Tikrit University

COLLAGE OF COMPUTER SCIENCE AND MATHEMATICS

Computer Networking

HISTORY & INTRODUCTION OF NETWORK

4th stage

Lecturer 1

Majid Hamid Ali

2024- 2023

1- A BRIEF HISTORY OF NETWORK

1. ARPANET

In the mid-1960s, mainframe computers in research organizations were stand-alone 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 together 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.

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.

2. Birth of the Internet

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. They wanted to link different networks together so that a host on one network could communicate with a host on a second, different network. There were many problems to overcome: diverse packet sizes, diverse interfaces, and diverse transmission rates, as well as differing reliability requirements. Cerf and Kahn devised the idea of a device called a gateway to serve as the intermediary hardware to transfer data from one network to another.

3. Transmission Control Protocol/Internetworking Protocol (TCP/IP)

Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of data. This was a new version of NCP. This paper on transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. A radical idea was the transfer of responsibility for error correction from the IMP to the host machine. This ARPA Internet now became the focus of the communication effort. Around this time responsibility for the ARPANET was handed over to the Defense Communication Agency (DCA).

In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication between networks was now possible.

Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The new combination became known as TCP/IP.

In 1981, under a DARPA contract, UC Berkeley modified the UNIX operating system to include TCP/IP. This inclusion of network software along with a popular operating system did much for the popularity of networking. The open (non-manufacturerspecific) implementation on Berkeley UNIX gave every manufacturer a working code base on which they could build their products.

In 1983, authorities abolished the original ARPANET protocols, and TCP/IP became the official protocol for the ARPANET. Those who wanted to use the Internet to access a computer on a different network had to be running TCP/IP.

4. MILNET

In 1983, ARPANET split into two networks: MILNET for military users and ARPANET for nonmilitary users.

5. CSNET

Another milestone in Internet history was the creation of CSNET in 1981. CSNET was a network sponsored by the National Science Foundation (NSF). The network was conceived by universities that were ineligible to join ARPANET due to an absence of defense ties to DARPA. CSNET was a less expensive network; there were no redundant links and the transmission rate was slower. It featured connections to ARPANET and Telenet, the first commercial packet data service.

6. NSFNET

With the success of CSNET, the NSF, in 1986, sponsored NSFNET, a backbone that connected five supercomputer centers located throughout the United States. Community networks were allowed access to this backbone, a T-1 line with a 1.544-Mbps data rate, thus providing connectivity throughout the United States.

In 1990, ARPANET was officially retired and replaced by NSFNET. In 1995, NSFNET reverted back to its original concept of a research network.

7. ANSNET

In 1991, the U.S. government decided that NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and MCI, filled the void by forming a nonprofit organization called Advanced Network and Services (ANS) to build a new, high-speed Internet backbone called ANSNET.

8. World Wide Web

The 1990s saw the explosion of the Internet applications due to the emergence of the World Wide Web (WWW). The web was invented at CERN by Tim Berners-Lee. This invention has added the commercial applications to the Internet.

Time Line

The following is a list of important Internet events in chronological order:

- **1969.** Four-node ARPANET established.
- **1970.** ARPA hosts implement NCP.
- **1973.** Development of TCP/IP suite begins.
- **1977.** An internet tested using TCP/IP.
- **1978.** UNIX distributed to academic/research sites.
- **1981.** CSNET established.
- **1983.** TCP/IP becomes the official protocol for ARPANET.
- **1983.** MILNET was born.
- **1986.** NSFNET established.
- **1990.** ARPANET decommissioned and replaced by NSFNET.
- **1995.** NSFNET goes back to being a research network.
- **1995.** Companies known as **Internet Service Providers (ISPs)** started.

2- NETWORKS

A **network** is the interconnection of a set of devices capable of communication. In this definition, a device can be a **host** (or an *end system* as it is sometimes called) such as a large computer, desktop, laptop, workstation, cellular phone, or security system. A device in this definition can also be a **connecting device** such as a router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on. These devices in a network are connected using wired or wireless transmission media such as cable or air. When we connect two computers at home using a plug-and-play router, we have created a network, although very small.

