Data Communication And Networking

3rd Class

Dr Mohammed Shweesh Ahmed

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*** 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. ***Information*** refers to processed data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cables or wireless.

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.

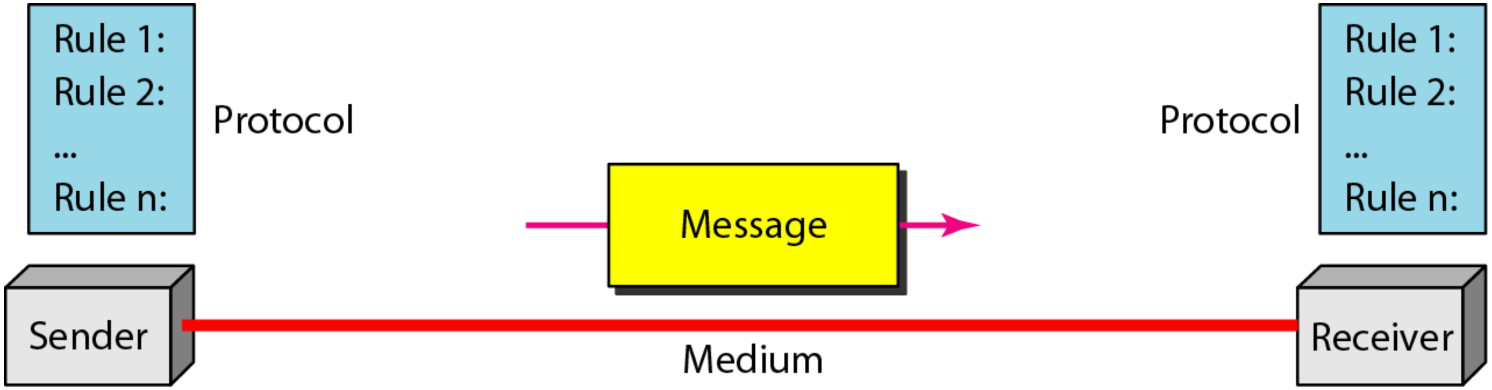
2. Accuracy: The system must deliver the data accurately. Data that have beenaltered in transmission and left uncorrected are unusable.

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.

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

Figure 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.

Data Representation

Information today comes in:

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.

Numbers

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

Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution.* After an image is divided into pixels, each pixel is assigned a bit pattern.

Audio

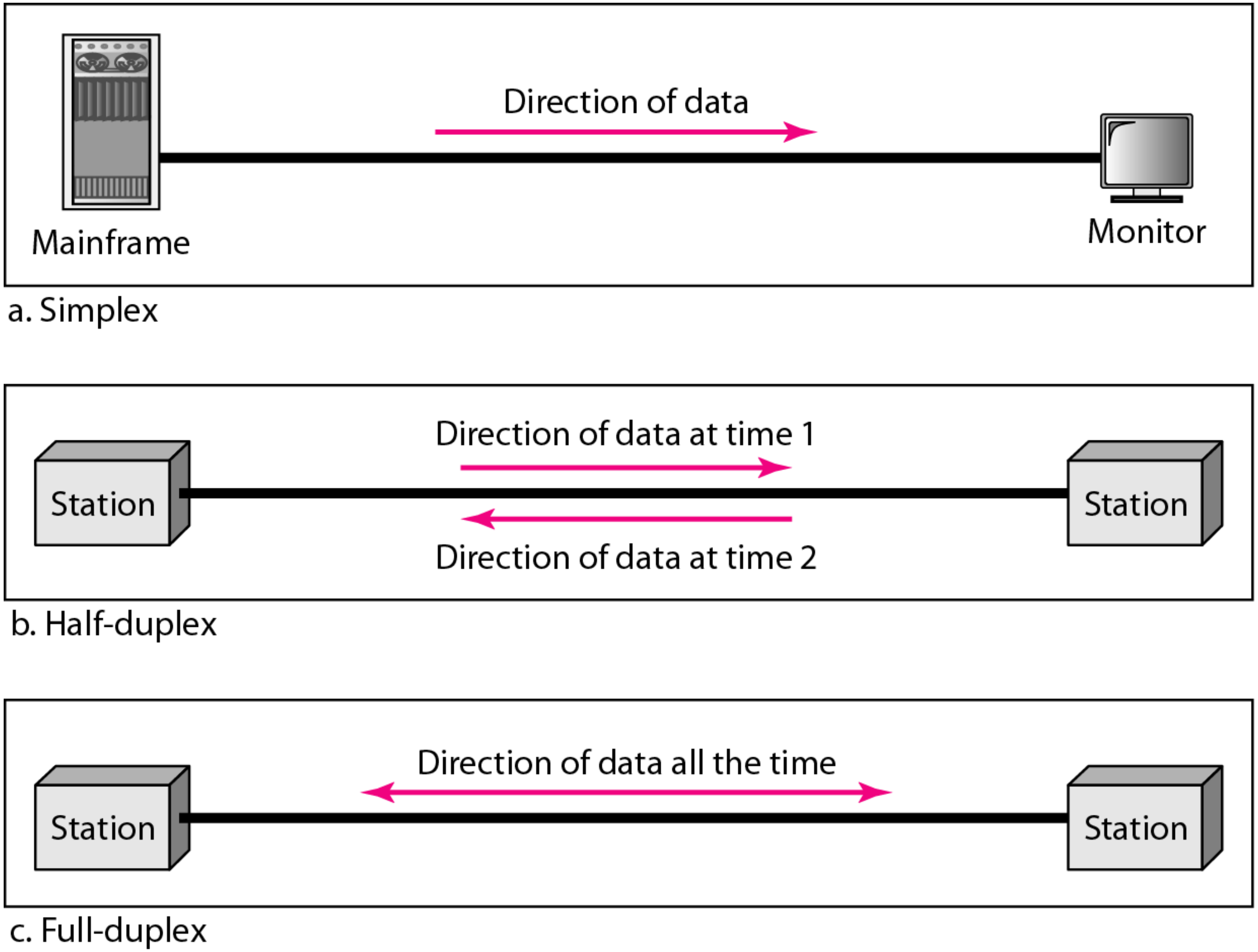
Audio refers to the recording or broadcasting of sound or music.

