TEVTA

GOVERNMENT OF THE PUNJAB

**DIPLOMA OF ASSOCIATE ENGINEER 2ND YEAR**

# A TEXT BOOK OF COMPUTER NETWORK CIT-223

**COMPUTER INFORMATION TECHNOLOGY APPROVED BY TEVTA PUNJAB**

**Developed By :**
**Academics Wing**
**Technical Educations & Vocational Training Authority Punjab**

# Computer Networks

# CIT-223

## FOR DAE 2nd Year

## TECHNICAL EDUCATION & VOCATIONAL TRAINING AUTHORITY PUNJAB

# PREFACE

The text book has been written to cover the syllabus of computer Networks 2nd year D.A.E (CIT) according to the new scheme of studies. The book has been written in order to cater the needs of latest concepts and needs of the course i.e. computer Networks and to be able to attempt D.A.E Examination of PBTE Lahore.

The aim of bringing out this book is to enable the students to have sound knowledge of the subject. Every aspect has been discussed to present the subject matter in the most concise, compact lucid & simple manner to help the subject without any difficulty. Frequent use of illustrative figures has been made for clarity. Short Questions and Self-tests have also been included at the end of each chapter which will serve as a quick learning tool for students.

The author would like to thank the reviewers whose valuable recommendations have made the book more readable and understandable. Constructive criticisms and suggestions for the improvements in future are welcome.

AUTHORS

# MANUAL DEVELOPMENT COMMITTEE

**MUHAMMAD AYAZ FAROOQ** (Chief Writer)

(GCT Attock)

**MUHAMMAD AZAM** (Member)

(GCT Kamalia)

**HAFIZ USMAN DILSHAD** (Member)

(GCT (M) Bahawalpur)

# Table of Contents

# 1 Principles of Data Communication and Networking

## Objectives

**After completion of this chapter students will be able to:**

- ✓ Learn Development of Communication and Data Communication
- ✓ Overview of OSI and TCP/IP model
- ✓ Understand Data Transmission
- ✓ Learn Analog Transmission
- ✓ Learn Digital Transmission
- ✓ Learn Signal Impairment
- ✓ Learn Transmission Media
- ✓ Learn Types of Cables and Connectors
- ✓ Learn Telephony and Wireless Communication

## 1.1 Data communications (DC)

Data communications is the process of using computing and communication technologies to transfer data from one place to another, and vice versa. It enables the movement of electronic or digital data between two or more nodes, regardless of geographical location, technological medium or data contents

## 1.2 Components of data communication system

A Communication system has following components:

1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

2. **Sender:** It is the device/computer that generates and sends that message.

3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer.

The distance between sender and receiver depends upon the types of networks used in between.

4. **Medium**: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

## 1.3 Characteristics of Data Communications:

### 1. Delivery:

The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

### 2. Accuracy:

The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

### 3. Timeliness:

The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

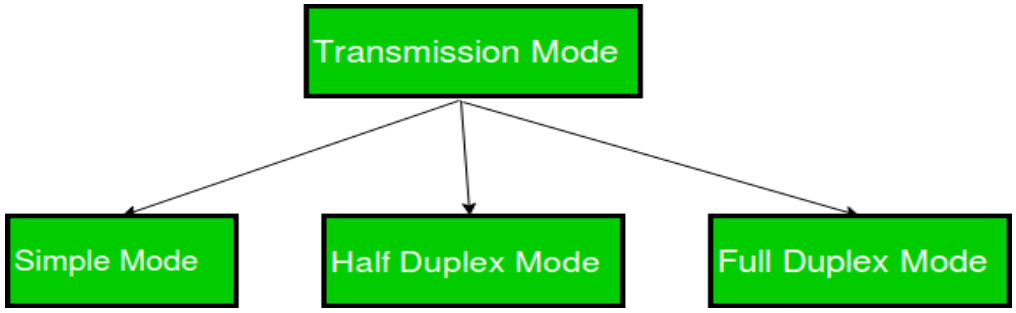
### 4. Jitter:

Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

## 1.4 MODES OF DATA COMMUNICATION

Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode: -

- ✓ Simplex Mode
- ✓ Half-Duplex Mode
- ✓ Full-Duplex Mode

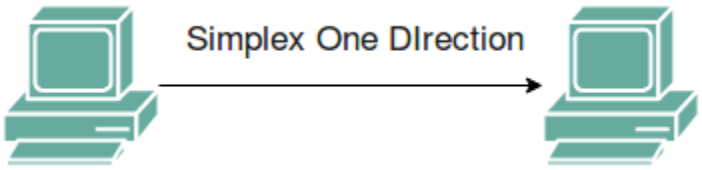



**1-1.4 Transmission Modes**

### Simplex Mode

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive.

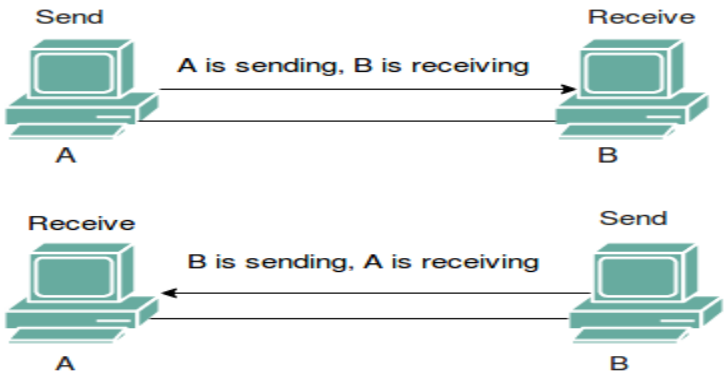
The simplex mode can use the entire capacity of the channel to send data in one direction. Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.




**1. SIMPLEX MODE**

## Half-Duplex Mode

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction. Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.




**1-2. Half Duplex Mode**

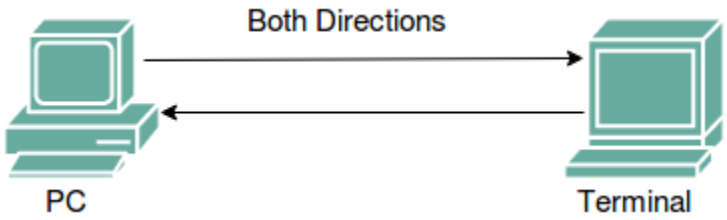
## Full-Duplex Mode

In full-duplex mode, both stations can transmit and receive simultaneously. In full duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:

- ✓ Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- ✓ Or the capacity is divided between signals travelling in both directions.

Full-duplex mode is used when communication in both direction is required all the time.

The capacity of the channel, however must be divided between the two directions. Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.




**1-3. Full Duplex**

# 1.5 Development of Communication and Data Communication

Data communications deals with the transmission of signals in a reliable and efficient manner. Networking deals with the technology and architecture of the communications networks used to interconnect communicating devices.

The 1970s and 1980s saw a merger of the fields of computer science and data communications that profoundly changed the technology, products, and companies of the now combined computer-communications industry. The computer-communications revaluation has produced several remarkable facts:

- ✓ There is no fundamental difference between data processing (computers) and data communications (transmission and switching equipment).
- ✓ There are no fundamental differences among data, voice, and video communications
- ✓ The distinction among single-processor computer, multiprocessor computer, local network, metropolitan network, and long-haul network has blurred.

One effect of these trends has been a growing overlap of the computer and communications industries, from component fabrication to system integration. Another result is the development of integrated systems that transmit and process all types of data and information. Both the technology and the technical standards organizations are driving toward integrated public systems that make virtually all data and information sources around the world easily and uniformly accessible.

## 1.6 Overview of OSI and TCP/IP model

The OSI Model or the Open Systems Interconnection Model is a conceptual framework which describes the functions of a networking system. It is used for the transfer of data over a network which moves through different layers.

OSI stands for Open Systems Interconnection. OSI model was developed by the International Organization for Standardization (ISO). It is a reference model for how applications communicate over a network. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. Before learning about the detailed structure of the model and its seven layers, given

below are a few points of introduction related to the Open Systems Interconnection Model which one must know.

- ✓ In the 1970s the OSI Model was proposed and in the year 1984, it was published by the International Organization of Standardization (ISO)
- ✓ Using this model, troubleshooting has become easier as the error can be detected at different levels
- ✓ This also helps in understanding the relationship and function of the software and hardware of a computer network
- ✓ The concept that the OSI Model should be a seven-layer structure, was proposed by Charles Bachman at Honeywell Information Systems
- ✓ The model initially did gain much popularity as it could not support the Internet protocol suite which was not acceptable to a lot of IT Companies
- ✓ The seven layers of the structure are divided into two parts: the upper layer or the host layer and lower layer or the media layer.

## 1.7 TCP / IP Model

The TCP/IP model is a part of the Internet Protocol Suite. This model acts as a communication protocol for computer networks and connects hosts on the Internet. It is a concise version of the OSI Model and comprises four layers in its structure.

The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

- ✓ Process/Application Layer
- ✓ Host-to-Host/Transport Layer

- ✓ Internet Layer
- ✓ Network Access/Link Layer

| Basics of TCP/IP Model | |
|---|---|
| **Full-Form** | Transmission Control Protocol/ Internet Protocol |
| **Developed By** | Department of Defense (DoD), United States |
| **Developed in** | During the 1970s |
| **Year for acknowledgement as a standard protocol by ARPANET** | 1983 |
| **Function of TCP** | Collecting and Reassembling Data Packets |
| **Function of IP** | Sending the Data Packets to the correct destination |
| **Number of Layers in TCP/IP Model** | 4 layers |

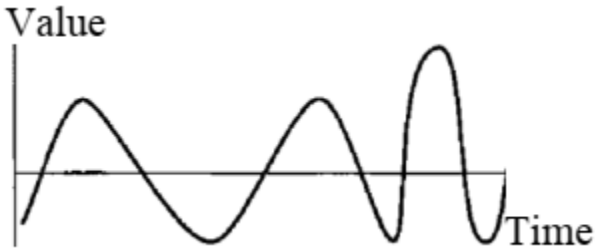
## 1.8 Analog Transmission

To send the digital data over an analog media, it needs to be converted into analog signal. There can be two cases according to data formatting.

Bandpass: The filters are used to filter and pass frequencies of interest. A bandpass is a band of frequencies which can pass the filter.

Low-pass: Low-pass is a filter that passes low frequencies signals.

When digital data is converted into a bandpass analog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into bandpass analog signal, it is called analog-to-analog conversion. Analog Transmission is the transmission of signals that vary smoothly with time, as shown in the diagram. An analog signal can take on any value in a specified range of values. A simple example is alternating current (AC), which continually varies between about +110 volts and -110 volts in a sine wave fashion 60 times per second




**1-4 Analog Transmission**

## 1.9 Digital Transmission

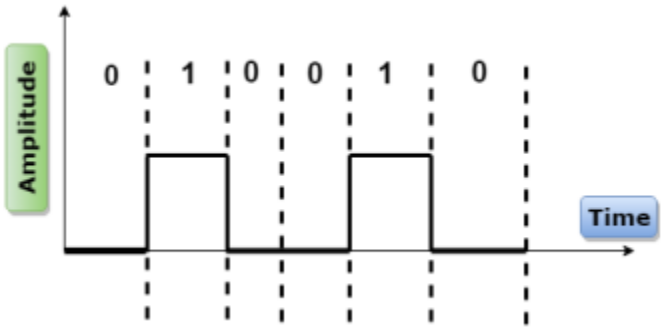
Digital Transmission is the transmission of signals that vary discretely with time between two values of some physical quantity, one value representing the binary number 0 and the other representing 1.

Transmission of signals that vary discretely with time between two values of some physical quantity, one value representing the binary number 0 and the other representing 1.

With copper cabling, the variable quantity is typically the voltage or the electrical potential. With fiber-optic cabling or wireless communication, variation in intensity or some other physical quantity is used.

Digital signals use discrete values for the transmission of binary information over a communication medium such as a network cable or a telecommunications link. On a serial transmission line, a digital signal is transmitted 1 bit at a time.

The opposite of digital transmission is analog transmission, in which information is transmitted as a continuously varying quantity. An analog signal might be converted to a digital signal using an analog-to-digital converter (ADC) and vice versa using a digital-to-analog converter (DAC). ADCs use a method called "quantization" to convert a varying AC voltage to a stepped digital one.

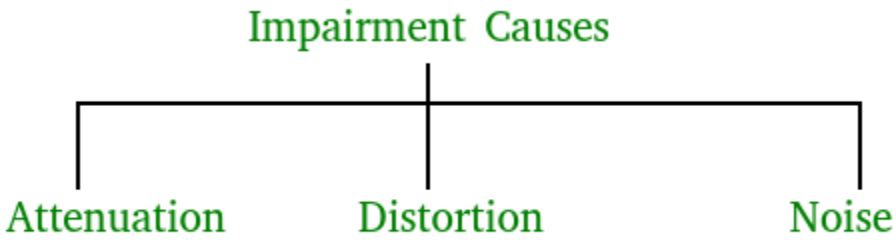



**1-5 Digital Transmission**

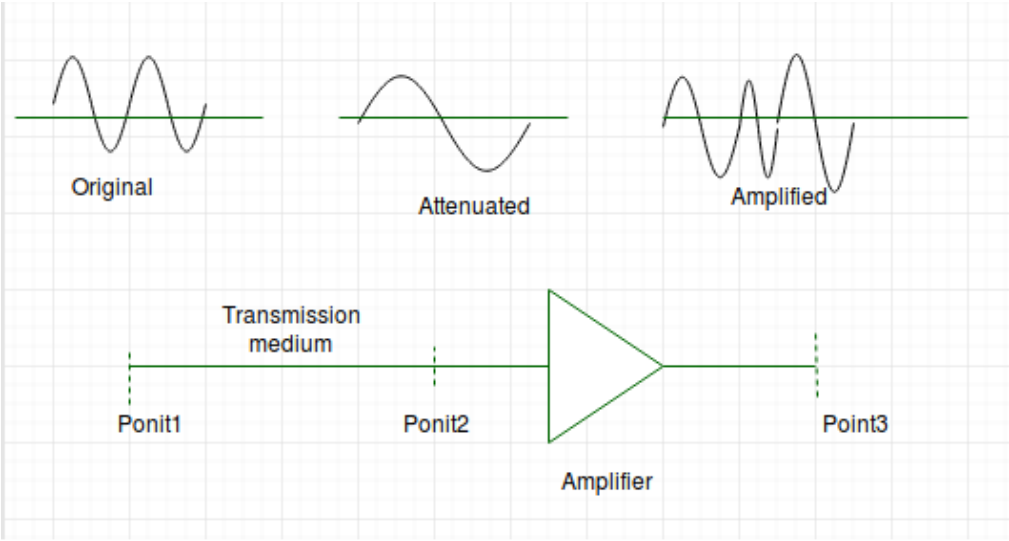
## 1.10 Signal impairment

In communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal, which means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. The imperfection causes signal impairment.

### Causes of impairment –




**Attenuation –** It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back and compensate for this loss.

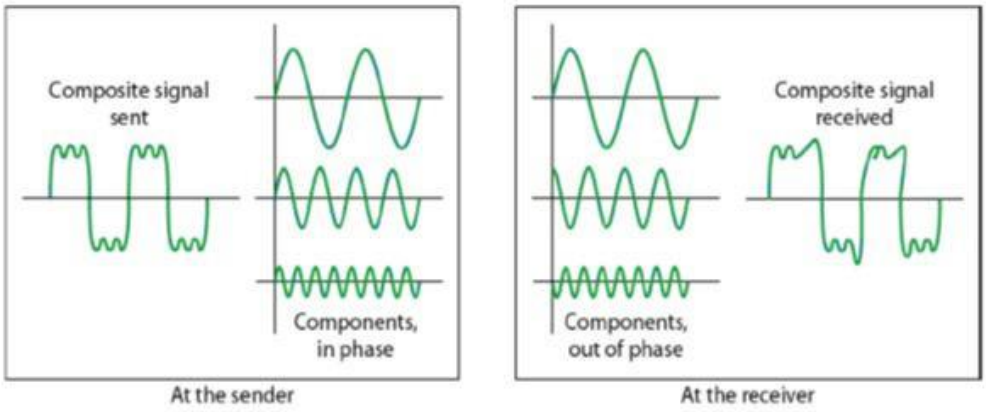



Attenuation is measured in **decibels (dB)**. It measures the relative strengths of two signals or one signal at two different point.

***Attenuation (dB) = 10log10 (P2/P1)***

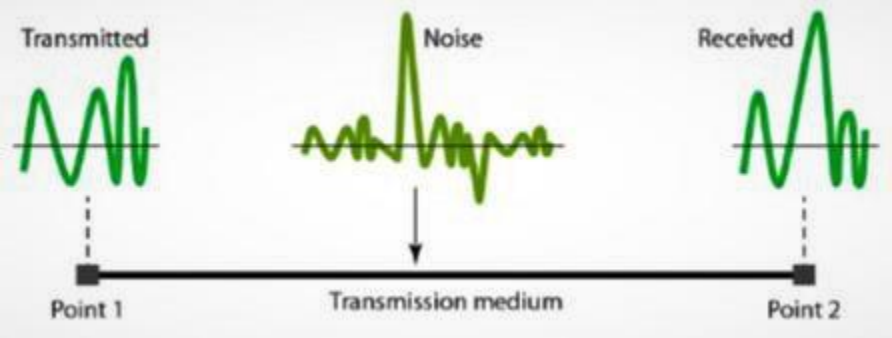
V1 is the voltage at sending end and V2 is the voltage at receiving end.

Distortion – It means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies. Each frequency component has its own propagation speed travelling through a medium. And that's why it delays in arriving at the final destination every component arrives at different time which leads to distortion. Therefore, they have different phases at receiver end from what they had at sender's end.




**Noise** – The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.

Induced noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium act as receiving antenna. Thermal noise is movement of electrons in wire which creates an extra signal. Crosstalk noise is when one wire affects the other wire. Impulse noise is a signal with high energy that comes from lightning or power lines.



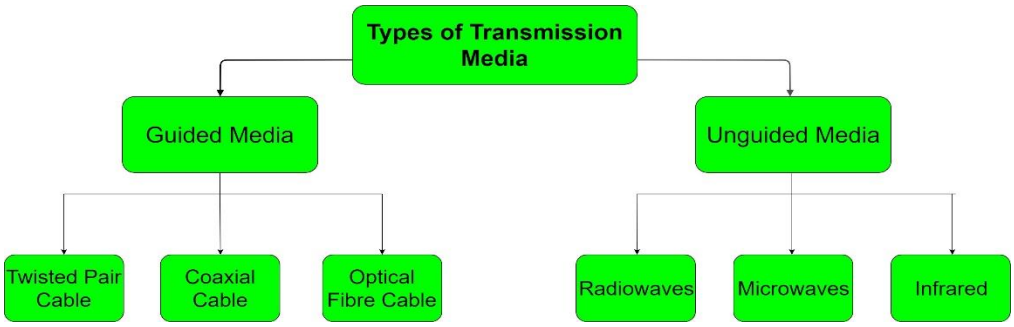

To find the theoretical bit rate limit, we need to know the ration .The signal-to-noise ratio is defined as

## 1.11 DATA TRANSMISSION

Data transmission is the process of sending digital or analog data over a communication medium to one or more computing, network, communication or electronic devices. It enables the transfer and communication of devices in a point-to-point, point-to-multipoint and multipoint-to-multipoint environment. Data transmission is also known as digital transmission or digital communications. Data transmission can be analog and digital but is mainly reserved for sending and receiving digital data. It works when a device or piece of equipment, such as a computer, intends to send a data object or file to one or multiple recipient devices, like a computer or server. The digital data originates from the source device in the form of discrete signals or digital bit streams. These data streams/signals are placed over a communication medium, such as physical copper wires, wireless carriers and optical fiber, for delivery to the destination/recipient device. Moreover, each outward signal can be baseband or passband.

In addition to external communication, data transmission also may be internally carried to a device. For example, the random-access memory (RAM) or hard disk that sends data to a processor is also a form of data transmission.

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:




**1-6 Types of Transmission Media**

## 1.12 What is Network Cabling?

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- ✓ Unshielded Twisted Pair (UTP) Cable
- ✓ Shielded Twisted Pair (STP) Cable
- ✓ Coaxial Cable
- ✓ Fiber Optic Cable

- ✓ Cable Installation Guides
- ✓ Wireless LANs
- ✓ Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

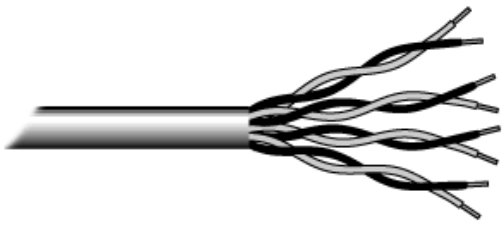


*Fig.1. Unshielded twisted pair*

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

### 1.12.1.1 Categories of Unshielded Twisted Pair

| Category | Speed | Use |
|---|---|---|
| 1 | 1 Mbps | Voice Only (Telephone Wire) |
| 2 | 4 Mbps | Local Talk & Telephone (Rarely used) |

| | | |
|---|---|---|
| 3 | 16 Mbps | 10BaseT Ethernet |
| 4 | 20 Mbps | Token Ring (Rarely used) |
| 5 | 100 Mbps (2 pair) | 100BaseT Ethernet |
| | 1000 Mbps (4 pair) | Gigabit Ethernet |
| 5e | 1,000 Mbps | Gigabit Ethernet |
| 6 | 10,000 Mbps | Gigabit Ethernet |

## Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

*Fig. 2. RJ-45 connector*

## 1.13Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

## 1.14 Coaxial Cable

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

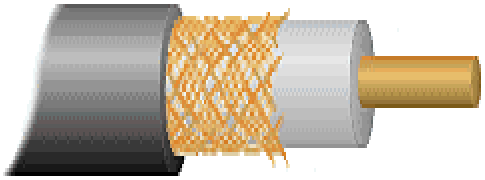


*Fig. 3. Coaxial cable*

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thin net. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thick net. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

## Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

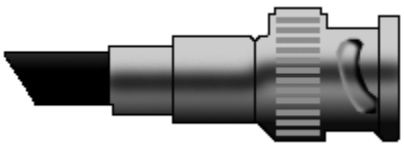


*Fig. 4. BNC connector*

## 1.15 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

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

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

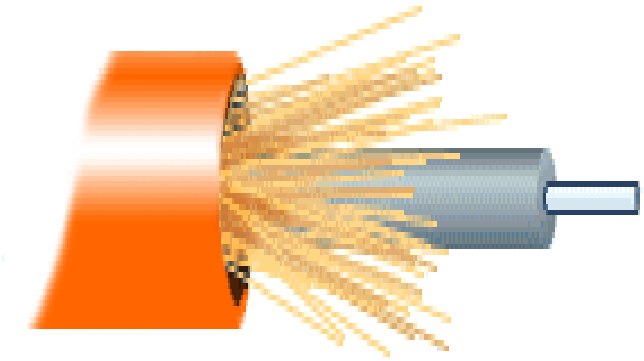


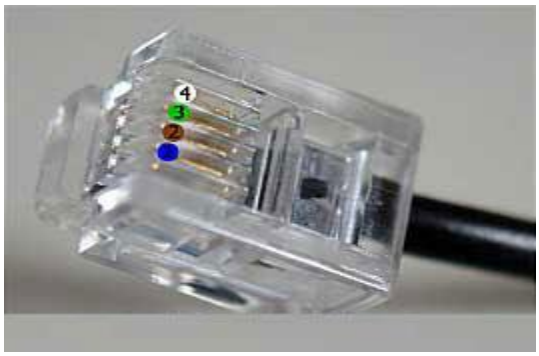
*Fig. 5. Fiber optic cable*

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

| Specification | Cable Type |
|---|---|
| **10BaseT** | Unshielded Twisted Pair |
| **10Base2** | Thin Coaxial |
| **10Base5** | Thick Coaxial |
| **100BaseT** | Unshielded Twisted Pair |
| **100BaseFX** | Fiber Optic |
| **100BaseBX** | Single mode Fiber |
| **100BaseSX** | Multimode Fiber |
| **1000BaseT** | Unshielded Twisted Pair |
| **1000BaseFX** | Fiber Optic |
| **1000BaseBX** | Single mode Fiber |
| **1000BaseSX** | Multimode Fiber |

## RJ-11 (Registered Jack)

Standard telephone cable connectors, **RJ-11** has 4 wires (and RJ-12 has 6 wires). **RJ-11** is the acronym for Registered Jack-11, a four- or six-wire connector primarily used to connect telephone equipment.