3- USES OF COMPUTER NETWORKS

- **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model:** Computer networking is used in the server-client model. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
- **E-commerce**: Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

4- Features Of Computer network

A list Of Computer network features is given below.

1. Communication speed

Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.

2. File sharing

File sharing is one of the major advantages of the computer network. Computer network provides us to share the files with each other.

3. Back up and Roll back is easy

Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

4. Software and Hardware sharing

We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

5. Security

Network allows the security by ensuring that the user has the right to access the certain files and applications.

6. Scalability

Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But, it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.

7. Reliability

Computer network can use the alternative source for the data communication in case of any hardware failure.

5- Network Criteria

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

1. 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, including the number of users, the type of transmission medium, the

capabilities of the connected hardware, and the efficiency of the software. 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.

2. 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.

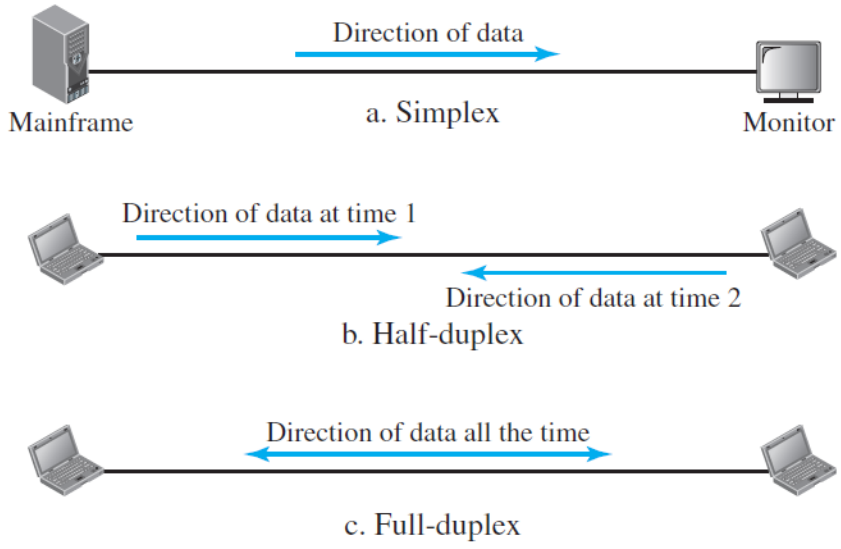
3. Security

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.

6- Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 2.

Figure 1.2 *Data flow (simplex, half-duplex, and full-duplex)*



1. 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. 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.

2. 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. 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.

3. Full-Duplex

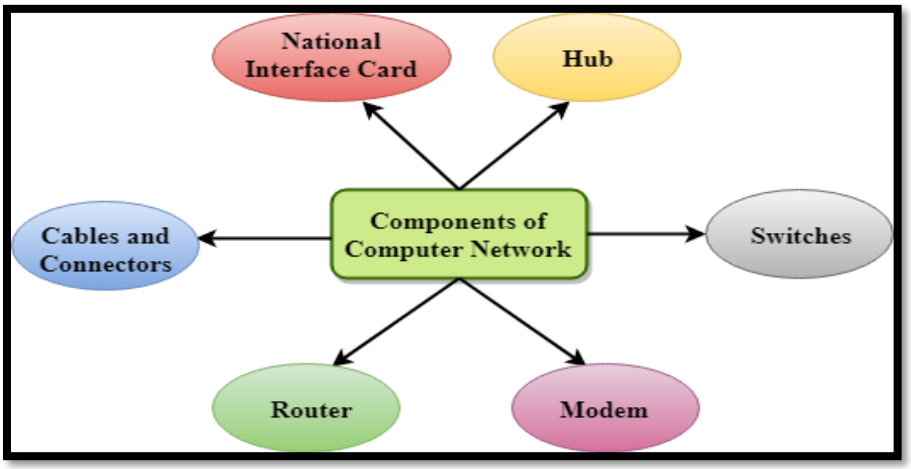
In **full-duplex mode** (also called *duplex*), both stations can transmit and receive simultaneously. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals 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 example 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.

