NASARAWA STATE UNIVERSITY, KEFFI

FACULTY OF NATURAL AND APPLIED SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

COURSE TITLE: DATA COMMUNICATION/NETWORK

COURSE CODE: CMP 316

Course Lecturer
Y. Kefas

OUTLINE

At the end of this study, You Should be able to understand:

- **Data Communication(Communication Model).**
  - **Message**
  - **Sender**
  - **Receiver**
  - **Transmission Medium**
  - **Protocol**

OUTLINE

- **Data Representation**
  - Text
  - Images
  - Audio
  - Video

OUTLINE

- **Data Flow/Mode of Transmission**
  - Simplex
  - Half Duplex
  - Full Duplex
  - Broadcast
  - Multicast
- **Networks**
  - Distributed Processing
  - Network Criteria
  - Network Structures
  - Network Models
  - Network Categories
  - Network Interconnections

OUTLINE

- **Internet**
  - Internet History
  - The Internet today
- Protocols and Standards
  - Protocols
  - Standards
  - Standard Organizations

OUTLINE

- **Networking Models**
  - OSI Model.
  - Internet Model(TCP/IP)
- **Data and Signals**
  - **Analog Signals**
  - **Digital Signals**
- **Transmission Impairments**
  - Attenuation
  - Distortion
  - Noise
- **Data Rate Limit**
  - **Noiseless Channel**
  - **Noisy Channel**

OUTLINE

- **Network Performance**
  - **Bandwidth**
  - **Throughput**
  - **Latency (Delay)**
  - **Jitter**
- **Digital Transmission**
  - **Line Coding**
  - **Line Coding Schemes**
  - **Block Coding**

OUTLINE

- ❑ **Analog Transmission**
- ❑ **Transmission Media**
  - **Guided**
  - **Unguided**
- ❑ **Multiplexing**
- ❑ **IP ADRESSING**
- ❑ **Circuit Switching and Packet switch networks**
- ❑ **Error and Flow Control Mechanism**
- ❑ **Introduction to networking using Packet Tracer**

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
Data Representation
Data Flow

Figure 1.1 *Five components of data communication*

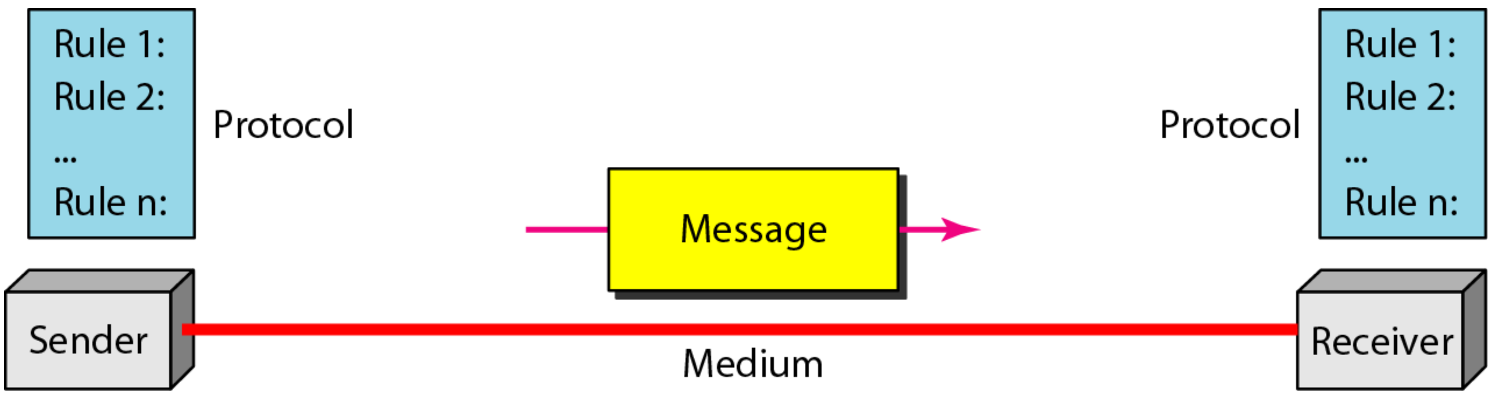


Figure 1.1 *Five components of data communication*

1.Message

Message is the information to be communicated by the sender to the receiver.

2.Sender

The sender is any device that is capable of sending the data (message).

3.Receiver

The receiver is a device that the sender wants to communicate the data (message).

4.Transmission Medium

It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.

Figure 1.1 *Five components of data communication*

5. Protocol

It is an agreed upon set or rules used by the sender and receiver to communicate data.

A protocol is a set of rules that governs data communication. A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language.

Data Representation

Text

Image

Sound

Video

Data Representation

- Data is collection of raw facts which is processed to deduce information.
- There may be different forms in which data may be represented. Some of the forms of data used in communications are as follows:

1. **Text**
   - Text includes combination of alphabets in small case as well as upper case.
   - It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode

Data Representation

2. **Numbers**

- Numbers include combination of digits from 0 to 9.
- It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode

3. **Images**

- ―An image is worth a thousand words‖ is a very famous saying. In computers images are digitally stored.
- A Pixel is the smallest element of an image. To put it in simple terms, a picture or image is a matrix of pixel elements.
- The pixels are represented in the form of bits. Depending upon the type of image (black n white or color) each pixel would require different number of bits to represent the value of a pixel.

Data Representation

Images

- The size of an image depends upon the number of pixels (also called resolution) and the bit pattern used to indicate the value of each pixel.
- Example: if an image is purely black and white (two color) each pixel can be represented by a value either 0 or 1, so an image made up of 10 x 10 pixel elements would require only 100 bits in memory to be stored.
- On the other hand an image that includes gray may require 2 bits to represent every pixel value (00 - black, 01 – dark gray,
- 10– light gray, 11 –white). So the same 10 x 10 pixel image would now require 200 bits of memory to be stored.
- Commonly used Image formats : jpg, png, bmp, etc

Data Representation

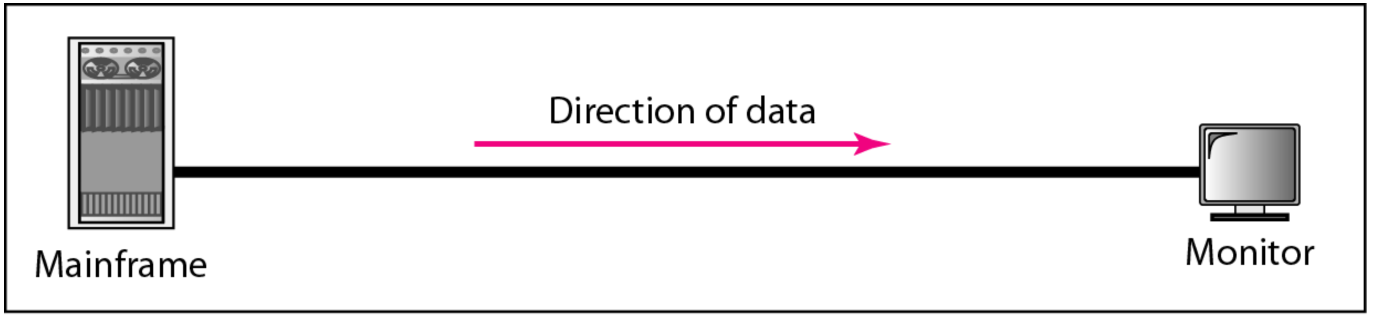
4. Audio

- Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information.
- Audio data is continuous, not discrete.

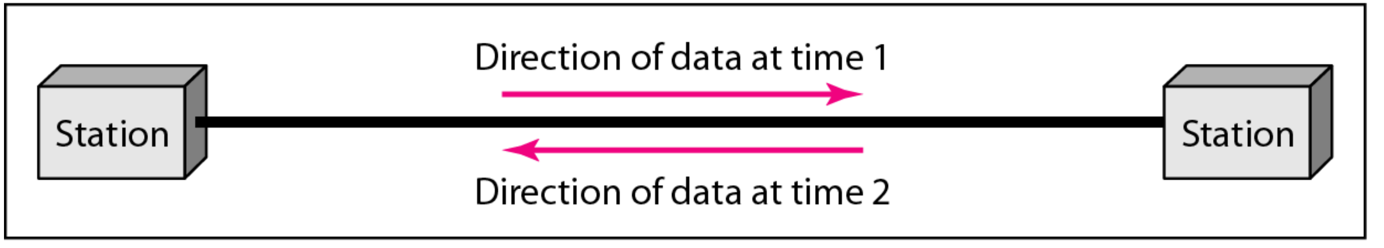
5. Video

- Video refers to broadcasting of data in form of picture or movie

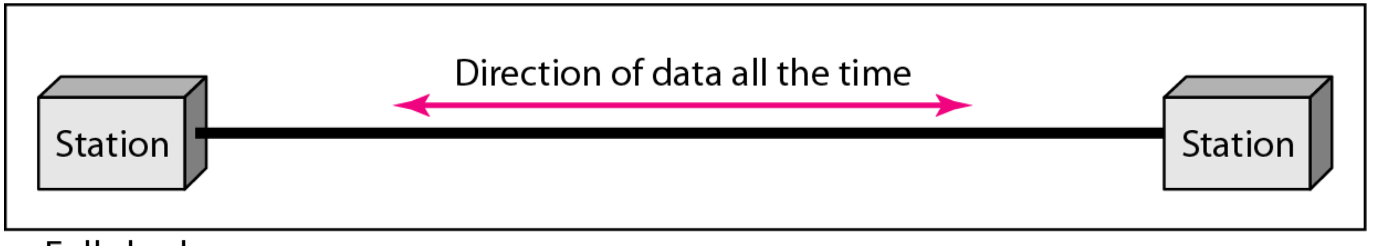
Figure 1.2 *Data flow (simplex, half-duplex, and full-duplex)*



a. Simplex



b. Half-duplex



c. Full-duplex

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.

Topics discussed in this section:

Distributed Processing
Network Criteria
Physical Structures
Network Models
Categories of Networks
Interconnection of Networks: Internetwork

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.

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
    - Type of transmission medium
    - Capabilities of the connected hardware, and
    - Efficiency of the software.

Network Criteria Cont'd

- Performance is often evaluated by two networking metrics:
  - ❖ **Throughput:** the amount of data or raw material that is processed over a given period
  - ❖ **Delay:** Failure of data to be delivered at the expected time

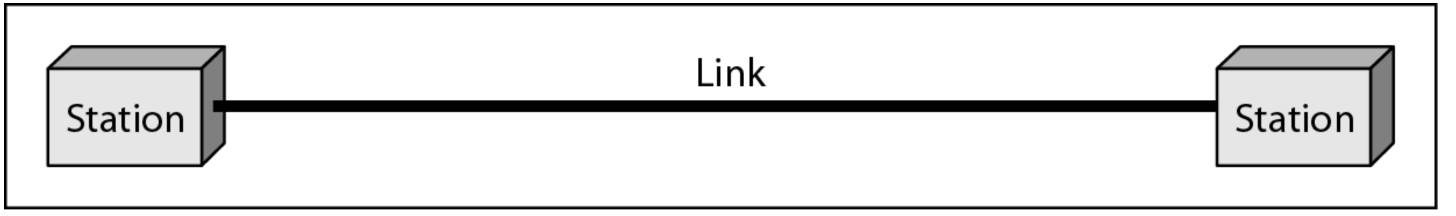
- ***Reliability***

  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.

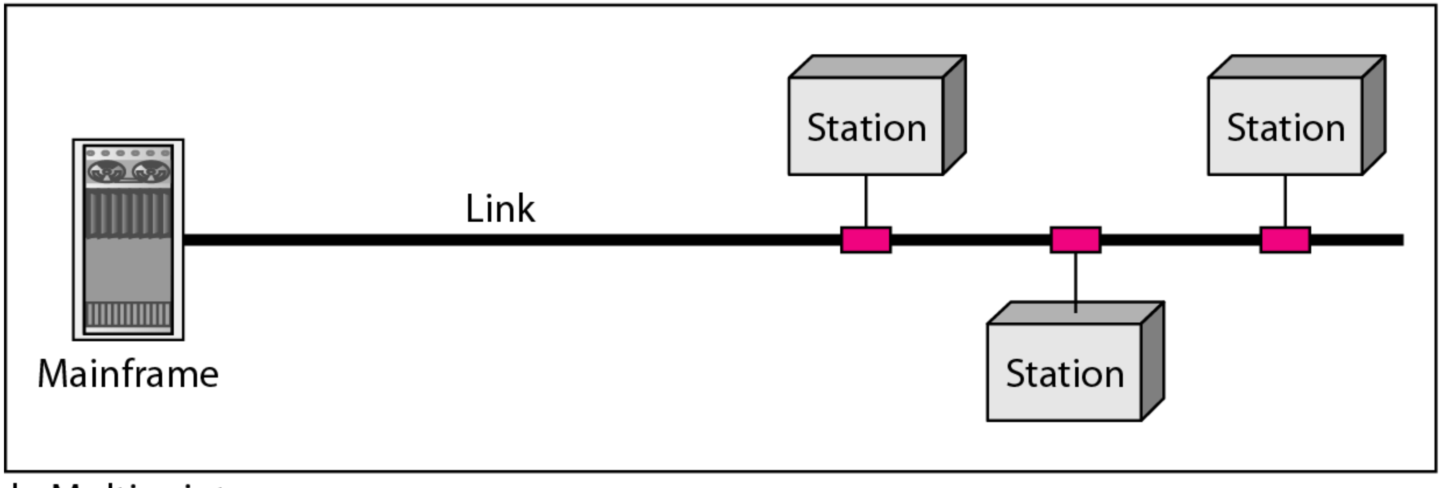
- ***Security***

  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.

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



a. Point-to-point



b. Multipoint

Figure 1.4 *Categories of topology*

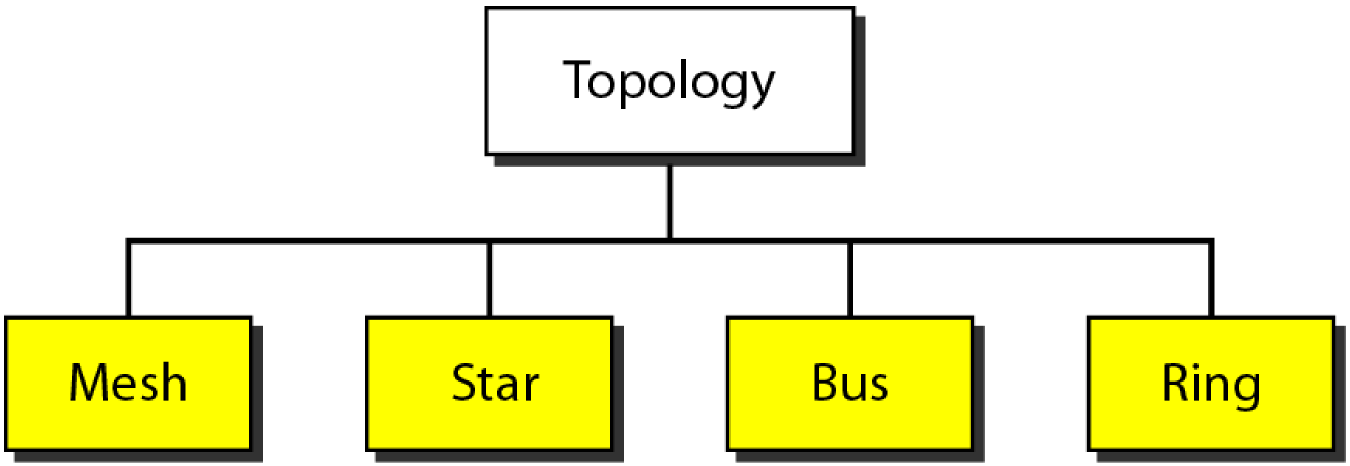
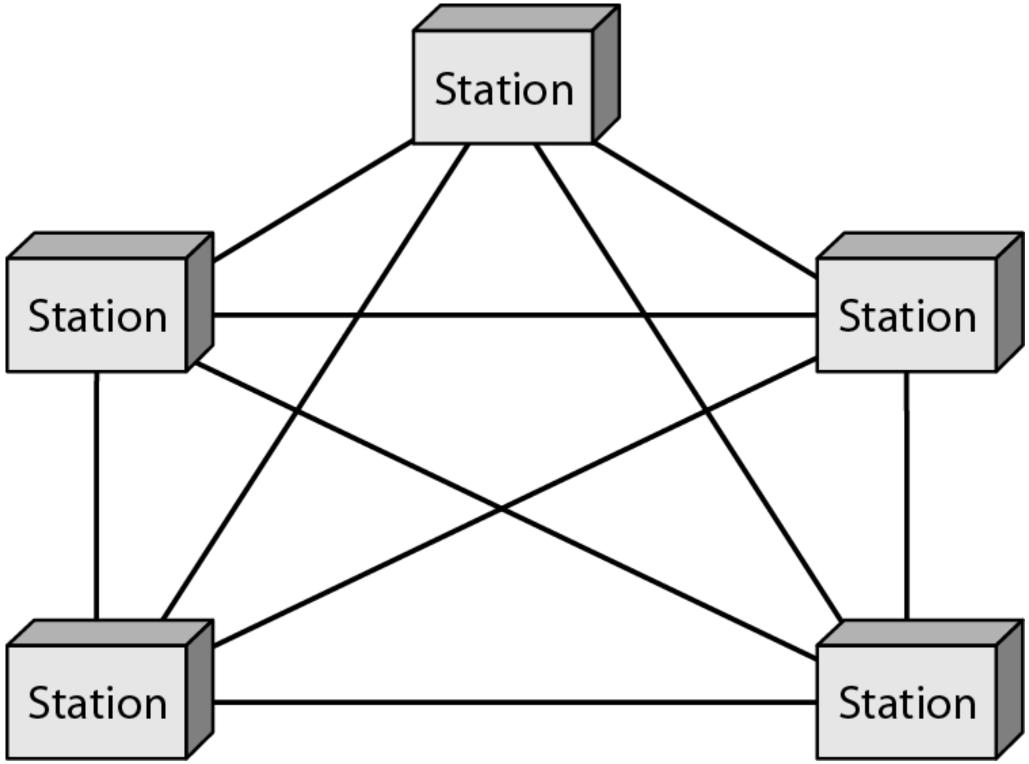


