Computer Network

1.1 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 three 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.

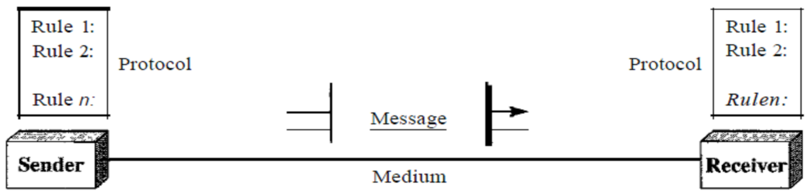
3. Timeliness: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time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

Communications System Components

A data communications system has five components (see Figure 1.1).

Figure 1.1 *Five components ofdata communication*



1**. Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

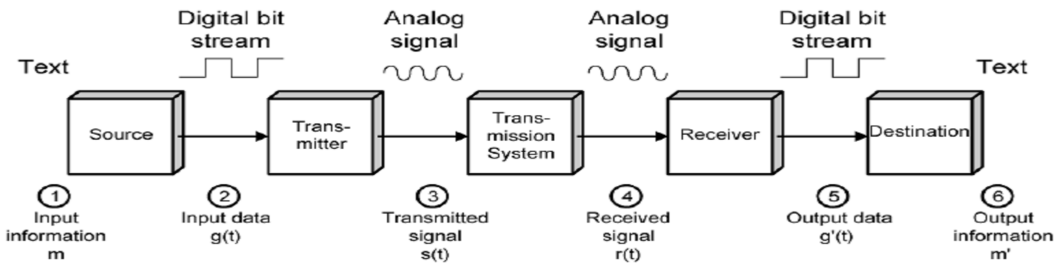
2. **Sender.** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

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.

Data Communications Model



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 (Os or Is). 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.

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. Appendix B discusses several different numbering systems.

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. 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 blackand- white dots (e.g., a chessboard), a I-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.

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. Again we can change video to a digital or an analog signal.

Transmission Mode (Data Flow)

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

1. simplex
2. half-duplex
3. 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 1.2a). 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 1.2a

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 1.2b). 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.

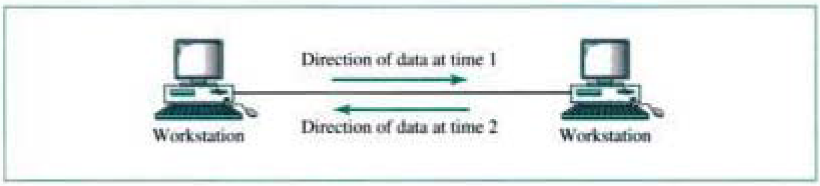


Figure 1.2b

<u>Full-Duplex</u>

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c). 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.

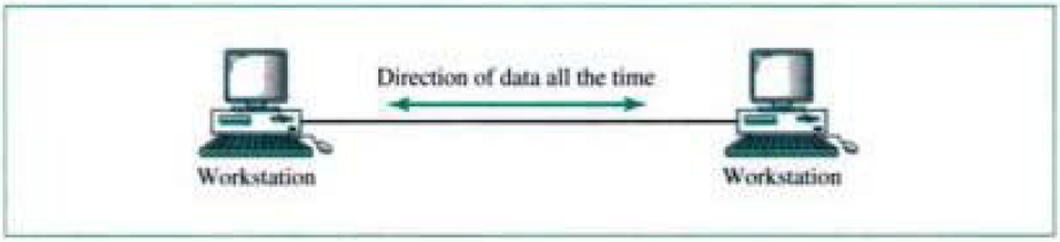


Figure 1.2c

1.2 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 use distributed processing, in which a task is divided among multiple computers.

