Republic of Iraq
Middle Technical University
Technical Engineering College of Artificial Intelligence
Cybersecurity Engineering Technology Department

Computer Network Fundamentals

Chapter One

Introduction to Networking

Prepared By:
Associate Prof. Dr. Mahmoud Shuker Mahmoud
mahmoud.shukur@mtu.edu.iq

Dr. Eng. M. S. Mahmoud

Introduction to Networking

A network is a set of devices (nodes) connected by communication links; each node is capable of sending and/or receiving data generated by other nodes on the network.

1.1- Data Communication:

- When we communicate, we are sharing information. This sharing can be **local** or **remote**. ***Local communication*** usually occurs face to face, while ***remote communication*** takes place over distance.

- The term ***Telecommunication,*** which includes telephony and television, means *communication at a distance*.

- ***Data communication*** is the exchange of *data* (in the form of 0's and 1's) between two *devices* via some form of *transmission medium* (such as a wire cable).

- The effectiveness of a data communications system depends on three fundamental characteristics: (Delivery, Accuracy, and Timeliness)
  1. **Delivery**: The system must deliver data to the correct destination; Data must be received by the intended device or user.
  2. **Accuracy:** The system must deliver the data accurately; Data that have been altered (delay) 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.

1.2- Components:

A data communication system is made up of five components (see Figure 1).

1. ***Message***: The message is the information (data) to be communicated. It can consist of text, numbers, pictures, sound, or video or any combination of these.
2. ***Sender***: The sender is the device that sends the data message. It can be a ***computer***, workstation, mobile phone, video camera, and so on.
3. ***Receiver***: The receiver is the device that receives the message. It can be a computer, workstation, mobile phone, television, and so on.
4. ***Medium:*** The transmission medium is the physical path by which a message travels from-sender to receiver. It can consist of twisted pair wire, coaxial cable, fiber- optic cable, laser, or radio waves.
5. ***Protocol***: A protocol is a set of rules that govern data communication. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating; just as a person who speaks, only Japanese cannot understand a person speaking French.

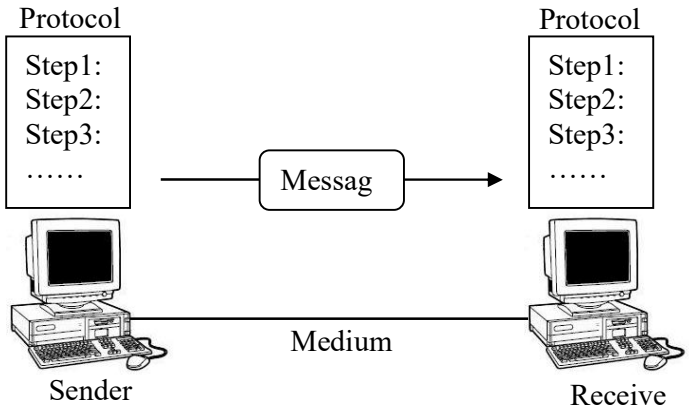


Figure (1) Components of a Data Communication System

1.3 Network Criteria:

To be considered effective and efficient, a network must meet a number of criteria. The most important of these are ***performance***, ***reliability***, and ***security***.

(A) Performance:

Performance can be measured in many *ways,* including *transit time* and *response time*.

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

The performance of a network ***depends on*** a number of factors:

- ✓ ***Number of users:***

Having a large number of concurrent users can slow response time in a network not designed to coordinate heavy traffic loads. The design of a given network is based on an assessment of the average number of users that will be communicating at any one time. How a network responds to loading is a measure of its performance.

- ✓ ***Type of transmission medium***:

The medium defines the speed at which data can travel through a connection (the data rate). Today's networks are moving to faster and faster transmission media, such as fiber optic cabling. A medium that can carry data at 1000 megabits per second is ten times more powerful than a medium that can carry data at only 100 megabits per second. Today transmission speeds have increased to 10Gps and 40Gps

(B) Reliability:

In addition to accuracy of delivery, network reliability is measured by frequency of failure, the time it takes a link to recover from a failure, and the network's robustness.

