كلية المامون الجامعة

قسم هندسة الاتصالات

المادة : شبكات الحاسوب

المرحلة : الرابعة

اعداد الدكتور : د. محمد كاظم

2021_2022

1-1 DATA COMMUNICATIONS

The term telecommunication means communication at a distance. 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.

Topics discussed in this section:

- Components of a data communications system
- Data Représentation
- Data Flow

Criteria of Effectiveness of Data Communication

- **Delivery:**
  - Data must arrive at the correct destination.
  - Data must be received by the intended device or user and only by that device or user.
- **Accuracy:**
  - The system must deliver the data accurately.
  - Data that have been altered in transmission and left uncorrected are unusable.
- **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).
- **Jitter:**
  - Variation in the data arrival time at the detonation

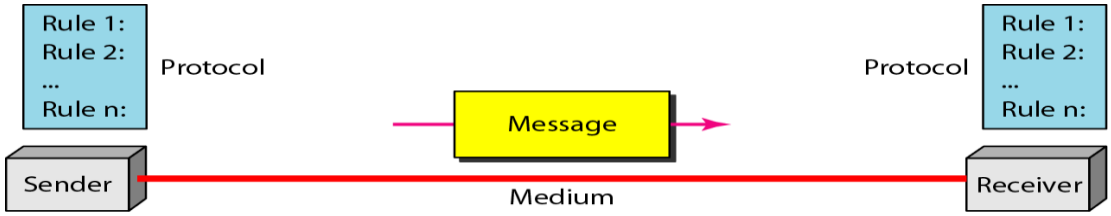


Figure 1.1: Components of a data communication system

Components of a data communication system

- **Message:**
  - The message is the information (data) to be communicated.
  - Popular forms of information include **text, numbers, pictures, audio, and video.**
- **Sender:**
  - The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
- **Receiver:**
  - The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- **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.

- **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

- **Text**
  - In data communications, text is represented as a bit pattern, a sequence of bits (Zero or One)
- **Numbers**
  - Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers
  - ASCII code: includes definitions for 128 characters
  - Unicode: current prevalent coding system for text
- **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

➢ **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

➢ **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.

Data flow (simplex, half-duplex, and full-duplex)

➢ **Simplex mode**

- In simplex mode, the communication is unidirectional, as on a one-way street
- Keyboard, mouse, traditional monitor

➢ **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
- Walkie-talkie
- Advantage: entire bandwidth can be used for transmission

➢ **Full duplex**

- In full-duplex mode , both stations can transmit and receive simultaneously
- The full-duplex mode is like a tow way street with traffic flowing in both directions at the same time

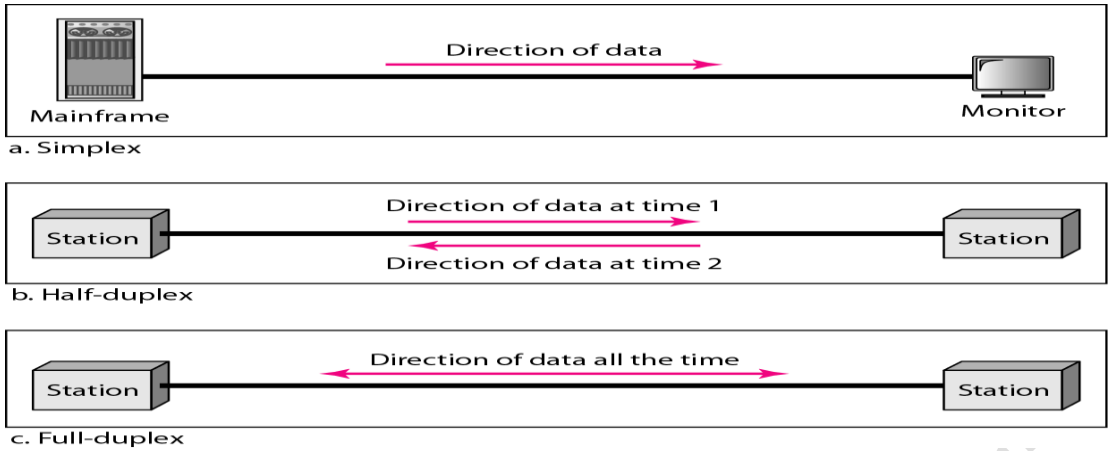


Figure 1.2: Data flow (simplex, half-duplex, and full-duplex)

➢ **Performance**

Performance can be measured in transit time and response time.