Advantage

1. Security/encapsulation A system designer can limit the kinds of interactions that a given user can have with the entire system, for example aback can allow user access to their own accounts through an automated teller machine (ATM) without allowing them access the bank's entire database.
2. Distributed databases No one system needs to provide storage capacity for the entire database. For example the Word Wide Web (www) given users access to the information that may be actually stored and manipulated any where on the internet.
3. Faster problem solving Multiple computers working on parts of a problem concurrently can often solve the problem faster than a single machine working alone for example network of PCs have broken encryption codes that where presumed to unbreakable because the amount of time it would take a single computer to crack them.
4. Security through redundancy Multiple computers running the same program at the same time can provide security through redundancy. For example space shuttle, three computer run the same program so that if one have hardware error , the other two can override it.
5. Collaborative processing Both multiple computers and multiple users may interact on a task, for example in multi-user network game the actions of each player are visible to and affect all the others.

Applications:

1- Marketing and sales 2- Financial services 3- Manufacturing
4- Electronic massaging 5- Directory services 6- Information services
7- Electronics Data Interchange (EDI) 8- Teleconferencing
9- Cellular telephone 10-Cable television

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 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.

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.

Network Basic Concepts

Types of Connections

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.**

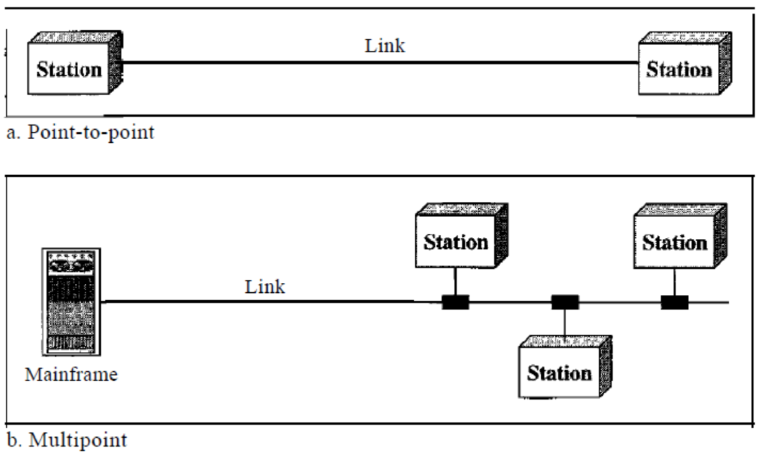
Point-to-Point

- 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 1.3a).
- 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.

Multipoint

- A multipoint (also called multi-drop) connection is one in which more than two specific devices share a single link (see Figure 1.3b).
- 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.

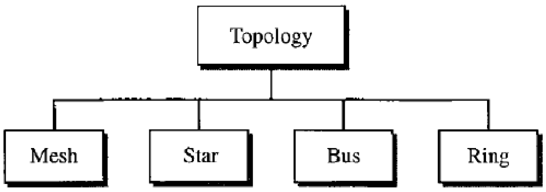
Figure 1.3 *Types of connections: point-to-point and multipoint*



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 1.4).

Figure **1.4** *Categories oftopology*



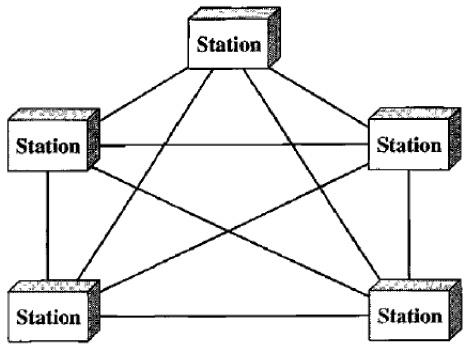
Mesh Topology

- 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. Node 1 must be connected to ***n* - 1** nodes, node 2 must be connected to ***n* – 1** nodes, and finally node *n* must be connected to ***n* - 1** nodes. 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 1.5) to be connected to the other *n* - 1 stations.

Figure 1.5 *A fully connected mesh topology (five devices)*



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.

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 1.6).

