CHAPTER - 1

1.1 INTRODUCTION

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

1.2 DATA & INFORMATION

Data refers to the raw facts that are collected while information refers to processed data that enables us to take decisions.

Example. When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed.

1.3 DATA COMMUNICATION

- Data Communication is a process of exchanging data or information.
- In case of computer networks this exchange is done between two devices over a transmission medium.
- This process involves a communication system which is made up of hardware and software.
- The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes.

- The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol.

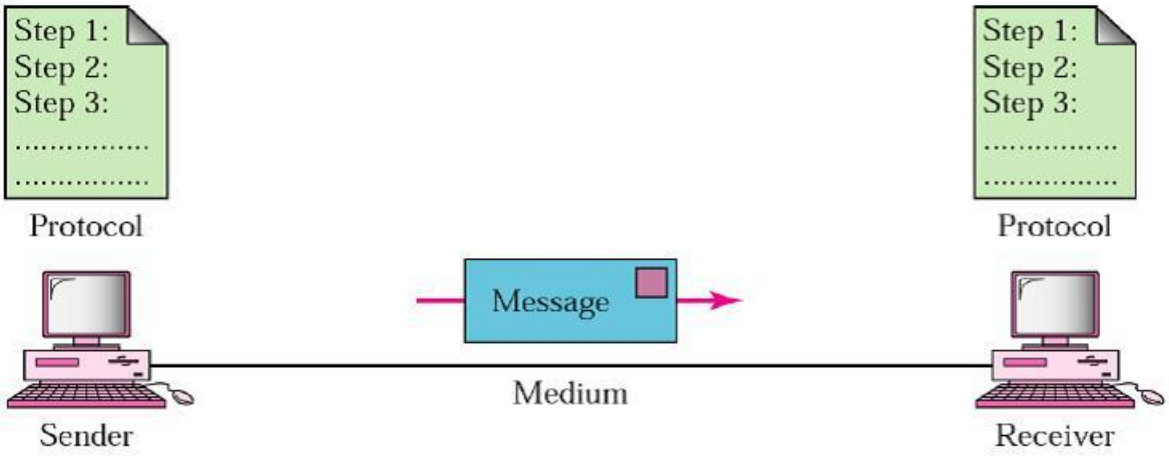
1.3.1 Characteristics of Data Communication

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

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

1.3.2 Components of Data Communication:

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



Components of a Data Communication System

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

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

3. Receiver: The receiver is a device that the sender wants to communicate the data (message).

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

1.4 DATA REPRESENTATION

Data is collection of raw facts which is processed to deduce information. There may be different forms in which data may be represented. Some of the forms of data used in communications are as follows:

1. Text includes combination of alphabets in small case as well as upper case. It is stored as a pattern of bits. Prevalent encoding system: ASCII, Unicode

2. Numbers include combination of digits from 0 to 9. It is stored as a pattern of bits. Prevalent encoding system: ASCII, Unicode

3. Images —An image is worth a thousand words‖ is a very famous saying. In computers images are digitally stored.

- **A Pixel is the smallest element of an image**. To put it in simple terms, a picture or image is a matrix of pixel elements. The pixels are represented in the form of bits. Depending upon the type of image (black n white or color) each pixel would require different number of bits to represent the value of a pixel.
- **The size of an image** depends upon the number of pixels (also called resolution) and the bit pattern used to indicate the value of each pixel.
- **Commonly used Image formats : jpg, png, bmp, etc**

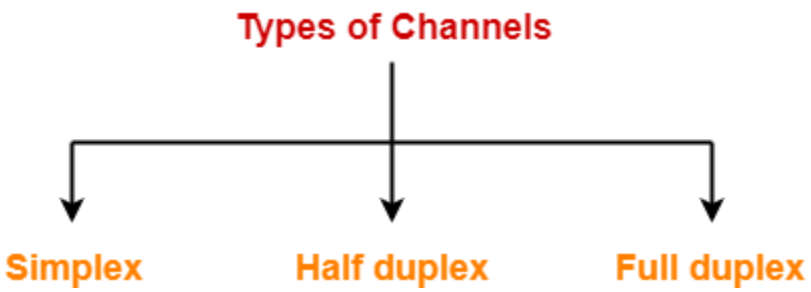
4. Audio Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information. Audio data is continuous, not discrete.

5. Video refers to broadcasting of data in form of picture or movie

1.5 DATA FLOW/ TYPES OF TRANSMISSION MODE

: Devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

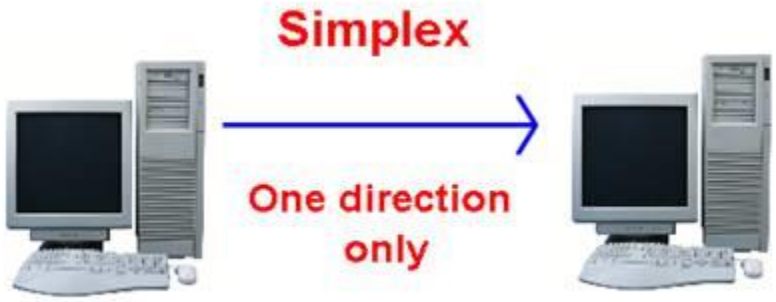
1. Simplex
2. Half Duplex
3. Full Duplex