Figure 1.5 *A fully connected mesh topology (five devices)*



For physical link allowing communications in both directions with n nodes, we have $\frac{n(n-1)}{2}$ duplex- mode links

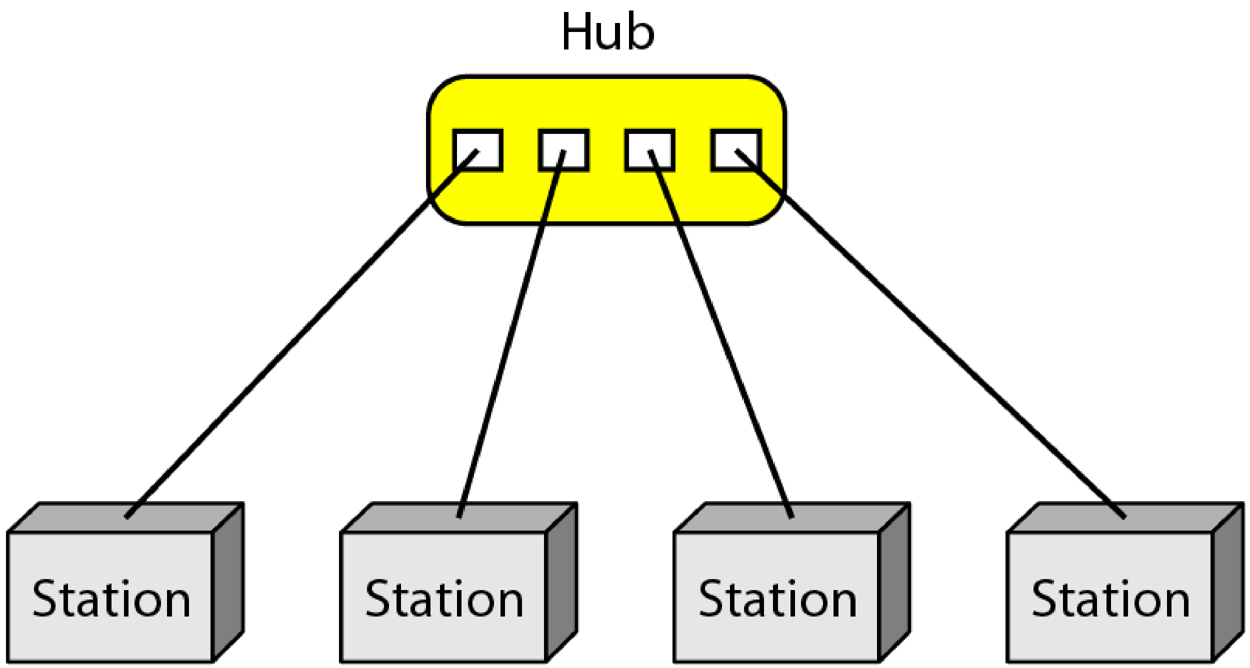
Advantages of Mesh a Topology

- Dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system
- There is the advantage of privacy or security
- Point-to-point links make fault identification and fault isolation easy

Disadvantages of Mesh a Topology

- Because every device must be connected to every other device, installation and reconnection are difficult
- The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive, thus, it is implemented in a limited fashion such as a backbone connecting the main computers of a hybrid network that can include several other topologies e.g. regional offices in which each regional office needs to be connected to every other regional office.

Figure 1.6 *A star topology connecting four stations*



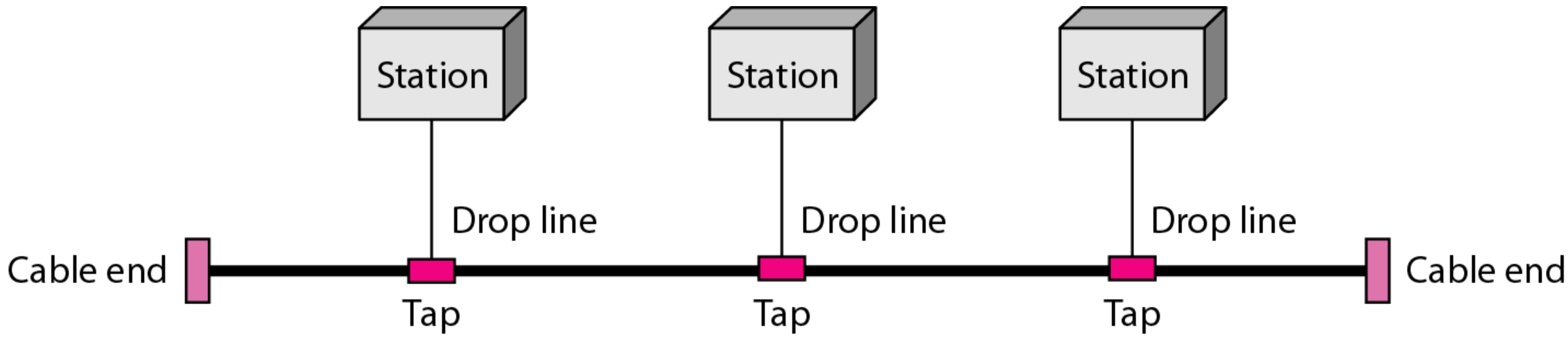
Advantages of a Star Topology

- A star topology is less expensive than a mesh topology
- 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.
- It is robust. If one link fails, only that link is affected. All other links remain active
- This factor also lends itself to easy fault identification and fault isolation.
- As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages of a Star Topology

- 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), and High-speed LANs use a star topology with a central hub.

Figure 1.7 *A bus topology connecting three stations*



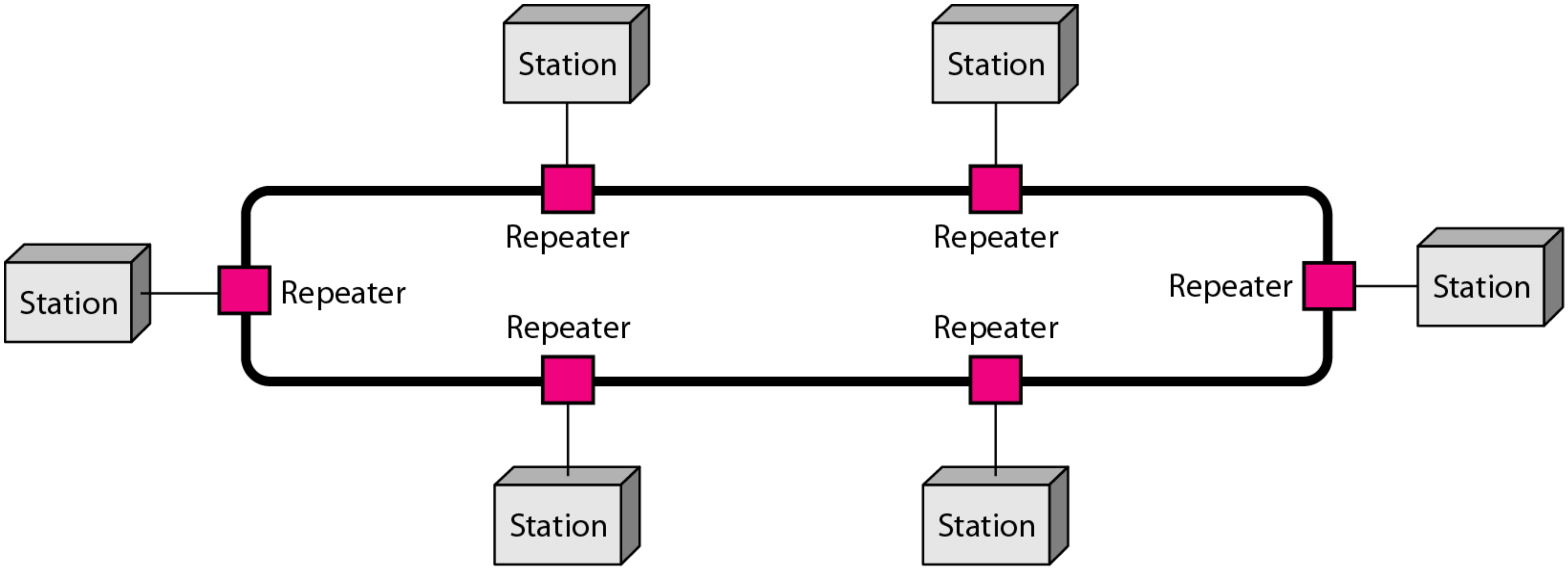
Advantages of a Bus Topology

- Easy 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 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 which is not case in star topology

Disadvantages of a Bus Topology

- 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.
- 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. Ethernet LANs can use a bus topology

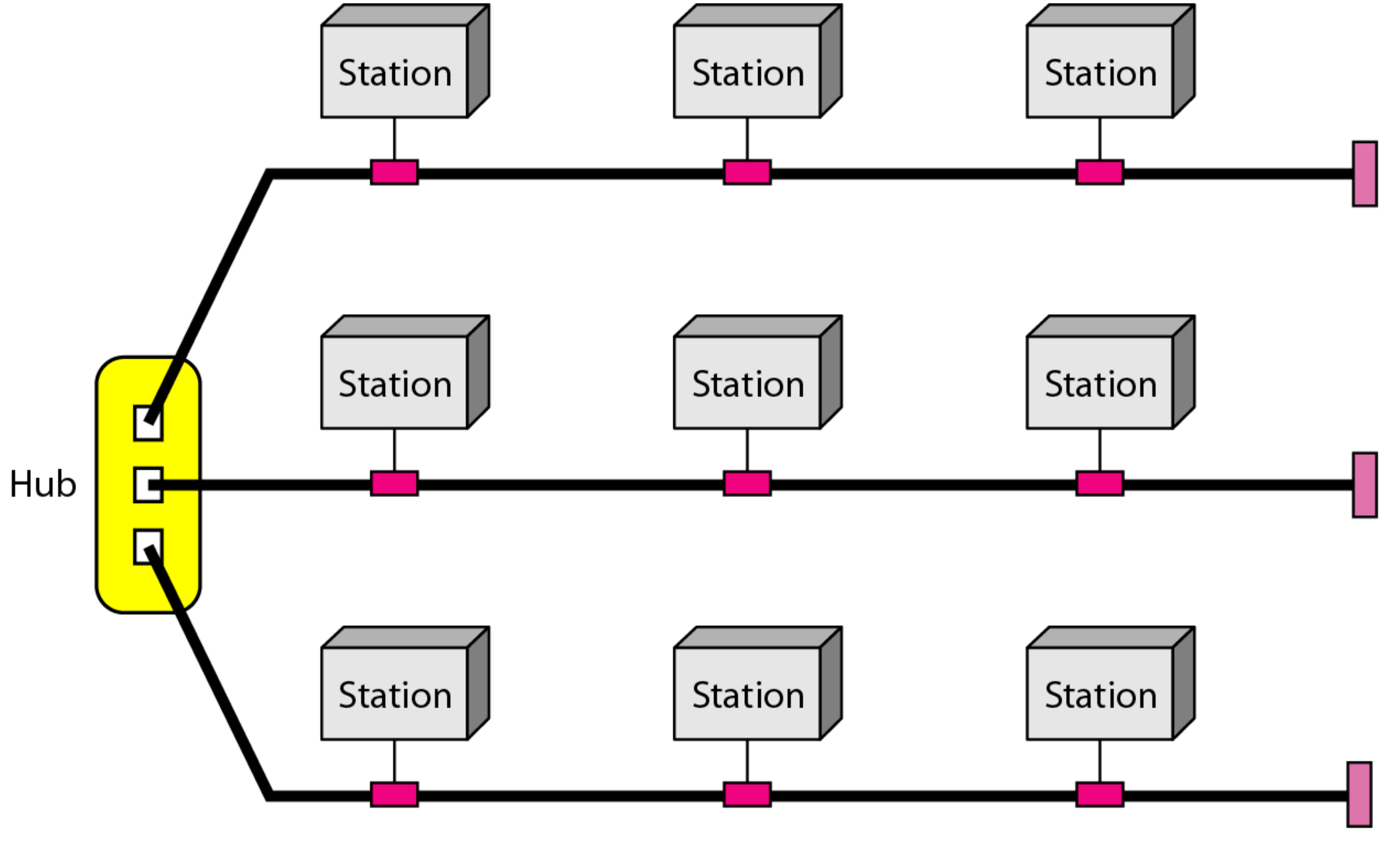
Figure 1.8 *A ring topology connecting six stations*



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.

