



**University of Thi-Qar**  
**College of Education for Pure Science**  
**Department of Computer Science**



# **Computer Networks**

**Dr. Ali Basim Al-Khafaji**

# Introduction

- ▶ **Data communications and networking** are changing the way we do business and the way we live. Business decisions have to be made ever more quickly, and the **decision makers** require immediate access to accurate information.
- ▶ Why wait a week for that **report** from Germany to arrive by mail when it could appear almost instantaneously through computer networks? Businesses today rely on **computer networks and internetworks**. But before we ask how quickly we can get hooked up, we need to know how networks operate, what types of technologies are available, and which design best fills which set of needs.

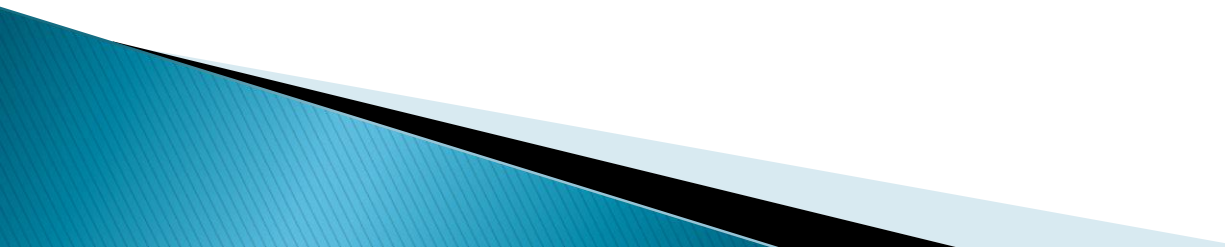
# Introduction

- ▶ The development of the personal computer brought about tremendous changes in business, industry, science, and education. A similar revolution is occurring in **data communications and networking**.
- ▶ Technological advances are making it possible for communications links to carry more and faster signals. As a result, services are evolving to allow the use of this expanded capacity. For example, established **telephone services** such as conference calling, call waiting, voice mail, and caller ID have been extended.
- ▶ Research in data communications and networking has resulted in new technologies. One goal is to be able to **exchange data** such as text, audio, and video from all points in the world. We want to access the Internet to download and upload information quickly and accurately and at any time.

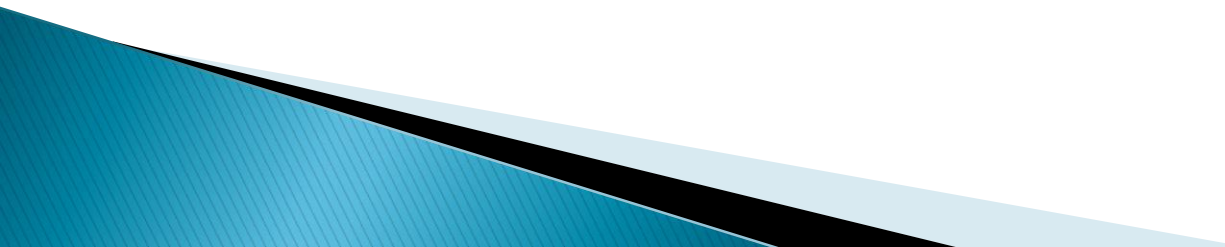
# Data Communications

- When we communicate, we are **sharing information**. This sharing can be **local or remote**. Between individuals, local communication usually occurs face to face, while remote communication takes place over a distance. The term **telecommunication** which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").
- The word **data** refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- **Data communications** are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

# Data Communications

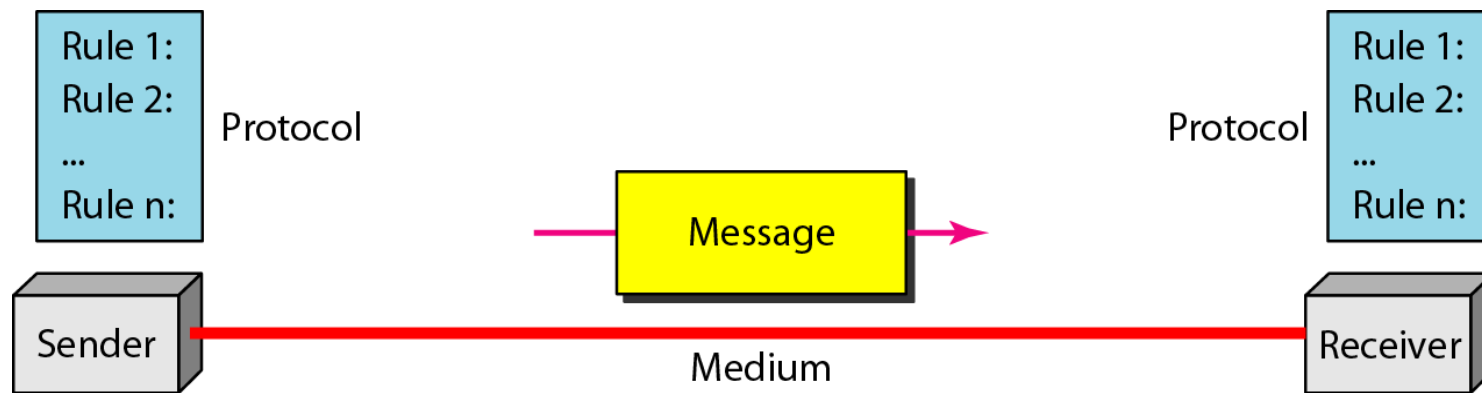
- The **effectiveness** of a data communications system depends on **four** fundamental characteristics: delivery, accuracy, timeliness, and jitter.
    1. **Delivery**. The system must deliver data to the **correct destination**. Data must be received by the intended device or user and only by that device or user.
    2. **Accuracy**. The system must deliver the **data accurately**. Data that have been altered in transmission and left uncorrected are unusable.
    3. **Timeliness**. The system must deliver data in a **timely manner**. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called **real-time transmission**.
- 

# Data Communications

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.
- 

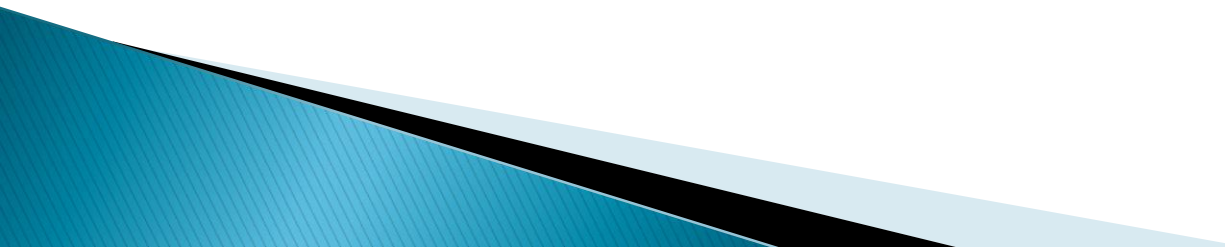
# Components

- A data communications system has five components (see Figure 1).



**Figure (1) Five components of data communication system**

# Components

1. **Message.** The message is the **information (data)** to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
  2. **Sender.** The sender is the device that **sends the data message**. It can be a computer, workstation, telephone handset, video camera, and so on.
  3. **Receiver.** The receiver is the device that **receives the message**. It can be a computer, workstation, telephone handset, television, and so on.
  4. **Transmission medium.** The transmission medium is the **physical path** by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber optic cable, and radio waves.
- 



# Components

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

# Data Representation

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

## ➤ Text

In data communications, text is represented as a **bit pattern**, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a **code**, and the process of representing symbols is called **coding**. Today, the prevalent coding system is called **Unicode**, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (**ASCII**), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

# Data Representation

## ➤ Numbers

Numbers are also represented by **bit patterns**. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

## ➤ Images

Images are also represented by **bit patterns**. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The image resolution depends on the number of the pixel. For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.

# Data Representation

- After an image is divided into **pixels**, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and-white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.
- If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include **gray scale**. For example, to show four levels of **gray scale**, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11.
- There are several methods to **represent color images**. One method is called **RGB**, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called **YCM**, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

# Data Representation

## ➤ Audio

Audio refers to the **recording or broadcasting** of sound or music. Audio is by nature different from text, numbers, or images. It is **continuous, not discrete**. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

