COMPUTER NETWORK & COMMUNICATION (BCSC0008)

Lecture 1

Text and Reference Books

Text Books:

1. Fourouzan B. A. (2004), “Data Communication and Networking”, 4th Edition, McGraw-Hill.

References:

1. Kurose, J. F. and Ross K. W. (2005), “Computer Networking: A Top-Down Approach Featuring the Internet”, 3rd Edition, Addison-Wesley.
2. A. S. Tanenbaum (2006), “Computer Networks”, 2nd Edition, Prentice Hall India.

Chapter 1: Introduction

Our goal:

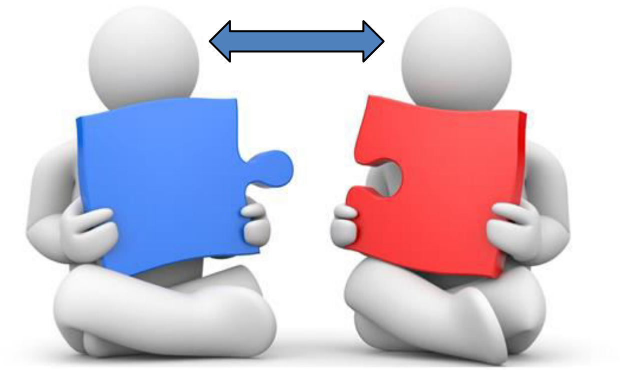
- get context, overview, "feel" of networking
- more depth, detail *later* in course
- approach:
  - descriptive
  - use Internet as example
- Teaching Style: Blended

Overview:

- What is Communication
- Voice Communication vs. Data Communication
- Analyzing Components for Communication
- How Communication is related to networking
- What, How and Why Networking
- Detail Concepts of Networking

Communication

- Communication
- Mechanism of exchanging / transferring information from one point to other.



- Many variants of communications:
  - Voice Communication
  - Data Communication
  - Mobile Communication …
- Voice Communication : Exchange of information between two humans

- We'll understand the concepts of voice communication to analyze it on data communication

Analyzing Voice Communication

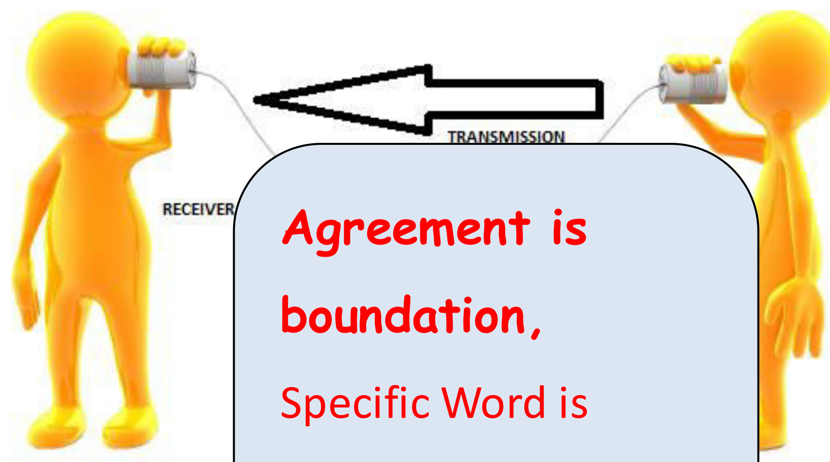
- T

Protocol may define the following

What data to be send
What is the format of data
How data is to be interpreted
When data to be sent
How fast they can be sent

Thus,

Syntax,
Semantics &
Timing is defined by protocol



Agreement is boundation,

Specific Word is

PROTOCOL

- Does
medi   is
sufficient to establish
communication

Voice Communication Vs. Data Communication

Conclusion:

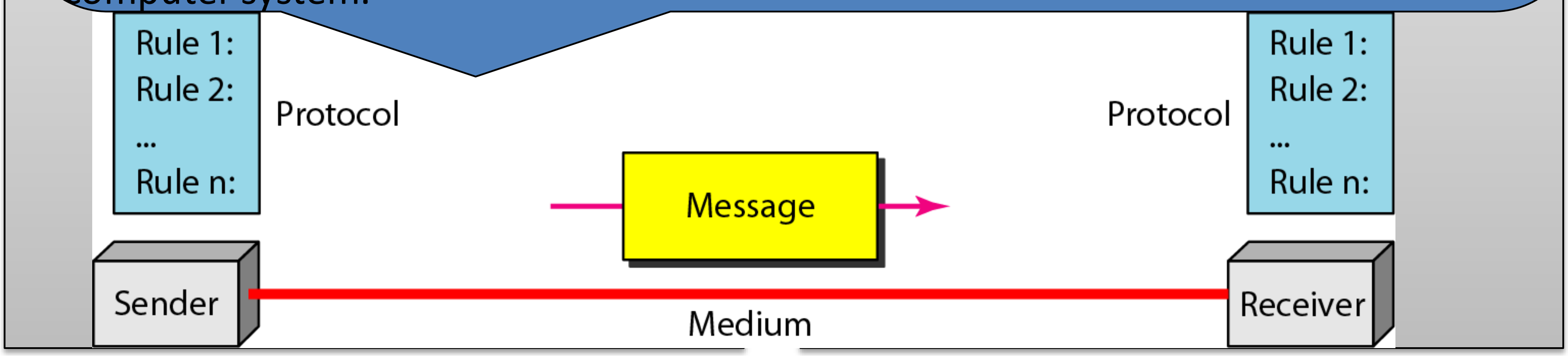
Minimum 2 devices required.