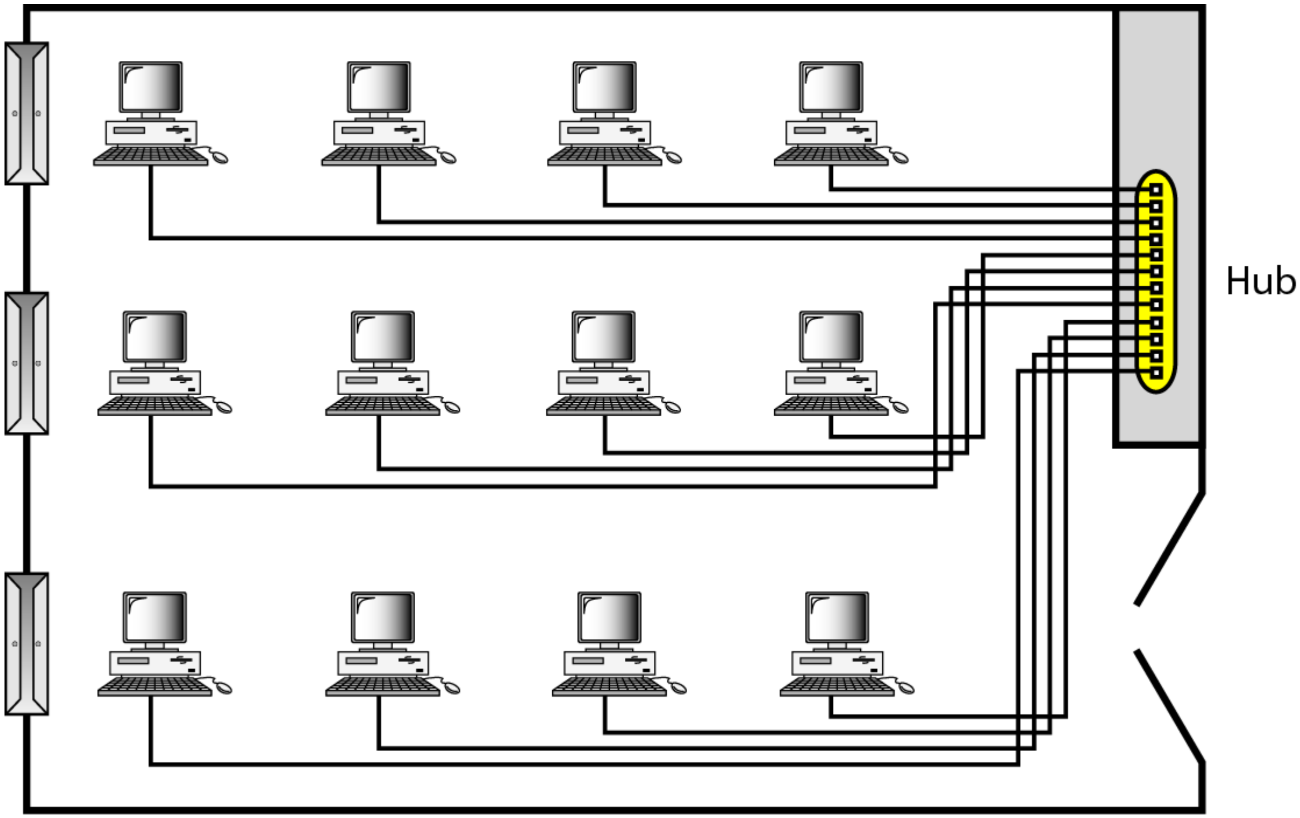
Figure 1.9 *A hybrid topology: a star backbone with three bus networks*



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 above.

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



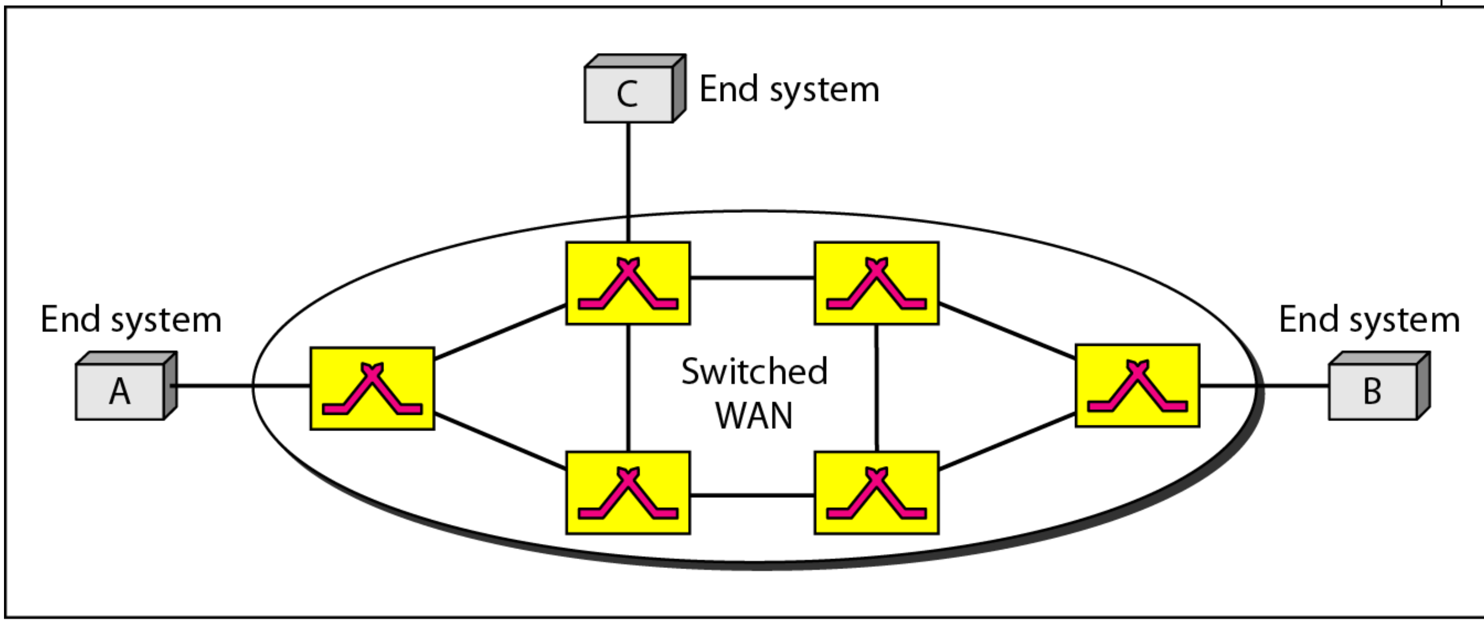
Categories of Networks Cont'd

- There are two primary categories of Networks:
  - **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.

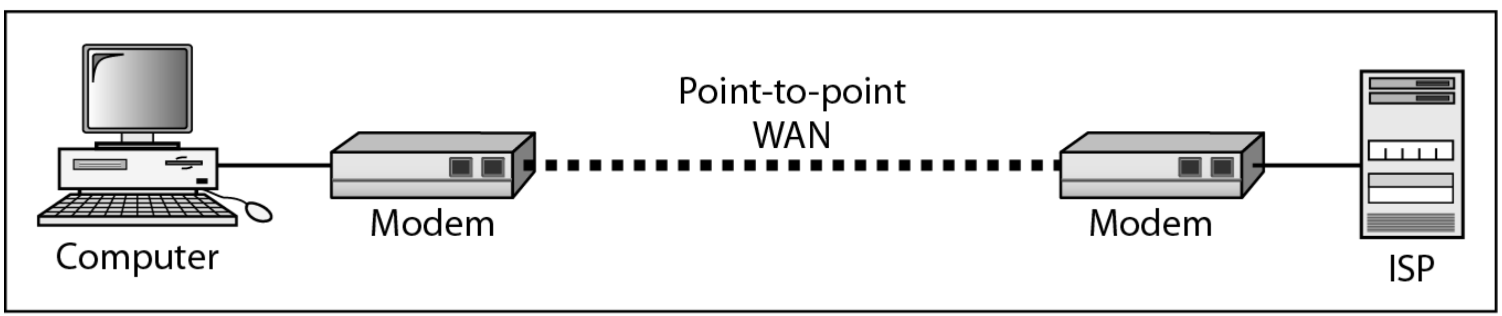
Categories of Networks: Local Area Network (LAN)

- LAN is usually privately owned and links the devices in a single office, building, or campus.
- 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.
- 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.

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



a. Switched WAN

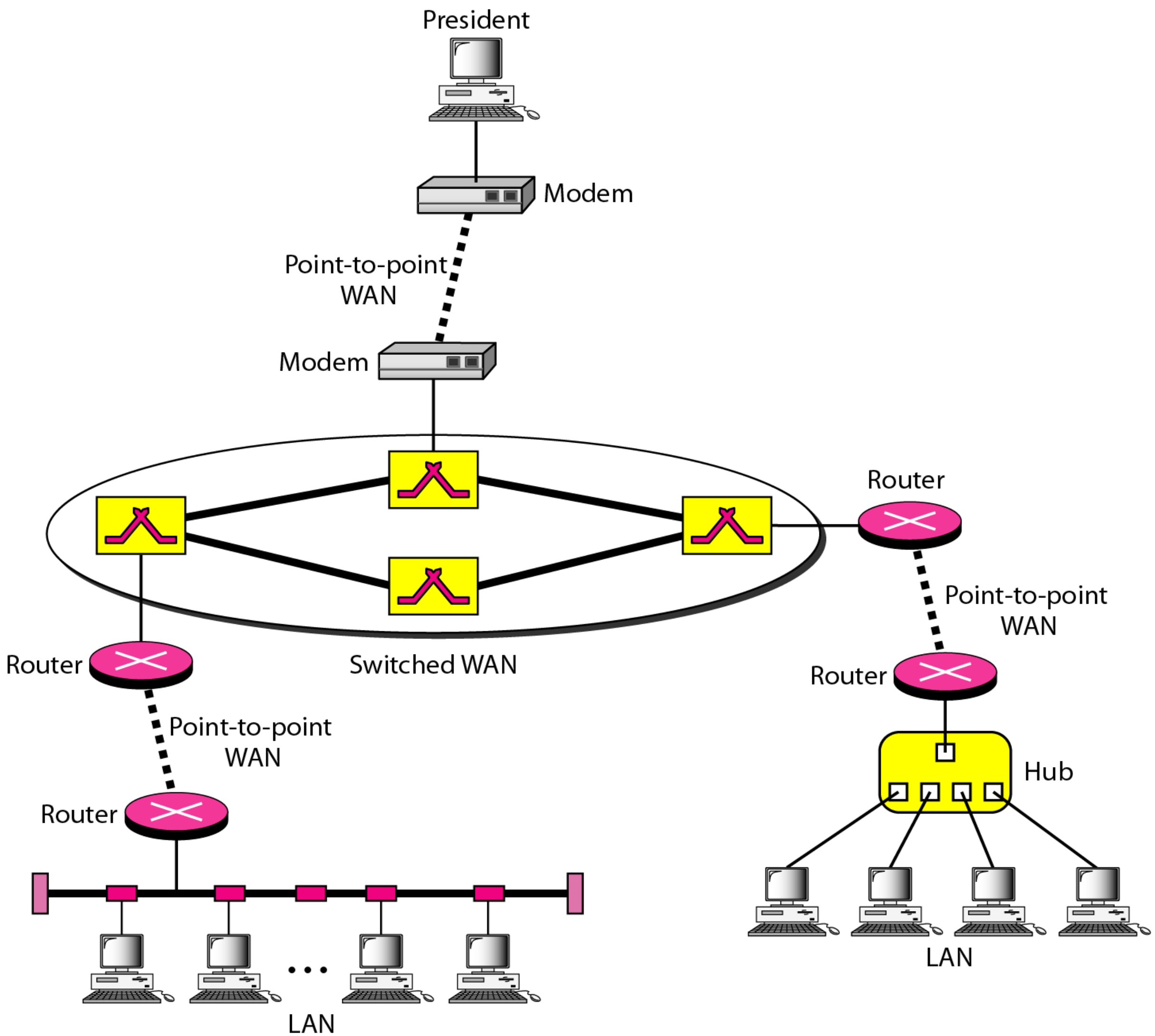


b. Point-to-point WAN

Categories of Networks: Wide Area Network (WAN)

- A 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 (switched WAN).
- 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 (point-to-point WAN).
- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP).

Figure 1.12 *A heterogeneous network made of four WANs and two LANs*



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.

Network Models

- Computer networks are created by different entities.
- Standards are needed so that these heterogeneous networks can communicate with one another.

The two best-known standards are the:

- OSI model(Physical, Datalink, Network, Transport, Session, Presentation and Application)
- The Internet model.

1-3 THE INTERNET

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

Topics discussed in this section:

A Brief History
The Internet Today (ISPs)

A Brief History

- *The Internet came in to being in the 1969*
- In the mid-1960s, mainframe computers in research organizations were standalone devices
- The Advanced Research Projects Agency (ARPA) in the Department of Defence (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.
- In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.

A Brief History Cont'd

- The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface message processor* (IMP).
- The IMPs, in turn, would be connected to one another.
- Each IMP had to be able to communicate with other IMPs as well as with its own attached host.
- By 1969, ARPANET was a reality
- Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network.

A Brief History Cont'd

- Software called the *Network Control Protocol* (NCP) provided communication between the hosts.
- In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Project1.*
- Cerf and Kahn's landmark (1973) paper outlined the protocols to achieve end-to-end delivery of packets.
- This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

A Brief History Cont'd

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

The Internet Today (ISPs)

- The Internet today is not a simple hierarchical structure.
- It is made up of many wide- and local-area networks joined by connecting devices and switching stations.
- The Internet is continually changing.
- New networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.
- Today most end users who want Internet connection use the services of Internet service providers (ISPs).

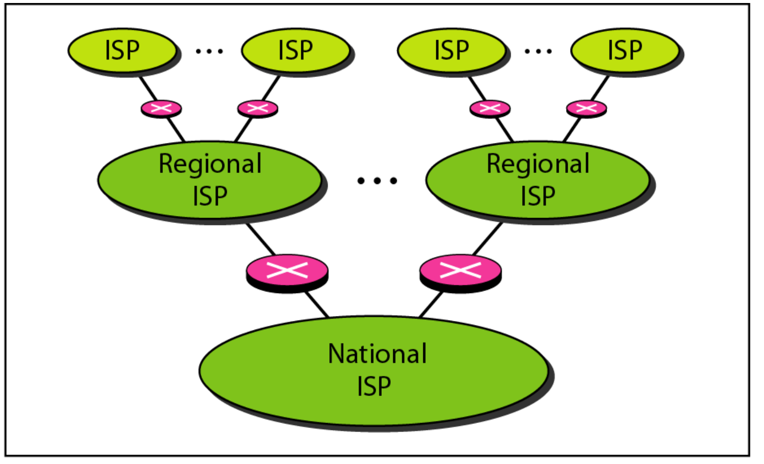
The Internet Today (ISPs)

- There are:
  - International service providers
  - National service providers
  - Regional service providers and
  - Local service providers.
- The Internet today is run by private companies, not the government

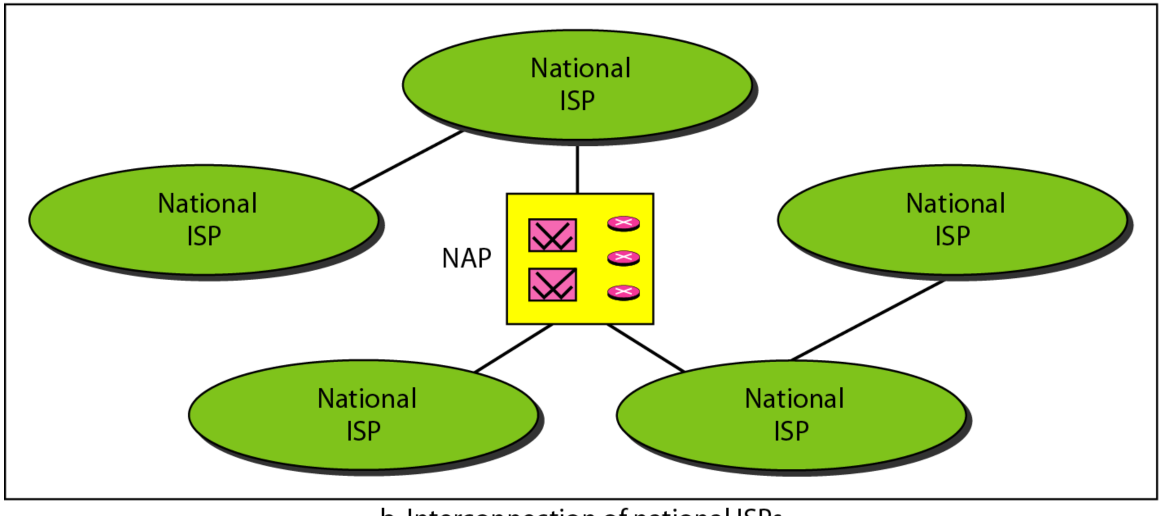
The Internet Today (ISPs)

- *International Internet Service Providers* are the international service providers that connect nations together.
- *National Internet Service Providers* are backbone networks created and maintained by specialized companies.
- *Regional Internet Service Providers* are smaller ISPs that are connected to one or more national ISPs.
- *Local Internet Service Providers* provide direct service to the end users.