- **Transit time** is the amount of time required for a message to travel from one device to another device
- **Response time** is the elapsed time between an inquiry and a response.

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. A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

Topics discussed in this section:

- Network Criteria
- Physical Structures
- Categories of Networks

Network criteria

- **Performance**

  Performance can be measured in transit time and response time.

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

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

The performance of a network depends on a number of factor including:

1. The number of users.
2. The type of transmission medium.
3. The capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput** and **delay.**

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**
  - Failure rate of network components
  - network reliability is measured by :
    1. The frequency of failure
    2. The time it takes a link to recover from a failure,
    3. The network's robustness in a catastrophe
- **Security**
  - Network security issues include :
    1. Protecting data from unauthorized access
    2. Protecting data from damage and development
    3. Implementing policies and procedures for recovery from breaches and data losses.
    4.

Type of Connection

- **Point to Point –single transmitter and receiver**
  - A point-to-point connection provides a dedicated link between two devices (see Figure 1.3a).
  - 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
- **Multipoint - multiple recipients of single transmission**
  - Multipoin**t** 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**.

1. If several devices can use the link simultaneously, it is a **spatially shared connection**.
2. If users must take turns, it is a **timeshared connection**.

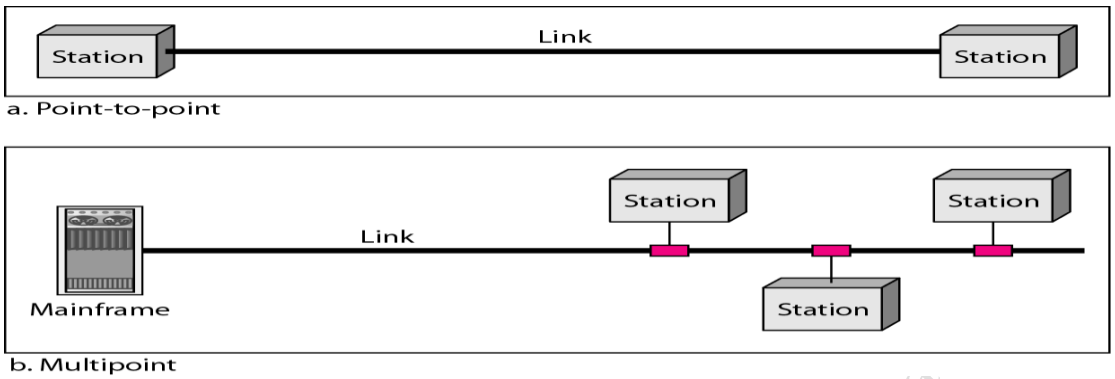


Figure 1.3 : Types of connections: point-to-point and multipoint

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.
- Topologies can be either **physical** or **logical.**
  - **Physical topologies** describe how the cables are run.
  - **Logical topologies** describe how the network messages travel
  - 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

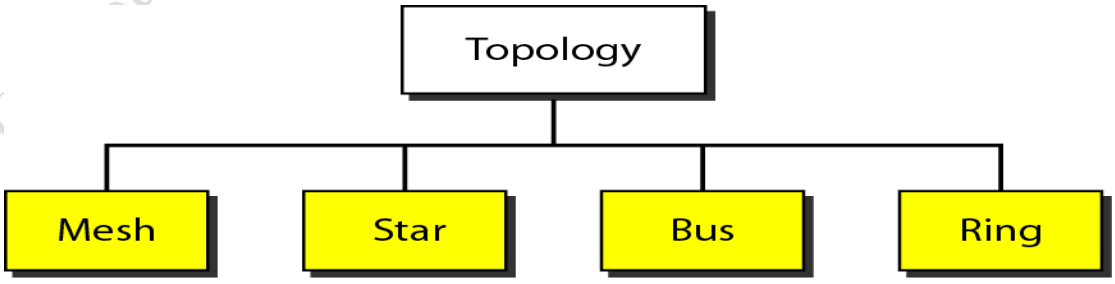


Figure 1.4: Categories *of topology*

Mesh Topology

- In a mesh topology, every device has a **dedicated** point-to-point link to every other device.
- 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 - I 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

Mesh Topology Advantages

- **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.