Video

Video refers to the recording or broadcasting of a picture or movie.

Data Flow

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


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

Figure 2 ***Data flow (simplex, half-duplex, and full-duplex)***

1-2 NETWORKS

A ***network*** is the interconnection of a set of devices capable of communication.

In this definition, a device can be a host 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.

Network Criteria (معايير)

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 (المنقضي) 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.

Reliability (دقة او صلابة)

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 (كارثة).

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 (خروقات او مخالفات) and data losses.

Type of Connections

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

Multipoint

A multipoint connection is one in which more than two specific devices share a single link.

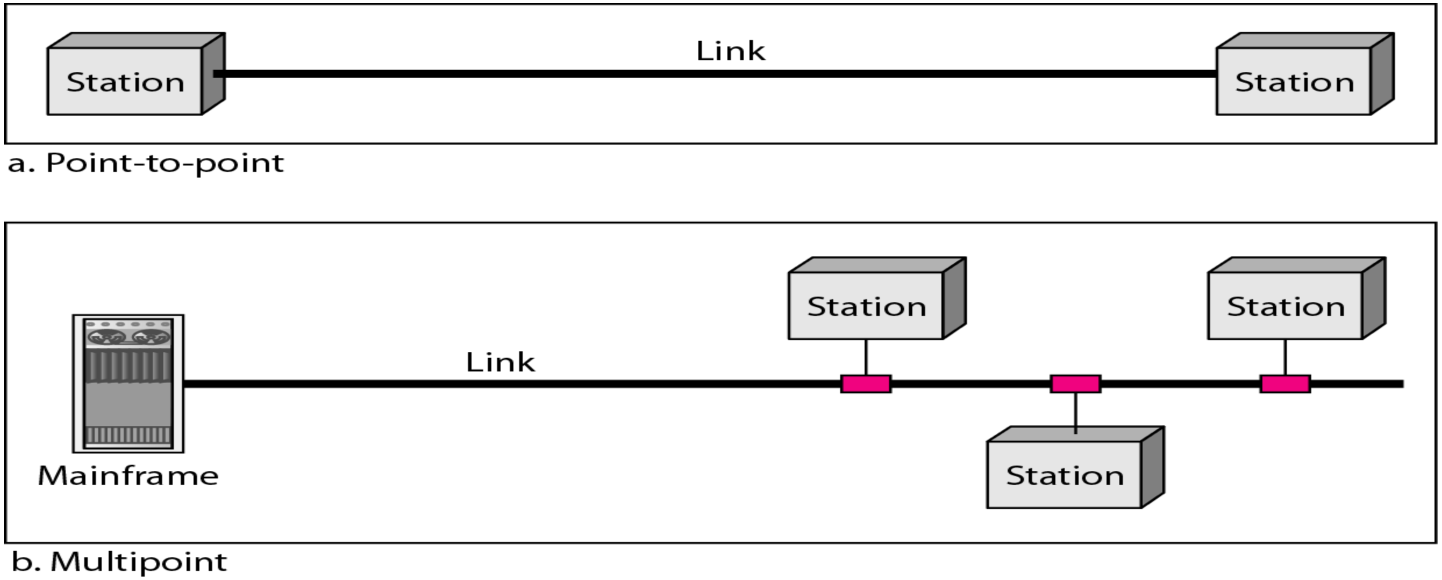


Figure 3 *Types of connections: point-to-point and multipoint*

Physical Topology

The term *physical topology* refers to the way in which a network is laid out (وضعت) 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

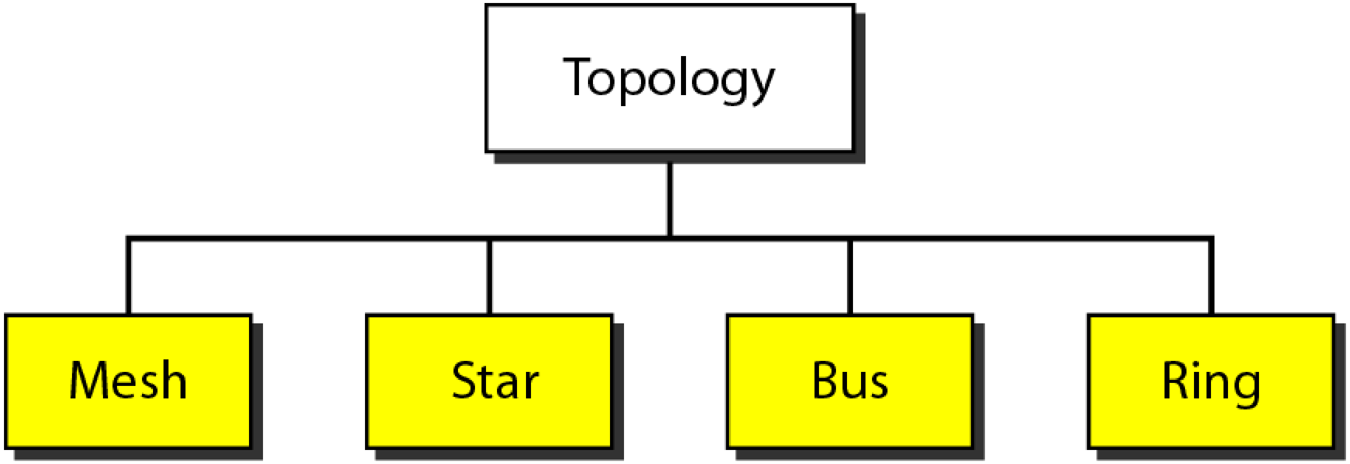


Figure 4 ***Categories of topology***

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 (Full-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.