- ✓ ***Frequency of failure***:

All networks fail occasionally. A network that fails often, however, is of little value to a user.

✓ ***Recovery time of a network after a failure***:

How long does it take to restore service? A network that recovers quickly is more useful than one that does not.

✓ ***Catastrophe*:**

Networks must be protected from catastrophic events such as fire or theft. One protection against unforeseen damage is a reliable system to back up network software.

(C) Security:

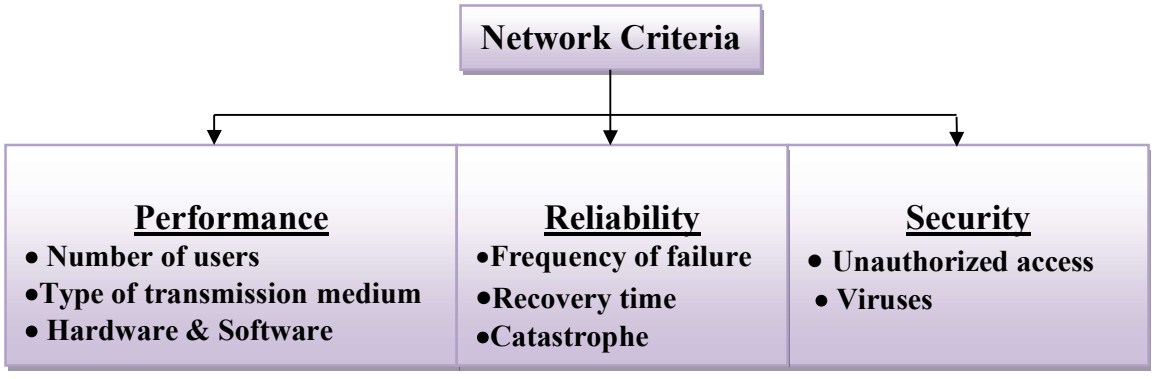
Network security issues include protecting data from unauthorized access and viruses.

✓ ***Unauthorized access***:

For a network to be useful, sensitive data must be protected from unauthorized access. Protection can be accomplished at a number of levels. At the lowest level are user identification codes and passwords. At a higher level are encryption techniques.

✓ ***Viruses***:

Because a network is accessible from many points, it can be susceptible to computer viruses. A virus is an illicitly introduced code that damages the system. A good network is protected from viruses by hardware and software designed specifically for that purpose.



1.4- Basic Concepts of Networking

Before examining the specifics of how data are transmitted from one device to another it is important to understand the relationship between the communicating devices. Five general concepts provide the basis for this relationship.

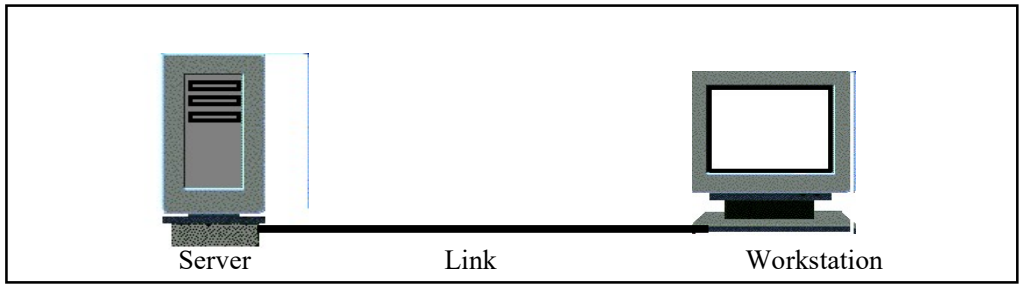
- Line configuration.
- Topology.
- Transmission mode.
- Categories of networks.
- Internetworks.

