UNIT-I

Overview of Computer Communications and Networking: Introduction to Computer Communications and Networking, Introduction to Computer Network, Types of Computer Networks, Network Addressing, Routing, Reliability, Interoperability and Security, Network Standards, the Telephone System and Data Communications.

INTRODUCTION

- This chapter provides an introduction to Computer networks and covers fundamental topics like data, information to the definition of communication and computer networks.
- The main objective of data communication and networking is to enable seamless exchange of data between any two points in the world.
- This exchange of data takes place over a computer network.

DATA & INFORMATION

- **Data** refers to the raw facts that are collected while **information** refers to processed data that enables us to take decisions.
- Ex. When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed.
- The word ***data*** refers to any information which is presented in a form that is agreed and accepted upon by its creators and users.

DATA COMMUNICATION

- Data Communication is a process of exchanging data or information
- In case of computer networks this exchange is done between two devices over a transmission medium.
- This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol.
- The following sections describes the fundamental characteristics that are important for the effective working of data communication process

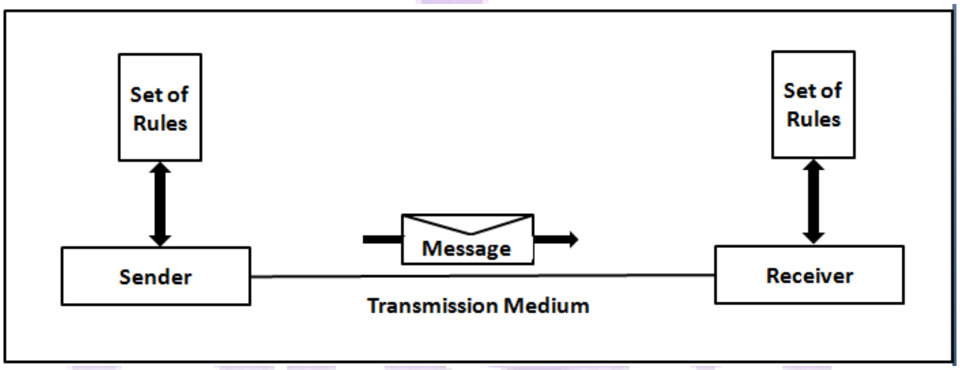
and is followed by the components that makeup a data communications system.

Characteristics of Data Communication

The effectiveness of any data communications system depends upon the following four fundamental characteristics:

1. **Delivery**: The data should be delivered to the correct destination and correct user.
2. **Accuracy**: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
3. **Timeliness**: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4. **Jitter**: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

Components of Data Communication



A Data Communication system has five components as shown in the diagram below:

Fig. Components of a Data Communication System

1. Message
Message is the information to be communicated by the sender to the receiver.

2. Sender
The sender is any device that is capable of sending the data(message).

3. Receiver
The receiver is a device that the sender wants to communicate the

data(message).

4. Transmission Medium

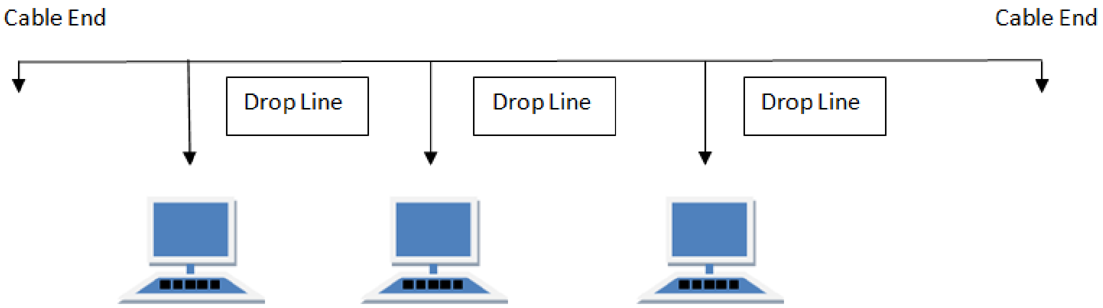
It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.

Types of Network Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

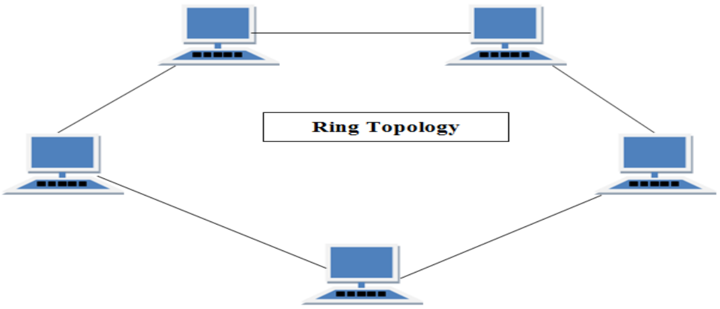
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

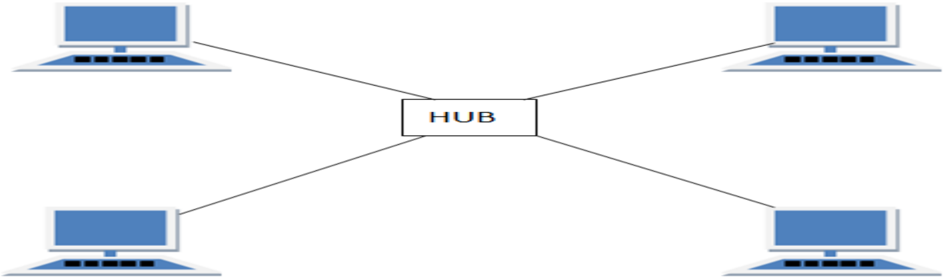
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.There are two techniques to transmit data over the Mesh topology, they are :

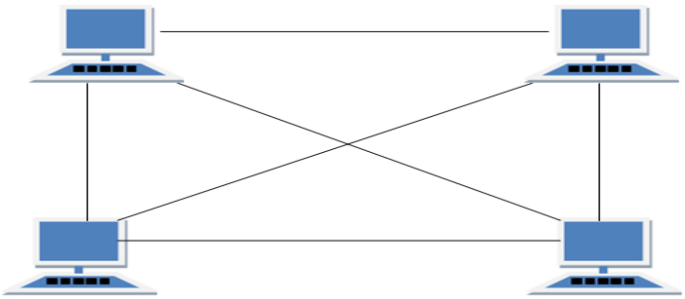
1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.

2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

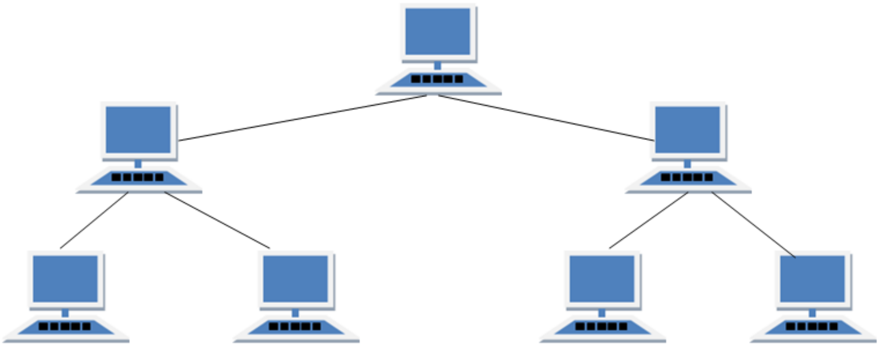
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

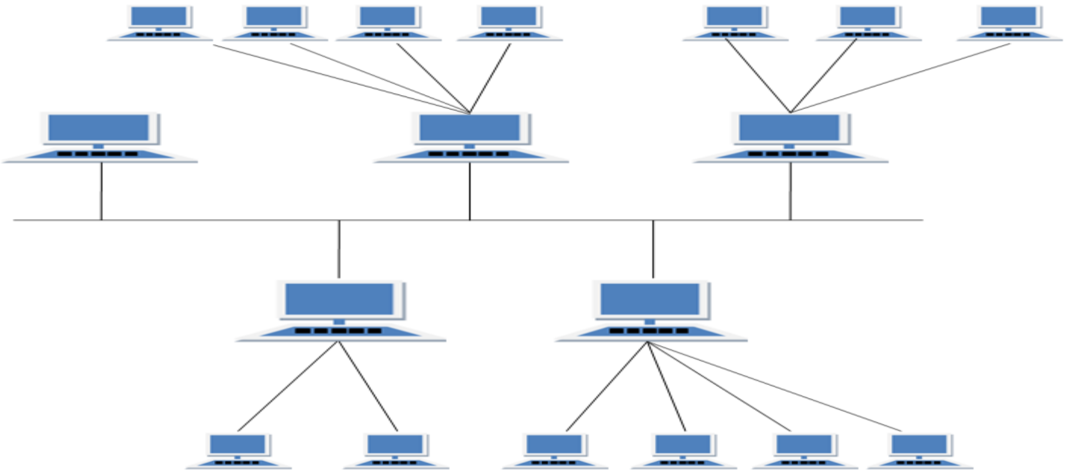
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

TYPES OF COMPUTER NETWORKS

Here are 11 types of networks:

1. Local area network (LAN)

A local area network, or LAN, is the most common network type. It allows users to connect within a short distance in a common area. Once they connect, users have access to the same resources. For example, you might use a LAN when you connect your laptop to the internet at your home and print a document from a printer on the same network.

2. Personal area network (PAN)

A personal area network, or PAN, is a small-scale network that revolves around one person or device. A PAN connects just a few devices in a small localized area. Rather than including many devices, PANs usually operate from one or two main devices. For example, if you use the Bluetooth functionality on your smartphone to share a photo with a nearby device, you're using a PAN.

3. Wireless local area network (WLAN)

A wireless local area network, or WLAN, operates similarly to a LAN because it transmits data within a small area. It's rarely necessary to have a wired connection for devices that use a WLAN. While typically less secure and slightly weaker than other networks, a WLAN provides users with the flexibility to use their devices in various locations. For example, a user might connect a baby monitor to a WLAN to ensure the device remains operational wherever their child sleeps.

4. Campus area network (CAN)

A campus area network, or CAN, is a network used in educational environments such as universities or school districts. While each department in a school might use its own LAN, all the school's LANs could connect through a CAN. Campus area networks combine several independent networks into one cohesive unit. For example, the English and engineering departments at a university might connect through a CAN to communicate with each other directly.

5. Metropolitan area network (MAN)

A metropolitan area network, or a MAN, is a medium-sized network that's larger than a CAN. While a MAN is a costly network, it provides efficient connectivity between devices across a wide geographical range. For example, a city government might operate with a MAN if it has offices across the entire metropolitan area.

6. Wide area network (WAN)

A wide area network, or a WAN, is an extensive network that's not confined to geographical space. Corporations and international companies may use WANs to provide a common network with far-reaching connectivity. For example, remote workers who use the internet to access information from their company make use of a WAN.

7. Storage area network (SAN)

A storage area network, or a SAN, is a network that teams use to store mass amounts of sensitive data. It provides a way to centralize data on a non-localized network that differs from the main operating one. One example of a SAN is if your team stores customer information on a separate network to maintain the high speeds of your main network.

8. Passive optical local area network (POLAN)

A passive optical local area network, or a POLAN, is a low-cost network that can link various locations to one central network. POLANs have the power to connect multiple entities to one hub of information. For example, if a school district's headquarters needs to connect with each school in its district, it may implement a POLAN.

9. Enterprise private network (EPN)

An enterprise private network, or an EPN, is an exclusive network that businesses build and operate to share company resources at high speeds. EPNs are typically unique to a specific company, which ensures the connection is secure. For example, a high-security technology company might use an EPN to reduce the risk of data breaches.

10. Virtual private network (VPN)

A virtual private network, or VPN, is a private network that's available through the internet. This type of network functions similarly to an EPN because it provides a secure, private connection. VPNs typically don't require the same infrastructure as EPNs. Both the general public and companies can use VPNs to ensure privacy and security.

11. System-area network (SAN)

A system area network, or a SAN, is a broad local network that provides connections in clusters. The various devices connected to a SAN operate as a single system. SANs are newly developing networks that operate at high speeds.

NETWORK ADDRESSING, ROUTING, RELIABILITY, INTEROPERABILITY AND SECURITY:

ADDRESSING

Network Addressing is one of the major responsibilities of the network layer.

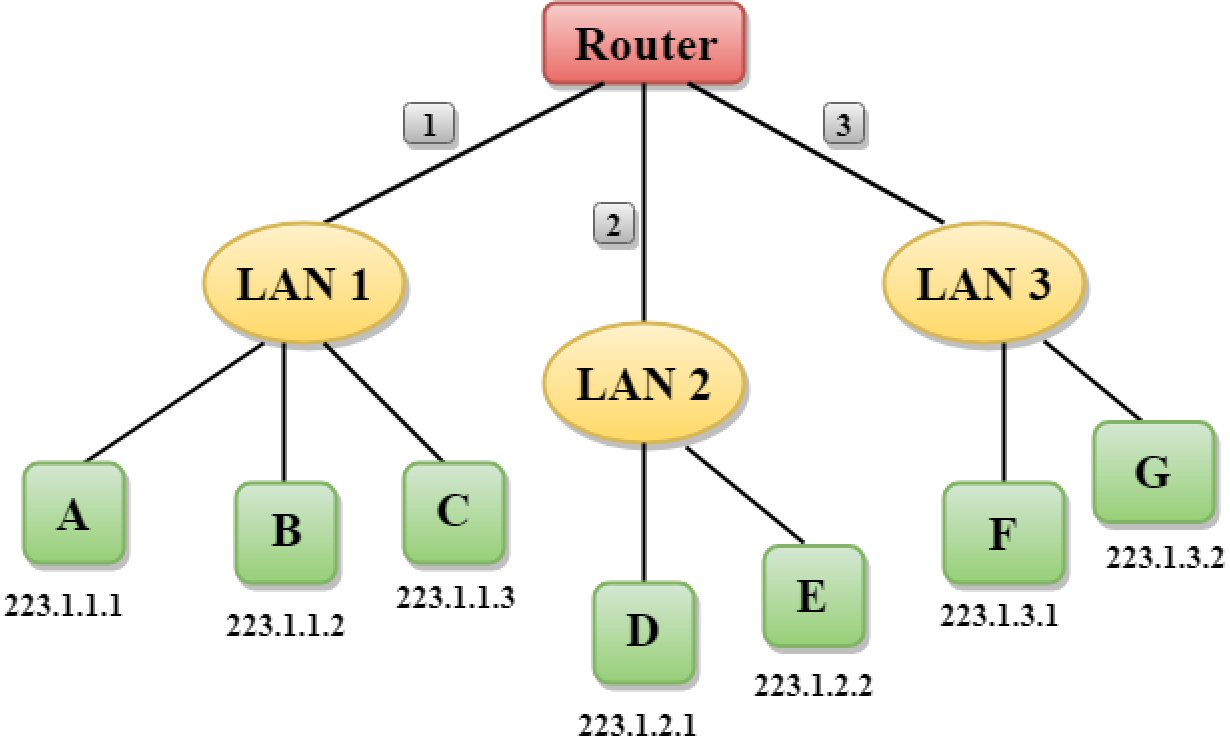
Network addresses are always logical, i.e., software-based addresses.

A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.

A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.

Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

- **Let's understand through a simple example.**



In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.

Each host contains its own interface and IP address.

All the interfaces attached to the LAN 1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN 2 and LAN 3 have an IP address in the form of 223.1.2.xxx and 223.1.3.xxx respectively.

Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

ROUTING

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

The routing process usually directs forwarding on the basis of routing tables. Routing tables maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols.

RELIABILITY

In computer networking, a **reliable** protocol is a communication protocol that notifies the sender whether or not the delivery of data to intended recipients was successful. Reliability is a synonym for **assurance**, which is the term used by the ITU and ATM Forum.

Reliable protocols typically incur more overhead than unreliable protocols, and as a result, function more slowly and with less scalability. This often is not an issue for unicast protocols, but it may become a problem for reliable multicast protocols.

A reliable service is one that notifies the user if delivery fails, while an *unreliable* one does not notify the user if delivery fails.[*citation needed*] For example, Internet Protocol (IP) provides an unreliable service. Together, Transmission Control Protocol (TCP) and IP provide a reliable service, whereas User Datagram Protocol (UDP) and IP provide an unreliable one.

In the context of distributed protocols, reliability properties specify the guarantees that the protocol provides with respect to the delivery of messages to the intended recipient(s).

An example of a reliability property for a unicast protocol is "at least once", i.e. at least one copy of the message is guaranteed to be delivered to the recipient.

Reliability properties for multicast protocols can be expressed on a per-recipient basis (simple reliability properties), or they may relate the fact of delivery or the order of delivery among the different recipients (strong reliability properties). In the context of multicast protocols, strong reliability properties express the guarantees that the protocol provides with respect to the delivery of messages to different recipients.

INTEROPERABILITY

Interoperability is the property that facilitates unrestricted sharing and use of data or resources between disparate systems via local area networks (LANs) or wide area networks (WANs). There are two types of data interoperability - syntactic interoperability, which is a prerequisite to semantic interoperability and enables different software components to cooperate, facilitating two or more systems to communicate and exchange data; and semantic interoperability, which refers to the ability of computer systems to exchange meaningful data with unambiguous, shared meaning.

Efficient automated data sharing between applications, databases, and other computer systems is a crucial component throughout networked computerized systems, especially interoperability in healthcare information and management systems.

SECURITY

Network security is any activity designed to protect the usability and integrity of your network and data.
It includes both hardware and software technologies
It targets a variety of threats
It stops them from entering or spreading on your network
Effective network security manages access to the network

STANDARDSINNETWORKING

- Standardsarenecessaryinnetworkingtoensureinterconnectivityandinteroperabilitybetweenvariousnetworking hardwareandsoftwarecomponents.

- Withoutstandardswewouldhaveproprietaryproductscreatingisolatedislandsofuserswhichcannot interconnect.

ConceptofStandard

- Standards provide guidelines to product manufacturers andvendorstoensurenationalandinternationalinterconnectivity.

- Datacommunicationsstandardsareclassifiedintotwocategories:

1. **DefactoStandard**
   - Thesearethestandardsthathavebeentraditionallyused andmean**byfact** or**byconvention**
   - Thesestandardsarenotapprovedbyanyorganizedbodybutareadoptedbywidespread use.

2. **Dejure standard**
   - Itmeans by**law**or**byregulation.**
   - oThesestandardsarelegislatedandapprovedbyanbodythatisofficiallyrecognized.

StandardOrganizationsinfieldofNetworking

oStandardsarecreatedby standardscreationcommittees,forums,andgovernmentregulatoryagencies.

o**ExamplesofStandardCreationCommittees**:

1. InternationalOrganizationforStandardization(ISO)
2. International Telecommunications Union — TelecommunicationsStandard (ITU-T)
3. AmericanNationalStandardsInstitute(ANSI)
4. InstituteofElectrical &ElectronicsEngineers(IEEE)
5. ElectronicIndustriesAssociates(EIA)

o **ExamplesofForums**

1. ATMForum
2. MPLSForum
3. Frame RelayForum

o**Examples of RegulatoryAgencies:**

1. FederalCommunications Committee(FCC)

THE TELEPHONE SYSTEM AND DATA COMMUNICATIONS

THE DEVELOPMENT OF THE TELEPHONE

As with many innovations, the idea for the telephone came along far sooner than it was brought to reality. While Italian innovator Antonio Meucci (pictured at left) is credited with inventing the first basic phone in 1849, and Frenchman Charles Bourseul devised a phone in 1854, Alexander Graham Bell won the first U.S. patent for the device in 1876. Bell began his research in 1874 and had financial backers who gave him the best business plan for bringing it to market.

In 1877-78, the first telephone line was constructed, the first switchboard was created and the first telephone exchange was in operation. Three years later, almost 49,000 telephones were in use. In 1880, Bell (in the photo below) merged this company with others to form the American Bell Telephone Company and in 1885 American Telegraph and Telephone Company (AT&T) was formed; it dominated telephone communications for the next century. At one point in time, Bell System employees purposely denigrated the U.S. telephone system to drive down stock prices of all phone companies and thus make it easier for Bell to acquire smaller competitors.

By 1900 there were nearly 600,000 phones in Bell's telephone system; that number shot up to 2.2 million phones by 1905, and 5.8 million by 1910. In 1915 the transcontinental telephone line began operating. By 1907, AT&T had a near monopoly on phone and telegraph service, thanks to its purchase of Western Union. Its president, Theodore Vail, urged at the time that a monopoly could most efficiently operate the nation's far-flung communications network. At the urging of the public and AT&T competitors, the government began to investigate the company for anti-trust violations, thus forcing the 1913 Kingsbury Commitment, an agreement between AT&T vice president Nathan Kingsbury and the office of the U.S. Attorney General. Under this commitment, AT&T agreed to divest itself of Western Union and provide long-distance services to independent phone exchanges.

During World War I, the government nationalized telephone and telegraph lines in the United States from June 1918 to July 1919, when, after a joint resolution of Congress, President Wilson issued an order putting them under the direction of the U.S. Post Office. A year later, the systems were returned to private ownership, AT&T resumed its monopolistic hold, and by 1934 the government again acted, this time agreeing to allow it to operate as a "regulated monopoly" under the jurisdiction of the FCC.

Public utility commissions in state and local jurisdictions were appointed regulators of AT&T and the nation's independent phone companies, while the FCC regulated long-distance services conducted across state lines. They set the rates the phone companies could charge and determined what services and equipment each could offer. This stayed in effect until AT&T's forced divestiture in 1984, the conclusion of a U.S. Department of Justice anti-trust suit that had been filed in 1974. The all-powerful company had become popularly known and disparaged as "Ma Bell." AT&T's local operations were divided into seven independent Regional Bell Operating Companies, known as the "Baby Bells." AT&T became a long-distance-services company.

By 1948, the 30 millionth phone was connected in the United States; by the 1960s, there were more than 80 million phone hookups in the U.S. and 160 million in the world; by 1980, there were more than 175 million telephone subscriber lines in the U.S. In 1993, the first digital cellular network went online in Orlando, Florida; by 1995 there were 25 million cellular phone subscribers, and that number exploded at the turn of the century, with digital cellular phone service expected to replace land-line phones for most U.S. customers by as early as 2010.

UNIT – II

ESSENTIAL TERMS AND CONCEPTS

An understanding of networking is important for anyone managing a server. Not only is it essential for getting your services online and running smoothly, it also gives you the insight to diagnose problems.

This article will provide an overview of some common networking concepts. We will discuss terminology, common protocols, and the responsibilities and characteristics of the different layers of networking.

This guide is operating system agnostic, but should be very helpful when implementing features and services that utilize networking on your server.

Networking Glossary

First, we will define some common terms that you will see throughout this guide, and in other guides and documentation regarding networking.

These terms will be expanded upon in the appropriate sections that follow:

- Connection: In networking, a connection refers to pieces of related information that are transferred through a network. Generally speaking, a connection is established before data transfer (by following the procedures laid out in a protocol) and may be deconstructed at the end of the data transfer.
- Packet: A packet is the smallest unit that is intentionally transferred over a network. When communicating over a network, packets are the envelopes that carry your data (in pieces) from one end point to the other.

  Packets have a header portion that contains information about the packet including the source and destination, timestamps, network hops, etc. The main portion of a packet contains the actual data being transferred. It is sometimes called the body or the payload.

- Network Interface: A network interface can refer to any kind of software interface to networking hardware. For instance, if you have two network cards in your computer, you can control and configure each network interface associated with them individually.

  A network interface may be associated with a physical device, or it may be a representation of a virtual interface. The “loopback” device, which is a virtual interface available in most Linux environments to connect back to the same machine, is an example of this.

- LAN: LAN stands for "local area network". It refers to a network or a portion of a network that is not publicly accessible to the greater internet. A home or office network is an example of a LAN.
- WAN: WAN stands for "wide area network". It means a network that is much more extensive than a LAN. While WAN is the relevant term to use to describe large, dispersed networks in general, it is usually meant to mean the internet, as a whole.

  If an interface is said to be connected to the WAN, it is generally assumed that it is reachable through the internet.

- Protocol: A protocol is a set of rules and standards that define a language that devices can use to communicate. There are a great number of protocols in use extensively in networking, and they are often implemented in different layers.

  Some low level protocols are TCP, UDP, IP, and ICMP. Some familiar examples of application layer protocols, built on these lower protocols, are HTTP (for accessing web content), SSH, and TLS/SSL.

- Port: A port is an address on a single machine that can be tied to a specific piece of software. It is not a physical interface or location, but it allows your server to be able to communicate using more than one application.
- Firewall: A firewall is a program that decides whether traffic coming or going from a server should be allowed. A firewall usually works by creating rules for which type of traffic is acceptable on which ports. Generally, firewalls block ports that are not used by a specific application on a server.
- NAT: NAT stands for network address translation. It is a way to repackage and send incoming requests to a routing server to the relevant devices or servers on a LAN. This is usually implemented in physical LANs as a way to route requests through one IP address to the necessary backend servers.
- VPN: VPN stands for virtual private network. It is a means of connecting separate LANs through the internet, while maintaining privacy. This is used to connect remote systems as if they were on a local network, often for security reasons.

There are many other terms that you will come across, and this list is not exhaustive. We will explain other terms as we need them. At this point, you should understand some high-level concepts that will enable us to better discuss the topics to come.

Network Layers

While networking is often discussed in terms of topology in a horizontal way, between hosts, its implementation is layered in a vertical fashion within any given computer or network.

What this means is that there are multiple technologies and protocols that are built on top of each other in order for communication to function. Each successive, higher layer abstracts the raw data a little bit more.

It also allows you to leverage lower layers in new ways without having to invest the time and energy to develop the protocols and applications that handle those types of traffic.

The language that we use to talk about each of the layering schemes varies significantly depending on which model you use. Regardless of the model used to discuss the layers, the path of data is the same.

As data is sent out of one machine, it begins at the top of the stack and filters downwards. At the lowest level, actual transmission to another machine takes place. At this point, the data travels back up through the layers of the other computer.

Each layer has the ability to add its own "wrapper" around the data that it receives from the adjacent layer, which will help the layers that come after decide what to do with the data when it is handed off.

TCP/IP Model

The TCP/IP model, more commonly known as the Internet protocol suite, is a widely adopted layering model. It defines the four separate layers:

- Application: In this model, the application layer is responsible for creating and transmitting user data between applications. The applications can be on remote systems, and should appear to operate as if locally to the end user. This communication is said to take place between peers.
- Transport: The transport layer is responsible for communication between processes. This level of networking utilizes ports to address different services.
- Internet: The internet layer is used to transport data from node to node in a network. This layer is aware of the endpoints of the connections, but is not concerned with the actual connection needed to get from one place to another. IP addresses are defined in this layer as a way of reaching remote systems in an addressable manner.
- Link: The link layer implements the actual topology of the local network that allows the internet layer to present an addressable interface. It establishes connections between neighboring nodes to send data.

As you can see, the TCP/IP model is abstract and fluid. This made it popular to implement and allowed it to become the dominant way that networking layers are categorized.

Interfaces

Interfaces are networking communication points for your computer. Each interface is associated with a physical or virtual networking device.

Typically, your server will have one configurable network interface for each Ethernet or wireless internet card you have.

In addition, it will define a virtual network interface called the "loopback" or localhost interface. This is used as an interface to connect applications and processes on a single computer to other applications and processes. You can see this referenced as the "lo" interface in many tools.

Many times, administrators configure one interface to service traffic to the internet and another interface for a LAN or private network.

In datacenters with private networking enabled (including DigitalOcean Droplets), your VPS will have two networking interfaces. The “eth0” interface will be configured to handle traffic from the internet, while the “eth1” interface will operate to communicate with a private network

Networking works by piggybacking a number of different protocols on top of each other. In this way, one piece of data can be transmitted using multiple protocols encapsulated within one another.

We will start with protocols implemented on the lower networking layers and work our way up to protocols with higher abstraction.

PROTOCOLS

Medium Access Control

Medium access control is a communications protocol that is used to distinguish specific devices. Each device is supposed to get a unique, hardcoded media access control address (MAC address) when it is manufactured that differentiates it from every other device on the internet.

Addressing hardware by the MAC address allows you to reference a device by a unique value even when the software on top may change the name for that specific device during operation.

MAC addressing is one of the only protocols from the low-level link layer that you are likely to interact with on a regular basis.

IP

The IP protocol is one of the fundamental protocols that allow the internet to work. IP addresses are unique on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the TCP/IP model.

Networks can be linked together, but traffic must be routed when crossing network boundaries. This protocol assumes an unreliable network and multiple paths to the same destination that it can dynamically change between.

There are a number of different implementations of the protocol. The most common implementation today is IPv4 addresses, which follow the pattern `123.123.123.123`, although IPv6 addresses, which follows the pattern `2001:0db8:0000:0000:0000:ff00:0042:8329`, are growing in popularity due to the limited number of available IPv4 addresses.

ICMP

ICMP stands for internet control message protocol. It is used to send messages between devices to indicate their availability or error conditions. These packets are used in a variety of network diagnostic tools, such as `ping` and `traceroute`.

Usually ICMP packets are transmitted when a different kind of packet encounters a problem. They are used as a feedback mechanism for network communications.

TCP

TCP stands for transmission control protocol. It is implemented in the transport layer of the TCP/IP model and is used to establish reliable connections.

TCP is one of the protocols that encapsulates data into packets. It then transfers these to the remote end of the connection using the methods available on the lower layers. On the other end, it can check for errors, request certain pieces to be resent, and reassemble the information into one logical piece to send to the application layer.