Figure 1.13 *Hierarchical organization of the Internet*



a. Structure of a national ISP



b. Interconnection of national ISPs

1-4 PROTOCOLS AND STANDARDS

In this section, we define two widely used terms: protocols and standards. First, we define protocol, which is synonymous with rule. Then we discuss standards, which are agreed-upon rules.

Topics discussed in this section:

Protocols
Standards
Standards Organizations
Internet Standards

PROTOCOLS

- *Protocol is synonymous with rule*
- For communication to occur, the entities must agree on a protocol.
- An entity is anything capable of sending or receiving information.
- The key elements of a protocol are:
  - syntax
  - semantics and
  - timing.
- *Syntax* refers to the structure or format of the data, meaning the order in which they are presented
- *Semantics* refers to the meaning of each section of bits.
- *Timing* refers to two characteristics:
  - when data should be sent and
  - how fast they can be sent

STANDARDS

- *Standards are agreed-upon rules*
- 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 are standards that have not been approved by an organized body but have been adopted as standards through widespread use.
- De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
- De jure standards are those standards that have been legislated by an officially recognized body

Standards Organizations

- ❑ Standards are developed through the cooperation of:
  - ➢ Standards creation committees
  - ➢ Forums and
  - ➢ Government regulatory agencies.
- ❑ *Standards Creation Committees*
- ❑ International Organization for Standardization (ISO) is active in developing cooperation in the realms of scientific, technological, and economic activity.
- ❑ International Telegraphy and Telephony (CCITT) was devoted to research and establishment of standards for telecommunications in general and for phone and data systems in particular.
- ❑ International Telecommunication Union-Telecommunication Standards Sector (ITU-T) which was formally CCIT is a standard for communication

Standards Organizations

- American National Standards Institute (ANSI), despite its name, it is a completely private, non-profit corporation not affiliated with the U.S. federal government.
  - However, all it's activities are undertaken with the welfare of the United States and its citizens occupying primary importance
- Institute of Electrical and Electronics Engineers (IEEE) is the largest professional engineering society in the world.
  - It oversees the development and adoption of international standards for computing and communications.
- Electronic Industries Association (EIA) is Aligned with ANSI
  - It is a non-profit organization devoted to the promotion of electronics manufacturing concerns.

Forums

- **Forums** made up of representatives from interested corporations.
  - It works with universities and users to test, evaluate, and standardize new technologies

Regulatory Agencies

- All communications technology is subject to regulation by government agencies such
as the **Federal Communications Commission** (FCC) in the United States and **National Communications Commission (NCC)** in Nigeria.
  - The purpose of these agencies is to protect the public interest by regulating:
    - radio
    - television and
    - wire/cable communications.
- The FCC has authority over interstate and international commerce as it relates to communications

Internet Standards

- An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet.
- There is a strict procedure by which a specification attains Internet standard status.
- A specification begins as an Internet draft.
- An **Internet draft** is a working document (a work in progress) with no official status and a 6-month lifetime.
- Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment** (RFC).
- Each RFC is edited, assigned a number, and made available to all interested parties.
- RFCs go through maturity levels and are categorized according to their requirement level.

Chapter 2

Network Models

OBJECTIVES

- Internet layering model
- Function of each Layers
- OSI Model

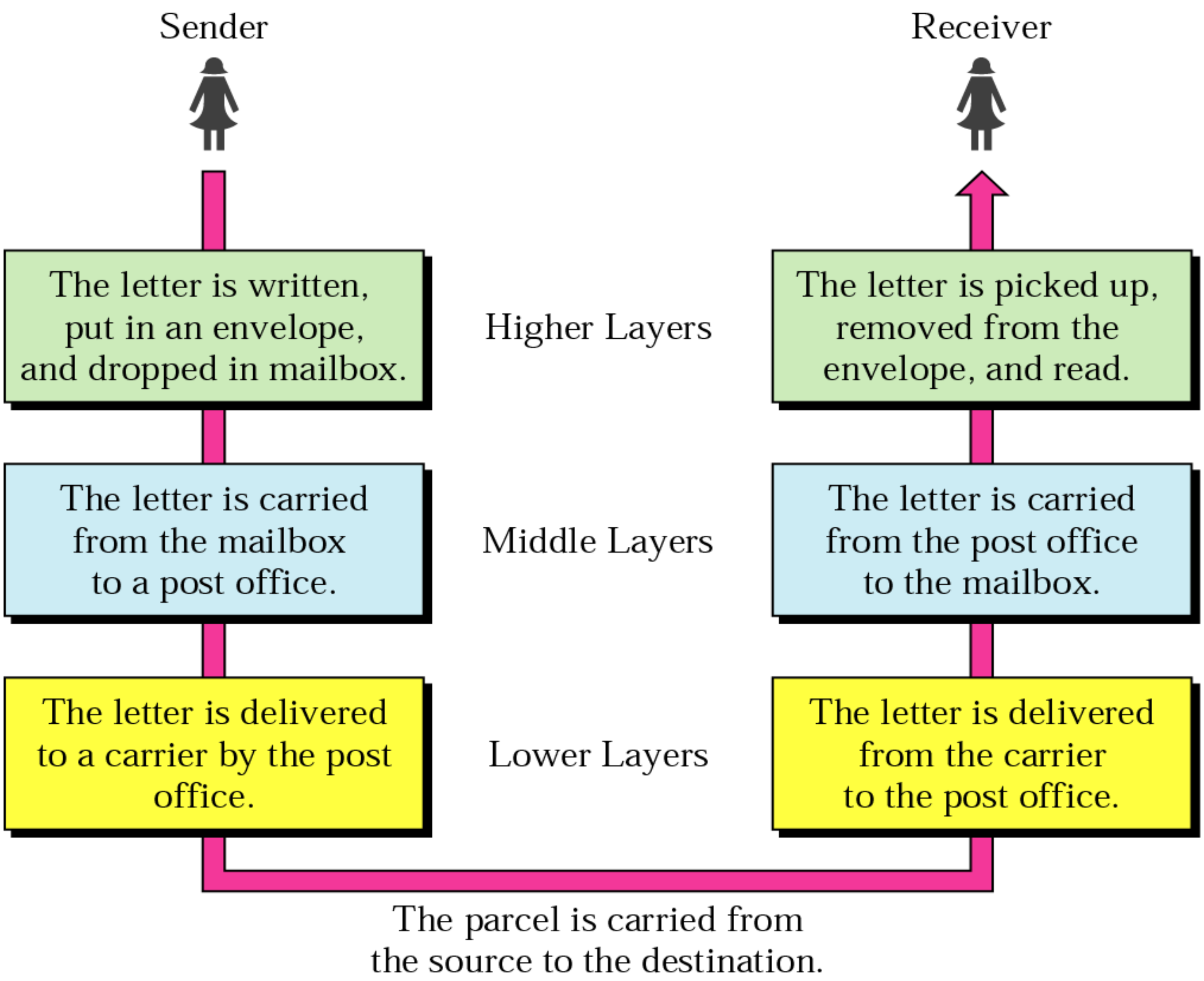
2.1 Layered Tasks

Sender, Receiver, and Carrier

Work must be done Hierarchically

Services: Use services of the layer immediately below it

Layer Task (Sending a Letter)



2.2 Internet Model

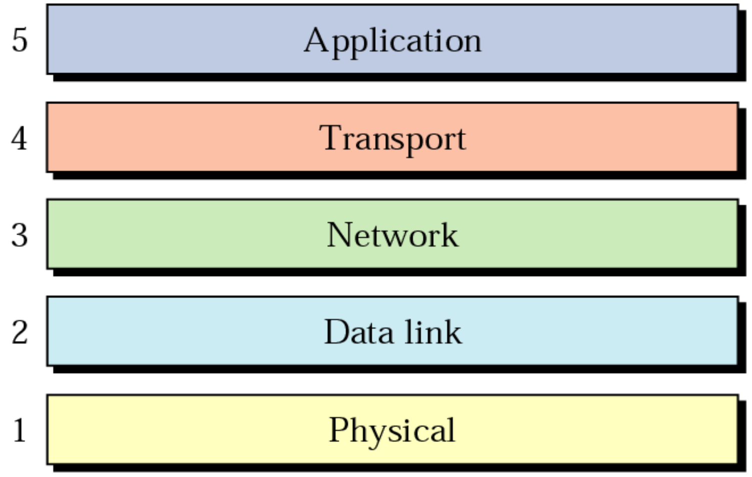
Peer-to-Peer Processes

Functions of Layers

Summary of Layers

Figure 2.2 ***Internet layers***

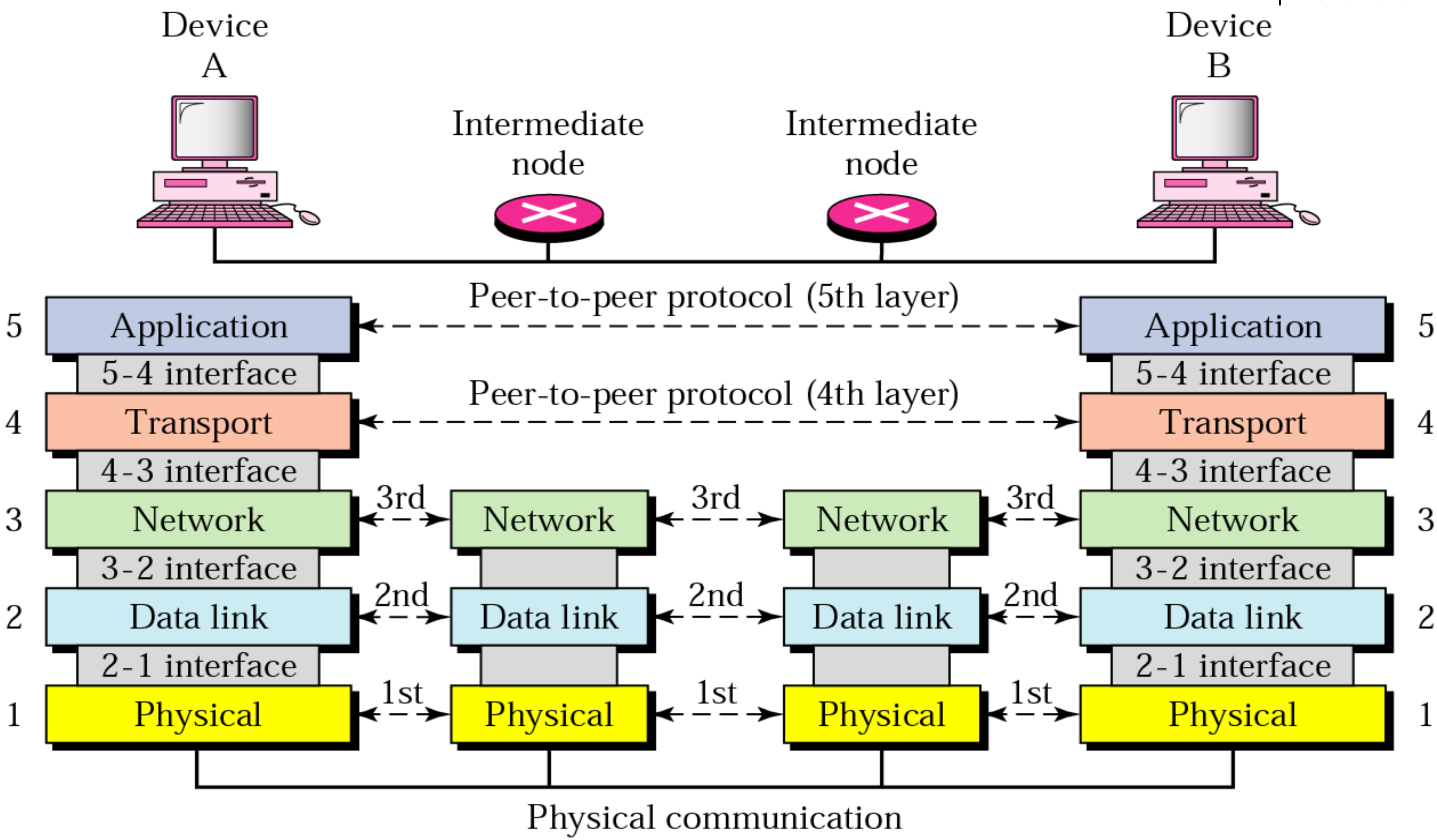
- Five-layer Internet Model → TCP/IP protocol suite
- TCP/IP protocol suite developed b/4 the OSI model has four layers: ***host-to-network, internet, transport, and application***
- Designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers.
- Five-layer Internet Model Layer functions are distinct thus:



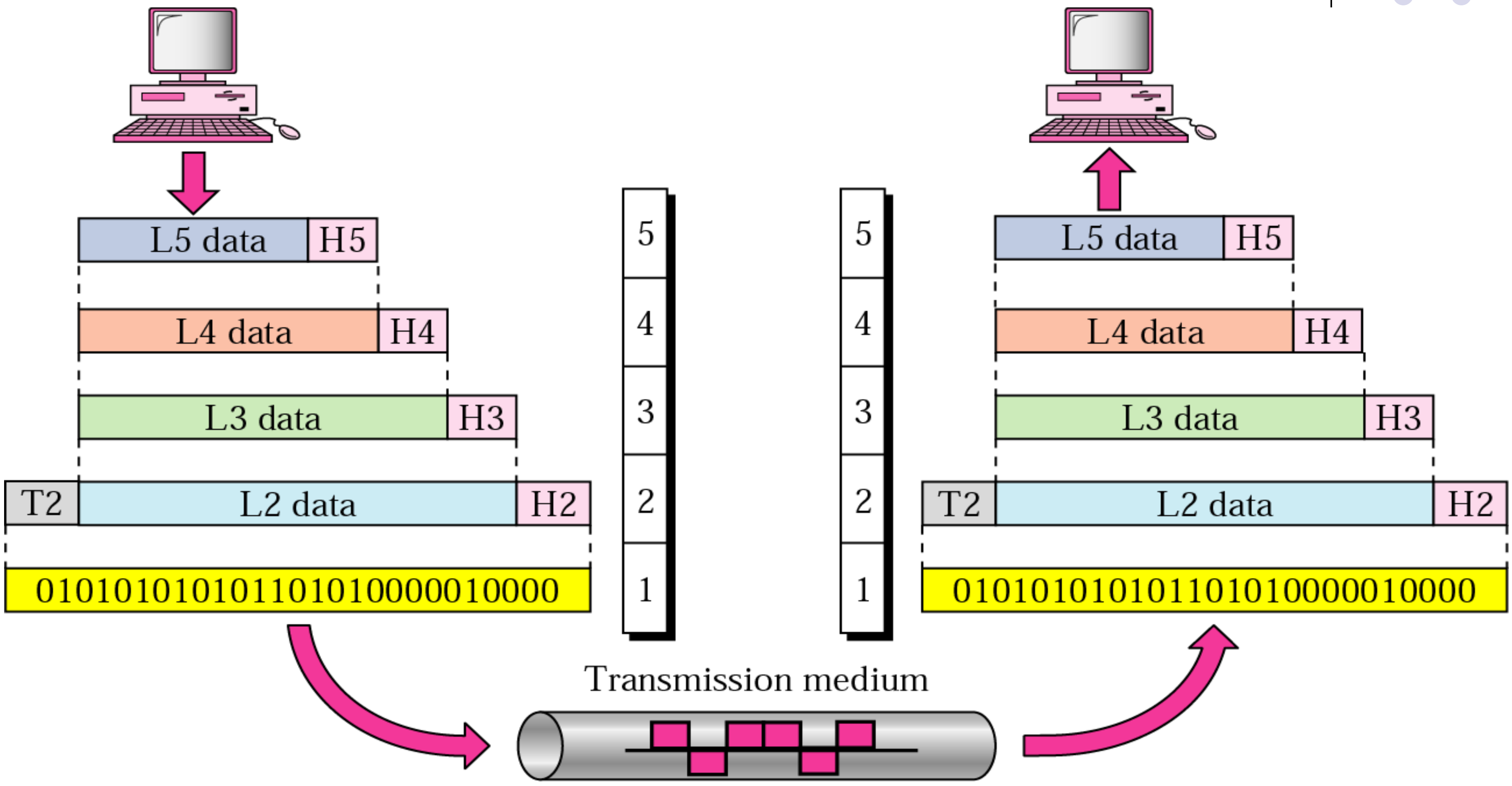
Peer-to-peer processes

- The Processes on each machine that communicate at a given layer are called peer-to-peer processes.
- Each layer in the sending device adds its own information to the message it receives from the layer above it and passes the whole package to the layer just below it.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.
- Passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.
- Each interface defines what information and services a layer must provide for the layer above it. Thus, provide modularity.