1.4.1- Line Configuration

A link is the physical communication pathway that transfers data from one device to another. Line configuration defines the attachment of communication devices to a link. There are two possible line configurations:

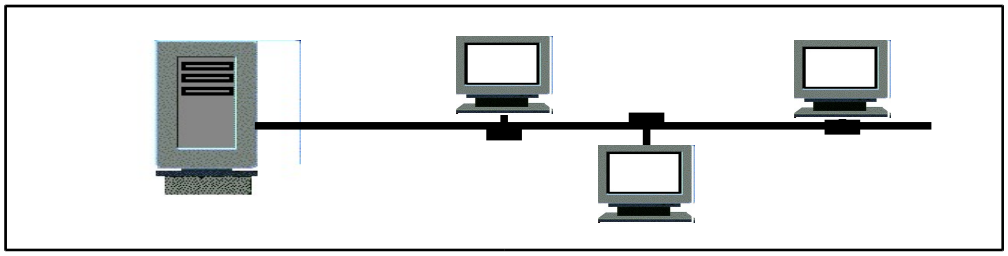
Point-to-Point

A point-to point line configuration provides a **dedicated** link between two devices. 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

A multipoint (also called multidrop) line configuration is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is **shared,** either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared line configuration. If users must take turns, it is a time-shared line configuration.



1.4.2- Topology

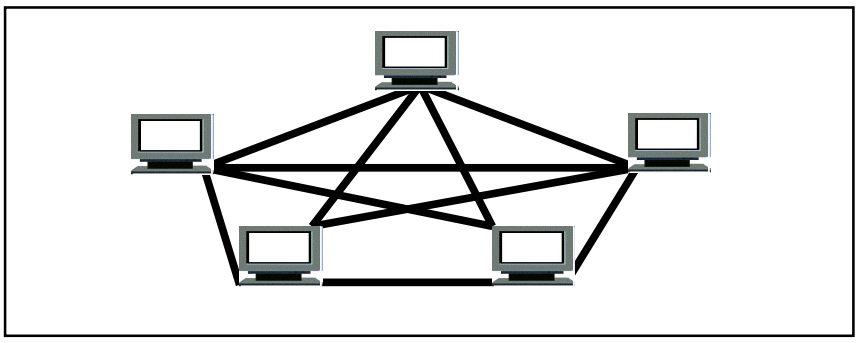
The term topology refers to the way a network is laid out, either *physically* or *logically*. Two or more devices connect to a link; two or more links form a topology. ***The topology of a network is the geometric representation of the relationship of all the links and linking devices (nodes) to each other***.

There are five basic topologies possible. These five labels describe how the devices in a network are interconnected rather than their physical arrangement.

Two relationships are possible: ***peer-to-peer***, where the devices, share the link equally, and ***client-server***, where one device controls traffic and the others must transmit through it. Ring and mesh topologies are more convenient for peer-to-peer transmission, while star and tree are more convenient for client-server. A bus topology is equally convenient for either.

❖ *Mesh Topology*

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.
A fully connected mesh network therefore has **[n (n-1) / 2**] physical channels to link it devices. (See Figure below).



A mesh offers ***several advantages*** over other network topologies:

1. The use of dedicated links guarantees that each connection can carry its data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. A mesh topology is robust; if one link becomes unusable, it does not affect the entire system.
3. Security where every message sent travels along a dedicated line, only the intended recipient sees it.
4. Point-to-point links make fault identification and fault isolation easy.