Basis for comparison	Simplex mode	Half-duplex mode	Full-duplex mode
Direction of communication	In simplex mode, the communication is unidirectional.	In half-duplex mode, the communication is bidirectional, but one at a time.	In full-duplex mode, the communication is bidirectional.
Send/Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Performance	The performance of half-duplex mode is better than the simplex mode.	The performance of full-duplex mode is better than the half-duplex mode.	The Full-duplex mode has better performance among simplex and half-duplex mode as it doubles the utilization of the capacity of the communication channel.
Example	Examples of Simplex mode are radio, keyboard, and monitor.	Example of half-duplex is Walkie-Talkies.	Example of the Full-duplex mode is a telephone network.

7- Components of Computer Network

Computer network components are the major parts which are needed to install the software. Some important network components are NIC, switch, cable, hub, router, and modem. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.



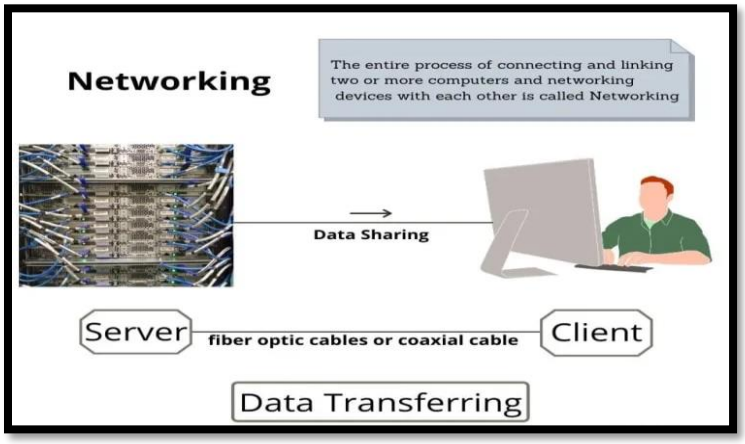
Following are the major components required to install a network:

1. Server

A server is a computer that serves the data to other computers and users. The network components can be in the form of a computer, a hardware device, or a computer program that is loaded so that it can send data and any information to other computers.

The term “server” usually refers to a computer system that receives a request for a web document and sends the request information to the client.

2. Client



The device that receives requests, and responses from the server, is called a client. When the server and its clients work together on the computer, we call it the client/server network.

3. Transmission media

Transmission media are the medium through which data is transferred from one device to another in a network. Transmission media can be used either in a physical transmission medium or wireless transmission medium.

Physical transmission medium includes the use of wires and cables like fiber optic cables, coaxial cable, etc; and wireless transmission medium includes the use of unguided media like infra-red waves, electromagnetic, microwaves, etc.

4. NIC (Network Interface cards)

Network Interface cards (NICs) are also called Network Interface Controller, Network adapter, LAN adapter, and Physical Network interface. NIC cards are hardware components used to connect computers with networks. Without NIC a computer cannot be connected to the network

It is installed in a computer circuit board that provides a network connection to the computer. Due to the popularity and low cost of Ethernet standards, the network interface is built directly into the motherboard in almost all new computers.

Types of NIC:

There are two types of NIC:

1. Internal Network Card (Wired NIC)

In internal network cards, the motherboard has a slot for the network card where it can be inserted. It requires a network cable to provide network access. There are two types of internal network cards. The first type uses Peripheral Component Interconnect (PCI) connections, while the second type uses Industry Standard Architecture (ISA).

2. External Network Card (Wireless NIC)

The external NIC is used by desktops and laptops because they do not have an internal NIC. External network cards are of two types: wireless and USB-based. Wireless network cards are required to be inserted into the motherboard. The USB based used to connect to a laptop when traveling or accessing wireless signals.