**1-7 RJ 11**

| RJ-11 Pin | Signal Name |
|---|---|
| 1 | VCC (5 volts regulated) |
| 2 | Power Ground |
| 3 | One Wire Data |
| 4 | One Wire Ground |

## RJ-45 (Registered Jack)

The acronym for **Registered Jack-45** is RJ-45. The **RJ-45** connector is an eight-wire connector that is commonly used to connect computers to a local area network (LAN), particularly Ethernet LANs. Although they are slightly larger than

the more commonly used **RJ-11** connectors, RJ-45s can be used to connect some

types of telephone equipment.

**1-8 RJ 45 Connector**

## 1.16 Telephony and Wireless Communication

Wireless communication can be used for cellular telephony, wireless access to the internet, wireless home networking, and so on

**Features of wireless telephony:**

As high acceptability of wireless telephony across world the wireless telephony requires a different set of features are as follows;

**1) High-Capacity Load Balancing:** The origin of wireless telephony to cover the smartphones, tablets, e-readers devices, etc. With the increased demand on the wireless telephony infrastructure, it must require incorporate high-capacity load balancing. The actual mean of load balancing is that when one access point is overloaded or number of users reaches up to the limit, the wireless telephony allows the system to actively shift wireless device users from one access point to another depending on the capacity that is available.

**2) Scalability:** The growth rate in popularity of new wireless gadgets has will only continue to grow. A wireless telephony needs to have the ability to start small, if

necessary, but expand in terms of coverage and capacity as needed without having to overhaul or build an entirely new network.

**3) Mobility:** Wireless telephony is more popular for their mobility features that assigning and controlling the wireless links for network connections. It provides the alerting function for wireless telephony devices for data completion to a wireless terminal.

**4) Centralized Management:** In current high technology world wireless telephony are much more complex and it may consist of hundreds or even thousands of access points. Therefore, wireless telephony will require a smarter way of managing all the access points within specified network that network is named as centralized management. Updates and configuration changes should be made once and the system updates all access points across over wireless telephony network.

**5) Real Time Wireless Visibility:** For all wireless telephony devices, administrator need to have the ability to see the wireless telephony network users in real time, what type of device uses are using, what type of coverage shows in that area, and the status of the different networking components that may affect the use of that device et. The wireless telephony administrator needs to be able to see what's going on in order to address any issues.

**6) Quality of Service/Application Prioritization:**

Quality of service simply means that wireless telephony system should be able to determine what uses are most important to their network.

## MCQs with answers

**1.** In a _____ connection, more than two devices can share a single link.
(a) Point-to-point
(b) Primary
(c) multi-point
(d) Secondary

**2.** Communication between a computer and a keyboard involves _____ transmission
(a) Full-duplex
(b) Half-duplex
(c) Simplex
(d) None of these

**3.** In a network with 25 computers, which topology would require the most extensive cabling?
(a) Star
(b) Mesh
(c) Bus
(d) None of these

**4.** The information to be communicated in a data communications system is the _____
a. Medium
b. Protocol
c. Transmission
d. Message

**5.** Which of the following items is not used in Local Area Networks (LANs)?

**a)** Computer Modem

**b)** Cable
**c)** Modem
**d)** Interface card

**6.** Which of the following represents the fastest data transmission speed?

**a)** Gbps
**b)** Kbps
**c)** Bps
**d)** Bandwidth

**7.** WI–FI uses

**a)** Phase line
**b)** Radio waves
**c)** Optic fiber
**d)** Sound waves

**8.** How many bits are there in the Ethernet address?

**a)** 6 bits
**b)** 32 bits
**c)** 48 bits
**d)** 64 bits

**9.** Which of the following is not a network device?

**a)** Router
**b)** Modem
**c)** Bridge
**d)** Switch

**10.** Frequency of failure and network recovery time after a failure are measures of the _____of a network.

**a)** Performance
**b)** Security
**c)** Reliability
**d)** Feasibility

**11.** Data flow between two devices can occur in a _____ way.

**a)** simplex
**b)** half-duplex
**c)** full-duplex
**d)** all of the above

**12.** The first Network was called _____
a) CNNET
b) NSFNET
c) ASAPNET
d) ARPANET

**13.** Which of this is not a network edge device?
a) PC
b) Smartphones
c) Servers
d) Switch

**14.** A _____ set of rules that governs data communication.
a) Protocols
b) Standards
c) RFCs
d) Servers

**15.** Three or more devices share a link in _____ connection.
a) Unipoint
b) Multipoint
c) Point to point
d) Simplex

| | | | | |
|---|---|---|---|---|
| 1. C | 2. C | 3. B | 4. D | 5. C |
| 6. A | 7. B | 8. C | 9. B | 10. C |
| 11. D | 12. D | 13. D | 14. A | 15. B |

## Short Questions

1. Define Analogue Signals?
2. Define Digital Signals?
3. Define data communication?
4. Define bounded media?
5. Define types of bounded media?
6. Define coaxial cable?
7. Define twisted pairs cables?
8. Define unguided media?
9. Define fiber optics?
10. Define data transmission?
11. Define half duplex?
12. Define full duplex?
13. Define data flow?
14. Define signal impairment?
15. Define connector?
16. Define network cabling?
17. Define STP cable?
18. Define OSI model?
19. Write briefly explain characteristics of data communication?
20. What is bandwidth

## Long Question

1. What is data communication also describe its modes?
2. What are the characteristics of data communication also describe with examples?
3. What is network cabling?

# 2 Data Link Control

## Objectives

**After completion of this chapter students will be able to:**

- ✓ Addressing scheme (Mac addresses)
- ✓ Error detection and correction

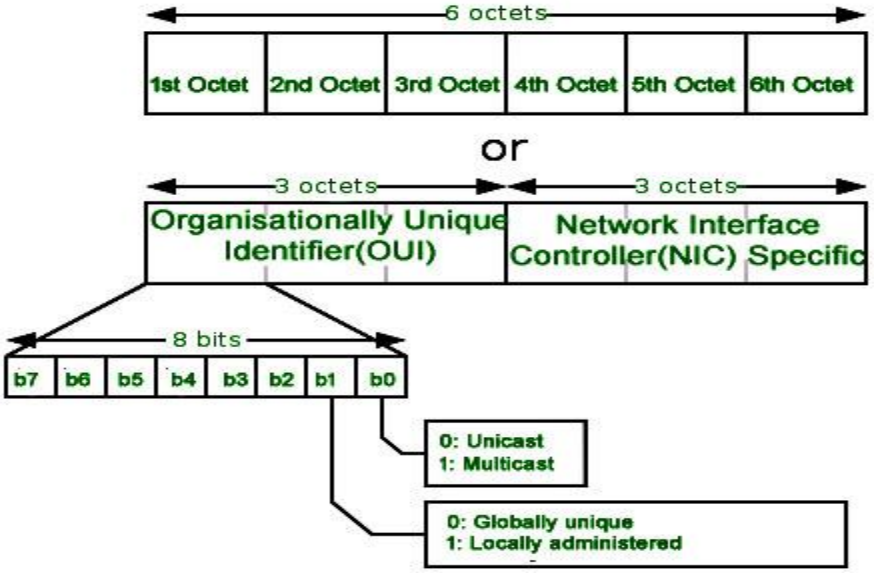
In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer.

## 2.1 Media Access Control (MAC) Address

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is worldwide unique, since millions of network devices exists and we need to uniquely identify each.




## 2.2 Format of MAC Address

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique Identifier**). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

Here are some OUI of well known manufacturers.

CC:46:D6 - Cisco

3C:5A:B4 - Google, Inc.

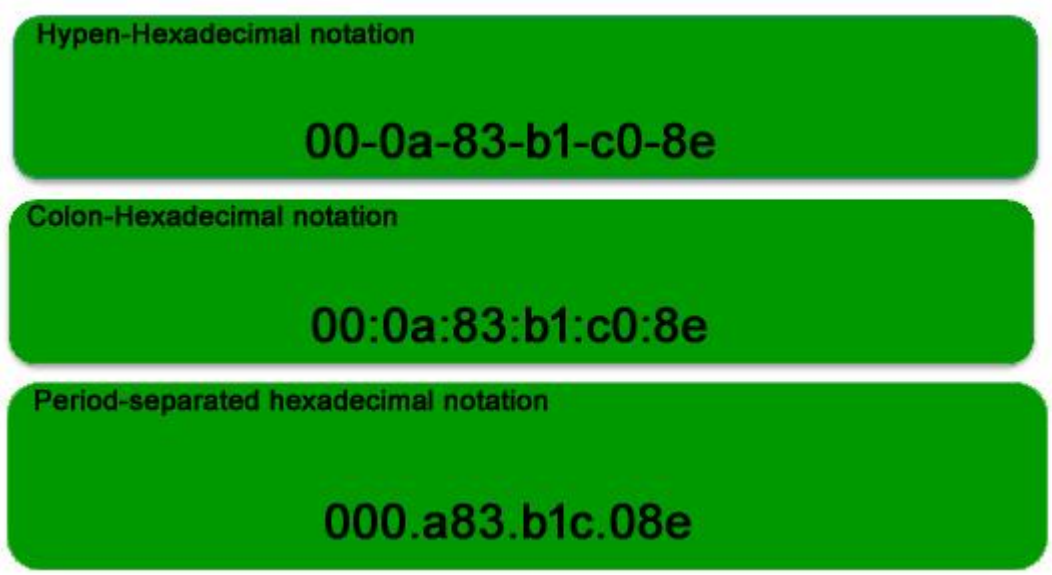
3C:D9:2B - Hewlett Packard

00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

The rightmost six digits represents **Network Interface Controller**, which is assigned by manufacturer.

As discussed above, MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory.

MAC address can be represented using any of the following formats:




**Note:** Colon-Hexadecimal notation is used by *Linux OS* and Period-separated Hexadecimal notation is used by *Cisco Systems*.

### 2.2.1 Types of MAC Address :

#### 1. Unicast

A Unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB (least significant bit) of first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.

#### 2.Multicast

Multicast address allow the source to send a frame to group of devices. In Layer-

2 (Ethernet) Multicast address, LSB (least significant bit) of first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.

### 3. Broadcast

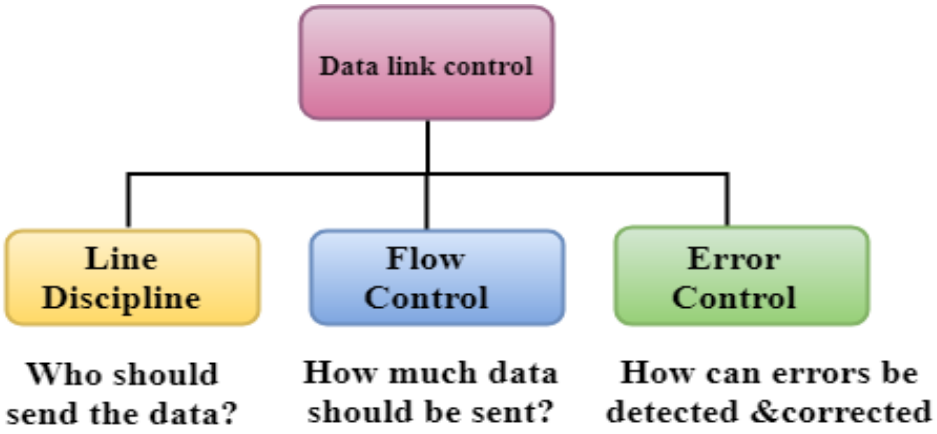
Similar to Network Layer, Broadcast is also possible on underlying layer( Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred as broadcast address. Frames which are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belong to that LAN segment.

**DATA LINK CONTROL**

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

## 2.3 The Data link layer provides three functions:

- ✓ Line discipline
- ✓ Flow Control
- ✓ Error Control




**2-1** Data Link Control

## 2.4 Line Discipline

✓ Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

### 2.4.1 Line Discipline can be achieved in two ways:

- ✓ ENQ/ACK
- ✓ Poll/select

**1. END/ACK**

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one. END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

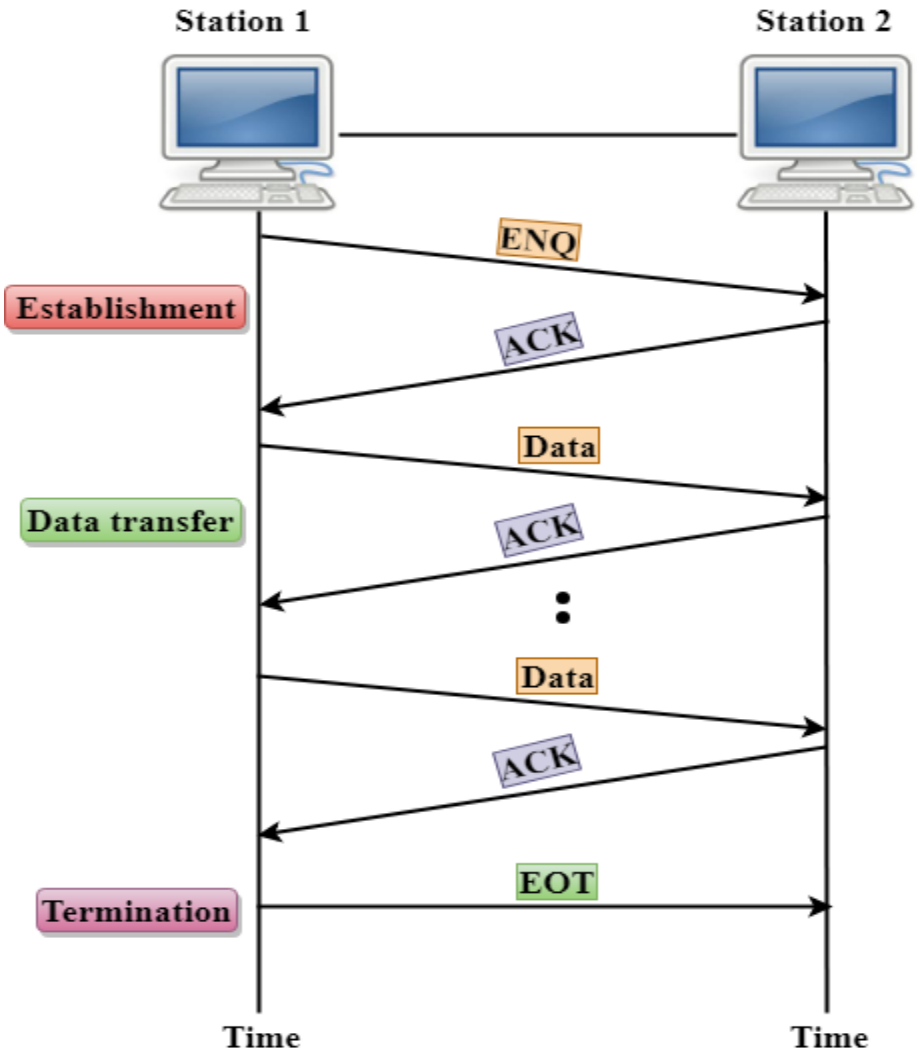
**Working of END/ACK**

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement (ACK) or with the negative acknowledgement (NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

**Following are the responses of the receiver:**

- ✓ If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- ✓ If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- ✓ If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.




ENQ/ ACK 1

2. **Poll/Select**

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

## Working of Poll/Select

✓ In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.

✓ The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.

✓ The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.

✓ If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.

✓ If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

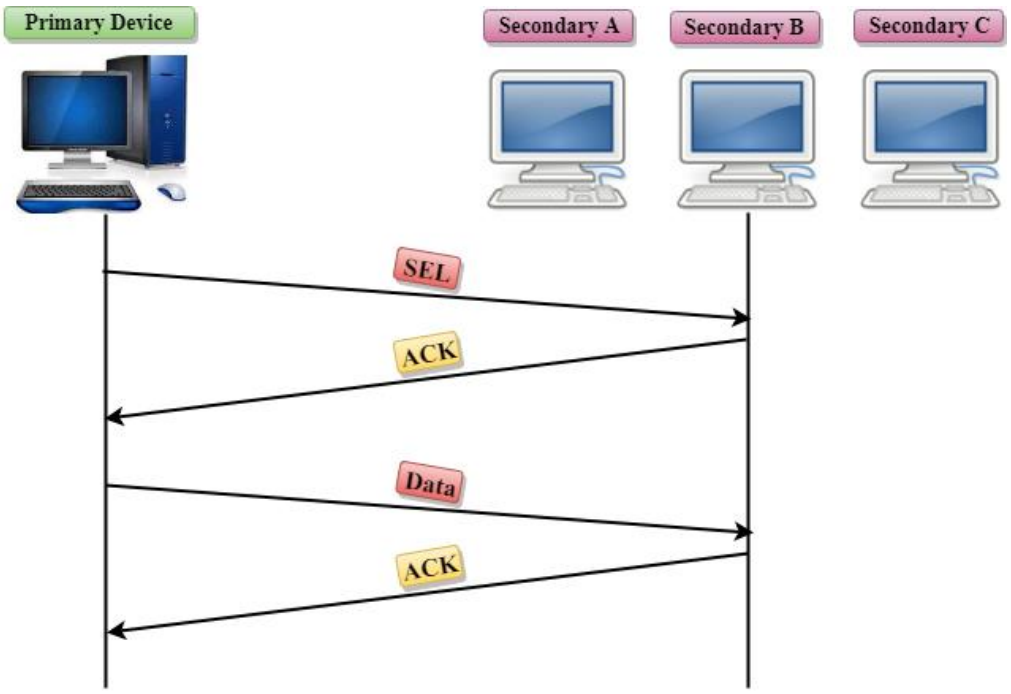
## Select

✓ The select mode is used when the primary device has something to send.

✓ When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.

✓ When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.

✓ If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.

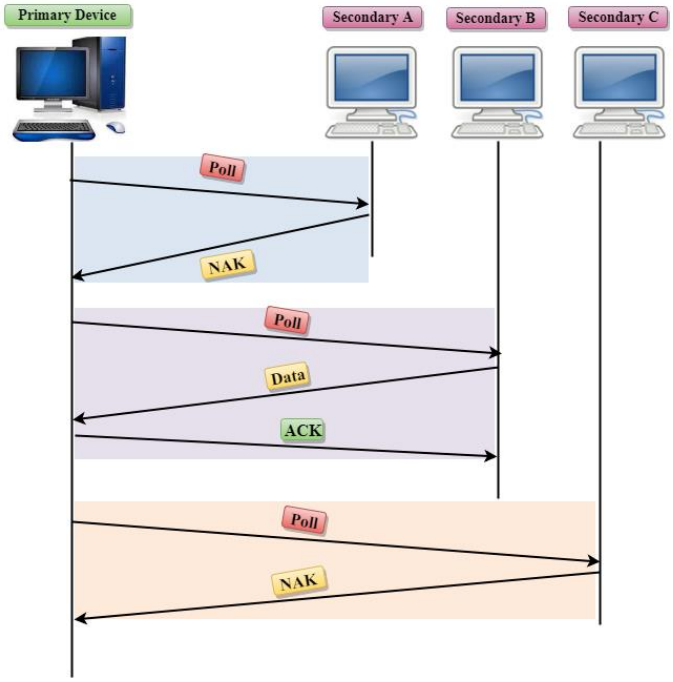



## Poll

✓ The Poll mode is used when the primary device wants to receive some data from the secondary device.

✓ When a primary device wants to receive the data, then it asks each device whether it has anything to send.

✓ Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.




**POLL 1**

## 2.5 Flow Control

✓ It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.

✓ The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.

✓ It requires a buffer, a block of memory for storing the information until they are processed.

### Two methods have been developed to control the flow of data:

✓ Stop-and-wait

✓ Sliding window

## Stop-and-wait

✓ In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.

✓ When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

## Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

## Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

## Sliding Window

✓ The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.

✓ In Sliding Window Control, multiple frames can be sent one after the other due to which capacity of the communication channel can be utilized efficiently.

✓ A single ACK acknowledge multiple frames.

✓ Sliding Window refers to imaginary boxes at both the sender and receiver end.

✓ The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.

✓ Frames can be acknowledged even when the window is not completely filled.

✓ The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....

✓ The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.