The protocol builds up a connection prior to data transfer using a system called a three-way handshake. This is a way for the two ends of the communication to acknowledge the request and agree upon a method of ensuring data reliability.

After the data has been sent, the connection is torn down using a similar four-way handshake.

TCP is the protocol of choice for many of the most popular uses for the internet, including WWW, SSH, and email.

UDP

UDP stands for user datagram protocol. It is a popular companion protocol to TCP and is also implemented in the transport layer.

The fundamental difference between UDP and TCP is that UDP offers unreliable data transfer. It does not verify that data has been received on the other end of the connection. This might sound like a bad thing, and for many purposes, it is. However, it is also extremely important for some functions.

Because it is not required to wait for confirmation that the data was received and forced to resend data, UDP is much faster than TCP. It does not establish a connection with the remote host, it just sends data without confirmation.

Because it is a straightforward transaction, it is useful for communications like querying for network resources. It also doesn't maintain a state, which makes it great for transmitting data from one machine to many real-time clients. This makes it ideal for VOIP, games, and other applications that cannot afford delays.

HTTP

HTTP stands for hypertext transfer protocol. It is a protocol defined in the application layer that forms the basis for communication on the web.

HTTP defines a number of verbs that tell the remote system what you are requesting. For instance, GET, POST, and DELETE all interact with the requested data in a different way. To see an example of the different HTTP requests in action, refer to How To Define Routes and HTTP Request Methods in Express.

DNS

DNS stands for domain name system. It is an application layer protocol used to provide a human-friendly naming mechanism for internet resources. It is what ties a domain name to an IP address and allows you to access sites by name in your browser.

SSH

SSH stands for secure shell. It is an encrypted protocol implemented in the application layer that can be used to communicate with a remote server in a secure way. Many additional technologies are built around this protocol because of its end-to-end encryption and ubiquity.

There are many other protocols that we haven’t covered that are equally important. However, this should give you a good overview of some of the fundamental technologies that make the internet and networking possible.

the differences between circuit switching and packet switching. Both are types of switching techniques. Initially, we will learn some basics of switching network technologies. After that, we will see differences between both of them.

CENTRALIZED, DECENTRALIZED AND DISTRIBUTED SYSTEMS

CENTRALIZED SYSTEMS

Centralized networks are built around a single, centralized server/master node, which handles all major data processing and stores data and user information that other users can access. From there, client nodes can be connected to the main server and submit data requests instead of performing them directly. The majority of web services — including YouTube, a mobile app store, or your online banking account — are coordinated by a centralized network owner, meaning that all data transactions within these networks require verification via a third-party authority.

Centralized networks are currently the most widely used type of network on the web. These networks are dependent on a central network owner to connect all the other satellite users and devices — which means there is a single point of failure that can be deliberately exploited by malicious actors.

DECENTRALIZED SYSTEMS

By contrast, a decentralized network distributes information-processing workloads across multiple devices instead of relying on a single central server. Each of these separate devices serves as a mini central unit that interacts independently with other nodes. As a result, even if one of the master nodes crashes or is compromised, the other servers can continue providing data access to users, and the overall network will continue to operate with limited or zero disruption.

Decentralized networks are made possible by recent technological advancements that have equipped computers and other devices with a significant amount of processing power and can be synced up and leveraged for distributed processing. However, while decentralized networks are substantially different from centralized networks, it's important to note that decentralized networks do not distribute data storage and processing evenly across the entire network and still rely on main servers, albeit more than one per network.

DISTRUBUTED SYSTEMS

A distributed network is similar to a decentralized network in the sense that it forgoes a single centralized master server in favor of multiple network owners. However, distributed networks are composed of equal, interconnected nodes, meaning that data ownership and computational resources are shared evenly across the entire network. The term "distributed network" is sometimes used to describe a network that is simply geographically distributed but may follow a top-down node hierarchy model. In most instances, though, the term refers to a network where node locations and computational resources are evenly distributed.

Because distributed networks do not have a central server or a separate set of master nodes, the burden of data processing is crowdsourced across the network, with all users granted equal access to data. The decision-making process on a distributed network therefore typically involves individual nodes voting to change to a new state, and the final behavior of the system changes in accordance with the aggregate results of the decisions each individual node votes on. The specific processes by which a distributed network votes and makes decisions is contingent on the network's consensus mechanism. All forms of distributed decision-making involve the network's individual components interacting with one another in order to achieve a common goal.

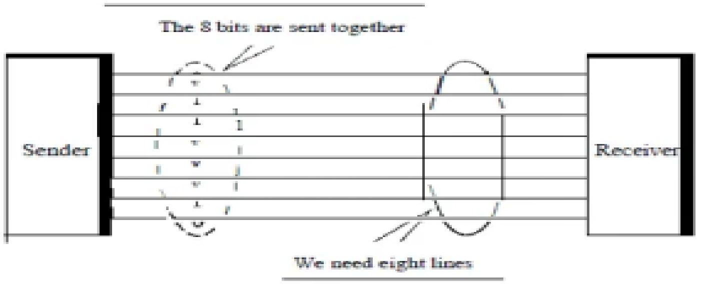
The basic data transmission types tell us which direction data moves between sender and receiver. These are:

- Simplex Data Transmission
- Half-Duplex Data Transmission
- Full-Duplex Data Transmission
- Serial and Parallel Transmission

There are two ways of grouping bits of data and sending them across a network. Serial transmission means bits are sent sequentially, whereas parallel transmission sends data packets simultaneously.

Parallel Data Transmission

In parallel transmission, binary data is grouped into bits. The number of groups corresponds to the number of threads between the sender and receiver, and the groups are transmitted simultaneously.



Source

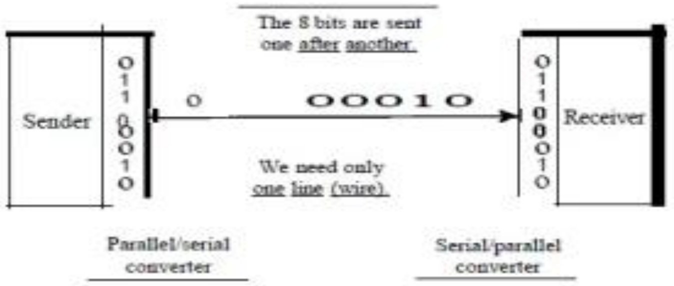
This method allows for groups of bits (bytes) to be transmitted faster than serial transmission. However, because separate lines are required for each bit, building infrastructure this way would be costly.

That’s why we mostly see parallel transmission within devices, like computer processors, for example. The communication between an API like RDD and the Spark codebase is another example of parallel transmission.

Serial Data Transmission

In serial data transmission, each bit is sent one after the other in sequence. This is the type of data transmission method devices use to communicate over a network.

Since the sending or receiving devices will use parallel transmission internally, converters (serial to parallel and parallel to serial) are used at the interface point between the device and the line.



Parallel transmission always happens in synchronicity with the system clock. Serial transmission, though, can be subdivided into three further groups based on the synchronization of the sending and receiving device.

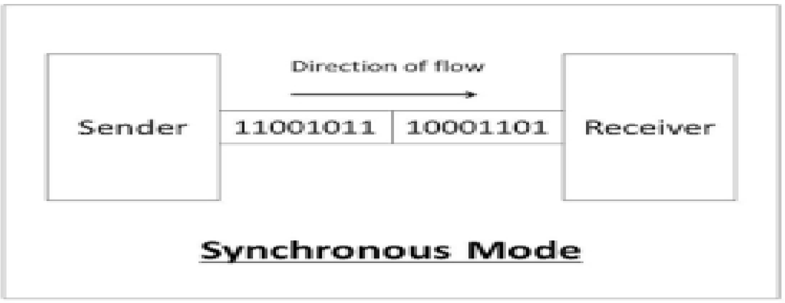
SYNCHRONOUS AND ASYNCHRONOUS TRANSMISSION

When data is sent at a synchronized rhythm, defined by the system clock, we call it synchronous transmission. Some types of data, like live video streams, need highly synchronized data feeds that arrive constantly. Other types can be sent asynchronously.

Synchronous Transmission:

In synchronous transmissions, data is sent in frames. These are long continuous strings of uninterrupted binary data. The receiving device counts the bits of binary data, using the synchronicity between devices (defined in the data layer) to count the length of a byte.

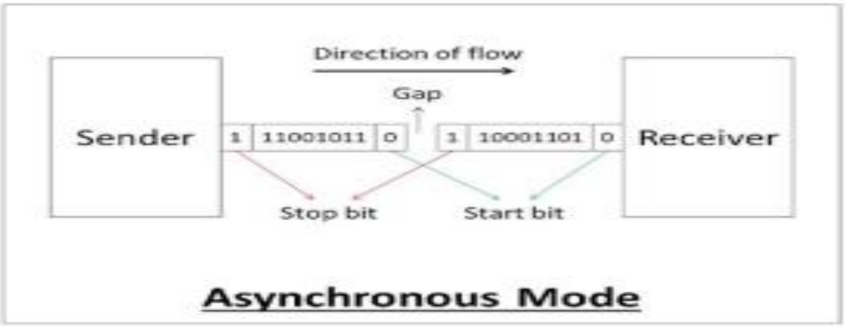
Since data is sent as a constant stream, synchronous transmission allows for high transfer speeds. This kind of transmission is used for high-speed connections between modern computer networks.



Asynchronous Transmission:

This method sends bytes with an additional “start” and “stop” bit at the beginning and end. That means the receiving device knows the length of a byte without synchronizing with the transmitter.

By counting the start and stop bits, the receiver can resynchronize the data stream at the byte level each time a new signal is received. This method is often used for low-speed transmissions, such as the input data from your keyboard or sporadic data from business microservices.



Isochronous Transmission:

When an image or audio signal needs to be broadcast at a specific frame rate, uninterrupted, then synchronous and asynchronous transmission both fall short. The entire bit stream needs to be synchronized and sent at a constant rate with no gaps between frames.

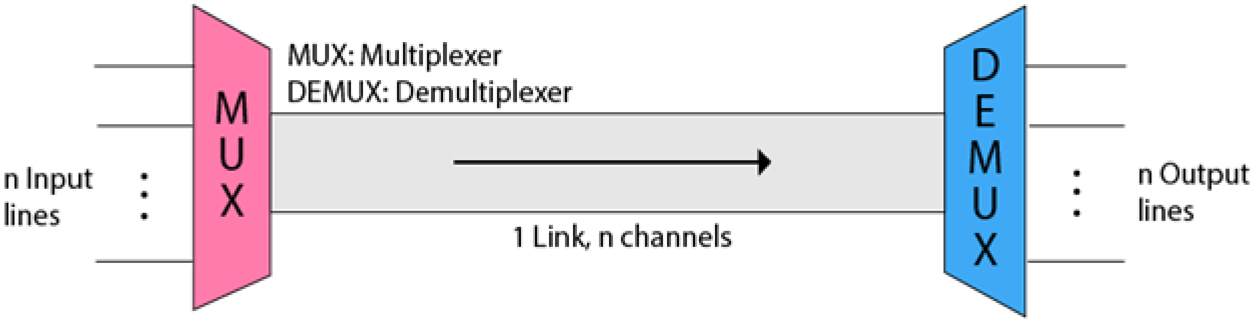
This is where Isochronous transmission is used. You might see this in a digital TV broadcast signal, or a live streaming service.

SPEED AND CAPACITY OF A COMMUNICATION CHANNEL

The terms *bandwidth* and *speed* are often used interchangeably but not correctly. The cause of the confusion may be due, in part, to advertisements by internet service providers (ISPs) that conflate the two by referring to greater *speeds* when they truly mean *bandwidth*.

Essentially, *speed* refers to the rate at which data can be transmitted, while the definition of *bandwidth* is the capacity for that speed. To use the water metaphor again, *speed* refers to how quickly water can be pushed through a pipe; *bandwidth* refers to the quantity of water that can be moved through the pipe over a set time frame.

MULTIPLEXING



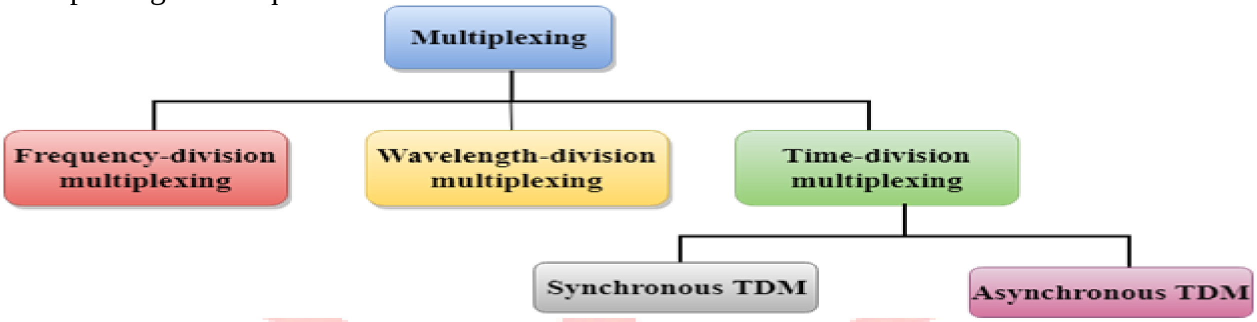
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.

- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

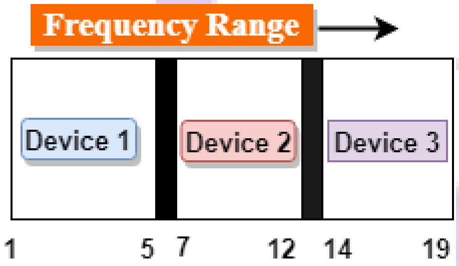
- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

Multiplexing Techniques can be classified as:

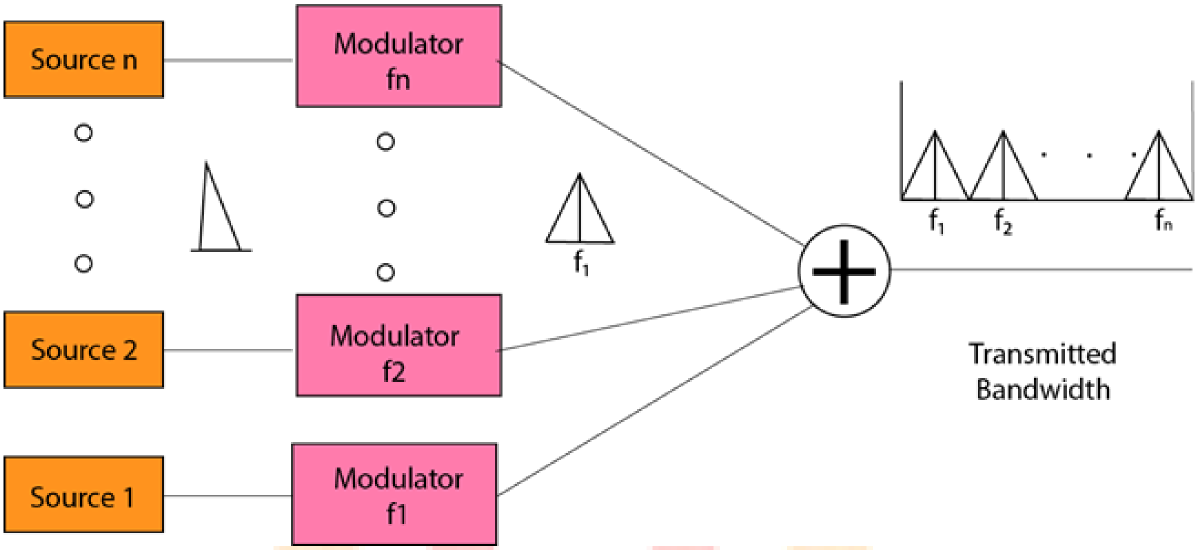

Multiplexing
Frequency-division multiplexing
Wavelength-division multiplexing
Time-division multiplexing
Synchronous TDM
Asynchronous TDM

Frequency-Division Multiplexing (FDM)

- It is an analog technique.
- Frequency Division Multiplexing is a technique in which the available bandwidth of a single transmission medium is subdivided into several channel



- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as sub-carriers. They are represented as f1,f2..fn.
- FDM is mainly used in radio broadcasts and TV networks.



Advantages Of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

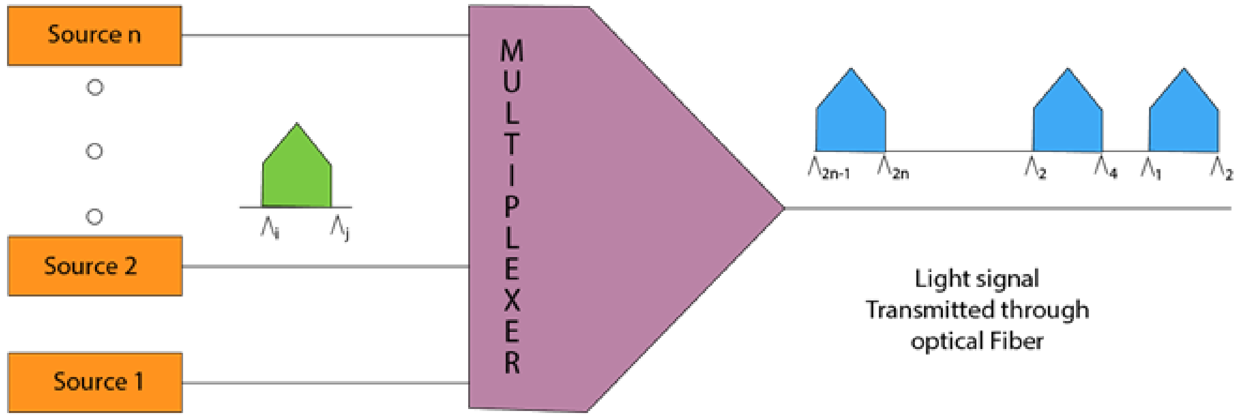
Disadvantages Of FDM:

- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

Applications Of FDM:

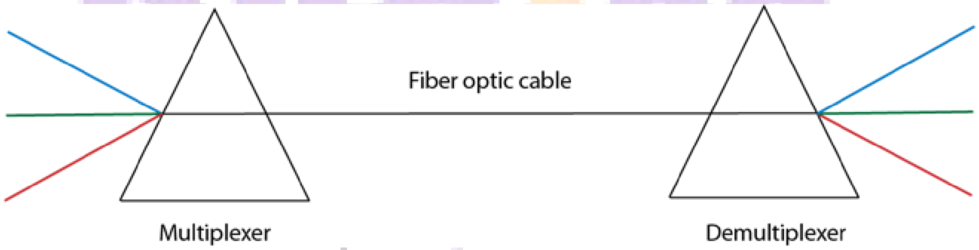
- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



WDM Transmitter

- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing

- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.

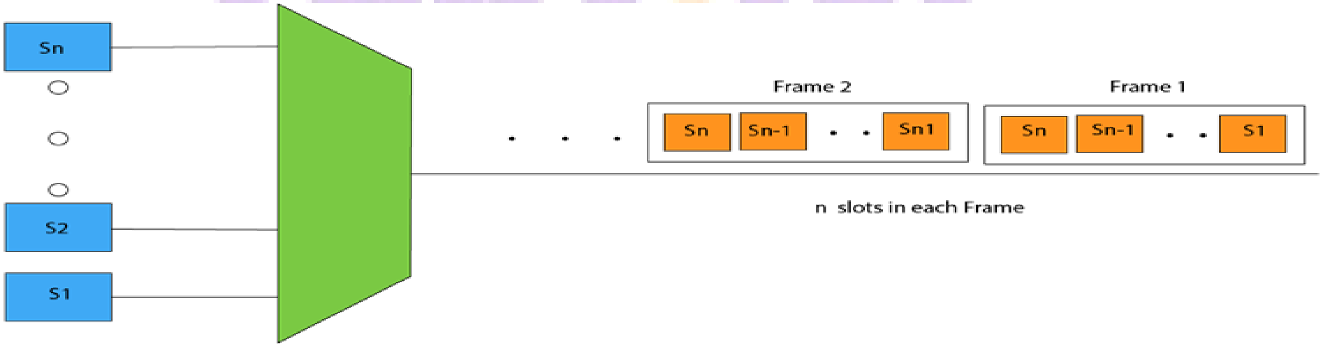
- In Time Division Multiplexing technique, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

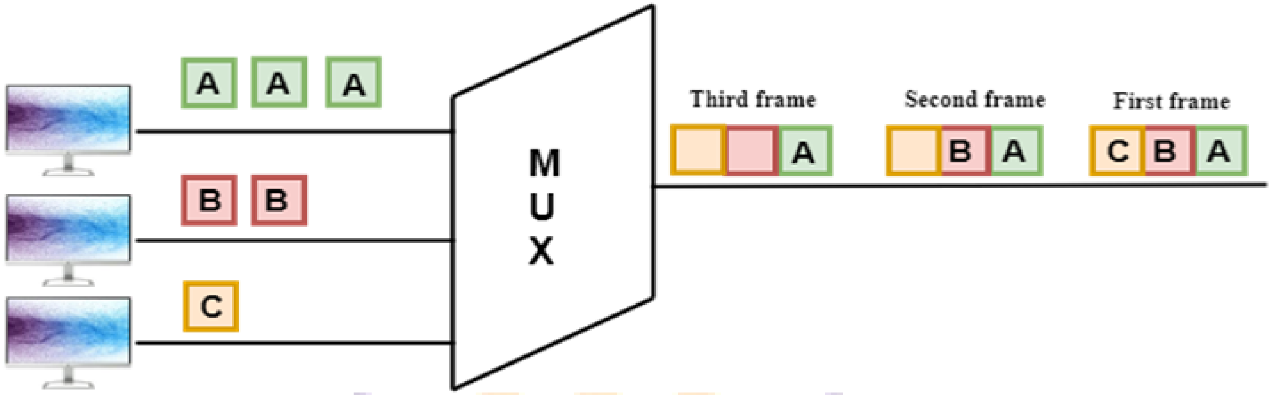
- Synchronous TDM
- Asynchronous TDM

Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



Concept Of Synchronous TDM



In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages Of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

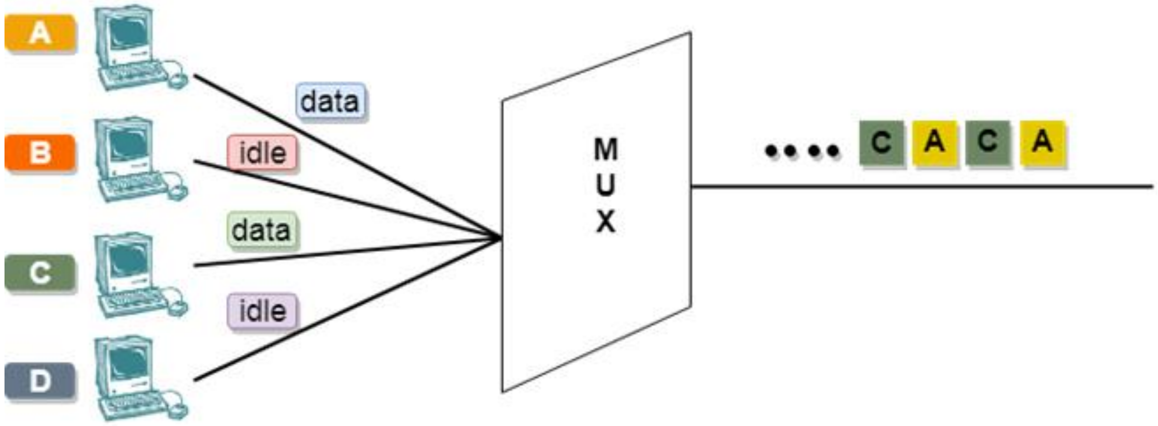
Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

ADDRESS	DATA

- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (m<n).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept Of Asynchronous TDM

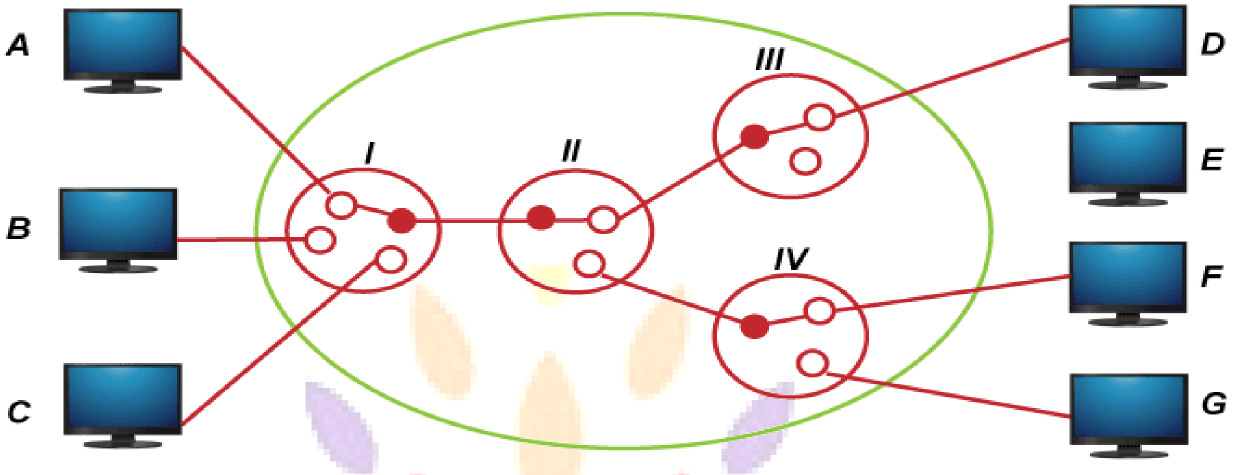


In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Circuit switching Network:

A circuit-switched network is one of the simplest data communication methods in which a dedicated path is established between the sending and receiving device. In this physical links connect via a set of switches.

Following figure displays the working of circuit switched network.



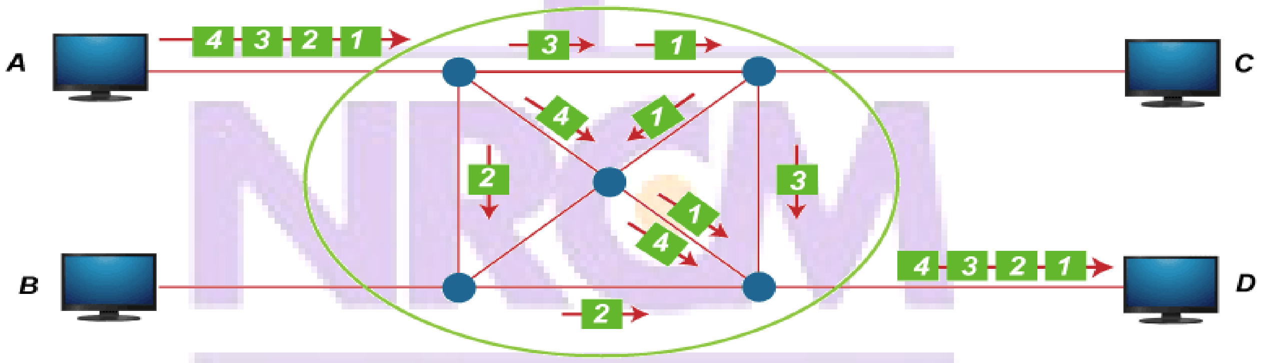
Circuit Switched Network

In the above figure it shows a circuit switched network in which computer connect via 4 switches with a point to point connections.

Packet switching Network:

In the Packet switching Network, the message is divide into packets. Each packet contains a header which includes the source address, destination address, and control information.

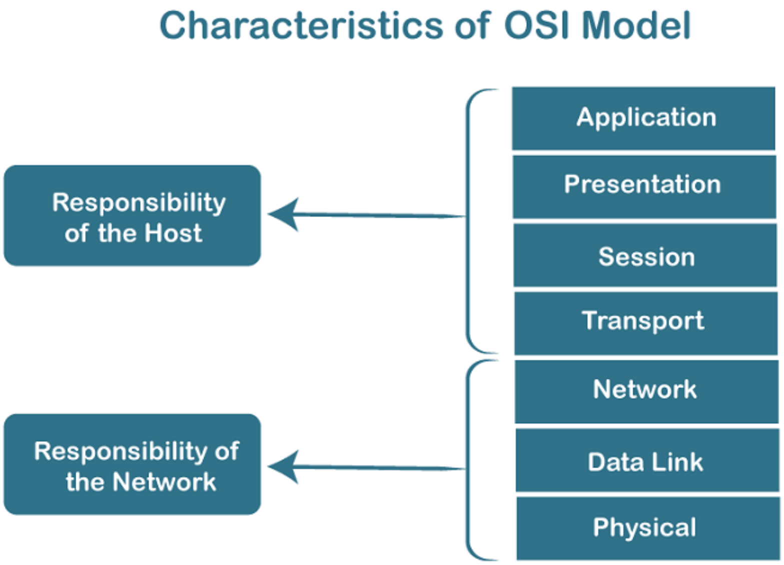
Following figure displays the working of packet switched network.



Packet Switched Network

In the above figure, it shows how a data gram approach is used to deliver four packets from station A to station D.