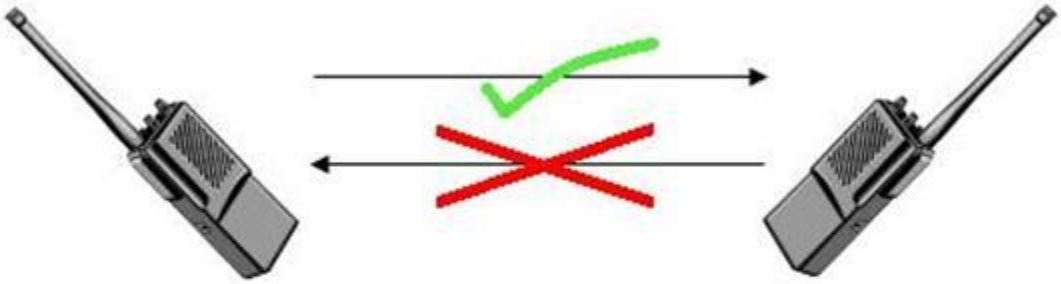


Simplex:

In Simplex, communication is unidirectional only one of the devices sends the data and the other one only receives the data.

Example: in the above diagram: a CPU send data while a monitor only receives data.

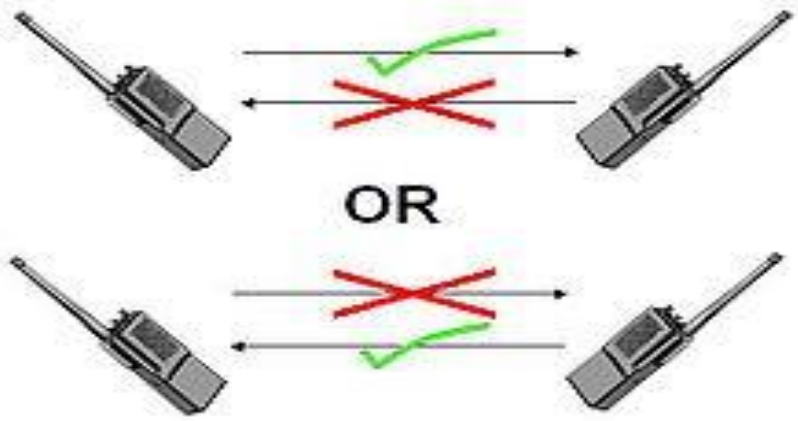




Half Duplex

In half duplex both the stations can transmit as well as receive but not at the same time. When one device is sending other can only receive and vice-versa (as shown in figure above.)

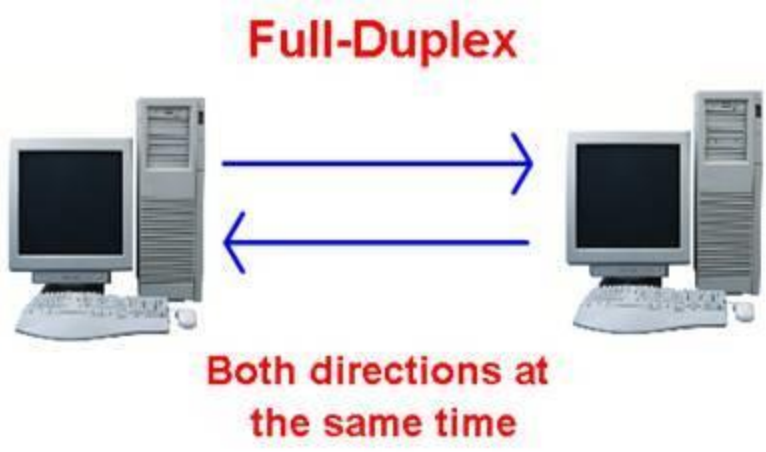
Example: A walkie-talkie.



<u>Full Duplex</u>

In Full duplex mode, both stations can transmit and receive at the same time.

Example: mobile phones



1.7 COMPUTER NETWORK

A computer network can be defined as a collection of nodes. A node can be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links.

A Computer Network must ensure three things:

Network Criteria:

The criteria that have to be met by a computer network are:

- **Performance –** It is measured in terms of transit time and response time.
  - ✓ Transit time is the time for a message to travel from one device to another
  - ✓ Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

- ✓ The number of users
- ✓ Type of transmission medium
- ✓ Capability of connected network
- ✓ Efficiency of software

- **Reliability –** It is measured in terms of

- ✓ Frequency of failure
- ✓ Recovery from failures
- ✓ Robustness during catastrophe
- ✓ If there are alternate sources of supply, all files could be replicated on two or, machines. If one of them is not available, due to hardware failure, the other copies could be used.

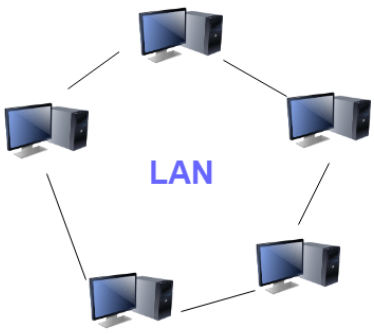
- **Security –** It means protecting data from unauthorized access.