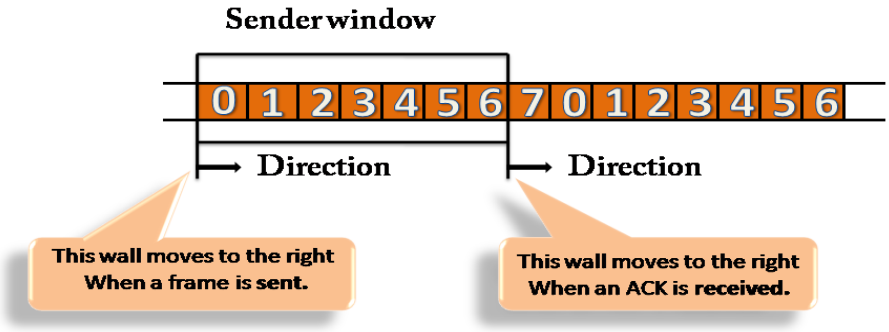
✓ When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

## Sender Window

✓ At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.

✓ Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.

✓ For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).




## Receiver Window

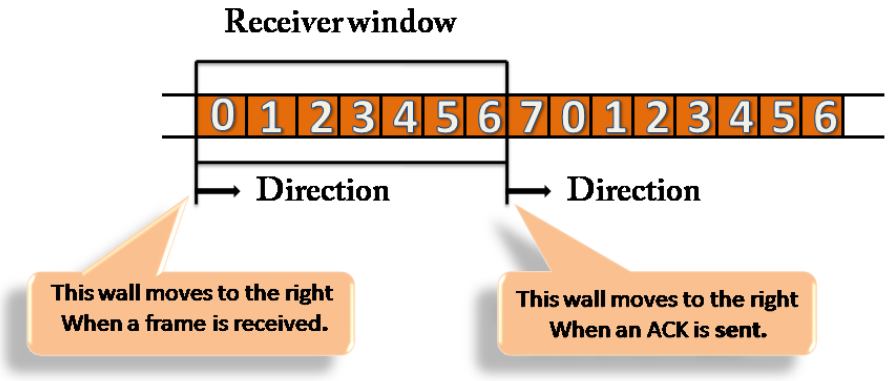
✓ At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.

✓ When the new frame arrives, the size of the window shrinks.

✓ The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).

✓ Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.

✓ Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.




## 2.6 What is Error Correction and Detection?

**Error detection** and correction has great practical importance in maintaining data (information) integrity across noisy Communication Networks channels and less than reliable storage media.

**Error Correction:** Send additional information so incorrect data can be corrected and accepted. Error correction is the additional ability to reconstruct the original, error-free data.

There are two basic ways to design the channel code and protocol for an error correcting system:

**Automatic Repeat-Request (ARQ):** The transmitter sends the data and also an error detection code, which the receiver uses to check for errors, and request re-transmission of erroneous data.

In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time.

**Forward Error Correction (FEC):** The transmitter encodes the data with an error-correcting code (ECC) and sends the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives into the "most likely" data.

The codes are designed so that it would take an "unreasonable" amount of noise to trick the receiver into misinterpreting the data.

**Error Detection:**

Send additional information so incorrect data can be detected and rejected. Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.

**Error Detection Schemes:**

In telecommunication, a redundancy check is extra data added to a message for the purposes of error detection. Several schemes exist to achieve error detection, and are generally quite simple. All error detection codes transmit more bits than were in the original data. Most codes are "systematic": the transmitter sends a fixed number of original data bits, followed by fixed number of check bits usually referred to as redundancy which are derived from the data bits by some deterministic algorithm.

The receiver applies the same algorithm to the received data bits and compares its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission.

In a system that uses a "non-systematic" code, such as some raptor codes, data bits are transformed into at least as many code bits, and the transmitter sends only the code bits.

**Repetition Schemes:**

Variations on this theme exist. Given a stream of data that is to be sent, the data is broken up into blocks of bits, and in sending, each block is sent some predetermined number of times. For example, if we want to send "1011", we

may repeat this block three times each. Suppose we send “1011 1011 1011”, and this is received as “1010 1011 1011”.

As one group is not the same as the other two, we can determine that an error has occurred. This scheme is not very efficient, and can be susceptible to problems if the error occurs in exactly the same place for each group e.g., “1010 1010 1010”

in the example above will be detected as correct in this scheme. The scheme however is extremely simple, and is in fact used in some transmissions of numbers stations.

**Parity Schemes:**

A parity bit is an error detection mechanism. A *parity bit* is an extra bit transmitted with a data item, chose to give the resulting bit seven or odd parity. *Parity* refers to the number of bits set to 1 in the data item. There are 2 types of parity

✓ ***Even parity*** – an even number of bits are 1 Even parity – data: 10010001, parity bit 1

✓ ***Odd parity*** – an odd number of bits are 1 Odd parity – data: 10010111, parity bit 0

The stream of data is broken up into blocks of bits, and the number of 1 bits is counted. Then, a “parity bit” is set (or cleared) if the number of one bits is odd (or even). This scheme is called even parity; odd parity can also be used. There is a limitation to parity schemes. A parity bit is only guaranteed to detect an odd number of bit errors (one, three, five, and so on). If an even number of bits (two, four, six and so on) are flipped, the parity bit appears to be correct, even though the data is corrupt. For example

- Original data and parity: 10010001+1 (even parity)
- Incorrect data: 10110011+1 (even parity!)

Parity usually used to catch one-bit errors

**MCQ WITH ANSWER**

1. How many fields frame in High-level Data Link Control (HDLC) may contain?

   A. three fields
   B. four fields
   C. five fields
   D. six fields

2. _____ control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

   A. Flow
   B. Error
   C. Transmission
   D. none of the above

3. _____ control refers to methods of error detection and correction.

   A. Flow
   B. Error
   C. Transmission
   D. none of the above

4. _____control in the data link layer is based on automatic repeat request, which is the retransmission of data.

   A. Flow
   B. Error
   C. Transmission
   D. none of the above

5. ARQ stands for _____.

   A. Automatic repeat quantization
   B. Automatic repeat request
   C. Automatic retransmission request
   D. Acknowledge repeat request

6. Both Go-Back-N and Selective-Repeat Protocols use a _____.

   A. sliding frame
   B. sliding window
   C. sliding packet
   D. none of the above

7. Data link control deals with the design and procedures for _____ communication.

   A. node-to-node
   B. host-to-host
   C. process-to-process
   D. none of the above

8. HDLC is an acronym for _____.

   A. High-duplex line communication
   B. High-level data link control
   C. Half-duplex digital link combination
   D. Host double-level circuit

9. In _____ framing, there is no need for defining the boundaries of frames.

   A. fixed-size
   B. variable-size
   C. standard
   D. none of the above

10. In _____ protocols, we use _____.

    A. character-oriented; byte stuffing
    B. character-oriented; bit stuffing
    C. bit-oriented; character stuffing
    D. none of the above

11. In _____, the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary.

    A. ABM
    B. NRM
    C. ARM
    D. NBM

12. In a _____ protocol, the data section of a frame is a sequence of bits.

    A. byte-oriented
    B. bit-oriented
    C. either (a) or (b)
    D. none of the above

13. In a _____ protocol, the data section of a frame is a sequence of characters.

    A. bit-oriented
    B. character-oriented
    C. either (a) or (b)
    D. none of the above

14. In PPP, _____ is a simple authentication procedure with a two-step process:

    A. NCP
    B. LCP
    C. CHAP
    D. PAP

15. In Selective Repeat ARQ, if 5 is the number of bits for the sequence number, then the maximum size of the receive window must be _____

    A. 15
    B. 16

C. 31
D. 1

16. In the _____ Protocol, the sender sends one frame, stops until it receives confirmation from the receiver, and then sends the next frame.

A. Stop-and-Wait
B. Simplest
C. Go-Back-N ARQ
D. Selective-Repeat ARQ

17. Stop-and-Wait ARQ is a special case of Go-Back-N ARQ in which the size of the send window is 1.

A. 2
B. 1
C. 8
D. none of the above

18. The _____ Protocol has flow control, but not error control.

A. Stop-and-Wait
B. Simplest
C. Go-Back-N ARQ
D. Selective-Repeat ARQ

19. The _____Protocol has both flow control and error control.

A. Stop-and-Wait
B. Go-Back-N ARQ
C. Selective-Repeat ARQ
D. both (b) and (c)

20. The Simplest Protocol and the Stop-and-Wait Protocol are for _____ channels.

A. noisy
B. noiseless
C. either (a) or (b)
D. neither (a) nor (b)

| | | | | |
|---|---|---|---|---|
| 1. D | 2. A | 3. A | 4. B | 5. B |
| 6. B | 7. A | 8. B | 9. A | 10. A |
| 11. B | 12. B | 13. B | 14. D | 15. B |
| 16. A | 17. B | 18. A | 19. D | 20. B |

**Short Questions**

1. Define DLC?
2. Define HDLC?
3. Define SDLC?
4. Define ARQ?
5. Define protocol?
6. Define MAC layer?
7. Define flow control
8. Define error control
9. What is error?
10. Advantage and disadvantage of Stop-and-wait

**Long Question**

1. Detail note on Flow control?
2. Detail notes on Error detection & correction?
3. Write a detail note on Mac Address

# 3 What is Multiplexing?

## Objectives

**After completion of this chapter students will be able to:**

- ✓ Frequency-Division Multiplexing
- ✓ 3.2. Time-Division Multiplexing

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

De-multiplexing is achieved by using a device called De-multiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that de-multiplexing follows the one-to-many approach.

### Why Multiplexing?

✓ The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.

✓ If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.

✓ When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.

✓ Transmission services are very expensive.

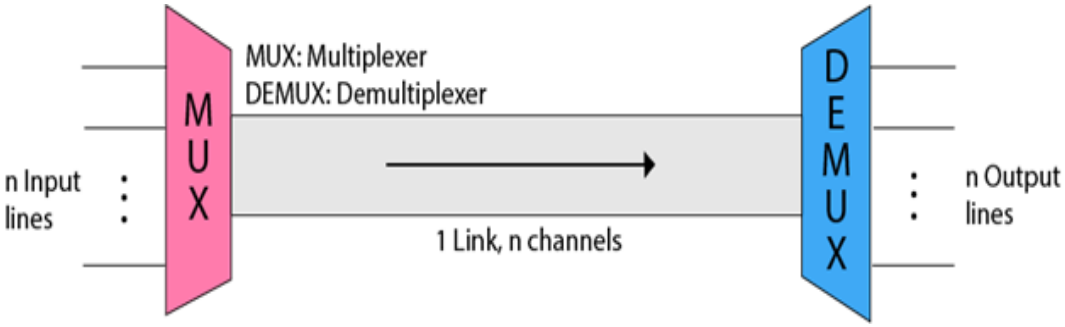
## History of Multiplexing

✓ Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.

✓ Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.

✓ George Owen Squire developed the **telephone carrier multiplexing** in 1910.

## Concept of Multiplexing




**MULTIPLEXING 1**

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

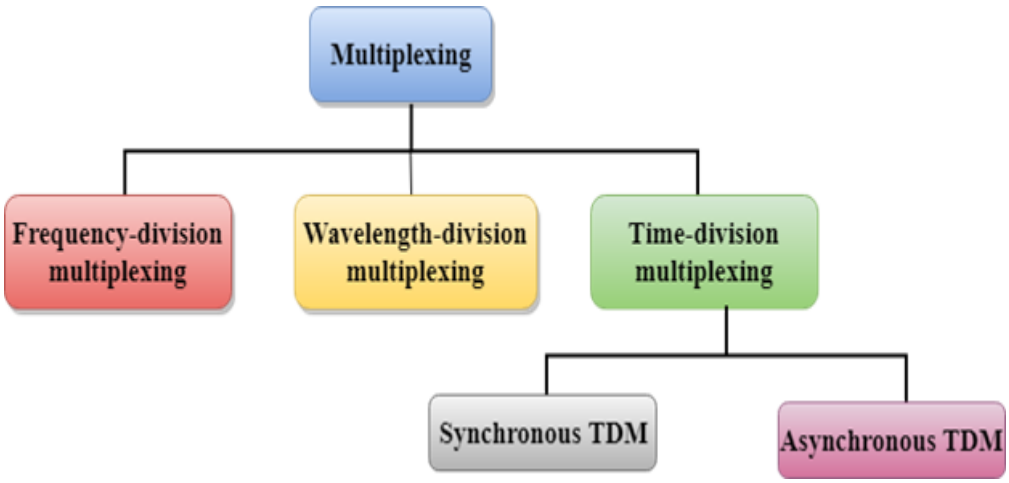
✓ The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

## 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

Multiplexing techniques can be classified as:

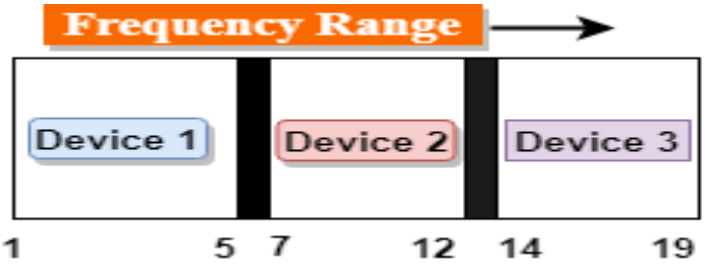



**Techniques Of Multiplexing 1**

## 3.1 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 channels.




✓ 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.

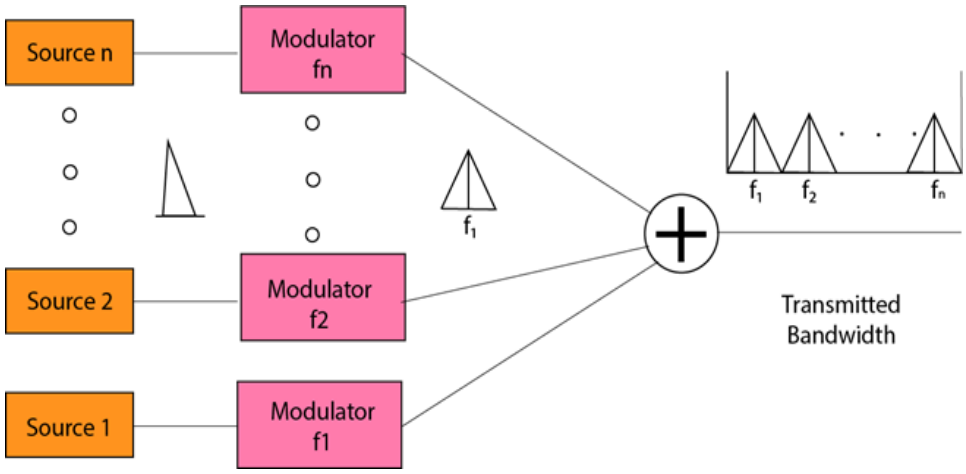
✓ The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.

✓ 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.




**FDM 1**

**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.

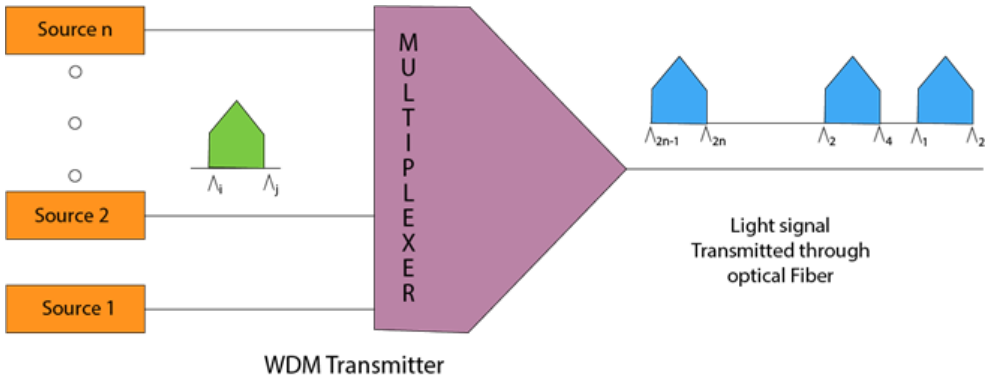
✓ It requires a high bandwidth channel.

**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.

## 3.2 Wavelength Division Multiplexing (WDM)




✓ Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fiber optic cable.

✓ WDM is used on fiber optics to increase the capacity of a single fiber.

✓ It is used to utilize the high data rate capability of fiber optic cable.

✓ It is an analog multiplexing technique.

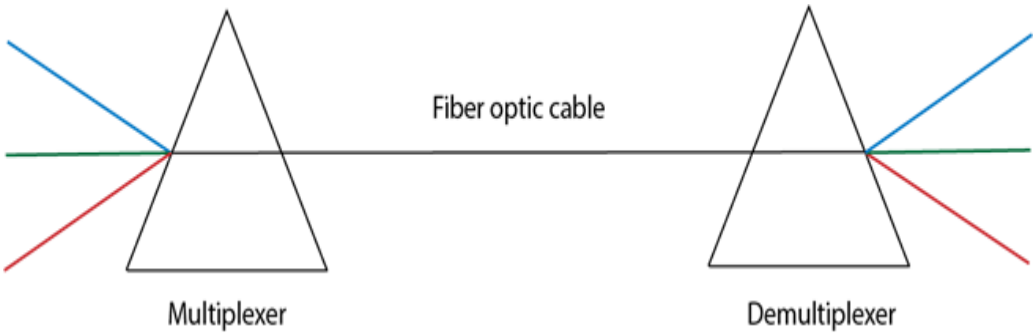
✓ Optical signals from different source are combined to form a wider band of light with the help of multiplexer.

✓ At the receiving end, de-multiplexer separates the signals to transmit them to their respective destinations.

✓ Multiplexing and De-multiplexing 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 fiber optical cable.

✓ Prism also performs a reverse operation, i.e., de-multiplexing the signal.




**FIBER OPTIC CABLE 1**

## 3.3 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.

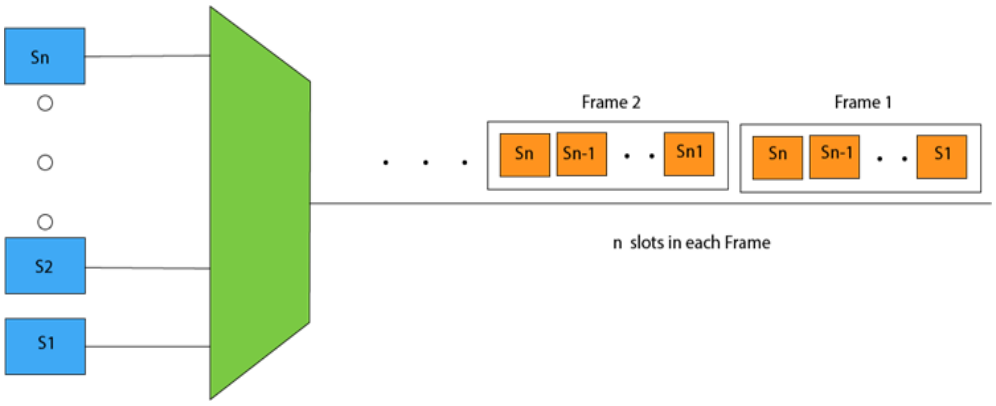
✓ In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.

✓ 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.

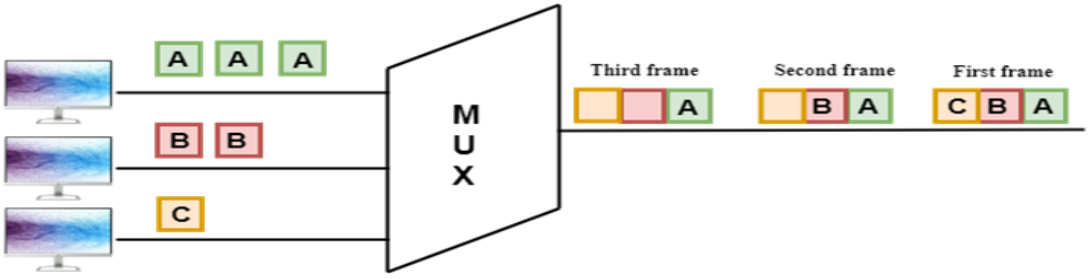
✓ The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.

✓ If there are n devices, then there are n slots.




**TDM 1**

**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.

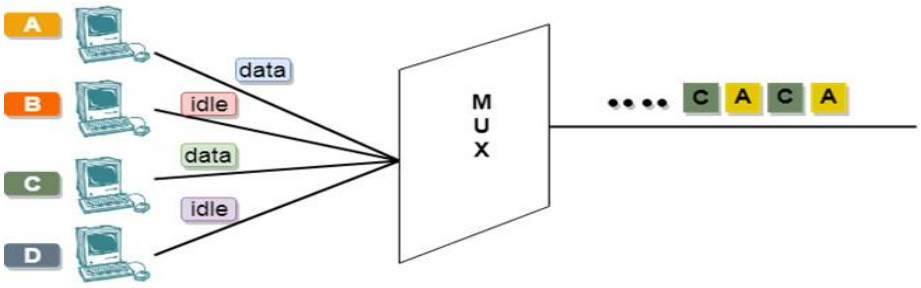
✓ In Asynchronous TDM, each slot contains an address part that identifies the source of the data.


✓ 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**).

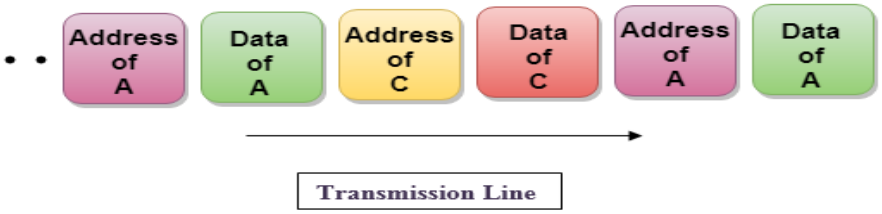
✓ The number of slots in a frame depends on the statistical analysis of the number of input lines.

**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.

**Frame of above diagram can be represented as:**




The above figure shows that the data part contains the address to determine the source.

## MCQ WITH Answers

1. The sharing of a medium and its link by two or more devices is called _____
   a) Fully duplexing
   b) Multiplexing
   c) Micropleixng
   d) Duplexing
2. Multiplexing is used in _____
   a) Packet switching
   b) Circuit switching
   c) Data switching
   d) Packet & Circuit switching
3. Which multiplexing technique used to transmit digital signals?
   a) FDM
   b) TDM
   c) WDM
   d) FDM & WDM
4. If link transmits 4000frames per second, and each slot has 8 bits, the transmission rate of circuit this TDM is _____
   a) 32kbps
   b) 500bps
   c) 500kbps
   d) 32bps
5. The state when dedicated signals are idle are called _____
   a) Death period
   b) Poison period
   c) Silent period
   d) Stop period
6. Multiplexing provides _____
   a) Efficiency
   b) Privacy

c) Anti jamming
d) Both Efficiency & Privacy

**7.** In TDM, slots are further divided into _____
a) Seconds
b) Frames
c) Packets
d) Bits

**8.** The sharing of a medium and its link by two or more devices is called _____.
a. modulation
b. encoding
c. line discipline
d. multiplexing

**9.** Which multiplexing technique transmits digital signals?
a. WDM
b. FDM
c. TDM
d. None of the above

**10.** The sharing of a medium and its link by two or more devices is called _____.
a. modulation
b. multiplexing
c. encoding
d. line discipline

| | | | | |
|---|---|---|---|---|
| 1.B | 2.B | 3.B | 4.A | 5.C |
| 6.D | 7.B | 8.D | 9.c | 10.b |

## SHORT QUESTIONS

1. Define Multiplexing?
2. Explain types of Multiplexing?
3. Define TDM?
4. Define FDM?
5. Define WDM?
6. Define Multiplexer?
7. What is transmitter?
8. Define receiver?
9. Explain the use of FDM?
10. Define synchronous TDM?