Characteristics of OSI Model:

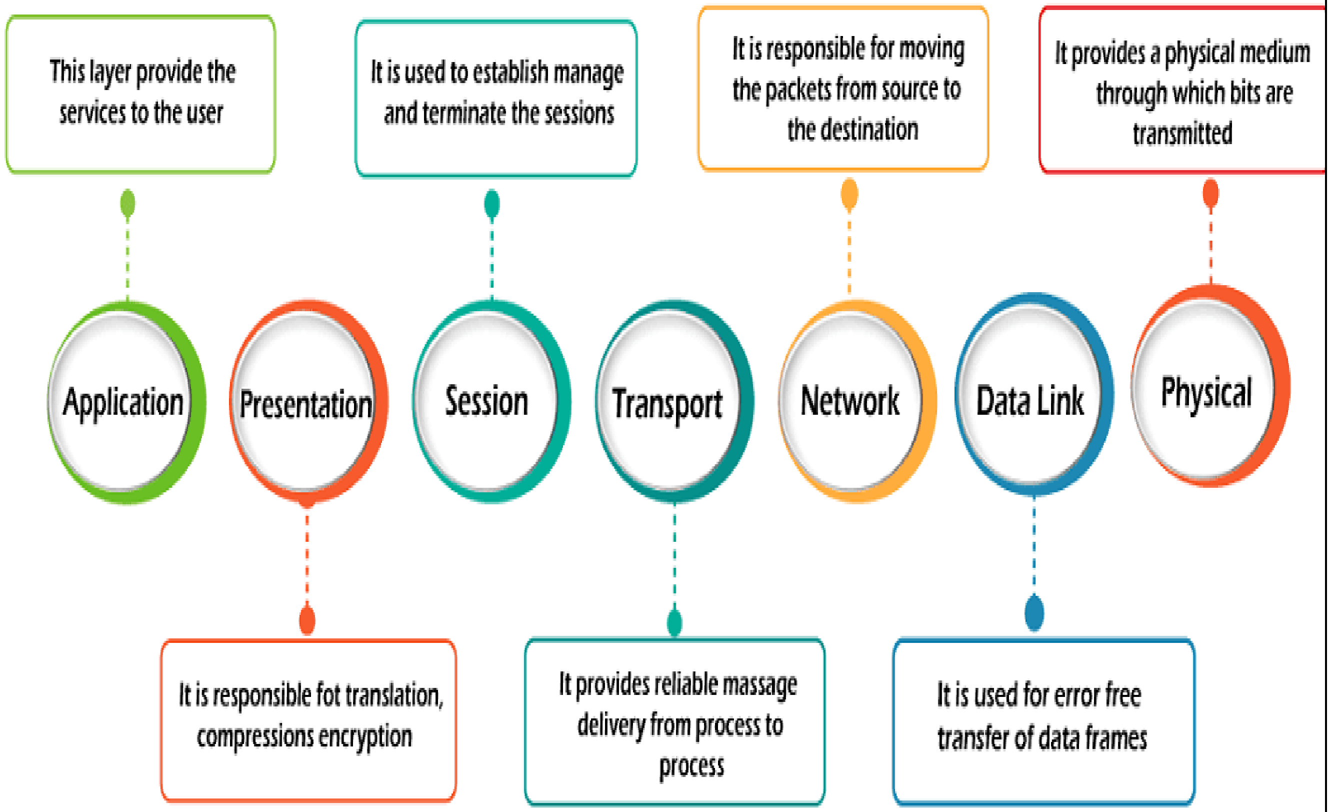

Characteristics of OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
Responsibility of the Host
Responsibility of the Network

- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer


This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames

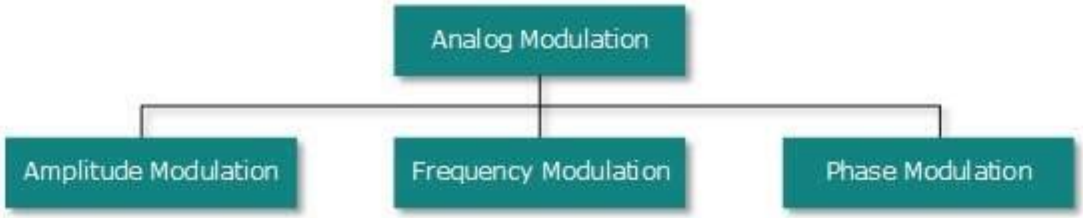
UNIT – III

ANALOG AND DIGITAL COMMUNICATION CONCEPTS

REPRESENTING DATA AS ANALOG SIGNALS

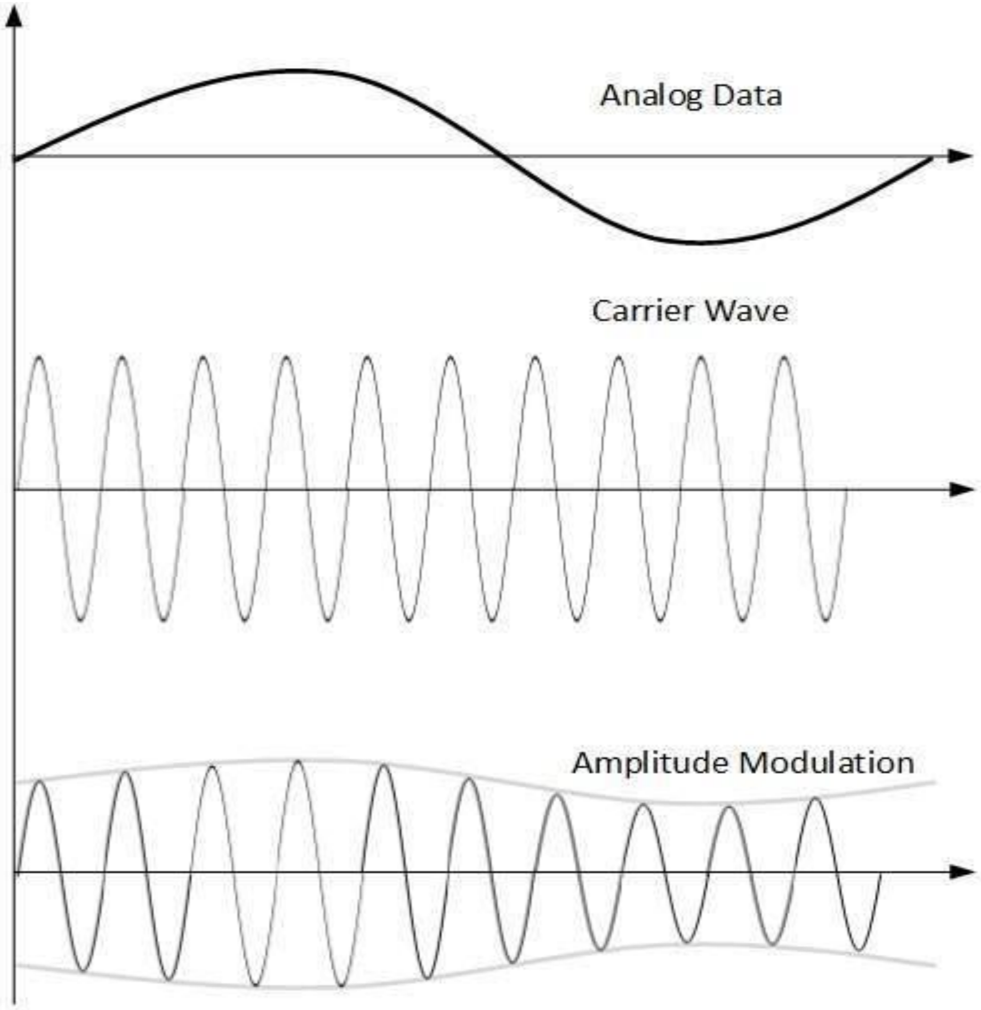
Analog-to-Analog Conversion

Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways:



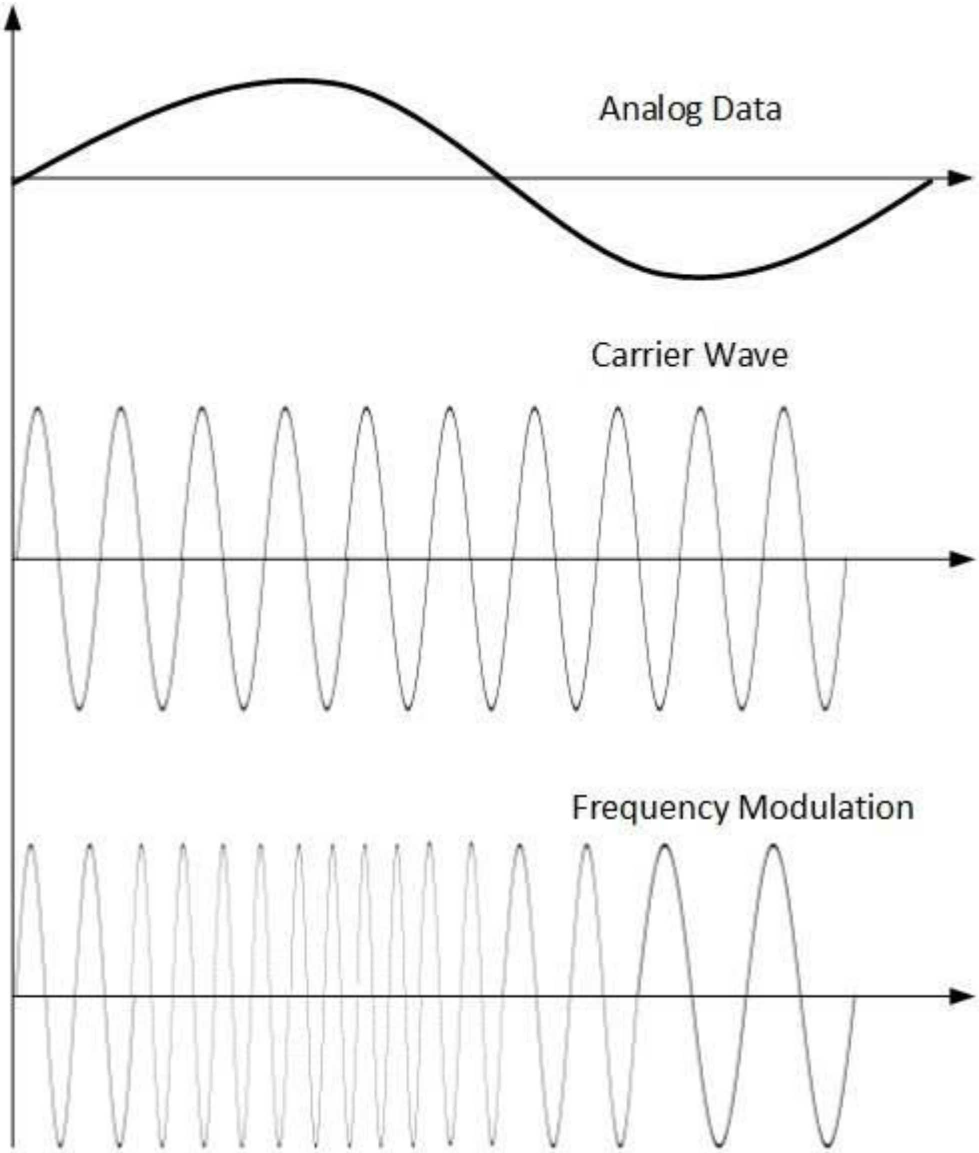
- **Amplitude Modulation**

In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.



Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.
The frequency and phase of carrier signal remain unchanged.

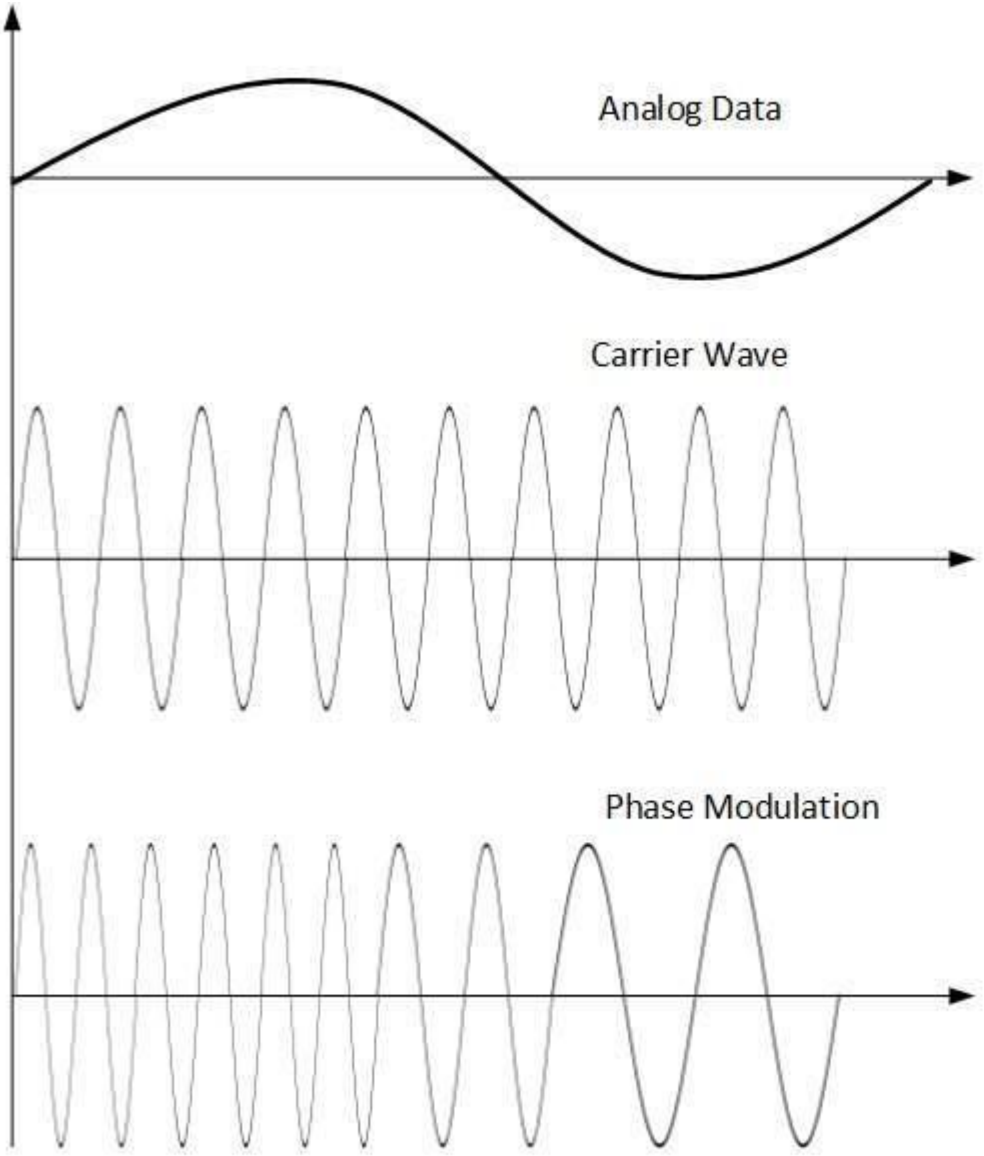
- **Frequency Modulation**
  In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).



The amplitude and phase of the carrier signal are not altered.

- **Phase Modulation**

  In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.



Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

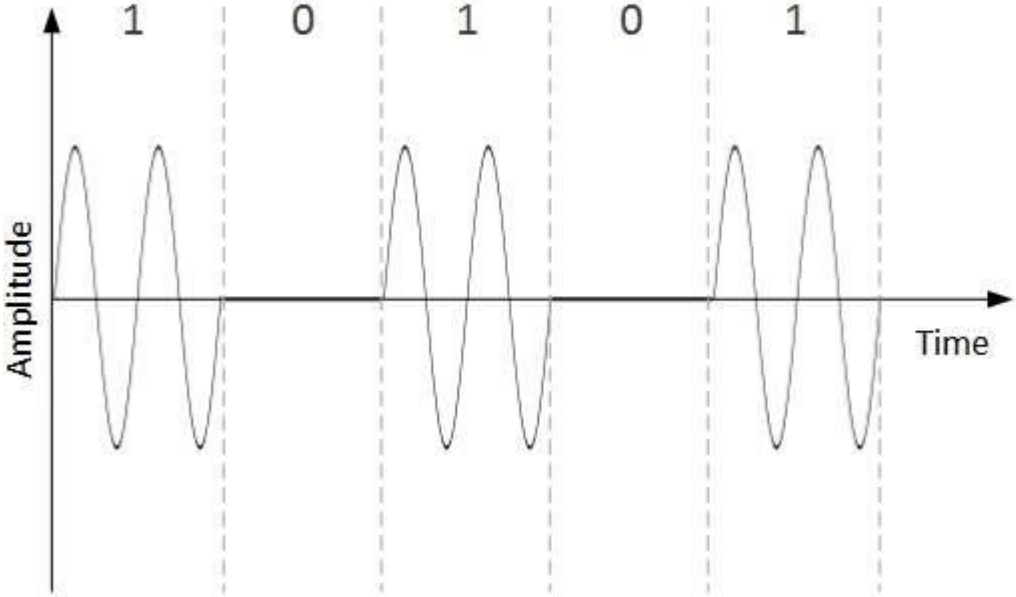
Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

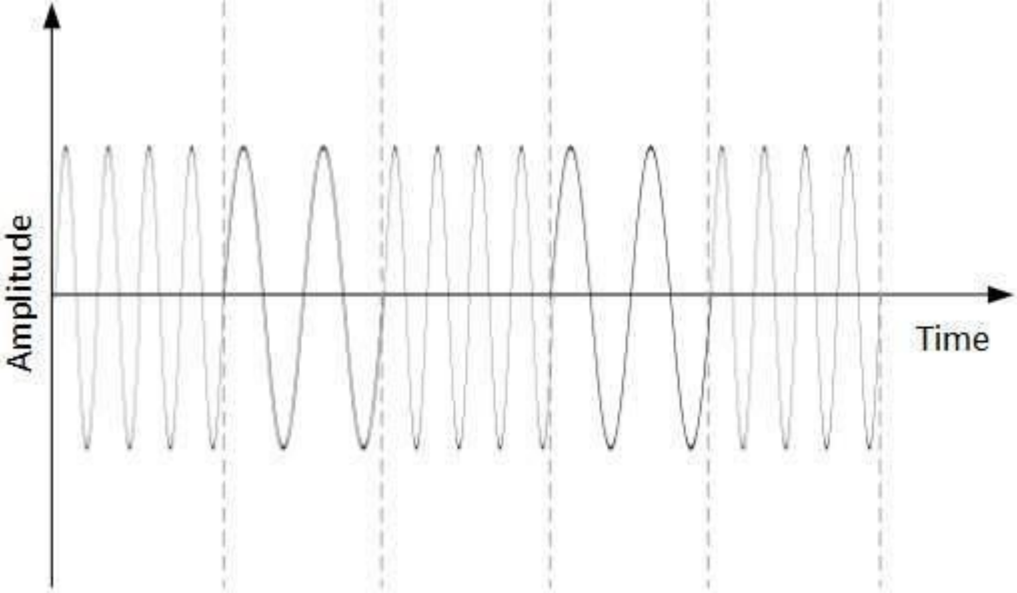
- **Amplitude Shift Keying**

In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



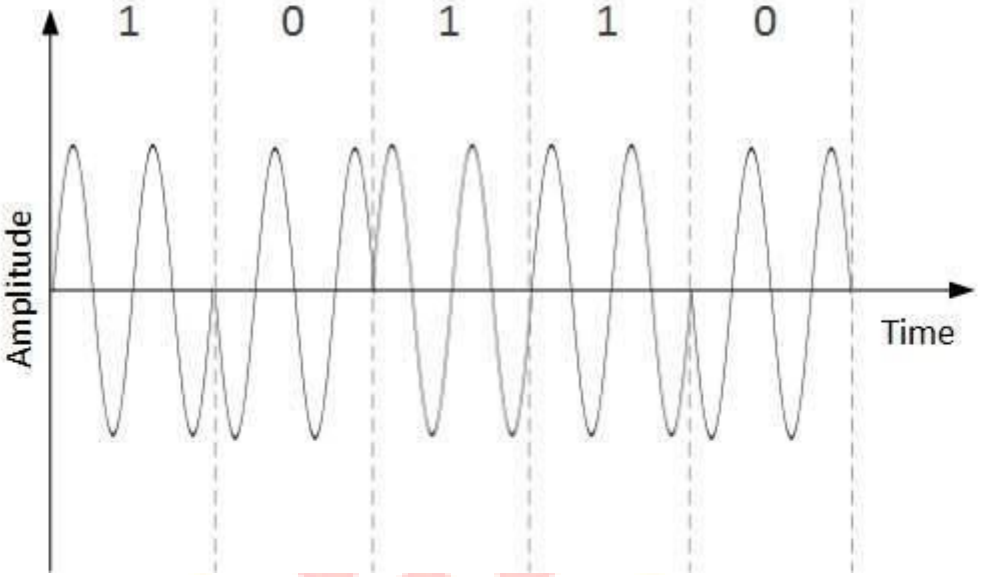
When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

- **Frequency Shift Keying**
  In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

- **Phase Shift Keying**
  In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



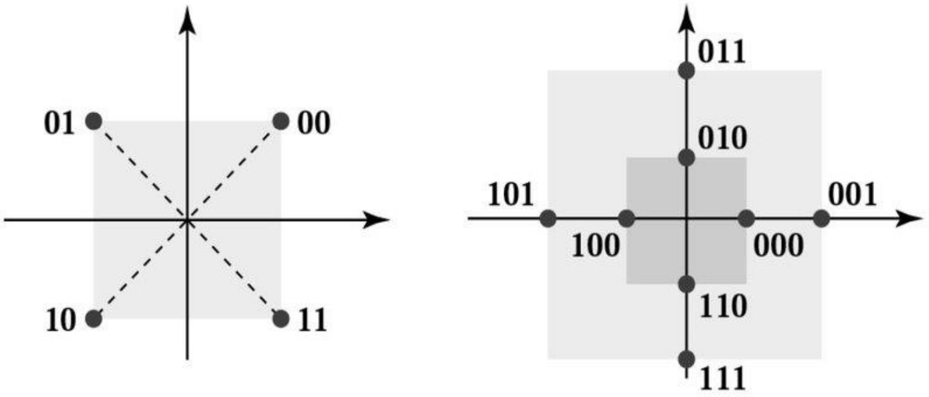
When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

- **Quadrature Phase Shift Keying**
  QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

Quadrature Amplitude Modulation (QAM)

It is possible to combine ASK, FSK and PSK. One benefit of combining different modulation methods is to increase the number of symbols available. Increasing the number of available symbols is a standard way to increase the bit rate, because increasing the number of symbols increases the number of bits per symbol. It is rare for all three methods to be combined, but very common for ASK and PSK to be combined to create **Quadrature amplitude modulation (QAM)**.

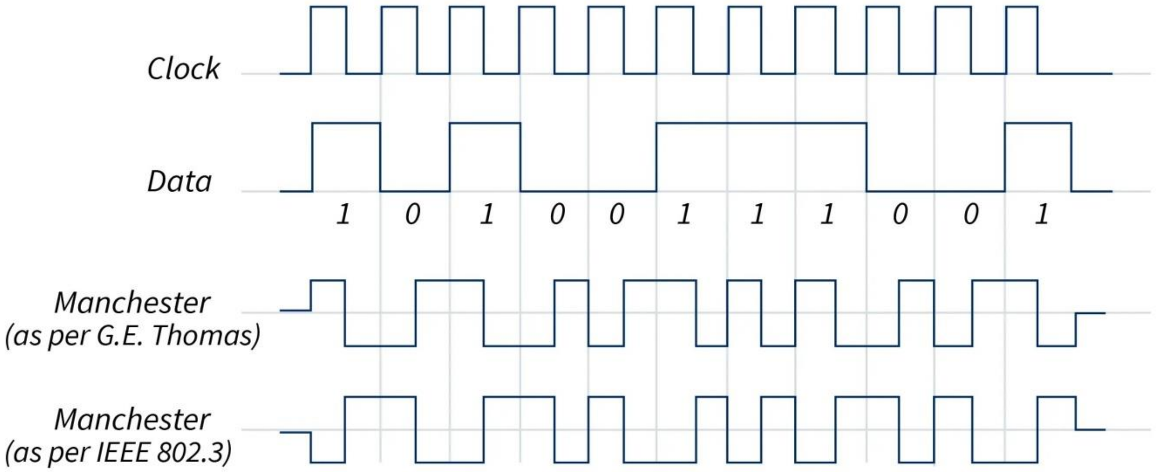
QAM is based on the application of ASK and PSK to two sinusoidal waves of the same frequency but with a phase difference of 90°. Sinusoidal waves 90° apart are said to be in a quadrature phase relationship. It is customary to refer to one of these waves as the **I wave**, or in-phase wave or component, and the other as the **Q wave**, or adrature wave or component



\

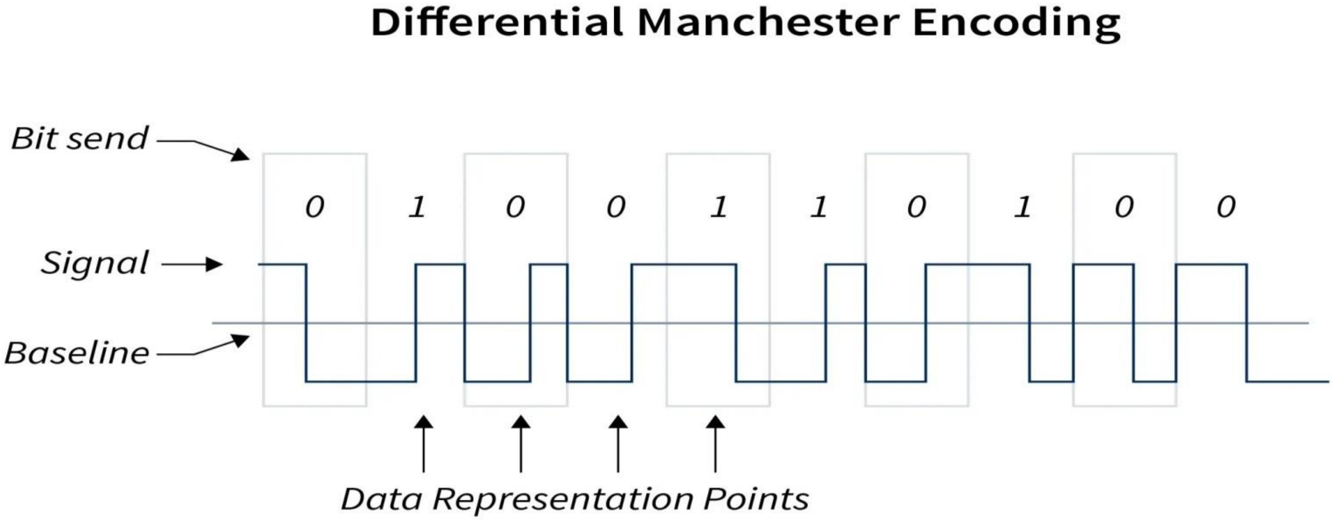
Digital-to-Digital Conversion

Manchester Encoding:
The physical layer of the Open System Interconnection [OSI] uses **Manchester** encoding, a synchronous clock encoding technique, to encode the clock and data of a synchronous bit stream. A logic zero is signaled by a transition from 1 to 0 in the middle of the bit in Manchester encoding (as specified by IEEE 802.3 standards for 10 Mbps), and a logic one is indicated by a **transition** from 0 to 1 in the same location


Clock
Data
1
0
1
0
0
1
1
1
0
0
1
Manchester (as per G.E. Thomas)
Manchester (as per IEEE 802.3)

Differential Manchester encoding
Differential Manchester encoding (DM) is a line code in digital frequency modulation in which data and clock signals are combined to form a single two-level self-synchronizing data stream. Each data bit is encoded by a presence or absence of signal level transition in the middle

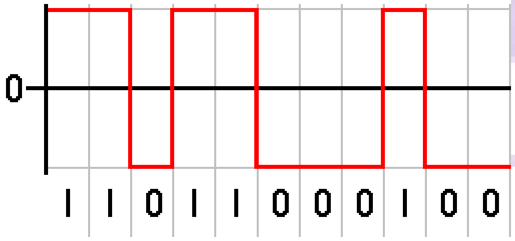
of the bit period, followed by the mandatory level transition at the beginning. The code is insensitive to an inversion of polarity.



Non-Return-to-Zero (NRZ)

In telecommunication, a **non-return-to-zero** (**NRZ**) line code is a binary code in which ones are represented by one significant condition, usually a positive voltage, while zeros are represented by some other significant condition, usually a negative voltage, with no other neutral or rest condition.

For a given data signaling rate, i.e., bit rate, the NRZ code requires only half the baseband bandwidth required by the Manchester code

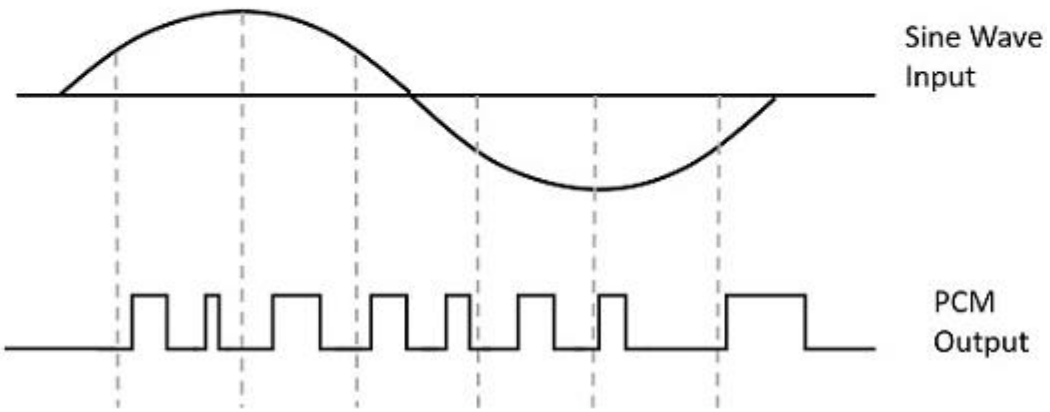


NRZ-L(level) refers to 1- constant, 0 - toggle
NRZ – I (inverse) refers to 1 - toggle, 0 - constant

Analog -to- Digital Conversion:

PULSE CODED MODULATION (PCM)

A signal is pulse code modulated to convert its analog information into a binary sequence, i.e., **1s** and **0s**. The output of a PCM will resemble a binary sequence. The following figure shows an example of PCM output with respect to instantaneous values of a given sine wave.