Mesh Topology Disadvantages

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

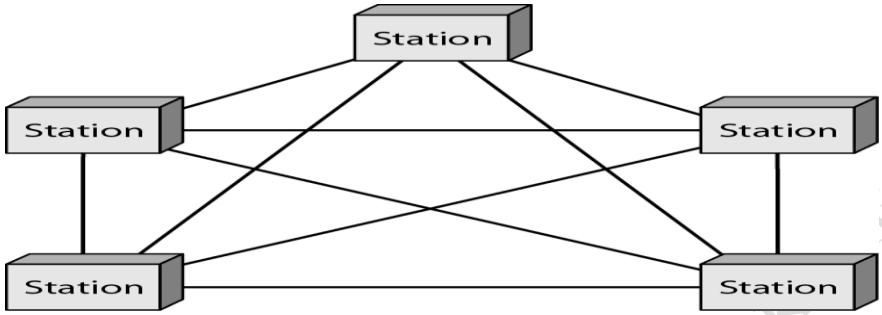
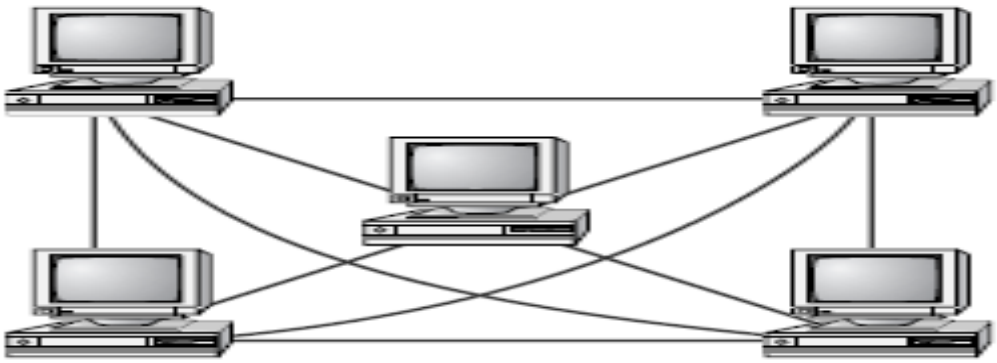


Figure 1.5 A fully connected mesh topology (five devices)



Mesh Topology

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).
- The star topology is used in **local-area networks (LANs).**
- High-speed LANs often use a star topology with a central hub.

Star Topology Advantages

- **First**, 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.

- **Second**, 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.

Star Topology Disadvantages

- **First**, 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.
- **Second**, 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).

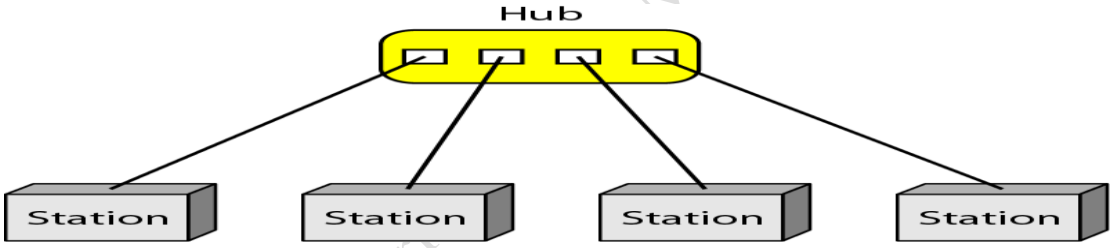
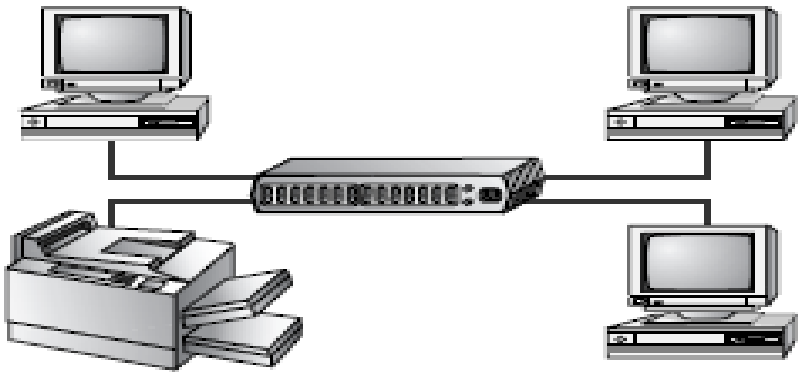


Figure 1.6 ***A star topology connecting four stations***



Star Topology

Bus Topology

- **Bus Topology: The** preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint.