5. Hub

A hub is a device that splits a network connection among multiple computers. It works similarly to a distribution center. When a computer requests information from one network or from a specific computer, then it sends the request to the hub through a cable. The hub then receives that request and transmits it to the entire network.

After that, every computer checks whether that network then belongs to them or not. If belongs then it broadcasts if the request doesn't belong it will be dropped.

However, such network components nowadays are very less in circulation and being replaced by more advanced communication devices such as Routers and Switches. This hub is basically a multiport repeater.

This hub is used to connect multiple connections that come from different branches, For example, the connector in star topology is used to connect different stations for data access.

6. Switch

The switch is a component that helps devices to connect the networks so that they can transfer data to other connected devices. These network switches are identical to network hubs, but a switch has more advanced features than a hub. It doesn't broadcast entire data on the network like a hub.

The advanced features of the switch imply that the network switch first inspects the incoming packet and determines its source, destination address, and routes after that sends the data at the correct destination accordingly to that packet. A network switch is also called the Switching hub, Bridging hub, and MAC bridge.

7. Router

The router is a hardware network component. Routers operate at the network layer of the OSI (Open system interconnection) reference model, using them to send packets over the network using a logical address.

Any data which travels from one network to another network as a Packet. The Router receives such Packet data and forwards it to the Destination Device after analyzing hidden information in the Data Packet. This Networking Device is used to connect different networks either it is wired or wireless.

These networks are mainly seen in the house as Wi–Fi from which anyone can access the Internet.

Types of Router:

There are two main types of routers:

1. Broadband Routers-

Broadband Router is used to connect computers and to connect to the Internet. Those who need to connect their phone to the Internet through Voice Over IP Technology. There have to use Broadband Router. These are Modem also include Ethernet and Phone Jacks.

2. Wireless router

Wireless Router is very popular and useful. They are used more at home, Office, College. This router makes the internet connection wireless from which anyone can use the internet directly with their computers, tablets, mobile phones through a wireless signal.

There are features of passwords and IP Addresses for connection access in wireless routers. These make the connection more secure.

8. Modem

The full form of the modem is 'Modulator/Demodulator'. The process of converting a digital signal into an analog signal is called modulation. These components allow a computer device, such as a router or switch, to connect to the Internet.

It converts or "modulates" an analog signal from a telephone or cable wire into a digital signal that a router or switch can easily recognize the data.

Similarly, when it converts outgoing digital data into an analog signal in a computer device such converting is called Demodulation. The speed of transmitting data by modem is modifiable. This speed of transfer is measured in bytes per second (bps) rate. The faster its speed, the faster one can send and receive information.

Types of Modem:

There are basically three types of modem:

1. **External Modem-**

It is connected to the serial port of the computer by a cable located outside the computer. Another wire connects the modem to the telephone line.

2. Internal Modem-

This system is a plug-in circuit board located within the unit. This modem is connected to the telephone line by a telephone cable.

3. Wireless Modem-

As the name suggests it doesn't need any wire. It sends and receives signals through the air.

9. Repeater

A repeater is a powerful network component that is used to regenerate signals. With this, the signal is fixed for a long time, so that the strength of the signal remains stable. Repeater takes data signals from the communication medium and amplifies them and sends them back to the communication medium. When the signal becomes weak, this device copies the signal bit by bit and then regenerates it to its original strength for making the internet connection stable.

A repeater is located in the first layer (physical layer) of the OSI layer. Repeaters are used in cables that have to cover distances of up to 100 meters. These components receive signals from cables like optical fibers, coaxial cables, and copper cables.

10. Bridges

This bridge is a device that has such functionality that it filters the content, for which it reads MAC addresses of both source and destination. The bridge connects two LANs (Local Area Network) using the same protocol. This device operates in the data link layer of the OSI Model.

These network components are very useful for filtering the data load of traffic, for which they divide them into segments or packets. The bridge controls the data traffic of LANs or other networks. These bridges are actually passive devices, as there is no interaction between bridged and paths of bridging.