Instead of a pulse train, PCM produces a series of numbers or digits, and hence this process is called as **digital**. Each one of these digits, though in binary code, represent the approximate amplitude of the signal sample at that instant.

In Pulse Code Modulation, the message signal is represented by a sequence of coded pulses. This message signal is achieved by representing the signal in discrete form in both time and amplitude.

DATA RATE AND BANDWIDTH REDUCTION

Data-reduction techniques can be broadly categorized into two main types:

- Data compression: This bit-rate reduction technique involves encoding information using fewer bits of data. Compression algorithms can be lossy (some information is lost, reducing the resolution of the data) and lossless (information is fully preserved by removing statistical redundancy).
- Data deduplication: Also known as dedupe, this process involves eliminating duplicate copies of data within a storage volume or across the entire storage system (cross-volume dedupe). It uses pattern recognition to identify redundant data and replace them with references to a single saved copy.

Bandwidth Reduction:

In telecommunication, the term **bandwidth compression** has the following meanings:

- The reduction of the bandwidth needed to transmit a given amount of data in a given time.
- The reduction of the time needed to transmit a given amount of data in a given bandwidth.

Bandwidth compression implies a reduction in normal bandwidth of an information-carrying signal without reducing the information content of the signal. This can be accomplished with lossless data compression techniques. For more information read the Increasing speeds section in the Modem article. Bandwidth Compression is a core feature of WAN Optimization appliances to improve bandwidth efficiency.

Digital Carrier Systems

T1 Digital Carrier system

- T1 digital carrier system is a North American digital multiplexing standard since 1963.
- T1 stands for transmission one and specifies a digital carrier system using PCM encoded analog signal.
- A T1 carrier system is time division multiplexes PCM encoded samples from 24 voice band channels for transmission over a single metallic wire pair or optical fiber transmission line.
- Each voice band channel has BW around 300Hz to 3000KHz.

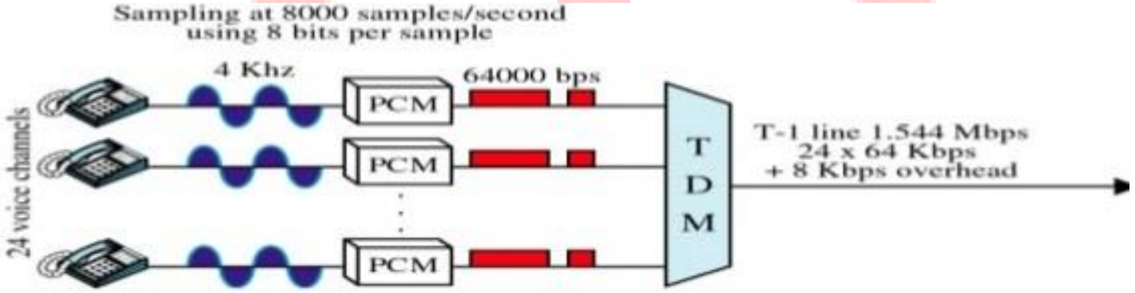


Fig 1: T1 digital system

- A multiplexer is simply a digital switch with 24 independent inputs and one time division multiplexed output.
- The PCM output signals from 24 voice band channels are sequentially selected and connected through the multiplexer to the transmission line.
- With T1 carrier system, there is sampling, encoding and multiplexing of 24 voice band channels.
- Each channel contains an 8-bit PCM code and sampled 8000 times a second.
- Each channel is sampled at same rate but not at same time.
- The figure shows that, each channel is sampled once in each frame, but not at same time.
- Each channel's sample is offset from previous channel's sample by 1/24 of total frame time.
- Therefore one 64Kbps PCM encoded sample is transmitted for each voice band channel during each frame. The line Speed is calculated as:

$$\frac{24\ Channels}{frame} \times \frac{8Bits}{Channel} = 192\text{bits per frame}$$

$$Thus\ \frac{192\ bits}{frame} \times \frac{8000\ frames}{second} = 1.536Mbps$$

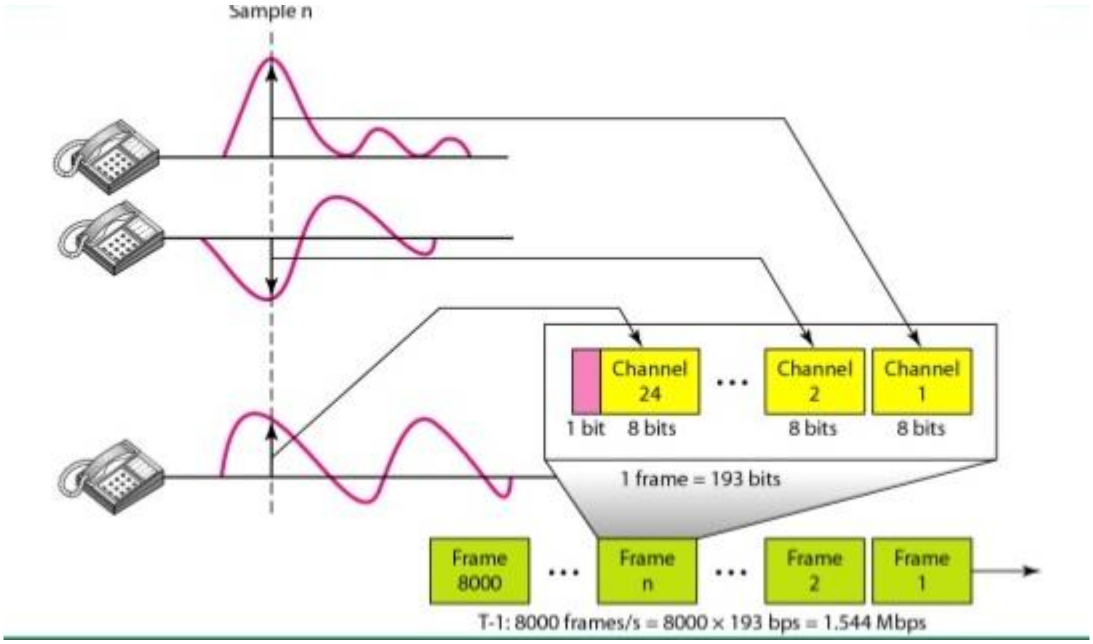


Fig 2: T1 frame structure

- An additional bit (called framing bit) is added to each frame.
- The framing bit occurs once per frame (8000bps rate) and recovered in receiver, where it is used to maintain frame and sample synchronization between TDM transmitter and receiver.
- So each frame contains 193 bits and line speed for T1 digital carrier system is

$$\frac{193\ bits}{frame} \times \frac{8000\ frames}{second} = 1.544Mbps$$

- AMI line coding is used for T1 digital Systems

Synchronous Optical Network (SONET)

The synchronous optical network or SONET is a standardized form of protocol that is used in digital communication between the sender and the receiver. SONET protocol uses fiber optic medium (optical fibers) to transmit a huge amount of data across a large distance. One of the main advantages that a synchronous optical network provides is that it can be used to transfer multiple streams of data simultaneously (at the same time) using optical fibers.

Some of the important points related to SONET are:

- SONET is used in the physical layer of the OSI model for broadband synchronized transmission of data such as voice, video, etc.
- It was developed by Bellcore in the mid-1980s and it was developed for the public telephone network.
- It is used in the North American region.
- SONET is standardized by the American National Standards Institute (ANSI).
- SONET is efficient and costs low for a few channels because of higher transmission rates.
- SONET is somewhat similar to the SDH which is used in regions like Japan and Europe.
- At the higher capabilities, there is a problem with bandwidth efficiency.
- There is more overhead related to the SONET protocol as it is complex to implement and we have to work with multiple channels.
- There is no standard compatible with the SONET protocol.
- Tributary services are used for transporting and switching payloads and for the tributary services, the mux services of SONET are necessary.

Why SONET is Called a Synchronous Network?

Let us now try to understand why SONET is a synchronous network.

In SONET, we have a single Primary Reference Clock (PRC) which handles the transmission timing of signals and the equipment used across the entire network. A typical PRC provides the reference signal for the timing or synchronization of other clocks within a network or section of a network. In particular, the PRC can also provide the reference signal to the slave clock

Synchronous Optical Network (SONET) and Asynchronous Transfer Mode (ATM) are together used to provide the capability for telecommunication to provide high-speed services for both voice and data over the same network.

SONET Network Elements

The various SONET network elements are

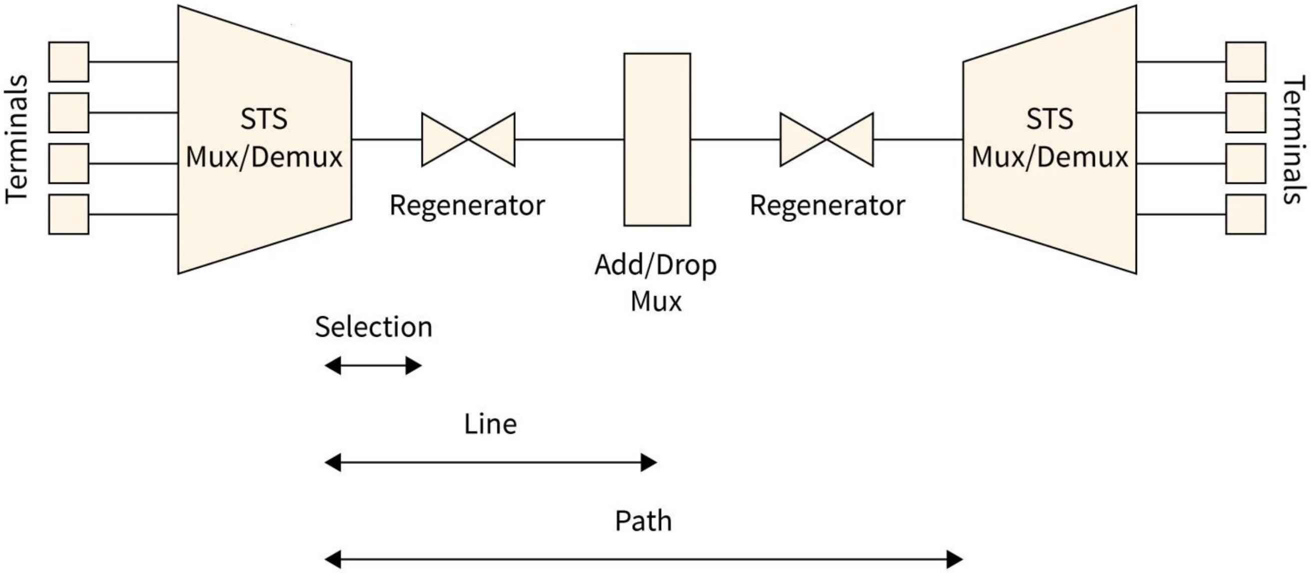
1. **STS Multiplexer:** It is used to perform multiplexing of the digital signals (combine all the different frequencies into a strengthened single signal at the sender's end so that transmission can take place easily) and it converts the electrical signals to optical signals. What are multiplexers? Well, a device that can combine all the different frequencies into a single signal (composite signal) at the sender's end so that transmission can take place easily is called a multiplexer.

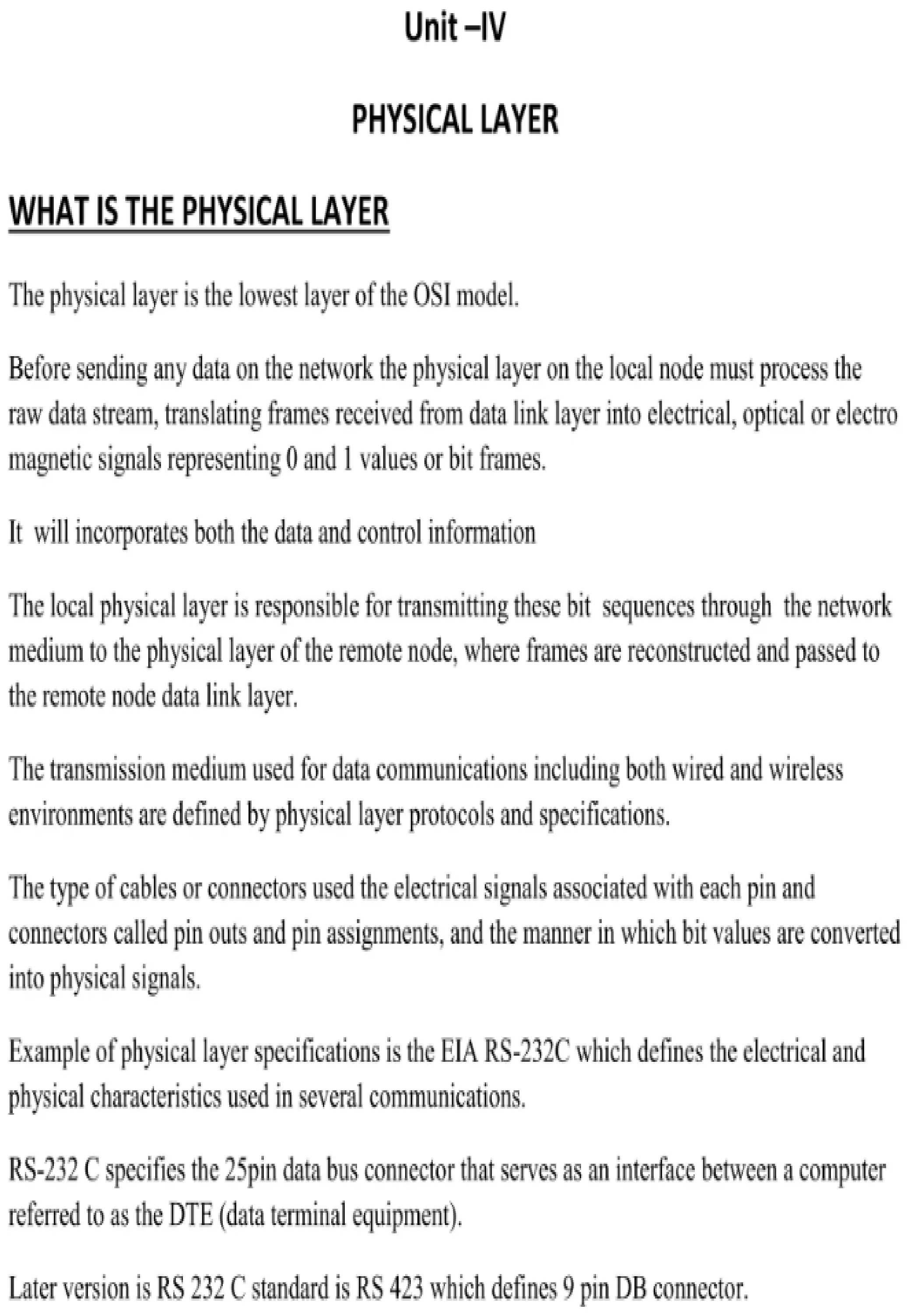
2. **STS Demultiplexer:** The STS Demultiplexer is just opposite to the multiplexer, it performs the de-multiplexing of the digital signals. Along with de-multiplexing, it converts the optical signals back into electrical signals. What are demultiplexers? Similar to the multiplexers, at the receiver's end, we use a device that can do the reverse work which is to extract the individual frequency. Theoretically, we can say that the device that combines the various frequencies into a single composite signal at the sender's end is termed a multiplexer (MUX) and the device that extracts the various frequencies from the composite signal at the receiver's end is termed a de-multiplexer (DEMUX).

3. **Regenerator:** A regenerator is nothing but a repeater that strengthens the provided optical signals. Hence, a regenerator is a device that increases the incoming optical signal and allows them to travel farther than it would have traveled without the regeneration of the signal.

4. **Add/ Drop Multiplexer:** It is a multiplexer that enables the signal to be added or removed from a source. The add or drop multiplexer adds the signals (to be sent to the receiver to create a strong single signal) from several sources to a particular path or removes the unuseful signal from the specified path so that the transmission of signals can take place more smoothly.

.





Unit –IV

PHYSICAL LAYER

WHAT IS THE PHYSICAL LAYER

The physical layer is the lowest layer of the OSI model.

Before sending any data on the network the physical layer on the local node must process the raw data stream, translating frames received from data link layer into electrical, optical or electro magnetic signals representing 0 and 1 values or bit frames.

It will incorporates both the data and control information

The local physical layer is responsible for transmitting these bit sequences through the network medium to the physical layer of the remote node, where frames are reconstructed and passed to the remote node data link layer.

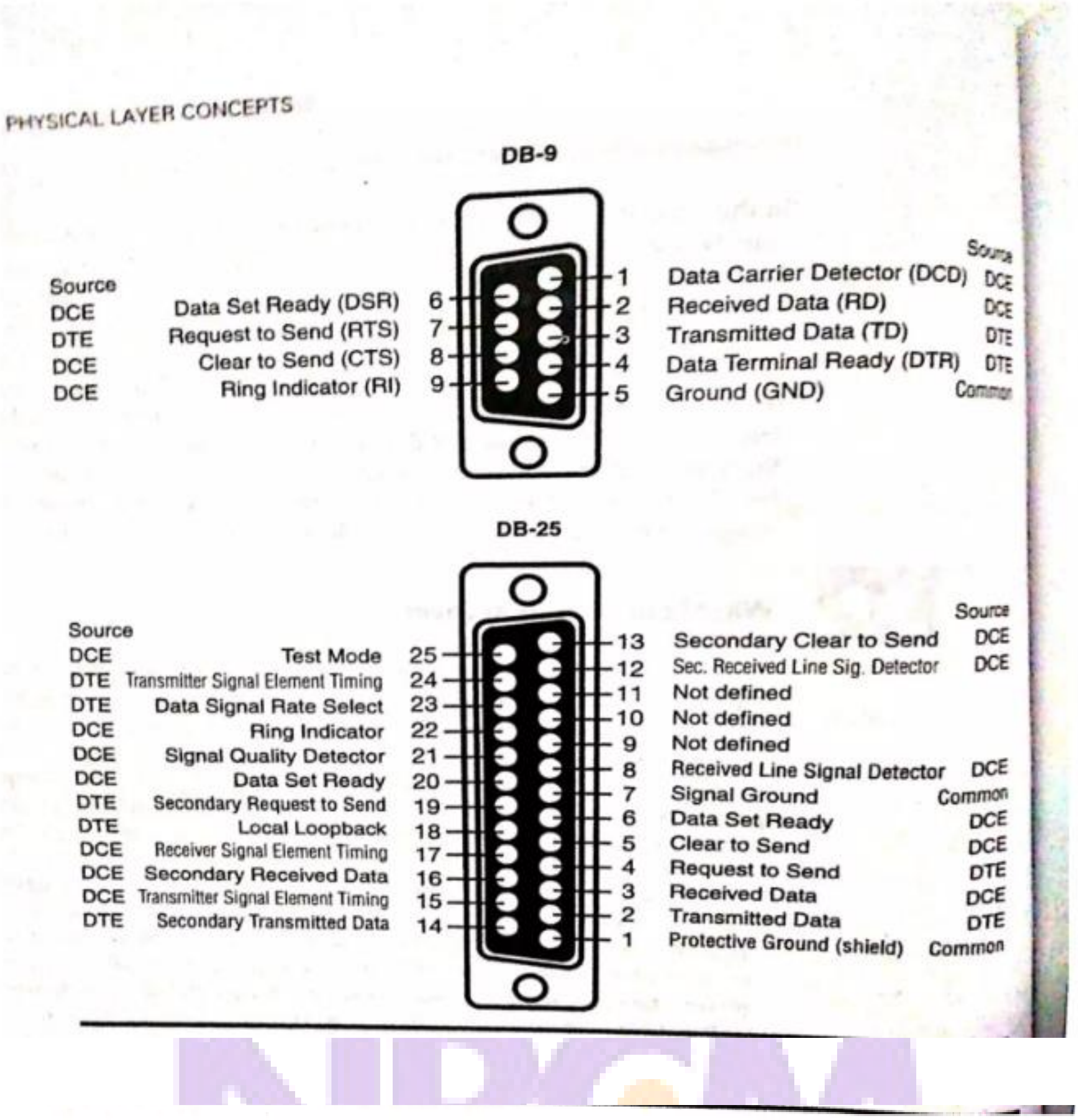
The transmission medium used for data communications including both wired and wireless environments are defined by physical layer protocols and specifications.

The type of cables or connectors used the electrical signals associated with each pin and connectors called pin outs and pin assignments, and the manner in which bit values are converted into physical signals.

Example of physical layer specifications is the EIA RS-232C which defines the electrical and physical characteristics used in several communications.

RS-232 C specifies the 25pin data bus connector that serves as an interface between a computer referred to as the DTE (data terminal equipment).

Later version is RS 232 C standard is RS 423 which defines 9 pin DB connector.


PHYSICAL LAYER CONCEPTS
DB-9
Source
DCE Data Set Ready (DSR) 6
DTE Request to Send (RTS) 7
DCE Clear to Send (CTS) 8
DCE Ring Indicator (RI) 9
Source
1 Data Carrier Detector (DCD) DCE
2 Received Data (RD) DCE
3 Transmitted Data (TD) DTE
4 Data Terminal Ready (DTR) DTE
5 Ground (GND) Common
DB-25
Source
DCE Test Mode 25
DTE Transmitter Signal Element Timing 24
DTE Data Signal Rate Select 23
DCE Ring Indicator 22
DCE Signal Quality Detector 21
DCE Data Set Ready 20
DTE Secondary Request to Send 19
DTE Local Loopback 18
DCE Receiver Signal Element Timing 17
DCE Secondary Received Data 16
DCE Transmitter Signal Element Timing 15
DTE Secondary Transmitted Data 14
Source
13 Secondary Clear to Send DCE
12 Sec. Received Line Sig. Detector DCE
11 Not defined
10 Not defined
9 Not defined
8 Received Line Signal Detector DCE
7 Signal Ground Common
6 Data Set Ready DCE
5 Clear to Send DCE
4 Request to Send DTE
3 Received Data DCE
2 Transmitted Data DTE
1 Protective Ground (shield) Common

The physical and electrical characteristics of a wire:

All physical media regardless of their type share 3 physical elements

Physical characteristics

1.conductor

The conductor serves as a medium for the physical signal.The conductor is composed of copper wire or glass or plastic fibre.

In case of copper wire it can be stranded(composed of several thin wires)

We can measure thickness in terms of gauges.

The lower the gauge thicker the wire. The 22 guage wire is more thicker than 24 guage wire.

We can measure in terms of AWG(American wire guage).

2.Insulator

The insulating material surrounding the conductor.It serves as a barrier to the conductor by preventing the signal from escaping and preventing electrical interference in entering.

Finally the conductor and insulator are encased in a outer sheath or jacket.

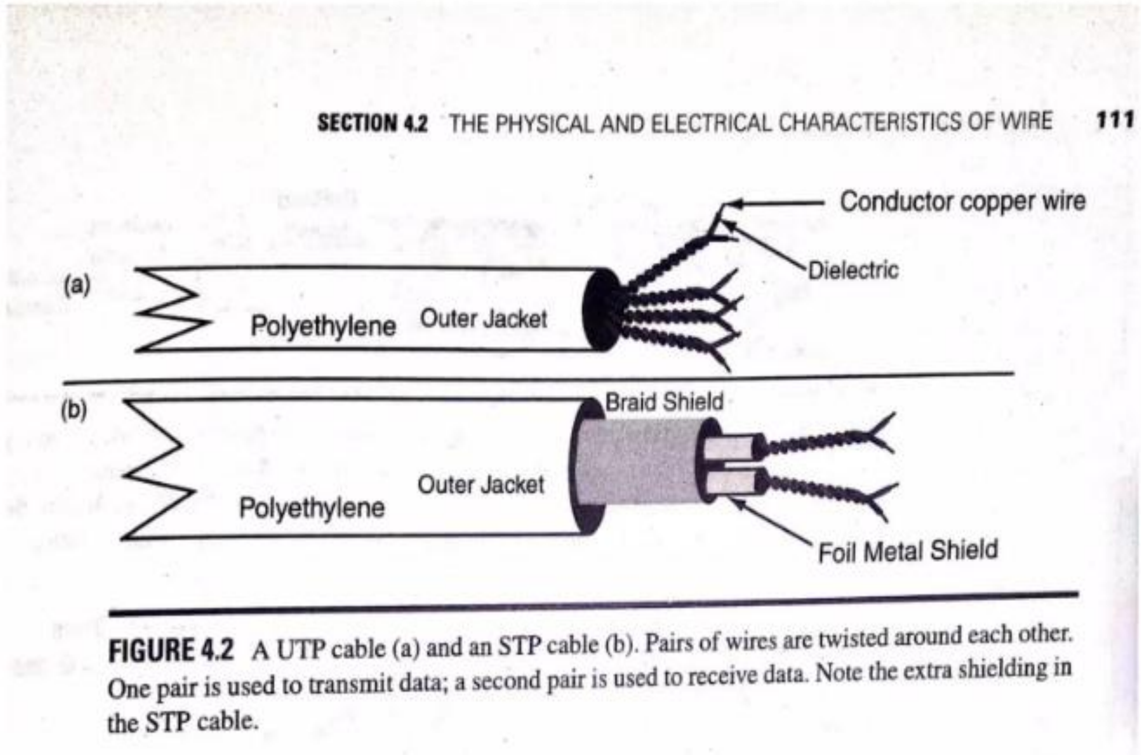
Pvc and Teflon are the materials used as insulating materials.

Teflon is fire resistant ,it takes much time to get into burning point.

The below diagram shows the physical composition of two commonly used network cables:

Unshielded twisted pairs

Shielded twisted pairs.



SECTION 4.2 THE PHYSICAL AND ELECTRICAL CHARACTERISTICS OF WIRE 111

FIGURE 4.2 A UTP cable (a) and an STP cable (b). Pairs of wires are twisted around each other. One pair is used to transmit data; a second pair is used to receive data. Note the extra shielding in the STP cable.

Twisted pairs

The twisted pairs consists of atleast 2 insulated copper wires that have been twisted together.

shielded twisted pairs

In STP because of braided shield and foil metal shield it is less susceptible to electrical interference and noise.

Twisted-pair is a type of cabling that is used for telephone communications and most modern Ethernet networks.

A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs.

There are two basic types, shielded twisted-pair (STP) and unshielded twisted-pair (UTP).

Unshieled twisted pairs

Consists of 4 pairs (8 wires) of insulated copper wires typically about 1 mm thick.

The wires are twisted together in a helical form.

Twisting reduces the interference between pairs of wires.

High bandwidth and High attenuation channel.

Flexible and cheap cable.

Category rating based on number of twists per inch and the material used

CAT 3, CAT 4, CAT 5, Enhanced CAT 5 and now CAT 6.

Coxial cables

Coaxial cable is a copper-cored cable surrounded by a heavy shielding and is used to connect computers in a network.

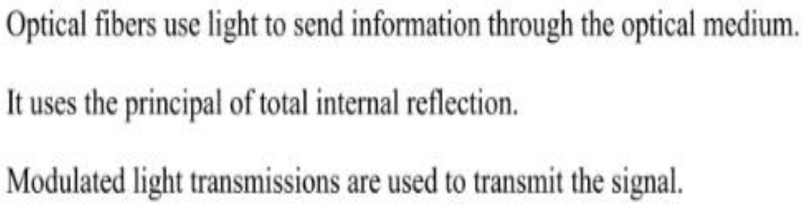
Outer conductor shields the inner conductor from picking up stray signal from the air.

High bandwidth but lossy channel.

Repeater is used to regenerate the weakened signals.

Fibre optic cables.

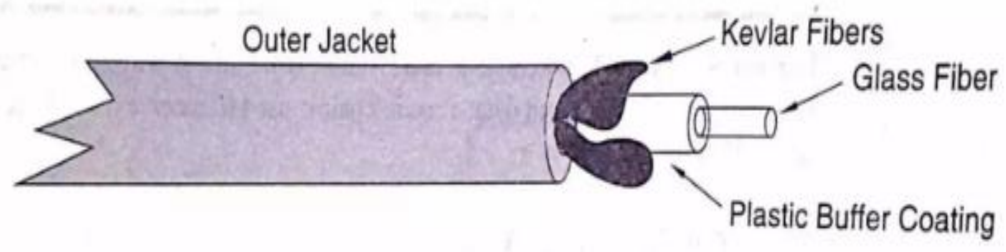
fibre optic cable consists of a glass fibre covered by a plastic buffer coating and surrounded by Kevlar fibres.The Kevlar fibre gives the cable its strength.These are used for bullet proof vests. And combat helmets.