## Long Question

1. Write the detail note on Multiplexing?
2. Describe Types of Multiplexing

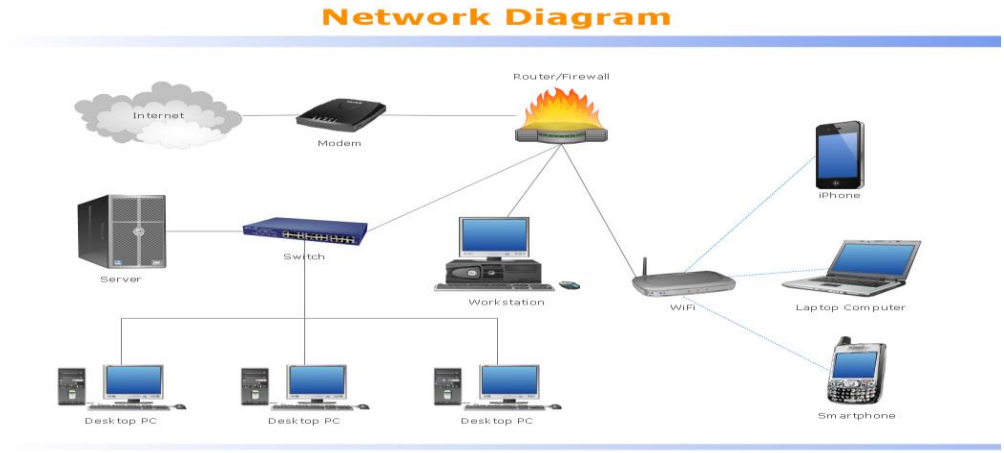
# 4 Local Area Network (LAN)

## Objectives

**After completion of this chapter students will be able to:**

- ✓ LAN Architecture
- ✓ Learn About Topologies
- ✓ Learn About LAN Systems
- ✓ Learn About Ethernet and Fast Ethernet (CSMA/CD)
- ✓ Learn About Token Ring and FDDI

**A local area network (LAN)** is a devices network that connect with each other in the scope of a home, school, laboratory, or office. Usually, a LAN comprise computers and peripheral devices linked to a local domain server. All network appliances can use a shared printers or disk storage. A local area network serve for many hundreds of users. Typically, LAN includes many wires and cables that demand a previously designed network diagram. They are used by IT professionals to visually document the LANs physical structure and arrangement. Concept Draw - Perfect Network Diagramming Software with examples of LAN Diagrams. Concept Draw Network Diagram is ideal for network engineers and network designers who need to draw Local Area Network diagrams.




**NETWORK DIAGRAM 1**

The **architecture** on which you choose to base your network is the single most important decision you make when setting up a LAN. The architecture defines the speed of the network, the medium access control mechanism it uses (for example, collision detection, token passing, and so on), the types of cables you can use, the network interface adapters you must buy, and the adapter drivers you install.

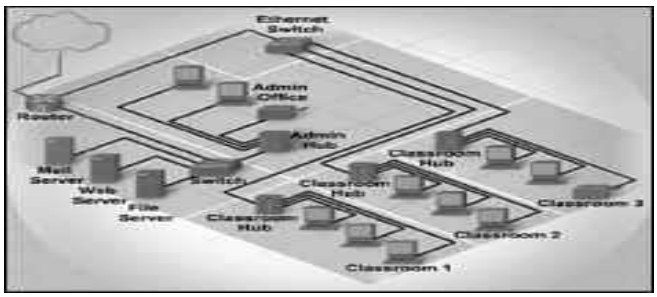
The **Institute of Electrical and Electronic Engineers (IEEE)** has defined and documented a set of standards for the physical characteristics of both collision-detection and token-passing networks. These standards are known as **IEEE 802.3 (Ethernet)** and **IEEE 802.5 (Token-Ring)**, respectively. **IEEE 802.11 (Wi-Fi)** defines wireless versions of Ethernet.

*Note: Be aware, however, that the colloquial names Ethernet and Token-Ring actually refer to earlier versions of these architectures, on which the IEEE standards were based. Minor differences exist between the frame definitions for true Ethernet and true IEEE 802.3. In terms of the standards, IBM's 16 Mb/s Token-Ring products are an extension of the IEEE 802.5 standard.*

## 4.1 LAN Architecture

Most of the computers that you work on will be part of a network. Topologies and architectures are building blocks for designing a computer network. Although you may not build a computer network, you need to understand how they are designed so that you can work on computers that are part of a network.

A LAN architecture is built around a topology. A LAN architecture comprises all the components that make up the structure of a communications system. These components include the hardware, software, protocols, and sequence of operations.



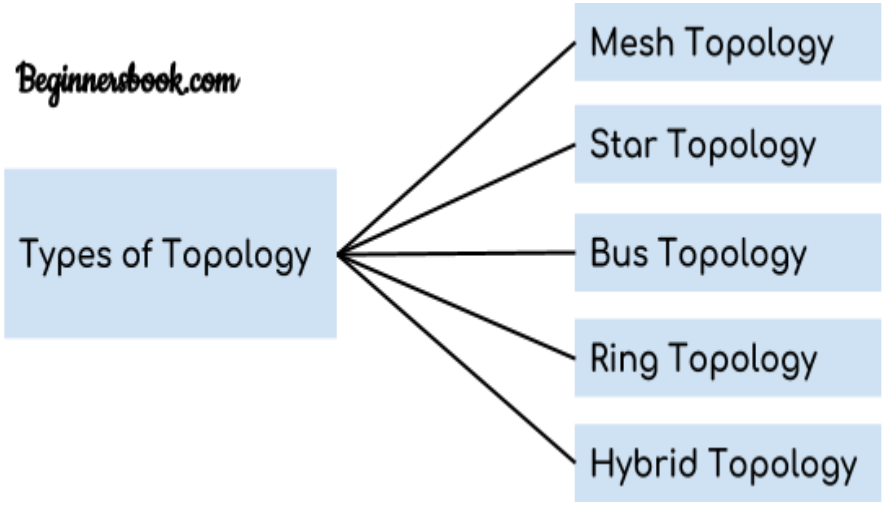

**Lan Architecture 1**

## 4.2 Topology

Geometric representation of how the computers is connected to each other is known as topology**.** There are five types of topologies – Mesh, Star, Bus, Ring and Hybrid.

### Types of Topologies

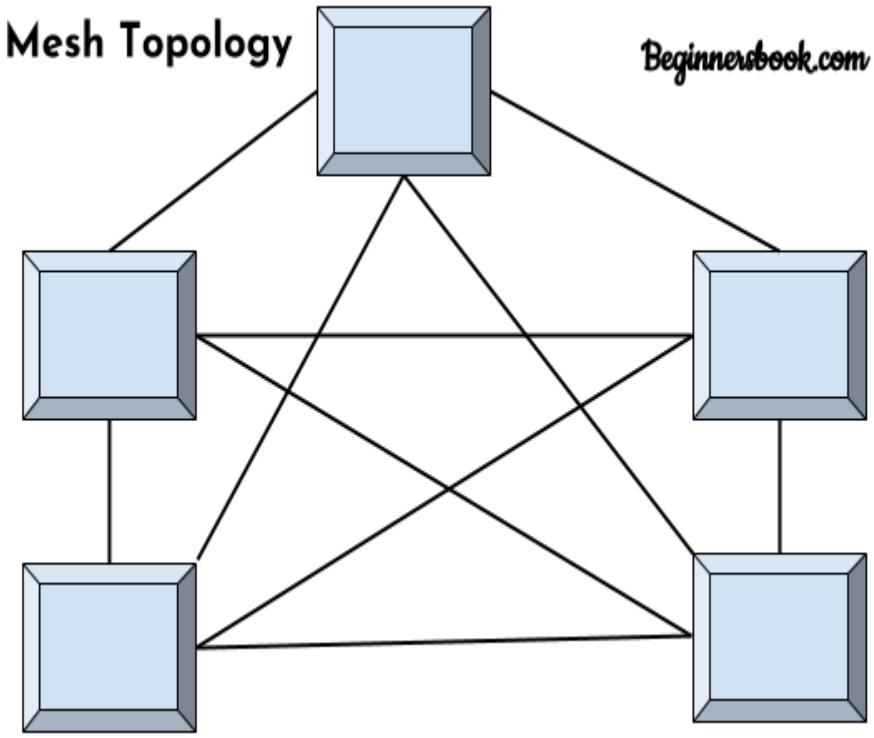
There are five types of topology in computer networks:




1. Mesh Topology

2. Star Topology
3. Bus Topology
4. Ring Topology
5. Hybrid Topology

### 4.2.1 Mesh Topology




**Mesh Topology 1**

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated, it means that the link only carries data for the two connected devices only. Let's say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

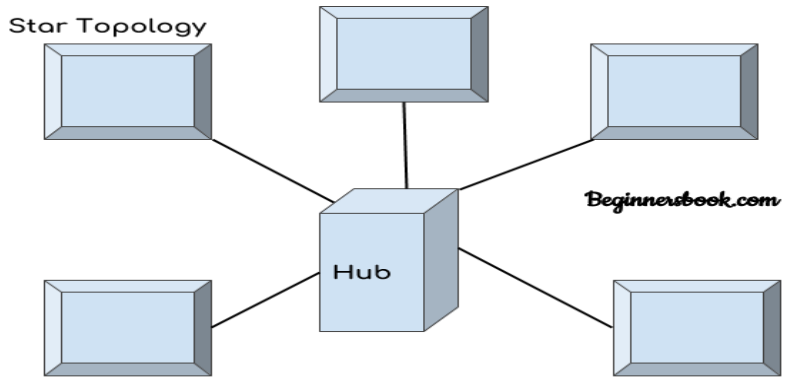
## Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point-to-point link thus unauthorized access is not possible.
4. Fault detection is easy.

## Disadvantages of Mesh topology

1. Number of wires required to connected each system is tedious and headache.
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

### 4.2.2 Star Topology




**Star Topology 1**

In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn't allow direct

communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmits that data to the designated device.

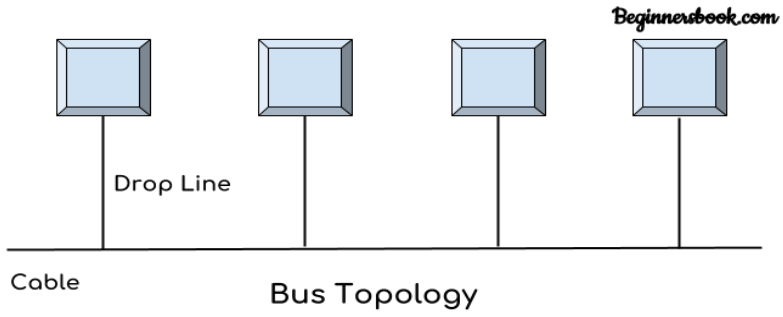
## Advantages of Star topology

1. Less expensive because each device only needs one I/O port and needs to be connected with hub with one link.
2. Easier to install
3. Less number of cables required because each device needs to be connected with the hub only.
4. Robust, if one link fails, other links will work just fine.
5. Easy fault detection because the link can be easily identified.

## Disadvantages of Star topology

1. If hub goes down everything goes down, none of the devices can work without hub.
2. Hub requires more resources and regular maintenance because it is the central system of star topology.

### 4.2.3 Bus Topology




**Bus Topology 1**

In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

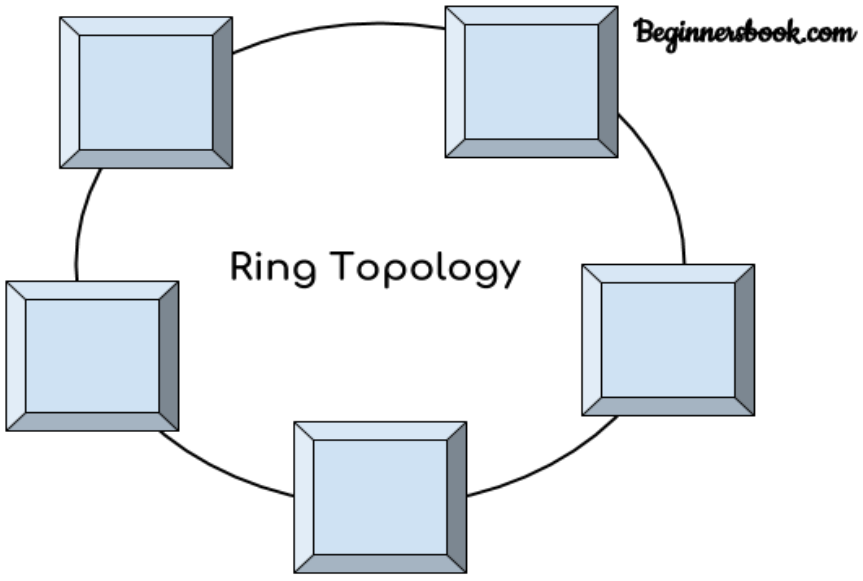
## Advantages of bus topology

1. Easy installation, each cable needs to be connected with backbone cable.
2. Less cables required than Mesh and star topology

## Disadvantages of bus topology

1. Difficultly in fault detection.
2. Not scalable as there is a limit of how many nodes you can connect with backbone cable.

### 4.2.4 Ring Topology




**Ring Topology 1**

In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device, then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device, then repeater forwards this data until the intended device receives it.

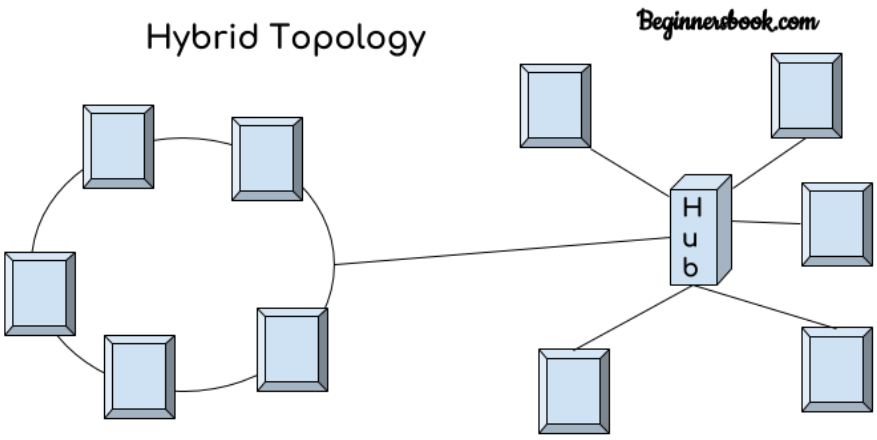
## Advantages of Ring Topology

1. Easy to install.
2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.

## Disadvantages of Ring Topology

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

### 4.2.5 Hybrid topology




**Hybrid Topology 1**

A combination of two or more topology is known as hybrid topology. For example, a combination of star and mesh topology is known as hybrid topology.

## Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

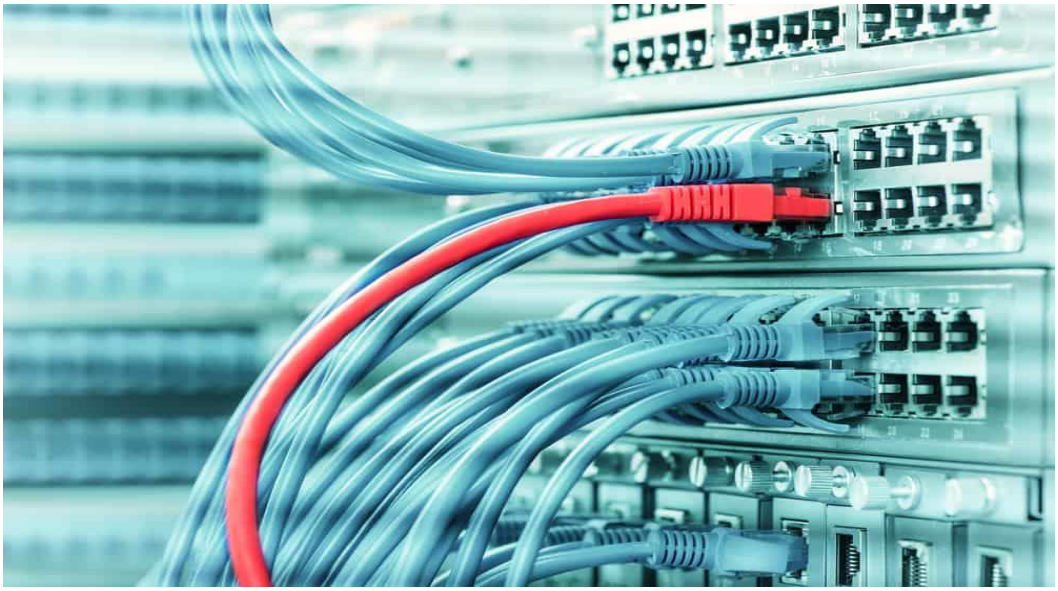
## Disadvantages of Hybrid topology

- ✓ Fault detection is difficult.
- ✓ Installation is difficult.
- ✓ Design is complex so maintenance is high thus expensive.

## 4.3 LAN SYSTEM

### 4.3.1 Ethernet

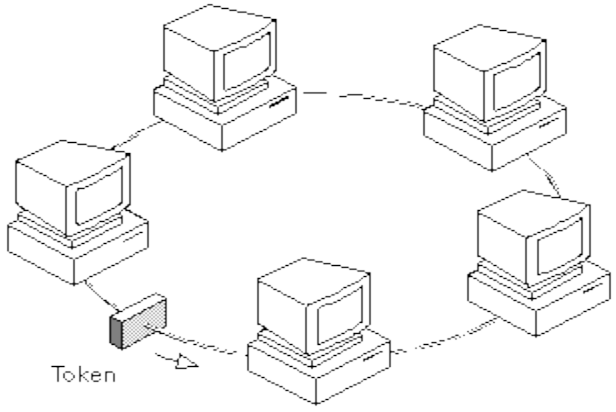
Ethernet is the most common network technology used in local area networks and can be easily identified by the RJ-45 connectors on each of their cables, which resemble extra-wide telephone jacks. Ethernet cables, which are usually blue, yellow or red, are a little slenderer than a drinking straw and have a maximum range of 328 feet. Ethernet can carry up to 10 megabits per second (Mbps), which is 10 million bits of information each second. Fast Ethernet can carry up to 100Mbps and gigabit Ethernet can carry up to 1000Mbps. Data is sent in packets, with each packet containing information to determine where the data is to be sent and a checksum that ensures that none of the data in the packet has been garbled or lost during transmission. One of the reasons Ethernet is so popular is because it supports the Transmission Control Protocol and Internet Protocol used by the Internet, a set of protocols familiarly known as TCP/IP.



### 4.3.2 Token Ring

Developed by IBM, Token ring was once a popular technology used in LANs before most organizations moved to Ethernet. Today it can be difficult to find. As its name suggests, computers are arranged in a ring and single token is continuously passed from computer to computer. When a computer wants to send data to another computer, it waits for the token to come around and then attaches its data to it. The token is then passed to the next computer in the ring until it reaches the recipient computer. The recipient attaches two bits of data to the token to inform the sender that the data was received. Other computers can't send data until the ring is free again. This may sound slow, but was actually lightning fast for its time - up to 16Mpbs.

A token ring is a data link for a local area network (LAN) in which all devices are connected in a ring or star topology and pass one or more tokens from host to host. A token is a frame of data transmitted between network points. Only a host that holds a token can send data, and tokens are released when receipt of the data is confirmed. IBM developed token ring technology in the 1980s as an alternative to Ethernet.




**What is a token ring network?**

Also known as IEEE (Institute of Electrical and Electronics Engineers) 802.5, a token ring network connects all devices, including computers, in a circular or closed-loop manner. In this scenario, the word token describes a segment of data sent through the network.

Token ring networks prevent data packets from colliding on a network segment because only a token holder can send data, and the number of tokens available is also controlled. When a device on the network successfully decodes that token, it receives the encoded data.

## Token ring history

Attached Resource Computer Network, Fiber Distributed Data Interface (FDDI) and the token bus used the token ring. But the most broadly deployed token ring protocols were those of IBM, released in the mid-1980s, and the standardized version of it known as IEEE 802.5, which appeared in the late 1980s.

The use of token rings and 802.5 started declining in the 1990s. Today, they are considered inactive and obsolete. Enterprise organizations gradually phased out the token ring and adopted Ethernet technology, which dominates LAN designs today. The IEEE 802.5 working group is now listed as disbanded.

Token rings were popular because they worked well with large amounts of traffic, but they were not well suited to large networks, particularly if those networks were spread widely or had physically remote nodes. To overcome some of these limitations, MultiTaction access units (MSAUs), which are like hubs on Ethernet, were added. MSAUs are centralized wiring hubs and are also known as concentrators.

## What is token ring star topology?

In a star topology, token ring access could connect up to 225 nodes at 4 million, 16 million or 100 million bits per second, conforming to the IEEE 802.5 standard. An MSAU connects all stations using a twisted pair cable. For example, users

could connect six nodes to an MSAU in one office and connect that MSAU to an MSAU in another office that served eight other nodes. In turn, that MSAU could connect to another MSAU that connected to the first MSAU.

Such a physical configuration is called a star topology. However, the actual configuration is a ring topology because every message passes through every computer, one at a time, until it forms a ring.

An advantage of an MSAU is that, if one computer fails in the ring, the MSAU can bypass it, and the ring will remain intact. Typically, each node connection cannot exceed 382 feet, depending on the cable type. However, you can increase this distance by up to a mile and a half using token ring repeaters.