- A bus is the simplest physical topology. It consists of a single cable that runs to every workstation, One long cable acts as a **backbone** to link all the devices in a network
- This topology uses the least amount of cabling, but also covers the shortest amount of distance.
- Each computer shares the same data and address path. With a logical bus topology, messages pass through the trunk, and each workstation checks to see if the message is addressed to itself. If the address of the message matches the workstation's address, the network adapter copies the message to the card's on-board memory.
- Have to completely reroute the cable and possibly run two additional lengths of it. if any one of the cables breaks, the entire network is disrupted. Therefore, **it is very expensive to maintain**
- Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology

Bus Topology Advantages

- **First,** 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 all the way to the hub.
- **Second,** 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 of cable reaching

Bus Topology Disadvantages

- Disadvantages include difficult **reconnection** and **fault isolation**.
- **First,** a bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- **Second,** 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.
- **Third**, 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.

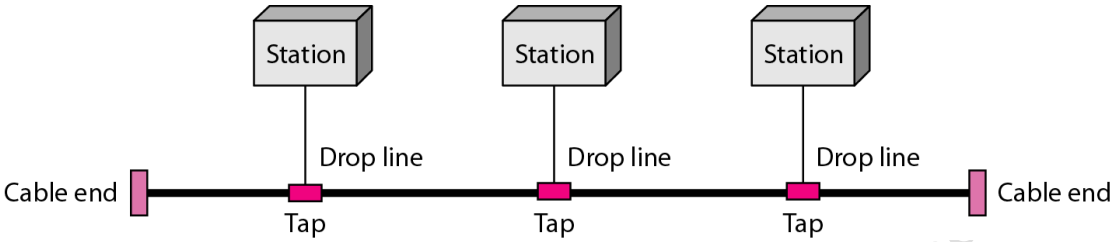
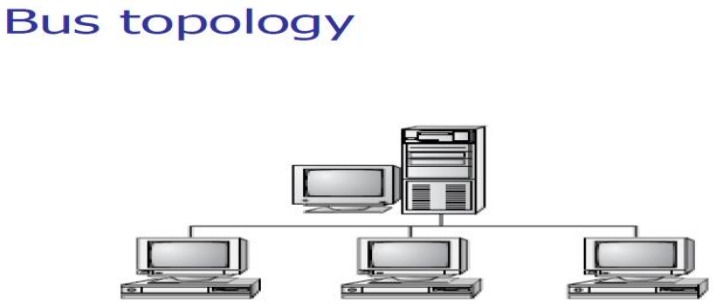


Figure 1.7 ***A bus topology connecting three stations***



Ring Topology

- 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).

Ring Topology Advantages

- **First**, a ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).
- **Second**, 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).

- **Third,** 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.

Ring Topology Disadvantages

- 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).

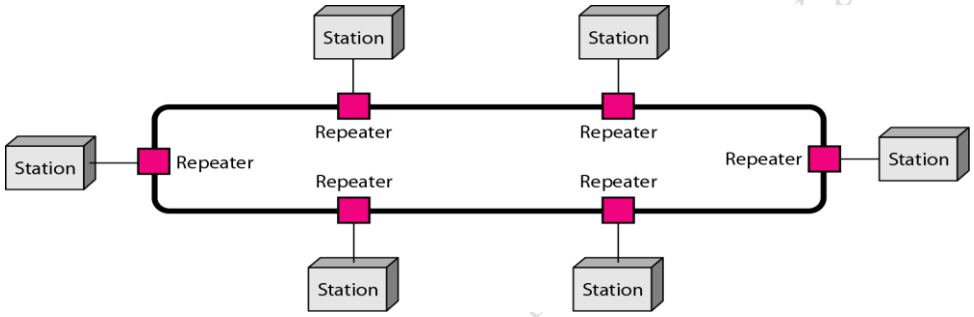
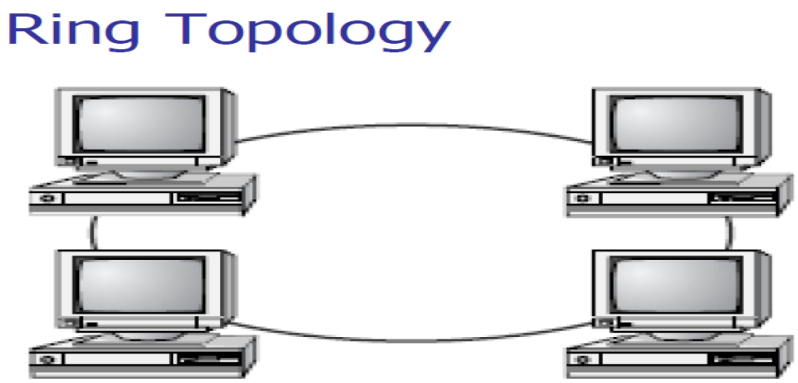