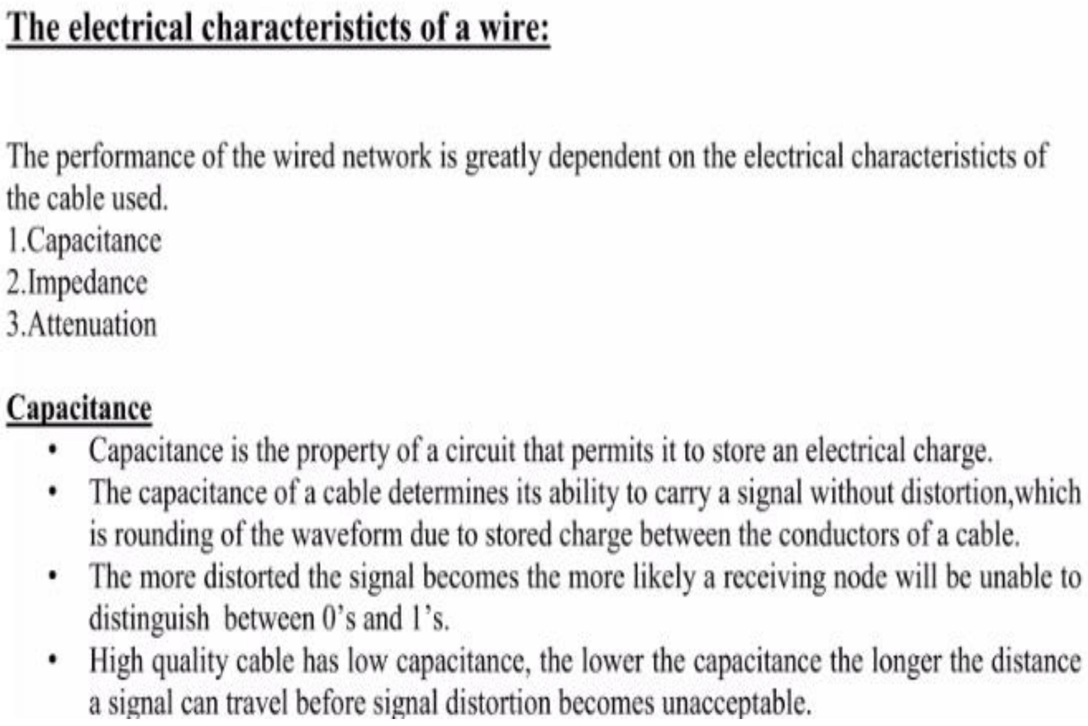


Optical fibers use light to send information through the optical medium.

It uses the principal of total internal reflection.

Modulated light transmissions are used to transmit the signal.





The electrical characteristicts of a wire:

The performance of the wired network is greatly dependent on the electrical characteristicts of the cable used.
1.Capacitance
2.Impedance
3.Attenuation

Capacitance

- Capacitance is the property of a circuit that permits it to store an electrical charge.
- The capacitance of a cable determines its ability to carry a signal without distortion,which is rounding of the waveform due to stored charge between the conductors of a cable.
- The more distorted the signal becomes the more likely a receiving node will be unable to distinguish between 0's and 1's.
- High quality cable has low capacitance, the lower the capacitance the longer the distance a signal can travel before signal distortion becomes unacceptable.

- Network cables can have low characteristicts capacitance per meter,the overall capacitance of a cable increases as the cable gets longer.
- Because of noise and other problems in the transmission, a maximum cable length of about 100m exists for for unshielded twisted pairs network cable.

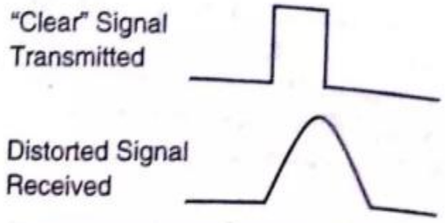


FIGURE 4.5 Capacitance eventually will distort a transmitted signal. Source: adapted & Chorey, 1991a.

Impedance

Impedance is a measure of the opposition to the flow of electrical current in an alternating current circuit.

It is measured in ohms.

Impedance is a function of capacitance ,resistance and inductance.

Impedance mismatches ,caused by mixing cables of different types with different characteristicts impedances,can result in signal distortion.

For example token ring network cable requires 150Ωof impedance .

Ethernet and twisted pair networks want 85-111 Ω

Attenuation

Attenuation is decrease in signal strength.whcich occurs as the signal travels through a circuit or along a cable.

The longer the cable the greater the attenuation.

The higher the frequency the greater the attenuation .

Different types of cables also subject to different amounts of attenuation.

In the twisted pairs the attenuation rises sharply ,as the signal frequency increases.

In the coaxial cables it rises less sharply as frequency increases.

It is measured in decibels of signal loss.

While selecting a cable,you should a type that has low mesure of attenuation for the network speeds and distances involved.

Signal quality is effected by the combination of the attenuation and capacitance.

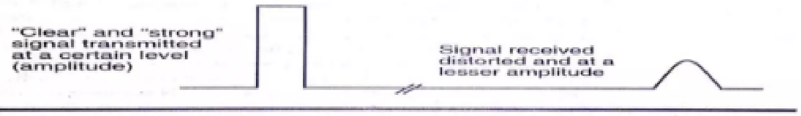

"Clear" and "strong" signal transmitted at a certain level (amplitude)
Signal received distorted and at a lesser amplitude

FIGURE 4.6 The combined effects of capacitance and attenuation result in a signal that is received distorted and weaker than what it was when transmitted. This can severely impact the performance of a network. Source: adapted from Leeds & Chorey, 1991a.

COPPER MEDIA

It consists of

1.STP

2.UTP

3.IBM CABLE

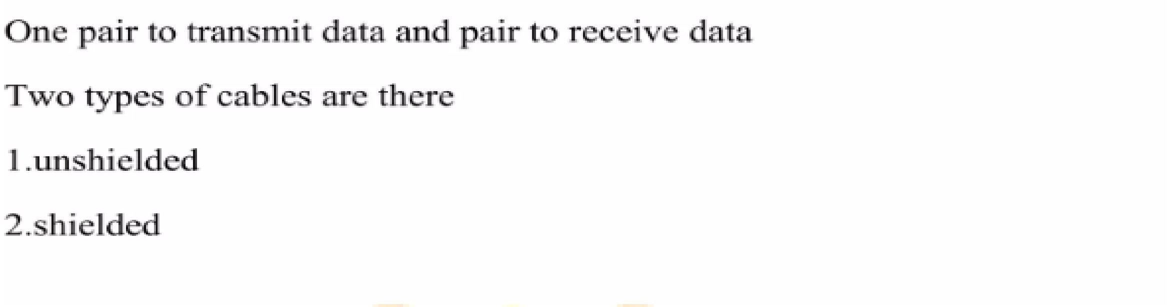
4.COAXIAL CABLE

UNSHIELDED AND SHIELDED TWISTED PAIR CABLE

Twisted pairs are the most popular type of cable used in networks today.

Twisted pair cable consists of 2 insulated copper wires that have been twisted together.

Data transmission requires 4 wires.



One pair to transmit data and pair to receive data

Two types of cables are there

1.unshielded

2.shielded

Standards of the UTP ans STP are provided by EIA/TIA-568 which is north american standard used world wide.

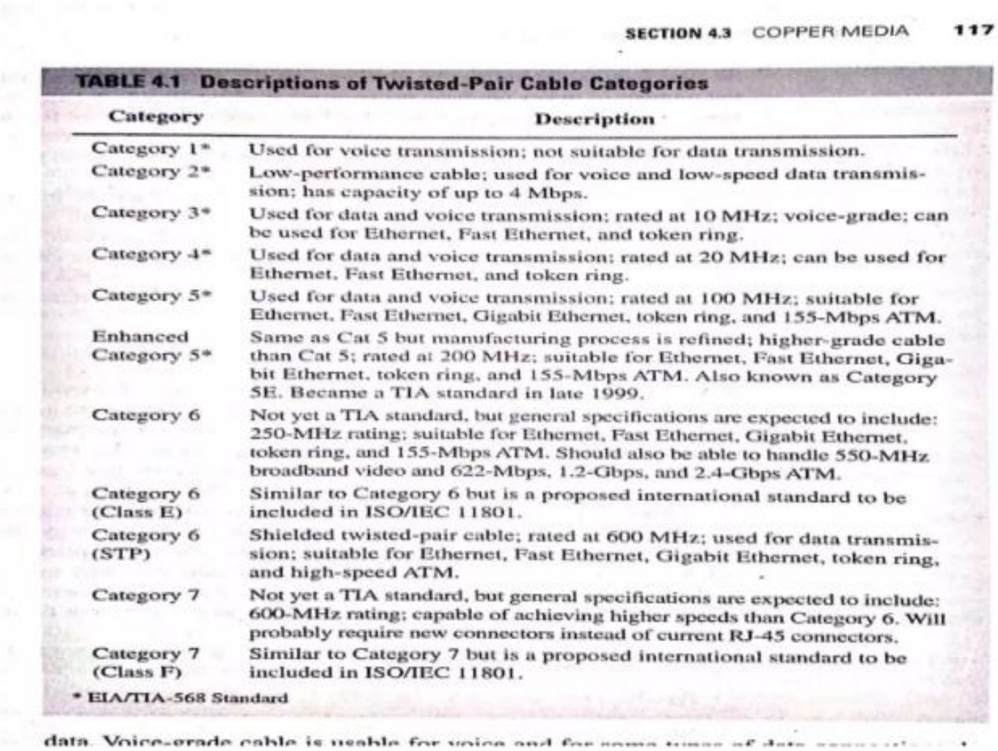


TABLE 4.1 Descriptions of Twisted-Pair Cable Categories

Category	Description
Category 1*	Used for voice transmission; not suitable for data transmission.
Category 2*	Low-performance cable; used for voice and low-speed data transmission; has capacity of up to 4 Mbps.
Category 3*	Used for data and voice transmission; rated at 10 MHz; voice-grade; can be used for Ethernet, Fast Ethernet, and token ring.
Category 4*	Used for data and voice transmission; rated at 20 MHz; can be used for Ethernet, Fast Ethernet, and token ring.
Category 5*	Used for data and voice transmission; rated at 100 MHz; suitable for Ethernet, Fast Ethernet, Gigabit Ethernet, token ring, and 155-Mbps ATM.
Enhanced Category 5*	Same as Cat 5 but manufacturing process is refined; higher-grade cable than Cat 5; rated at 200 MHz; suitable for Ethernet, Fast Ethernet, Gigabit Ethernet, token ring, and 155-Mbps ATM. Also known as Category 5E. Became a TIA standard in late 1999.
Category 6	Not yet a TIA standard, but general specifications are expected to include: 250-MHz rating; suitable for Ethernet, Fast Ethernet, Gigabit Ethernet, token ring, and 155-Mbps ATM. Should also be able to handle 550-MHz broadband video and 622-Mbps, 1.2-Gbps, and 2.4-Gbps ATM.
Category 6 (Class E)	Similar to Category 6 but is a proposed international standard to be included in ISO/IEC 11801.
Category 6 (STP)	Shielded twisted-pair cable; rated at 600 MHz; used for data transmission; suitable for Ethernet, Fast Ethernet, Gigabit Ethernet, token ring, and high-speed ATM.
Category 7	Not yet a TIA standard, but general specifications are expected to include: 600-MHz rating; capable of achieving higher speeds than Category 6. Will probably require new connectors instead of current RJ-45 connectors.
Category 7 (Class F)	Similar to Category 7 but is a proposed international standard to be included in ISO/IEC 11801.

* EIA/TIA-568 Standard

data. Voice-grade cable is usable for voice and for some types of data

Categories 3 and 5 mostly used for voice transmission

UTP poses two main problems in data transmission at the higher frequencies

1. cross talk

2. attenuation.

The combined effects of cross talk and distortion results in the irregular variation in the shape or timing of a signal.

This irregular variation is called jitter.

Jitter is mainly caused by shielded and unshielded cable.

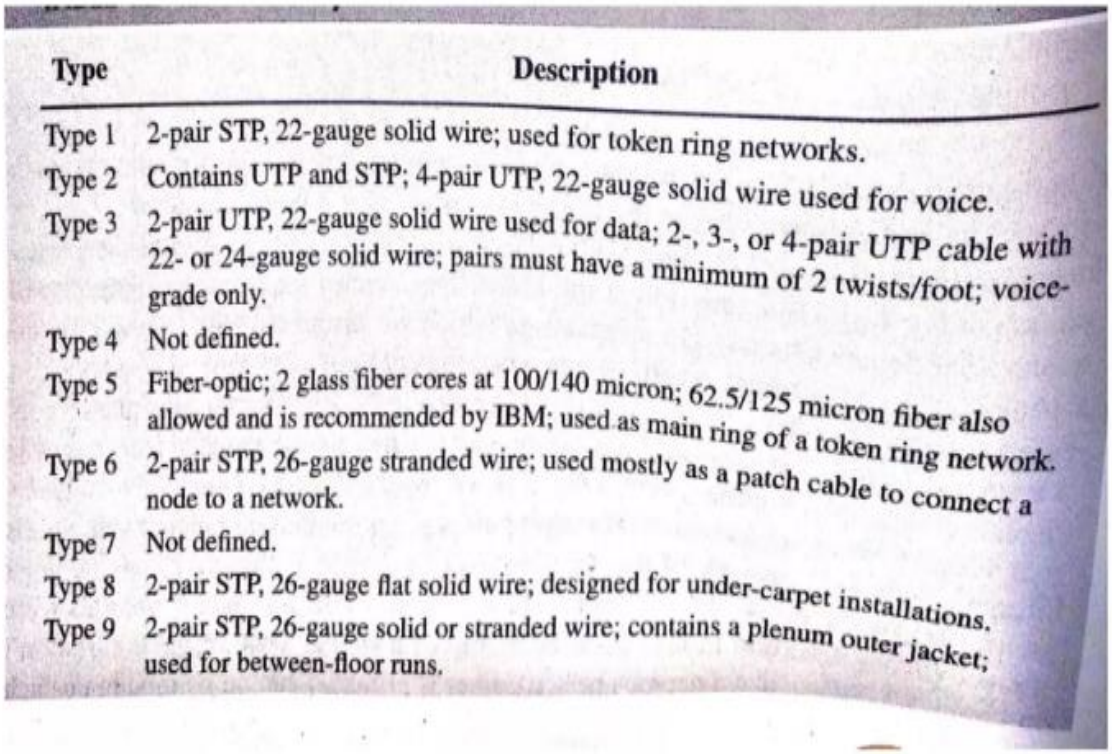
IBM CABLE

IBM has its own classification cable, the IBM cable system which specifies nine cable types.

TYPE:

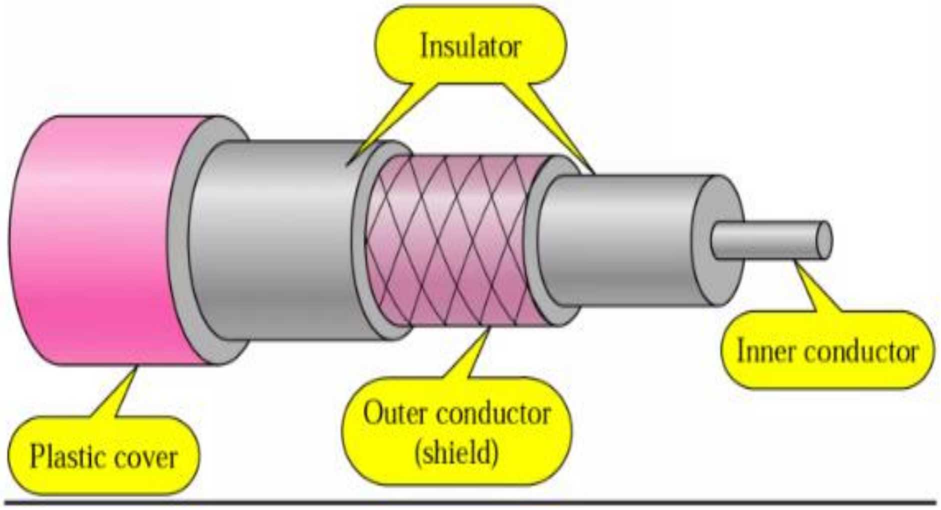
It is a grouping of categories and fiber optic cables in a bundle based up on which type is being conducted.

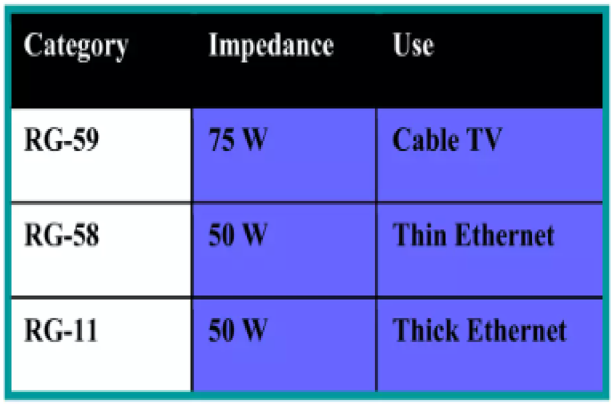
A category is an EIA specification for the cables construction.



Type	Description
Type 1	2-pair STP, 22-gauge solid wire; used for token ring networks.
Type 2	Contains UTP and STP; 4-pair UTP, 22-gauge solid wire used for voice.
Type 3	2-pair UTP, 22-gauge solid wire used for data; 2-, 3-, or 4-pair UTP cable with 22- or 24-gauge solid wire; pairs must have a minimum of 2 twists/foot; voice-grade only.
Type 4	Not defined.
Type 5	Fiber-optic; 2 glass fiber cores at 100/140 micron; 62.5/125 micron fiber also allowed and is recommended by IBM; used as main ring of a token ring network.
Type 6	2-pair STP, 26-gauge stranded wire; used mostly as a patch cable to connect a node to a network.
Type 7	Not defined.
Type 8	2-pair STP, 26-gauge flat solid wire; designed for under-carpet installations.
Type 9	2-pair STP, 26-gauge solid or stranded wire; contains a plenum outer jacket; used for between-floor runs.

Coaxial cables





Category	Impedance	Use
RG-59	75 W	Cable TV
RG-58	50 W	Thin Ethernet
RG-11	50 W	Thick Ethernet

Another type of copper cable is coaxial cable, In computer networking, coax is described as either thick (or) thin.

Thick coaxial is used as the medium for thick Ethernet which is knows as IEEE 802.3 10 Base5

Thin coaxial cable is used as medium for "Thin Ethernet" which is known as IEEE 802.3 10 Base2

In analog coaxial networks such as residential cable television networks, cable such as RG-9 may be used

RG-59 with an impedance of 75 OHMS is used for home TV cable but looks almost same as RG-58

All the cables are not same, we should select the right one for the types of network equipment being considered for use

A base band network transmits the digital signals directly without modulating their transmission

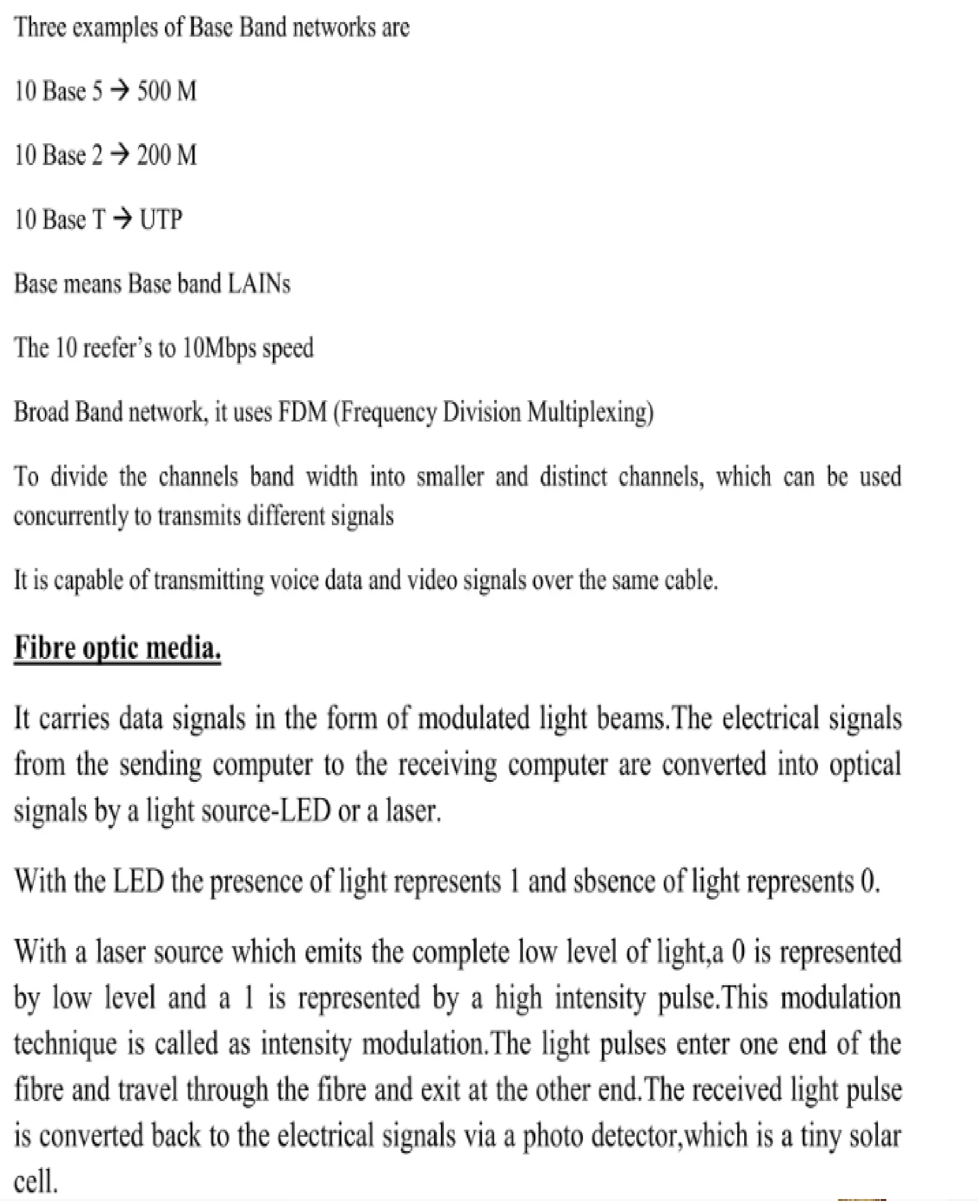
A base band network is capable of transmitting only a single stream of data, That means the transmission medium uses the entire band width to carry a single signal

It doesn't mean however that the channel cannot be shared

Using multiplexing techniques such as TDM, nodes connected to a base band network can share the medium but they can only transmit when the channel is not busy.

The transmission media of a base band network can include twisted pair cable, coaxial cable and fiber optic cable.

Various topologies are also available including star, ring and bus



Three examples of Base Band networks are

10 Base 5 → 500 M

10 Base 2 → 200 M

10 Base T → UTP

Base means Base band LAINs

The 10 reefer's to 10Mbps speed

Broad Band network, it uses FDM (Frequency Division Multiplexing)

To divide the channels band width into smaller and distinct channels, which can be used concurrently to transmits different signals

It is capable of transmitting voice data and video signals over the same cable.

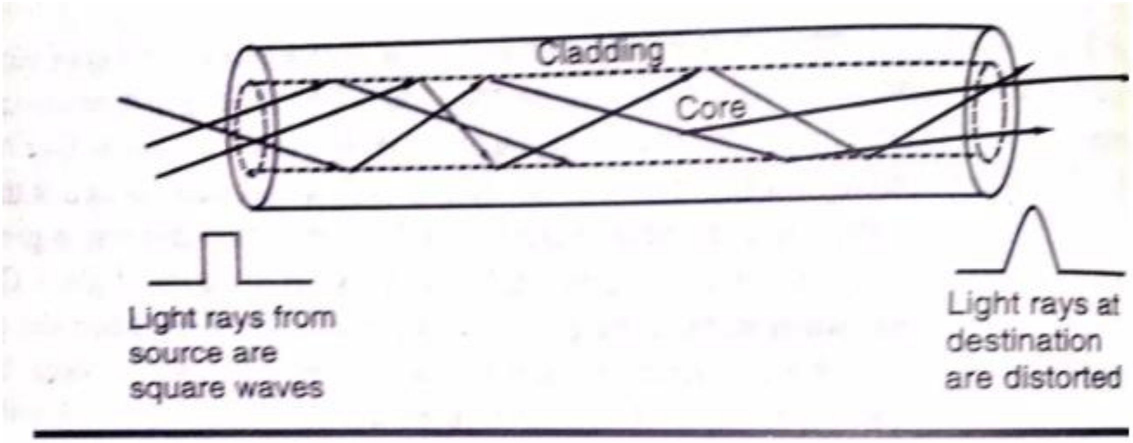
Fibre optic media.

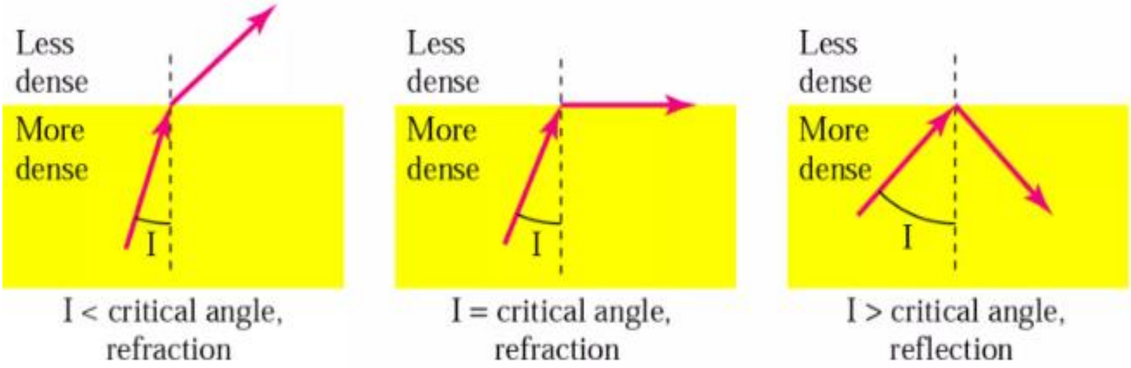
It carries data signals in the form of modulated light beams.The electrical signals from the sending computer to the receiving computer are converted into optical signals by a light source-LED or a laser.

With the LED the presence of light represents 1 and sbsence of light represents 0.

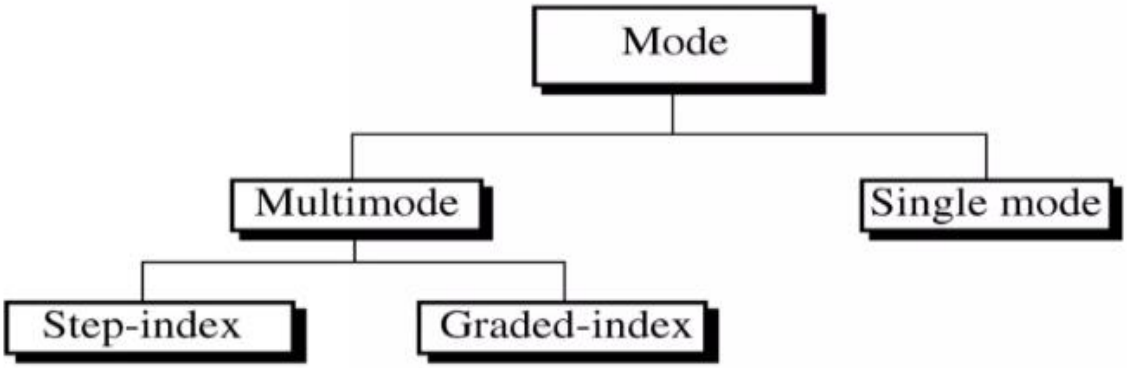
With a laser source which emits the complete low level of light,a 0 is represented by low level and a 1 is represented by a high intensity pulse.This modulation technique is called as intensity modulation.The light pulses enter one end of the fibre and travel through the fibre and exit at the other end.The received light pulse is converted back to the electrical signals via a photo detector,which is a tiny solar cell.

Physical Layer Concepts:


Cladding
Core
Light rays from source are square waves
Light rays at destination are distorted


Less dense
More dense
I
I < critical angle, refraction
Less dense
More dense
I
I = critical angle, refraction
Less dense
More dense
I
I > critical angle, reflection

The diagram shows the properties of light based on total internal reflection.



Multimode

•Multimode is so named because multiple beams from a light source move through the core in different paths

- In multimode **step-index fiber**, the density of the core remains constant from the center to the edges.