Figure 2.3 *Peer-to-peer processes*



An exchange using the Internet model



- Physical, data link and network are network support layers.
- They deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).
- Application layer: User support layer; interoperability among unrelated software systems.
- Transport layer: Links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.
- Each layer adds a header; Data link layer adds a header and a trailer.
- Formatted data is converted into electromagnetic signal and transported along a physical link.

Figure 2.5 ***Physical Layer***

- Deals with mechanical and electrical specifications of the interface and transmission media.
- Defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
  - Physical characteristics of interfaces and media
  - Representation of bits
  - Data rate: Transmission rate – number of bits sent per second
  - Synchronization of bits
- The physical layer is responsible for transmitting individual bits from one node to the next.

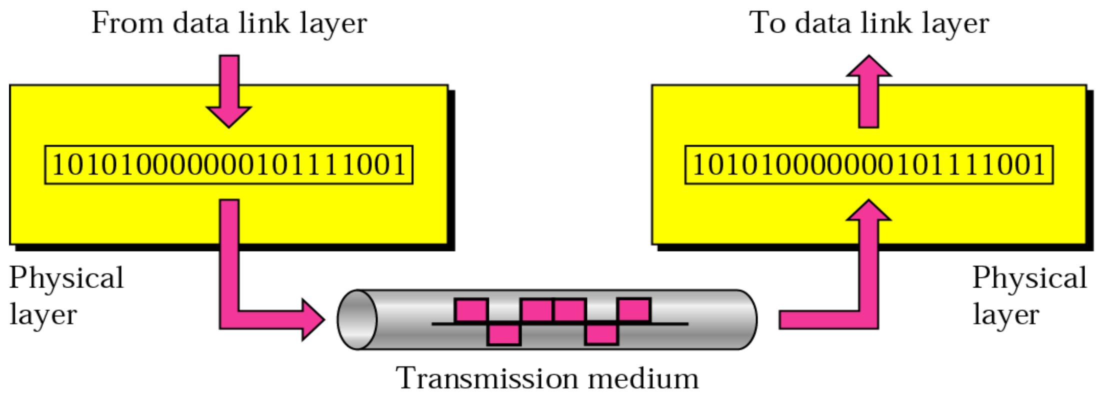


Figure 2.6 *Data link layer*

- Transforms the physical layer, a raw transmission facility, to a reliable link.
- Makes the physical layer appear error-free to the upper layer (network layer).
  - Framing: divide the stream of bits from network layer into frames
  - Physical addressing
  - Flow control: Prevent overwhelming the receiver.
  - Error control: Detect and retransmit damaged or lost frames; Prevent duplication of frames; using trailer.
  - Access control: Determine which device has control over the link at any given time.
- The data link layer is responsible for transmitting frames from one node to next.

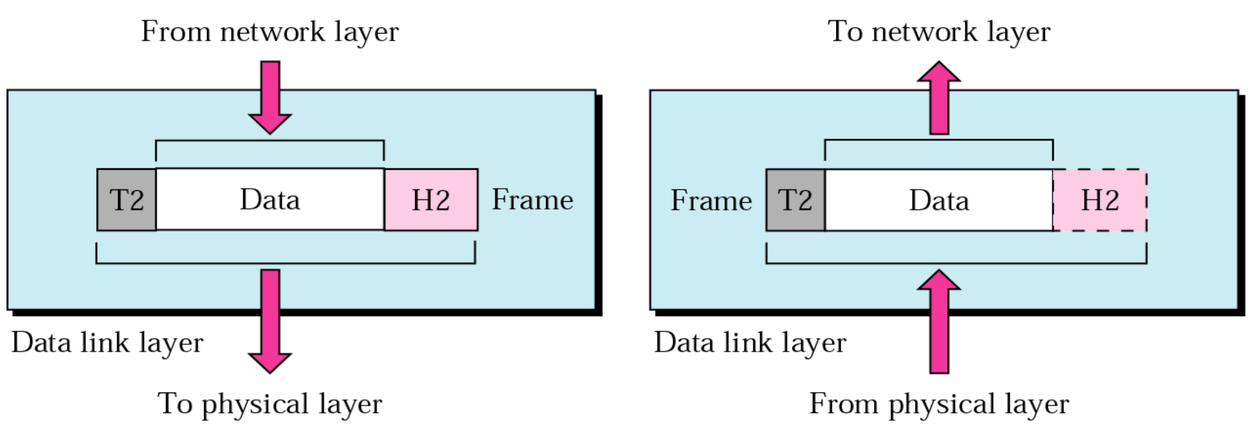
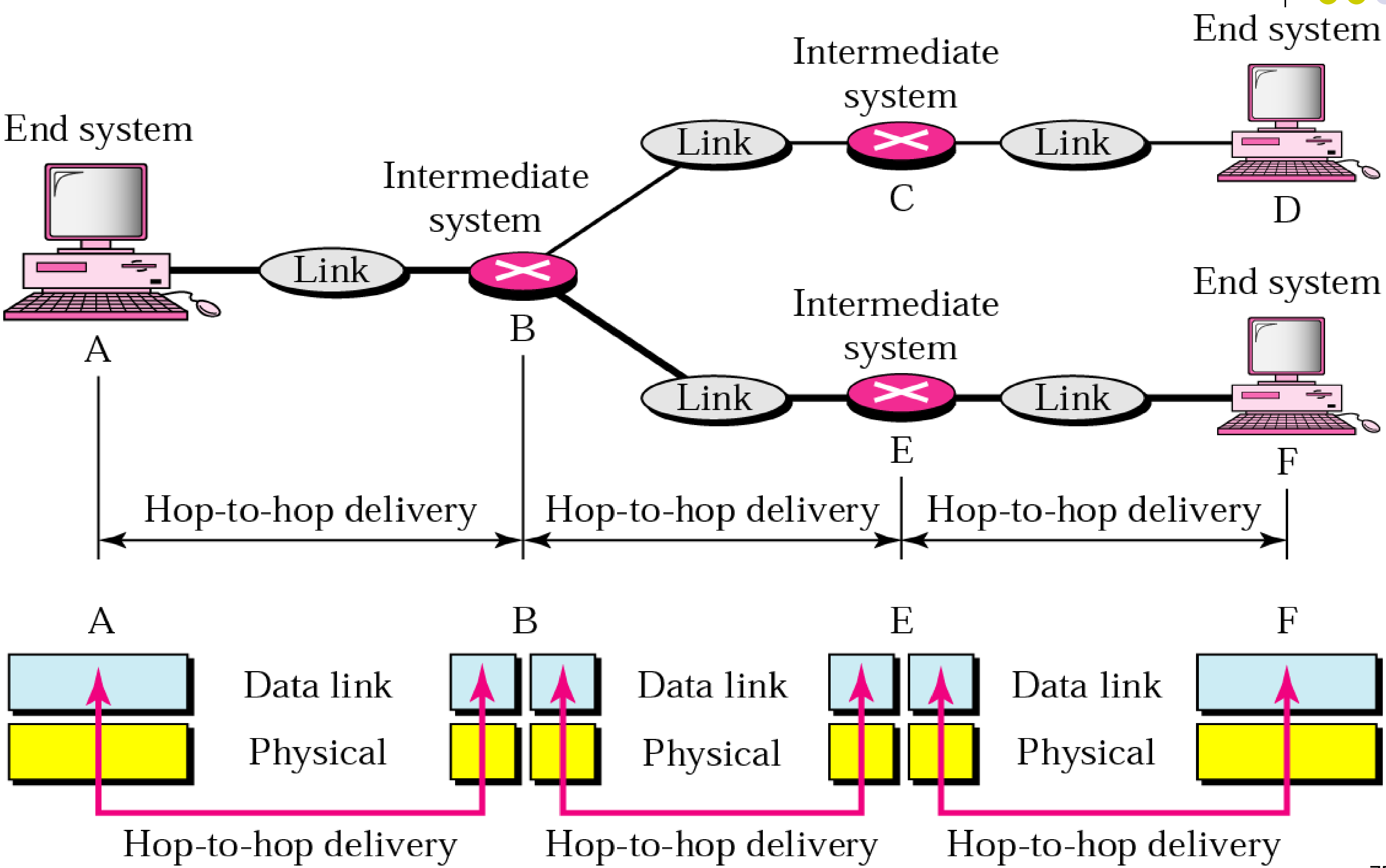


Figure 2.7 *Node-to-node delivery*



Example 1

In Figure 2.8 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link. At the data link level this frame contains physical addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection

Figure 2.8 *Example 1*

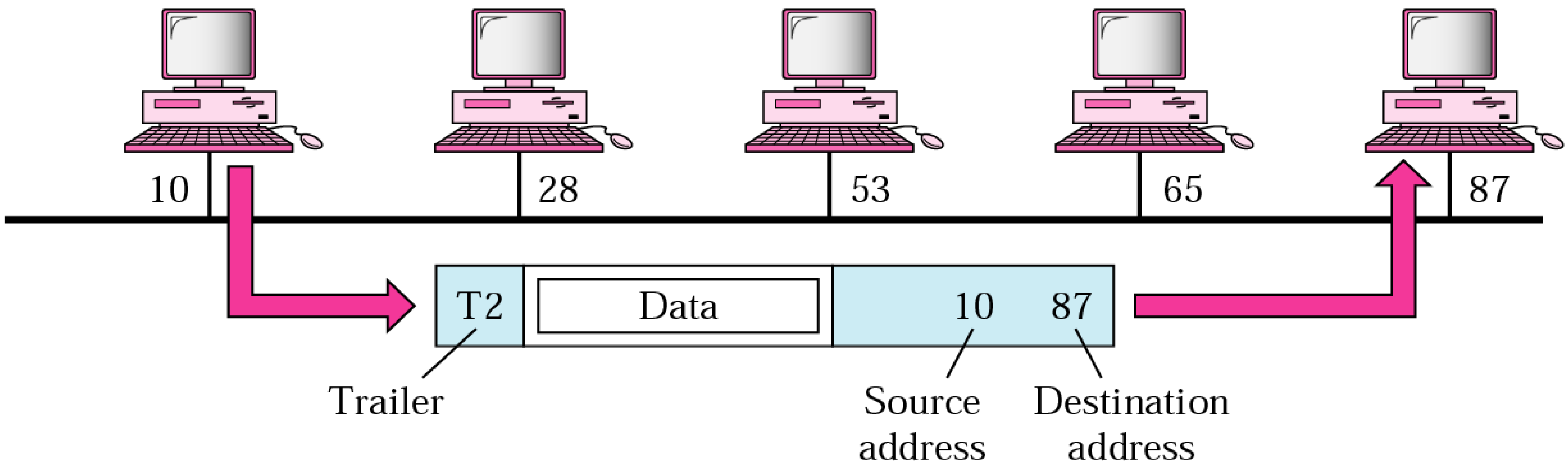
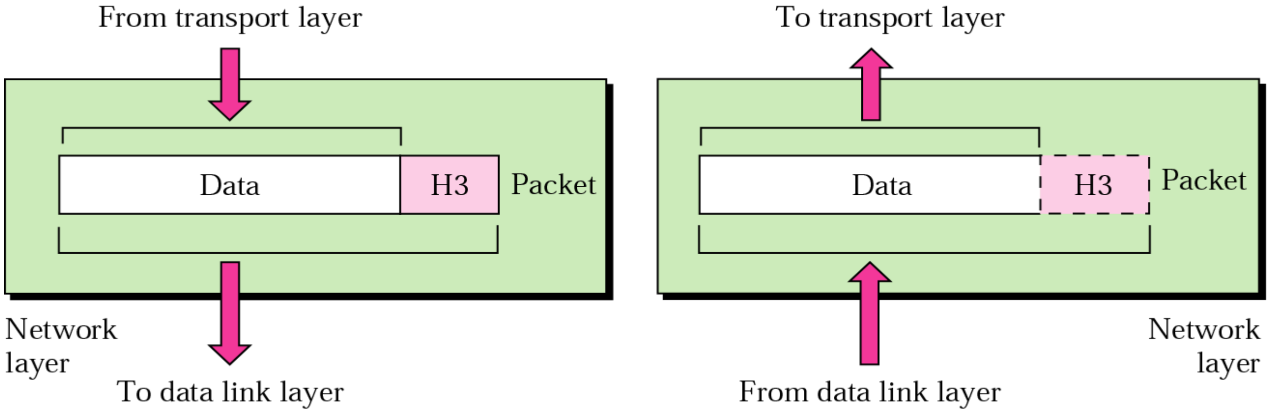


Figure 2.9 *Network layer*

- Responsible for the source-to-destination delivery of a packet possibly across multiple networks.
- Data link layer oversees the delivery of the packet between two systems on the same network.
- Network layer ensures that each packet gets from its point of origin to its final destination.
  - If two systems are connected to the same link, there is usually no need for a network layer.

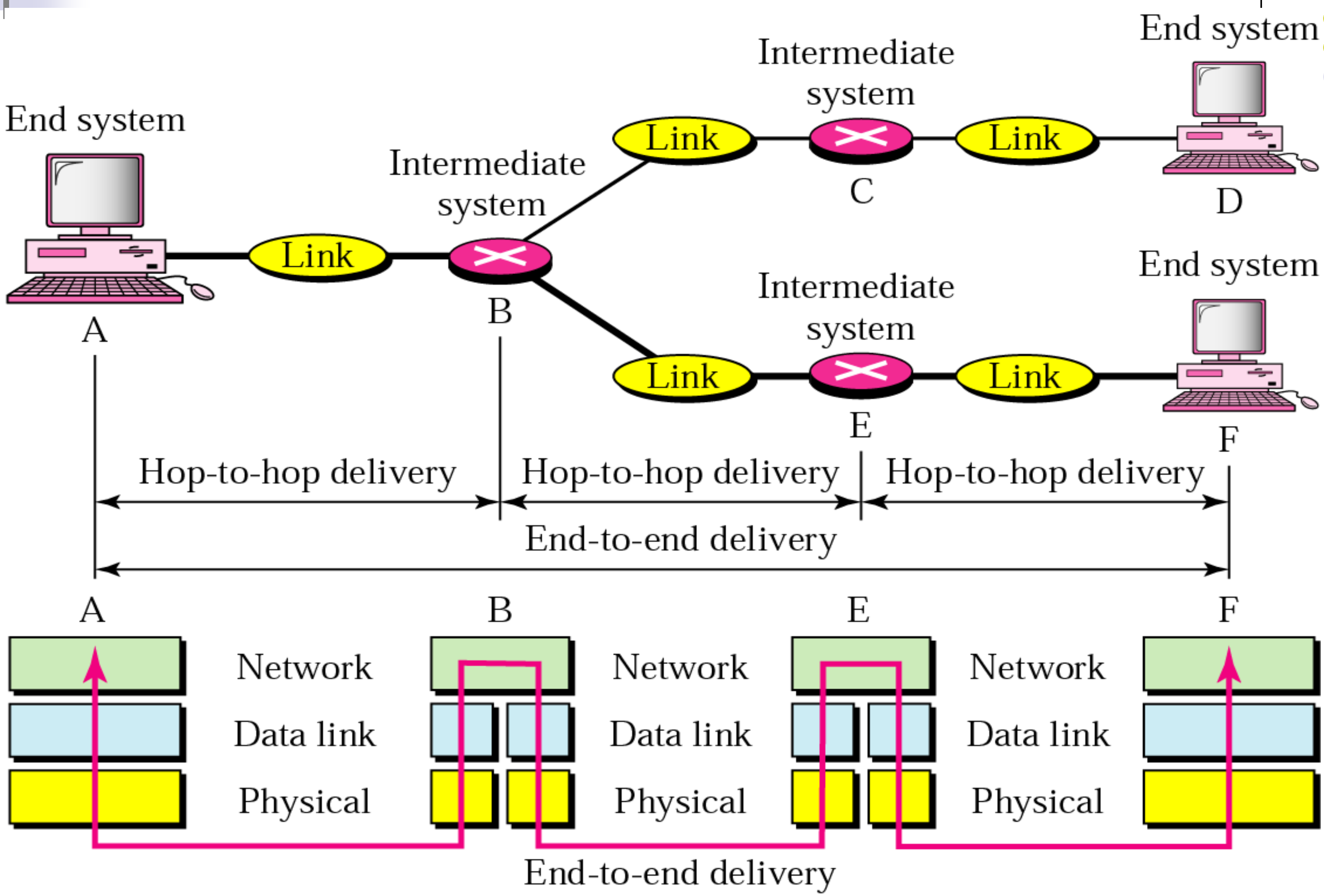


The network layer is responsible for the delivery of packets from the original source to the final destination.