## ➤ Video

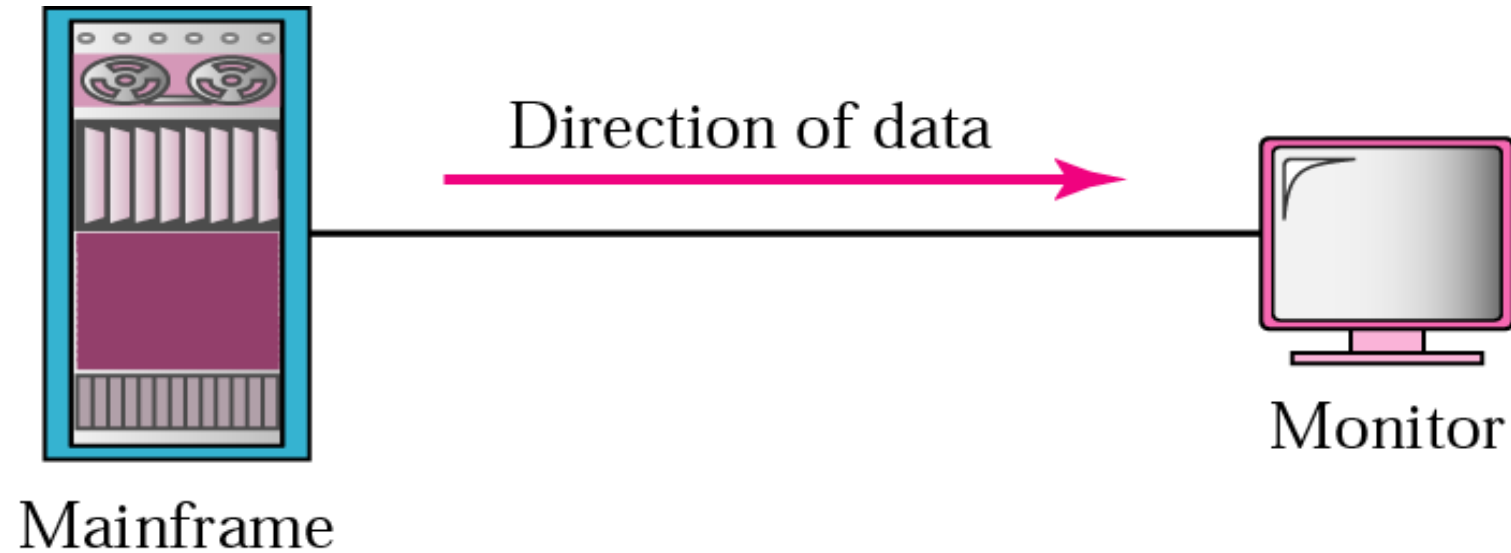
Video refers to the **recording or broadcasting** of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. We can change video to a **digital or an analog signal**.

# Data Flow

- ▶ **Communication** between two devices can be simplex, half-duplex, or full-duplex.

- ▶ **Simplex**

In simplex mode, the communication is **unidirectional**, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 2). **Keyboards and traditional monitors** are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

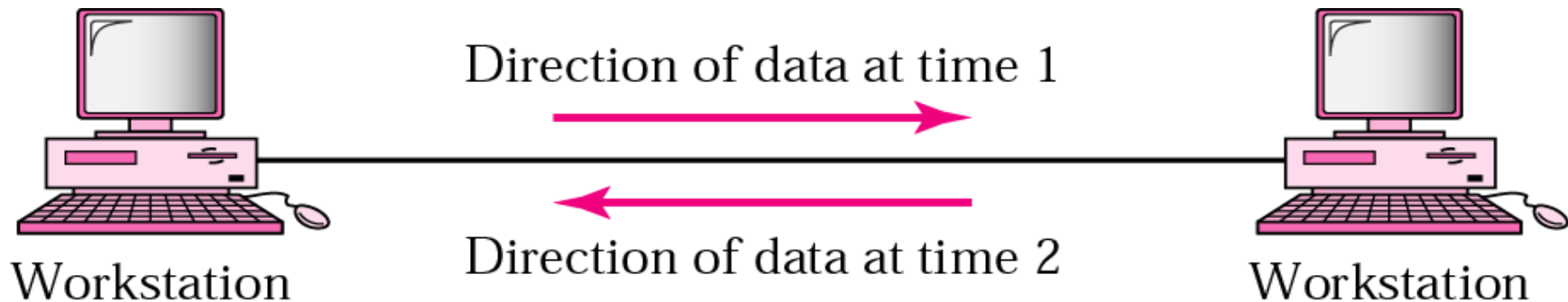


**Figure (2) Data flow (simplex)**

➤ **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 3).

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



**Figure (3) Data flow (half-duplex)**

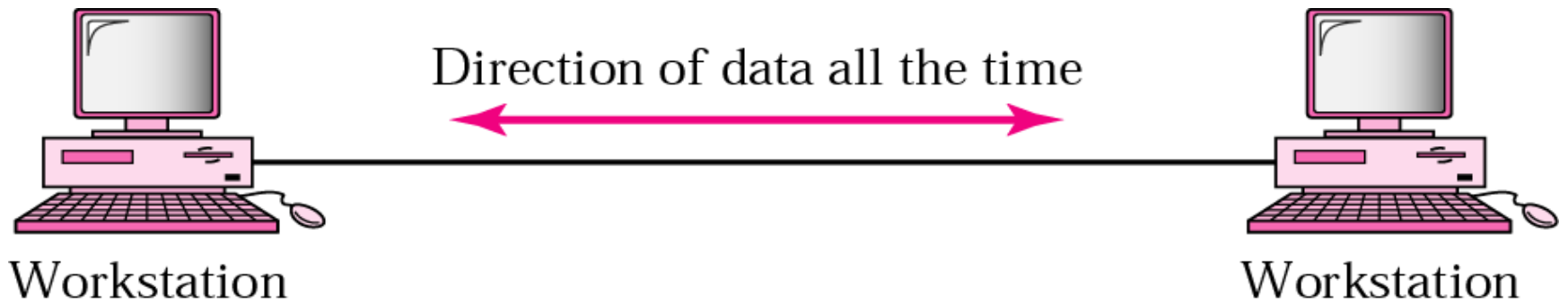


## ➤ Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive **simultaneously** (see Figure 4).

The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, **signals going in one direction share the capacity** of the link with signals going in the other direction. This **sharing can occur in two ways**: Either the link must contain two physically **separate transmission paths**, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

- One common examples of full-duplex communication is the **telephone network**. When two people are communicating by a telephone line, both can **talk and listen** at the same time. The full-duplex mode is used when communication in **both directions is required all the time**. The capacity of the channel, however, must be divided between the two directions.



**Figure (4) Data flow (full-duplex)**

# Networks

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

## Distributed Processing

- ▶ Most networks use distributed processing, in which a task is **divided** among **multiple computers**. Instead of one single large machine being responsible for all aspects of a process, **separate computers** (usually a personal computer or workstation) handle a subset.

## Networks VS Distributed Systems

- ▶ A distributed system is a **software system** built on top of a network. The software gives it a high degree of cohesiveness and transparency. Thus, the distinction between a network and a distributed system lies with the software (especially the operating system), rather than with the hardware.

- The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system.
- Often a layer of software on top of the operating system, called middleware, is responsible for implementing this model. A well-known example of a distributed system is the World Wide Web, in which everything looks like a document (Web page).
- In a computer network, this coherence, model, and software are absent. Users are exposed to the actual machines, without any attempt by the system to make the machines look and act in a coherent way. If the machines have different hardware and different operating systems, that is fully visible to the users. If a user wants to run a program on a remote machine, he has to log on to that machine and run it there.

# Network Criteria

- ▶ A network must be able to meet a certain number of criteria. The most important of these are **performance**, **reliability**, and **security**.

- ▶ **Performance**

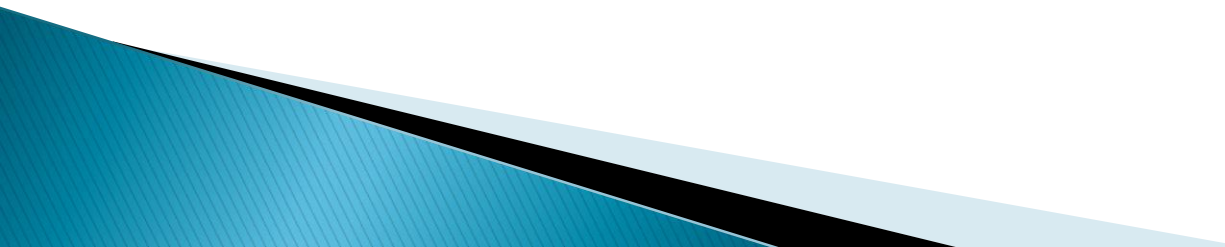
Performance can be measured in many ways, including **transmit time and response time**. Transmit time is the **amount of time required** for a message to travel from one device to another. Response time is the **elapsed time** between an inquiry and a response. Performance is often **evaluated** by two networking metrics: **throughput and delay**. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

# Network Criteria

- The performance of a network depends on a number of factors, including:
  - 1- **Number of users.** Having a large number of concurrent users can slow response time in a network not designed to coordinate heavy traffic load.
  - 2- **Type of transmission medium.** The medium defines the speed at which data can travel through a connection (the data rate). Today networks are moving to faster and faster transmission media, such as fiber optic cabling. A medium that can carry data at 100 megabits per second is ten times more powerful than a medium that can carry data at only 10 megabits per second. The speed of light imposes an upper bound on the data rate.
  - 3- **The capabilities of the connected hardware.** The type of hardware included in a network affects both the speed and capacity of transmission. A higher-speed computer with greater storage capacity provides better performance.

# Network Criteria

4- **The efficiency of the software.** The software used to process data at the sender, receiver, and intermediate nodes also affects network performance. Moving a message from node to node through a network requires processing to transform the **raw data** into transmittable signals, route these signals to the proper destination, to ensure error-free delivery, and recast the signals into a form the receiver can use. The software that provides these services affects both the speed and the reliability of a network link. Well-designed software can speed the process and make transmission more effective and efficient.



# Network Criteria

## ➤ Reliability

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

## ➤ Security

Network security issues include **protecting** data from **unauthorized access**, protecting data from **damage** and **development**, and implementing policies and procedures for **recovery** from **breaches** and **data losses**.



# Physical Structures

- Before discussing networks, we need to define some **network attributes**.