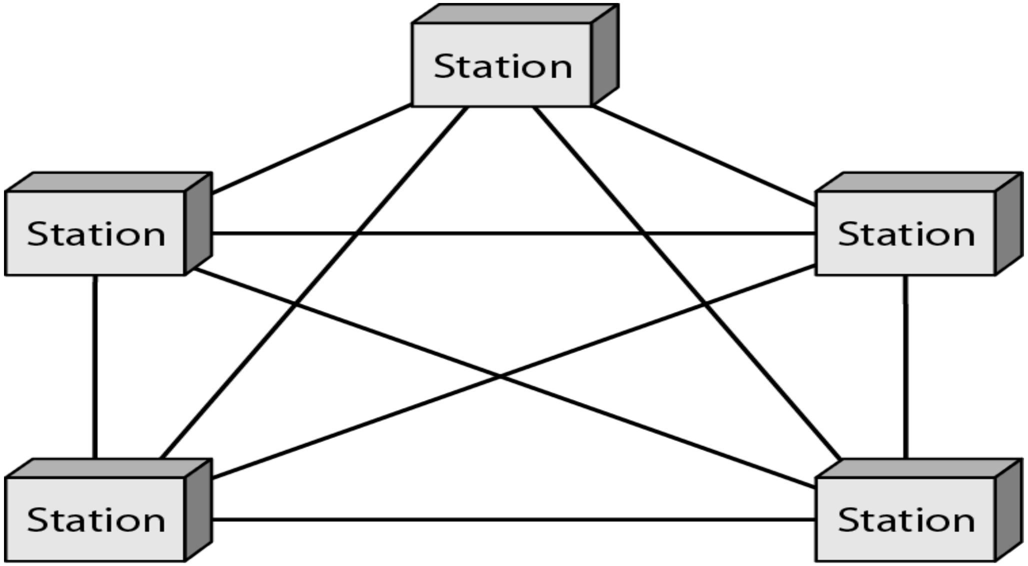


Figure 5 ***A fully connected mesh topology (five devices)***

Mesh advantages

1. 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.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate (يعجز او يضعف) the entire system.
3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
4. Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected (يشتبه) problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Mesh disadvantages

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

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

Second, the sheer bulk (الحجم المطلق) of the wiring can be greater than the available space (in walls, ceilings (السقوف) , or floors (الارضيات)) can accommodate (يستوعب) .

Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive (باهظة التكلفة) .

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 (يرحل) the data to the other connected device.

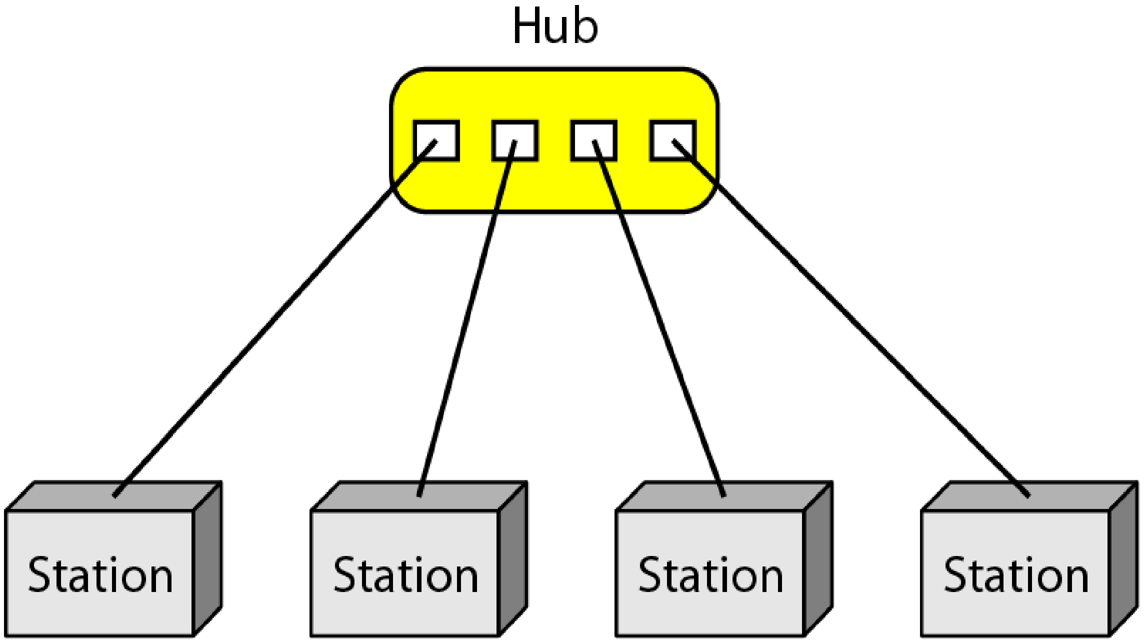


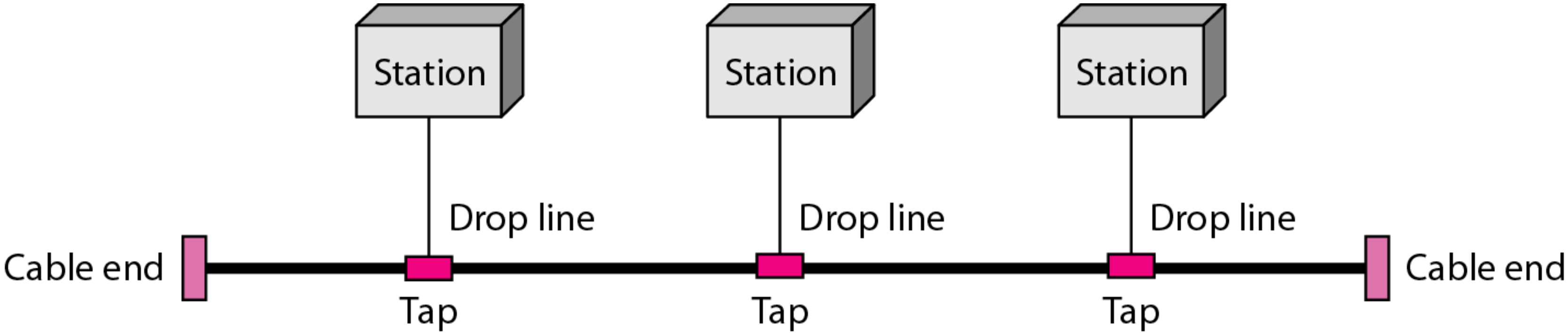
Figure 6 ***A star topology connecting four stations***

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

Disadvantages: One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

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 .