Logical addressing: Physical addressing in data link layer handles the addressing problem locally.

Routing: When independent networks or links are connected to create an internetwork (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

Figure 2.10 *Source-to-destination delivery*



Example 2

In Figure 2.11 we want to send data from a node with network address A and physical address 10, located on one LAN, to a node with a network address P and physical address 95, located on another LAN. Because the two devices are located on different networks, we cannot use physical addresses only; the physical addresses only have local jurisdiction. What we need here are universal addresses that can pass through the LAN boundaries. The network (logical) addresses have this characteristic.

Figure 2.11 *Example 2*

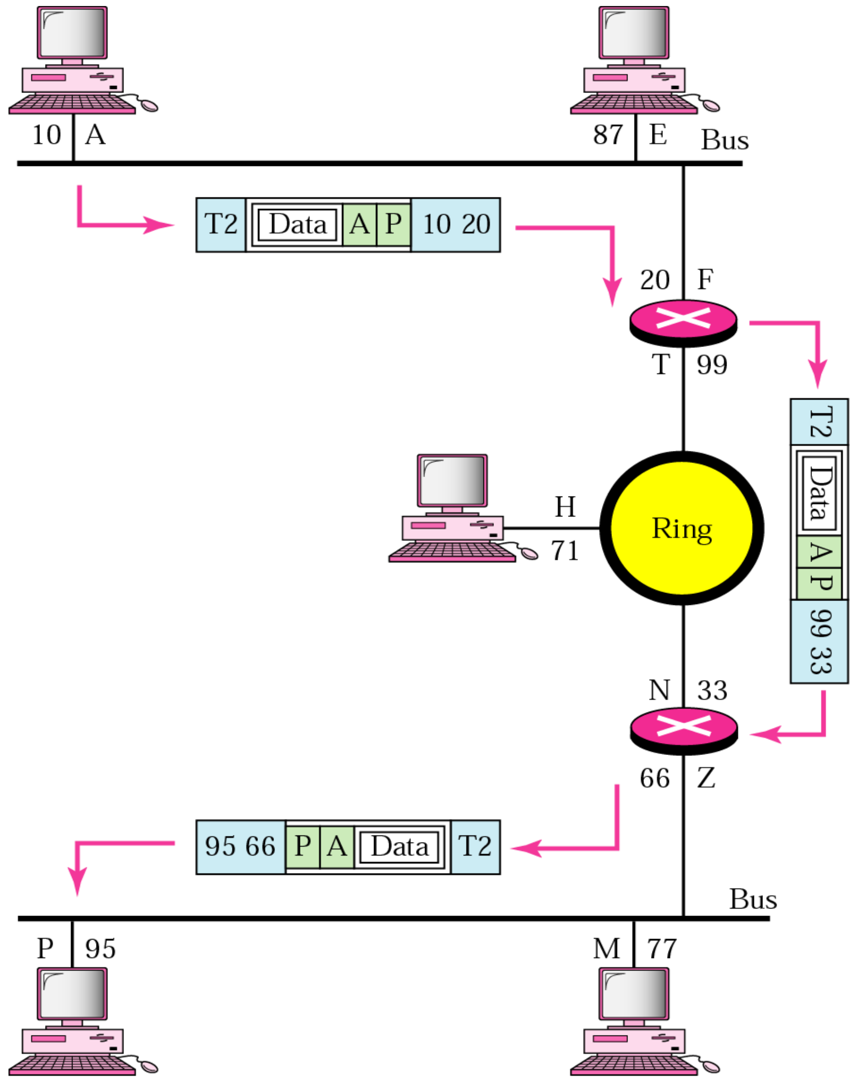
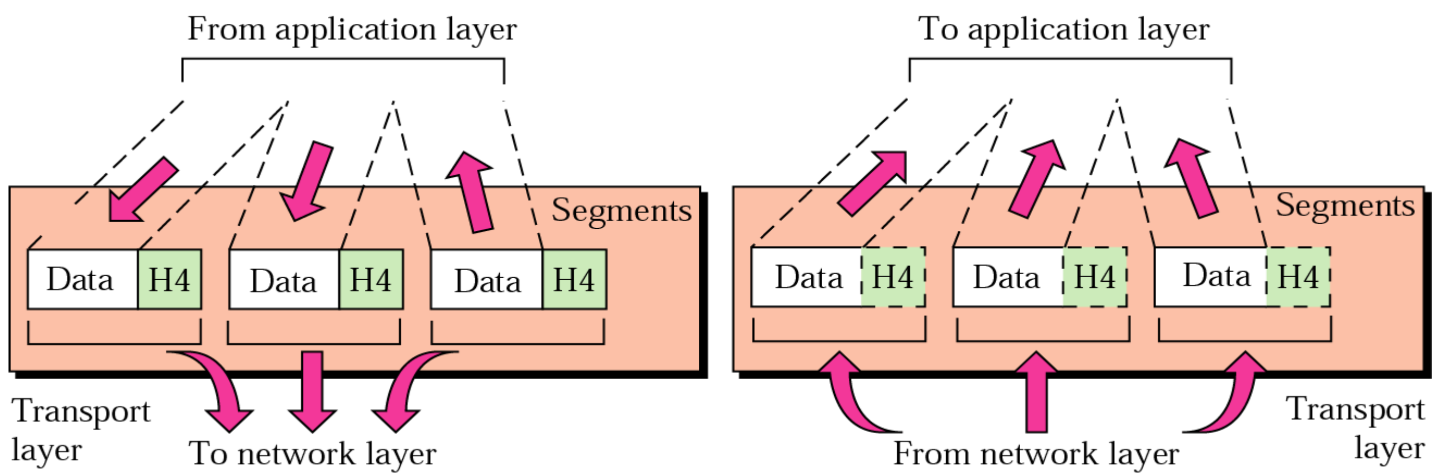


Figure 2.12 ***Transport layer***

- Process-to-Process delivery
- Network layer oversees host-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
- Ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the process-to-process level.



The transport layer is responsible for delivery of a message from one process to another.

•Port addressing: indicating a process

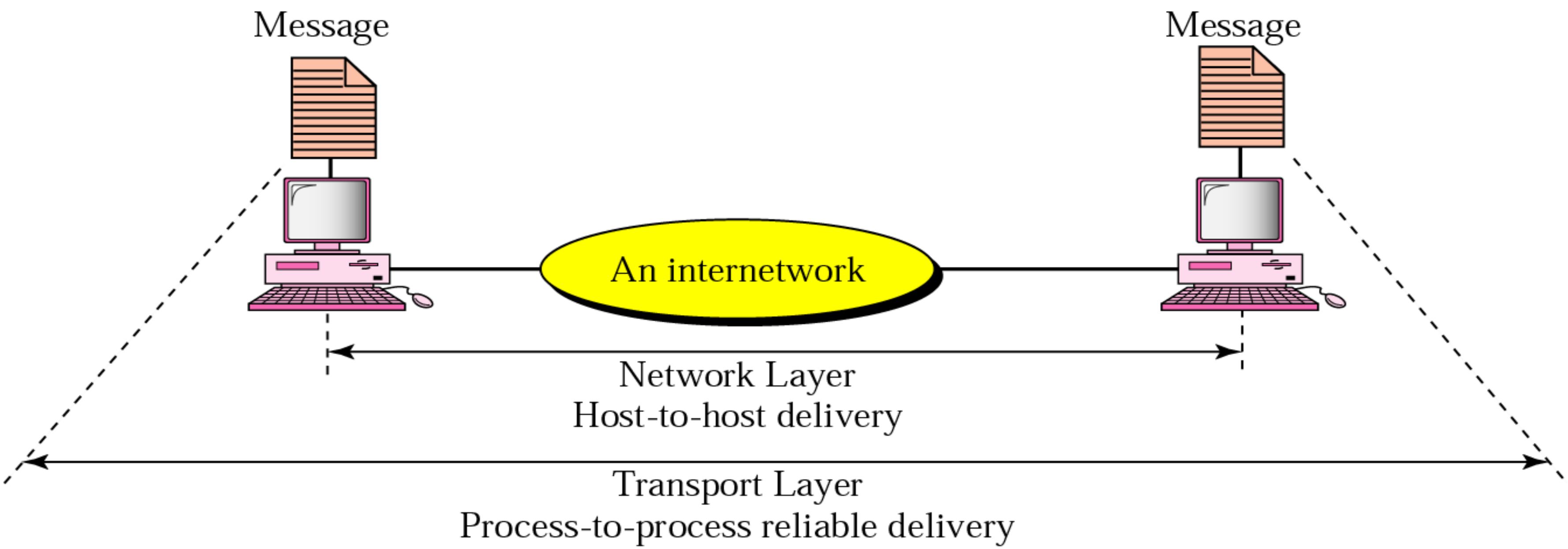
•Segmentation and reassembly: divide into segments having sequence number.

•Connection control: connection-oriented and connectionless

•Flow control: end to end rather than across a single link.

•Error control: End to end rather than across a single link. Sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).

Figure 2.12 Reliable process-to-process delivery of a message



Example 3

Figure 2.14 shows an example of transport layer communication. Data coming from the upper layers have port addresses j and k (j is the address of the sending process, and k is the address of the receiving process). Since the data size is larger than the network layer can handle, the data are split into two packets, each packet retaining the port addresses (j and k). Then in the network layer, network addresses (A and P) are added to each packet.

Figure 2.14 *Example 3*

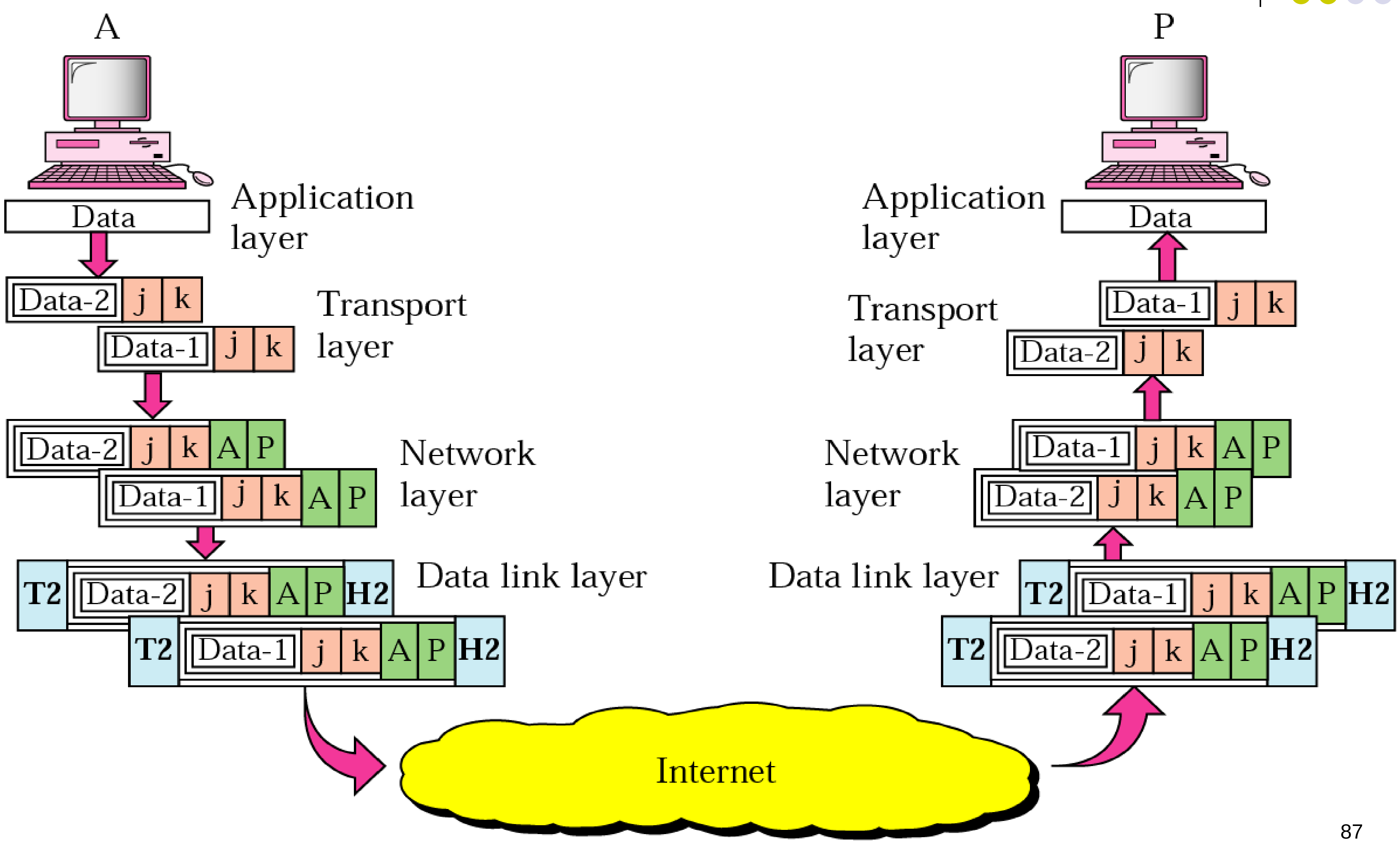
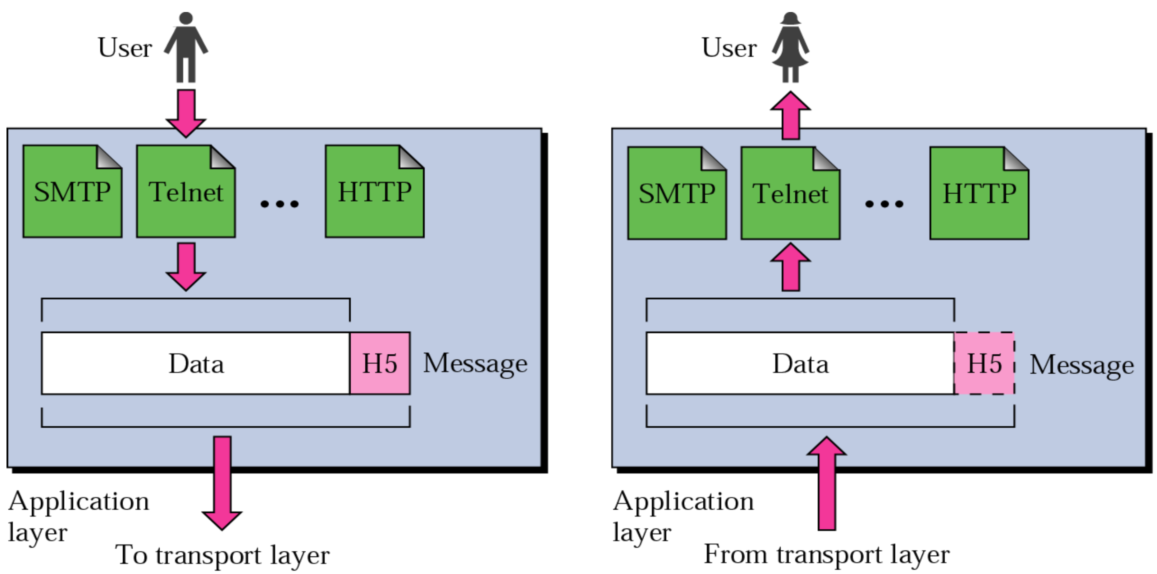


Figure 2.15 *Application layer*

- Enables the user, whether human or software, to access the network.
- Provides user interfaces and support for services such as electronic mail, remote file access and transfer, access to WWW, and so on.