## Type of Connection

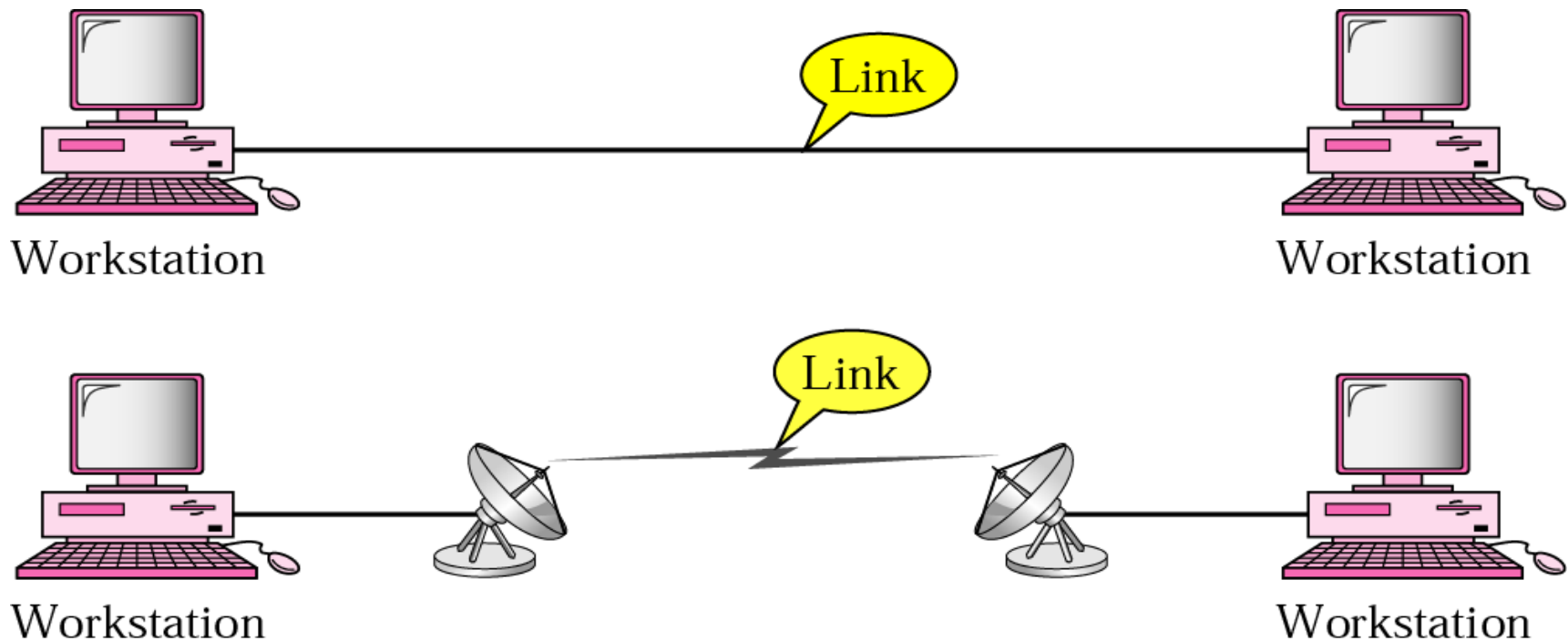
- A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time.
- There are two possible **types of connections**: point-to-point and multipoint.

- **Point-to-Point**

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections 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 (see Figure 5).

# Physical Structures

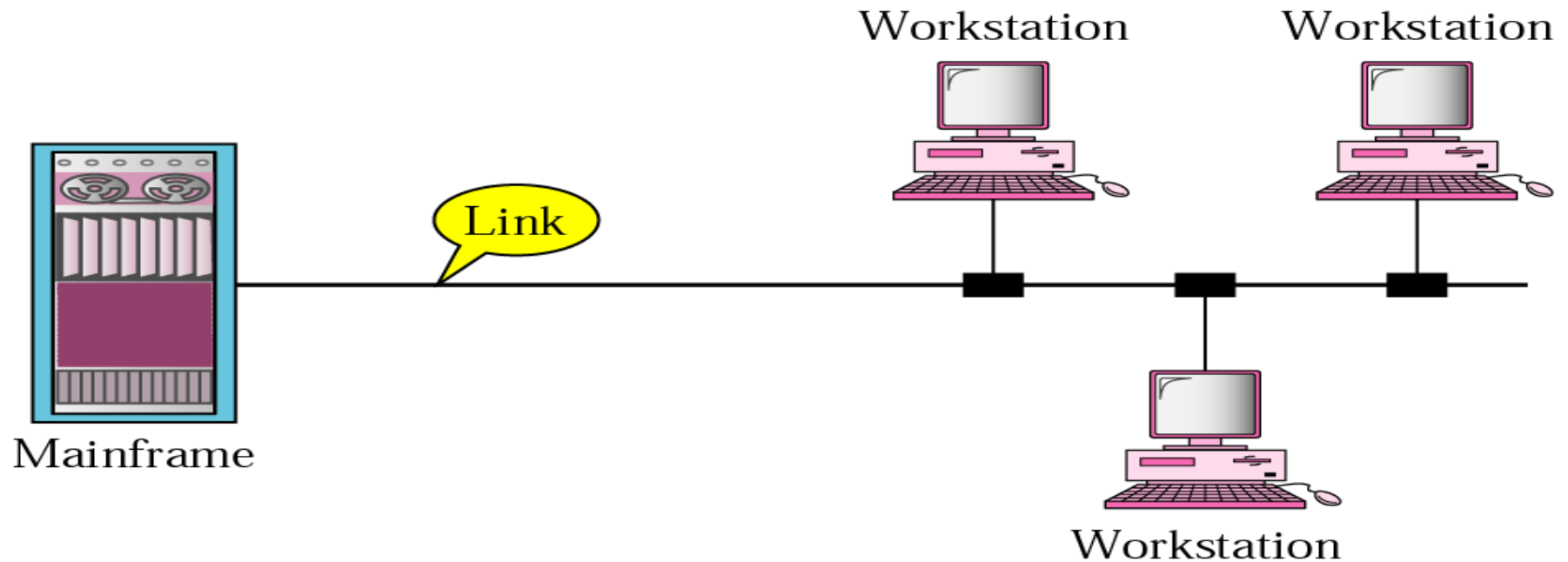
- When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.



**Figure (5) Point-to-point connection**

# Physical Structures

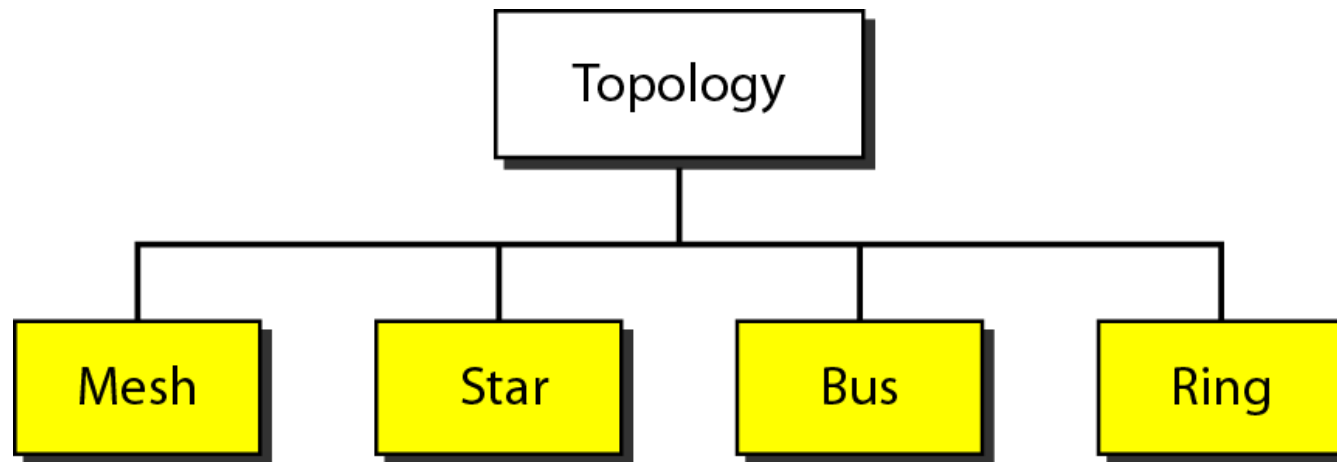
- **Multipoint:** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 6). In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



**Figure (6) Multipoint connection**

# Physical Topology

- ▶ The term physical topology refers to the way in which a network is laid out physically. 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 (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring (see Figure 7).



**Figure (7) Categories of topology**

# Physical Topology

- ▶ The **selecting of the topology** is depends on some **factors** :
  - 1- Type and number of devices we are planning to use.
  - 2- The application and data transmission rate.
  - 3- The required response time.
  - 4- The cost.