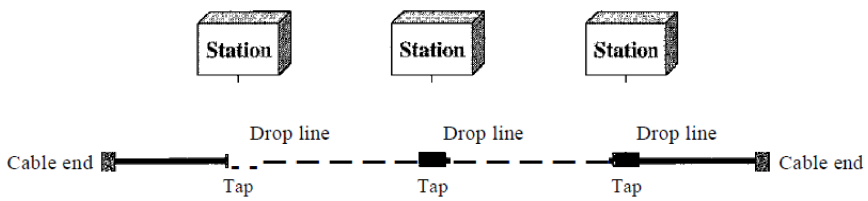
Advantages:

- 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.
- 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.

Bus Topology

The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is **multipoint.** One long cable acts as a **backbone** to link all the devices in a network (see Figure 1.7).

Figure 1.7 *A bus topology connecting three 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 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, **<u>for example</u>**, 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 include:

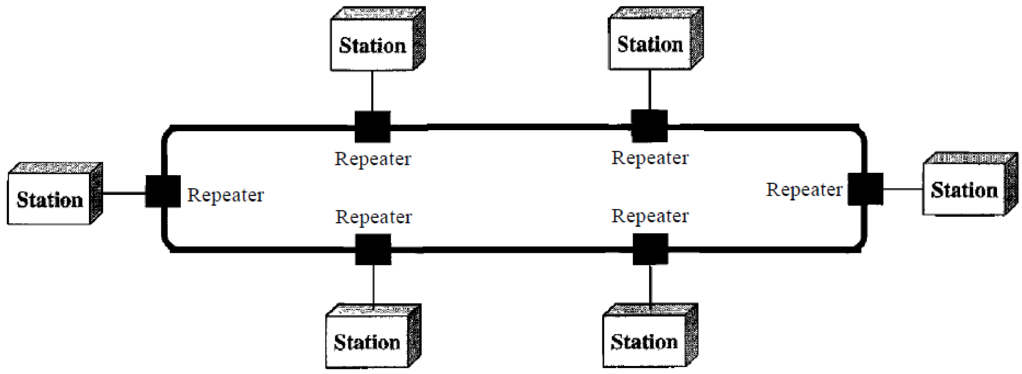
- difficult reconnection and fault isolation.
- A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable.
- Adding new devices may therefore require modification or replacement of the backbone.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects

signals back in the direction of origin, creating noise in both directions. **Bus topology** was the one of the first topologies used in the design of early **local area networks.**

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 1.8).

Figure 1.8 *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 (either physically or logically). To add or delete a device requires changing only two connections.

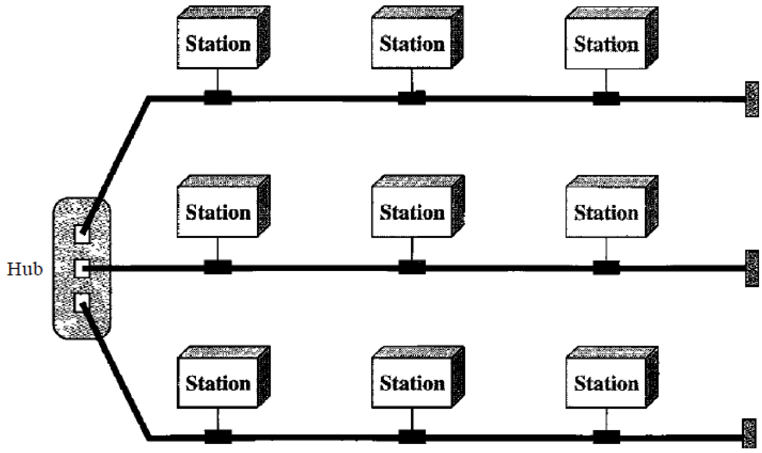
Disadvantage:

- 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.
- However, 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.** Ring topology was prevalent when IBM introduced its