(حنفية، التقط الارسال، تنصت)

Figure 7 ***A bus topology connecting three stations***

Advantages of a bus topology include:

1. Ease of installation. Backbone cable can be laid (يوضع) along the most efficient path, then connected to the nodes by drop lines of various lengths.
2. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches (يمتد) through the entire facility (المرفق بكامله) . Each drop line has to reach only as far as (بقدر ما، الى حد) 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 (**حنفية، التقط الارسال، تنصت**) can cause degradation (تراجع) 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.

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 (يدمج، يمزج) a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Figure 8).

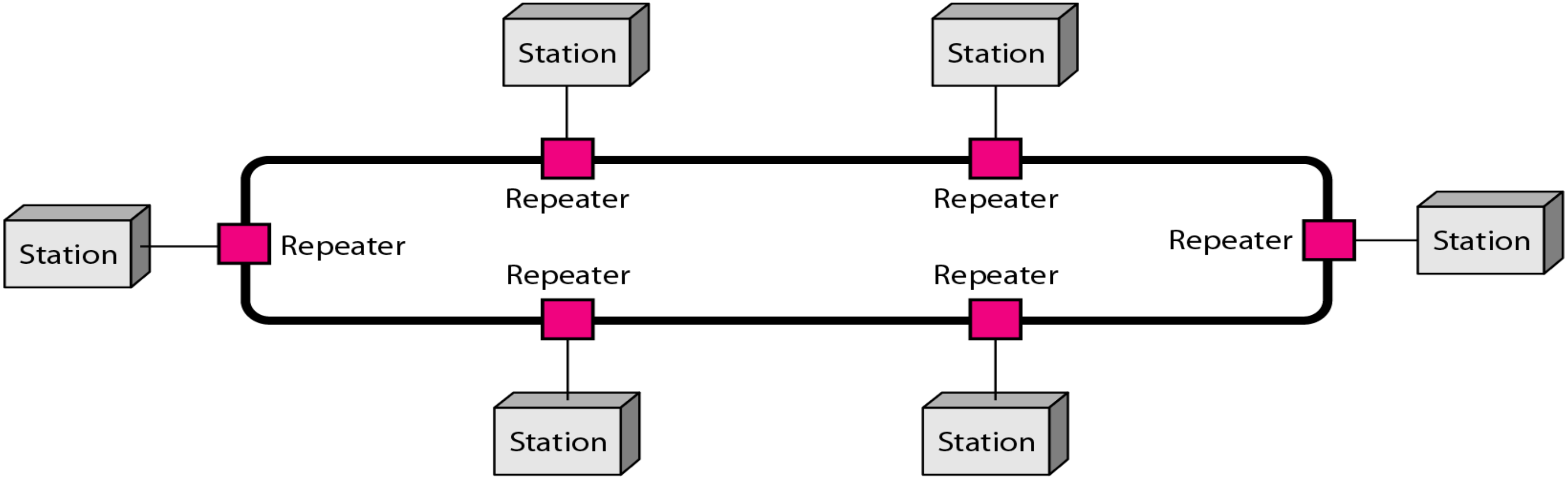
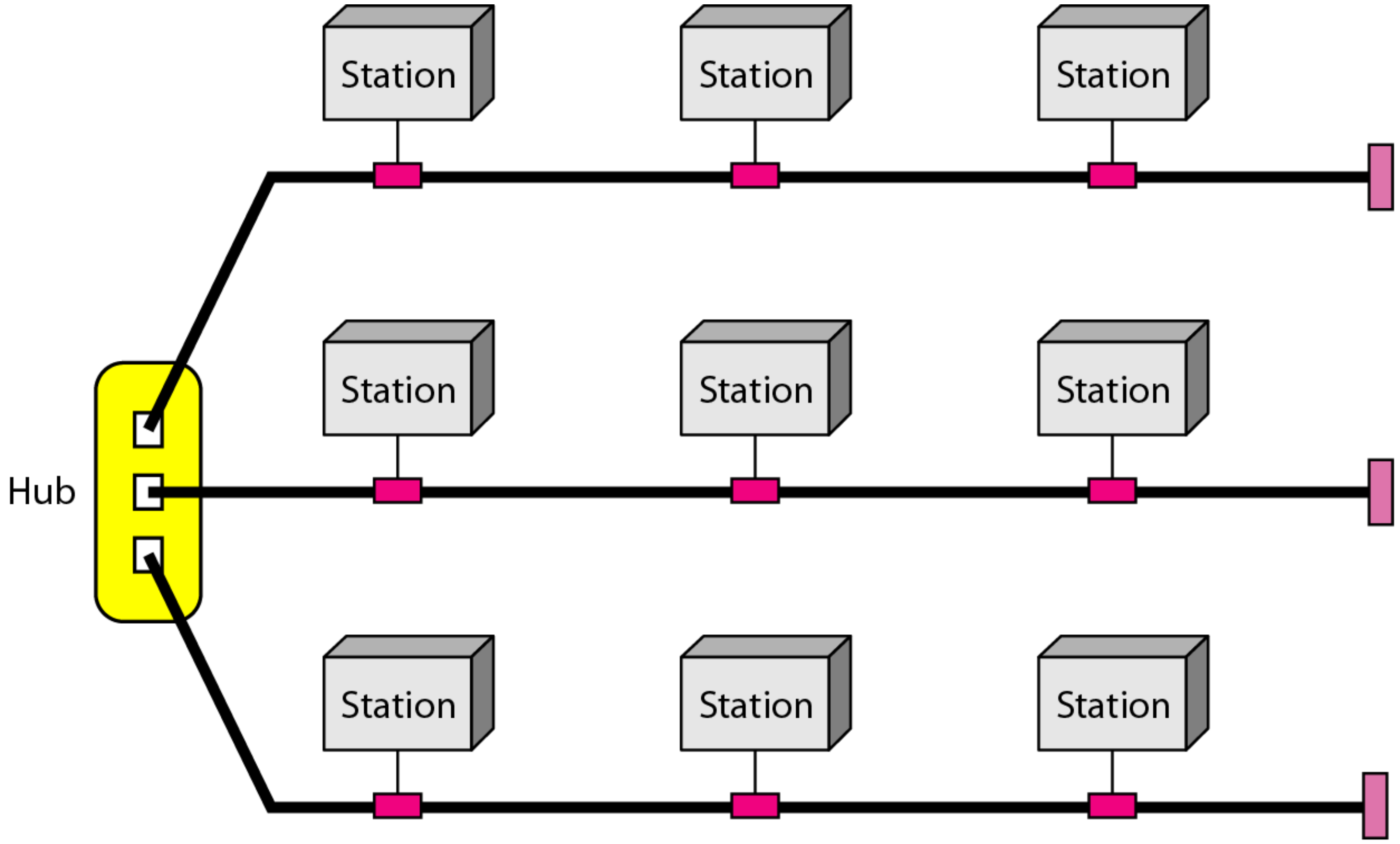