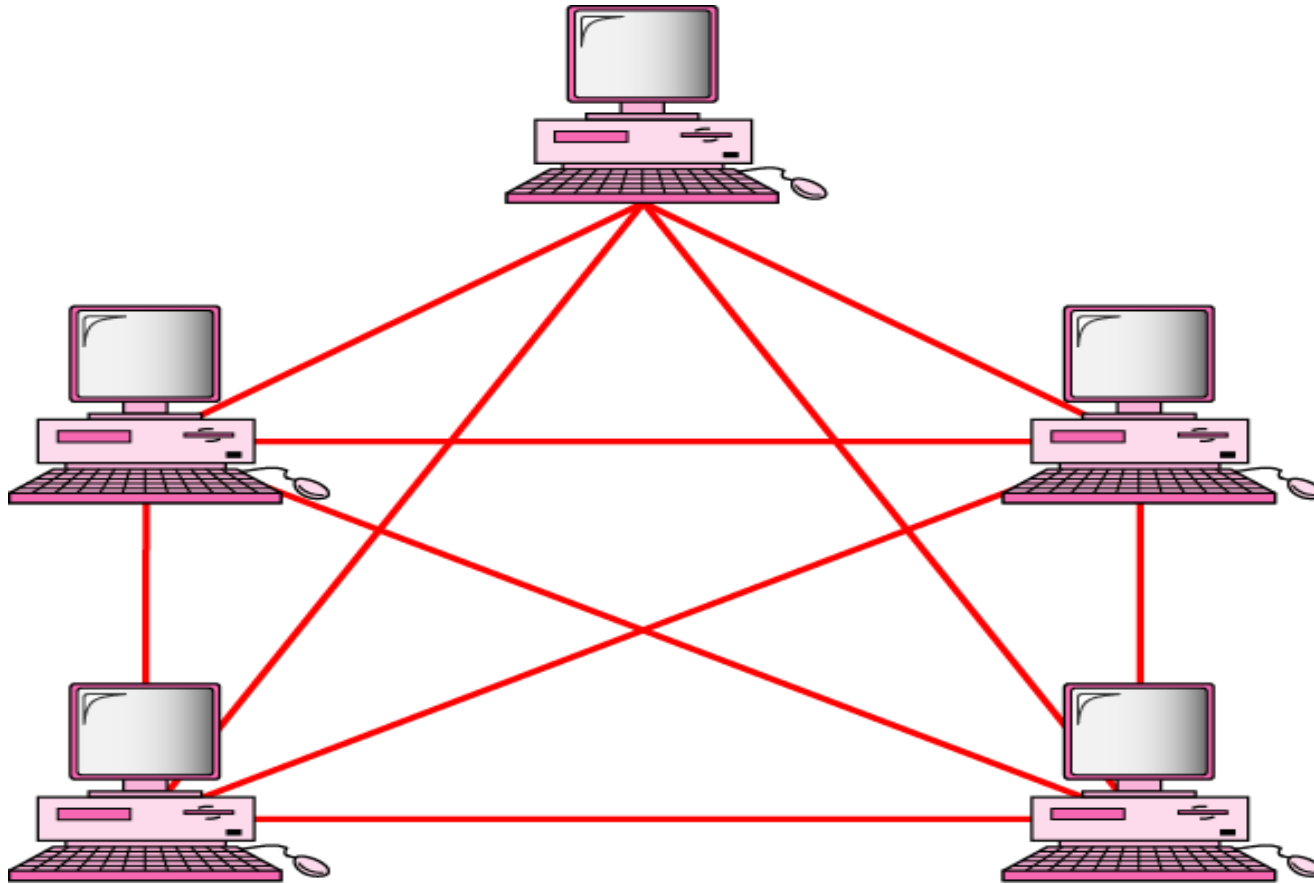
## Mesh Topology

- ▶ 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. To find the number of physical links in a fully connected mesh network with  $n$  nodes, we first consider that each node must be connected to every other node. Node1 must be connected to  $n-1$  nodes, node2 must be connected to  $n-1$  nodes, and finally node  $n$  must be connected to  $n-1$  nodes.

# Mesh Topology

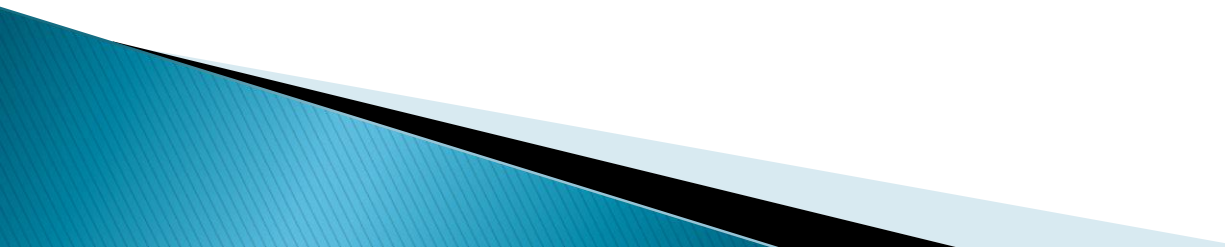
- ▶ We need  $n(n-1)$  physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need  $n(n-1) / 2$  duplex-mode links.
- ▶ To accommodate that many links, every device on the network must have  $n-1$  input/output (I/O) ports (see Figure 8) to be connected to the other  $n-1$  stations.
- ▶ **Numbers of cables and hosts**  
Number of cables:  $n(n-1) / 2$   
Number of ports:  $n(n-1)$        $n$ : number of hosts

# Mesh Topology



**Figure (8) A fully connected mesh topology (five devices)**

## Advantages:

- A mesh offers several advantages over other network topologies:
    - First**, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
    - Second**, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
    - Third**, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
    - Finally**, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.
- 



## Disadvantages:

- The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

**First**, because every device must be connected to every other device, installation and reconnection are difficult.

**Second**, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

**Finally**, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies. One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

# Star Topology

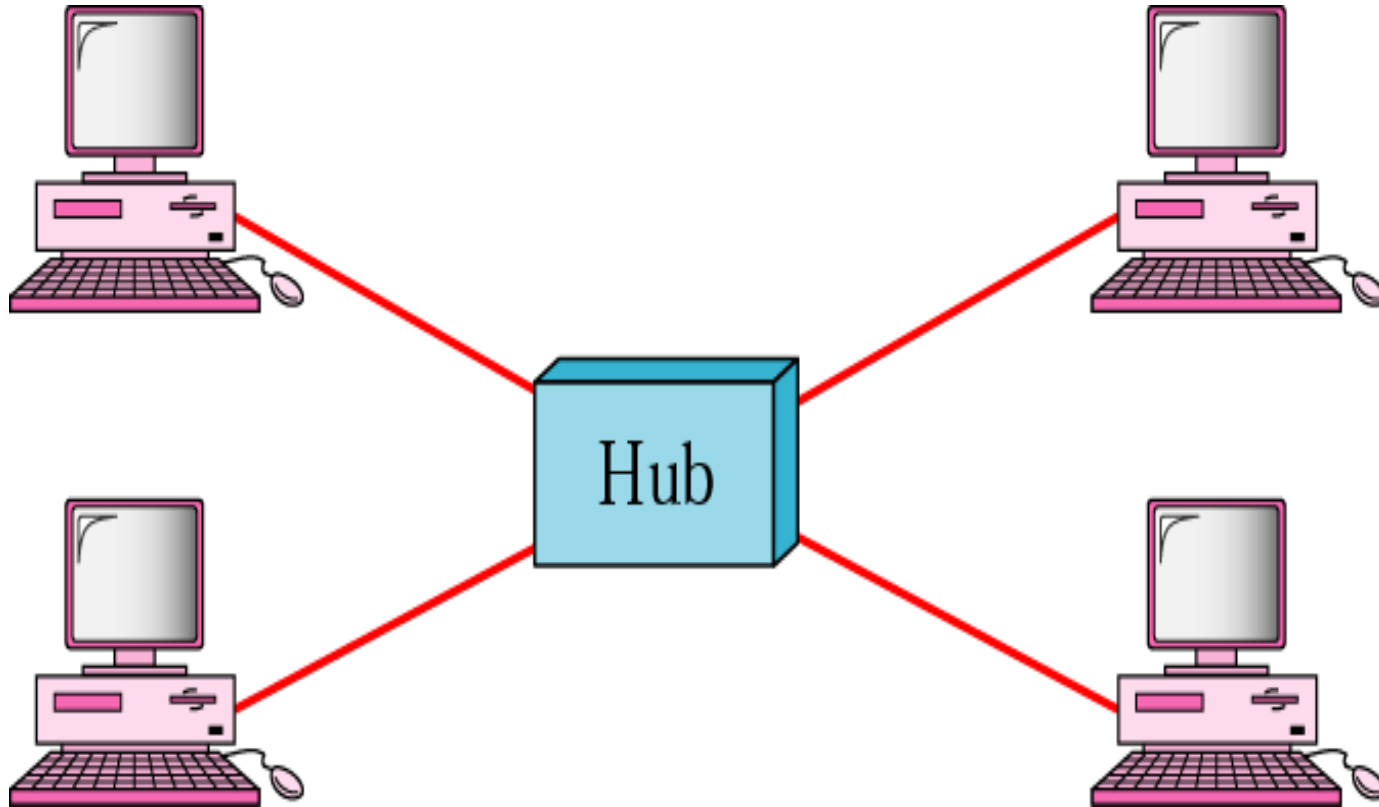
- ▶ In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 9).

- ▶ **Numbers of cables and hosts**

Number of cables:  $1 \times n$

Number of ports:  $1 \times n$        $n$ : number of hosts

# Star Topology



**Figure (9) A star topology connecting four stations**

## Advantages:

- A **star topology** is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it **easy to install and reconfigure**. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection between that device and the hub. Other advantages include **robustness**. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to 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.