The devices may be geographically located anywhere.

Both devices connected with medium.

They are able to communicate hence t**hey can exchange and share information and resources.**

Resources may be file, folder, printer, disk drive or any thing that may exist on computer system.



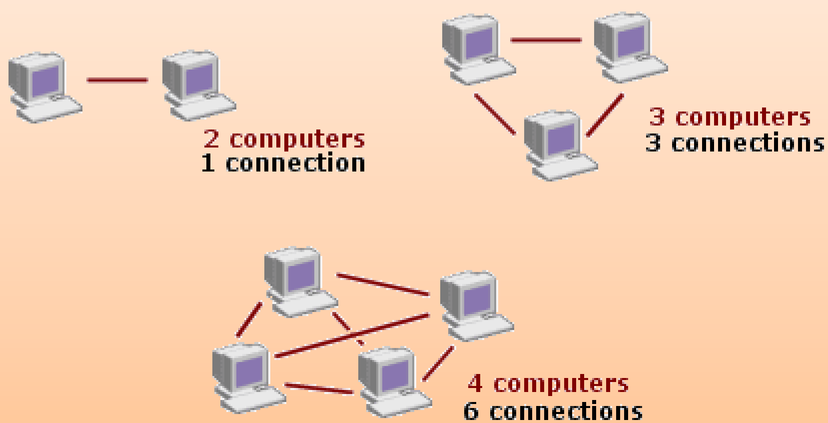
Two methods of Connecting (Based on the communication link and not devices)

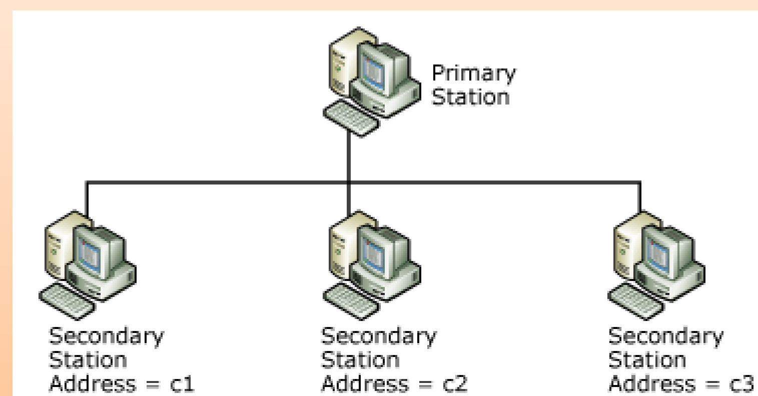
Point to Point (P2P)

Multipoint

P2P: One communication link is connected by only 2 devices.

Multipoint: One communication link is connected by more than 2 devices.





So, How many Kinds of Network??

- Based on Transmission Media
- Wired (UTP, Coaxial, fiber optic) or Wireless (Air, Water)
- Based on Network Size
- LAN, MAN and WAN
- Based on Management Method
- Peer to Peer and Client Server
- Based on topology (Connectivity)
- Bus, Star, Ring, Mesh, Hybrid
- Based on Data Flow Direction
- Simplex, Half Duplex, Full Duplex

- **Thank You**
- **Discussion & Doubt session will be in lecture.**

Important terms to keep in mind

1. **<u>Communication</u>**
2. **<u>Network</u>**
3. **<u>Point to Point Connection</u>**
4. **<u>Multipoint Connection</u>**

COMPUTER NETWORKS (BCSC 0008)

Lecture 2
Simplex, Half Duplex, Duplex, Topology

Text and Reference Books

Text Books:

1. Fourouzan B. A. (2004), “Data Communication and Networking”, 4th Edition, McGraw-Hill.

References:

1. Kurose, J. F. and Ross K. W. (2005), “Computer Networking: A Top-Down Approach Featuring the Internet”, 3rd Edition, Addison-Wesley.
2. A. S. Tanenbaum (2006), “Computer Networks”, 2nd Edition, Prentice Hall India.