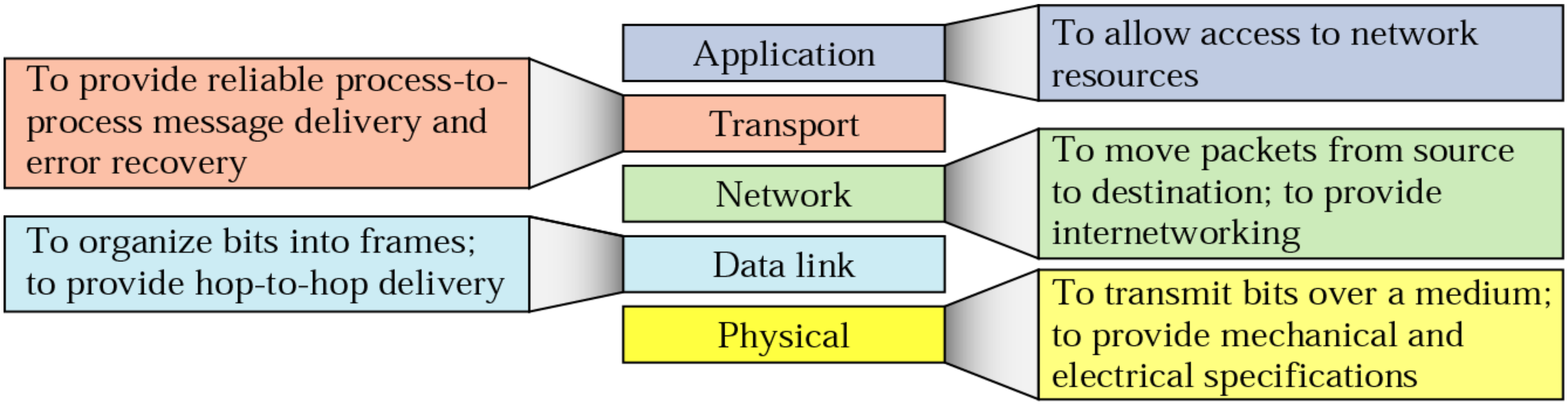
The application layer is responsible for providing services to the user.

- ***Mail services***
- ***File transfer and access***
- ***Remote log-in***
- ***Accessing the WWW***

Contd …

- Application layer
  - Network virtual terminal
    - Logon to a remote host.
  - File transfer, access, and management
    - Access files in a remote host.
  - Mail services
    - Basis for email forwarding and storage.
  - Directory services
    - Distributed database sources and access for global information about various objects and services.

Figure 2.16 ***Summary of duties***



2.3 OSI Model

A comparison

- **Seven-layer model**
- **Never seriously implemented as a protocol Stack**
- **Theoretical model designed to show how a Protocol stack should be implemented**
- **Session & Presentation layer**

Figure 2.17 *OSI model*

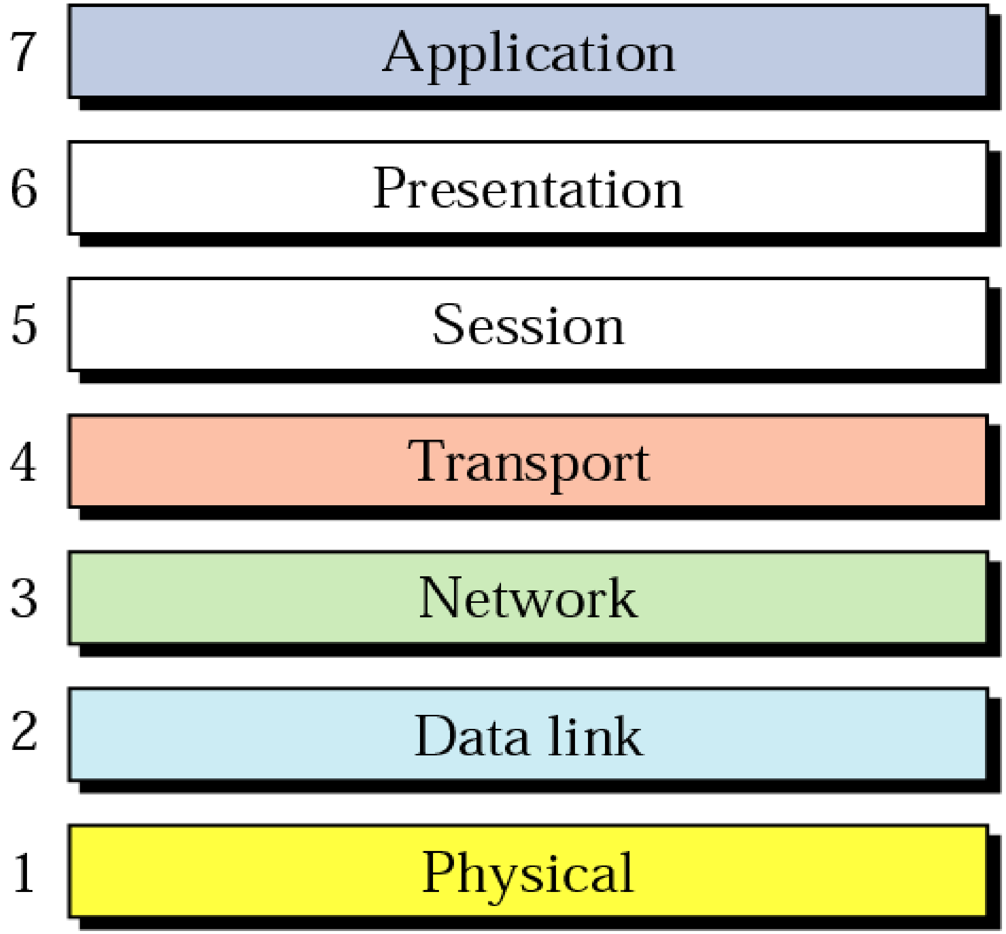


Figure 2.17 *OSI model: Physical layer*

- The physical layer is responsible for movements of individual bits from one hop (node) to the next.
- The physical layer is also concerned with the following:
  - Physical characteristics of interfaces and medium
  - Representation of bits
  - Data rate
  - Synchronization of bits
  - Line configuration
  - Physical topology
  - Transmission mode

Figure 2.17 *OSI model: Data Link Layer*

- The data link layer is responsible for moving frames from one hop (node) to the next
- Other responsibilities of the data link layer include the following:
  - Framing
  - Physical addressing
  - Flow control
  - Error control
  - Access control

Figure 2.17 *OSI model: Network Layer*

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- Other responsibilities of the network layer include the following:
  - Logical addressing
  - Routing

Figure 2.17 *OSI model: Transport*

- The transport layer is responsible for the delivery of a message from one process to another.
- Other responsibilities of the transport layer include the following:
  - Service-point addressing
  - Segmentation and reassembly
  - Connection control
  - Flow control
  - Error control

OSI Model

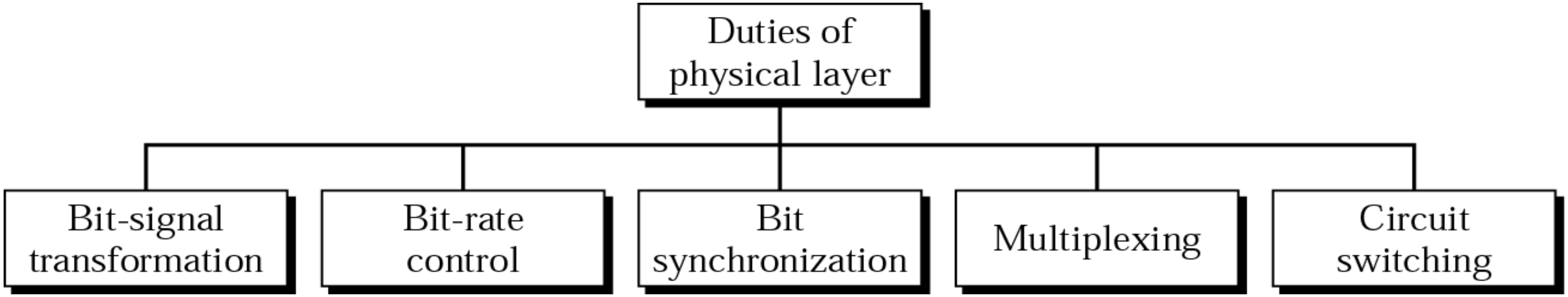
- Session Layer
  - Dialog control: Allows two systems to enter into a dialog, either half or full duplex.
    - Terminal to mainframe is half duplex.
  - Synchronization: Add check points (synchronization points) into a stream of data.
- Presentation layer
  - Translation: Interoperability between these different encoding methods.
  - Encryption: For privacy.
  - Compression: Reduces the number of bits contained in the information; useful in video, audio, …

OSI Model: Application Layer

- The application layer is responsible for providing services to the user.
- Specific services provided by the application layer include the following:
  - Network virtual terminal
  - Mail services
  - Directory services

Physical Layer

Services


Duties of physical layer
Bit-signal transformation
Bit-rate control
Bit synchronization
Multiplexing
Circuit switching

Chapters

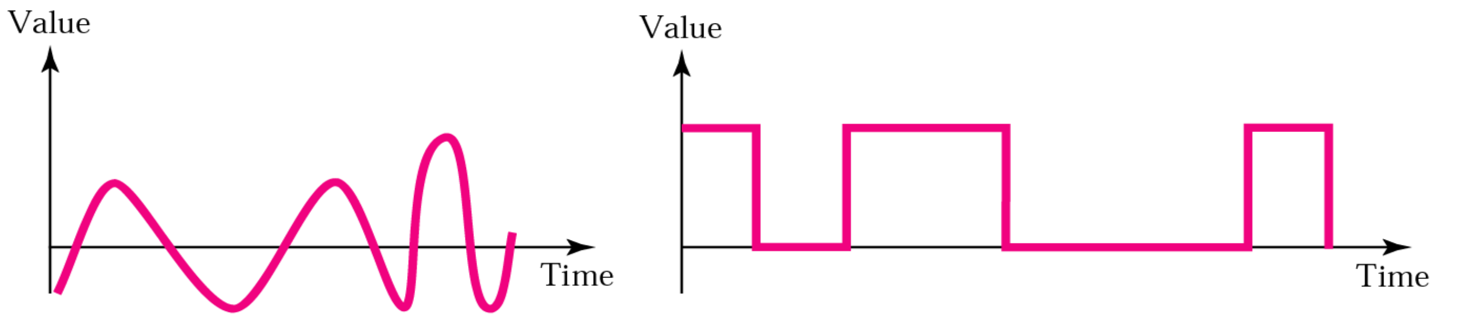
Chapter 3 ***Signals***

Chapter 4 ***Digital Transmission***

Chapter 3

Signals

- To be transmitted, data must be transformed to electromagnetic signals
- Signals can be analog or digital. Analog signals can have an infinite number of values in a range; digital signals can have only a limited number of values.

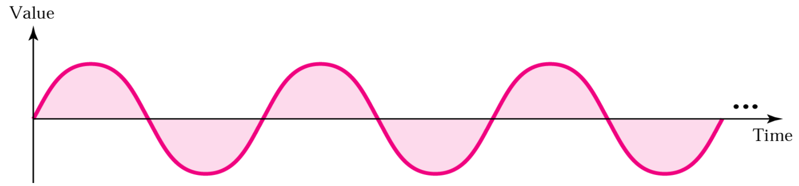


a. Analog signal
b. Digital signal

- In data communication, we commonly use periodic analog signals and aperiodic digital signals.
- Periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.
- An aperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

Figure 3.2 *A sine wave*

- Analog signals can be simple or composite.
- A simple periodic analog signal (Sine wave) cannot be decomposed into simpler signals. A composite analog signal is composed of multiple sine waves.



- Peak amplitude of a signal represents the absolute value of its highest intensity, proportional to the energy it carries.
- For electric signals, peak amplitude is normally measured in *volts*

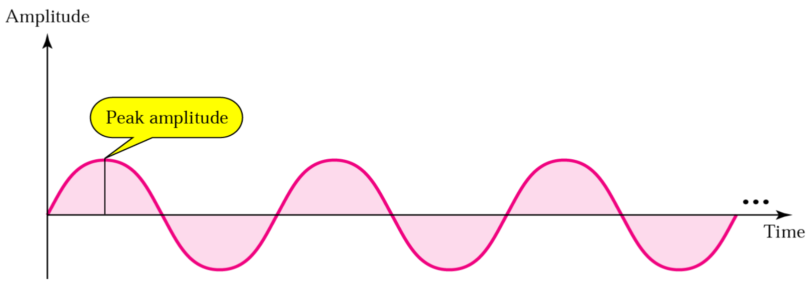


Figure 3.4 *Period and frequency*

- Period refers to the amount of time, in seconds, a signal needs to complete one cycle.
- Frequency refers to the number of periods in one second.
- Frequency and period are inverses of each other.
- Frequency is normally expressed in hertz (Hz).

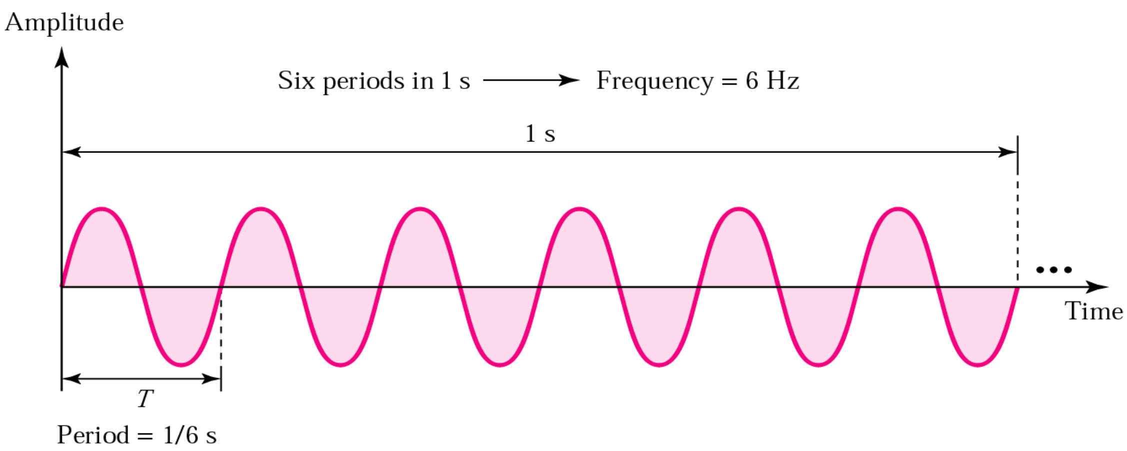


Table 3.1 Units of periods and frequencies

Unit	Equivalent	Unit	Equivalent
Seconds (s)	1 s	hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	kilohertz (KHz)	10^{3} Hz
Microseconds (μs)	10^{-6} s	megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	terahertz (THz)	10^{12} Hz

METRIC UNITS

Example 1

Express a period of 100 ms in microseconds, and express the corresponding frequency in kilohertz.