## Disadvantages:

- **One big disadvantage** of a star topology is the dependency of the whole topology on **one single point**, the hub. If the hub goes down, the whole system is dead. Although **a star requires far less cable than a mesh**, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as **ring or bus**). The star topology is used in local-area networks (LANs). High-speed LANs often use a star topology with a central hub.

**Example:** Assume we have 5 hosts in mesh and star topologies. What the numbers of cables and ports are needed?

**For Mesh Topology:**

Number of cables:  $n(n - 1) / 2$

$$5(5 - 1) / 2 = 10 \text{ cables}$$

Number of ports:  $n(n - 1)$

$$5(5 - 1) = 20 \text{ ports}$$

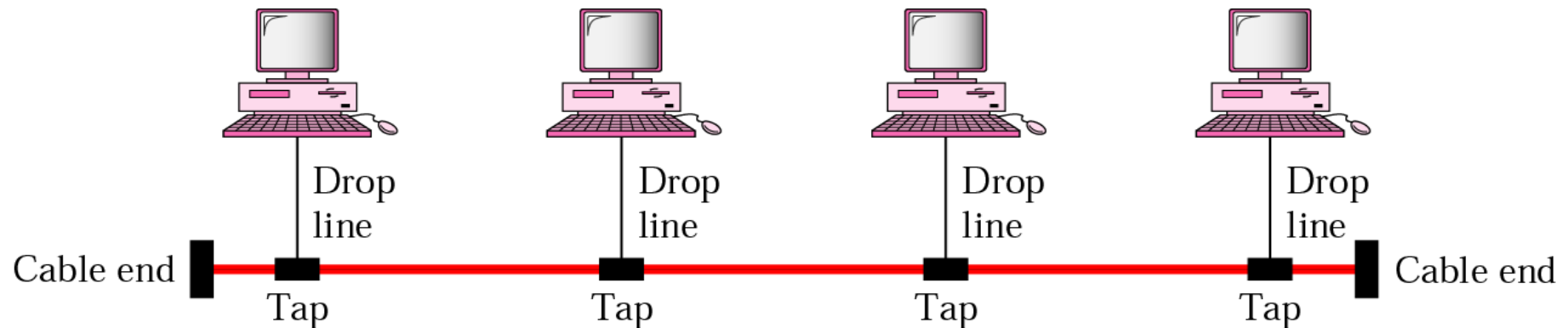
**For Star Topology:**

Number of cables:  $1 \times n = 5 \text{ cables}$

Number of ports:  $1 \times n = 5 \text{ ports}$

# Bus Topology

- ▶ The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is **multi-point**. One long cable acts as a backbone to link all the devices in a network (see Figure 10).



**Figure (10) A bus topology connecting four stations**

- ▶ Nodes are connected to the bus cable by **drop lines and taps**. A drop line is a connection running between the **device and the main cable**. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

## Advantages:

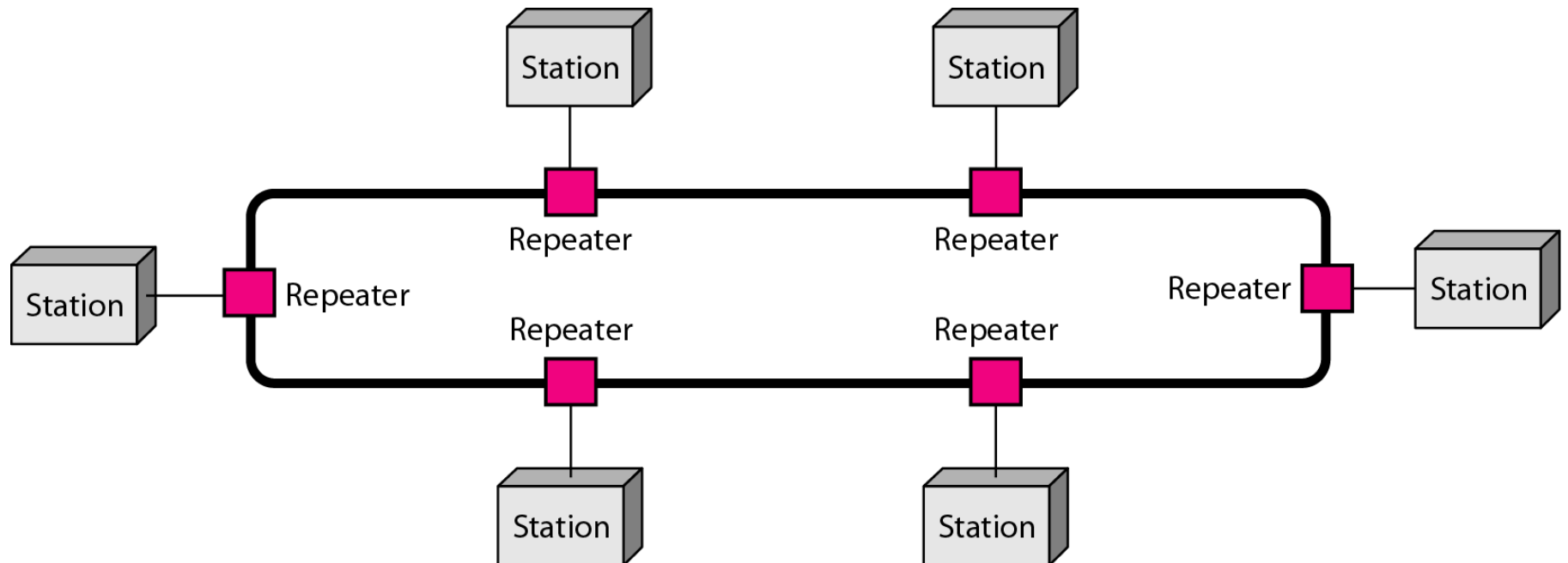
- Advantages of a bus topology include **ease of installation**. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, **a bus uses less cabling than mesh or star topologies**. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. **In a bus, this redundancy is eliminated**. Only the backbone cable stretches through the entire facility. Each **drop line** has to reach only as far as the nearest point on the backbone.

## Disadvantages:

- Disadvantages include **difficult reconnection and fault isolation**. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to **add new devices**. **Signal reflection** at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. 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** connection with only 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 (see Figure 11).



**Figure (11) A ring topology connecting six stations**



## Advantages:

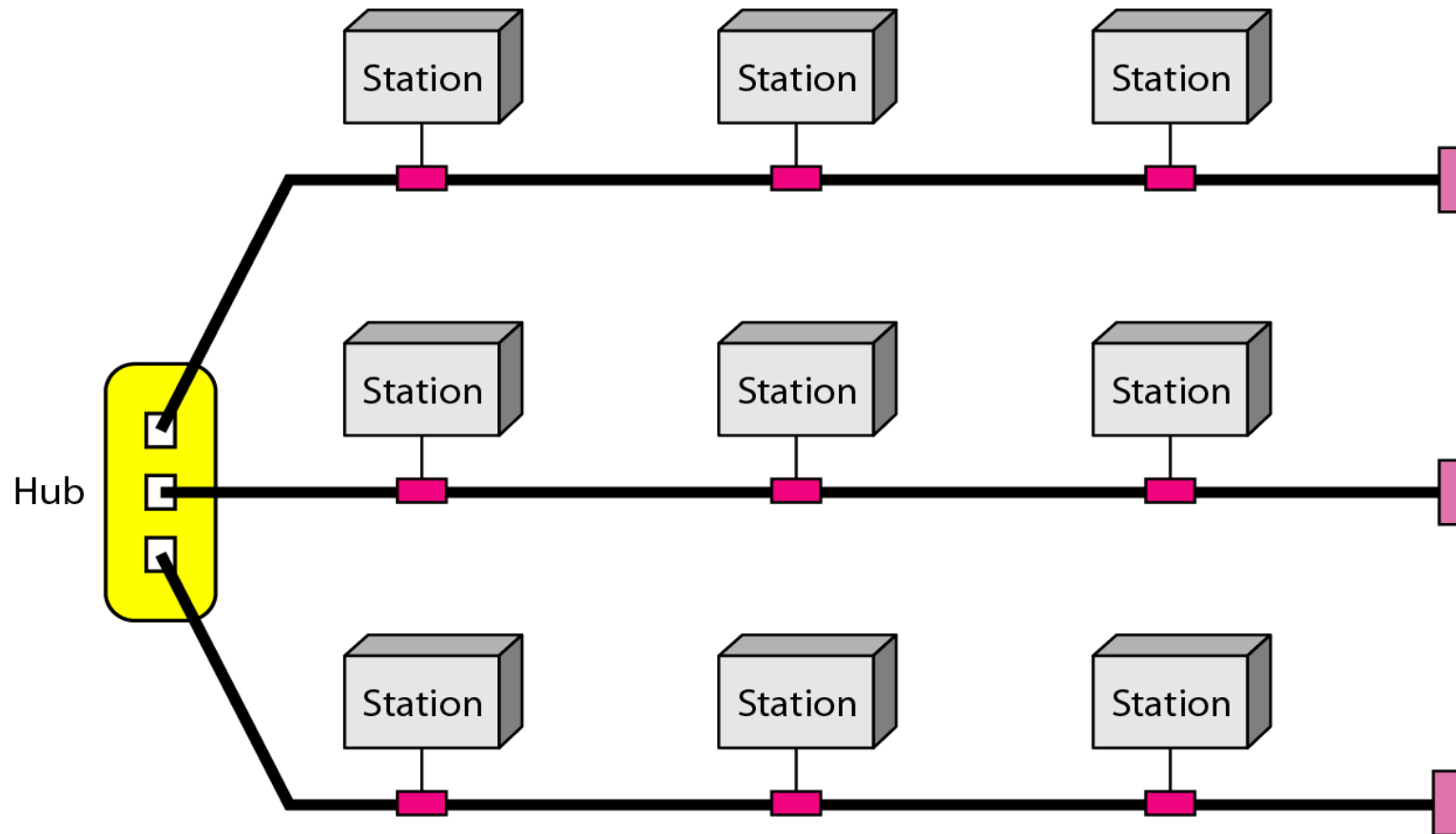
- A ring is relatively easy to **install and reconfigure**. Each device is linked to only its **immediate neighbors**. To **add or delete** a device requires changing only two connections. The only constraints are media and traffic considerations (**maximum ring length and number of devices**). In addition, fault isolation is simplified.
- Generally in a ring, a signal is **circulating** at all times. If one device does not receive a signal within a specified period, **it can issue an alarm**. The alarm alerts the **network operator** to the problem and its location.