Previous discussed topics:

1. **Communication**
2. **Network**
3. **Point to Point Connection**
4. **Multipoint Connection**

Now we will discuss:

1. **Categories of Network**
2. **Simplex, Half Duplex, Full Duplex Network**
3. **Topology : Bus, Star, Ring, Mesh, Hybrid**

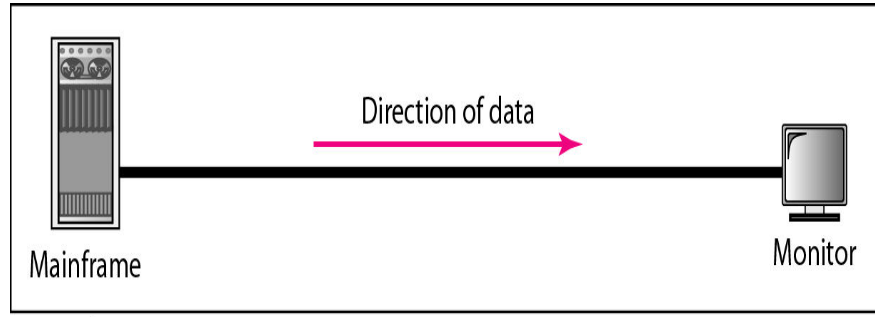
So, How many Kinds of Network??

- Based on Transmission Media
- Based on Network Size
- Based on Management Method
- Based on topology (Connectivity)
- Based on Data Flow Direction

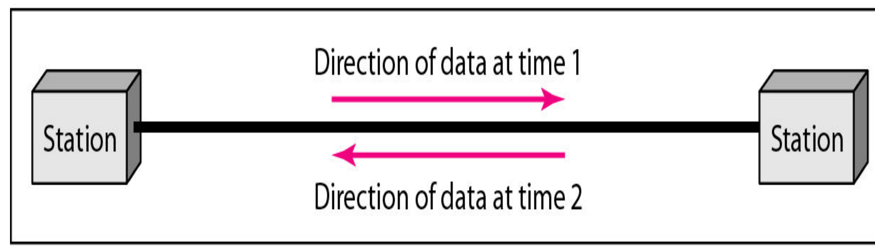
- Wired (UTP, Coaxial, fiber optic) or Wireless (Air, Water)
- LAN, MAN and WAN
- Peer to Peer and Client Server
- Bus, Star, Ring, Mesh, Hybrid
- Simplex, Half Duplex, Full Duplex

Based on Data Flow Direction

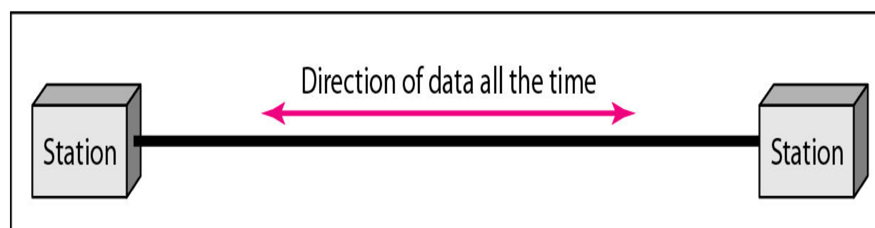
- **Simplex (Always Unidirectional)**
- **One device permanent sender and other permanent receiver.** For example *Computer-Printer*, *Computer-Speaker*
- **Half Duplex (Bidirectional but any particular time unidirectional)**
- **The role of devices may vary with respect to time [Both cannot be in same role at any time].** For example *Walkie-Talkie*
- **Full Duplex or Duplex (Bidirectional Always)**
- **Both devices may or may not be in the same role at any time.** For example *Telephone or Cellular*



a. Simplex



b. Half-duplex



c. Full-duplex

Based on Topology (Connectivity)

- Bus (can be both logical and physical)
- Star (physical only)
- Ring (can be both logical and physical)
- Mesh (can be both logical and physical)

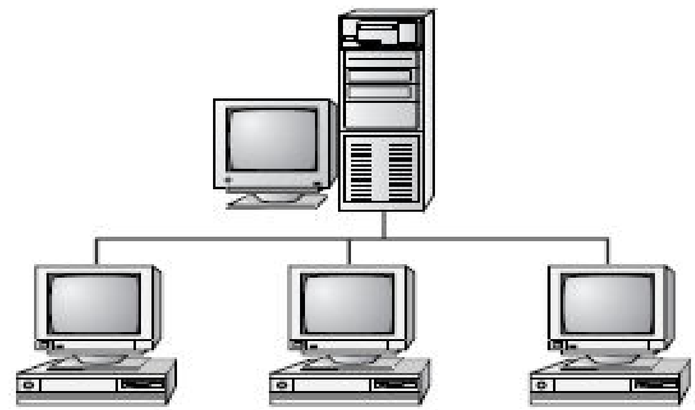
BUS Topology

- A bus is the ... physical top... ...le cable th...
- ... ount ... the ... e.
- In a ... gy, signals are broadca... to all stations