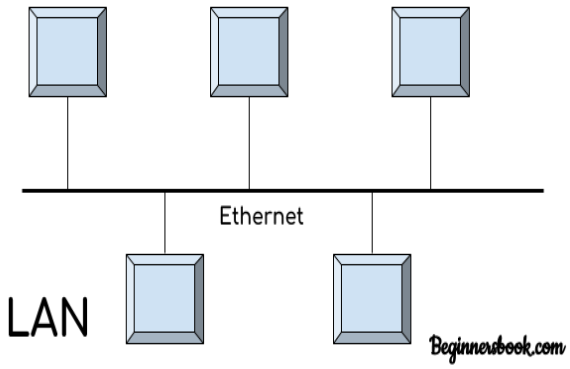
1.7.1 CATEGORIES OF NETWORK

Networks are categorized on the basis of their size. The three basic categories of computer networks are:

- **LAN - Local Area Network**

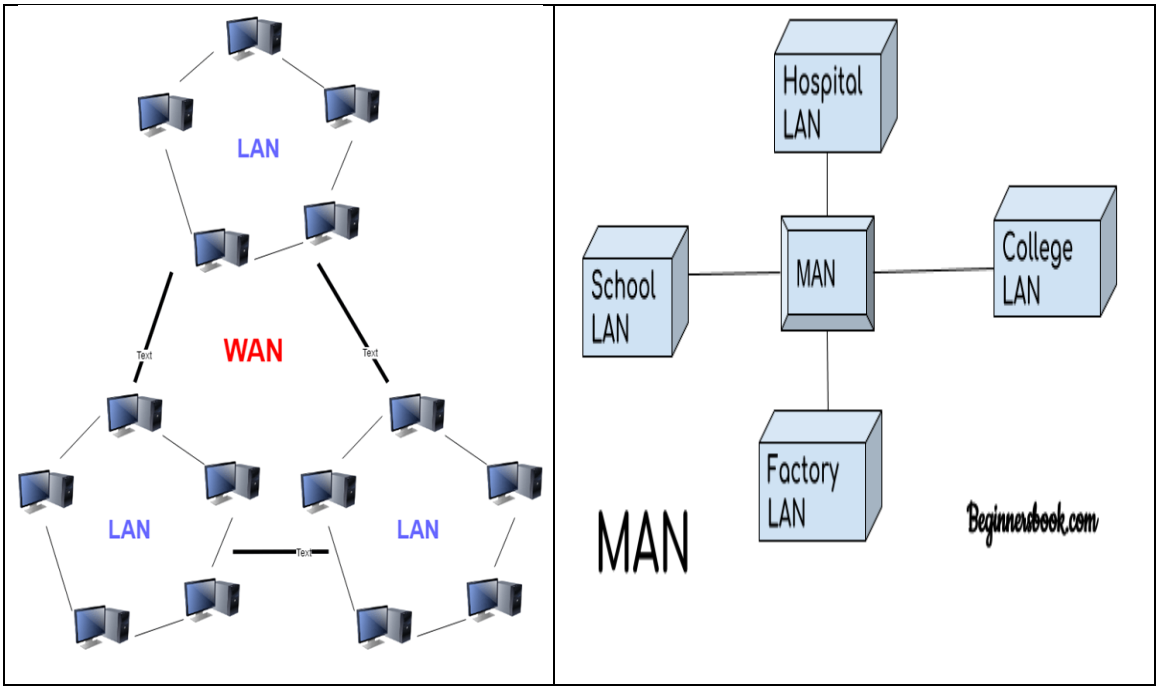
  A Local Area Network (LAN) is a private network that connects computers and devices within a limited area like a residence, an office, a building or a campus. On a small scale, LANs are used to connect personal computers to printers.