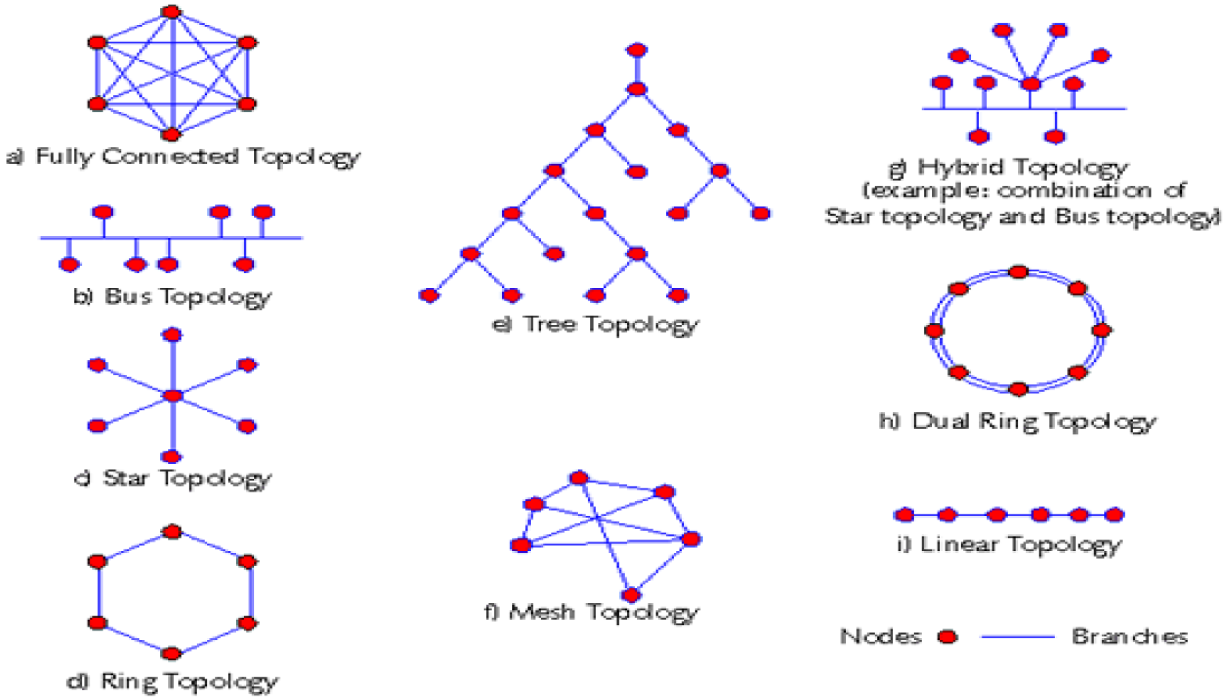
local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

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 1.9.

Figure 1.9 A *hybrid topology: a star backbone with three bus networks*



Hybrid topologies Often a network combines several topologies as a 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.



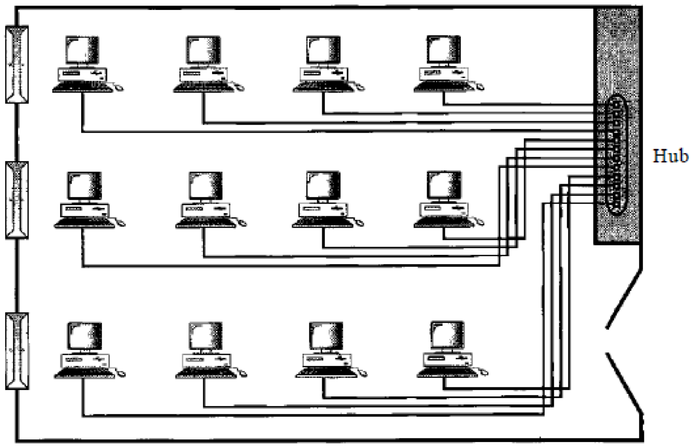
Categories of Networks

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 miles** 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 1.10). 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.