## Disadvantages:

- **Unidirectional traffic** can be a disadvantage. In a simple ring, a break in the ring (**such as a disabled station**) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

# Hybrid Topology

- ▶ A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure (12).



**Figure (12) A hybrid topology: a star backbone with three bus networks**

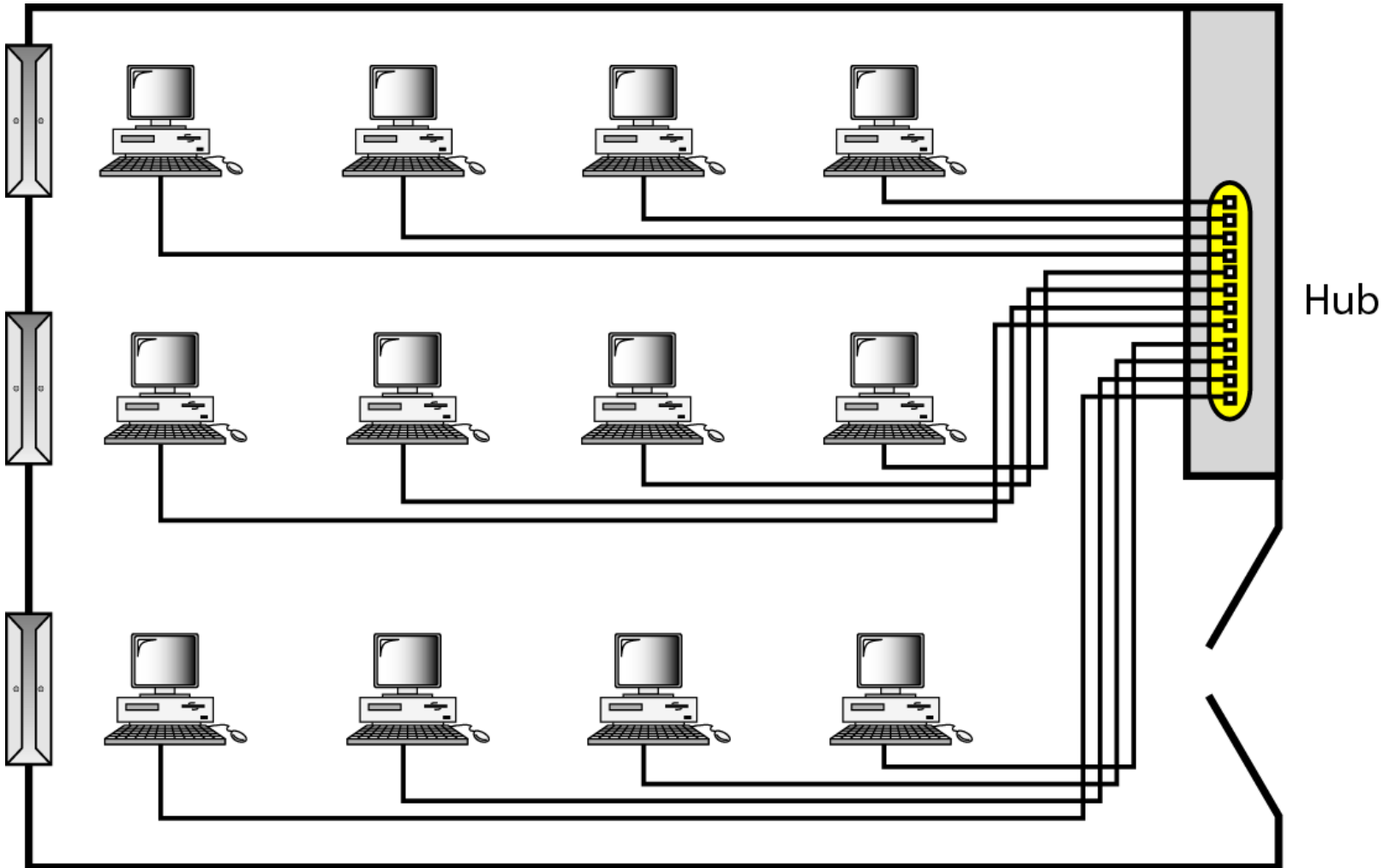
# Categories of Networks

- Today when we speak of networks, we are generally referring to two primary categories: **local-area networks** and **wide-area networks**. The category into which a network falls is determined by its size. A LAN normally covers an area less than 2 mile; a WAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.

## Local Area Network

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus (see Figure 13). 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 audio and video peripherals. Currently, LAN size is limited to a few kilometers.

# Local Area Network



**Figure (13) An isolated LAN connecting 12 computers to a hub in a closet**

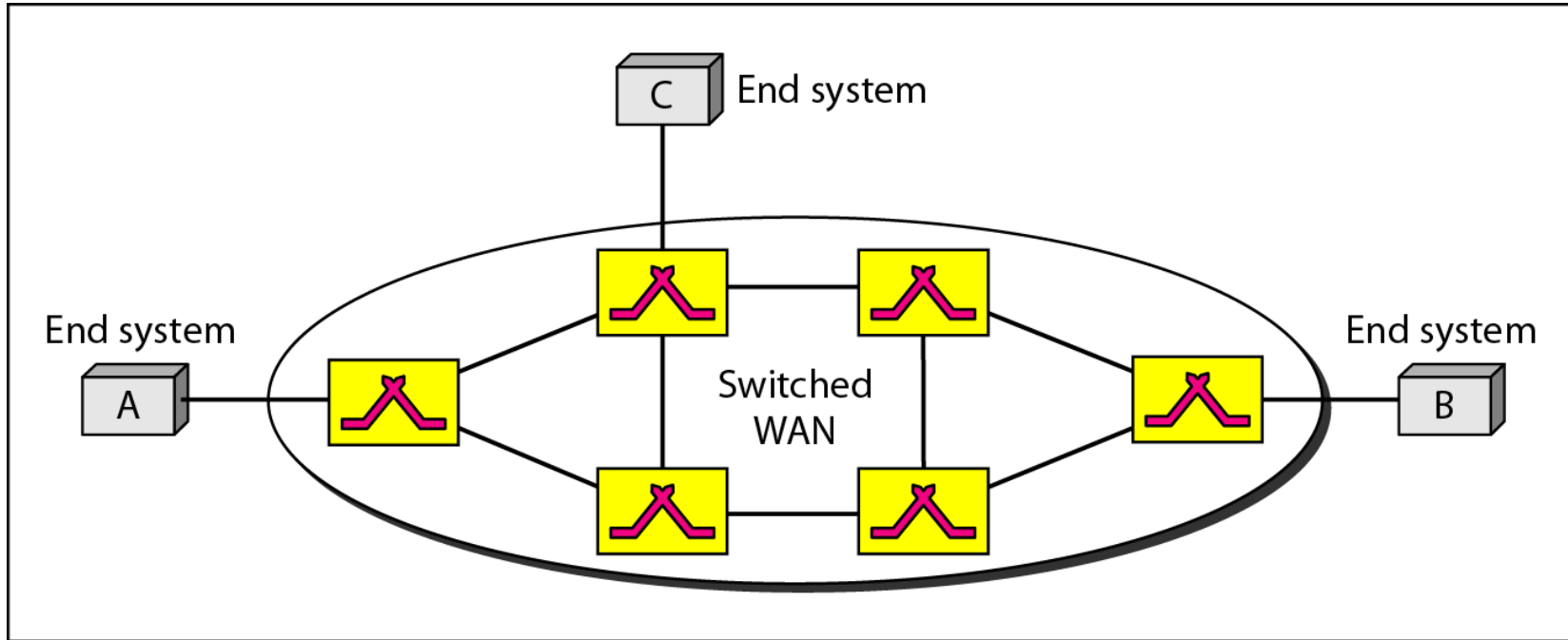
# Local Area Network

- LANs are designed to allow **resources** to be **shared** between personal computers or workstations. The resources to be shared can include **hardware** (e.g., a printer), **software** (e.g., an application program), or **data**. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, **for example, engineering workstations or accounting PCs**. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this **central server** and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.
- In addition to size, LANs are distinguished from other types of networks by their **transmission media and topology**. In general, a given LAN will use only one type of transmission medium. **The most common LAN topologies are bus, ring, and star**. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