Figure 8 ***A ring topology connecting six stations***

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. 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.

Figure 9 *A hybrid topology: a star backbone with three bus networks*



NETWORK TYPES

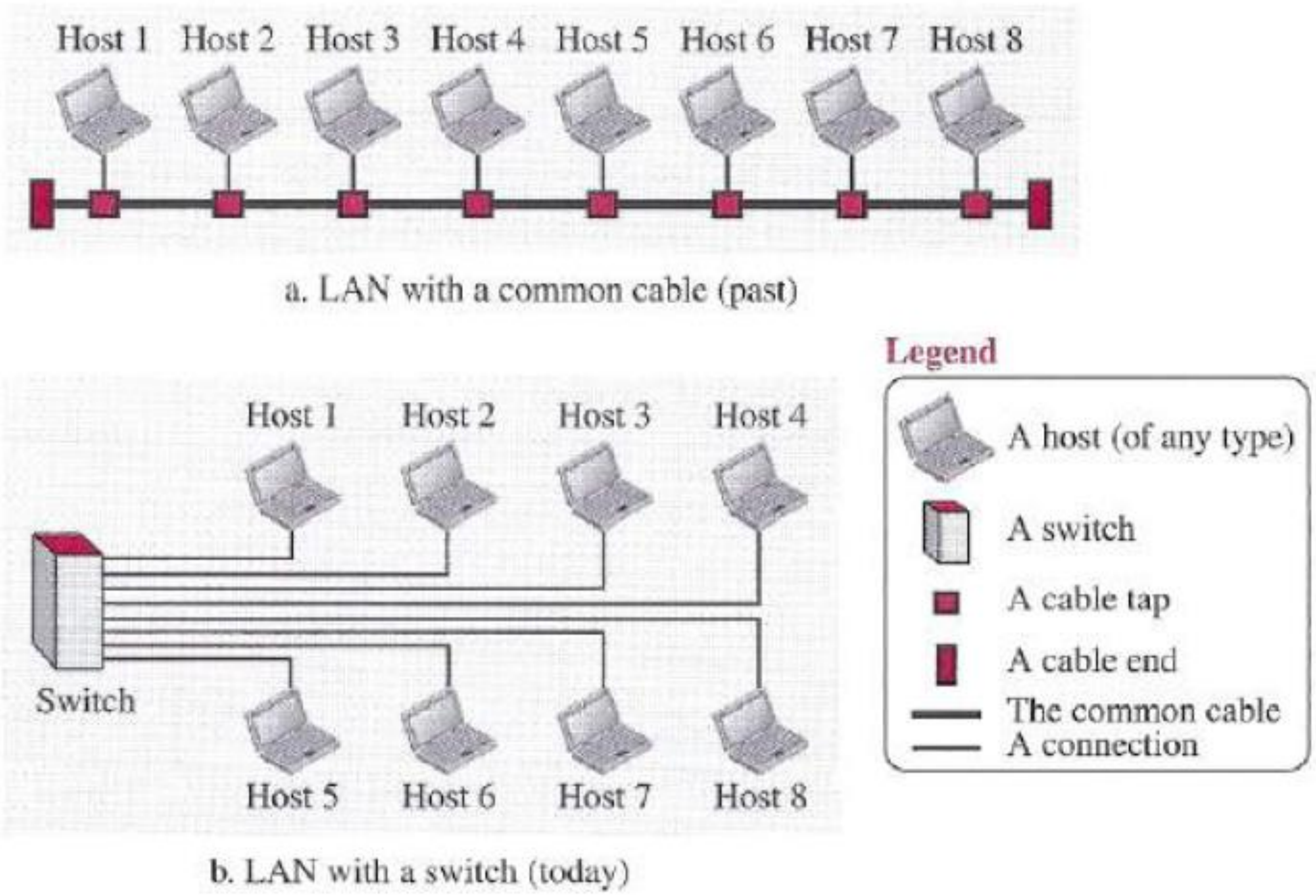
The criteria of distinguishing one type of network from another is difficult and sometimes confusing. We use a few criteria such as size, geographical coverage, and ownership to make this distinction.

1. Local Area Network

A **local area network** (LAN) is usually privately owned and connects some hosts in a single office, building, or campus. Depending on the needs of an organization, 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 devices.

In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet.

Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts.