Figure 1.10 *An isolated LAN connecting 12 computers to a hub in a closet*

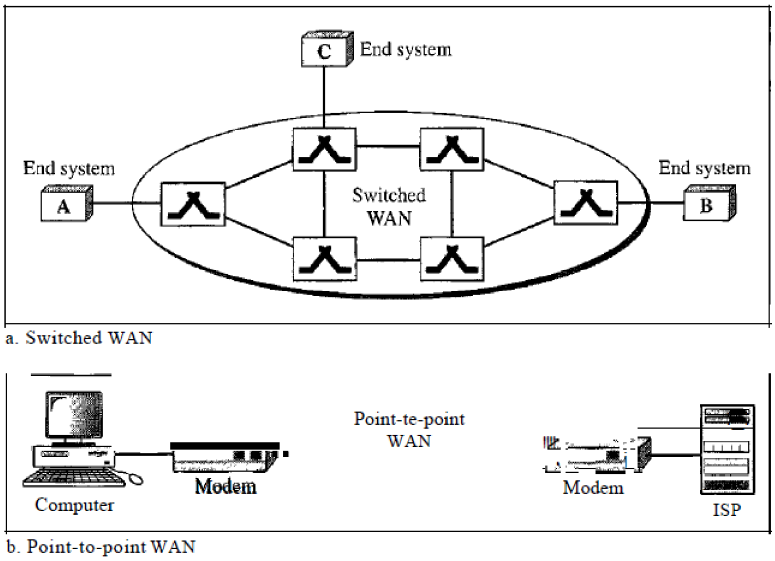


LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. **A common example of a LAN**, found in many business environments, links a workgroup of task-related 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 1.11). 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 (lSP). This type of WAN is often used to provide Internet access.

Figure 1.11 *WANs: a switched WAN and a point-to-point WAN*



An **early example** of a switched WAN is X.25, a network designed to provide connectivity between end users. X.25 is being gradually replaced by a high-speed, more efficient network called Frame Relay. A good **example** of a switched WAN is the Asynchronous Transfer Mode (ATM) network, which is a network with fixed-size data unit packets called cells. Another example of WANs is the wireless WAN that is becoming more and more popular.

Metropolitan Area Networks

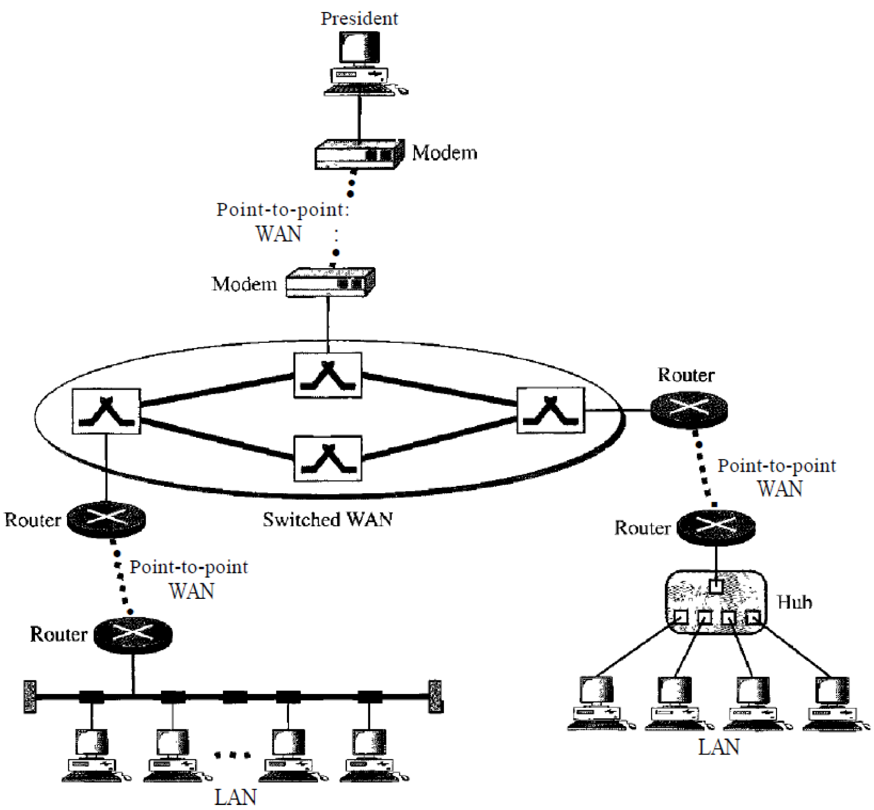
A metropolitan area network (MAN) is a network with a **size** between a LAN and a WAN. It normally **covers** the area inside a town or a city. It is **designed for** customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good **example** of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another **example** is the cable TV network that originally was designed for cable TV, but today
can also be used for high-speed data connection to the Internet.