### 4.3.3 FDDI

Fiber Distributed Data Interface is a set of standards for transmitting data over fiber-optic cable over a span of up to 124 miles. FDDI is usually used as a backbone in a Wide Area Network (WAN), like that connecting two different buildings in the same city. FDDI is similar to old-fashioned Token Ring, but it uses two token rings: a primary ring and a secondary ring, each able to carry 100Mbps. If the primary ring is working correctly, the backup ring can also be used, doubling the capacity to 200Mbps. However, a dual ring has a maximum distance of only 62 miles. For distances greater than that, only one ring can be used at a time.

### 4.3.4 Wireless

Although Wireless can refer to many technologies, in networks the most common technology used in home and offices is the 802.11 Wireless Local Area Network (WLAN), also called Wi-Fi. Access to a WLAN is controlled by a wireless access point, which is most commonly a wireless router. Any computer or wireless device -- like an iPhone, laptop or smart TV -- must request access from the access point and supply the appropriate password if requested before joining the wireless network. Currently, the fastest wireless is 802.11n

technology, which can transmit up to 300Mbps. Upcoming 802.11ac technology can transfer up to 433Mbps. Although range is affected by obstructions and even atmospheric conditions, range is generally up to 230 feet indoors and 800 feet outdoors.

**MCQ with Answers**

1. A LAN (Local Area Network) can cover a distance of ___ KM.
    a. 2
    b. 8
    c. 16
    d. 32
2. Multiple LANs can be connected to form a single MAN (Metropolitan Area Network). State TRUE/FALSE.
    a. TRUE
    b. FALSE
    c. None of these
3. The types of transmission channel or media used for LAN or WAN are __.
    a. Twisted Pair Cables
    b. Coaxial Cables
    c. Fiber-Optic Cables and Radio Waves
    d. All the above
4. A simple WIFI modem forms a __ wireless network.
    a. LAN
    b. MAN
    c. WAN
    d. None
5. Which type of network supports transmitting voice, video and data?
    a. LAN
    b. MAN
    c. WAN
    d. All the above
6. WAN or MAN may also contain __ in between to complete the network.
    a. Leased lines
    b. Satellite links
    c. SMDS (Switched Multi-megabit Data Services) offered by telecom companies on point-to-point basis.
    d. All the above
7. If a WAN is wholly owned by a single company including all intermediate links, it is called a __ network.

a. Duplex network
b. Whole network
c. Enterprise network
d. Residential network

8. The largest WAN existing on this earth is ___.
   a. Extranet
   b. Internet
   c. ARPANET
   d. SONET
9. The technologies used in a WAN network are __.
   a. SONET
   b. Frame Relay
   c. ATM
   d. All the above
10. The main hardware used to access a LAN resource is __.
    a. Motherboard
    b. NIU (Network Interface Unit) or NIC (Network Interface Card)
    c. RAM
    d. Hard disk
11. The three main services used in a LAN are __.
    a. File Server
    b. Print Server
    c. Modem Server (Sharing Internet)
    d. All the above
12. Choose a LAN operating system from the below list.
    a. Ethernet, LAN Server
    b. Novel Netware, Curves, ArcNet
    c. Omni Net, PC Net, IBM PC LAN, Etherlink Plus
    d. All the above
13. What is the other name for an Ethernet network?
    a. WAN
    b. Mesh Network
    c. DIX
    d. DIG

14. An Ethernet Jack is ___.
    a. RJ11
    b. RJ14
    c. RJ45
    d. None
15. Choose the topologies used in a LAN network below.
    a. BUS
    b. RING
    c. STAR, TREE
    d. All the above
16. In a ___ topology, all the nodes or stations are connected to a main central cable.
    a. BUS
    b. STAR
    c. TREE
    d. RING
17. In ___ topology, all the nodes are connected like a ring when drawn pictorially on a paper.
    a. BUS
    b. STAR
    c. RING
    d. TREE
18. In a ___ topology, the nodes or stations of a network are connected to a central hub or server.
    a. BUS
    b. STAR
    c. RING
    d. TREE
19. A group of STAR topology networks connected to a BUS like a cable form or create the ___ topology as a whole.
    a. BUS
    b. STAR
    c. RING
    d. TREE
20. Which is a network topology that is easy to build?

A) BUS, STAR
b. RING
c. TREE
d. All the above

| | | | | |
|---|---|---|---|---|
| 1.A | 2. A | 3. D | 4. A | 5. D |
| 6.D | 7. C | 8. B | 9. D | 10. B |
| 11.D | 12. D | 13.C | 14.C | 15.D |
| 16.A | 17.C | 18.B | 19.D | 20. A |

**Short Question**

1. what is Lan Architecture
2. what is Topology
3. write the advantages of Mesh topology
4. what is bus topology
5. describe briefly ring topology
6. what is hybrid topology
7. what is Ethernet
8. what is token ring
9. what is FDDI
10. FDDI stand for

**Long Question**

1. Write a note on Lan Architecture?
2. Write the note on Topologies
3. Write the note on Lan System

# 5 Connecting Device

## Objectives

**After completion of this chapter students will be able to:**

- ✓ Modems
- ✓ Hubs and Repeaters
- ✓ Bridges, Routers and Gateways

### What Are Connected Devices?

Connected devices are physical objects that can connect with each other and other systems via the internet. They span everything from traditional computing hardware, such as a laptop or desktop, to common mobile devices, such as a smartphone or tablet, to an increasingly wide range of physical devices and objects. This growing list of objects includes household appliances, heating and cooling systems, vehicles, health and fitness monitors, environmental sensors, and more. These devices, which are commonly embedded with technology such as processing chips, software, and sensors, collect data and share it with other devices and systems. Connected devices are typically monitored and controlled remotely. They connect with the internet and each other via various wired and wireless networks and protocols, such as WIFI, NFC, 3G and 4G networks.

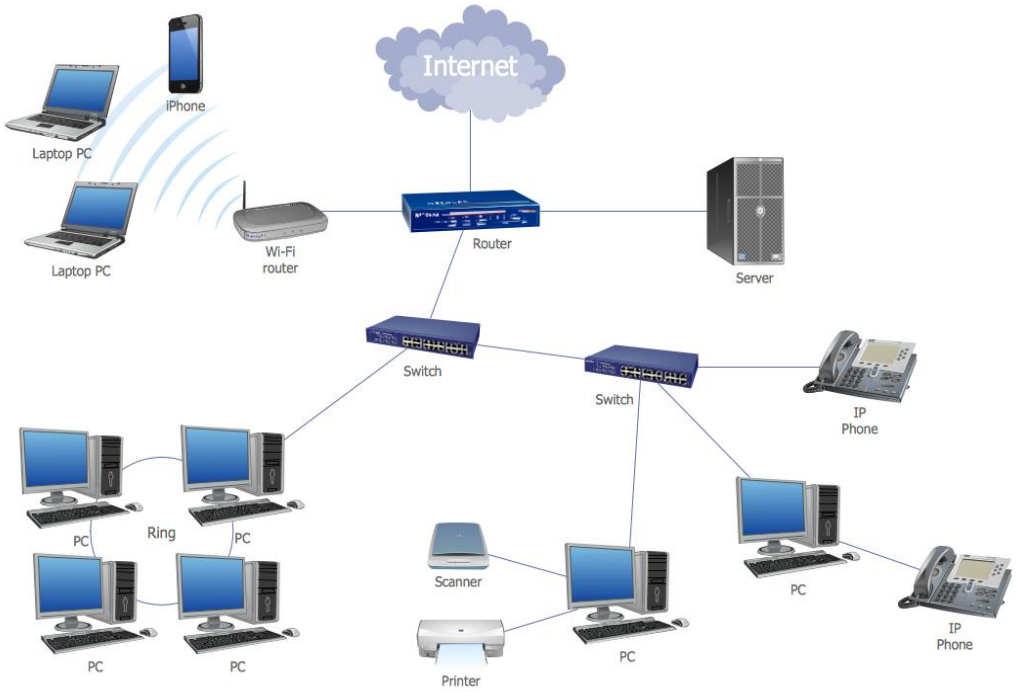



**Figure 5-1 connecting device**

## 5.1 Modem

A modem converts data to a signal so it can be easily sent and received over a phone line, cable, or satellite connection. For transmission over an analog telephone line—which was once the most popular way to access the internet—the modem converts data between analog and digital formats in real time for two-way network communication. In the case of the high-speed digital modems popular today, the signal is much simpler and doesn't require the analog-to-digital conversion.


**Figure 5-2: MODEM**

### 5.1.1 History of Modems

The first devices called modems converted digital data for transmission over analog telephone lines. The speed of these modems was measured in baud (a unit of measurement named after Emile Baudot), although as computer technology developed, these measures were converted into bits per second. The first commercial modems supported a speed of 110 bps and were used by the U.S. Department of Defense, news services, and some large businesses.

Modems gradually became familiar to consumers in the late 1970s through the 1980s as public message boards and news services like CompuServe were built on early internet infrastructure. Then, with the explosion of the World Wide Web in the mid and late 1990s, dial-up modems emerged as the primary form of internet access in many households around the world.

### 5.1.2 Dial-Up Modems

Modems used on dial-up networks convert data between the analog form used on telephone lines and the digital form used on computers. An external dial-up modem plugs into a computer at one end and a telephone line on the other end. In the past, some computer makers integrated internal dial-up modems into the computer.

Modern dial-up network modems transmit data at a maximum rate of 56,000 bits per second. However, the inherent limitations of public telephone networks often limit modem data rates to 33.6 Kbps or lower.

When you connect to a network through a dial-up modem, the modem relays through a speaker the distinctive handshaking sounds between your device and the remote modem. Because the connection process and data patterns are similar each time, hearing the sound pattern helps you verify whether the connection process is working.


### 5.1.3 Broadband Modems

A broadband modem like those used for DSL or cable internet access uses advanced signaling techniques to achieve dramatically higher network speeds

than earlier-generation dial-up modems. Broadband modems are often referred to as high-speed modems. Cellular modems are a type of digital modem that establishes internet connectivity between a mobile device and a cell phone network.

External broadband modems plug into a home broadband router or other home gateway device on one end and the external internet interface such as a cable line on the other. The router or gateway directs the signal to all the devices in the business or home as needed. Some broadband routers include an integrated modem as a single hardware unit.

Many broadband internet providers supply suitable modem hardware to their customers at no charge or for a monthly fee.

**5-3Broadband Modems**

## 5.2 Repeater

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to

extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.


## 5.3 Hub

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out best path for data packets which leads to inefficiencies and wastage.

### Types of Hubs

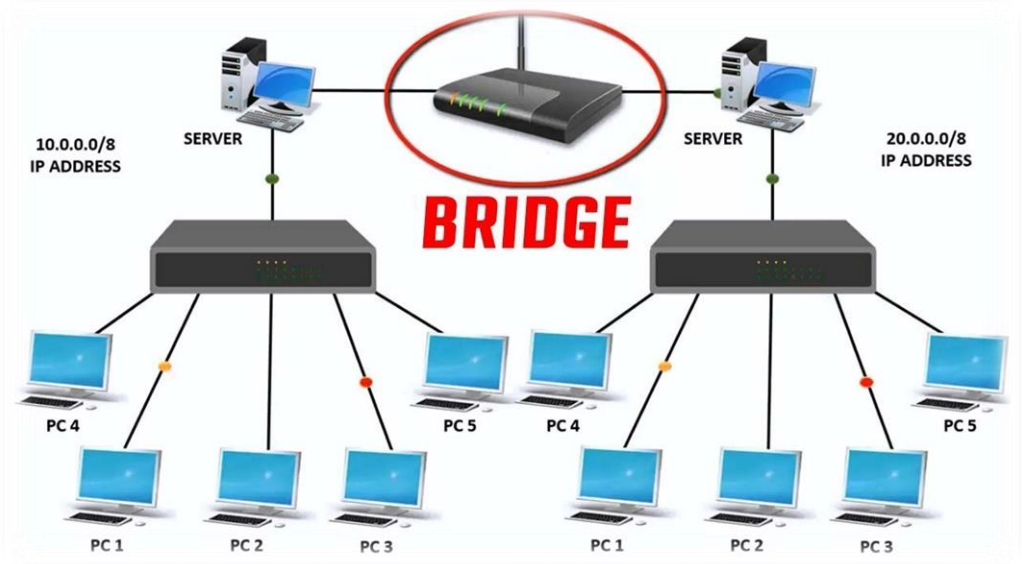
✓ **Active Hub: -** These are the hubs which have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as wiring center. These are used to extend the maximum distance between nodes.

✓ **Passive Hub**: - These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

✓ **Intelligent Hub**: - It work like active hubs and include remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

## 5.4 Bridge

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.




## Types of Bridges

### ✓ Transparent Bridges: -

These are the bridge in which the stations are completely unaware of the bridge's existence i.e., whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e., bridge forwarding and bridge learning.

### ✓ Source Routing Bridges: -

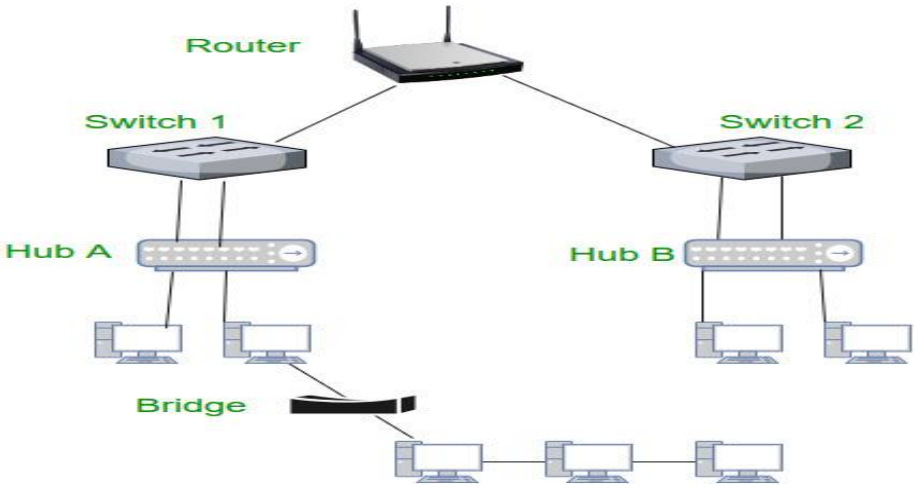
In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The host can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

## 5.5 Switch

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

## 5.6 Routers

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



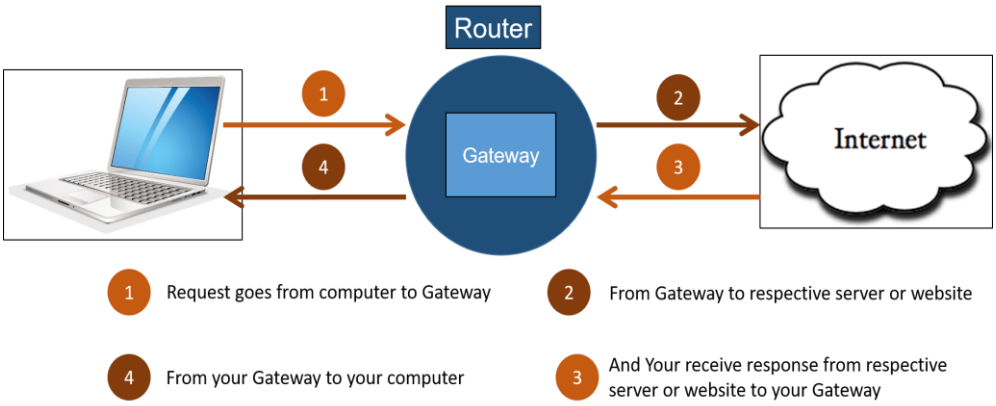

5-4 Router

## Features of Routers

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

## 5.7 Gateway

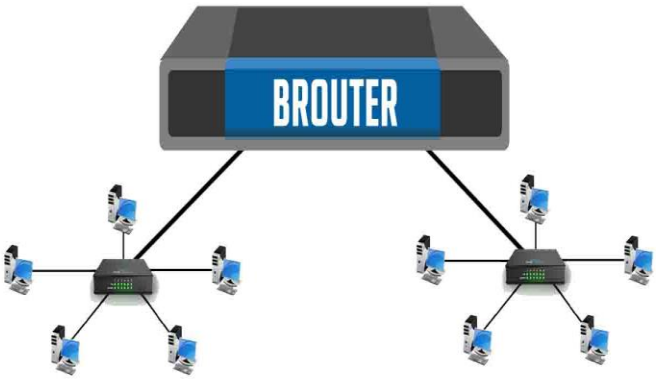
A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.




5-5 Gateway

## 5.8 Brouter

It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.


BROUTER

## MCQ with Answers

1. Modulator and demodulator as combinedly is known as –
   A: Modulus B: Modem C: Mod switch D: Mod access
2. Which of the following network device has the slowest type of connection?
   A: DSL B: Router C: Bridges D: Dial-up modems
3. Which of the following is an example of Personal Area Networking?
   A: Bluetooth B: WAN C: WLAN D: All of the above
4. A place where there is a field of signal through which you can access WiFi internet is called –
   A: WiFi Hotspots B: WiFi Internet C: WiFi Zone D: WiFi Range
5. Which network is able to connect and send data to each computer via central hub or switch without looking where the data is sent?
   A: Star B: Router C: Bus D: LAN
6. Which network is able to connect to each computer through a common central line?
   A: Bus B: Star C: router D: WAN
7. Which topology allow to connect computers including server in a ring?
   A: Star B: Tree C: Ring D: LAN
8. Which type of network is used for small geographical area such as in a one building?
   A: WLAN B: MAN C: LAN D: WAN
9. Which networking device connect one LAN to other LAN using same protocol?
   A: Router B: Switch C: Bridge D: Modem
10. IEEE 802.8 is/was –
    a) IBM Token Bus b) Integrated Services LAN
    c) Wireless LAN and Mesh d) Fiber Optic TAG

11. What is the function of Network Interface Cards?
    a) Connects the clients, servers and peripherals to the network through a port
    b) Allows you to segment a large network into smaller, efficient networks

c) Connects networks with different protocols like TCP/IP
d) Boost the signal between two cable segments or wireless access points

12. A device which is used to boost the signal between two cable segments or wireless access points is

    a) Booster b) Repeater
    c) Switch d) Router

13. A server is a ___ that controls a number of computers and also has full control over the network.
    a. Printer
    b. Switch
    c. Hub
    d. Computer with a special software
14. Choose a WAN device from the below list.
    a. Bridge
    b. Router
    c. Gateway
    d. All the above
15. A network hub works at __ layer of OSI reference model.
    a. layer 1
    b. layer 2
    c. layer 3
    d. layer 4
16. A network Switch works more or like a Hub except that it ___ packets to destination device and filters forwarding to remaining ports or devices.
    a. forwards
    b. filters
    c. duplicates
    d. None
17. A network switch usually uses __ to determine the destination device before forwarding a packet.
    a. Serial Number

b. ESN Number
c. MAC address
d. Base address

18. A network Gateway device converts one protocol to another protocol to connect two __ LAN networks or simply networks.
    a. Same
    b. Different
    c. Identical
    d. None
19. A network Bridge device connects two or more networks to form a ___ LAN network.
    a. Single
    b. Duplicate
    c. Multi
    d. None
20. A network bridge device works at __ layer of OSI reference model.
    a. Layer 1
    b. Layer 2
    c. Layer 3
    d. Layer 4
21. A network Router device connects two or more ___ networks.
    a. LAN
    b. WAN
    c. Both LAN and WAN networks
    d. None
22. A network Router works at a __ layer of an OSI reference model.
    a. Layer 1
    b. Layer 2
    c. Layer 3
    d. Layer 4
23. The work of the Router to do in a network.
    a. identified on which outing link a packet is to be sent
    b. send a packet to the next free outgoing link

c. send a packet to all outgoing links
d. send a packet to all outgoing links except the originated link

24. The Routing processor searches in the routing table is known as
    a. switch fabric
    b. table lookup
    c. buffer
    d. rolling table
25. Null modems are type of
    a. Modem
    b. Modem eliminator
    c. Protocol converter
    d. Multiplexer
26. A device that connects networks with different protocols –
    a. Switch
    b. Hub
    c. Gateway
    d. All of these
27. A device that is used to connect a number of LANs is –
    a. Router
    b. Repeater
    c. Bridge
    d. All of these

28. Which of the following network device has the slowest type of connection?
    a. DSL
    b. Router
    c. Dial-up modems
    d. None Of the Above

| | | | | | |
|---|---|---|---|---|---|
| 1. B | 2. D | 3. A | 4. A | 5. A | 6. A |
| 7. C | 8. C | 9. B | 10. D | 11. A | 12. C |
| 13. d | 14. d | 15. a | 16. a | 17. c | 18. b |
| 19. a | 20. b | 21 c | 22. c | 23. a | 24. b |
| 25. b | 26. c | 27. a | 28. c | | |

**Short Question**

1. What are connectivity devices?
2. What is modem?
3. Types of modems
4. What is hub?
5. What is gateway?
6. Types of hubs?
7. What is repeater?
8. What is bridge?
9. Type of Bridge?
10. What is protocol?
11. What is token ring?

**LONG**

1. Write a note on connecting device
2. Write detail note on modem also describe its types
3. Write detail note on bridge also describe its types
4. Write detail note on Hub also describe its types

# 6 Internetworking

## Objectives

**After completion of this chapter students will be able to understand:**

- Principles of Internetworking
- Protocols
- OSI Model
- TCP/IP Suite
- Internet Protocol (IP) and
- Addressing scheme at NW layer (IP address classes)
- Routing Protocol
- Transport Protocols and Transport Services
- Addressing scheme at Transport layer (Port addresses)
- Application Layer protocols
- Addressing scheme at Application layer (DNS)

## 6.1 Principals of Internetworking

Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.

Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the Internet Routing Protocol. The Internet is the largest pool of networks geographically located throughout the world but these networks are interconnected using the same protocol stack, TCP/IP. Internetworking is only possible when the all the connected networks use the same protocol stack or communication methodologies.

### 6.1.1 Type of Internetworking

- ✓ Extranet
- ✓ Intranet
- ✓ Internet

### 6.1.1 Extranet

An extranet is a private network that only authorized users can access. These authorized users may include business partners, suppliers, and even some customers. They can use the extranet to exchange information with each other without having to enter the host company's main network.

### 6.1.2 Intranet

Intranet is defined as private network of computers within an organization with its own server and firewall. Moreover, we can define Intranet as:

- ✓ Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.
- ✓ Usually, each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- ✓ Every computer in internet is identified by a unique IP address.
- ✓ Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.

### 6.1.3 Internet

Internet is defined as an Information super Highway, to access information over the web. However, it can be defined in many ways as follows:

- ✓ Internet is a world-wide global system of interconnected computer networks.
- ✓ Internet uses the standard Internet Protocol (TCP/IP).
- ✓ Every computer in internet is identified by a unique IP address.
- ✓ IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.