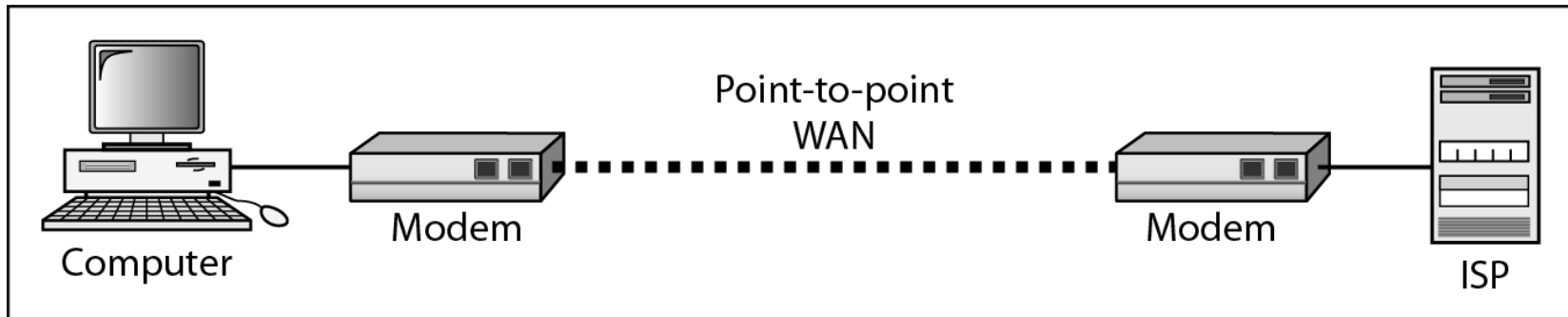
# Wide Area Network

- A wide area network (WAN) provides **long-distance transmission** of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet.
- We normally refer to the first as a **switched WAN** and to the second as a **point-to-point WAN** (Figure 14). **The switched WAN** connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. **The point-to-point WAN** is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often used to provide Internet access.

# Wide Area Network



a. Switched WAN

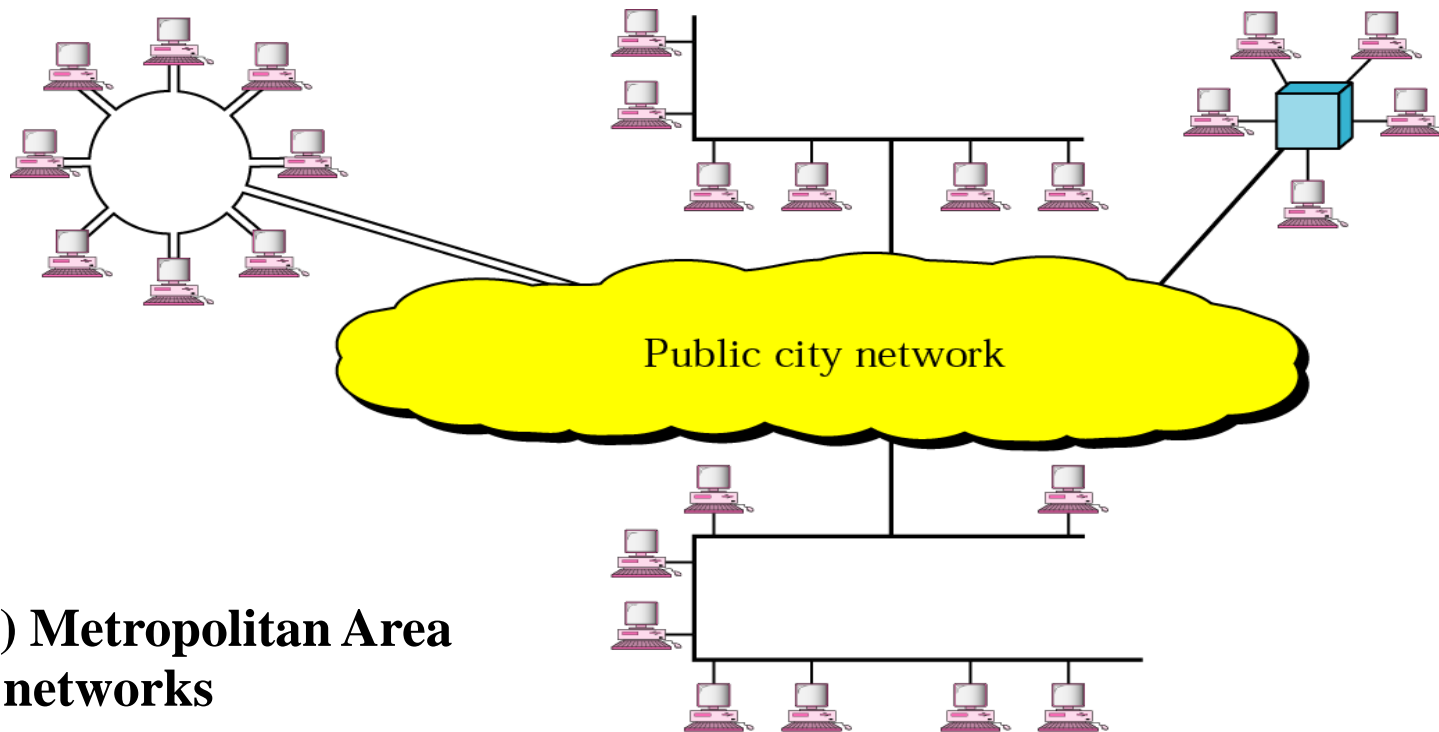


b. Point-to-point WAN

**Figure (14) WANs: a switched WAN and a point-to-point WAN**

# Metropolitan Area Networks

- A metropolitan area network (MAN) is a network with a size between a **LAN and a WAN**. It normally covers the area inside a town or a city. It is designed for customers who need a **high-speed connectivity**, normally to the Internet, and have endpoints spread over a city or part of city.
- A **good example** of a MAN is the part of the telephone company network that can provide a high-speed DSL line (Digital Subscriber Line) to the customer.



**Figure (15) Metropolitan Area networks**



# Interconnection of Networks: Internetwork

- ▶ Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become an **internetwork**, or internet.
- ▶ As **an example**, assume that an **organization** has **two offices**, one on the **east coast** and the other on the **west coast**. The established **office** on the **west coast** has a **bus topology LAN**; the newly opened **office** on the **east coast** has a **star topology LAN**. The **president** of the **company** lives somewhere in the **middle** and needs to have **control** over the company from her home. To create a **backbone WAN** for connecting these **three entities** (two LANs and the president's computer), a **switched WAN** (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modem line offered by a cable TV provider as shown in Figure (16).