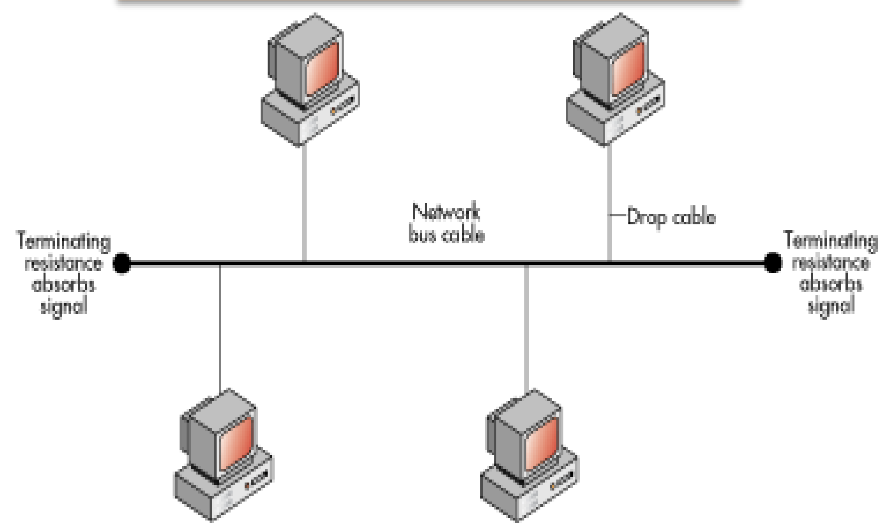
When Signal is passed to all the station , it is termed as broadcast

Then according to broadcast, the packet must be received and accessed by all ??

No, Why ??

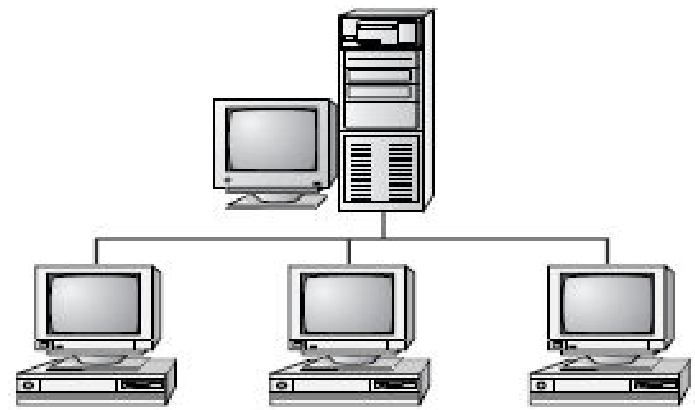


Multipoint Connection

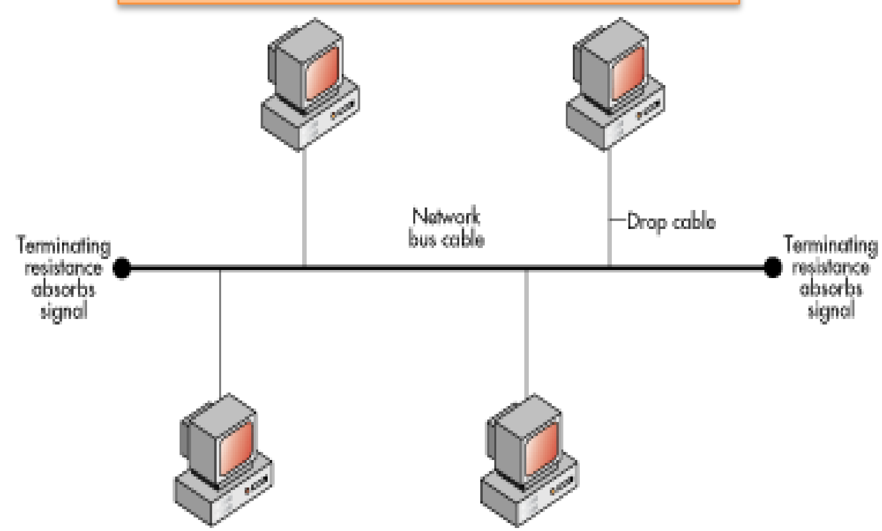


BUS Topology

- Each computer checks the address on the signal (data frame) as it passes along the bus.
- If the signal's address matches that of the computer, the computer accepts the signal.
- If the address doesn't match, the computer takes no action and the signal travels on down the bus.