Figure 1.8 ***A ring topology connecting six stations***



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.

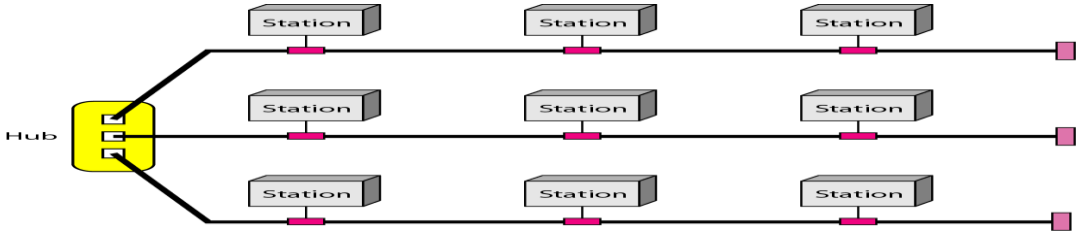


Figure 1.9 : A hybrid topology: a star backbone with three bus networks

Advantages and Disadvantages of Network Topologies

Topology	Advantages	Disadvantages
Bus	Cheap. Easy to install.	Difficult to reconfigure. Break in bus disables entire network.
Star	Cheap. Easy to install. Easy to reconfigure. Fault tolerant.	More expensive than bus.
Ring	Efficient. Easy to install.	Reconfiguration difficult. Very expensive.
Mesh	Simplest. Most fault tolerant.	Reconfiguration extremely difficult. Extremely expensive. Very complex.

Categories of Networks

There are generally two primary categories of Network:
Local-area networks and Wide-area networks.

Local Area Networks (LANs)

- 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.**
  - **Short distances**
  - **Designed to provide local interconnectivity**

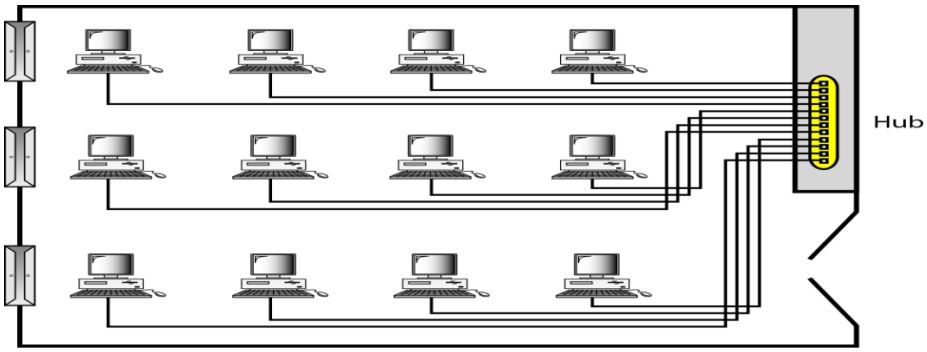
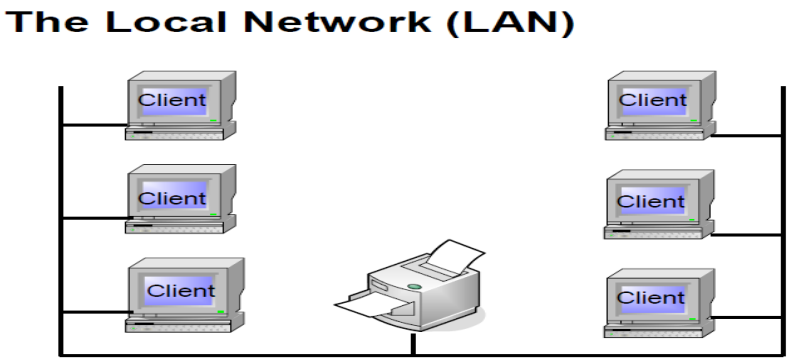