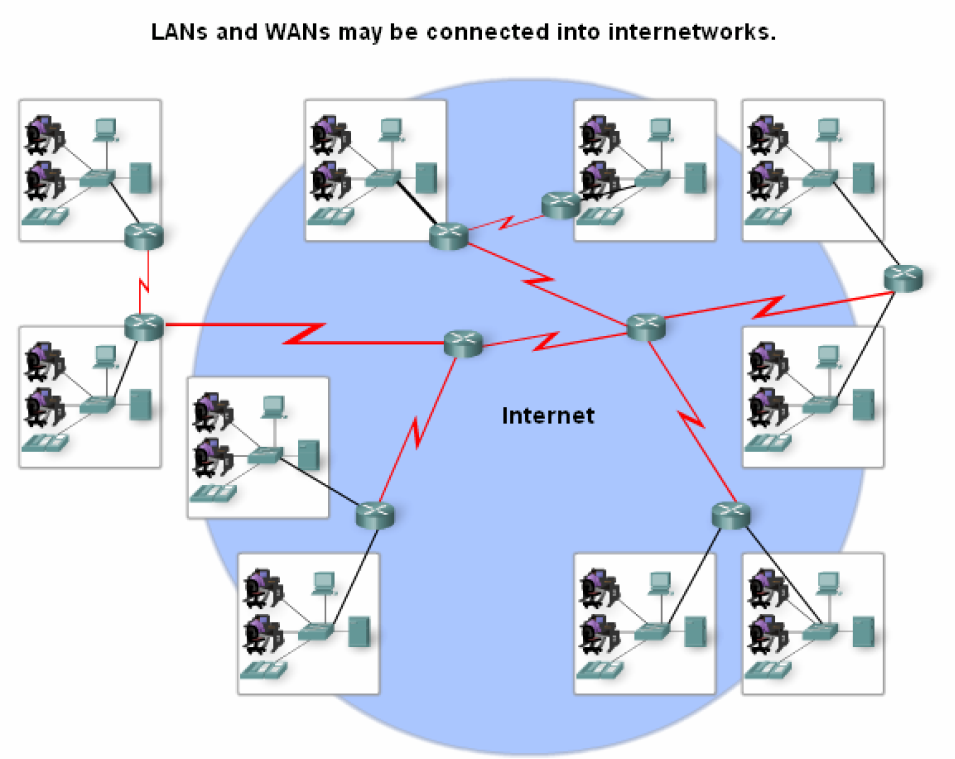
Interconnection of Networks: Internetwork

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 horne.
- 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 modern line offered by a cable TV provider as shown in Figure 1.12.

Figure 1.12 *A heterogeneous network made offour WANs and two LANs*





PROTOCOL S 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?.
- 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").

- 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

1- **ISO(The International Standard Organization)** created in 1947 is an organization dedicated to worldwide agreement on international standards in a variety of fields(scientific, technological, economic activity) OSI model .

2-**ITU-T(International Telecommunication Union Telecommunication Standards Sector)** is an international standards organization related to the United Nations that develops standards for telecommunications.

3- **ANSI(American National Standard Institute)** is a nonprofit organization and is the U.S. voting representative to be both the ISO and the ITU-T

4- ETSI(European Telecommunications Standards Institute)

5- IEEE(Institute of Electrical and Electronic Engineers) is the largest national professional group involved in developing standards for computing, communication, electrical engineering, and electronics)

6- EIA(Electronic Industries Association) is an association of electronics manufactures in the United States. (EIA-232-D, EIA-530 standards).