Multipoint Connection



BUS Topology

Advantages

- Cheapest topology
- Only 1 cable is associated with all devices.
- Less complex network

Disadvantages

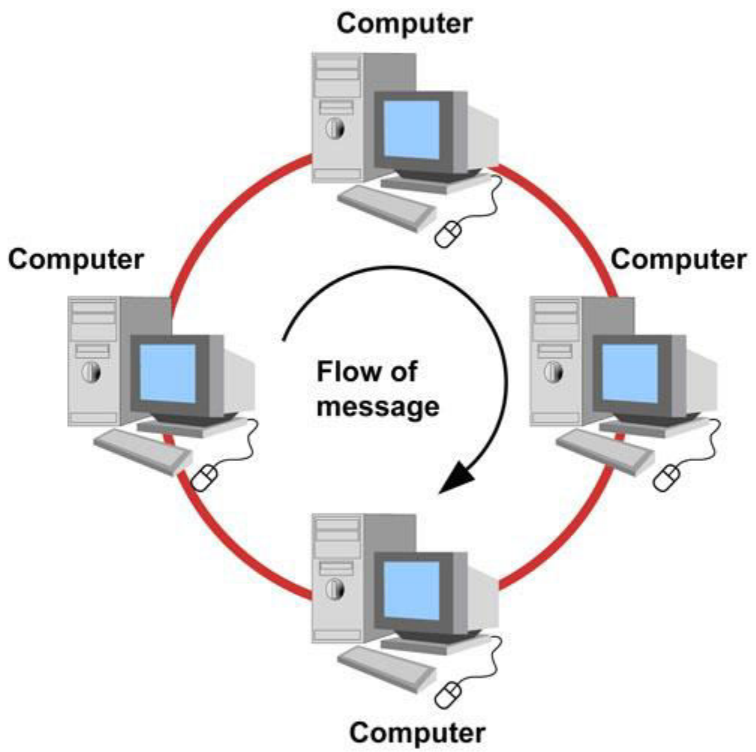
- If main cable breaks, the whole system shuts.
- Limited cable length and number of stations
- Only one device can transmit (send) data (signal) at any time.

RING Topology

- Each computer connects to two other computers, joining them in a circle creating a unidirectional path where messages move device to device.

- Each entity participating in the ring reads a message, then regenerates it (serves as a repeater) and hands it to its neighbor on a different network cable.

- "n" cables required for "n" devices



Point to Point Connection

RING Topology

Advantages

- Data is quickly transferred without a ‘bottle neck’. (very fast, all data traffic is in the same direction)
- The transmission of data is relat… …s packets travel in…
- A… …des has very litt… …dwidth

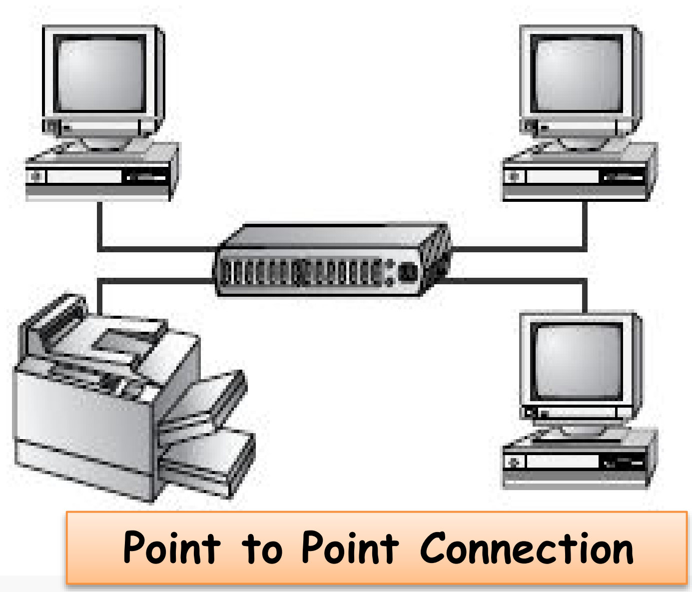
Signal transmitted with respect to time

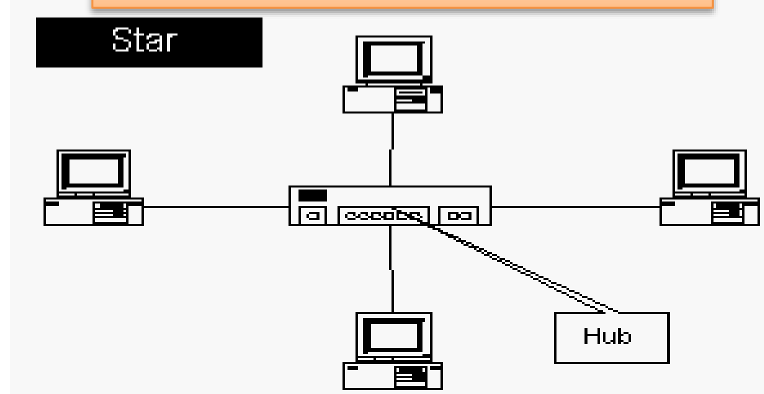
Disadvantages

- Data packets must pass through every computer between the sender and recipient therefore this makes it slower.
- If any of the nodes fail then the ring is broken and data cannot be transmitted successfully.
- In order for all computers to communicate with each other, all computers must be turned on.