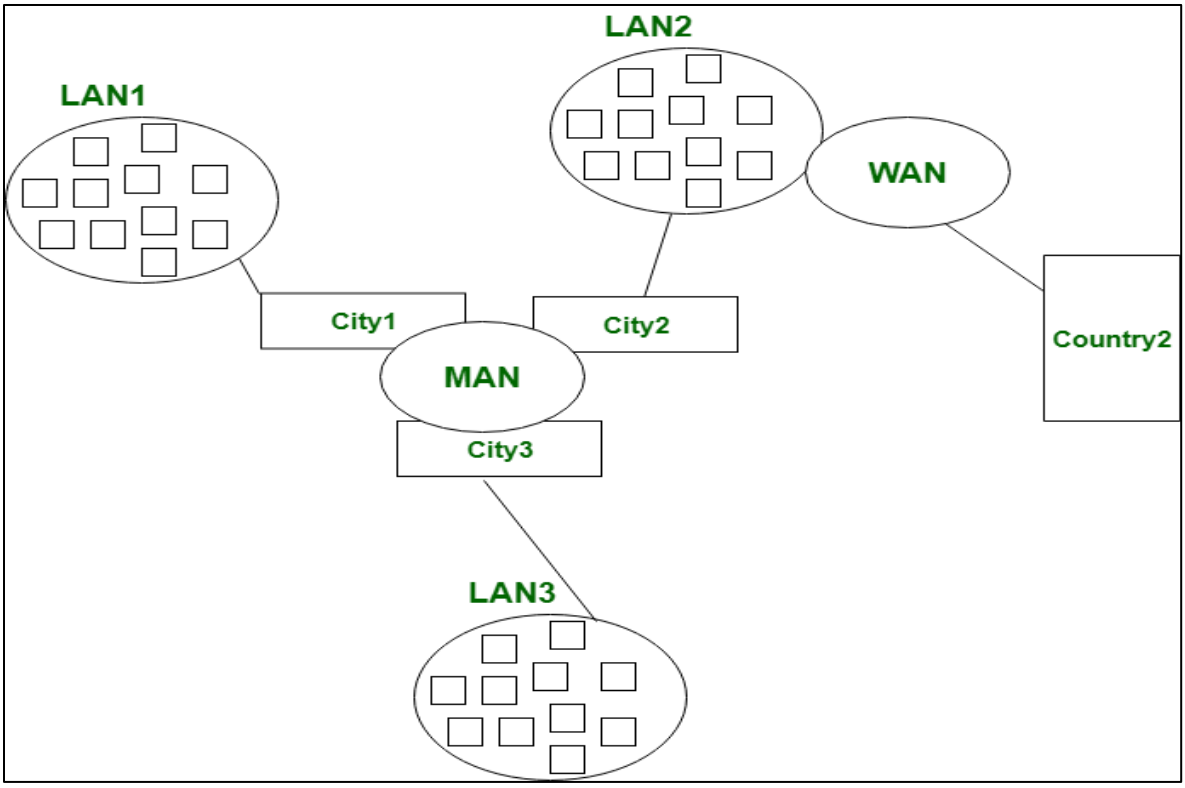
- **MAN - Metropolitan Area Network**

  A Metropolitan Area Network (MAN) is a larger network than LAN. It often covers multiple cities or towns. It is quite expensive and a single organization may not have own it.



- **WAN - Wide Area Network**

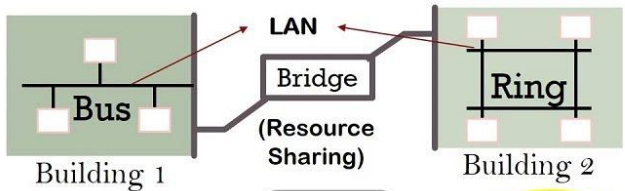
  A Wide Area Network (WAN) is a much larger network than LAN and MAN. It often covers multiple countries or continents. It is quite expensive and a single organization may not have own it. Satellite is used to manage WAN

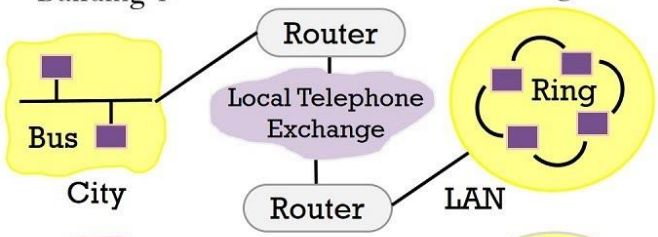

LAN2
LAN1
WAN
City1
City2
Country2
MAN
City3
LAN3

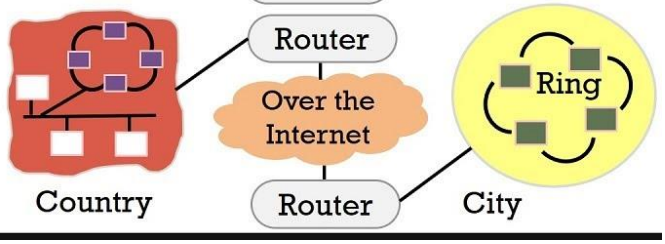
LAN

MAN

WAN


LAN
Bridge
Bus
Ring
(Resource Sharing)
Building 1
Building 2


Router
Local Telephone Exchange
Bus
Ring
City
Router
LAN


Router
Over the Internet
Ring
Country
Router
City

Following are the important differences between LAN, MAN and WAN.

Sr. No.	Key	LAN	MAN	WAN
1	Definition	LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
2	Ownership	LAN is often owned by private organizations.	MAN ownership can be private or public.	WAN ownership can be private or public.
3	Speed	LAN speed is quiet high.	MAN speed is average.	WAN speed is lower than that of LAN.
4	Delay	Network Propagation Delay is short in LAN.	Network Propagation Delay is moderate in MAN.	Network Propagation Delay is longer in WAN.
5	Congestion	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
6	Fault Tolerance	Fault Tolerance of LAN is higher than WAN.	Fault Tolerance of MAN is lower than LAN.	Fault Tolerance of WAN is lower than both LAN and MAN.

7	Maintenance	Designing and maintaining LAN is easy and less costly than WAN.	Designing and maintaining WAN is complex and more costly than LAN.	Designing and maintaining WAN is complex and more costly than both LAN and MAN.
8	Devices used for Transmission	WiFi, Ethernet Cables.	Modem and Wire/Cable	Optic wires, Microwaves, Satellites.
9	Range in Km	1 KM	5-50 KM	Over 50 Kms

1.8 Line Configuration

Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another. For communication to occur, two devices must be connected in same way to the same link at the same time.