•A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding

•step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

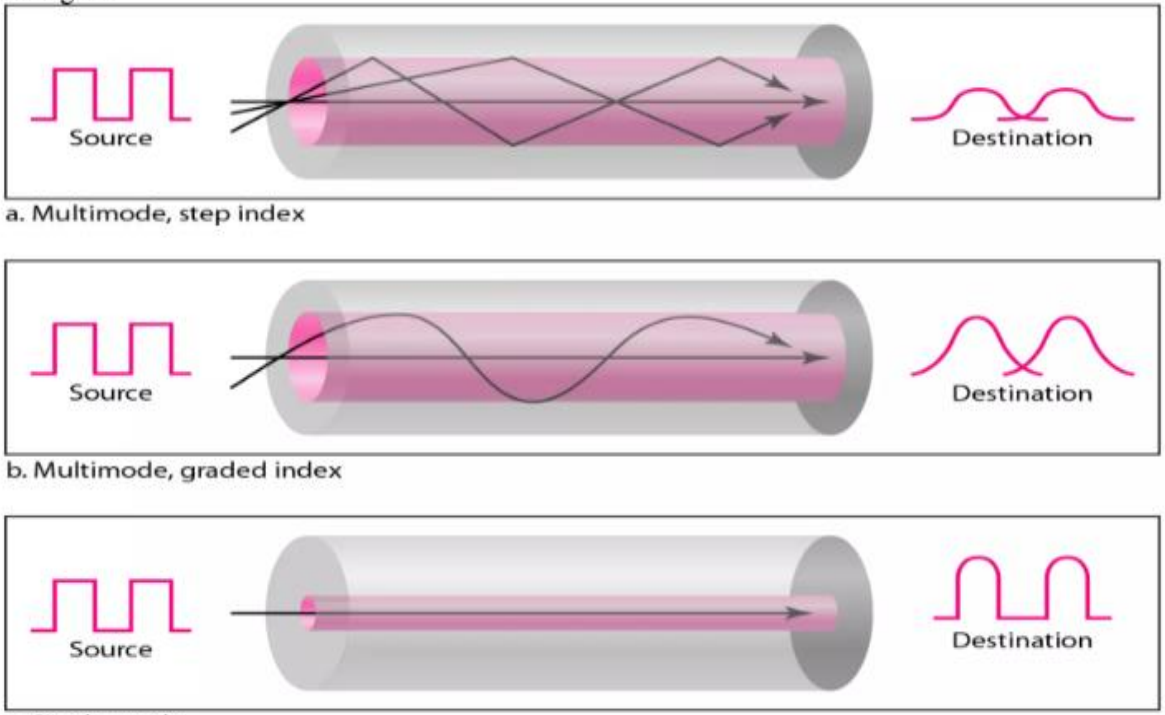
multimode **graded-index fiber**, decreases this distortion of the signal through the cable

•A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.

Single-Mode

•Single-mode uses step-index fiber and a highly focused source of light

- that limits beams to a small range of angles, all close to the horizontal
- propagation of different beams is almost identical, and delays are negligible.
- All the beams arrive at the destination "together" and can be recombined with little distortion to the signal .



a. Multimode, step index

b. Multimode, graded index

c. Single mode

Applications

•Fiber-optic cable is often found in **backbone networks**

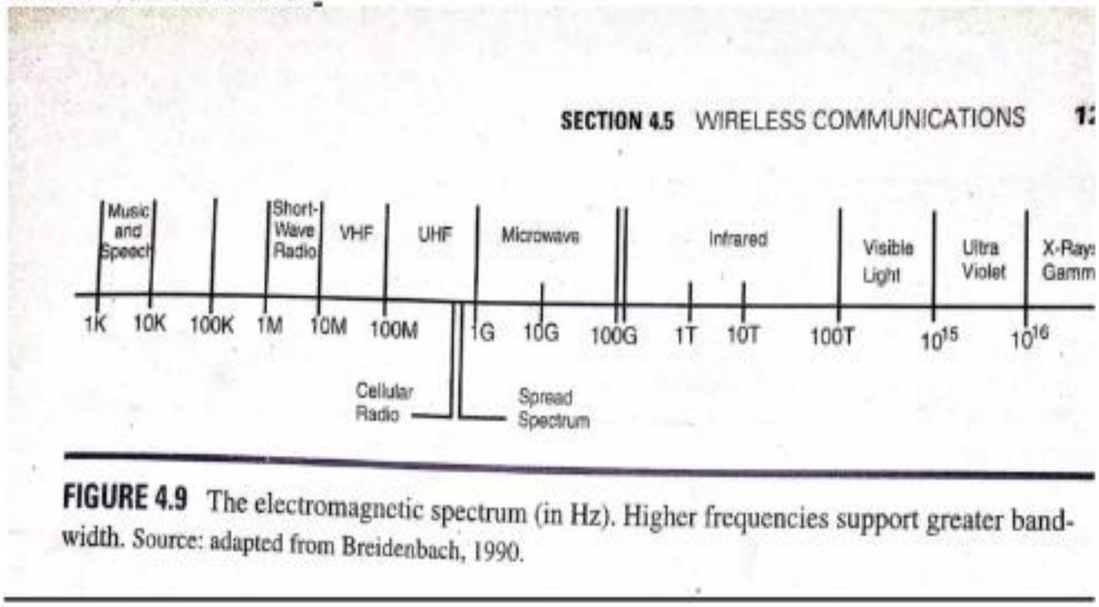
•cable TV companies use a combination of **optical fiber and coaxial cable**, thus creating a hybrid network

•Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable .

Wireless communications

In wireless communications signals travels through space instead of through a physical cable.There are 2 general types of wireless communications are there

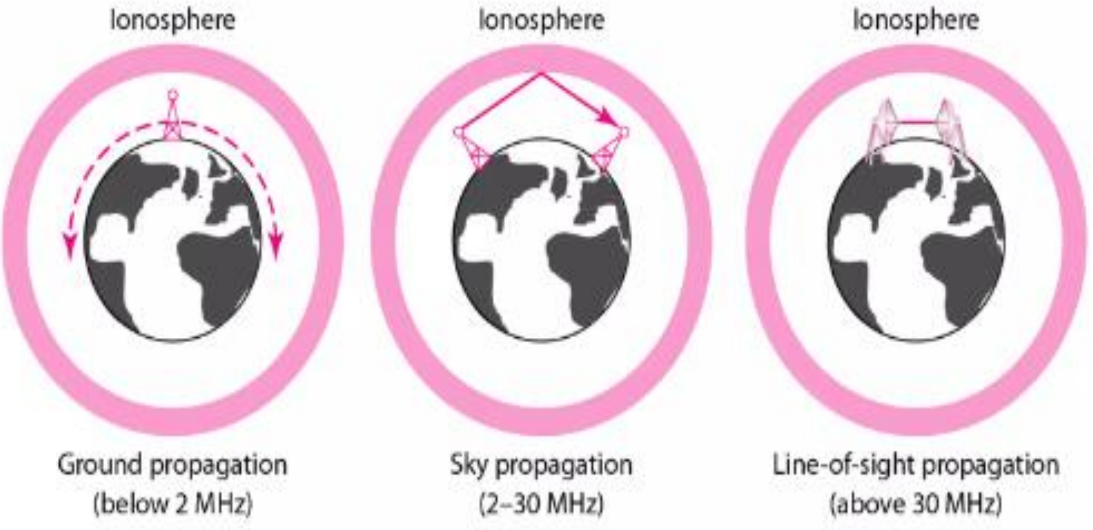
1.radio transmission
2.Infra red transmission.



SECTION 4.5 WIRELESS COMMUNICATIONS 1:

FIGURE 4.9 The electromagnetic spectrum (in Hz). Higher frequencies support greater bandwidth. Source: adapted from Breidenbach, 1990.

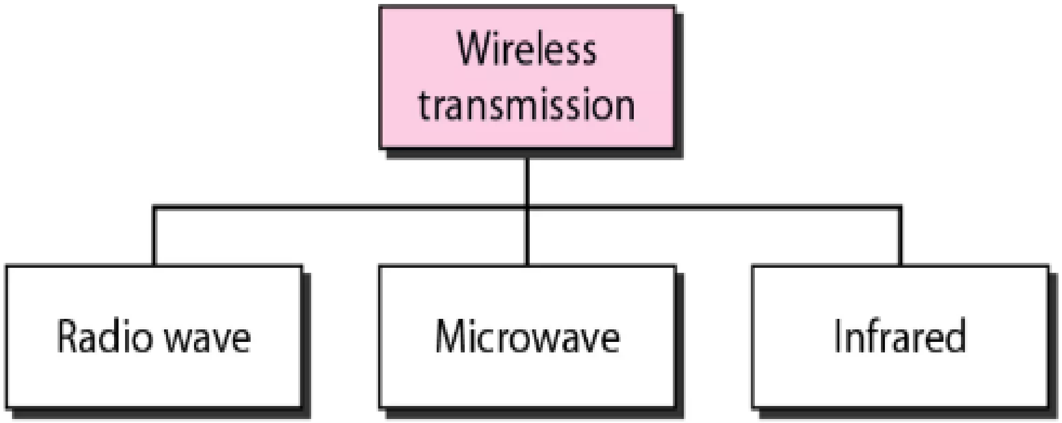
Propagation Methods



Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation.

Propagation Methods

- In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth
- In sky propagation, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to earth.
- 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.

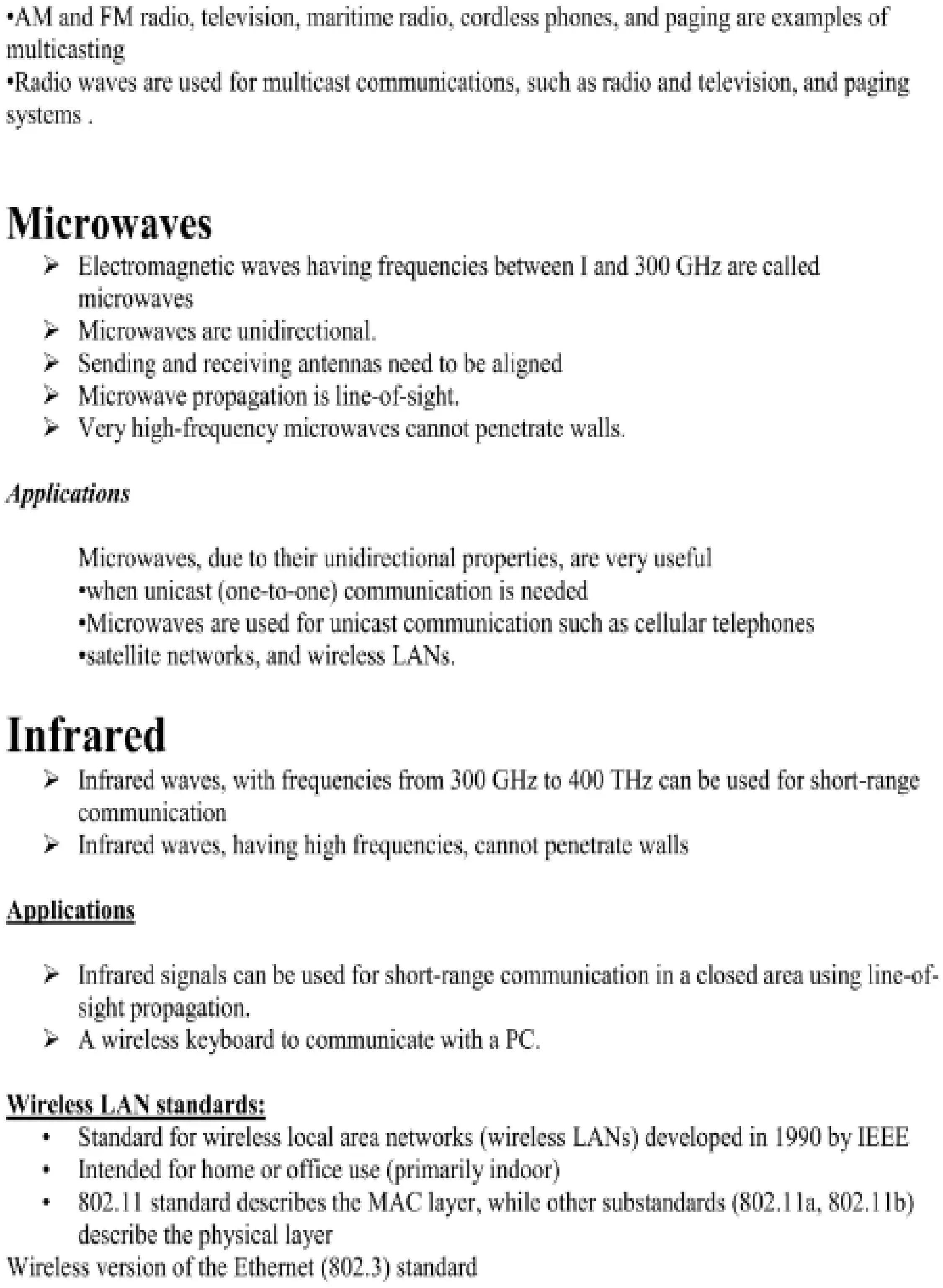


Radio Waves

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are called radio waves.
- Radio waves, for the most part, are omni directional.
- When an antenna transmits radio waves, they are propagated in all directions
- The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency
- Radio waves, particularly those of low and medium frequencies, can penetrate walls.

Applications

Applications:



•AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting
•Radio waves are used for multicast communications, such as radio and television, and paging systems .

Microwaves

- Electromagnetic waves having frequencies between I and 300 GHz are called microwaves
- Microwaves are unidirectional.
- Sending and receiving antennas need to be aligned
- Microwave propagation is line-of-sight.
- Very high-frequency microwaves cannot penetrate walls.

Applications

Microwaves, due to their unidirectional properties, are very useful
•when unicast (one-to-one) communication is needed
•Microwaves are used for unicast communication such as cellular telephones
•satellite networks, and wireless LANs.

Infrared

- Infrared waves, with frequencies from 300 GHz to 400 THz can be used for short-range communication
- Infrared waves, having high frequencies, cannot penetrate walls

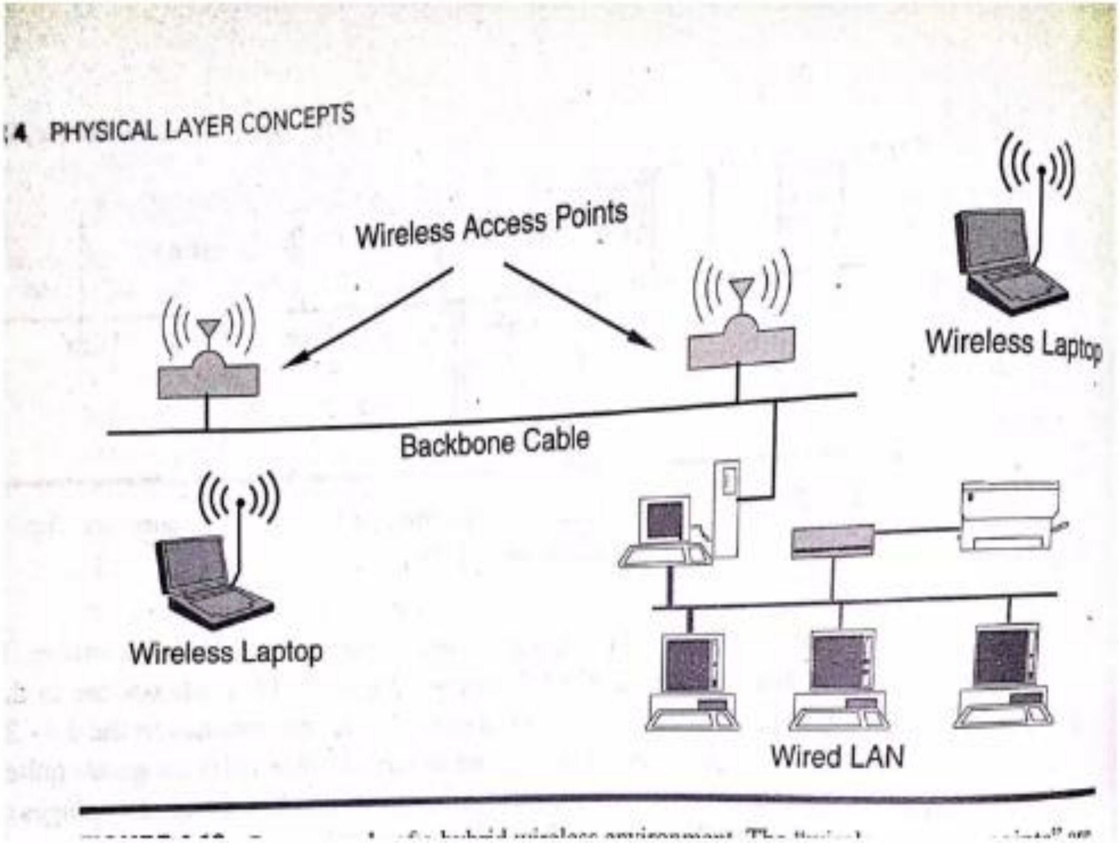
Applications

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.
- A wireless keyboard to communicate with a PC.

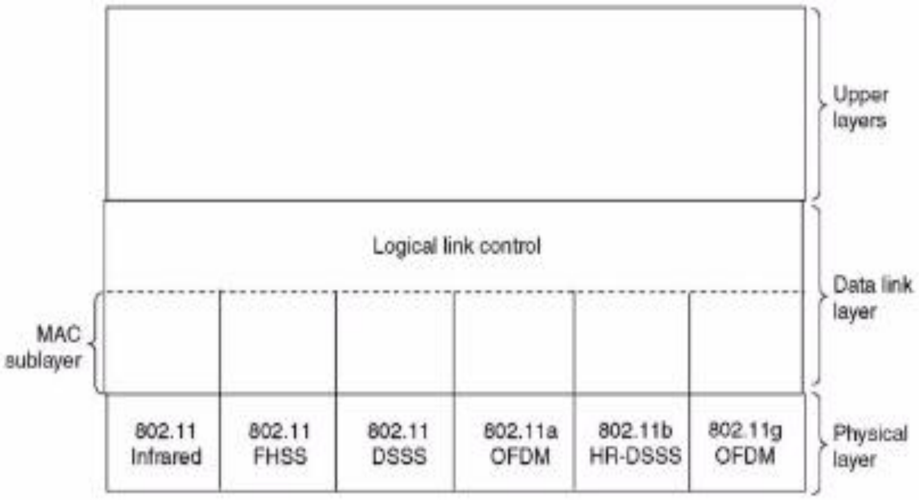
Wireless LAN standards:

- Standard for wireless local area networks (wireless LANs) developed in 1990 by IEEE
- Intended for home or office use (primarily indoor)
- 802.11 standard describes the MAC layer, while other substandards (802.11a, 802.11b) describe the physical layer

Wireless version of the Ethernet (802.3) standard



- ***Base Station*** :: all communication through an ***Access Point*** **(AP)** {note hub topology}. Other nodes can be fixed or mobile.
- ***Infrastructure Wireless*** :: AP is connected to the wired Internet.
- ***Ad Hoc Wireless*** :: wireless nodes communicate directly with one another.
- ***MANETs*** **(Mobile Ad Hoc Networks) ::** ad hoc nodes are mobile.



- Physical layer conforms to OSI (five options)
  - 1997: **802.11** infrared, FHSS, DSSS {FHSS and DSSS run in the 2.4GHz band}
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
- **802.11** ***Infrared***
  - Two capacities: **1 Mbps or 2 Mbps**.
  - Range is 10 to 20 meters and cannot penetrate walls.
  - Does not work outdoors.
- **802.11** ***FHSS*** **(*Frequence Hopping Spread Spectrum*)**
  - **The main issue is *multipath fading*.**
  - ***[P&D] The idea behind spread spectrum is to spread the signal over a wider frequency to minimize the interference from other devices.***
  - 79 non-overlapping channels, each 1 Mhz wide at low end of 2.4 GHz ISM band.
  - The same pseudo-random number generator used by all stations to start the hopping process.
  - Dwell time: min. time on channel before hopping (400msec).
- **802.11** ***DSSS*** **(*Direct Sequence Spread Spectrum*)**
  - ***The main idea is to represent each bit in the frame by multiple bits in the transmitted signal (i.e., it sends the XOR of that bit and n random bits).***
  - Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Tanenbaum sec. 2.6.2).
  - Each bit transmitted using an 11-bit chipping Barker sequence, PSK at 1Mbaud.
  - This yields a capacity of 1 or 2 Mbps.

Satellite communications:

- Two Stations on Earth want to communicate through radio broadcast but are too far away to use conventional means.
- The two stations can use a satellite as a relay station for their communication
- One **Earth Station** sends a transmission to the satellite. This is called a **Uplink**.
- The satellite **Transponder** converts the signal and sends it down to the second earth station. This is called a **Downlink**.

84 PHYSICAL LAYER CONCEPTS

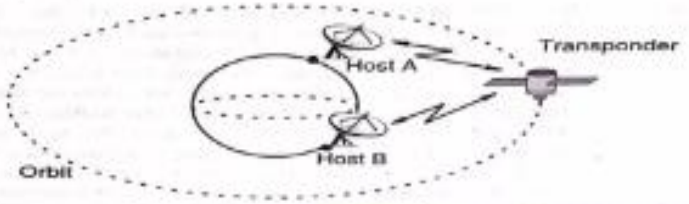
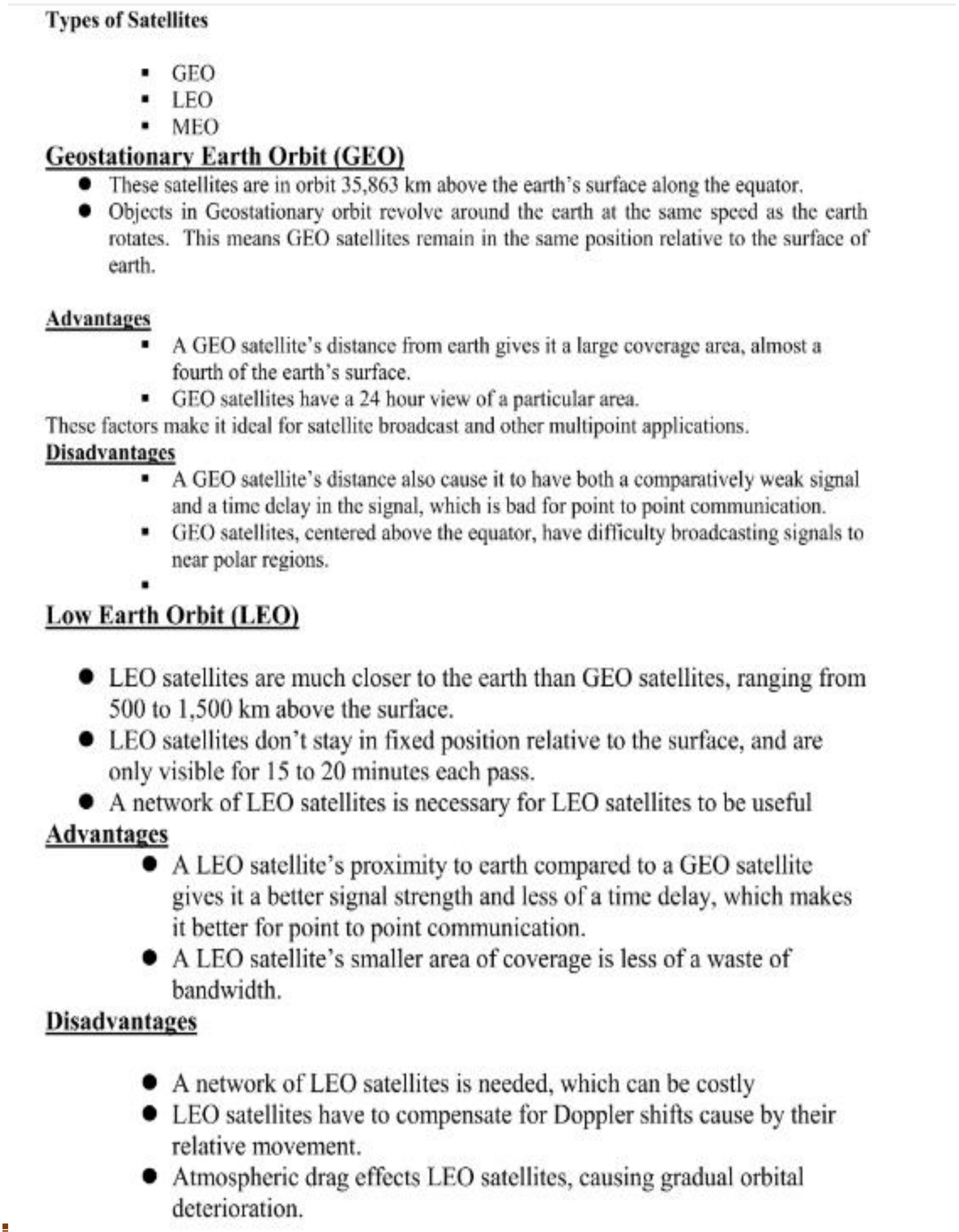


FIGURE 4.11 A satellite communication system. The transponder, a type of repeater, listens to some part of the spectrum. When it hears an incoming signal, it amplifies the signal and then rebroadcasts it at a different frequency. The downward signals can cover a large or narrow area.



Types of Satellites

- GEO
- LEO
- MEO

Geostationary Earth Orbit (GEO)

- These satellites are in orbit 35,863 km above the earth's surface along the equator.
- Objects in Geostationary orbit revolve around the earth at the same speed as the earth rotates. This means GEO satellites remain in the same position relative to the surface of earth.

Advantages

- A GEO satellite's distance from earth gives it a large coverage area, almost a fourth of the earth's surface.
- GEO satellites have a 24 hour view of a particular area.

These factors make it ideal for satellite broadcast and other multipoint applications.

Disadvantages

- A GEO satellite's distance also cause it to have both a comparatively weak signal and a time delay in the signal, which is bad for point to point communication.
- GEO satellites, centered above the equator, have difficulty broadcasting signals to near polar regions.

Low Earth Orbit (LEO)

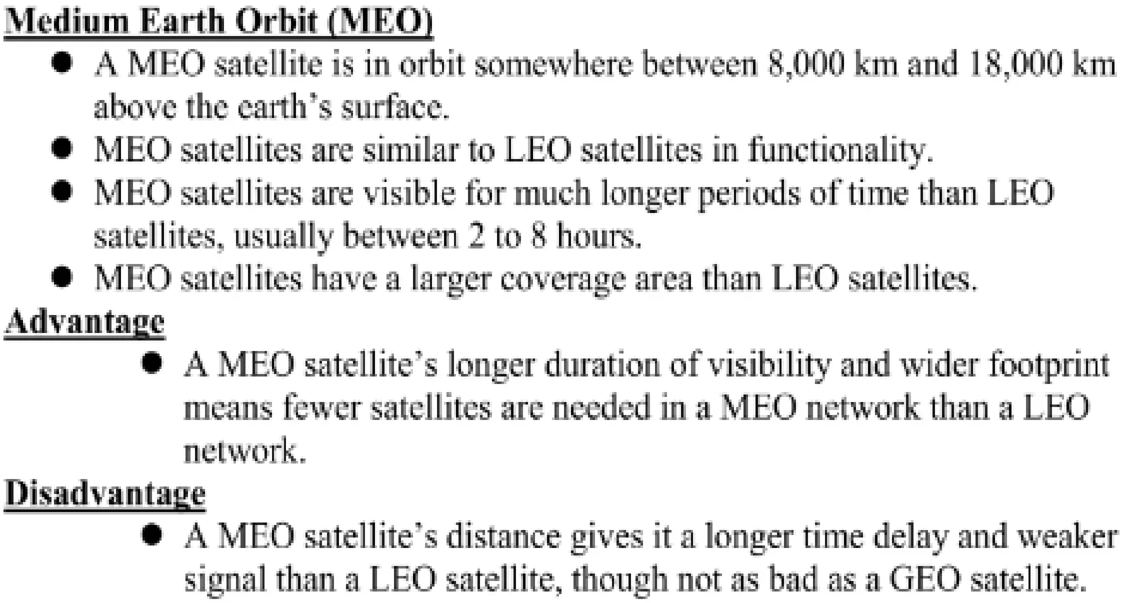
- LEO satellites are much closer to the earth than GEO satellites, ranging from 500 to 1,500 km above the surface.
- LEO satellites don't stay in fixed position relative to the surface, and are only visible for 15 to 20 minutes each pass.
- A network of LEO satellites is necessary for LEO satellites to be useful

Advantages

- A LEO satellite's proximity to earth compared to a GEO satellite gives it a better signal strength and less of a time delay, which makes it better for point to point communication.
- A LEO satellite's smaller area of coverage is less of a waste of bandwidth.

Disadvantages

- A network of LEO satellites is needed, which can be costly
- LEO satellites have to compensate for Doppler shifts cause by their relative movement.
- Atmospheric drag effects LEO satellites, causing gradual orbital deterioration.