STAR Topology

- All of the stations in a ***star topology*** are connected to a central unit called a ***hub.***
- If a cable is cut, it only affects the computer that was attached to it. This eliminates the single point of failure problem associated with the bus topology. (Unless, of course, the hub itself goes down.)
- Star topologies are easy to install. A cable is run from each workstation to the hub.





STAR Topology

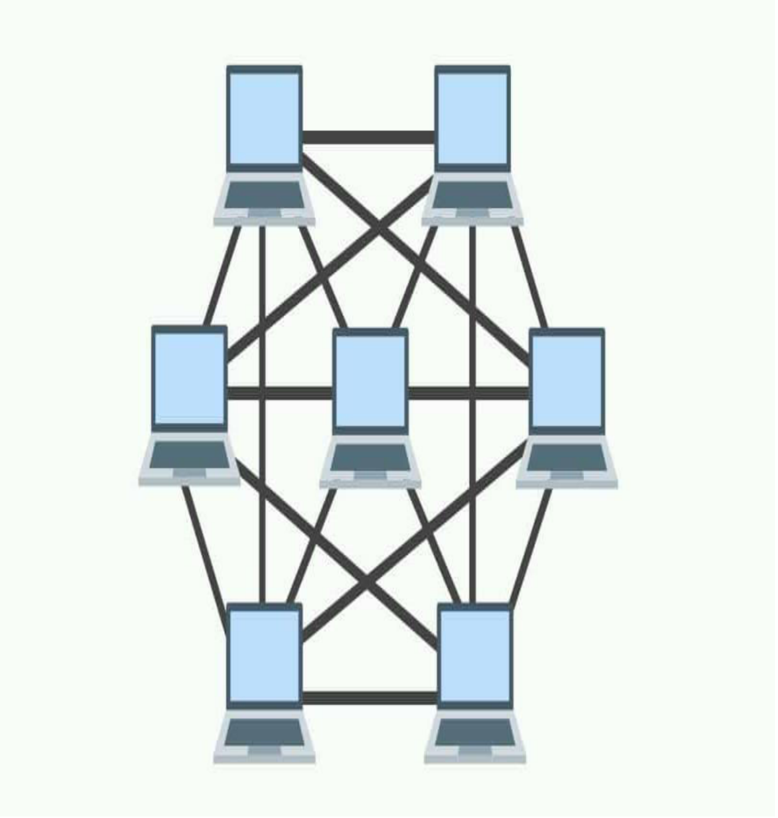
- Star topologies are normally implemented using twisted pair cable, specifically unshielded twisted pair (UTP).
- Star topologies are more expensive to install than bus networks, because there are several more cables that need to be installed, plus the cost of the hubs that are needed.

- Advantages of star topology:
  - Easy to add new stations
  - Easy to monitor and troubleshoot
  - Failure of one station does not affect the whole system

- Disadvantages of star topology:
  - Failure of hub cripples attached stations
  - More cable required

MESH Topology

- Simplest logical topology in terms of data flow, but it is the most complex in terms of physical design.
- In this physical topology, each device is connected to every other device
- Very rare topology
- For ‘n’ devices n(n-1)/2 cables required
- The only advantage is high fault tolerance.



- **Thank You**
- **Discussion & Doubt session will be in lecture.**

Important terms to keep in mind

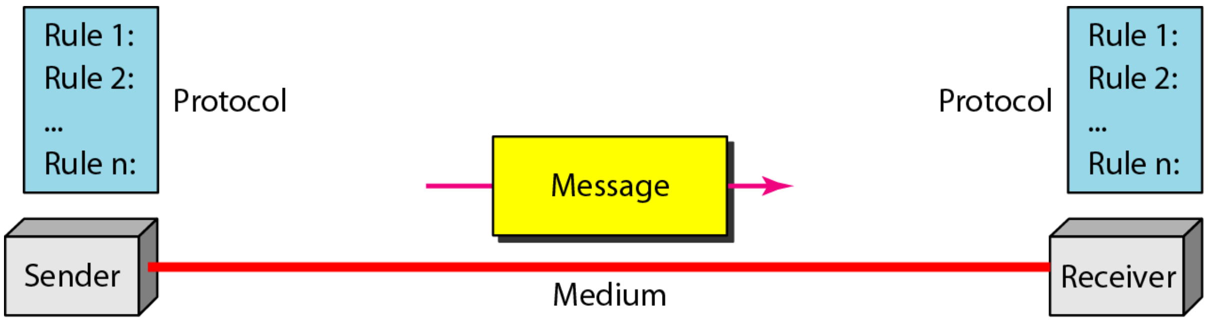
1. **<u>Categories of Network</u>**
2. **<u>Simplex, Half Duplex and Duplex network</u>**
3. **<u>Bus, Ring, Star, Mesh topology</u>**