- ✓ A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.

For example, a DNS server will resolve a name **http://www.tevta.gop.pk** to a particular IP address to uniquely identify the computer on which this website is hosted. Internet is accessible to every user all over the world.

## 6.2 Protocol

A network protocol is a set of established rules that dictate how to format, transmit and receive data so that computer network devices -- from servers and routers to endpoints -- can communicate, regardless of the differences in their underlying infrastructures, designs or standards.

To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. In networking, support for protocols can be built into software, hardware or both.

Without computing protocols, computers and other devices would not know how to engage with each other. As a result, except for specialty networks built around a specific architecture, few networks would be able to function, and the internet as we know it wouldn't exist. Virtually all network end users rely on network protocols for connectivity.

### 6.2.1 OSI Model

- ✓ OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- ✓ OSI consists of seven layers, and each layer performs a particular network function.

✓ OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.

✓ OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

✓ Each layer is self-contained, so that task assigned to each layer can be performed independently.

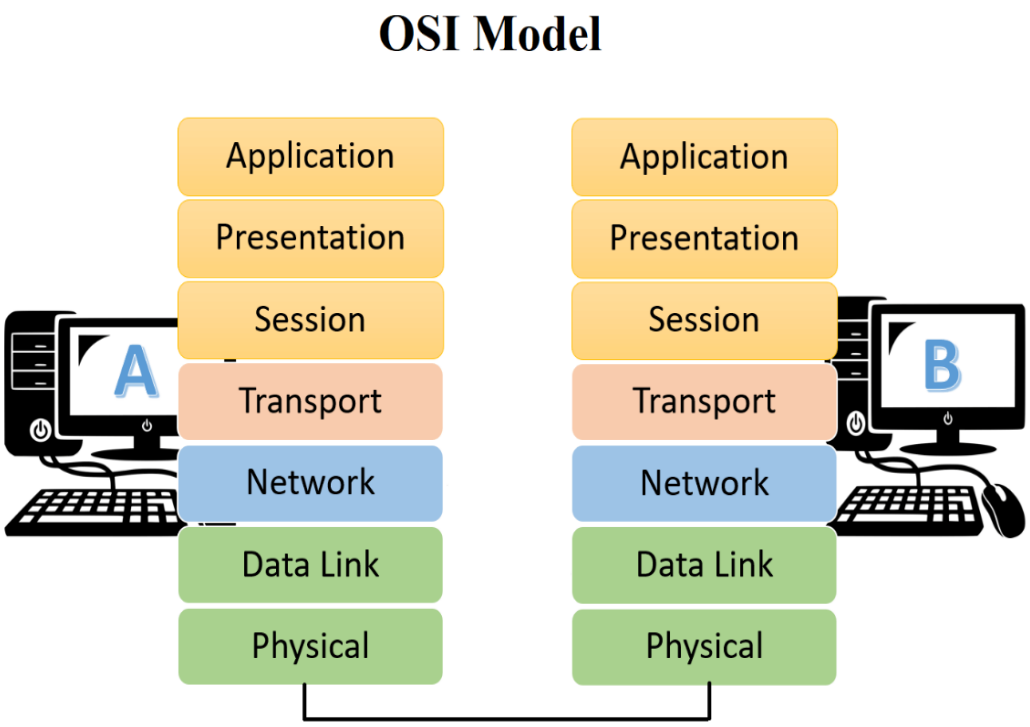



**Figure 6-1 OSI MODEL**

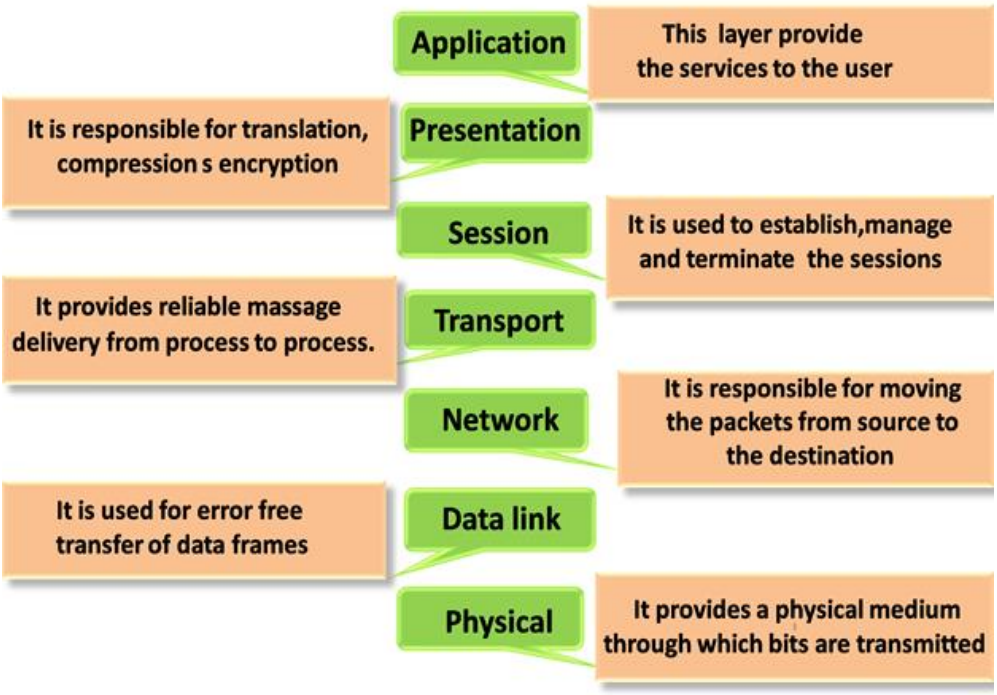
## Characteristics of OSI Model

- ✓ 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.

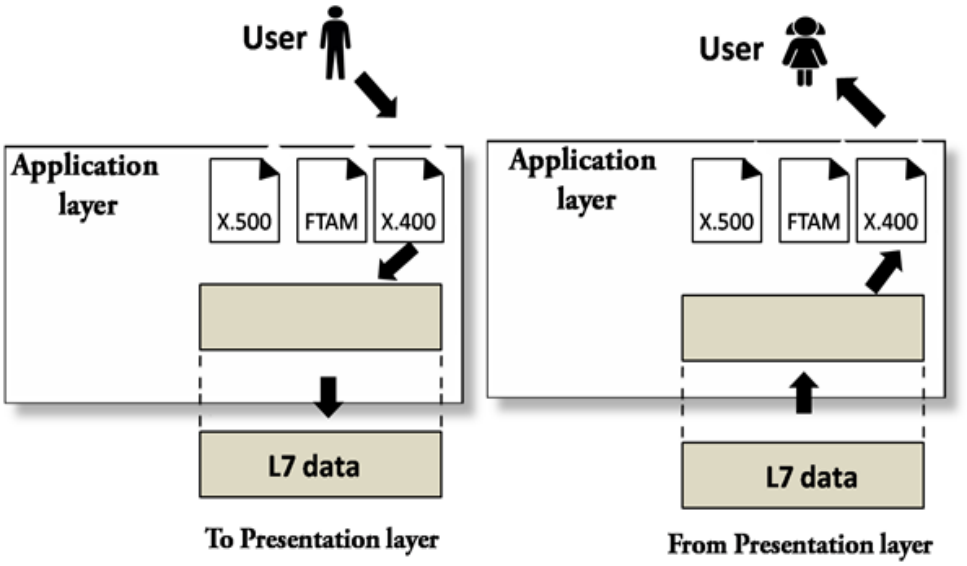
## Functions of the OSI Layers

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

- ✓ Application Layer
- ✓ Presentation Layer
- ✓ Session Layer
- ✓ Transport Layer
- ✓ Network Layer
- ✓ Data-Link Layer
- ✓ Physical Layer




### 6.2.1.1 Application Layer

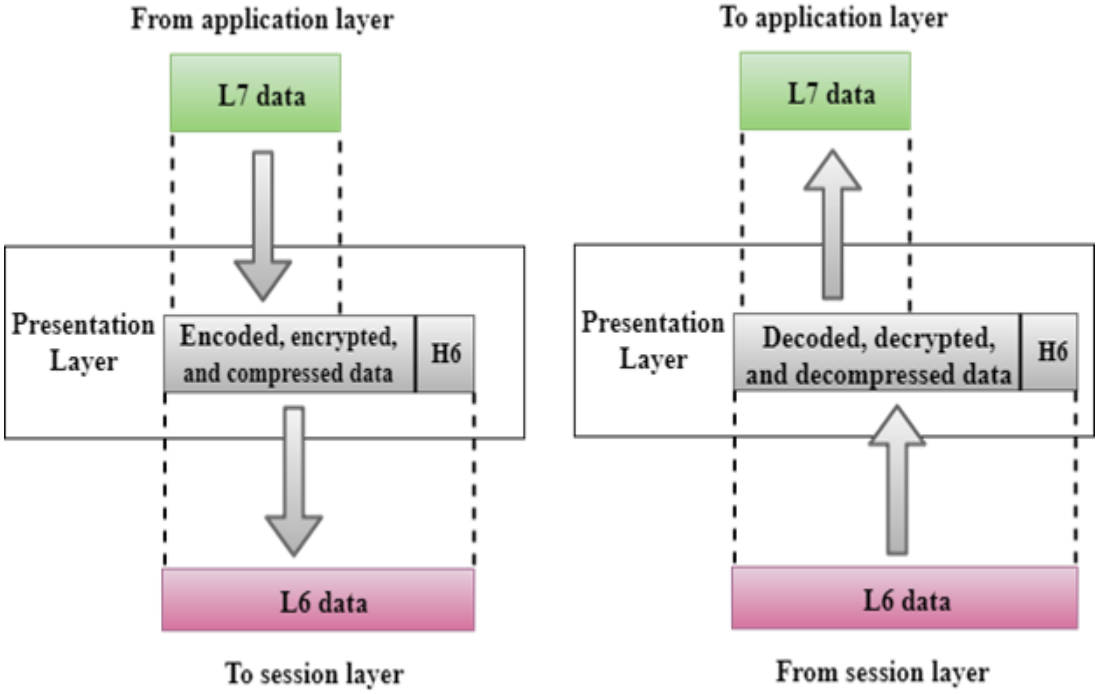


- ✓ An application layer serves as a window for users and application processes to access network service.
- ✓ It handles issues such as network transparency, resource allocation, etc.
- ✓ An application layer is not an application, but it performs the application layer functions.
- ✓ This layer provides the network services to the end-users.

## Functions of Application layer

- ✓ **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- ✓ **Mail services:** An application layer provides the facility for email forwarding and storage.
- ✓ **Directory services**: An application provides the distributed database sources and is used to provide that global information about various objects.

### 6.2.1.2 Presentation Layer




✓ A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.

✓ It acts as a data translator for a network.

✓ This layer is a part of the operating system that converts the data from one presentation format to another format.

✓ The Presentation layer is also known as the syntax layer.

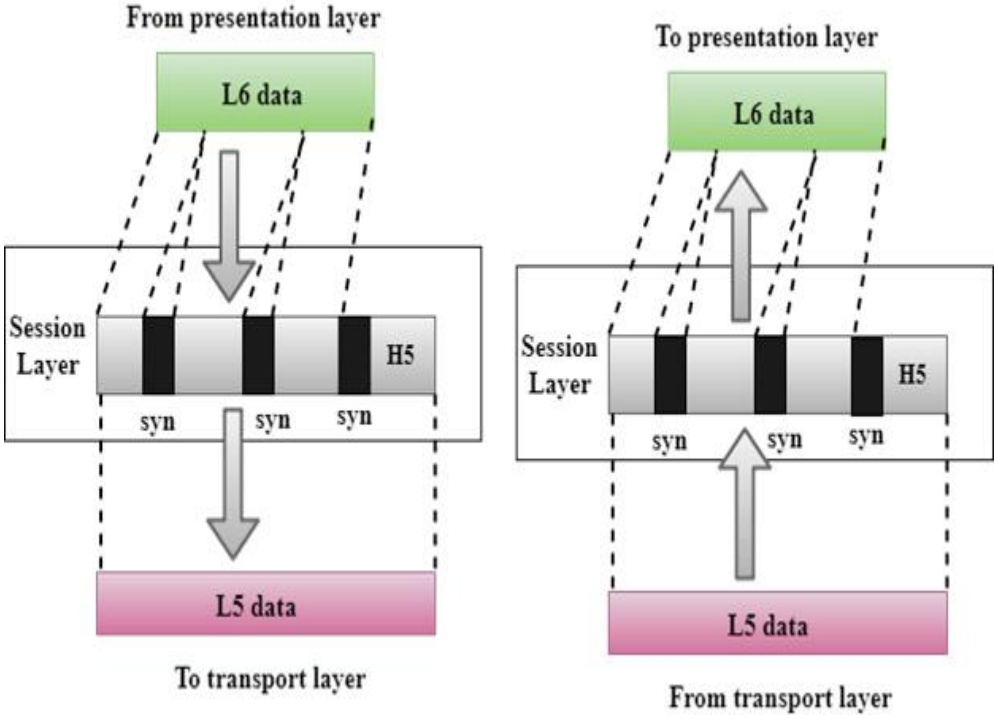
**Functions of Presentation layer:**

✓ **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

✓ **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

✓ **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

### 6.2.1.3 Session Layer




✓ It is a layer 5 in the OSI model.

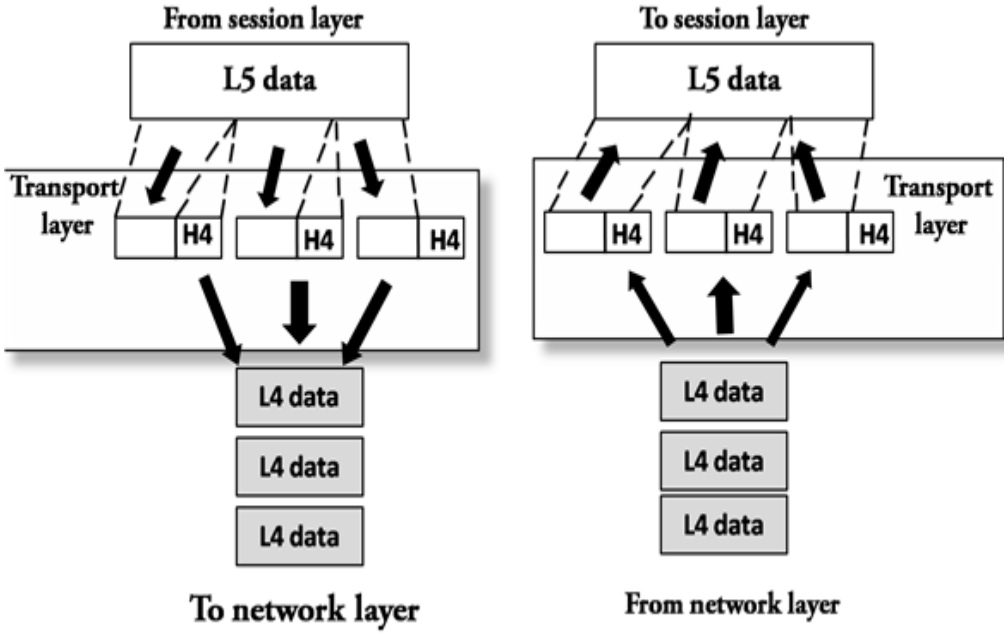
✓ The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

## Functions of Session layer:

✓ **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

✓ **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

### 6.2.1.4 Transport Layer




✓ The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.

✓ The main responsibility of the transport layer is to transfer the data completely.

✓ It receives the data from the upper layer and converts them into smaller units known as segments.

✓ This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

## The two protocols used in this layer are:

### Transmission Control Protocol

✓ It is a standard protocol that allows the systems to communicate over the internet.

✓ It establishes and maintains a connection between hosts.

✓ When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

### User Datagram Protocol

✓ User Datagram Protocol is a transport layer protocol.

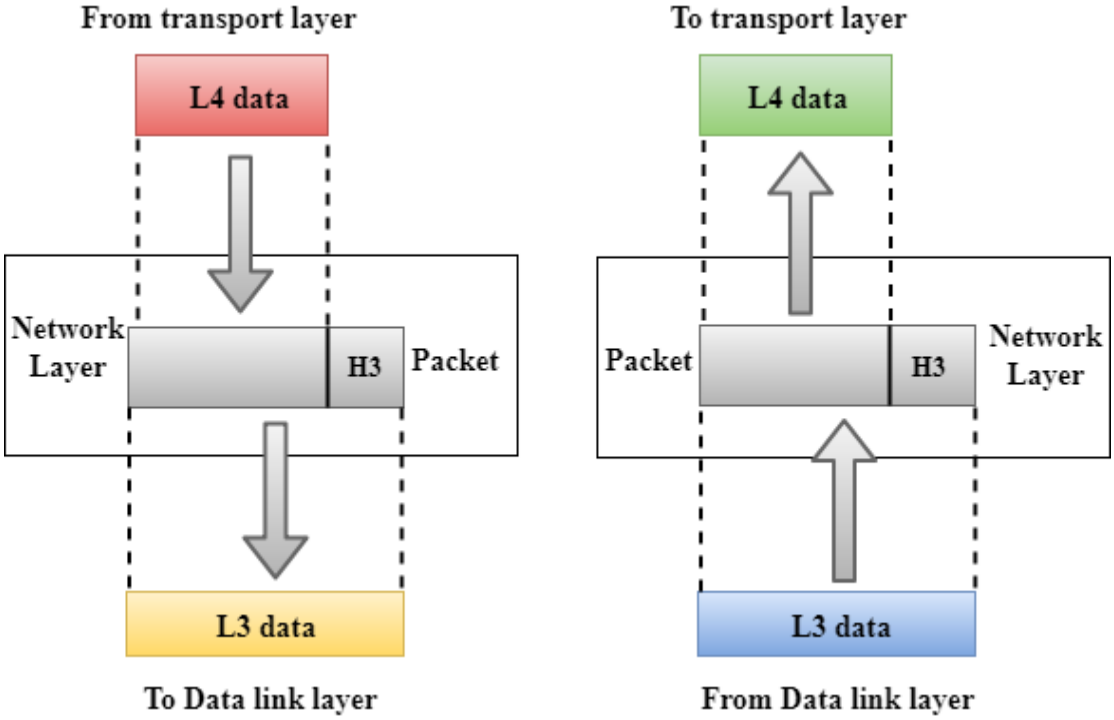
✓ It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

## Functions of Transport Layer:

✓ **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

- ✓ **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- ✓ **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- ✓ **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- ✓ **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

### 6.2.1.5 Network Layer




✓ It is a layer 3 that manages device addressing, tracks the location of devices on the network.

✓ It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.

✓ The Data link layer is responsible for routing and forwarding the packets.

✓ Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.

✓ The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

**Functions of Network Layer:**

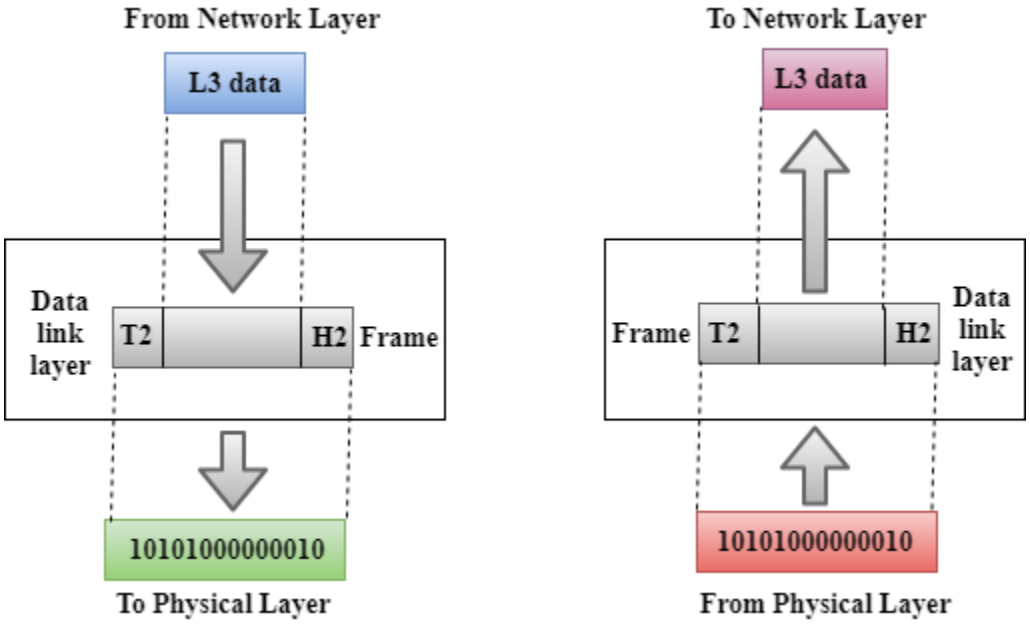
✓ **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.

✓ **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

✓ **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

✓ **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

### 6.2.1.6 Data-Link Layer




✓ This layer is responsible for the error-free transfer of data frames.

✓ It defines the format of the data on the network.

✓ It provides a reliable and efficient communication between two or more devices.

✓ It is mainly responsible for the unique identification of each device that resides on a local network.

✓ It contains two sub-layers:

- **Logical Link Control Layer**
  - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
  - It identifies the address of the network layer protocol from the header.
  - It also provides flow control.
- **Media Access Control Layer**
  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - It is used for transferring the packets over the network.