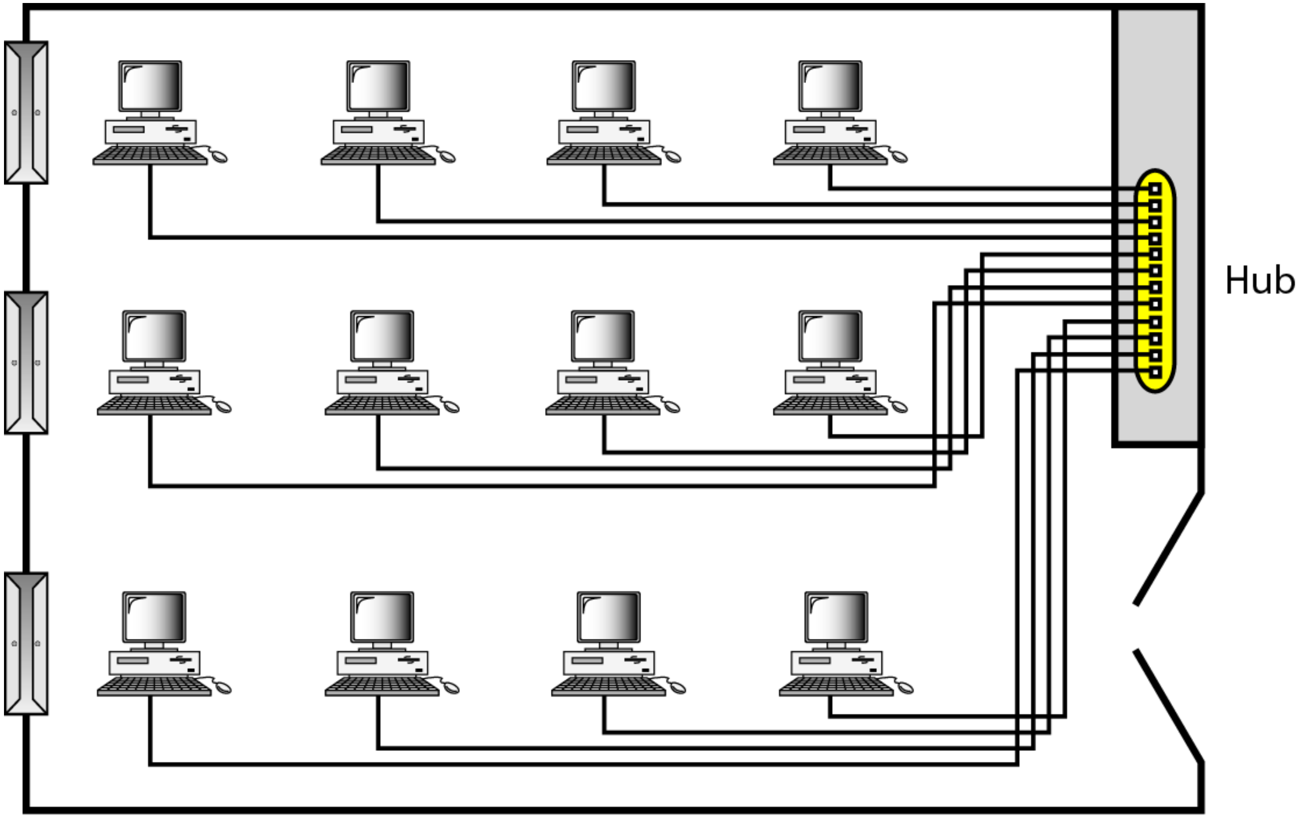


a. LAN with a common cable (past)

b. LAN with a switch (today)

Figure 10 *An isolated LAN in the past and today*

Figure 11 *An isolated LAN connecting 12 computers to a hub in a closet*



Wide Area Network (WAN)

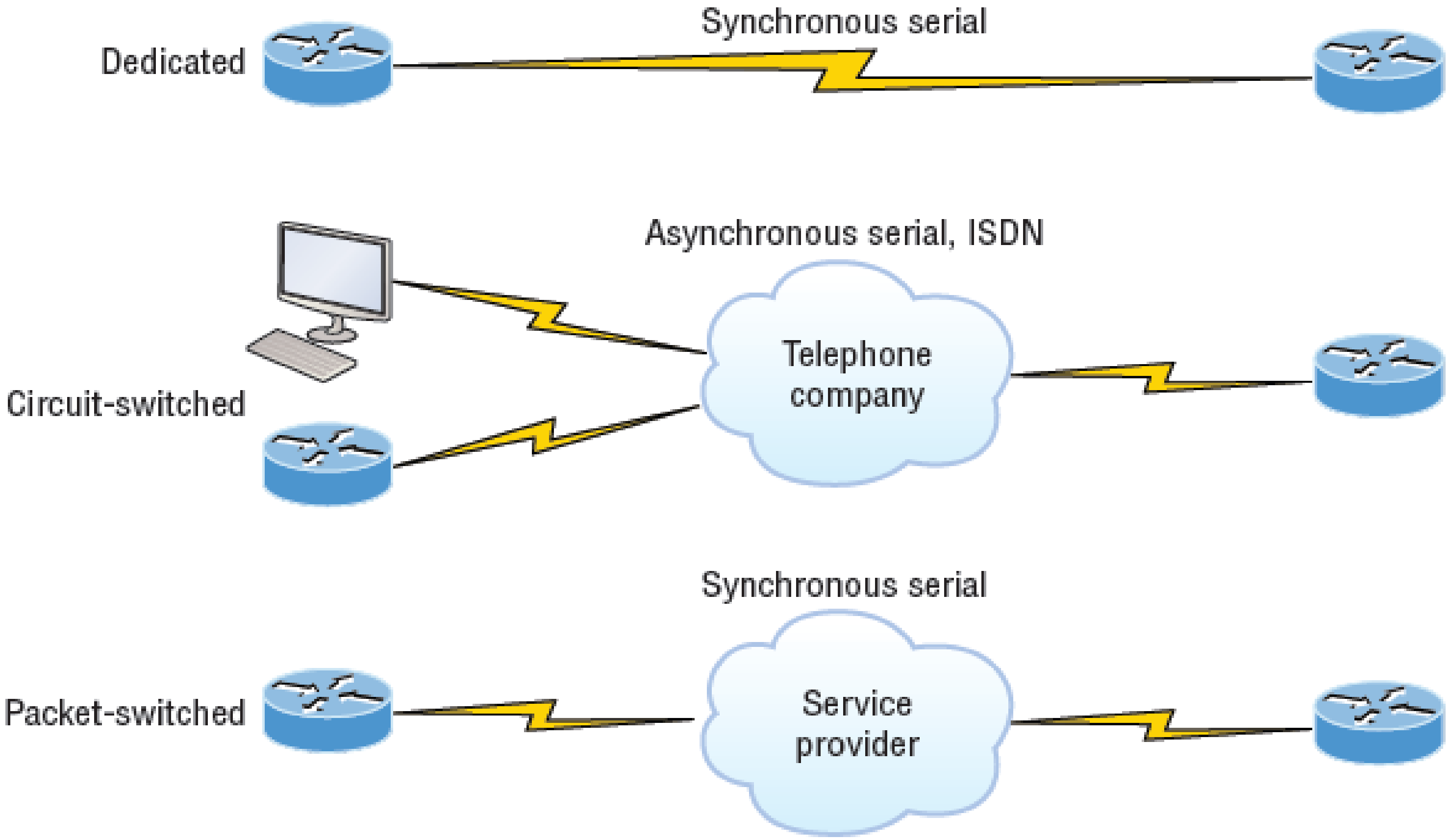
A wide area network (WAN) is also an interconnection of devices capable of communication.