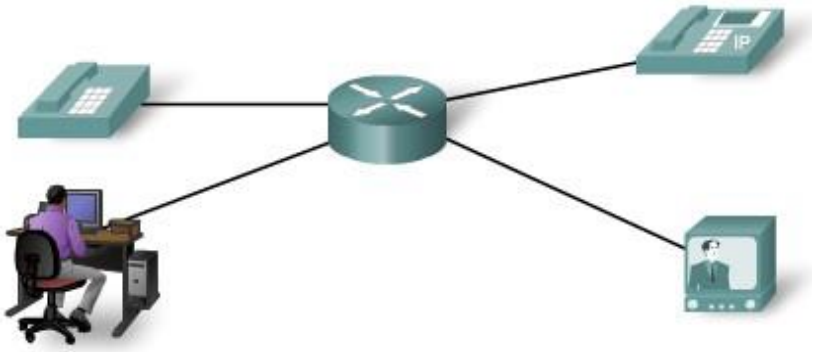
11. Gateway

This gateway is a hardware device that acts as a "gate" within two networks. It can also be a router, firewall, server, or any other device that enables traffic to flow in and out of the network. Gateways are used to connect networks based on different protocols. As a bridge is used to join two similar types of networks, similarly, the gateway is used to join two dissimilar networks.

This gateway node is located at the edge of the network and all the data flows through it which enters or exits the network. In addition, it can also translate received data that is received from outside networks, into a format or protocol that can be identified by devices within the internal network.

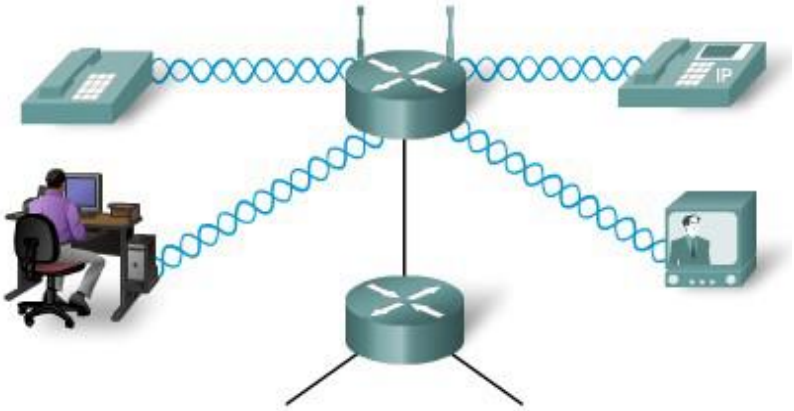
8- Elements of Network:

Wired networks used physical cables to connect devices.



Wireless networks use radio waves to communicate between devices.

Wireless networks are also connected to wired networks, at some point.



Desktop Computer

LAN Switch

Laptop

Firewall

Server

Router

IP Phone

Wireless Router

LAN Media

Cloud

Wireless Media

WAN Media

9- 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 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).

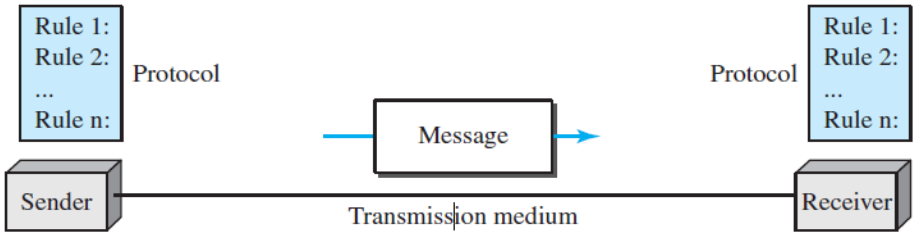
The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

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.
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 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

10- Components

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

Figure 1.1 *Five components of data communication*



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.
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.

11- Data Representation

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

A. 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.**

B. 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.

C. 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 size of the pixel depends on the *resolution.* 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.

D. 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.

E. 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.