Solution

From Table 3.1 we find the equivalent of 1 ms.We make the following substitutions:

$100 \text{ ms} = 100 \times 10^{-3} \text{ s} = 100 \times 10^{-3} \times 10^{6} \text{ µs} = 10^{5} \text{ µs}$

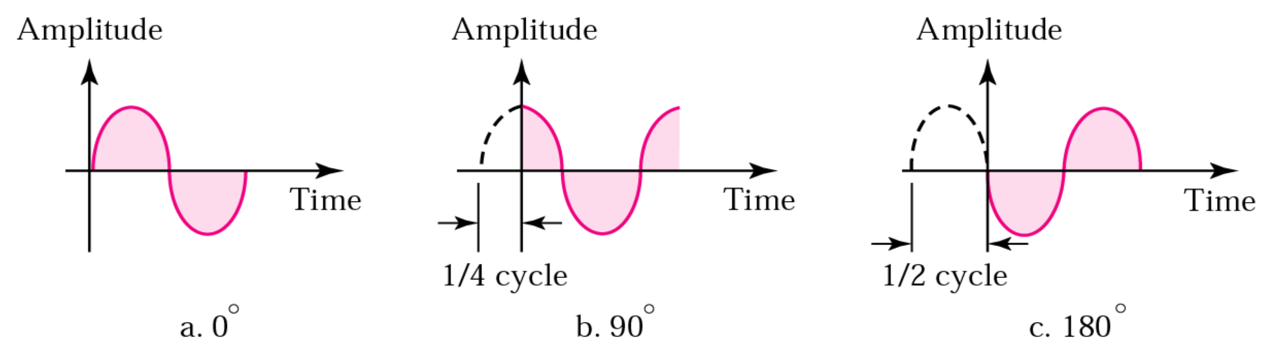
Now we use the inverse relationship to find the frequency, changing hertz to kilohertz

$100 \text{ ms} = 100 \times 10^{-3} \text{ s} = 10^{-1} \text{ s}$

$f = 1/10^{-1} \text{ Hz} = 10 \times 10^{-3} \text{ KHz} = 10^{-2} \text{ KHz}$

Figure 3.5 *Relationships between different phases*

- Frequency is the rate of change with respect to time. Change in a short span of time means high frequency. Change over a long span of time means low frequency.
- If a signal does not change at all, its frequency is zero. If a signal changes instantaneously, its frequency is infinite.
- Phase describes the position of the waveform relative to time zero.
- When a signal changes instantaneously, its period is zero; since frequency is the inverse of period, the frequency is infinite.
- If a signal does not change at all, it never completes a cycle, so its frequency is 0 Hz



Example 2

A sine wave is offset one-sixth of a cycle with respect to time zero. What is its phase in degrees and radians?

Solution

We know that one complete cycle is 360 degrees.

Therefore, 1/6 cycle is

$(1/6)\ 360 = 60$ degrees $= 60 \times 2\pi / 360$ rad $= 1.046$ rad

Figure 3.6 *Sine wave examples*

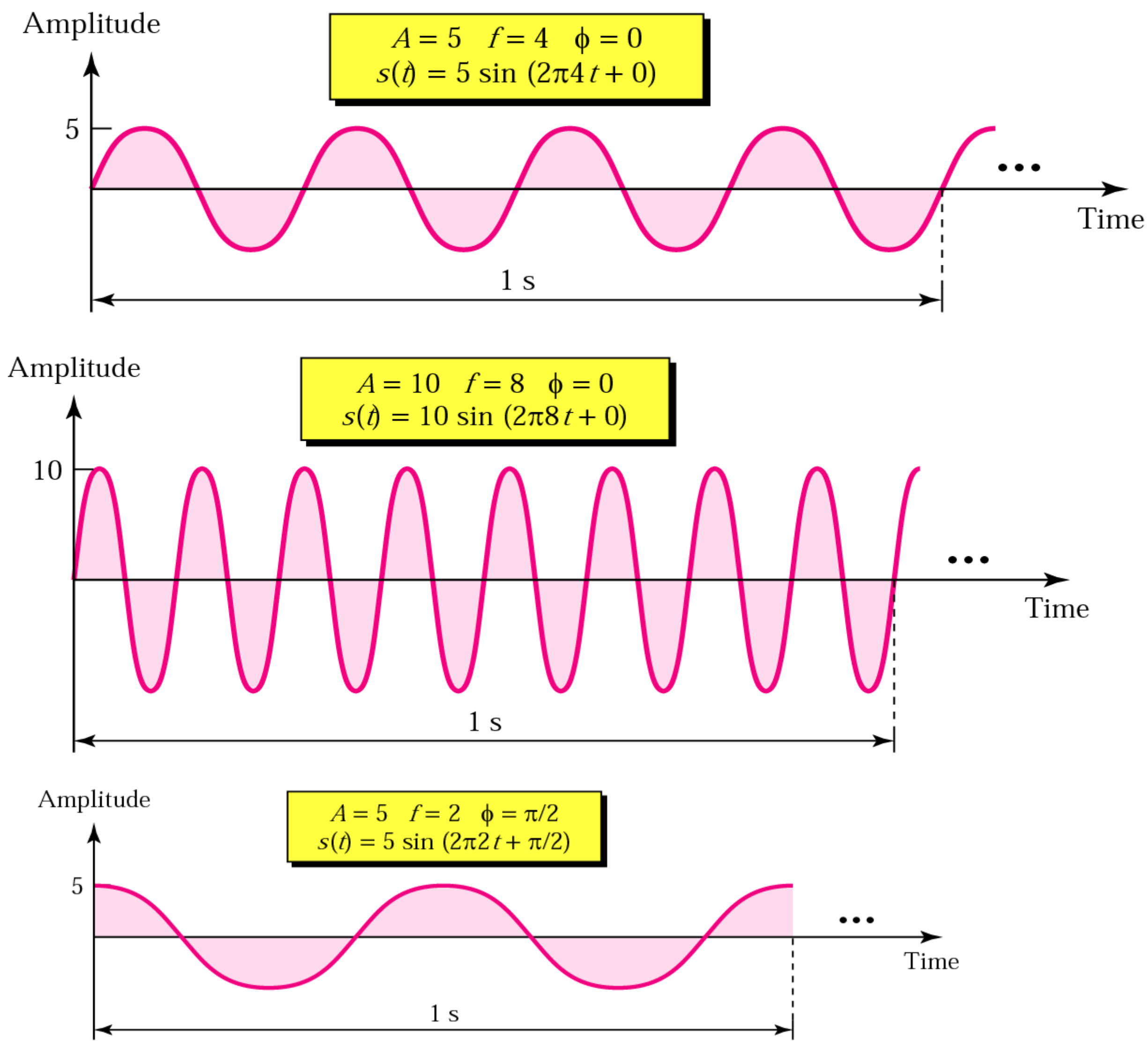
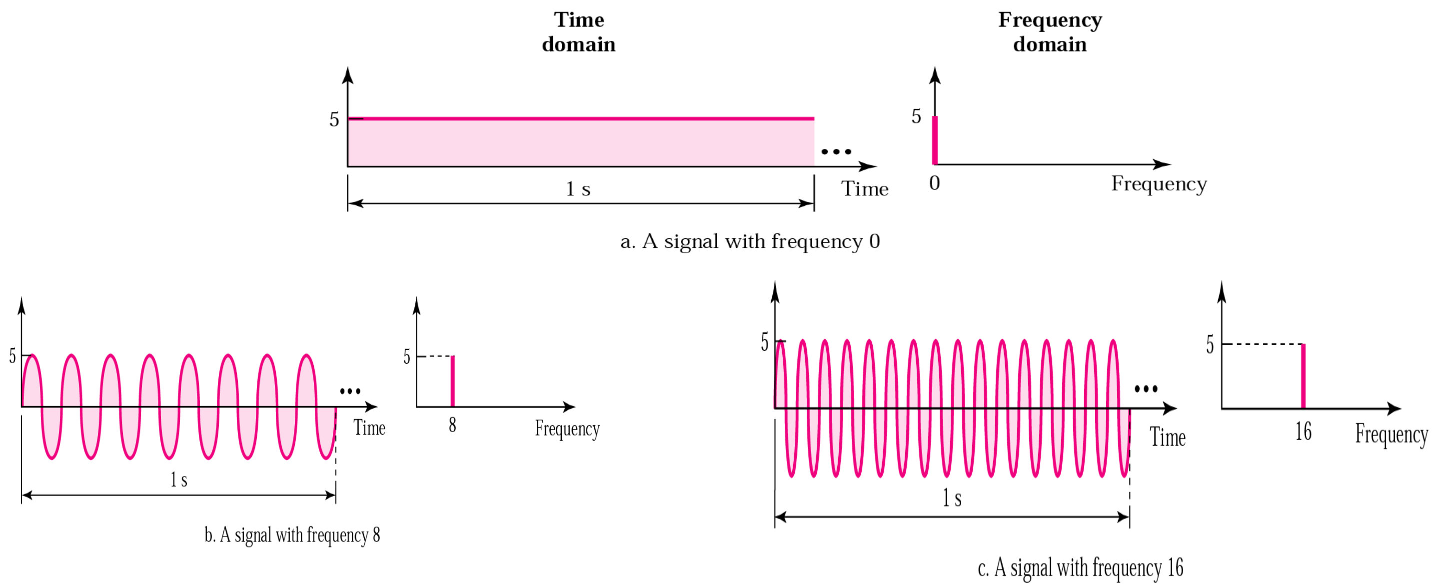


Figure 3.7 *Time and frequency domains*

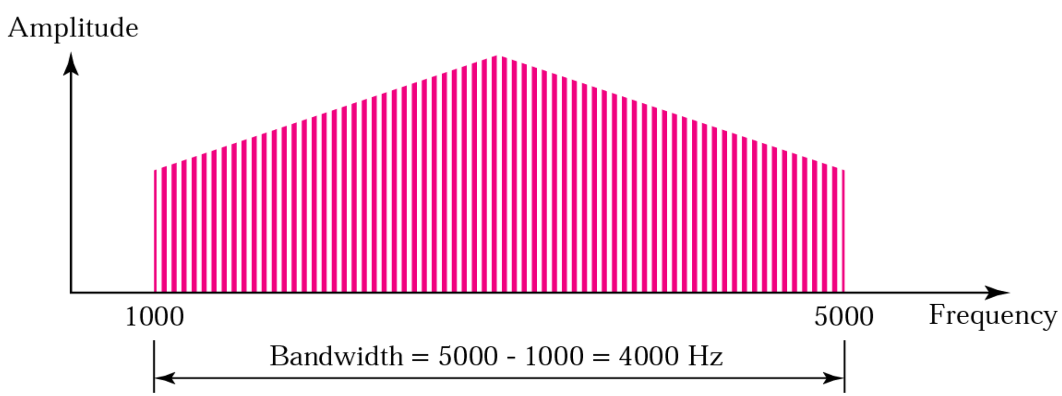
- Time-domain plot shows changes in signal amplitude with respect to time. *Phase and frequency are not explicitly measured on a time-domain plot.*
- Frequency-domain plot shows the relationship between amplitude and frequency.
- An analog signal is best represented in the frequency domain.



- A single-frequency sine wave is not useful in data communications; we need to change one or more of its characteristics to make it useful
- When we change one or more characteristics of a single-frequency signal, it becomes a composite signal made of many frequencies
- According to Fourier analysis, any composite signal can be represented as a combination of simple sine waves with different frequencies, phases, and amplitudes

Figure 3.13 *Bandwidth*

- The bandwidth is a property of a medium: It is the difference between the highest and the lowest frequencies that the medium can satisfactorily pass
- In this slide, we use the term bandwidth to refer to the property of a medium or the width of a single spectrum



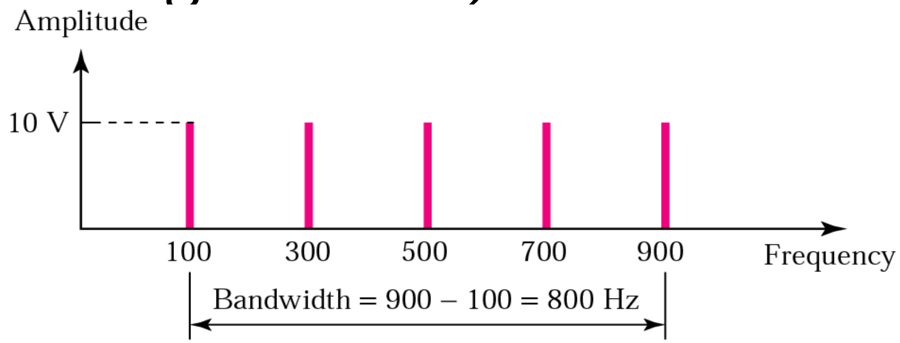
Example 3

If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is the bandwidth? Draw the spectrum(range of values), assuming all components have a maximum amplitude of 10 V.

Solution

$B = f_h - f_l = 900 - 100 = 800$ Hz

The spectrum has only five spikes, at 100, 300, 500, 700, and 900 (see Figure 13.4)



Example 4

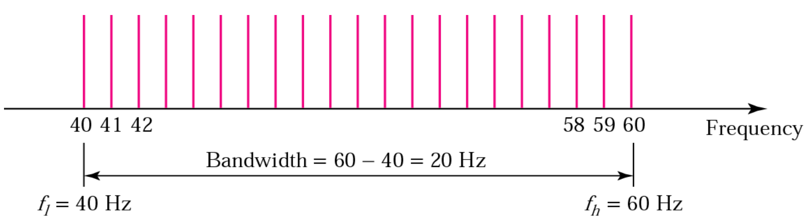
A signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency? Draw the spectrum(range of values) if the signal contains all integral frequencies of the same amplitude.

Solution

$B = f_h - f_l$

$20 = 60 - f_l$

$f_l = 60 - 20 = 40$ Hz



Example 5

A signal has a spectrum(range of values) with frequencies between 1000 and 2000 Hz (bandwidth of 1000 Hz). A medium can pass frequencies from 3000 to 4000 Hz (a bandwidth of 1000 Hz). Can this signal faithfully pass through this medium?

Solution

The answer is definitely no. Although the signal can have the same bandwidth (1000 Hz), the range does not overlap. The medium can only pass the frequencies between 3000 and 4000 Hz; the signal is totally lost.

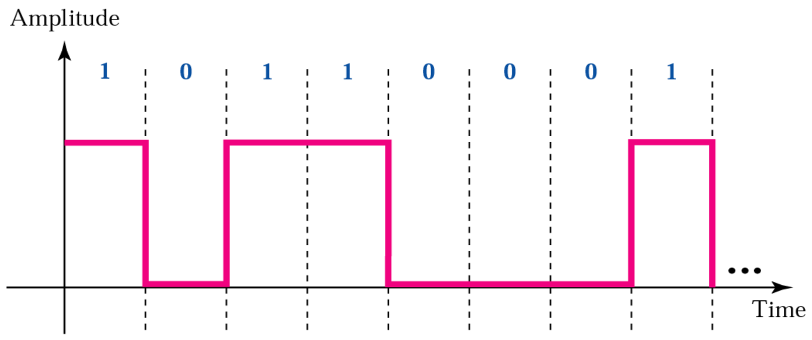
- While the frequency of a signal is independent of the medium, the wavelength depends on both the frequency and the medium.
- Wavelength is a property of any type of signal.
- Wavelength describes the transmission of light in an optical fiber.
- *The wavelength is the distance a simple signal can travel in one period*.
- Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal.
- If we represent wavelength by A, propagation speed by c (speed of light), and frequency by*1,* we get:

- Wavelength = propagation speed x period = $\frac{\text{propagation speed}}{\text{frequency}}$

- The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal
- E.g. In a vacuum, light is propagated with a speed of 3×10^8 ms.
- That speed is lower in air and even lower in cable.
- The wavelength is normally measured in micrometers (microns) instead of meters.
- E.g., The wavelength of red light (frequency $=4 \times 10^{14}$) in air is
- $$ƛ = \frac{c}{f} = \frac{3 \times 10^8}{4 \times 10^{14}} = 0.75 * 10^{-6}\text{m} = 0.75\mu$$
- In a coaxial or fiber-optic cable, the wavelength is shorter (0.5 µm) because the propagation speed in the cable is decreased.

Figure 3.16 *A digital signal*

- 1 can be encoded as a positive voltage and a 0 as zero voltage.
- Most digital signals are aperiodic, and thus period of frequency is not appropriate.
- Bit interval (instead of period) is the time required to send one single bit.
- Bit rate (instead of frequency) is the number of bit intervals per second. It is the number of bits sent in 1sec, usually expressed in bits per second (bps).



Example 6

A digital signal has a bit rate of 2000 bps. What is the duration of each bit (bit interval)

Solution

The bit interval is the inverse of the bit rate.

Bit interval = 1/ 2000 s = 0.000500 s
= 0.000500 x 10^6 μs = 500 μs