**Functions of the Data-link layer**

✓ **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

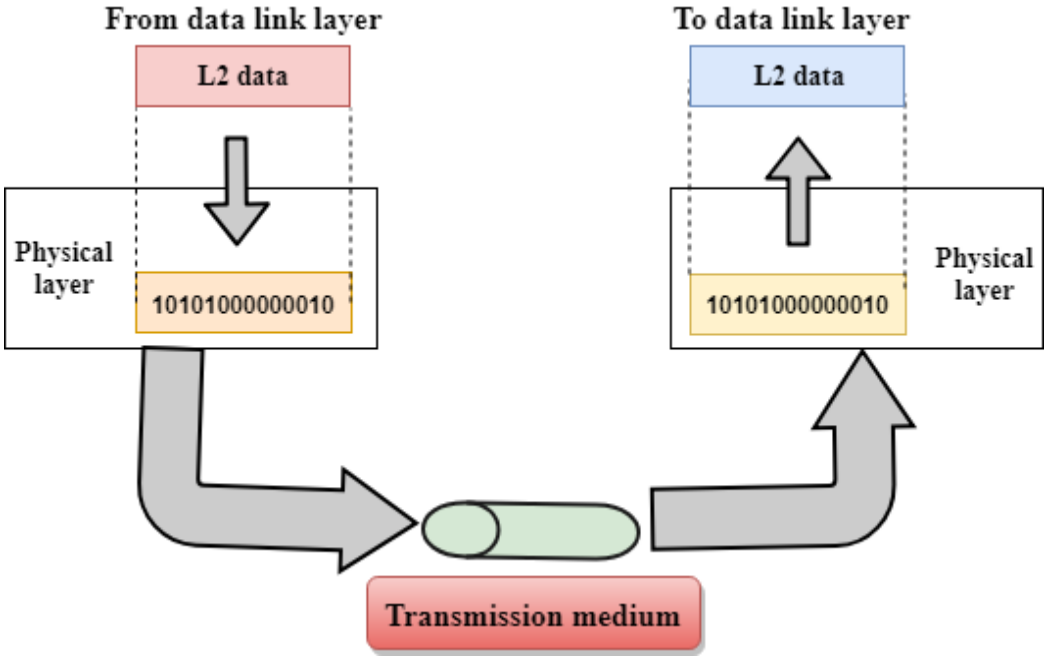

✓ **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.

✓ **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

✓ **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

✓ **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

### 5.1.1.7 Physical layer




✓ The main functionality of the physical layer is to transmit the individual bits from one node to another node.

✓ It is the lowest layer of the OSI model.

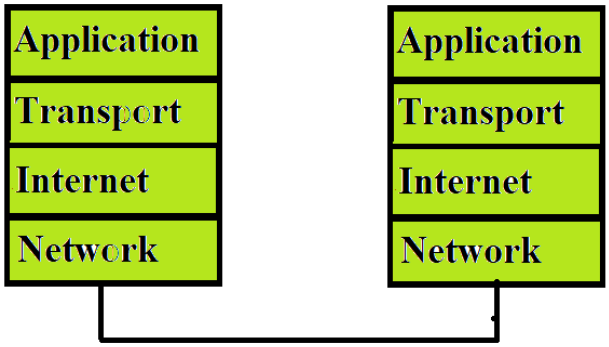
✓ It establishes, maintains and deactivates the physical connection.

✓ It specifies the mechanical, electrical and procedural network interface specifications.

## Functions of a Physical layer:

- ✓ **Line Configuration:** It defines the way how two or more devices can be connected physically.
- ✓ **Data_Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- ✓ **Topology:** It defines the way how network devices are arranged.
- ✓ **Signals:** It determines the type of the signal used for transmitting the information.

## 6.3 TCP /IP MODEL




### 6.3.1 Application Layer

✓ An application layer is the top most layer in the TCP/IP model.

✓ It is responsible for handling high-level protocols, issues of representation.

✓ This layer allows the user to interact with the application.

✓ When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

✓ There is an ambiguity that occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example, text editor cannot be considered in the application layer while web browsers using the **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

**Following are the main protocols used in the application layer:**

✓ **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the

efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

✓ **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

✓ **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

✓ **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

✓ **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and the remote computer in such a way that the local terminal appears to be a terminal at the remote system.

✓ **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting files from one computer to another computer.

### 6.3.2 Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data that is being sent over the network.

The two protocols used in the transport layer are the **User Datagram Protocol and Transmission control protocol**.

### User Datagram Protocol (UDP)

✓ It provides connectionless service and end-to-end delivery of transmission.

✓ It is an unreliable protocol as it discovers the errors but does not specify the error.

✓ User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that the user datagram has been damaged.

**UDP consists of the following fields:**

- ✓ Source port address: The source port address is the address of the application program that has created the message.
- ✓ Destination port address: The destination port address is the address of the application program that receives the message.
- ✓ Total length: It defines the total number of bytes of the user datagram in bytes Checksum: The checksum is a 16-bit field used in error detection.
- ✓ UDP does not specify which packet is lost. UDP contains the only checksum; it does not contain any ID of a data segment.

## Transmission Control Protocol (TCP)

✓ It provides full transport layer services to applications.

✓ It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.

✓ TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.

✓ At the sending end, TCP divides the whole message into smaller units known as the segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.

✓ At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

### 6.3.3 Internet Layer

- ✓ An internet layer is the second layer of the TCP/IP model.
- ✓ An internet layer is also known as the network layer.
- ✓ The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

## Following are the protocols used in this layer are:

**IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- ✓ **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- ✓ **host-to-host communication:** It determines the path through which the data is to be transmitted.
- ✓ **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into a message known as an IP datagram.
- ✓ **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as the Maximum Transmission Unit (MTU). If the size of the IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. On the receiver side, all the fragments are reassembled to form an original message.

- ✓ **Routing:** When an IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

## ARP Protocol

- ✓ ARP stands for Address Resolution **Protocol**.
- ✓ ARP is a network layer protocol that is used to find the physical address from the IP address.

**The two terms are mainly associated with the ARP Protocol:**

- ✓ **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
- ✓ **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but the only recipient recognizes the IP address and sends back its physical address in the form of an ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

**ICMP Protocol**

- ✓ **ICMP** stands for Internet Control Message Protocol.
- ✓ It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- ✓ A datagram travels from router to router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire, or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

- ✓ An ICMP protocol mainly uses two terms:
- ✓ **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
- ✓ **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- ✓ The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ✓ ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

### 6.3.4 Network Layer

- ✓ A network layer is the lowest layer of the TCP/IP model.
- ✓ A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- ✓ It defines how the data should be sent physically through the network.
- ✓ This layer is mainly responsible for the transmission of the data between two devices on the same network.
- ✓ The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping IP addresses into physical addresses.
- ✓ The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

## 6.4 Internet Protocol (IP)

Internet Protocol (IP) is a set of rules that dictate how data should be delivered over the public network (Internet). Often works in conjunction with

the transmission control protocol (TCP), which divides traffic into packets for efficient transport through the Internet; together they are referred to as TCP/IP.

For example, when an email (using the simple mail transfer protocol – SMTP) is sent from an email server, the TCP layer in that server will divide the message up into multiple packets, number them and then forward them to the IP layer for transport. At the IP layer, each packet will be transported to the destination email server. While each packet is going to the same place, the route they take to get there may be different. When it arrives, the IP layer hands it back to the TCP layer, which reassembles the packets into the message and hands it to the email application, where it shows up in the Inbox.

### 6.4.1 Ip Address Classes

An IP (Internet Protocol) address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication.

IP addresses act as an identifier for a specific machine on a particular network. It also helps you to develop a virtual connection between a destination and a source. The IP address is also called an IP number or internet address. It helps you to specify the technical format of the addressing and packets scheme.

An IP address consists of four numbers, each number contains one to three digits, with a single dot (.) separates each number or set of digits.

- ✓ **Prefix:** The prefix part of the IP address identifies the physical network to which the computer is attached. . Prefix is also known as a network address.
- ✓ **Suffix**: The suffix part identifies the individual computer on the network. The suffix is also called the host address.

IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit

organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

### 6.4.2 How do IP addresses work?

1. Your device indirectly connects to the internet by connecting at first to a network connected to the internet, which then grants your device access to the internet.

2. When you are at home, that network will probably be your Internet Service Provider (ISP). At work, it will be your company network.

3. Your IP address is assigned to your device by your ISP.

4. Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.

There are a few reserved IPv4 address spaces that cannot be used on the internet. These addresses serve a special purpose and cannot be routed outside the Local Area Network.

### 6.4.3 Private IP Addresses

Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.

| Class A IP Range | Subnet Mask |
|---|---|
| 10.0.0.0 – 10.255.255.255 | 255.0.0.0 |
| 172.16.0.0 – 172.31.255.255 | 255.240.0.0 |
| 192.168.0.0 – 192.168.255.255 | 255.255.0.0 |

To communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.

### 6.4.4 Loopback IP Addresses

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address. This loopback IP address is managed entirely by and within the operating system. Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine.

### *6.4.5* Public IP addresses

A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

| **Class** | **Address range** | **Supports** |
|---|---|---|
| **Class A** | 1.0.0.1 to 126.255.255.254 | Supports 16 million hosts on each of 127 networks. |

| | | |
|---|---|---|
| **Class B** | 128.1.0.1 to 191.255.255.254 | Supports 65,000 hosts on each of 16,000 networks. |
| **Class C** | 192.0.1.1 to 223.255.254.254 | Supports 254 hosts on each of 2 million networks. |
| **Class D** | 224.0.0.0 to 239.255.255.255 | Reserved for multicast groups. |
| **Class E** | 240.0.0.0 to 254.255.255.254 | Reserved for future use, or research and development purposes. |

With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Each class allows for a range of valid IP addresses, shown in the following table.

Ranges 127.x.x.x are reserved for the loopback or localhost, for example, 127.0.0.1 is the loopback address.

✓ A class A network number uses the first eight bits of the IP address as its "network part." The remaining 24 bits comprise the host part of the IP address. The values assigned to the first byte of class A network numbers fall within the range 0-127. Consider the IP address 75.4.10.4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4.10.4, establish the host address. The Inter NIC assigns only the first byte of a class A number. Use of the remaining three bytes is left to the discretion of the owner of the network number.

✓ A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a class B network number is in the range 128-191. In the number 129.144.50.56, the first two bytes, 129.144, are assigned by the Inter NIC and comprise the network address. The last two bytes, 50.56, make up the host address and are assigned at the discretion of the owner of the network number.

✓ Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts--the maximum being 254. A class C network number occupies the first three bytes of an IP address. Only the fourth byte is assigned at the discretion of the network owners.

### 6.4.6 Internet Protocol v6 (IPv6)

IETF (Internet Engineering Task Force) has redesigned IP addresses to mitigate the drawbacks of IPv4. The new IP address is version 6 which is 128-bit address, by which every single inch of the earth can be given millions of IP addresses.

## 6.5 Routing Protocols

**Routing Protocols** are the set of defined rules used by the routers to communicate between source & destination. They do not move the information to the source to a destination, but only update the routing table that contains the information.

Network Router protocols helps you to specify way routers communicate with each other. It allows the network to select routes between any two nodes on a computer network.

There are mainly two types of Network Routing Protocols

- Static
- Dynamic

### 6.5.1 Static Routing Protocols

Static routing protocols are used when an administrator manually assigns the path from source to the destination network. It offers more security to the network.

## Advantages

- ✓ No overhead on router CPU.
- ✓ No unused bandwidth between links.
- ✓ Only the administrator is able to add routes

## Disadvantages

- ✓ The administrator must know how each router is connected.
- ✓ Not an ideal option for large networks as it is time intensive.
- ✓ Whenever link fails all the network goes down which is not feasible in small networks.

### 6.5.2 Dynamic Routing Protocols

Dynamic routing protocols are another important type of routing protocol. It helps routers to add information to their routing tables from connected routers automatically. These types of protocols also send out topology updates whenever the network changes' topological structure.

## Advantage:

- ✓ Easier to configure even on larger networks.
- ✓ It will be dynamically able to choose a different route in case if a link goes down.
- ✓ It helps you to do load balancing between multiple links.

## Disadvantage:

- ✓ Updates are shared between routers, so it consumes bandwidth.
- ✓ Routing protocols put an additional load on router CPU or RAM.

### 6.5.3 Types of routing protocols

- ✓ Distance Vector Routing Protocol
- ✓ Link State Routing Protocol
- ✓ Path Vector Routing Protocol
- ✓ Hybrid Routing Protocol

#### 6.5.3.1 Distance Vector Routing Protocol (DVR)

Distance Vector Protocols advertise their routing table to every directly connected neighbor at specific time intervals using lots of bandwidths and slow converge.

In the Distance Vector routing protocol, when a route becomes unavailable, all routing tables need to be updated with new information.

#### 6.5.3.2 Routing Information Protocol (RIP)

Routing Information Protocol or RIP is one of the first routing protocols to be created. RIP is used in both Local Area Networks (LANs) and Wide Area Networks (WANs), and also runs on the Application layer of the OSI model. There are multiple versions of RIP including RIPv1 and RIPv2. The original version or RIPv1 determines network paths based on the IP destination and the hop count of the journey.

RIPv1 interacts with the network by broadcasting its IP table to all routers connected to the network. RIPv2 is a little more sophisticated than this and sends its routing table on to a multicast address. RIPv2 also uses authentication to keep data more secure and chooses a subnet mask and gateway for future

traffic. The main limitation of RIP is that it has a maximum hop count of 15 which makes it unsuitable for larger networks.

### 6.5.3.3 Interior Gateway Protocol (IGP)

IGRP is a subtype of the distance-vector interior gateway protocol developed by CISCO. It is introduced to overcome RIP limitations. The metrics used are load, bandwidth, delay, MTU, and reliability. It is widely used by routers to exchange routing data within an autonomous system.

This type of routing protocol is the best for larger network size as it broadcasts after every 90 seconds, and it has a maximum hop count of 255**.** It helps you to sustain larger networks compared to RIP. IGRP is also widely used as it is resistant to routing loop because it updates itself automatically when route changes occur within the specific network. It is also given an option to load balance traffic across equal or unequal metric cost paths.

### 6.5.3.4 Exterior Gateway Protocol (EGP)

EGP is a protocol used to exchange data between gateway hosts that are neighbors with each other within autonomous systems. This routing protocol offers a forum for routers to share information across different domains. The full form for EGP is the Exterior Gateway Protocol. EGP protocol includes known routers, network addresses, route costs, or neighboring devices.

### 6.5.3.5 Link State Routing Protocol

Link State Protocols take a unique approach to search the best routing path. In this protocol, the route is calculated based on the speed of the path to the destination and the cost of resources.

## 1-Open Shortest Path First (OSPF)

*Open Shortest Path First* (OSPF) is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. OSPF is an Interior Gateway Protocol (IGP).

OSPF routing allows you to maintain databases detailing information about the surrounding topology of the network. It also uses the Dijkstra algorithm (Shortest path algorithm) to recalculate network paths when its topology changes. This protocol is also very secure, as it can authenticate protocol changes to keep data secure.

Here are some main differences between these Distance Vector and Link State routing protocols:

## 2-Intermediate System-to-Intermediate System (IS-IS)

ISIS CISCO routing protocol is used on the Internet to send IP routing information. It consists of a range of components, including end systems, intermediate systems, areas, and domains.

The full form of ISIS is Intermediate System-to-Intermediate System. Under the IS-IS protocol, routers are organized into groups called areas. Multiple areas are grouped to make form a domain.

### 6.5.3.6 Path Vector routing protocols

A path-vector routing protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates that have looped through the network and returned to the same node are easily detected and discarded

### 6.5.3.7 Border Gateway Protocol (BGP)

BGP is the last routing protocol of the Internet, which is classified as a DPVP (distance path vector protocol). The full form of BGP is the Border Gateway Protocol.

This type of routing protocol sends updated router table data when changes are made. Therefore, there is no auto-discovery of topology changes, which means that the user needs to configure BGP manually.

### 6.5.3.8 Hybrid routing protocols

Hybrid Routing Protocol (HRP) is a network routing protocol that combines Distance Vector Routing Protocol (DVRP) and Link State Routing Protocol (LSRP) features. HRP is used to determine optimal network destination routes and report network topology data modifications.

### 6.5.3.9 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a hybrid routing protocol that provides routing protocols, distance vector, and link-state routing protocols. The full form routing protocol EIGRP is Enhanced Interior Gateway Routing Protocol. It will route the same protocols that IGRP routes using the same composite metrics as IGRP, which helps the network select the best path destination.

**Comparison of Distance vector and Link state routing protocols.**

| Distance Vector | Link State |
|---|---|
| Distance Vector protocol sends the entire routing table. | Link State protocol sends only link-state information. |
| It is susceptible to routing loops. | It is less susceptible to routing loops. |

| Distance Vector | Link State |
|---|---|
| Updates are sometimes sent using broadcast. | Uses only multicast method for routing updates. |
| It is simple to configure. | It is hard to configure this routing protocol. |
| Does not know network topology. | Know the entire topology. |
| Example RIP, IGRP. | Examples: OSPF IS-IS. |

## Purpose of Routing Protocols

Routing protocols are required for the following reasons:

- ✓ Allows optimal path selection
- ✓ Offers loop-free routing
- ✓ Fast convergence
- ✓ Minimize update traffic
- ✓ Easy to configure
- ✓ Adapts to changes
- ✓ Scales to a large size
- ✓ Compatible with existing hosts and routers
- ✓ Supports variable length

## 6.5.3.10 Transport Protocols

There are two general types of transport protocols:

✓ A **connectionless protocol** treats each datagram as independent from all others. Each datagram must contain all the information required for its delivery.

An example of such a protocol is **User Datagram Protocol (UDP)**. UDP is a datagram-level protocol built directly on the IP layer and used for application-to-application programs on a TCP/IP host. UDP does not guarantee data delivery, and is therefore considered unreliable. Application programs that require reliable delivery of streams of data should use TCP.

✓ A connection-oriented protocol requires that hosts establish a logical connection with each other before communication can take place. This connection is sometimes called a virtual circuit, although the actual data flow uses a packet-switching network. A connection-oriented exchange includes three phases:

1. Start the connection.
2. Transfer data.
3. End the connection.

An example of such a protocol is **Transmission Control Protocol (TCP)**. TCP provides a reliable vehicle for delivering packets between hosts on an internet. TCP breaks a stream of data into datagrams, sends each one individually using IP, and reassembles the datagrams at the destination node. If any datagrams are lost or damaged during transmission, TCP detects this and re-sends the missing or damaged datagrams. The data stream that is received is therefore a reliable copy of the original.

**Addressing scheme at Transport layer (Port addresses)**

A network layer header contains both IP addresses of a source node and a destination node. A Transport layer (layer 4) address has 2-byte (16-bit) field called port number that is represented by a 16-bit number, such as 4,892. The port numbers identify the two end hosts' ports in a communication. Any host can be running several network applications at a time and thus each application needs to be identified by another host communicating to a targeted application.

### 6.5.4 Addressing scheme at Transport layer (Port addresses)

A network layer header contains both IP addresses of a source node and a destination node. A Transport layer (layer 4) address has 2-byte (16-bit) field called port number that is represented by a 16-bit number, such as 4,892. The port numbers identify the two end hosts' ports in a communication. Any host can be running several network applications at a time and thus each application needs to be identified by another host communicating to a targeted application.

## 6.6 Application Layer protocol:-

### 6.6.1 TELNET:

Telnet stands for the **Tel**ecommunications **Net**work. It helps in terminal emulation. It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

### *5.1.2* FTP:

FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program. FTP promotes sharing of files via remote computers with reliable and efficient data transfer. Port number for FTP is 20 for data and 21 for control.

### 5.1.3 SMTP:

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called “store and forward,” SMTP moves your email on and across networks. It works closely with something called the Mail Transfer

Agent (MTA) to send your communication to the right computer and email inbox. Port number for SMTP is 25.

### 5.1.4 DHCP:

It stands for Dynamic Host Configuration Protocol (DHCP).It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

## 6.7 Addressing scheme at Application layer (DNS)

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

**MCQ WITH ANSWERS**

1. Who developed standards for the OSI reference model?
    a. ANSI - American National Standards Institute
    b. ISO - International Standards Organization
    c. IEEE - Institute of Electrical and Electronics Engineers
    d. ACM - Association for Computing Machinery
2. How many layers are there in the OSI reference model of networking?
    a. 5
    b. 6
    c. 7
    d. 4
3. Each layer of the OSI model receives services or data from a ___ layer
    a. below layer
    b. above layer
    c. 1st layer
    d. 5th layer
4. OSI stands for _____
    a. open system interconnection
    b. operating system interface
    c. optical service implementation
    d. open service Internet

5. What layer in the TCP/IP stack is equivalent to the Transport layer of the OSI model?
    a. Application
    b. Host-to-Host
    c. Internet
    d. Network Access
6. What is the format of IP address?
    a. 34 bit
    b. 64 bit

c. 16 bit
d. 32 bit

7. Version 6 of IP address has how many bits.
   a. 64 bits
   b. 128 bits
   c. 32 bits
   d. 256 bits
8. VLSM stands for _____
   a. Version Length Subnet Masking
   b. Variable Length Subnet Masking
   c. Variable Length Surface Masking
   d. Version Length Surface Masking
9. _____ adjusts the segment size to be smaller than MTU.
   a. Internet Protocol 6
   b. User Datagram Protocol
   c. Internet Protocol 4
   d. Transmission Control Protocol
10. Which NetWare protocol works on layer 3–network layer—of the OSI model?
   a. IPX
   b. NCP
   c. SPX
   d. NetBIOS
11. Which NetWare protocol provides link-state routing?
   a. NLSP
   b. RIP
   c. SAP
   d. NCP
12. Transmission control protocol _____
   a. is a connection-oriented protocol
   b. uses a three way handshake to establish a connection
   c. receives data from application as a single stream
   d. all of the mentioned

13. Transport layer protocols deals with?
    a. Application to application communication
    b. Process to process communication
    c. Node to node communication
    d. Man to man communication
14. A _____ is a TCP name for a transport service access point.
    a. Port
    b. Pipe
    c. Node
    d. Protocol
15. Transport layer protocols deals with _____
    a. application to application communication
    b. process to process communication
    c. node to node communication
    d. man to man communication

| | | | | |
|---|---|---|---|---|
| 1. B | 2. C | 3. | 4. A | 5. B |
| 6. D | 7. B | 8. B | 9. D | 10. A |
| 11. A | 12. D | 13. B | 14. A | 15. B |

**Short Questions**

1. What is internet?
2. What is protocol?
3. How many layers of OSI model?
4. How many layers of TCP/IP model?
5. What is Extranet?
6. What is IP?
7. What is Mac Address?
8. What is Routing protocol?
9. What is Application Layer?
10. What is session Layer
11. What is the function of Physical Layer?
12. What is Port Address
13. What is internet?
14. What is protocol?
15. How many layers of OSI model?
16. How many layers of TCP/IP model?
17. What is Extranet?
18. What is IP?
19. What is Mac Address?
20. What is Routing protocol?
21. What is Application Layer?
22. What is session Layer
23. What is the function of Physical Layer?
24. What is Port Address

Long Question

1. Write the detail Note of OSI Model?
2. Write the detail note on TCP/IP Model?
3. Write the note on Routing protocols
4. Briefly explain the IPv4

# 7 Network Administration and Management

## Objectives

**After completion of this chapter students will be able to:**

- ✓ 7.1. Types of Servers
- ✓ 7.2. Managing Accounts
- ✓ 7.3. Performance Monitoring

**A Computer Architecture** is a design in which all computers in a computer network are organized. An architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc. The two most popular computer architectures are P2P (Peer to Peer) and Client-Server architecture.