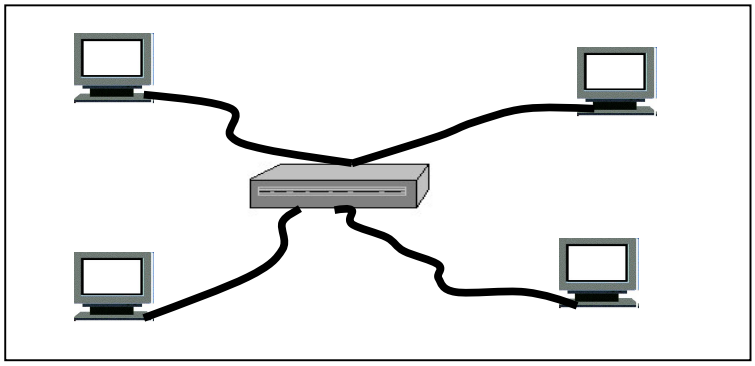
The main ***disadvantages*** of a mesh topology are:

1. Difficult installation and reconfiguration because every device must be connected to every other device.
2. The bulk of the wiring can be greater than the available space can accommodate.
3. The hardware required to connect each link can be expensive.

Due to these reasons, a mesh topology is usually of limited use

❖ *Star Topology*

In a star topology, each device has a dedicated point-to-point link only to a *central controller,* usually called a **hub or switch**. The devices are not linked to each other. Unlike a mesh topology, a star topology ***does not*** allow direct traffic between devices. The controller acts as an exchange. If one device wants to send data to another, it sends to the controller, which then relays the data to the other connected devices.



The ***advantages*** of star topology are:

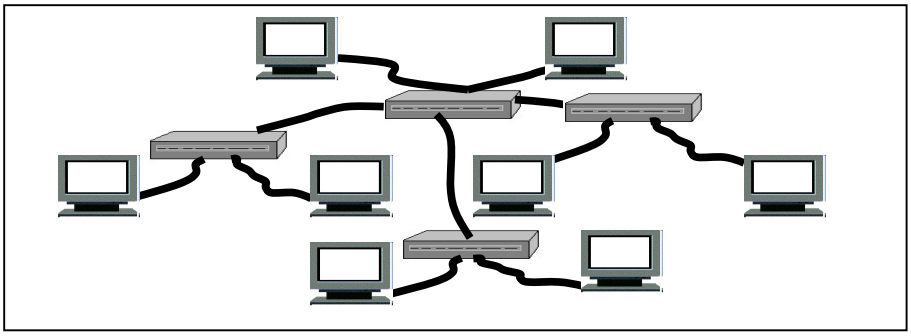
1. Less expensive than a mesh topology.
2. Easy to install.
3. Robustness; If one link fails, only that link is affected.
4. Easy fault identification and fault isolation; As long as the hub is working, it can be used to monitor link problems and bypass defective links.

The ***disadvantages*** of the star topology are:

1. Any fault occur to the central controller will drop down the entire network.
2. Although the star needs less cabling than mesh, it still needs more cables than ring and tree topology.

❖ *Tree Topology*

A tree topology is a variation of a star. However, not every device plugs directly into the central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub.



The central hub in the tree is an active hub. An ***active hub*** contains a repeater, which is a hardware device that regenerates the received bit patterns before sending them out. Repeating strengthens transmissions and increases the distance a signal can travel between sender and receiver.

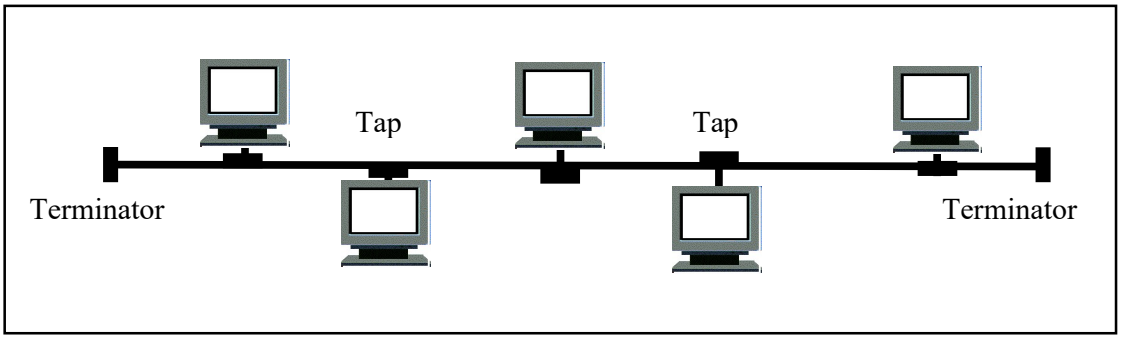
The secondary hubs may be active or ***passive hubs***. A passive hub provides a simple physical connection between the attached devices. Internally, each passive hub contains a set of resistors to balance the circuit linking the connected devices.