Figure 1.10 ***An isolated LAN connecting 12 computers to a hub in a closet***



Wide Area Networks (WANs)

- 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 largest and most well-known example of a WAN is the **Internet**.
  - **Long distances**
  - **Provide connectivity over large areas**

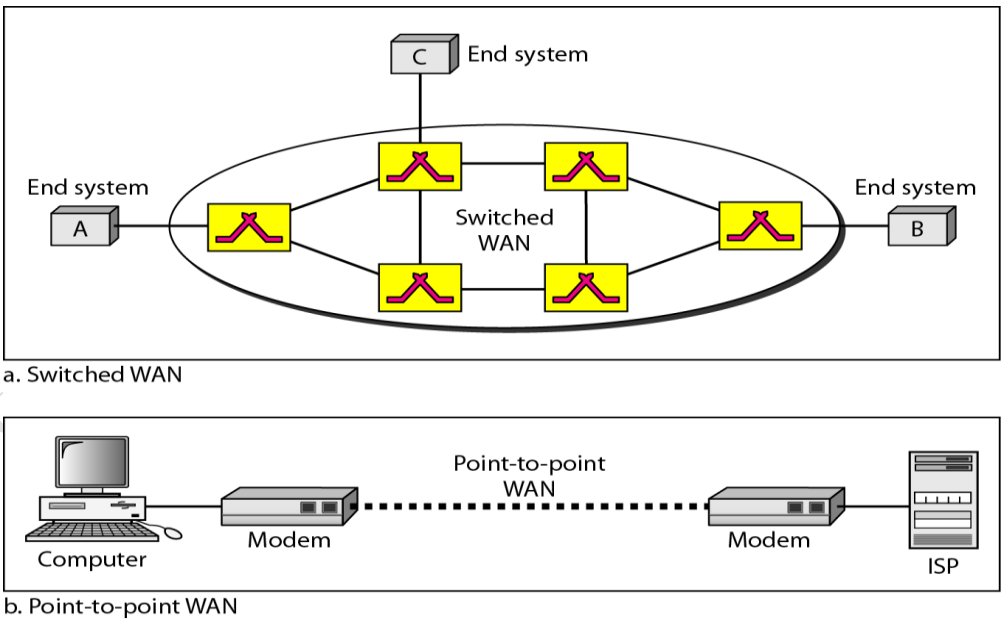
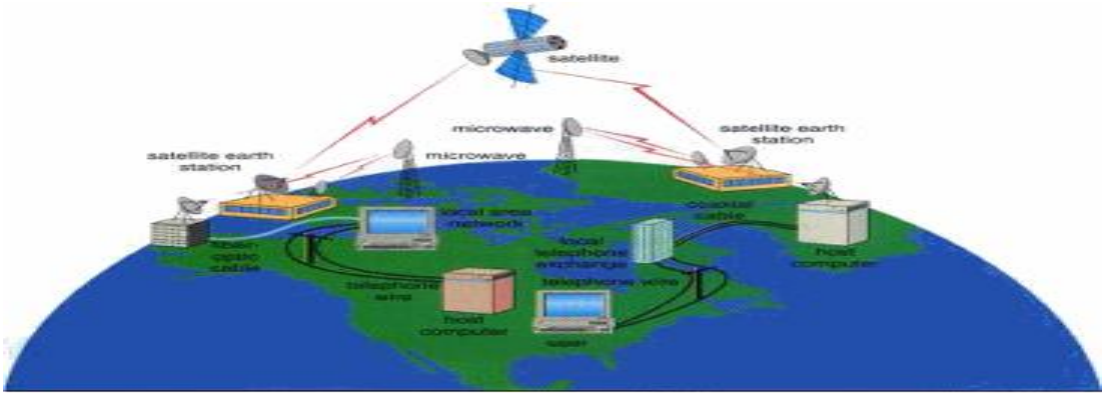