# Interconnection of Networks: Internetwork

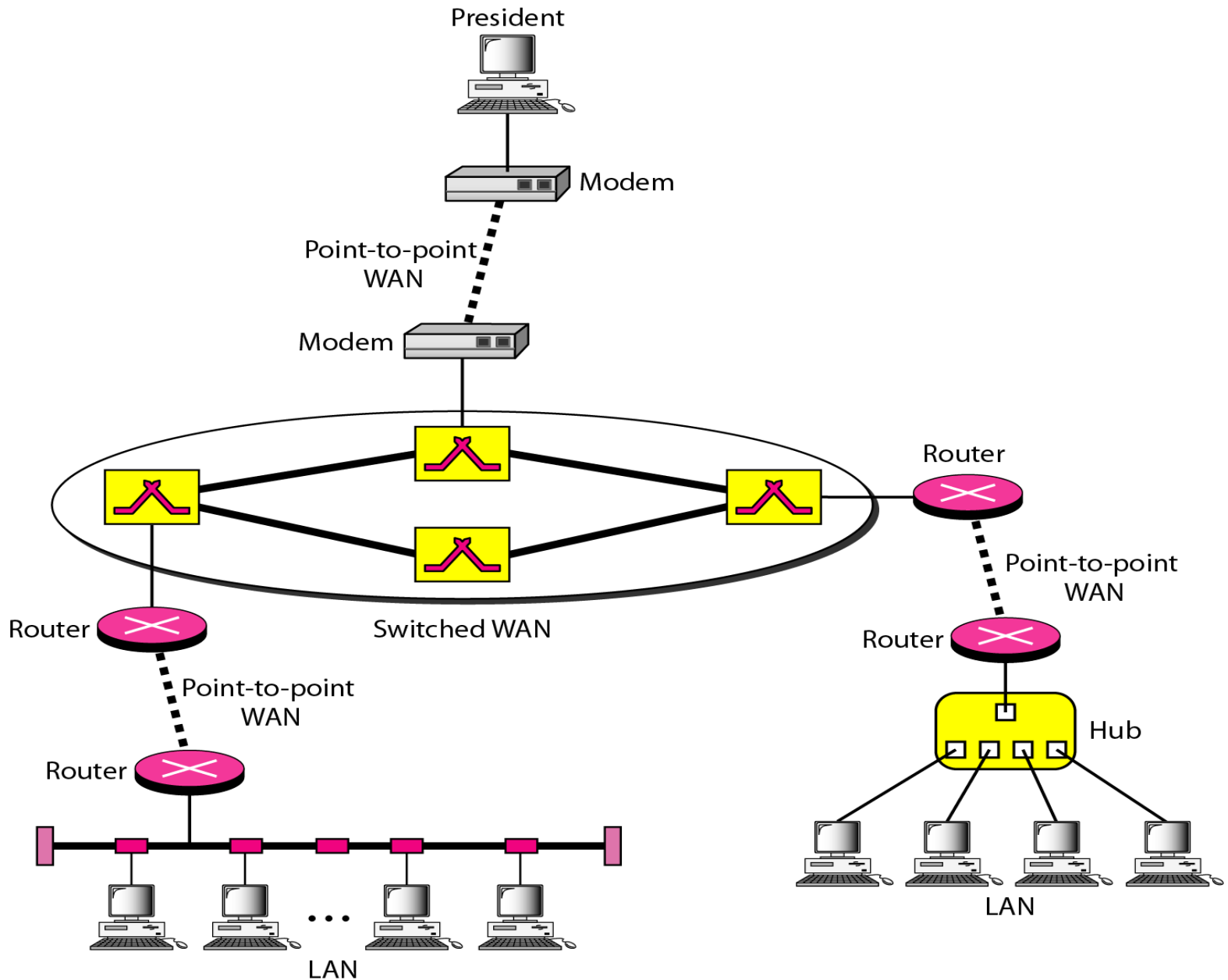


Figure (16) A heterogeneous network made of four WANs and two LANs

# THE INTERNET

- ▶ The **Internet** has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The **Internet** is a structured, organized communication system that has brought a wealth of information to our fingertips and organized it for our use.
- ▶ A **network** is a group of connected communicating devices such as computers and printers. An **internet** (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than **hundreds of thousands of interconnected networks**. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in **1969**.

# THE INTERNET

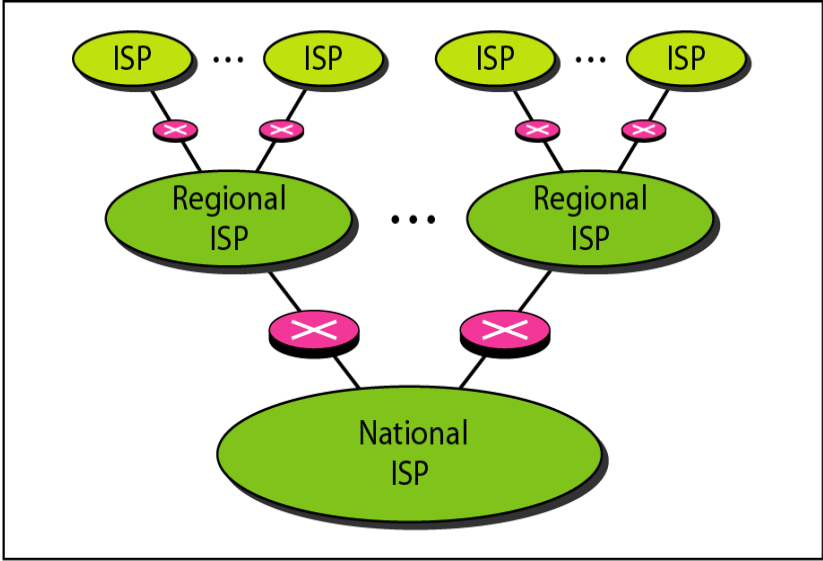
- ▶ In the **mid-1960s**, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another. The **Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD)** was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.
- ▶ In **1967**, at an Association for **Computing Machinery (ACM)** meeting, ARPA presented its ideas for **ARPANET**, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an **interface message processor (IMP)**. The IMPs, in turn, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

# THE INTERNET

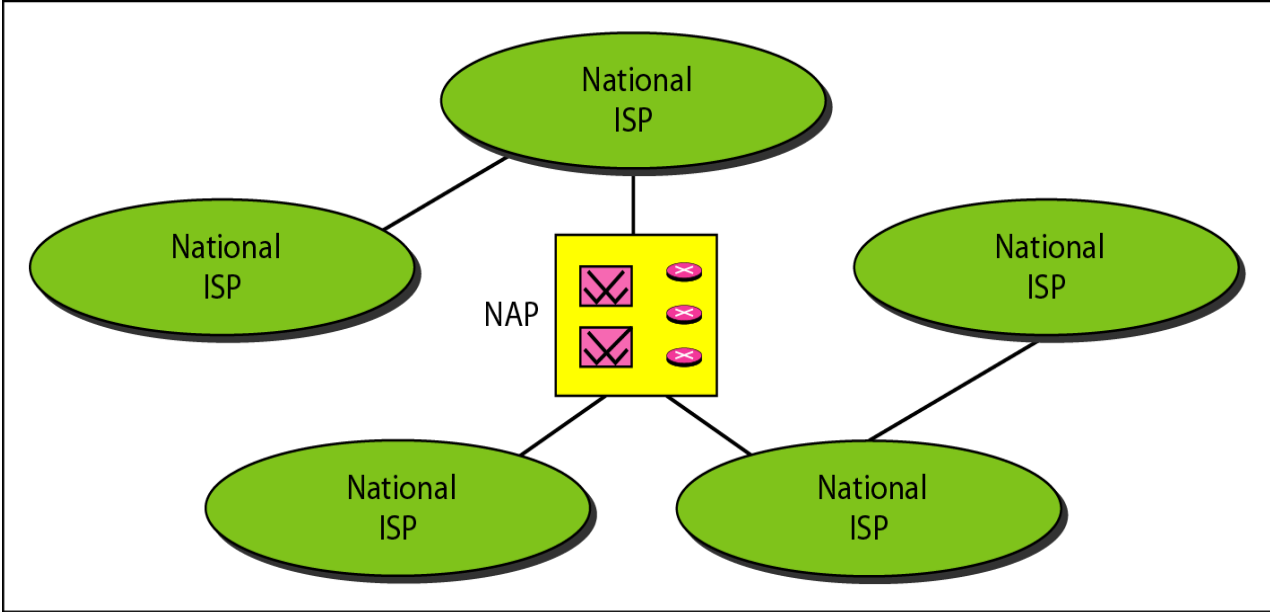
- ▶ By 1969, **ARPANET** was a reality. **Four nodes**, at the University of California at **Los Angeles** (UCLA), the University of California at **Santa Barbara** (UCSB), **Stanford Research Institute** (SRI), and the University of **Utah**, were connected via the IMPs to form a network. Software called the **Network Control Protocol (NCP)** provided communication between the hosts.
- ▶ In **1972**, **Vint Cerf and Bob Kahn**, both of whom were part of the core **ARPANET group**, collaborated on what they called the Internetting Project. Cerf and Kahn's landmark **1973** paper outlined the protocols to achieve **end-to-end delivery of packets**. This paper on **Transmission Control Protocol (TCP)** included concepts such as **encapsulation**, the **datagram**, and the **functions of a gateway**.
- ▶ Shortly thereafter, authorities made a decision to split **TCP** into two protocols: **Transmission Control Protocol (TCP)** and **Internetworking Protocol (IP)**. IP would **handle datagram routing** while TCP would be responsible for **higher-level functions** such as **segmentation, reassembly, and error detection**. The internetworking protocol became known as **TCP/IP**.

# THE INTERNET

- ▶ The **Internet** has come a long way since the **1960s**. The Internet today is not a simple **hierarchical structure**. It is made up of many wide- and local-area networks joined by connecting devices and switching stations.
- ▶ It is **difficult** to give an **accurate representation** of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.
- ▶ Today most end users who want Internet connection use the services of Internet service providers (ISPs). There are **international service providers, national service providers, regional service providers, and local service providers**. The Internet today is run by private companies, not the government. Figure (17) shows a conceptual (not geographic) view of the Internet.
- ▶ The term **intranet** is often used to refer to a **private connection** of LANs and WANs that belongs to an organization, and is designed to be accessible only by the **organization's members**, employees, or others with authorization.



a. Structure of a national ISP



b. Interconnection of national ISPs

**NAP=network access points**

**Figure (17) Hierarchical organization of the Internet**

# THE INTERNET

- ▶ **International Internet Service Providers**

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

- ▶ **National Internet Service Providers**

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



# THE INTERNET

## ▶ Regional Internet Service Providers

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

## ▶ Local Internet Service Providers

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

# PROTOCOLS AND STANDARDS

## ➤ **Protocols**

In computer networks, **communication** occurs between entities in different systems. An **entity** is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A **protocol is a set of rules** that govern data communications. A protocol defines **what** is communicated, **how** it is communicated, and **when** it is communicated. **The key elements** of a protocol are syntax, semantics, and timing.

- **Syntax.** The term syntax refers to the **structure or format** of the data, meaning the **order** in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- **Semantics.** The word **semantics** refers to the **meaning of each section** of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

# PROTOCOLS AND STANDARDS

- **Timing.** The term **timing** refers to **two characteristics**: when **data** should be **sent** and **how fast** they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.
- **Standards**  
Standards are essential in **creating and maintaining** an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories: **de facto** (meaning "by fact" or "by convention") and **de jure** (meaning "by law" or "by regulation").

## Standards

**De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

**De jure.** Those standards that have been legislated by an officially recognized body are de jure standards.

# Standards Organizations

- Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

## Standards Creation Committees

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

- 1- **International Organization for Standardization (ISO)**. The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
- 2- **International Telecommunication Union-Telecommunication Standards Sector (ITU-T)**. By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT).

# Standards Organizations

- 3- **American National Standards Institute (ANSI)**. Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.
- 4- **Institute of Electrical and Electronics Engineers (IEEE)**. The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.

# Standards Organizations

- 5- **Electronic Industries Association (EIA)**. Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.