COMPUTER NETWORKS (BCSC 0008)

Lecture 3

Analyzing components in N/W

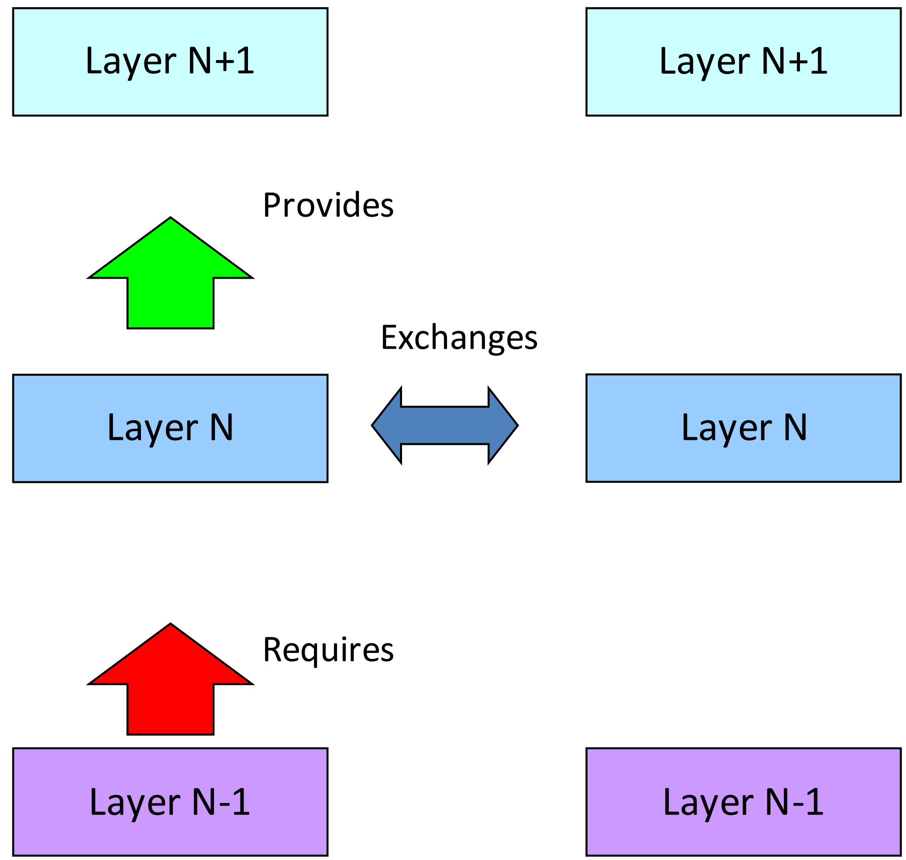
- Previously discussed components are
  - Sender
  - Receiver
  - Message
  - Medium
  - Protocol
  - MUX/DEMUX
  - Modem
  - Transceiver (Optional)



Demultiplexer:It takes single input and gives several output.
Multiplexer :It takes several input and gives one output

Network Models

- Network models use **layers** to describe networks
- Each layer describes the **services** provided to the layer above it and those required from the layer below it
- It also describes the format of exchanges between **peer** layers on different network hosts
- Because the layers "**stack**" on top of one another, we often refer to network protocol "stacks" when we talk about the implementation



- **Building complex systems is hard!**
  - **Approach: "Divide and conquer".**
  - **Split job into smaller jobs, or layers.**

Each step dependent on the previous step but does not need to be aware of how the previous step was done.

Analogy: Air Travel

- *The problem: air travel.*
- *Decomposed into series of steps:*

Arrival at airport	Departure from airport
Check-in	Baggage claim (check out)
Boarding	Deplane
Takeoff	Landing

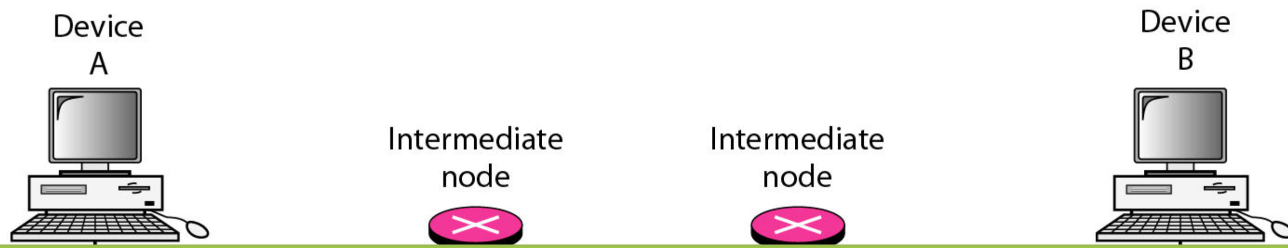
Traveling

Network Models

- The most well-known network model is the OSI (Open Systems Interconnect) Reference Model defined and maintained by the Organization for International Standardization (ISO)
- It consists of seven layers, numbered from the bottom (closest the network) to the top (closest the user)