However, there are some differences between a LAN and a WAN. A LAN is normally limited in size, spanning (يمتد) an office, a building, or a campus; a WAN has a wider geographical span, spanning a town, a state, a country, or even the world.

A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems.

A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.

Basically, there are various WAN connection types, such as Dedicated (leased lines), circuit switching and packet switching, as shown in the Figure below.
(**Integrated Services Digital Network (ISDN)**)



WAN connection types

Dedicated (leased lines) These are usually referred to as a *point-to-point* or dedicated connections. A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air). A *leased line* is a pre-established WAN communications path that goes from one device to another.

H.W.:

Explain some technologies that use point-to-point.

Circuit switching When you hear the term *circuit switching*, think phone call. The big advantage is cost. No data can transfer before an end-to-end connection is established. Circuit switching uses dial-up modems or **Integrated Services Digital Network** (**ISDN**) and is used for low-bandwidth data transfers.

H.W.:

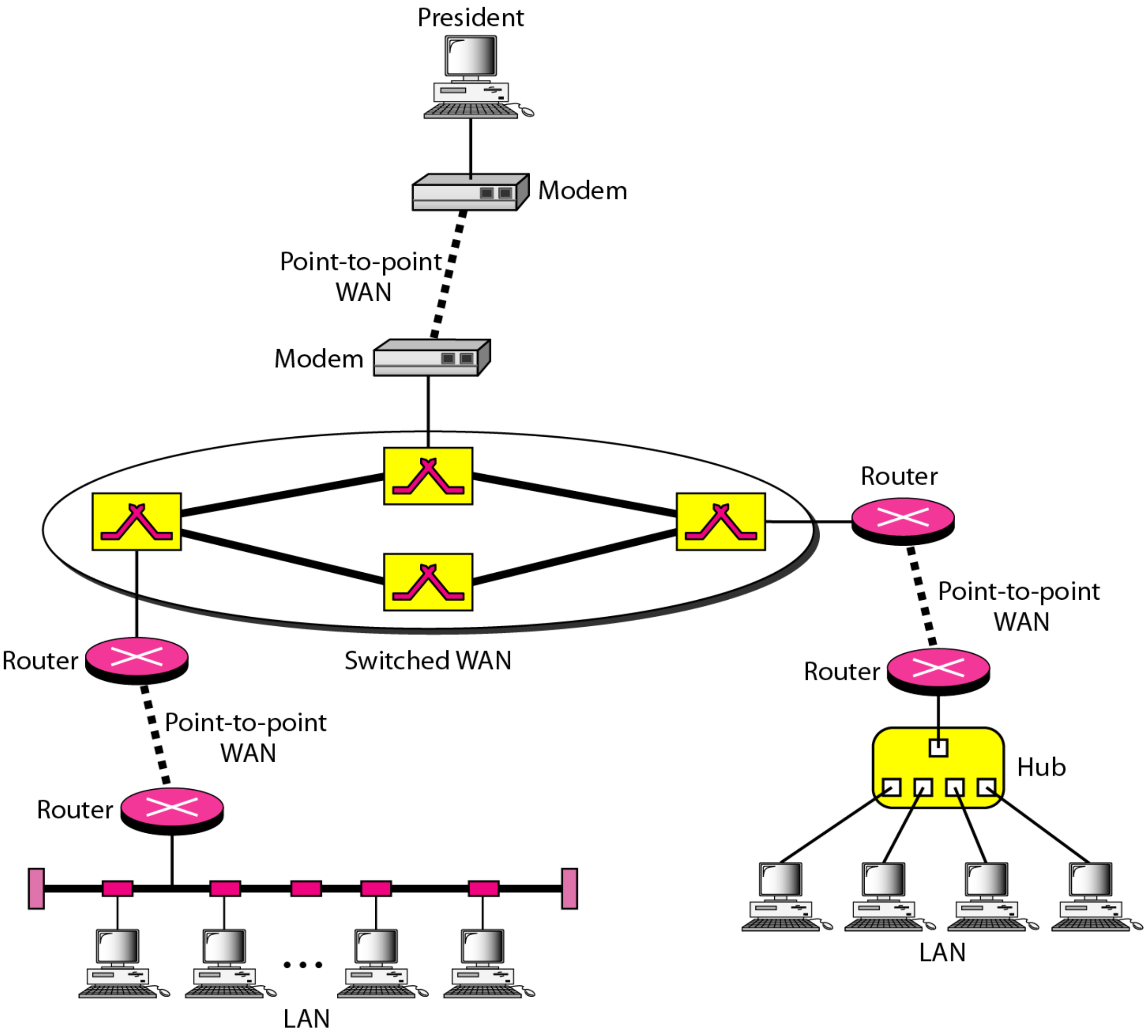
1. What are the modems? After all, with all the wireless technologies available, who would use a modem these days?
2. What is the ISDN? What are the newer WAN technologies that are used circuit switching.