The advantages and disadvantages of a tree topology are generally the same as those of a star. The addition of secondary hubs however, brings two ***further advantages.***

First, it allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
Second, it allows the network to isolate and prioritize communications from different computers.

❖ ***Bus Topology***

The preceding examples all describe point-to-point configurations A bus topology on the other hand, is multipoint. One long cable act as a backbone to link all the devices in the network.



Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection that running between the device and the main cable, a tap is a connector that splices into the main. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker the farther it has to travel. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.

The ***advantages*** of a bus topology are:

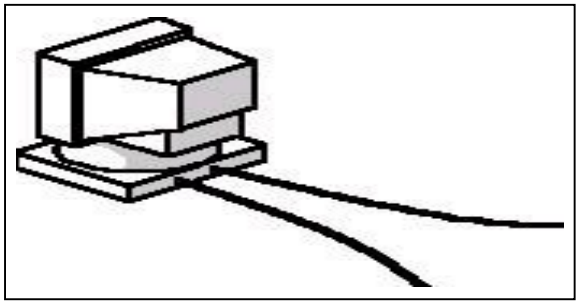
1. Ease of installation.
2. Use less cabling than mesh, star, and tree topologies.

While the ***disadvantages*** are:

1. Difficult reconfiguration and fault isolation.
2. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.
3. Adding new devices may therefore require modification or replacement of the backbone.

❖ *Ring Topology*

In a ring topology, each device has a dedicated point-to-point line configuration only with the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



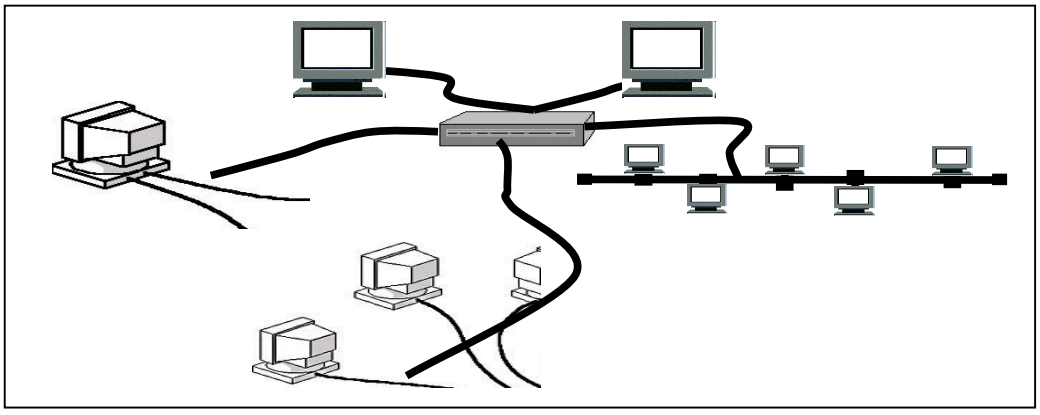
The ***advantages*** of ring topology are:

1. Relatively easy to install and reconfigure.
2. Addition or deletion of a device requires moving only two connections.

The ***disadvantage*** of the ring topology is that a break in the ring (such as a disabled station) can disable the entire network, and it is one way data flow.