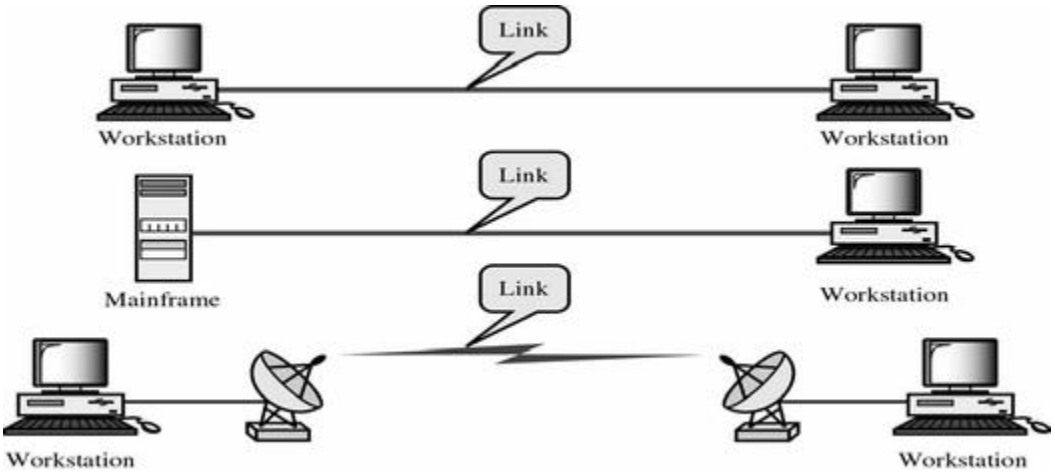
There are two possible line configurations.

1. Point-to-Point.
2. Multipoint.

Point-to-Point

A **Point to Point Line Configuration** Provide dedicated link between **two devices** use actual length of wire or cable to connect the two end including microwave & satellite link. Infrared remote control & TV remote control.

The entire capacity of the channel is reserved for transmission between those two devices. Most point-to-point line configurations use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

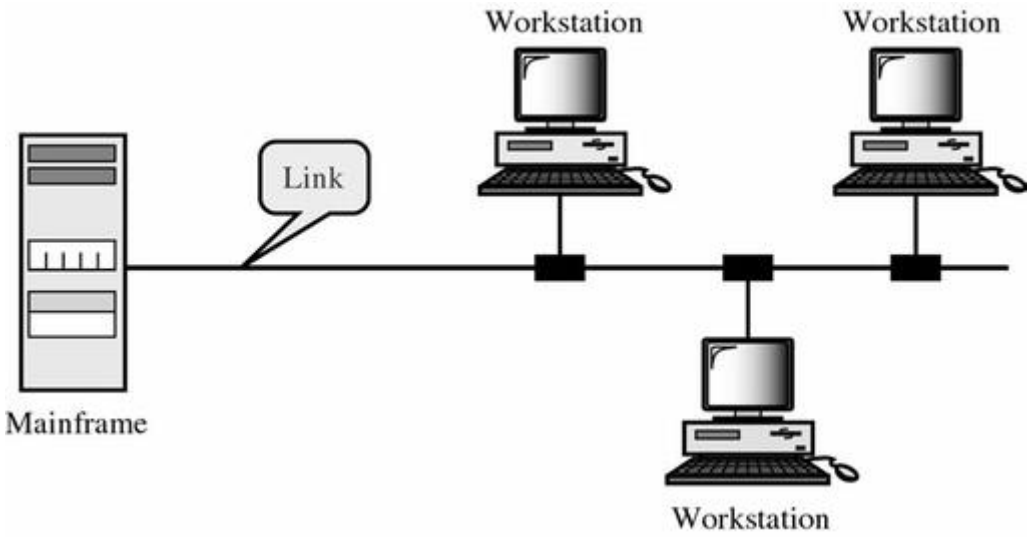


Multipoint Configuration

Multipoint Configuration also known as **Multidrop line configuration** one or **more than two specific devices** share a single link capacity of the channel is shared.

More than two devices share the Link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line Config:

- **Spatial Sharing**: If several devices can share the link simultaneously, it's called Spatially shared line configuration
- **Temporal (Time) Sharing**: If users must take turns using the link , then it's called Temporally shared or Time Shared Line Configuration



1.9 TYPES OF NETWORK TOPOLOGY

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology

The nodes in a network can have following two relationships:

1. Peer to Peer: In this relationship, all the devices in the network have equal status in sharing the link. For example, Ring & Mesh topology.

2. Primary-Secondary: In this, one device controls the traffic and all other devices transmit through primary device. *e.g.* Star topology.

The various network topologies are:

a) Mesh Topology:
In mesh topology, every device is connected to another device via particular channel.

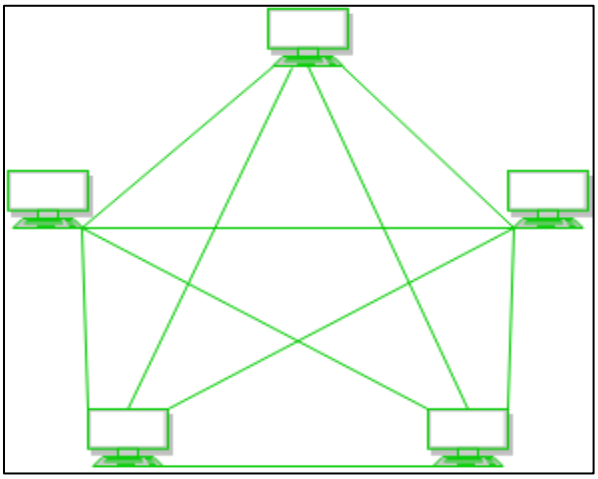


Figure 1: Every device is connected with another via dedicated channels. These channels are known as links.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is? N-1. In the Figure 1,
- There are 5 devices connected to each other, hence total number of ports required is 4.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is **n(n-1)/2**

- In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5*4/2 = 10.