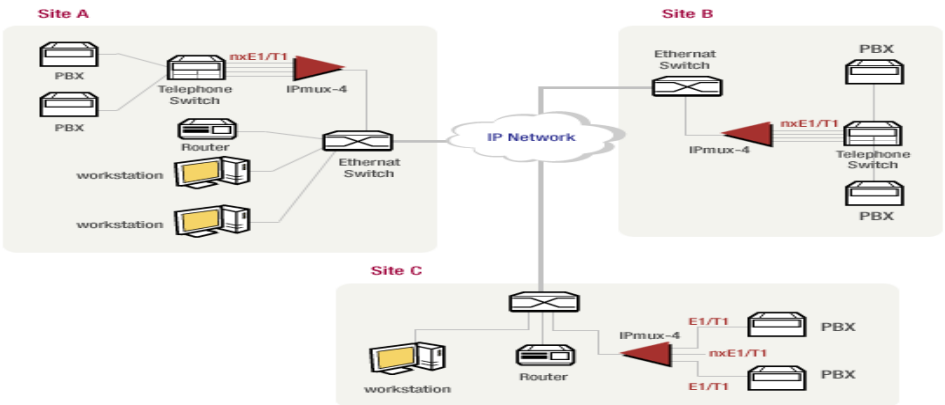
Figure 1.11 WANs: a switched WAN and a point-to-point WAN



Wide Area Network (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 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
- **Provide connectivity over areas such as a city, a campus**



Metropolitan Area Network (MAN)

1-3 THE INTERNET (International Network)

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 communication system that has brought a wealth of information to our fingertips and organized it for our use.

Topics discussed in this section

Organization of the Internet
Internet Service Providers (ISPs)

International Internet Service Providers (ISPs)

- 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.

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

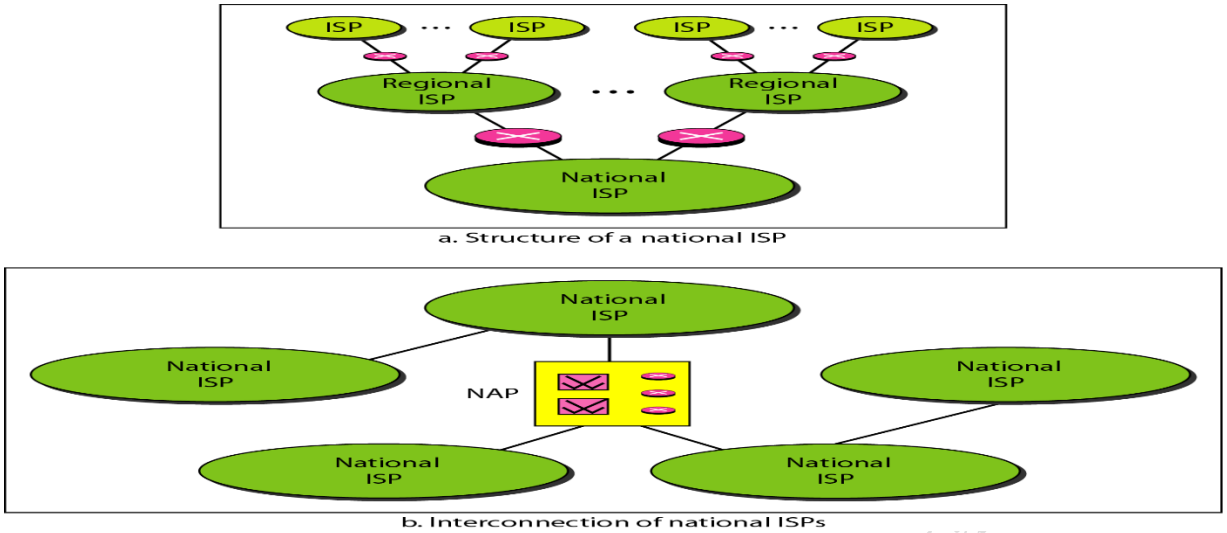


Figure 1.13 : ***Hierarchical organization of the Internet***

1-4 PROTOCOLS

A protocol is synonymous with rule. It consists of a **set of rules** that govern data communications. It determines what is communicated, how it is communicated and when it is communicated. The key elements of a protocol are syntax, semantics and timing.

- 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.
- A protocol similar to human language (syntax, semantics, timing)

Elements of a Protocol

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.
  - **Structure or format of the data**
  - **Indicates how to read the bits - field delineation**

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?
  - **Interprets the meaning of the bits**
  - **Knows which fields define what action**

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.
  - When data should be sent and what
  - Speed at which data should be sent or speed at which it is being received.