Forums

Telecommunications technology development is moving faster than the ability of standards committees to ratify standards. Standards committees are procedural bodies and by nature slow-moving. To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have developed **forums** made up of representatives from interested corporations. The forums work with universities and users to test, evaluate, and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies. ***Forums are special-interest groups that quickly evaluate and standardize new technologies.***

Network Models

A network is a combination of hardware and software that sends data from one location to another. The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network.

We can compare the task of networking to the task of solving a mathematics problem with a computer. The fundamental job of solving the problem with a computer is done by computer hardware. However, this is a very tedious task if only hardware is involved. We would need switches for every memory location to store and manipulate data. The task is much easier if software is available. At the highest level, a program can direct the problem-solving process; the details of how this is done by the actual hardware can be left to the layers of software that are called by the higher levels. Compare this to a service provided by a computer network. For example, the task of sending an e-mail from one point in the world to another can be broken into several tasks, each performed by a separate software package. Each software package uses the services of another software package. At the lowest layer, a signal, or a set of signals, is sent from the source computer to the destination computer.

LAYERED TASKS

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office. Figure (1) shows the steps in this task.

Sender, Receiver, and Carrier

In Figure (1) we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site

Let us first describe, in order, the activities that take place at the sender site.

- Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

- Middle layer. The letter is picked up by a letter carrier and delivered to the post office.

- Lower layer. The letter is sorted at the post office; a carrier transports the letter.

0n the Way

The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

- Lower layer. The carrier transports the letter to the post office.

- Middle layer. The letter is sorted and delivered to the recipient's mailbox.

- Higher layer. The receiver picks up the letter, opens the envelope, and reads it.

Hierarchy

According to our analysis, there are three different activities at the sender site and another three activities at the receiver site. The task of transporting the letter between the sender and the receiver is done by the carrier. Something that is not obvious immediately is that the tasks must be done in the order given in the hierarchy.

At the sender site, the letter must be written and dropped in the mailbox before being picked up by the letter carrier and delivered to the post office. At the receiver site, the letter must be dropped in the recipient mailbox before being picked up and read by the recipient.

<u>Services</u>

Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier. The layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCPIIP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