No of Links: n(n-1)/2 **No of Ports : n-1**

Q: A company has fully connected mesh network consisting of 8 devices: Calculate the total no of ports needed for each device and no. of cable links

Ans: No of ports: n-1 = 7
No of Links : n(n-1)/2 = 28

Advantages of this topology:

- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Problems with this topology:

- Installation and configuration is difficult.
- Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
- Cost of maintenance is high.

b) Star Topology:

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. The hub can be passive? In nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active? Hubs. Active hubs have repeaters in them.

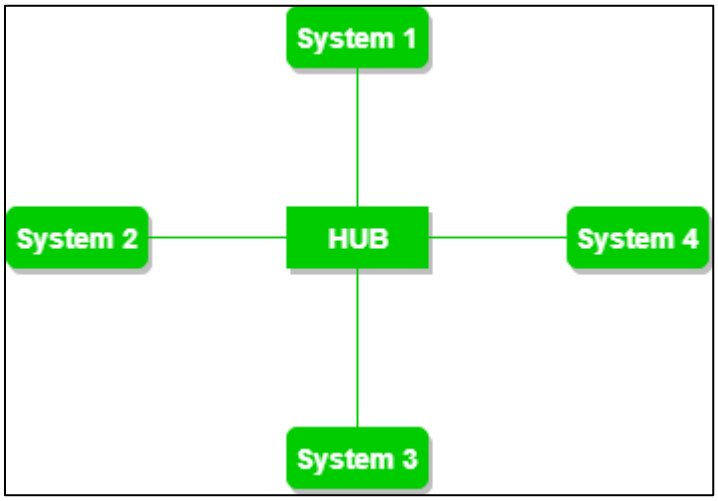


Figure 2: A star topology having four systems connected to single point of connection i.e. hub.

Advantages of this topology:

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device require only 1 port i.e. to connect to the hub.

Problems with this topology:

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Performance is based on the single concentrator i.e. hub.

c) Bus Topology:

Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

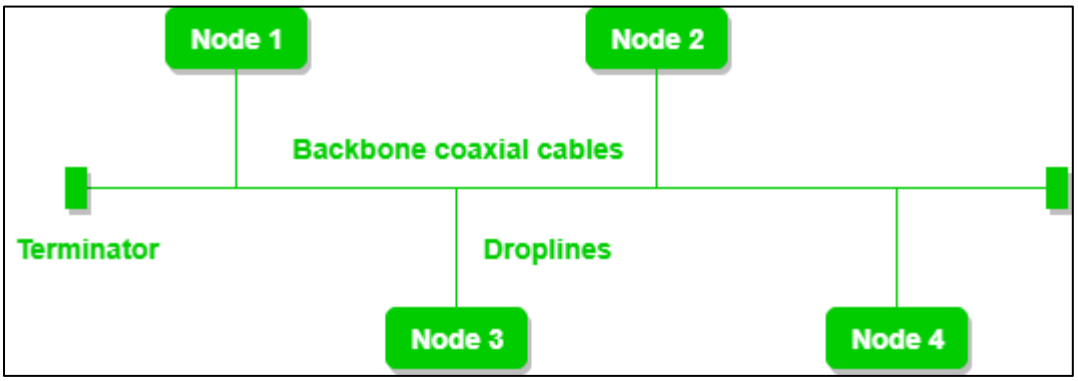


Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology:

- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.

- Cost of the cable is less as compared to other topology, but it is used to build small networks.

Problems with this topology:

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, and CSMA/CD etc

d) Ring Topology:

In this topology, it forms a ring connecting a devices with its exactly two neighboring devices.