❖ *Hybrid Topologies*

Often a network combines several topologies as sub-networks linked together in a larger topology. For instance, one department of a business may have decided to use a bus topology while another department has a ring. The two can be connected to each other via a central controller in a star topology.



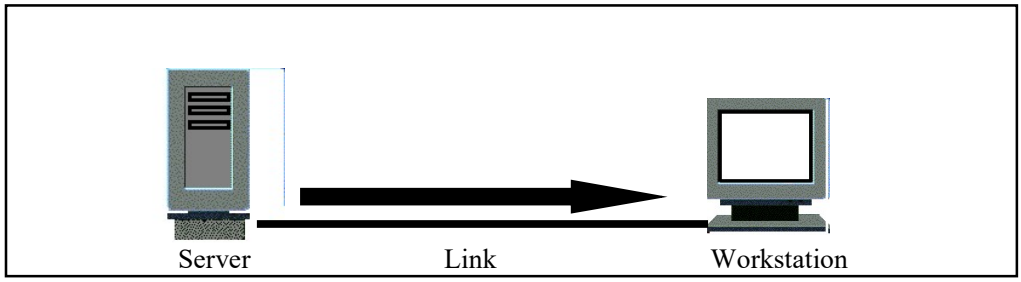
1.4.3- Transmission Modes

The term transmission mode is used to define the direction of signal flow between two linked devices. There are *three* types of transmission modes:

- ***Simplex.***
- ***Half duplex.***
- ***Full duplex***

Simplex

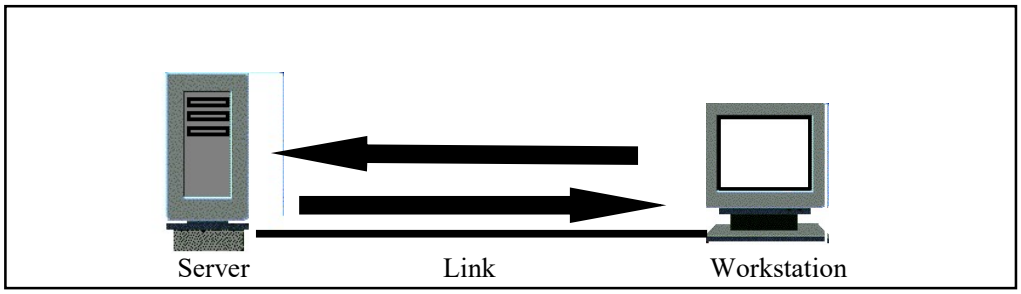
In, simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two stations on a link can transmit the other can only receive.



Keyboards and traditional monitors are both examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.

Half-Duplex

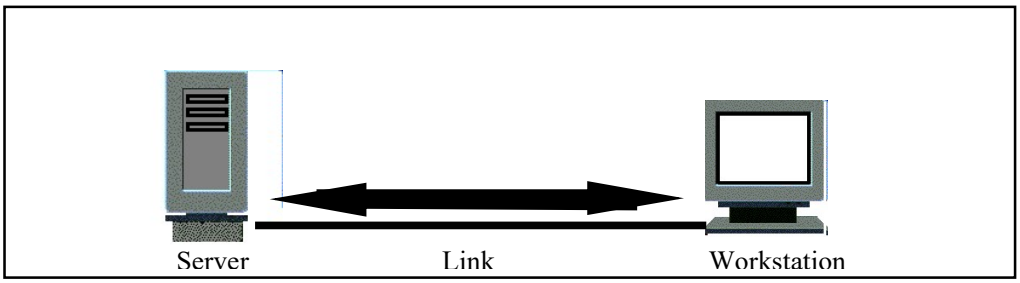
In half-duplex mode, each station can both transmit and receive, but not at the same time When one device is sending, the other can only receive, and vice versa (see Figure below).



The half-duplex mode is like a one-lane road with two-directional traffic. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies are half-duplex systems.

Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously.



The full-duplex mode is like a two-way street with traffic flow in both directions at the same time. In full-duplex mode, signals going in either direction share the capacity of the link.