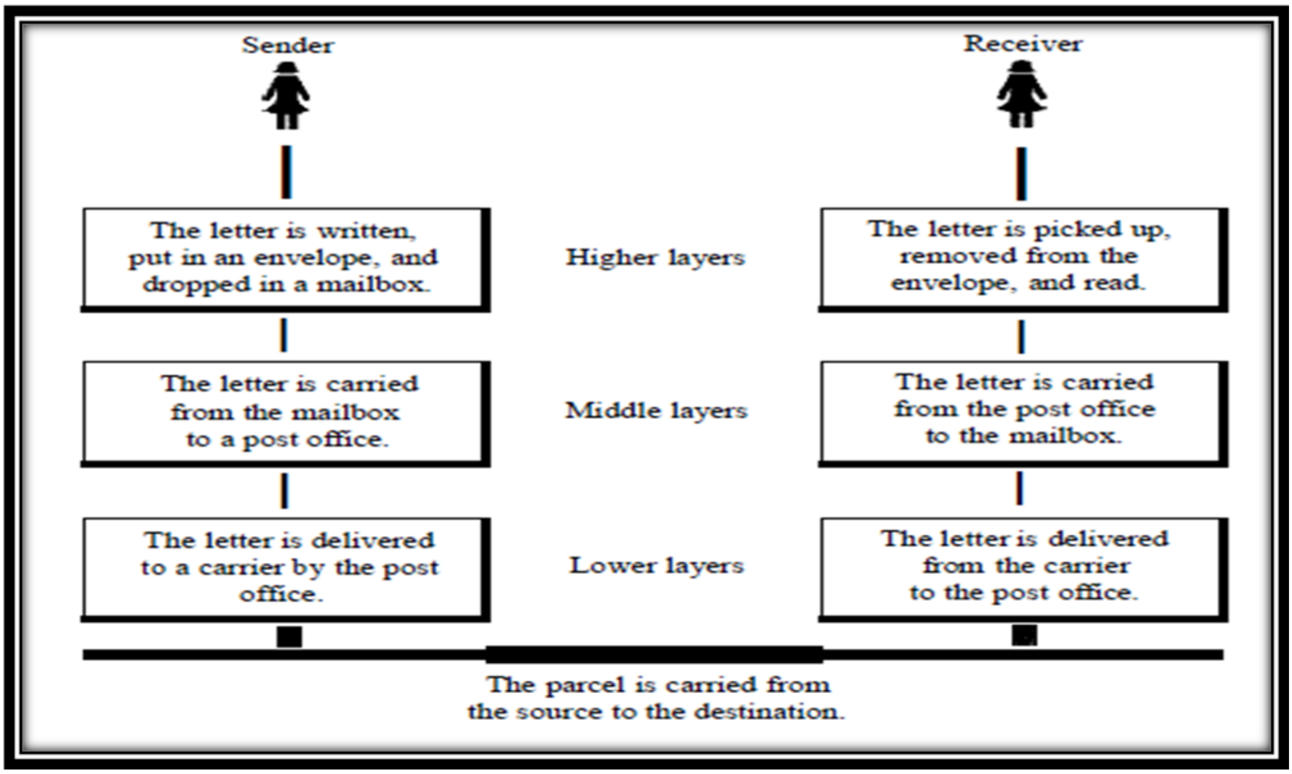


Figure (1) Tasks involved in sending a letter

THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s***. In order to enable heterogeneous computer systems to interconnect and network regardless if their manufactures models, complexity and age layered communication architecture have been established. An open system is a set of protocols that allows any two***

different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. ISO is the organization. OSI is the model. The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2). An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

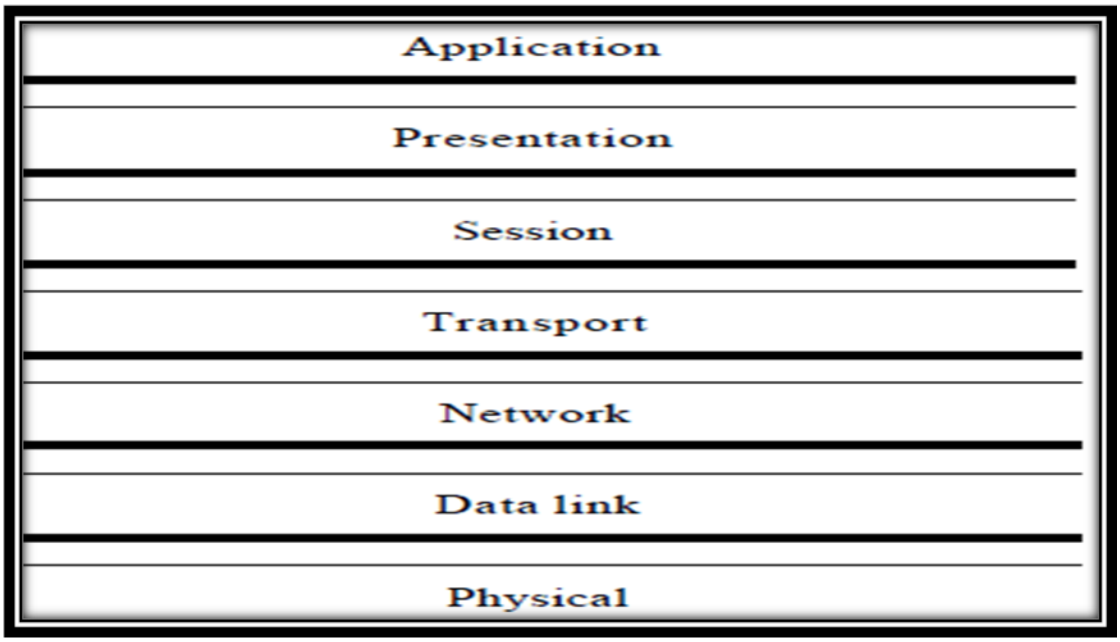


Figure (2) Tasks involved in sending a letter