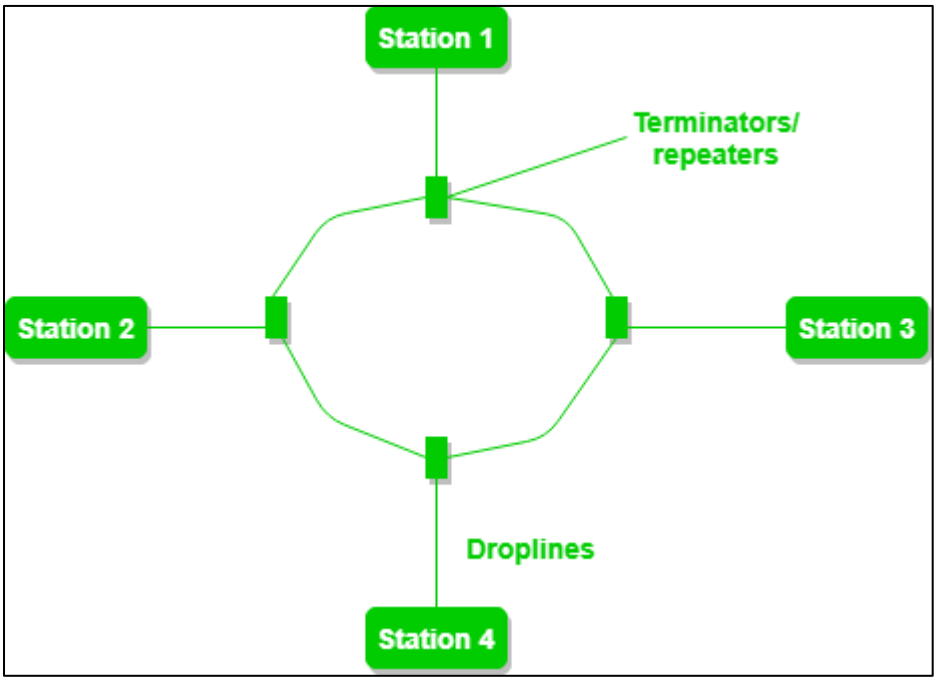


Figure 4: A ring topology comprises of 4 stations connected with each forming a ring.

The following operations takes place in ring topology are:

1. To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.

Advantages of this topology:

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Problems with this topology:

- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

e) Tree Topology:

This topology is the variation of Star topology. This topology have hierarchical flow of data.

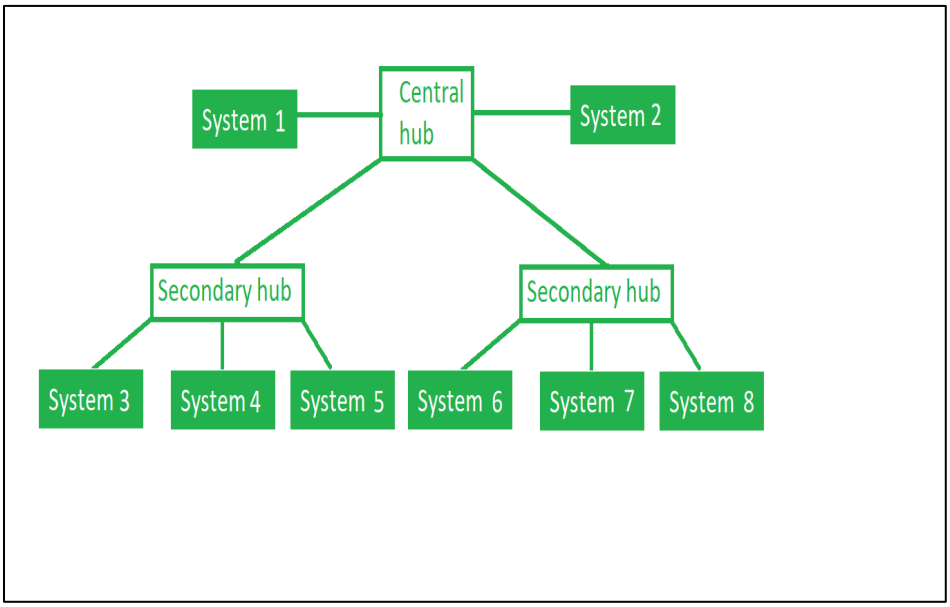


Figure 5: In this the various secondary hubs are connected to the central hub which contains the repeater. In this data flow from top to bottom i.e. from the central hub to secondary and then to the devices or from bottom to top i.e. devices to secondary hub and then to the central hub.

Advantages of this topology:

- It allows more devices to be attached to a single central hub thus it increases the distance that is travel by the signal to come to the devices.
- It allows the network to get isolate and also prioritize from different computers.

Problems with this topology:

- If the central hub gets fails the entire system fails.
- The cost is high because of cabling.

f) Hybrid Topology:

This topology is a collection of two or more topologies which are described above. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly topology.

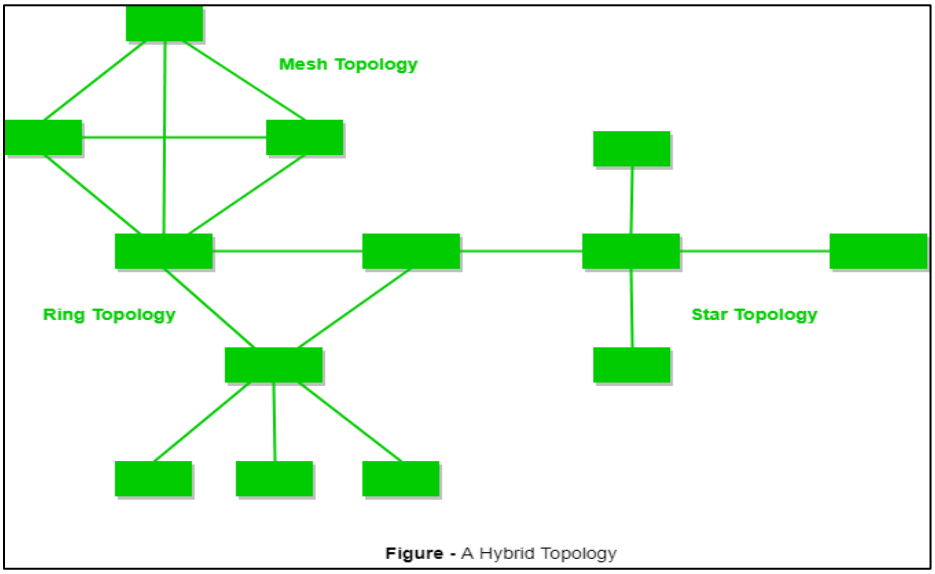


Figure - A Hybrid Topology

Figure 6: A hybrid topology which is a combination of ring and star topology.

