls various cell offices in a cellular system.

(a) MTSO (b) TCO

(c) AMPS (d) satellite

Ans: (a) MTSO

28. In star topology, the central hub is called _____.

(a) active hub (b) passive hub

(c) inactive hub (d) live hub

Ans: (a) active hub

29. In case of _____, a direct physical connection path is established between two computers.

(a) circuit switching (b) packet switching

(c) message switching (d) datagram approach

Ans: (a) circuit switching

30. _____ is more suitable for computer communications.

(a) circuit switching (b) packet switching

(c) message switching (d) None of the above

Ans: (b) packet switching

31. The _____ layer is responsible for node-to-node delivery of packets.

(a) physical (b) transport

(c) data link (d) application

Ans: (c) data link

32. The _____ layer is responsible for routing packets within or across networks.

(a) physical (b) network

(c) data link (d) application

Ans: (b) network

33. The _____ layer ensures the correct delivery of a complete message.

(a) data link (b) transport

(c) session (d) presentation

Ans: (b) transport

34. Encryption is handled by the _____ layer.

(a) data link (b) transport

(c) session (d) presentation

Ans: (d) presentation

35. The WWW is a _____ layer protocol.

(a) physical (b) application

(c) data link (d) session

Ans: (b) application

36. Data compression happens in the _____ layer.

(a) physical (b) data link

(c) network (d) presentation

Ans: (d) presentation

37. A _____ spans the largest distance among the category of computer networks.

(a) LAN (b) MAN

(c) WAN (d) Internet

Ans: (d) Internet

38. In _____, the transmission media is shared between all the computers on a network.

(a) LAN (b) MAN

(c) WAN (d) X.25

Ans: (a) LAN

39. A transceiver connects a _____ to _____.

(a) computer, computer (b) network, network

(c) computer, Ethernet (d) Ethernet, Ethernet

Ans: (c) computer, Ethernet

40. The _____ performs all network-related work on a computer connected to a network.

(a) transceiver (b) CPU

(c) hard disk (d) NIC

Ans: (d) NIC

41. _____ helps Ethernet recover from simultaneous transmissions causing errors.

(a) CSMA/CD (b) CSMA

(c) CD (d) Collision

Ans: (a) CSMA/CD

42. An Ethernet address can be _____.

(a) unique (b) duplicated

(c) optional (d) never duplicated

Ans: (d) never duplicated

43. The basic hardware device in a WAN is called a _____.

(a) circuit (b) circuit switch

(c) packet switch (d) ring

Ans: (c) packet switch

44. In a _____, the transmission medium is not shared.

(a) LAN (b) MAN

(c) WAN (d) None of the above

Ans: (c) WAN

45. Each switch on a WAN maintains a _____ for forwarding packets.

(a) array (b) hash table

(c) route (d) next-hop table

Ans: (d) next-hop table

46. In internetworking, the two or more networks that connect with each other _____ incompatible with one another.

(a) have to be (b) may be

(c) must not be (d) None of the above

Ans: (b) may be

47. Usually, a _____ is used for internetworking purposes.

(a) host (b) wire

(c) router (d) joiner

Ans: (c) router

48. A router must have at least _____ NICs.

(a) 2 (b) 3

(c) 4 (d) 5

Ans: (a) 2

49. There are _____ incompatibility issues when forming an internet out of networks.

(a) both hardware and software (b) only hardware

(c) only software (d) software but not hardware

Ans: (a) both hardware and software

50. A bridge is a _____ device.

(a) networking (b) connecting

(c) internetworking (d) routing

Ans: (c) internetworking

51. A _____ is the simplest of all networking/internetworking devices.

(a) repeater (b) bridge

(c) router (d) gateway

Ans: (a) repeater

52. Generally, a _____ is used to divide a network into segments.

(a) repeater (b) bridge

(c) router (d) gateway

Ans: (b) bridge

53. A _____ builds its mapping table as and when it gets more information about the network.

(a) simple bridge (b) repeater

(c) adaptive bridge (d) regenerator

Ans: (c) adaptive bridge

54. A logical address is _____ the physical address.

(a) the same as (b) tightly coupled with

(c) sometimes related to (d) completely unrelated to

Ans: (d) completely unrelated to

55. A _____ can understand multiple networking protocols.

(a) repeater (b) bridge

(c) router (d) gateway

Ans: (d) gateway

56. _____ first introduced the idea of store and forward packet switching.

(a) Baran (b) Barak

(c) Daran (d) Daran Barak

Ans: (a) Baran

57. A _____ waits for requests from a _____.

(a) Web browser, Web server (b) client, server

(c) Web server, Web browser (d) None of the above

Ans: (c) Web server, Web browser

58. A home user dials into _____.

(a) ISP (b) NAP

(c) backbone (d) router

Ans: (a) ISP

59. The _____ for all computers on the same physical network is the same.

(a) host id (b) physical address

(c) IP address (d) network id

Ans: (d) network id

60. Currently, the IP address has a size of _____ bits.

(a) 128 (b) 64

(c) 32 (d) 16

Ans: (c) 32

61. Transport layer protocols are useful for ensuring _____ delivery.

(a) host to host (b) host to router

(c) network to network (d) end to end

Ans: (d) end to end

62. _____ is a reliable delivery mechanism.

(a) IP (b) TCP

(c) UDP (d) ARP

Ans: (b) TCP

63. When a single packet reaches the destination twice, it should be handled by _____.

(a) sequence control (b) error control

(c) loss control (d) duplication control

Ans: (d) duplication control

64. When packet 2 reaches packet 1 at the destination, it should be handled by _____.

(a) sequence control (b) error control

(c) loss control (d) duplication control

Ans: (a) sequence control

65. TCP uses the mechanism of _____.

(a) physical connections (b) virtual connections

(c) circuit switching (d) virtual circuits

Ans: (b) virtual connections

66. The mechanism of _____ is used if the acknowledgement is not received in a specified time interval.

(a) packet deletion (b) packet retransmission

(c) packet holding (d) packet caching

Ans: (b) packet retransmission

67. UDP is iterative because _____.

(a) it processes multiple requests at the same time

(b) it performs round-robin checks

(c) it processes only one request at a time

(d) it performs parallel processing

Ans: (c) it processes only one request at a time

68. TCP is concurrent because _____.

(a) it processes multiple requests at the same time

(b) it performs round-robin checks

(c) it processes only one request at a time

(d) it performs parallel processing

Ans: (a) it processes multiple requests at the same time

69. _____ is a storage area to store emails.

(a) Database (b) File

(c) Mailbox (d) Server

Ans: (c) Mailbox

70. The sender of an email needs to have email _____ software.

(a) server (b) mailbox

(c) sharing (d) client

Ans: (d) client

71. The _____ symbol is used to connect the user name and the domain name portions of an email id.

(a) & (b) @

(c) * (d) $

Ans: (b) @

72. _____ protocol is used to retrieve emails from a remote server.

(a) POP (b) IP

(c) POP (d) SMTP

Ans: (a) POP

73. _____ protocol is used for transferring mails over the Internet.

(a) POP (b) IP

(c) POP (d) SMTP

Ans: (d) SMTP

74. In an email id, the prefix refers to the _____.

(a) domain name (b) user name

(c) IP address (d) None of the above

Ans: (b) user name

75. _____ allows non-text data to be sent along with an email message.

(a) PGP (b) MIME

(c) PEM (d) MTA

Ans: (b) MIME