1-Peer-To-Peer network

2-Client/Server network

_____

## 7.1 Peer-To-Peer network

- ✓ Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- ✓ Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- ✓ Peer-To-Peer network has no dedicated server.
- ✓ Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

### Advantages of Peer-To-Peer Network:

- ✓ It is less costly as it does not contain any dedicated server.
- ✓ If one computer stops working but, other computers will not stop working.

- ✓ It is easy to set up and maintain as each computer manages itself.

### Disadvantages of Peer-To-Peer Network:

- ✓ In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- ✓ It has a security issue as the device is managed itself.

## 7.2 Client/Server Network

- ✓ Client/Server network is a network model designed for the end users called clients, to access the resources such as files, documents, software etc. from a central computer known as Server.
- ✓ The central controller is known as a server while all other computers in the network are called clients.
- ✓ A server performs all the major operations such as security and network management.
- ✓ A server is responsible for managing all the resources such as files, directories, printer, etc.
- ✓ All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

**Advantages of Client/Server network:**

- ✓ A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- ✓ A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- ✓ Security is better in Client/Server network as a single server administers the shared resources.
- ✓ It also increases the speed of the sharing resources.

**Disadvantages of Client/Server network:**

- ✓ Client/Server network is expensive as it requires the server with large memory.
- ✓ A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- ✓ It requires a dedicated network administrator to manage all the resources.

### Client:

A client is a computer that connects to and uses the resources of a server.

### Server:

A server is a computer designed to process requests and deliver data to another computer over the internet or a local network.

## 7.3 Types of servers:

### 7.3.1 File Server

A file server is a central server in a computer network that provides file systems or at least parts of a file system to connected clients. File servers therefore offer users a central storage place for files on internal data media, which is accessible to all authorized clients. Here, the server administrator defines strict rules regarding which users have which access rights: For instance, the configuration or file authorizations of the respective file system enable the admin to set which files can be seen and opened by a certain user or user group, and whether data can only be viewed or also added, edited, or deleted.

### 7.3.2 Application server

These servers hosts web apps (computer programs that run inside a web browser) allowing users in the network to run and use them preventing the

installation a copy on their own computers. These servers need not be part of the World Wide Web. There clients are computers with a web browser.

### 7.3.3 Fax server

These severs share one or more fax machines over a network which eliminates the hassle of physical access. Any fax sender or recipient are the clients of these servers.

### 7.3.4 Mail servers:

Mail servers send and receive email using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The IMAP and POP3 protocols receive messages and are used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes.

### 7.3.5 Web Server

A web server offers web pages or other content to the web browser by loading the information from a disc and transfer files by using a network to the user's web browser. It is used by a computer or collection of computers to provide content to several users over the internet. This exchange was done with the help of HTTP communicating between the browser and the server.

## 7.4 Managing User Accounts

User accounts are the backbone of network security administration. Through the use of user accounts, you can determine who can access your network, as well as what network resources each user can and cannot access. You can restrict access to the network to just specific computers or to certain hours of the day. In addition, you can lock out users who no longer need to access your network.

### 7.4.1 User Accounts

Every user who accesses a network must have a user account. User accounts allow the network administrator to determine who can access the network and what network resources each user can access.

Every user account is associated with a username and password

### 7.4.2 Built-In Accounts

Most network operating systems come preconfigured with two built-in accounts, named "Administrator" and "Guest."

### 7.4.3 The Administrator account

The Administrator account is the King of the Network. The Administrator account has unlimited access to your network, it is imperative that you secure it immediately after you install the server. When the NOS Setup program asks for a password for the Administrator account, start off with a good random mix of uppercase and lowercase letters, numbers, and symbols. Don't pick some easy-to-remember password to get started, thinking you will change it to something more cryptic later.

- You can't delete it. The system must always have an administrator.
- You can grant administrator status to other user accounts.

You should use it only when you really need to do tasks that require administrative authority.

The default name for the Administrator account is usually simply "Administrator."

### 7.4.4 The Guest accounts

Another commonly created default account is called the Guest account. This account is set up with a blank password and few access rights

## 7.5 User Rights

User accounts and passwords are only the front line of defense in the game of network security. After a user gains access to the network by typing a valid user ID and password, the second line of security defense - rights - comes into play.

**Log on locally:**
The user can log on to the server computer directly from the server's keyboard.

**Change system time:**
The user can change the time and date registered by the server.

**Shut down the system:**
The user can perform an orderly shutdown of the server.

**Back up files and directories:**
The user can perform a backup of files and directories on the server.

**Restore files and directories:**
The user can restore backed-up files.

**Take ownership of files and other objects:**
The user can take over files and other network resources that belong to other users. NetWare has a similar set of user rights.

## 7.6 Group account:

A group account is an account that does not represent an individual user. Instead, it represents a group of users who use the network in a similar way. Instead of granting access rights to each of these users individually, you can grant the rights to the group and then assign individual users to the group. When you assign a user to a group, that user inherits the rights specified for the group.

For example, suppose that you create a group named "Accounting" for the accounting staff and then allow members of the Accounting group access to the network's accounting files and applications. Then, instead of granting each accounting user access to those files and applications, you simply make each accounting user a member of the Accounting group.

## 7.7 Performance Monitoring:

Network performance management NPM is the collection of methods that manage, enable, and ensure a computer network's optimal performance levels. Typically, network performance management demands the routine monitoring of quality and performance service levels for each network component and device.

**Key network performance management functions include:**

- Error rates
- Network delays
- Packet loss
- Packet transmission
- Throughput

Network performance management takes a proactive approach to identifying and reducing bottlenecks and other network problems. These issues affect not

only end users, but also business operations as a whole, including basic internal maintenance tasks.

## MCQ with Answers

1. A Computer network consists of __ number of computers or servers or systems.

   A) 2
   B) 3
   C) More than 2
   D) all

2. A computer network may contain __.

   A) Computers
   B) Printers
   C) Intelligent devices capable of receiving and sending data
   D) All the above

3. Each server in a computer dedicated server network is known as

   A. dedicated server
   B. dedicated receiver
   C. dedicated client
   D. dedicated sender

4. A typical _____ program creates some remote objects, makes references to these objects accessible, and waits for clients to invoke methods on these objects.
   A. Server
   B. Client
   C. Thread
   D. concurrent
5. A typical _____ program obtains a remote reference to one or more remote objects on a server and then invokes methods on them.
   A. Server

B. Client
C. Thread
D. Concurrent

6. An object acting as a gateway for the client side.
   a) skeleton
   b) stub
   c) remote
   d) server
7. The Performance management, is closely related to
   **A.** Risk Management
   **B.** Fault management
   **C.** Security Management
   **D.** Configuration management
8. A set of rules that govern all aspects of information communication is called
   A. Server
   B. Internet
   C. Protocol
   D. OSI Model
9. The processes on each machine that communicate at a given layer are called
   A. UDP process
   B. Intranet process
   C. Server technology
   D. Peer-peer process
10. A switch can allow fast handling of the
    A. Tokens
    B. Frames
    C. Packets
    D. Slots

| | | | | |
|---|---|---|---|---|
| 1. D | 2. D | 3. A | 4. A | 5. B |
| 6. B | 7. B | 8. C | 9. C | 10. C |

## Short Question

1. what is server
2. what is client
3. what is peer to peer network
4. what is client server network
5. what is network administrator
6. what is file server
7. what Is application server
8. what is NTFS
9. what is mail server
10. what is fax server
11. what is Group account
12. what is performance monitoring

## Long Question

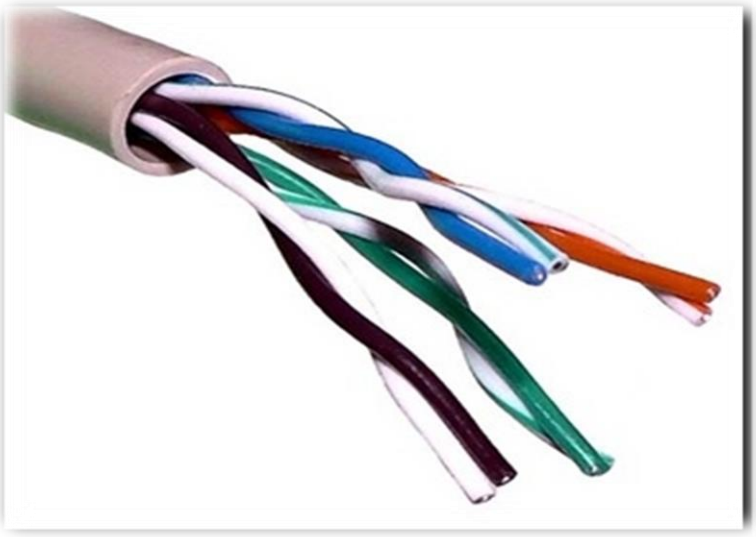
1. What is server also describe its types?
2. How we can manage User accounts?

# 8 Network Troubleshooting

Structured Cabling is defined as building or campus telecommunications cabling infrastructure that consists of several standardized smaller elements (structured)

## 8.1 Twisted-pair cable:

One of the earliest guided transmission media is twisted pair cables. A twisted pair cable comprises two separate insulated copper wires, which are twisted together and run in parallel. The copper wires are typically 1mm in diameter. One of the wires is used to transmit data and the other is the ground reference.



**8-1 Twisted paired Cable**

Following are the two types of Twisted-Pair Cables.

## 8.2 Unshielded Twisted Pair

A twisted pair includes two insulated conductors twisted together in the spiral form, as shown in the figure. It can be shielded with a plastic cover. The UTP cables are very low-cost and simple to install.

## 8.3 Shielded Twisted Pair

In this, each insulated twisted pair are shielded by a metal foil or braided mesh. This mesh is also known as a metal shield. It decreases the interference of the disturbance caused by the surrounding. This property makes the cable bulky and expensive.

**Advantages of Twisted Pair Cables**

- ✓ It is easiest to install, manpower to repair, and service are readily available.
- ✓ It can be the least costly for short distances.
- ✓ If part of a twisted-pair cable is broken, the whole network is not shut down.
- ✓ It is flexible and easy to connect.
- ✓ It has a low weight.

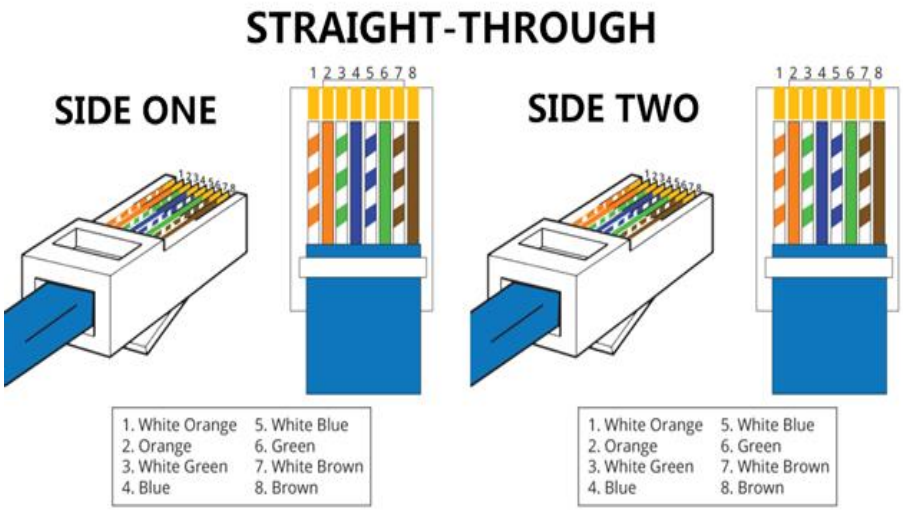
**Disadvantages of Twisted Pair Cables**

- ✓ It is higher error rates when the line length is more than 100 meters because it is easily affected by more signals.
- ✓ It has low bandwidth.

**We make two types of twisted pair cable**

**1-Straight through cable**

A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straight-through cables use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard. The following figure shows a straight-through cable of which both ends are wired as the T568B standard.



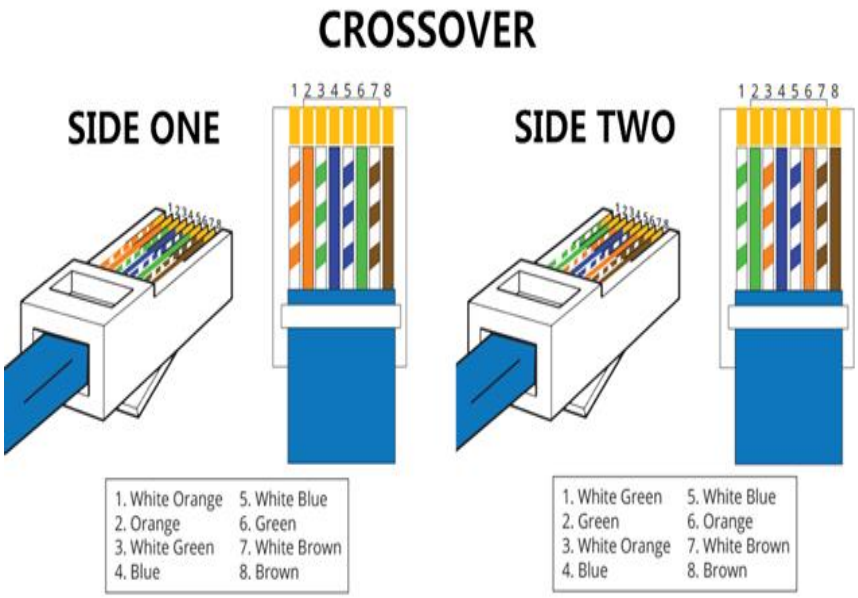

Use straight through cable for the following

- ✓ Switch to PC or server
- ✓ Hub to PC or server

## 8.4 Cross over cable

A crossover Ethernet cable is a type of Ethernet cable used to connect computing devices directly. Unlike straight-through cable, the RJ45 crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most

often used to connect two devices of the same type: e.g. two computers (via network interface controller) or two switches to each other.

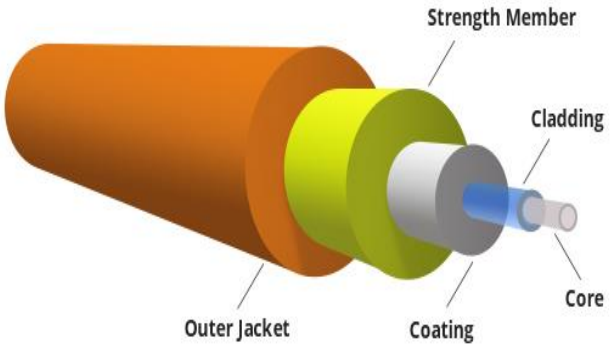



Use crossover cables for the following

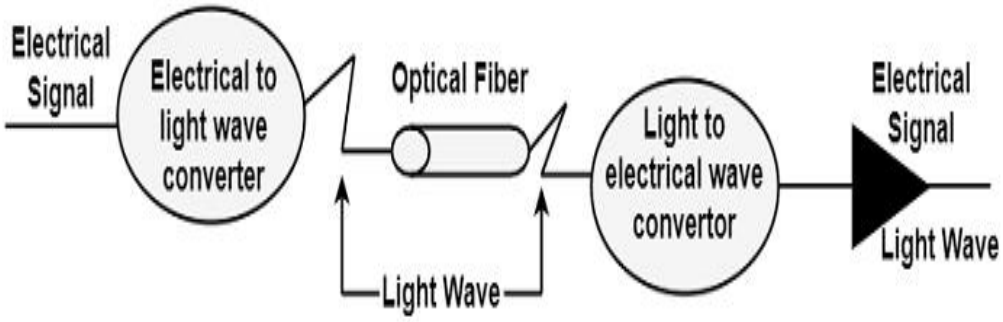
- ✓ Switch to switch
- ✓ Hub to hub
- ✓ Router to router
- ✓ PC to PC

## 8.5 Fiber Optic cable:

Fiber optic cable is made of glass or plastic and transmits signals in the structure of light signals. The structure of an optical fiber cable is displayed in the figure. It involves an inner glass core surrounded by a glass cladding that reflects the light into the core. Each fiber is encircled by a plastic jacket.




In fiber optics, semiconductor lasers transmit data in the form of light along with hair-thin glass (optical) fibers at the speed of light (186,000 miles second) with no significant loss of intensity over very long distances. The system includes fiber optic cables that are made of tiny threads of glass or plastic.




## Single Mode cable

A single Mode cable is a single strand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310nm

or 1550nm. Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width.

## Multimode cable

**Multimode cable** is made of glass fibers, with a common diameter in the 50-to-100 micron range for the light carry component (the most common size is 62.5). POF is a newer plastic-based cable that promises performance similar to glass cable on very short runs but at a lower cost. Multimode fiber gives you high bandwidth at high speeds over medium distances. Light waves are dispersed into numerous paths, or modes, as they travel through the cable's core typically 850 or 1300nm. Typical multimode fiber core diameters are 50, 62.5, and 100 micrometers.

### 8.5.1 Characteristics of Optical Fiber Cables

The main characteristics of Optical Fiber cables are as follows −

- ✓ Fiber optic cabling can support too high bandwidths in the range from 100 Mbps to 2 gigabytes because light has a much greater frequency than electricity.
- ✓ The several nodes that a fiber optic can provide do not rely upon its length but on the hub or hubs that linked cables.
- ✓ Fiber optic cable is not concerned by EMI effects and can be used in locations where high voltages pass.
- ✓ The value of fiber optic cable is more distinguished from twisted pair.
- ✓ The setup of fiber optic cables is complex and endless.

## Advantages of Optical Fibers

The advantage of optical fiber is as follows −

- ✓ **Small Size and lightweight** − The size (diameter) of the optical fibers is minimal (comparable to the diameter of a human hair).

- ✓ **Easily available** − The material used for producing the optical fibers is silica glass. This material is readily applicable. Therefore, the optical fibers cost lower than the cables with metallic conductors.
- ✓ **No electrical or electromagnetic interface** − Since the transmission occurs in light rays, the signal is not affected by electrical or electromagnetic interference.
- ✓ **Large Bandwidth** − As the light arrays have a very high frequency in the GHz range, the optical fiber bandwidth is vast. This allows the transmission of more numbers of channels. Therefore, the information-carrying capacity of an optical fiber is much higher than that of twisted pair and a Co-axial cable.

**Disadvantages of Optical Fibers**

The disadvantage of optical fiber are as follows −

- ✓ **High Cost** − The cable and the interfaces are associatively more expensive than those of other guided media.
- ✓ **Unidirectional light propagation** − Since the optical transmission is inherently unidirectional two-way communication requires either two fibers or two frequency bands on one fiber.
- ✓ **Installation and Maintenance** − FIber is different technology requiring skills; most engineers do not occupy it.

It is defined as fixed point-to-point ground installations.

## 8.6 Network Testing Tools

Network Testing Tools are a collection of software used for measuring various aspects of a network. These tools range from ping monitoring tool, SNMP ping tool, query tool, and more. Network testing tools help network admins to make quick and informed decisions for network troubleshooting.

1. SolarWinds Network Bandwidth Analyzer Pack EDITOR'S CHOICE

Easily monitor network traffic, identify the top talkers on your network, and prioritize bandwidth utilization.

2. SolarWinds Real-Time Bandwidth Monitor (FREE TOOL)

Monitor bandwidth usage in real-time; offers easy to understand graphs.

3. ExtraHop Enterprise solution with the ability to automatically detect and correlate network issues
4. Comparitech Speed Test Free and simple test that's perfect if you just need to check one or a handful of devices.
5. Iperf Open-source tool used for taking active measurements of throughput on a network.
6. NetCPS – freeware bandwidth monitor. NetCPS is a Windows Command Line utility.
7. Netperf – free to use and a fairly popular tool for measuring throughput and benchmarking network speeds.

## 8.7 Basic Network Problems

✓ **Cable Problem**: The cable which is used to connect two devices can get faulty, shortened, or can be physically damaged.

✓ **Connectivity Problem**: The port or interface on which the device is connected or configured can be physically down or faulty due to which the source host will not be able to communicate with the destination host.

✓ **Configuration Issue**: Due to a wrong configuration, looping the IP, routing problem, and other configuration issues, network fault may arise and the services will get affected.

✓ **Software Issue**: Owing to software compatibility issues and version mismatch, the transmission of IP data packets between the source and destination is interrupted.

✓ **Traffic overload:** If the link is over-utilized then the capacity or traffic on a device is more than the carrying capacity of it and due to overload conditions the device will start behaving abnormally.

✓ **Network IP issue:** Due to improper configuration of IP addresses and subnet mask and routing IP to the next hop, the source will not be able to reach the destination IP through the network.

## MCQs with Answers

1- The cable that accepts and transports signals in the form of light is
   a- Unwired
   b- fiber optic cable
   c- coaxial cable
   d- twisted pair cable

2- Which transmission media has the highest transmission speed in a network?
   a- coaxial cable
   b- twisted pair cable
   c- optical fiber
   d- electrical cable

3- Bits can be sent over guided and unguided media as analog signal by
   a- digital modulation
   b- amplitude modulation
   c- frequency modulation
   d- phase modulation

4- Which of the following is not a transmission medium?
   a- telephone lines
   b- coaxial cables
   c- modem
   d- microwave systems

5- The loss in signal power as light travels down the fiber is called
   a- Attenuation
   b- Prorogations
   c- Scattering
   d- Interruption

6- The copper wire is the example of
   a- Unguided media
   b- Guided media
   c- Group media
   d- None

7- Transmission media are usually categorized as _____.
   a- fixed or unfixed
   b- guided or unguided

c- determinate or indeterminate
d- metallic or nonmetallic

8- _____ cable consists of an inner copper core and a second conducting outer sheath.
a- Twisted-pair
b- Coaxial
c- Fiber-optic
d- Shielded twisted-pair

9- In fiber optics, the signal is _____ waves.
a- Light
b- Radio
c- Infrared
d- very low-frequency

10- _____ consists of a central conductor and a shield.
a- Coaxial
b- Fiber-optic
c- Twisted-pair
d- none of the above

**MCQ'S Answers**

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| B | C | A | C | A | B | B | B | A | A |

## Short questions:

1- what is twisted pair cable
2- what is UTP
3- What is STP
4- What is cross over cable
5- What is straight through cable
6- What is RJ-45 connector
7- What is fiber optic cable
8- What is single mode cable
9- What is multimode cable
10-What is Network Testing Tools
11-what is network trouble shooting

## Long Question

1. What is network troubleshooting also describe the types of cable ?
2. What is network testing tools