1.10 PROTOCOL

A set of rules: for successful communication to occur, the sender and receiver must agree upon certain rules called protocol.

A Protocol is defined as a set of rules that governs data communications. A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

1.8.1 Elements of a Protocol

There are three key elements of a protocol:

- **Syntax**

✓ It means the structure or format of the data.

✓ It is the arrangement of data in a particular order.

- **Semantics**

✓ It tells the meaning of each section of bits and indicates the interpretation of each section.

✓ It also tells what action/decision is to be taken based on the interpretation.

- **Timing**

✓ It tells the sender about the readiness of the receiver to receive the data

✓ It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

1.11 STANDARDS IN NETWORKING

Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components.

Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.

1.11.1 Concept of Standard

Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.

Data communications standards are classified into two categories:

- **De facto Standard (by fact)**

These standards are not approved by any organized body but are adopted by widespread use.

- **De jure standard (by law)**

It means by **law** or **by regulation.**

These standards are legislated and approved by a body that is officially recognized.

1.11.2 Standard Organizations in field of Networking

Standards are created by standards creation committees, forums, and government regulatory agencies.

Examples of Standard Creation Committees:

1. International Organization for Standardization (ISO)
3. American National Standards Institute (ANSI)
4. Institute of Electrical & Electronics Engineers (IEEE)
5. Electronic Industries Associates (EIA)

2. International Telecommunications Union – Telecommunications Standard (ITU-T)

1.12 FORUMS:

Telecommunications technology development is moving faster than the ability of standards committee to ratify standards.

Standards committees are procedural bodies and by nature slow moving to accommodate the need from working models and agreements and to facilitate the standardization process, many special-interest groups have developed *forums* made up of representatives from interested corporations.

The forums work with universities and users to test, evaluate and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community.

The forums present their conclusions to the standards bodies. Some important forums for the telecommunications industry include the following:

- **Frame Relay Forum.** The Frame Relay Forum was formed by digital equipment Corporation, Northern Telecom, Cisco, and StrataCom to promote the acceptance and implementation of frame relay. Today, it has around 40 members representing North America, Europe, and the Pacific Rim. Issues under Review include flow control. Encapsulation, translation, and multicasting. **The forum's results are submitted to the ISO.**

- **ATM Forum. http://www.atmforum.com/** The ATM Forum provides acceptance and use of Asynchronous Transfer Mode (ATM) technology. The ATM Forum is made up of Customer Premises Equipment (e.g., PBX systems) vendors

and Central Office (e.g., telephone exchange) providers. It is concerned with the standardization of service to ensure interoperability.

1.13 REGULATORY AGENCIES

Human beings are animals that communicate intensively, and all communication systems, beginning with spoken and written languages, are regulated in at least informal ways.

Most people feel that there are certain things that should not be said or written and that certain forms of speech and writing are appropriate for different contexts.

However, with the development of physical communication systems such as the postal system and even more with that of the telegraph, telephone, radio, and television, regulation guided by ethical principles has become an increasingly prominent feature of those technologies?

Ethical principles concerning content and access have created the foundation for regulation of communication systems.

Concerns about content include privacy and anonymity, copyright, defamation, censorship, and profanity. Ethical issues relating to access include concerns about the availability of communication systems and control of content production.

Federal Communications Commission (FCC). http://www.fcc.gov/ The Federal Communications Commission (FCC) has authority over interstate and international commerce as it relates to communications.

PROTOCOLS IN DETAIL

A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

You can think of a protocol as a spoken language. Each language has its own rules and vocabulary. If two people share the same language, they can communicate effectively.

Similarly, if two hardware devices support the same protocol, they can communicate with each other, regardless of the manufacturer or type of device. For example, an Apple iPhone can send an email to an Android device using a standard mail protocol. A Windows-based PC can load a webpage from a Unix-based web server using a standard web protocol.

Protocols exist for several different applications. Examples include wired networking (e.g., Ethernet), wireless networking (e.g., 802.11ac), and Internet communication (e.g., IP). The Internet protocol suite, which is used for transmitting data over the Internet, contains dozens of protocols. These protocols may be broken up into four catagories:

1. **Link layer** - PPP, DSL, Wi-Fi, etc.
2. **Internet layer** - IPv4, IPv6, etc.
3. **Transport layer** - TCP, UDP, etc.
4. **Application layer** - HTTP, IMAP, FTP, etc.

Link layer protocols establish communication between devices at a hardware level. In order to transmit data from one device to another, each device's hardware must support the same link layer protocol. Internet layer protocols are used to initiate data transfers and route them over the Internet. Transport layer protocols define how packets are sent, received, and confirmed. Application layer protocols contain commands for specific applications. For example, a web browser uses HTTPS to securely download the contents of a webpage from a web server. An email client uses SMTP to send email messages through a mail server.

Protocols are a fundamental aspect of digital communication. In most cases, protocols operate in the background, so it is not necessary for typical users to know how each protocol works. Still, it may be helpful to familiarize yourself with some common protocols so you can better understand settings in software programs, such as web browsers and email clients.