Medium Earth Orbit (MEO)

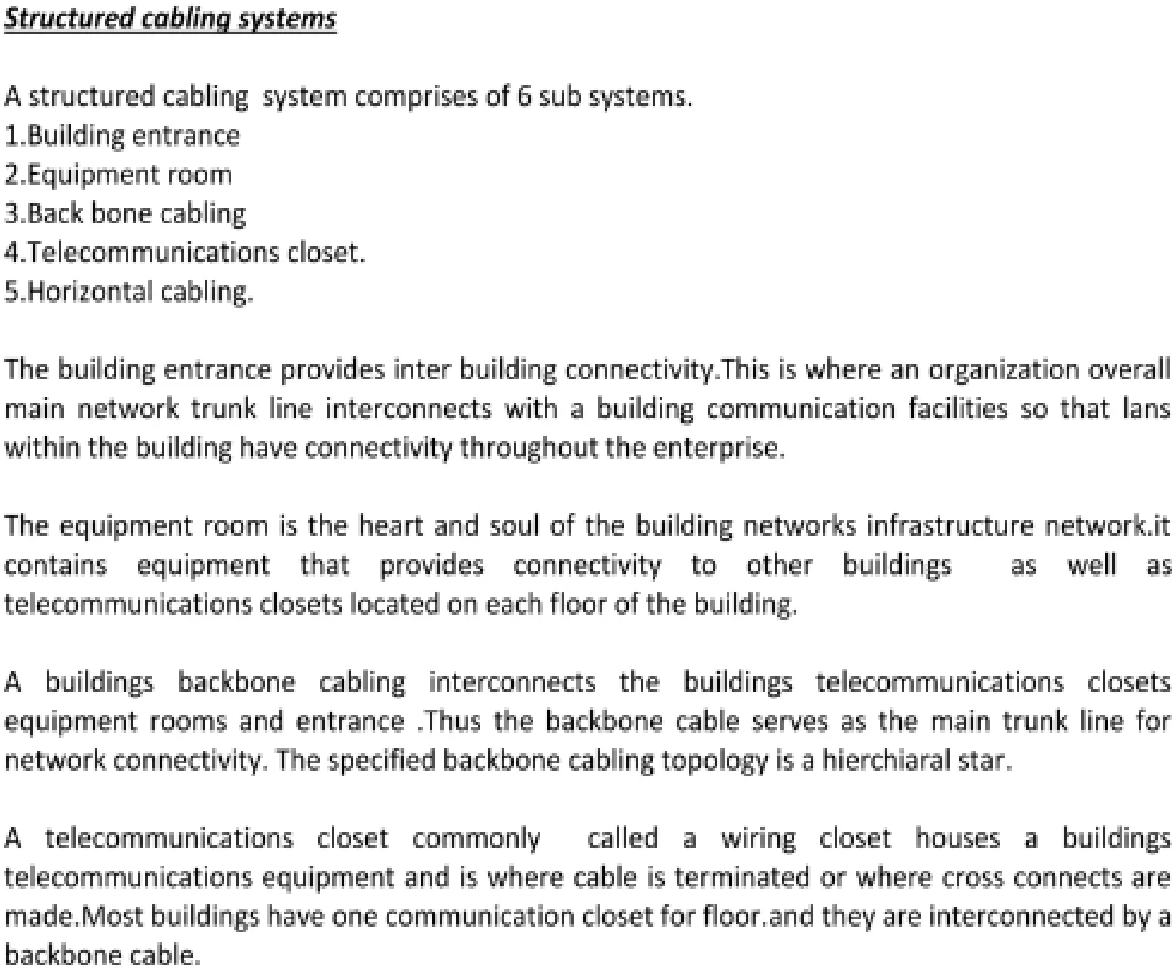
- A MEO satellite is in orbit somewhere between 8,000 km and 18,000 km above the earth's surface.
- MEO satellites are similar to LEO satellites in functionality.
- MEO satellites are visible for much longer periods of time than LEO satellites, usually between 2 to 8 hours.
- MEO satellites have a larger coverage area than LEO satellites.

Advantage

- A MEO satellite's longer duration of visibility and wider footprint means fewer satellites are needed in a MEO network than a LEO network.

Disadvantage

- A MEO satellite's distance gives it a longer time delay and weaker signal than a LEO satellite, though not as bad as a GEO satellite.



Structured cabling systems

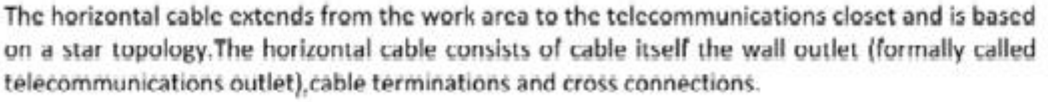
A structured cabling system comprises of 6 sub systems.
1.Building entrance
2.Equipment room
3.Back bone cabling
4.Telecommunications closet.
5.Horizontal cabling.

The building entrance provides inter building connectivity.This is where an organization overall main network trunk line interconnects with a building communication facilities so that lans within the building have connectivity throughout the enterprise.

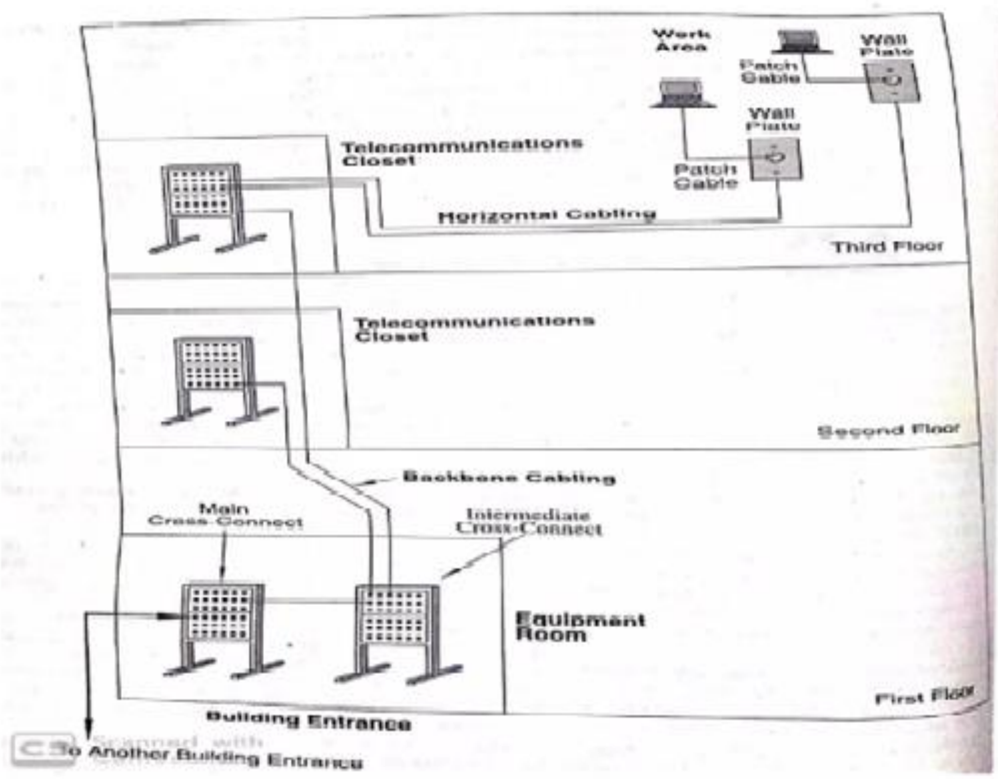
The equipment room is the heart and soul of the building networks infrastructure network.it contains equipment that provides connectivity to other buildings as well as telecommunications closets located on each floor of the building.

A buildings backbone cabling interconnects the buildings telecommunications closets equipment rooms and entrance .Thus the backbone cable serves as the main trunk line for network connectivity. The specified backbone cabling topology is a hierchiaral star.

A telecommunications closet commonly called a wiring closet houses a buildings telecommunications equipment and is where cable is terminated or where cross connects are made.Most buildings have one communication closet for floor.and they are interconnected by a backbone cable.



The horizontal cable extends from the work area to the telecommunications closet and is based on a star topology.The horizontal cable consists of cable itself the wall outlet (formally called telecommunications outlet),cable terminations and cross connections.



Introduction to Data-link Layer :

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

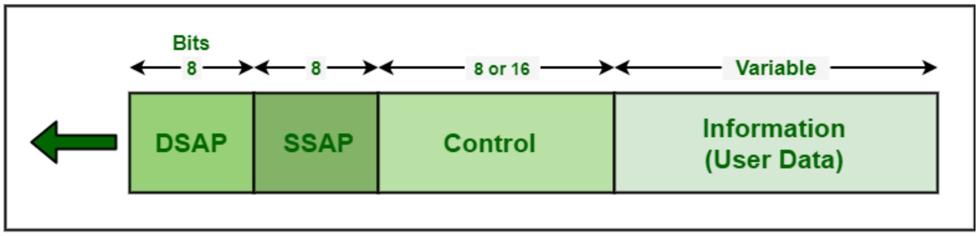
Functionality of Data-link Layer:

Data link layer does many tasks on behalf of upper layer. These are:

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

Logical Link Control (LLC) Protocol Data Unit:

Logical Link Control (LLC) is a sub layer that generally provides the logic for the data link as it controls the synchronization, multiplexing, flow control, and even error-checking functions of DLL (Data Link Layer). DLL is divided into two sub layers i.e. LLC sub layer and MAC (Medium Access Control) sub layer.
The basic model of LLC protocols is modeled after the HDLC (High-Level Data Link Control). These protocols are unacknowledged connectionless service, Connection-oriented service, and acknowledged connectionless service. All of these protocols use the same PDU (Protocol Data Unit) format as shown –



PDU Format

This PDU format basically contains 4 different fields given below –

1. **Destination Service Access Point (DSAP) Field –**
   DSAP is generally an 8-bit long field that is used to represent the logical addresses of the network layer entity meant to receive the message. It indicates whether this is an individual or group address.

2. **Source Service Access Point (SSAP) Field –**
   SSAP is also an 8-bit long field that is used to represent the logical addresses of the network layer entity meant to create a message. It indicates whether this is a command or response PDU. It simply identifies the SAP that has started the PDU.

3. **Information Field –**
   This field generally includes data or information.

4. **Control Field –**
   This field identifies and determines the specific PDU and also specifies various control functions. It is an 8 or 16-bit long field, usually depending on the identity of the PDU. It is used for flow and error control. There are basically three types of PDU. Each PDU has a different control field format. These are given below –
   - **Information (I) –**
     It generally includes 7-bit sequence number (N(S)) and also a piggybacked sequence number (N(R)). It is used to carry data or information.

   - **Supervisory (S) –**
     It generally includes an acknowledgment sequence number (N(R)) and also a 2-bit S field for three different PDU formats i.e. RNR (Receive Not Ready), RR (Receive Ready), and REJ (Reject). It is generally used for flow and error control.

   - **Unnumbered (U) –**
     It is generally a 5-bit M bit that is used to indicate the type of PDU. It is used for various protocol PDUs.

Some functions of LLC Sub layer are –

- It is responsible to manage and to ensure the integrity of data transmissions.
- They provide the logic for the data link.

- It also controls the synchronization, multiplexing, error checking or correcting functions, flow control of the DLL.
- It also allows multipoint communication over a range of computer networks.

Medium Access Control Sublayer
(MAC sub layer)

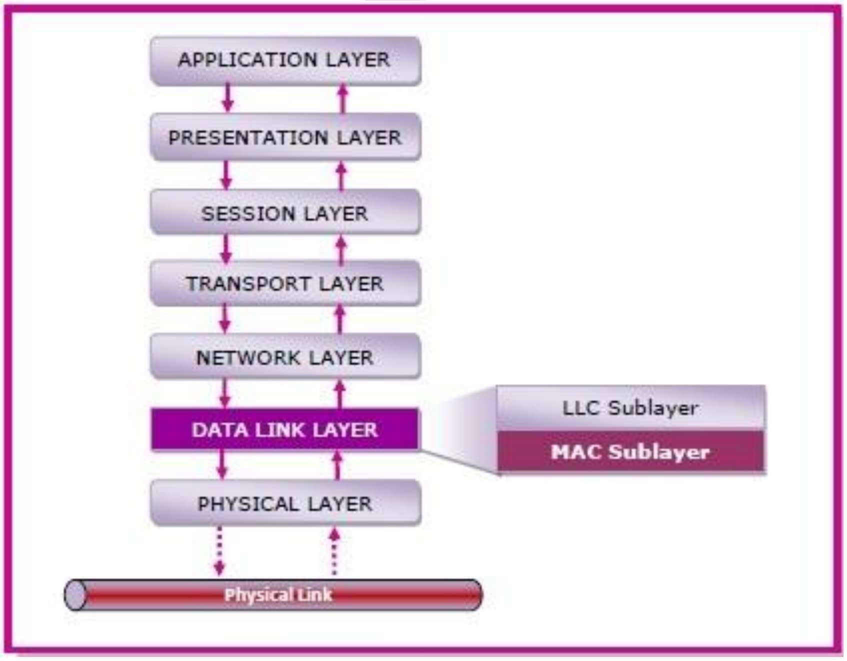
The medium access control (MAC) is a sub layer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sub layers −

- The logical link control (LLC) sub layer
- The medium access control (MAC) sub layer

The following diagram depicts the position of the MAC layer −



Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

UNIT -V

Physical Components of the Network:

End Devices or Hosts: These devices form the interface between users and the underlying communication network. Examples of end devices are Computers (work stations, laptops, file servers, web servers), Network printers, VoIP phones, Mobile handheld devices, and … etc. – A host device is either the source or destination of a message transmitted over the network.

Intermediary Network Devices: Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork. Examples of intermediary devices are switches, wireless access points, routers, firewalls, and … etc. – These devices use the destination host address to determine the path that messages should take through the network.

Network Media: The medium provides the channel over which the message travels from source to destination. The three types of media are Copper, Fiber Optic, and Wireless.

CONNECTORS

A device that eliminates a section of cabling or implements a state of access for network devices, including PCs, hubs, and switches. Connectors can be famous for their physical presentation and mating features, including jacks and attachment (male connectors) or attachments and ports (female connectors).

Connectors are used to connect the guided (wired) transmission media to devices like the hub, server, workstations etc.

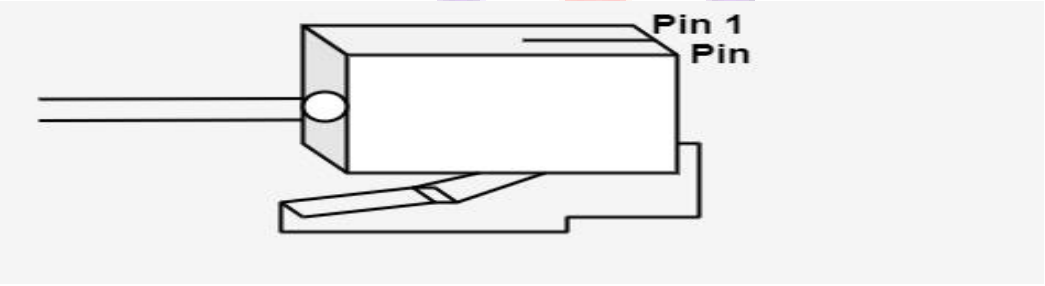
Types of Connectors

There are several types of connectors as follows −

Twisted Pair Cable Connectors

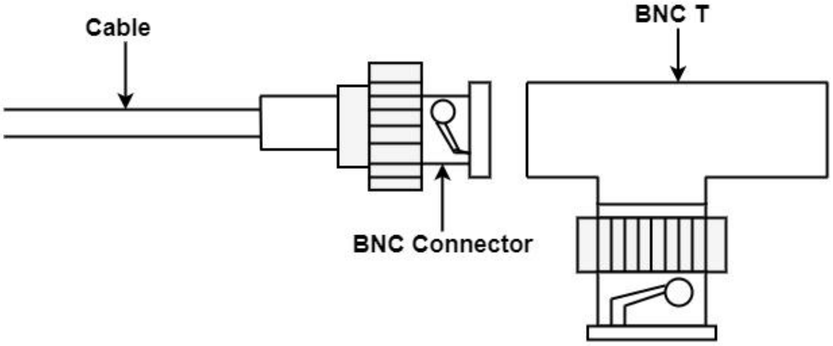
For the past various years, virtually all new connections have been constructed using a twisted pair cabling mechanism. UTP (Unshielded Twisted Pair) is used rather than STP (Shielded Twisted Pair) in almost all cases because it is less costly, simpler to install and handle.

The standard UTP connector is **RJ45** (RJ represents Registered Jack). RJ45 connector is similar to modular telephone connectors used in homes but larger, as displayed in the figure −



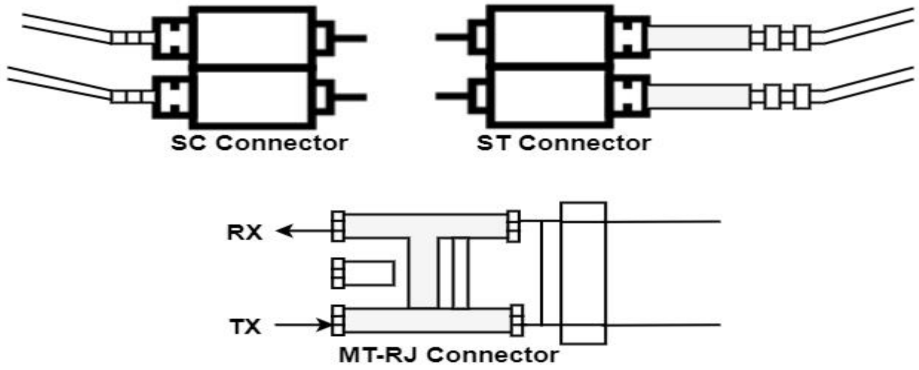
Coaxial Cable Connector

To connect coaxial cable to devices, we require coaxial connectors. The general type of connector that can be used is the **Bayonne Neill Concelman (BNC)** connector, as displayed in the figure below



Fiber-optic Cable Connector

There are three methods of connectors for fiber-optic cables, as displayed in the figure.



The Subscriber Channel (SC) connector is used for cable T.V. It uses a push/pull locking system. The straight-tip (ST) connector is used for linking wire to networking devices. It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is a similar size to RJ45.

Network Cable Connectors Types and Specifications

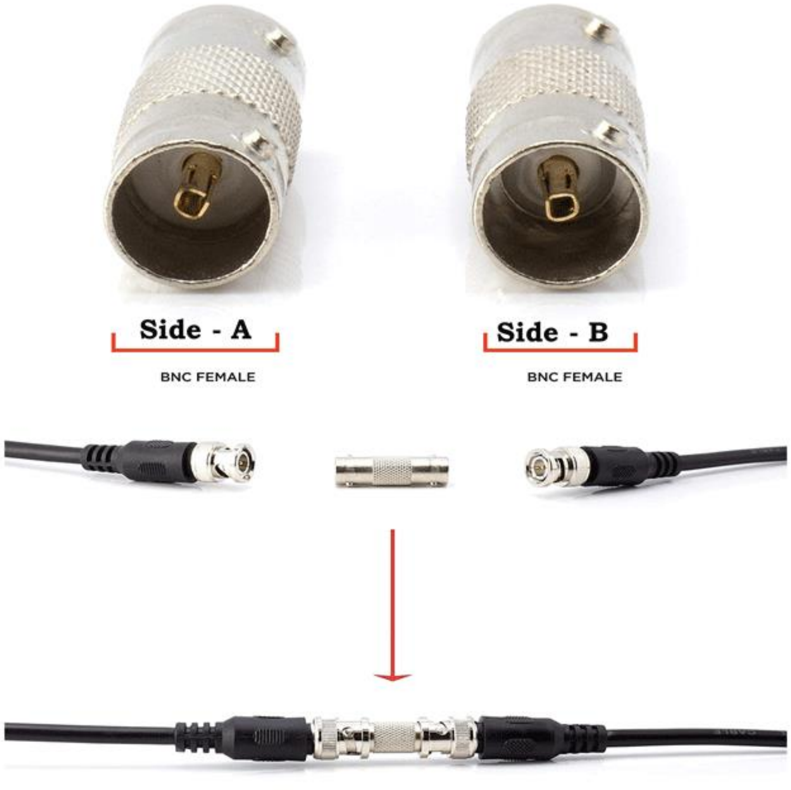
This tutorial explains which network media cables use which connectors. Learn the specifications of the most common types of network media connectors.

There are several types of network cables. Each type of network cable uses specific types of connectors to connect to another network cable or network interface card. To join two network cables or to connect a network cable to a NIC, you need appropriate connectors. In the following section, we will discuss some most common and popular network media connectors.

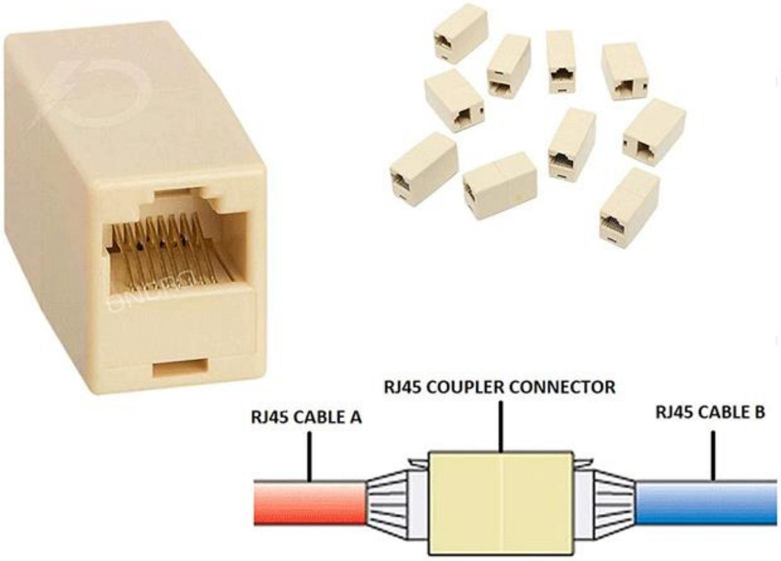
Barrel connectors

Barrel connectors are used to join two cables. Barrel connectors are female connectors on both sides. They allow you to extend the length of a cable. If you have two small cables, you can make a long cable by joining them through the barrel connector.

Barrel connectors that are used to connect coaxial cables are known as **BNC barrel connectors**. The following image shows BNC barrel connectors.



Barrel connectors that are used to connect STP or UTP cables are known as **Ethernet LAN jointers** or **couplers**. The following image shows Ethernet LAN jointers or couplers.



Barrel connectors do not amplify the signals. It means, after joining, the total cable length must not exceed the maximum supporting length of the cable. For example, a standard UTP cable supports a maximum distance of 100 meters. You can join two UTP cables if their sum is not more than 100.

For example, you can join the following cables.

Cable 1 (45 meters) + cable 2 (30 meters) = joint cable (75 meters = 45 meters + 30 meters)

The length of the joint cable is less than 100 meters.

But you can't join the following cables.

Cable 1 (65 meters) + cable 2 (45 meters) = joint cable (110 meters = 65 meters + 45 meters)

The length of the joint cable is more than 100 meters.

F connectors

An **F** connector is used to attach a coaxial cable to a device. **F** connectors are mostly used to install home appliances such as dish TV, cable internet, CCTV camera, etc. The following image shows F connectors.

Terminator connectors

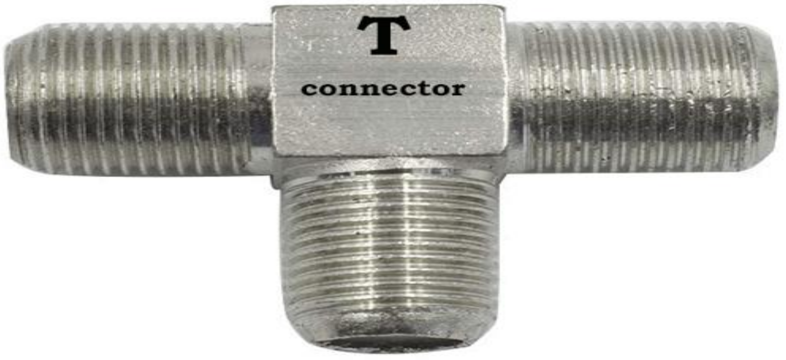
When a device places signals on the coaxial cable, the signals travel along the end of the cable. If another device is connected to the other end of the cable, the device will receive the signal. But if the other end of the cable is open, the signals will bounce and return in the same direction they came from. To stop signals from bouncing back, all endpoints must be terminated.

A terminator connector is used to terminate the endpoint of a coaxial cable. The following image shows terminator connectors.

T type connectors

A T connector creates a connection point on the coaxial cable. The connection point is used to connect a device to the cable.

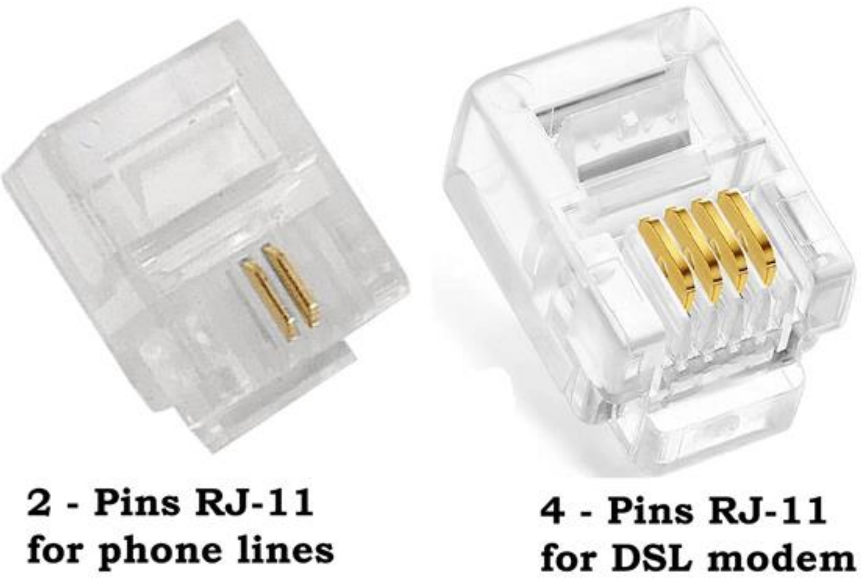
The following image shows T-type connectors.



RJ-11 Connectors

RJ-11 connectors have the capacity for six small pins. However, in many cases, only two or four pins are used. For example, a standard telephone connection uses only two pins, and a DSL modem connection uses four pins. They have a small plastic flange on top of the connector to ensure a secure connection.

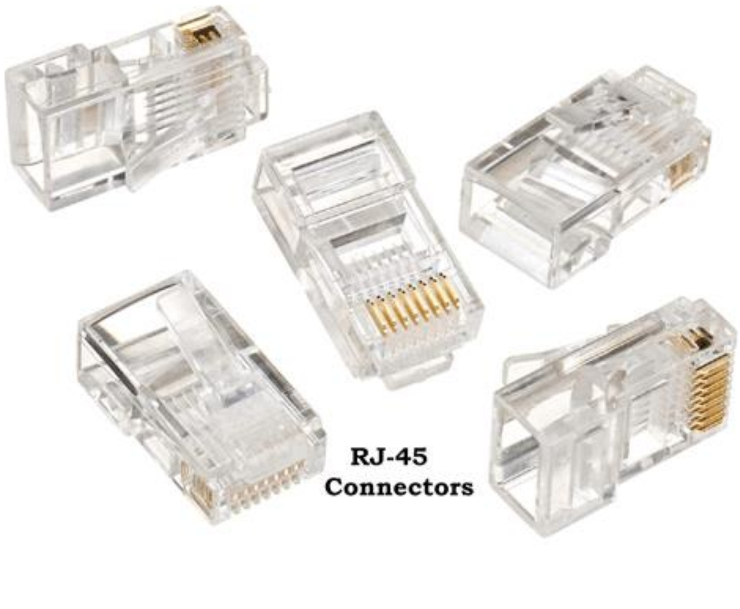
The following image shows RJ-11 connectors.



RJ-45 connectors

RJ-45 connectors look likes RJ-11 connectors, but they are different. They have 8 pins. They are also bigger in size than RJ-11. RJ-45 connectors are mostly used in computer networks. They are used with STP and UTP cables. Some old Ethernet implementations use only four of the eight pins. Modern Ethernet implementation uses all 8 pins to achieve the fastest data transfer speed.

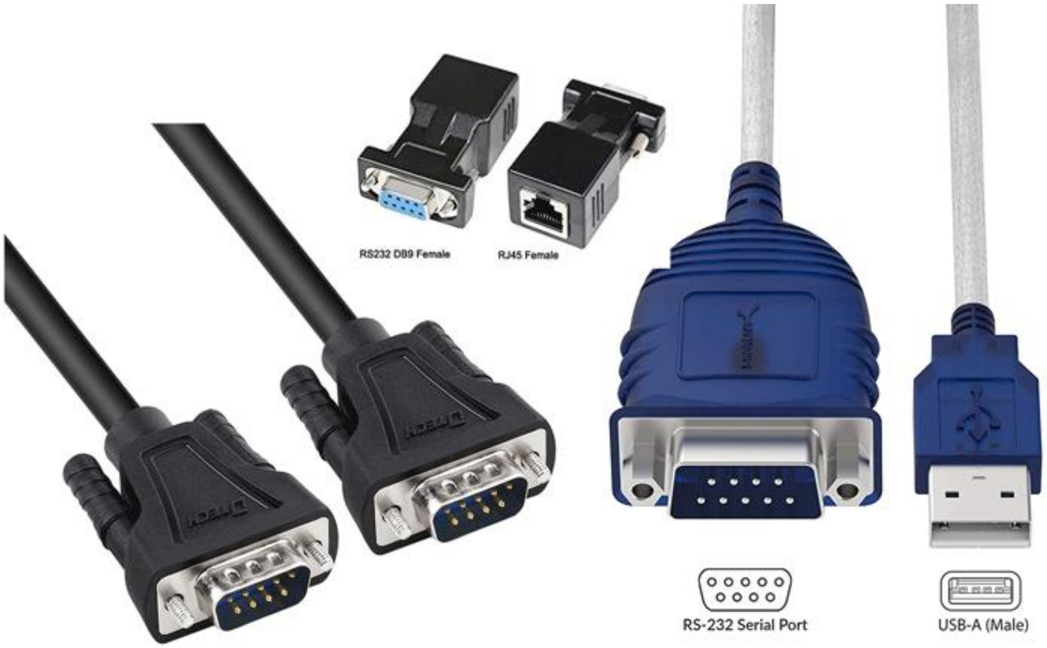
The following image shows RJ-45 connectors.



DB-9 (RS-232) connectors

A DB-9 or RS-232 connector connects a device over a serial port. It has 9 pins. It is available in both male and female connectors. It is used for asynchronous serial communication. The other side of the cable can be connected to any popular connector type. For example, you can connect one side of the cable with a DB-9 connector and the other side of the cable with another DB-9 connector or with an RJ-45 connector or with a USB connector.