1.4.4- Categories of Networks

The category of a network can be determined

- According to its size.
- According to its physical architecture (center of control).
- According to transmission technology.
- According to its ownership.
- According to service providing.

(A) According to the size:

We are generally referring to three primary categories:

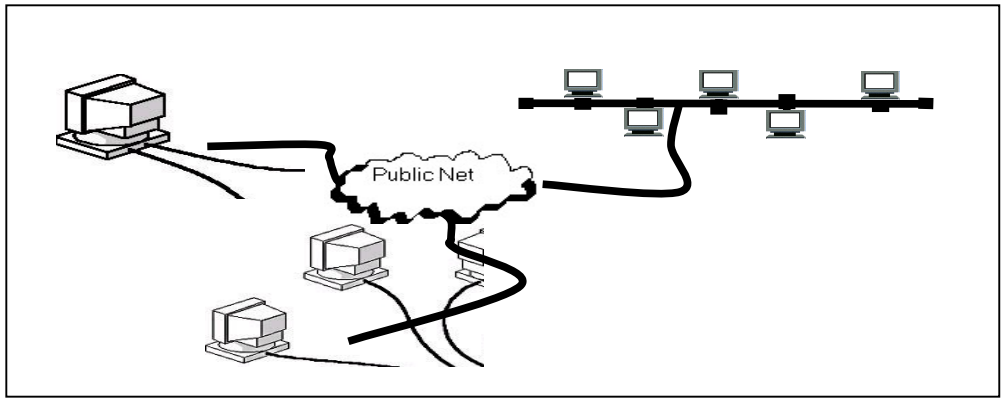
- ***Local area networks (LANs).***
- ***Metropolitan area networks (MANs).***
- ***Wide area networks (WANs).***

❖ Local Area Network (LAN)

A local area network is usually privately owned and links the devices in a single office building, or campus. Depending on the needs of an organization and the type of technology used. A LAN can be as simple as two PCs and a printer in someone's home office or it can extend throughout a company and include voice, sound, and video peripherals. Currently, LAN size ***is limited to a few Kilometers.***

❖ Metropolitan Area Network (MAN)

A metropolitan area network is designed to ***extend over*** an entire city. It may be a single network such as a cable television network or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device. For example, a company can use a MAN to connect the LANs in all of its offices throughout a city.



A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company.

❖ Wide Area Network (WAN)

A wide area network provides ***long-distance*** transmission of data; voice, image, and video information over large geographical areas that may comprise a country, a continent, or even the whole world. In contrast to LANs (which depend on their own hardware for transmission), WANs may utilize public, leased, or private communication devices, usually in combinations, and can therefore span an unlimited number of miles. A WAN that is wholly owned and used by a single company is often referred to as an *enterprise network*.

(B) <u>According to the physical architecture (center of control)</u>

❖ Centralized Networks

A central computer "Mini computer or Mainframe" that manages all communication and requests in the network.

- **Distributed Network**

  A group of Personal Computers (PC's) works together and share the same input / output devices.
- **Hybrid Network**

  A combination of centralized and distributed networks

(C) According to the ownership

- **Public Network**

  On a network that is owned, managed, and operated by a public company.
- **Private Network**

  Owned and managed by a private organization

(D) According to transmission technology

- **Broadcasting Network**

  It does not restrict or determine a specified destination. It has a single communication channel that is shared by all the machines on the network. Short messages, called packets sent by any machine are received by all the others. Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field.

- **Point to Point Network**

  Data or packets are sent to a specify destination which is able to reflect an each of the receiving.

(E) According to service providing

- **Peer to Peer Network**

  Any PC connected to this network can provide services to any other PC and request for services from any.
- **Client/Server Network**

  The most popular network, the network depends on a PC act as a service Provider called the **SERVER**. The server restricts the same policy to control the determination of the client how will get the service and type of service.