Packet switching This is a WAN switching method that allows you to share bandwidth with other companies to save money. There’s definitely a serious downside to this technology. If you need to transfer data constantly, well, just forget about this option and get a leased line instead! Packet switching will only really work for you if your data transfers are bursty (انفجاري), not continuous..

H.W.:

Explain some technologies that use Packet switching.

Figure 12 *A heterogeneous (غير متجانس) network made of four WANs and two LANs*

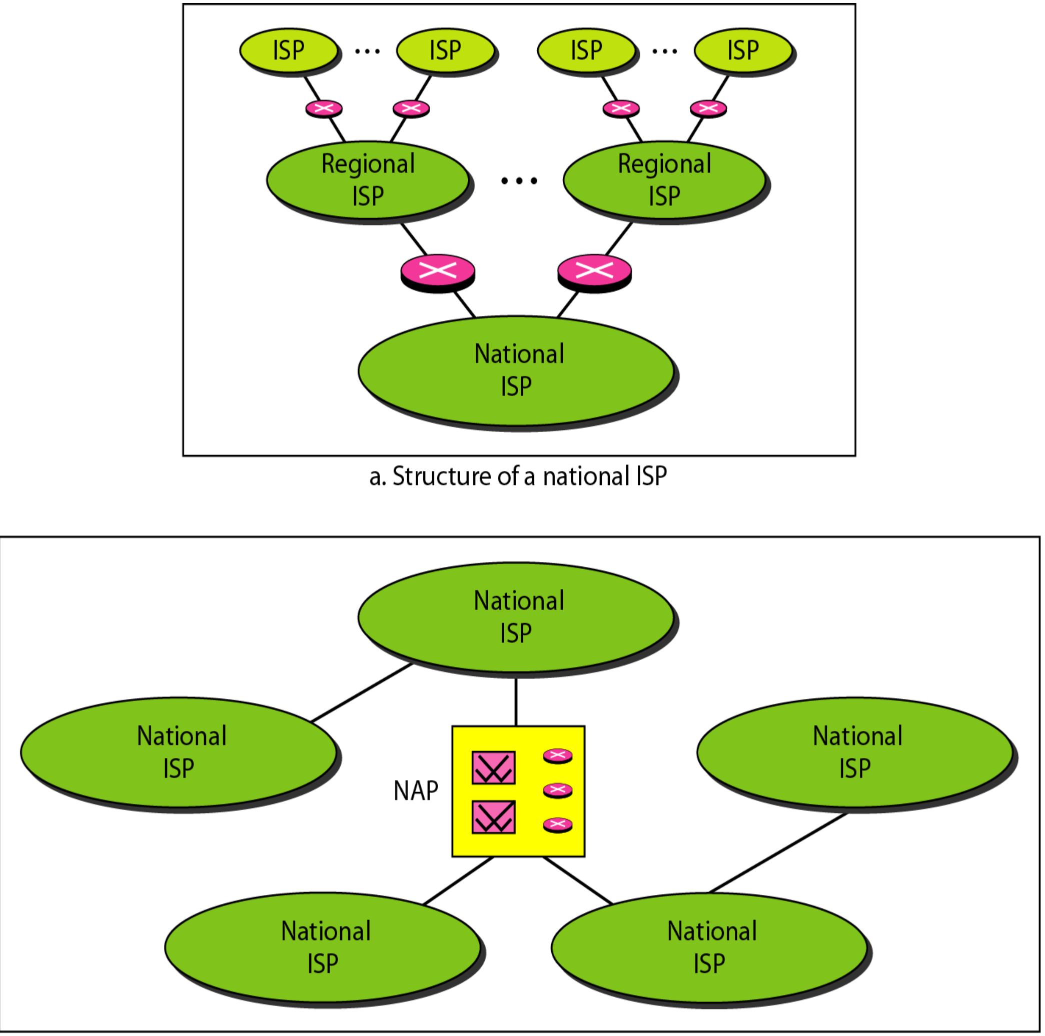


THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time (وقت الفراغ). The Internet is a communication system that has brought a wealth (ثروة) of information to our fingertips (طبعة الاصابع) and organized it for our use.

An internet is a network of networks. The Internet is a collection of many separate networks.

Figure 13 *Hierarchical organization of the Internet*



a. Structure of a national ISP

b. Interconnection of national ISPs

NAP (network access points): Short for network access point, a public network exchange facility where Internet Service Providers (ISPs) can connect with one another in peering (متناظر) arrangements. The NAPs are a key component of the Internet backbone because the connections within them determine how traffic is routed. They are also the points of most Internet congestion (اختناق).

PROTOCOLS AND STANDARDS

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* (بناء الجملة)**. 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* (دلالات الالفاظ)**. 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 (تنافسي) market for equipment manufacturers and in guaranteeing national and international interoperability (التوافق) of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors (الباعة), government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace (السوق التجارية) and in international communications.

Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention (عرف، تقليد)") and *de jure* (meaning "by law" or "by regulation").

o De facto (في الواقع). De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

o De jure (شرعي). Those standards that have been legislated (تشريع) by an officially recognized (معترف به رسميا) body are de jure standards.

Some example of standards:

o International Organization for Standardization (ISO).

o International Telecommunication Union-Telecommunication Standards Sector (ITU-T).

o American National Standards Institute (ANSI).

o Institute of Electrical and Electronics Engineers (IEEE).

o Electronic Industries Association (EIA).