The following image shows DB-9 connectors.



One of the most popular uses of a DB-9 connector is to connect the serial port on a computer with an external modem.

Universal serial bus (USB) connectors

USB connectors are the most popular. They support 127 devices in the series. All modern computers have USB ports. Most devices that you can connect to the system have USB ports. Some examples of devices that support or have USB ports are mice, printers, network cards, digital cameras, keyboards, scanners, mobile phones, and flash drives.

Keyboard
Usb Hub
Mouse
Pendrive
Dongle
Bluetooth
Cardreader
Laptop & P.C. To.

If the device has a USB port, you can use a cable that has a USB connector on both ends to connect the device to the computer. If the device does not have a USB port, you can still connect the device to the USB port. For that, you can use a cable that has a USB connector on one side and the corresponding connector on the other.

Fiber cable connectors

A variety of connectors are used to connect fiber cables. Some popular connectors are ST, SC, LC, and MTRJ. Let's discuss these connectors.

SC connectors

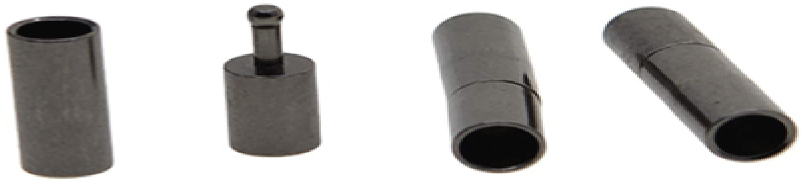
SC connectors are also known as **subscriber connectors**, **standard connectors**, or **square connectors**. An SC connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device. It uses a push-pull connector similar to audio and video plugs and sockets.

The following image shows SC connectors.

Straight tip (ST) connectors

Straight tip (ST) connectors are also known as **bayonet connectors**. They have a long tip extending from the connector. They are commonly used with MMF cables. They use a half-twist bayonet type of lock. An ST connector connects to a terminating device by pushing the connector into the terminating equipment and then twisting the connector housing to lock it in place.

The following image shows ST connectors.



LC connectors

LC connectors are known as **Lucent Connectors**. For a secure connection, they have a flange on top, similar to an RJ-45 connector. An LC connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pressing the tab on the connector and pulling it out of the terminating device.

The following image shows LC connectors.

MTRJ connectors

An MTRJ connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device. It includes two fiber strands: a transmit strand and a receive strand in a single connector.

The following image shows MTRJ connectors.

TRANSCEIVERS

Definition: It is a combination of transmitter (Tx)/receiver (Rx) in an only package. This device is used in wireless communications devices like cordless telephone sets, cellular telephones, radios, etc.. Irregularly the transceiver name is used as a reference to Tx or Rx devices within cable otherwise optical fiber systems. The **transceiver diagram** is shown below.

transceiver

The main function of this device is to transmit as well as receive different signals. This is most commonly used to illustrate the component in LAN to apply signals over the network wire & detect signals flowing through the wire. For several LANs, it is embedded in the NIC (network interface card). Some kinds of networks require an exterior transceiver.

Working

In a radio transceiver, as the transmitter transmits the signals, the receiver will be silenced. An electronic switch lets the transmitter & receiver to be allied to the similar antenna, so that transmitter o/p can be protected from the damage of the receiver.
In a transceiver type, it is not possible to get signals while transmitting, which is known as half-duplex. Some of the transceivers are mainly designed for permitting reception of signals throughout transmission stages which are known as full-duplex. The transmitter & receiver operate on different frequencies so that the transmitter signal does not interfere with the receiver. This kind of operation is used in cordless & cellular phones.

Satellite communication networks frequently use full-duplex transceivers on the subscriber points based on the surface. The transceiver to satellite or transmitted signal is known as the uplink, whereas the satellite to the transceiver or received signal is known as the downlink.

Types of Transceivers

Transceivers are classified into different types which include the following.

- RF Transceivers
- Fiber-optic Transceivers
- Ethernet Transceivers

- Wireless Transceivers

In the above-mentioned types are different but the working remains the same. Each type has its own characteristics like the no. of ports accessible for connecting the network and supports full-duplex communication.

1). RF Transceivers

RF transceiver is one type of module that includes both a Tx as well as Rx. Generally, this can be used in any wireless communication system by arranging in between baseband modem as well as PA/LNA. Here PA is a power amplifier whereas LNA is a low noise amplifier. Baseband Modem includes chipsets of numerous analog or digital modulation methods & ADC/DAC chips. RF Transceivers are used to transmit the data in the form of voice or video over the wireless medium. RF Transceiver is used to convert intermediate frequency (IF) to radiofrequency (RF). These are used in satellite communication for transmission & reception of TV signal, radio transmission & reception, and ITE networks/Zigbee/ WiMax/WLAN.

rf-transceivers

2). Fiber-optic Transceivers

This is also called as fiber optical transceiver, optics module, optical module, etc. This device employs fiber optic technology for data transmission. This is an essential component in the optical network devices that include electronic components to encode or decode the information into light signals. After that, these signals can be transmitted as electrical signals through another end. Here the data can be transmitted in the form of light which uses a light source like VSCEL, DFB laser, and FP.

fiber-optic-transducers

3). Ethernet Transceivers

An Ethernet transceiver is used to connect electronic devices or computers in a network to transmit & receive messages. An alternate name of an Ethernet transceiver is MAU (media access unit). This is used in the specifications of IEEE 802.3 & Ethernet. In the ISO network model, Ethernet is the physical layer component and the main **functions of transceivers** are for detecting a collision, conversion of digital data, Ethernet interface processing, and provides access for the network.

ethernet-transceivers

4). Wireless Transceivers

A wireless transceiver is an essential component in the wireless communication system and the quality of this can be determined by the efficiency as well as data delivery within the wireless system. This includes two functional layers like a physical layer & a media access control layer. The physical layer includes an RF front end as well as a baseband processor, this processor changes a bit stream to a collection symbol flow for data transmission. The MAC layer gives link traffic control used for the transmitter to contact the wireless links, evade collisions & enhance data throughput.

wireless-transceivers

Applications of Transceiver

The transceiver applications are

- This module is applicable in wireless communication
- The main function of this is to transmit the data in the form of voice or data or video over the wireless medium.
- This modem is used to change the frequency from IF to RF
- RF transceiver module is used in satellite communication, radio transmission for TV signal transmission.

MEDIA CONVERTERS

A media converter is a networking device that transparently converts Ethernet or other communication protocols from one cable type to another type, usually copper CATx/UTP to fibre. Media converters are often used in pairs to insert a fibre segment into copper networks to increase cabling distances and enhance immunity to electromagnetic interference. They can also extend LANs, and convert link speeds and fibre modes.

Benefits of Media Converters

- **Extend LAN Distance with Fibre**

Copper-based Ethernet connections are limited to a data transmission distance of 100 metres when using UTP cable. By using Ethernet to fibre conversion, you can extend link distance up to 80 kilometres or more.

- **Maintain Investments in Existing Equipment**

Media converters enable you to migrate a local network to fibre while protecting your investment in existing copper-based hardware. This means no costly, time-consuming overhaul to your infrastructure.

- **Protect Data from Interference**

Electromagnetic interference, or EMI, can cause corruption of data over copper-based Ethernet links. Data transmitted over fibre optic cable is completely immune to this type of noise, ensuring optimal data transmission and network performance.

- **Speed Conversion**

Media converters allow you to convert link speeds from 10 Mbps to 100 Mbps or from 100 Mbps to 1000 Mbps.

- **Power over Ethernet**

Power over Ethernet, or PoE, simplifies installation of Wi-Fi access point, IP cameras and more by eliminating the need for a local AC power circuit.

Types of Media Converters

Copper-to-Fibre Media Converters

Copper-to-fibre media converters enable connections of copper-based Ethernet equipment over a fibre optic link. This extends links over greater distances with fibre optic cable, protects data from noise and interference, and future-proofs a network with additional bandwidth capacity. Discover our wide selection of copper-to-fibre media converters.

Fibre-to-Fibre Media Converters

Fibre-to-fibre media converters connect different fibre optic networks and support conversion from one wavelength to another. They provide connectivity between single-mode and multimode fibre, as well as between dual and single fibre.

Discover our fibre-to-fibre media converters.

PoE Media Converters

Power-over-Ethernet (PoE) media converters provide reliable and cost-effective fibre distance extension to PoE-powered devices. PoE media converters can power devices like IP phones, videoconferencing equipment, IP cameras and Wi-Fi devices over copper UTP cabling.

Learn more about our vast selection of PoE media converters.

Stand-Alone vs. Chassis-Based Media Converters

Stand-alone media converters are compact and can be AC or DC powered. They are commonly used to convert one copper link to fibre in point-to-point installs. These converters are easy to deploy and offer a range of useful functionality for your network, such as auto-MDI/MDIX, link fault pass through and more.

Chassis-based media converters are used in high-density locations such as a data centre or equipment room. They mount in racks alongside network switches, enabling the conversion of copper ports on legacy switches to fibre.

Managed vs. Unmanaged Media Converters

Managed media converters give network administrators complete control of data, bandwidth and traffic. This lets admins manage and troubleshoot a network remotely and securely to achieve and maintain optimal performance and reliability. Thus, these converters are most suitable for environments requiring a medium- to large-scale deployment of media converters.

Shop our selection of managed media converters now.

Unmanaged media converters are "plug-and-play" converters which are easy to install and troubleshoot. Unlike managed converters, these do not provide the same level of monitoring, fault detection and configuration.

Commercial vs. Industrial Media Converters

Commercial media converters are designed for typical office and data centre environments where ambient temperature is controlled. These converters provide a cost-effective way to extend the distance of your network and improve the life of copper-based equipment. They are perfect for commercial applications that do not deal with extreme environmental issues.

Industrial media converters convert data between twisted pair cabling and multimode or single-mode fibre optic cabling, extending the distance of a network. They are able to withstand extreme temperatures (-40°C to 75°C) and harsh conditions, feature redundant power design and are designed for high shock and vibration locations. This makes them a perfect fit for industrial networks. Industrial media converters are commonly used in applications such as building automation, oil and gas drilling and mining.

Applications and Use Cases for Media Converters

- **Overcoming Copper's Limits**

Media converters extend LAN reach far beyond the 100 metre limit of copper CATx cabling by converting links to fibre. Fibre links enable link distances of up to 80 kilometres.

- **Enterprise**

PoE media converters backhaul Wi-Fi data and power access points, improving network functionality and reliability in commercial applications.

- **Security and Surveillance**

PoE+ simplifies installation of IP security cameras by eliminating the need for a power circuit near the installed device. PoE+ media converters power these devices and backhaul signals to remote data centres or operations centres.

- **Government and Defense**

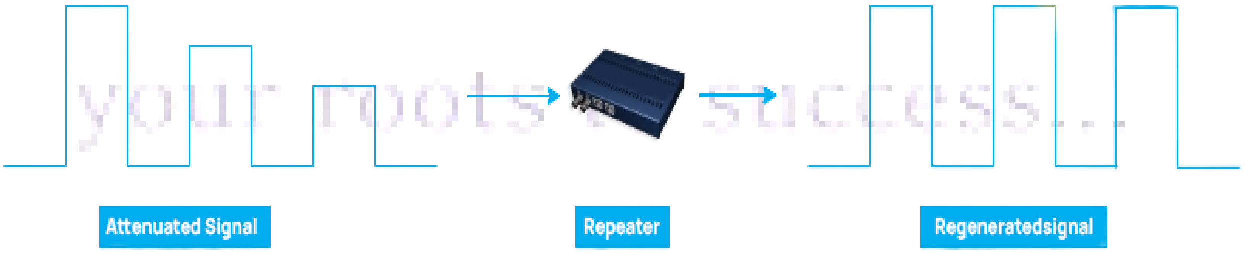
Media converters provide secure, high-performance LAN connections from the data centre to desktops with fibre. Highly reliable with unsurpassed bandwidth, speed and security, fibre-to-the-desktop is a perfect fit for government and defense applications.

- **Fibre Mode Conversion**

Never worry about varying fibre types in your application again. Convert fibre links from multimode to single-mode and vice versa with media converters.

REPEATERS IN COMPUTER NETWORK

In computer networks, a repeater is a device that amplifies and regenerates signals as they pass through the network. The primary purpose of a repeater is to extend the distance of a network by increasing the strength and quality of signals over long distances or through dense blocks. Repeaters are often used in LANs (Local Area Networks) and WANs (Wide Area Networks) to improve the performance and reliability of the network. They can help to prevent data loss, reduce errors, and ensure that the signal arrives at its intended destination with sufficient strength and quality.



Features of Repeaters in Computer Network

Here are some features of repeaters in computer networks:

- It extends network range by amplifying or regenerating signals.
- It improves signal strength and quality over long distances or through blocks.
- It can be used in both analog and digital networks.
- They regenerate the signal without modifying its content.
- They can be applied to raise the efficiency and dependability of networks.
- It may be limited in the number of repeaters that can be used in a network.
- They may add delay or complexity to the network.
- It requires power to operate.
- It can be used in local area networks (LANs) and wide area networks (WANs).
- It helps to prevent data loss and reduce errors

Types of Repeaters in Computer Network

There are two main types of repeaters used in computer networks:

1. Analog
2. Digital.

- **Analog repeaters:** These repeaters work by amplifying the incoming signal and regenerating it at the output. It is used in older network technologies that operate on analog signals.
- **Digital repeaters:** These repeaters work by regenerating the digital signal without amplifying it. It is used in modern network technologies which operate on digital signals.

On basis of area LANs connected
Repeaters can be categorized as local or remote, depending on their location in the network.

- **Local repeaters:** Local repeaters are typically used in small networks where the distance between devices is limited.
- **Remote repeaters:** Remote repeaters are typically used in larger networks where the distance between devices is greater.

On basis of types of network-connected
In other types of networks that they connect, repeaters can be divided into two types

- **Wired network:** A repeater takes an incoming signal and repeats it, allowing the signal to travel a greater distance without losing strength.
- **Wireless network:** A repeater receives a wireless signal from a router and broadcasts it to extend the network’s coverage.

How does a Repeater work in a Computer Network?

Here’s how a repeater works:

- A signal is transmitted from a source, such as a radio or a cell phone.
- The signal travels through the air or a cable, but its strength weakens as it gets farther from the source.
- The weakened signal is received by the repeater, which amplifies it to increase its strength.
- The amplified signal is transmitted from the repeater to its destination, such as another radio or cell phone.
- The signal is now stronger and can travel a greater distance without losing quality.
- Repeaters are commonly used in wireless networks, such as cellular and Wi-Fi networks, to extend their range and improve signal strength.
- They can also be used in wired networks, such as Ethernet networks, to extend the length of a cable run.

Advantages of Repeaters in a Computer Network

Here are the advantages of repeaters in a computer network:

- Repeaters amplify signals, maintaining their strength throughout the line.
- It enables faster data transfer, critical for high-speed applications like video streaming.
- They reduce noise and distortions, leading to more stable and reliable signals.
- These allow signals to travel longer distances without losing strength or quality.

Disadvantages of Repeaters in a Computer Network

Here are the disadvantages of repeaters in a computer network:

- The cost to build and maintain these is very high.
- These require a power source to operate, which can be a constraint in some situations.
- They introduce a delay in signal transmission, which can be difficult in real-time applications
- Adding repeaters can increase its complexity, making troubleshooting and maintenance more difficult.

Conclusion

In conclusion, repeaters can be a useful tool for maintaining signal strength and quality in very short lines. They offer several benefits, including signal amplification, increased data rate, improved signal quality, and longer transmission distances. However, they also come with some disadvantages, such as cost, power requirements, delay, and increased complexity. Ultimately, whether to use repeaters in a particular application will depend on a range of factors, including the specific requirements of the system, the available resources, and the costs and benefits associated with repeater installation and maintenance.

Frequently Asked Questions(FAQs)

Q1. What is a repeater in a computer network?
Ans: A repeater is a device used in computer networks to regenerate and amplify signals as they pass through the network. The primary function of a repeater is to extend the distance of a network by increasing the strength and quality of signals over long distances or through dense obstacles.

Q2. What is the difference between an analog repeater and a digital repeater?
Ans: An analog repeater amplifies the incoming signal and regenerates it at the output, while a digital repeater regenerates the digital signal without amplifying it. Analog repeaters are used in older network technologies that operate on analog signals, while digital repeaters are used in modern network technologies that operate on digital signals.

Q3. Where are repeaters typically used in a computer network?
Ans: Repeaters are typically used in Local Area Networks (LANs) and Wide Area Networks (WANs) to improve the performance and reliability of the network. They can help to prevent data loss, reduce errors, and ensure that the signal arrives at its intended destination with sufficient strength and quality.

Q4. How many repeaters can be used in a network?
Ans: The number of repeaters that can be used in a network depends on the specific technology being used, the distance between devices, and other factors such as both the signal’s strength and the cable’s quality. In general, it is recommended to limit the number of repeaters in a network to ensure optimal performance.

Q5. Are there any disadvantages to using repeaters in a computer network?
Ans: Yes, there are some disadvantages to using repeaters in a network. These can include cost, power requirements, delay, and increased complexity. Additionally, if too many repeaters are used in a network, it can lead to signal degradation and reduced performance.

Network Interface Card (NIC)

Network Interface Card (NIC) is a **hardware component** that is present on the computer. It is used to **connect different networking devices** such as computers and servers to share data over the connected network. It provides functionality such as support for I/O interrupt, Direct Memory Access (DMA) interfaces, partitioning, and data transmission.

NIC is important for us to establish a wired or wireless connection over the network.

Network Interface Card is also known as **Network Interface Controller, Network Adapter, Ethernet card, Connection card**, and **LAN (Local Area Network) Adapter.**

Functions of the Network Interface Card

A list of functions of the Network Interface Card is given below -

1. NIC is used to convert data into a digital signal.
2. In the OSI model, NIC uses the physical layer to transmit signals and the network layer to transmit data packets.
3. NIC offers both wired (using cables) and wireless (using Wi-Fi) data communication techniques.
4. NIC is a middleware between a computer/server and a data network.
5. NIC operates on both physical as well as the data link layer of the OSI model.

Components of Network Interface Card

Network Interface Card contains the following essential components -

1. Memory

Memory is one of the most important components of the NIC. It is used to store the data during communication.

2. Connectors

connectors are used to connect the cables to the Ethernet port.

3. Processor

Processor is used for converting the data message into a suitable form of communication.

4. Jumpers

Jumpers are the small device that is used to control the communication operations without the need of any software. It is also used to determine settings for the interrupt request line, I/O address, upper memory block, and type of transceiver.

5. Routers

To provide wireless connectivity, routers are used.

6. MAC address

MAC address is also referred to as a **physical network address**. It is a unique address that is present to the network interface card where ethernet packets are communicated with the computer.

Types of Network Interface Cards

There are the following two types of NICs -

1. Ethernet NIC

Ethernet NIC was developed by **Robert Metcalf in 1980**. It is made by ethernet cables. This type of NIC is most widely used in the LAN, MAN, and WAN networks.

Example: TP-LINK TG-3468 Gigabit PCI Express Network Adapter.

2. Wireless Networks NIC

It is a wireless network that allows us to connect the devices without using the cables. These types of NICs are used to design a Wi-Fi connection.

Example: Intel 3160 Dual-Band Wireless Adapter

Advantages of NIC

A list of advantages of NIC is given below -

1. As compared to the wireless network card, NIC provides a secure, faster, and more reliable connection.
2. NIC allows us to share bulk data among many users.
3. It helps us to connect peripheral devices using many ports of NIC.
4. Communication speed is high.
5. Network Interface cards are not expensive.
6. NICs are easy to troubleshoot.

Disadvantages of NIC

A list of disadvantages of NIC is given below -

1. NIC is inconvenient as compared to the wireless card.
2. For wired NIC, a hard-wired connection is required.
3. NIC needs a proper configuration to work efficiently.
4. NIC cards are not secure, so the data inside NIC is not safe.

PC cards

A PC card, also known as a PCMCIA card, is a credit card-sized memory or input/output (I/O) device that fits into a PC, usually a laptop. Developed by the Personal Computer Memory Card International Association, a PC card adds peripheral capability to a laptop. In this sense, it is an expansion card.

The PC card is not to be confused with another credit card-sized electronic card, the smart card, which contains an embedded microprocessor and memory, and is commonly used to authenticate users for a wide range of applications.

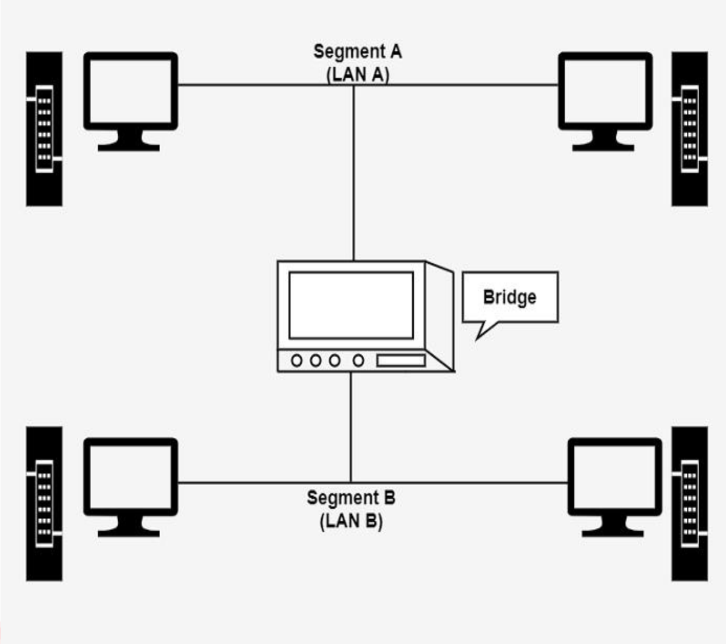
In the 1990s, the PC card added peripheral functionality to laptop computers, similar to what plugin boards did for desktops. The card was a plugin module containing a peripheral device, such as a modem, network adapter or storage drive. Although originally developed for use with many devices, including digital cameras, PC cards were most frequently used with laptop computers as many were equipped with ports that accommodated PC cards. The port made it possible to upgrade a laptop without opening the device, which was especially useful when an internal component stopped working or became obsolete.

BRIDGES IN COMPUTER NETWORK

Bridges are used to connect two subnetworks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.

Working of Bridges

A bridge accepts all the packets and amplifies all of them to the other side. The bridges are intelligent devices that allow the passing of only selective packets from them. A bridge only passes those packets addressed from a node in one network to another node in the other network.

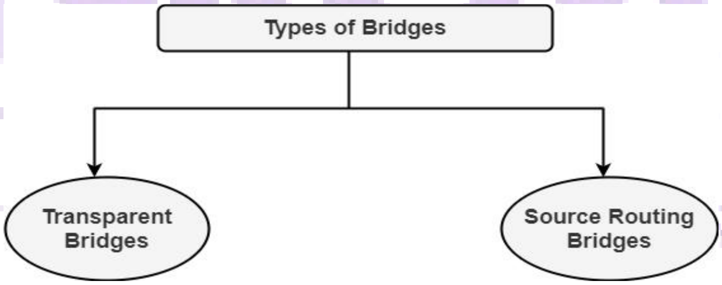


A bridge performs in the following aspect −

- A bridge receives all the packets or frame from both LAN (segment) A and B.
- A bridge builds a table of addresses from which it can identify that the packets are sent from which LAN (or segment) to which LAN.
- The bridge reads the send and discards all packets from LAN A sent to a computer on LAN A and that packets from LAN A send to a computer on LAN B are retransmitted to LAN B.
- The packets from LAN B are considered in the same method.

Types of Bridges

There are generally two types of bridges which are as follows −



Transparent Bridges

It is also called learning bridges. Bridge construct its table of terminal addresses on its own as it implements connecting two LANs. It facilitates the source location to create its table. It is self-updating. It is a plug and plays bridge.

Source Routing Bridge

This sending terminal means the bridges that the frames should stay. This type of bridge is used to prevent looping problem.

Uses of Bridges

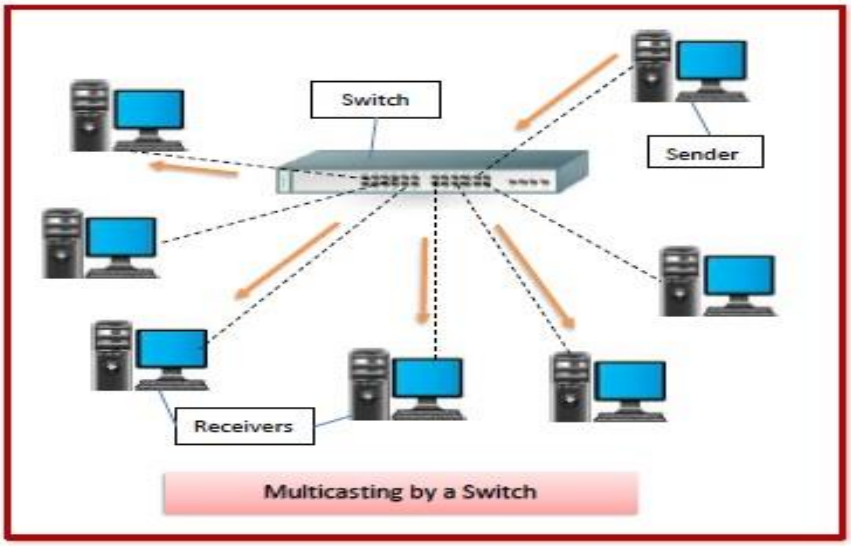
The main uses of bridges are −

- Bridges are used to divide large busy networks into multiple smaller and interconnected networks to improve performance.
- Bridges also can increase the physical size of a network.
- Bridges are also used to connect a LAN segment through a synchronous modem relation to another LAN segment at a remote area.

SWITCHES IN COMPUTER NETWORK

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s). It supports unicast, multicast as well as broadcast communications.



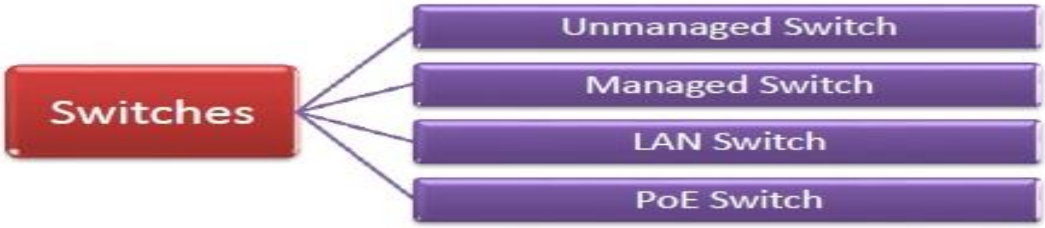
Features of Switches

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.

- It is supports unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48.

Types of Switches

There are variety of switches that can be broadly categorised into 4 types −



- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

SWITCHES Vs ROUTERS

Both of these are connecting devices that help in networking. We use a router for settling on the shortest path through which any given packet can easily achieve its intended destination. There is a difference between router and switch. A router's main objective is to establish a connection between various networks in a simultaneous manner. Also, it works on the network layer. A switch's main objective is to establish a simultaneous connection among various devices. It basically functions on the data link layer. In this article, we will discuss the difference between router and switch in further detail.

What is a Router?

A router is a device for computer networking that serves two of the main functions: (1) the creation and maintenance of a local area network (2) the management of data that enters and leaves a network along with the data that moves inside of the network.

In other words, a router assists its users in handling various networks, and it also routes the network traffic present between them. In the case of a home network, a router establishes a connection to the private LAN and establishes another one to the Internet. Also, various routers have various built-in switches. These switches allow a user to connect various wired devices.

What is a Switch?

A network switch is basically a computer networking device that helps in connecting multiple devices on one computer network. One can also use it for routing the information into an electronic form of data (that transmits over various networks). We can also call switches bridging devices because the process of establishing a link between network segments is known as bridging.

Difference Between Router and Switch

Parameters	**Router**	**Switch**
Operating Layer	A typical router can easily operate at the third layer (Network) in an OSI model.	The switches in a network operate at the second layer (Data Link Layer) in an OSI model.
Services Offered	A router can easily offer QoS, NetFlow, and NAT services.	A switch does not offer any such services.
Maintenance of Addresses	A router stores IP addresses in its routing table and maintains its own address.	A switch stores MAC addresses in its lookup table and maintains its own address. But in this case, a switch can easily learn the MAC addresses.
Ports	It is a networking device with 2/4/8 ports.	It is a type of multi-port bridge with 24/48 ports.

Duplex	It is less duplex in nature.	It is full-duplex in nature. Thus, no collision occurs here.
NAT	It can easily perform NAT.	It cannot perform NAT.
Speed Limit	It has a speed limit of about 1-10 Mbps (Megabytes per second) for wireless connection and 100 Mbps in case of a wired connection.	It has a speed limit of about 10/100 Mbps.
Routing Decision	A router helps its users in taking a faster routing decision.	A switch will more likely take a routing decision which is way more complex.
Broadcast Domain	Every port in a router contains a broadcasting domain of its own.	A switch contains a broadcasting domain of its own except the implemented VLAN.
Faster Performance	In the case of various network environments (like WAN/MAN), a router will work much faster than the switches.	A switch can work comparatively faster than a router when deployed in a LAN environment.
Type of Addresses	The operations of a router revolve around the IP addresses.	In the case of switches, they work with the MAC addresses. It is because these operate within a single network only.
Wiring of Connections	It can easily work with both- wireless as well as wired situations of a network.	The uses of a switch are confined to only wired network connections.