Layer 7 – Application
Layer 6 – Presentation
Layer 5 – Session
Layer 4 – Transport
Layer 3 – Network
Layer 2 – Data Link
Layer 1 – Physical

The interaction between layers in the OSI model



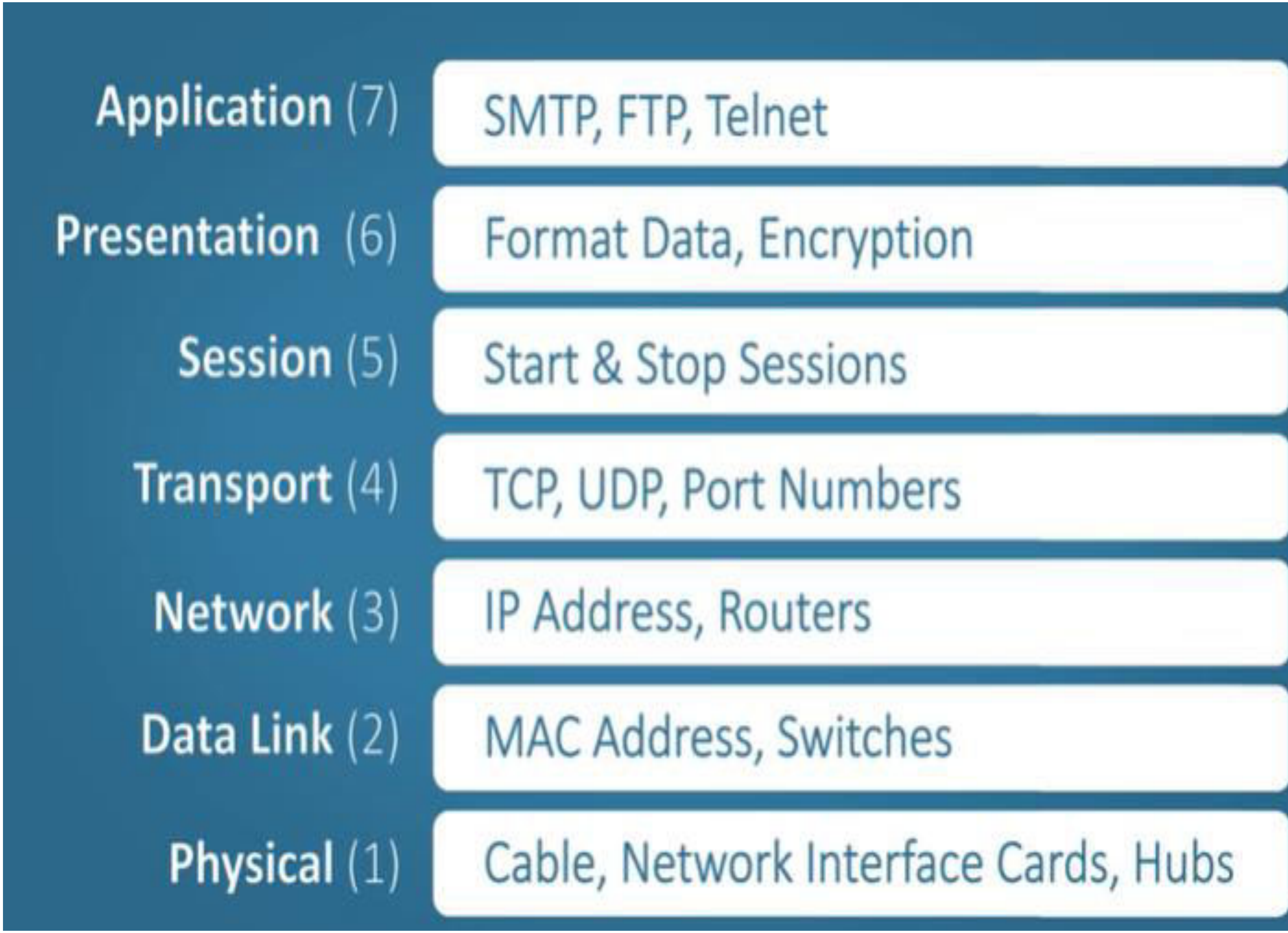
On <u>Intermediary Device</u> Data Packet <u>can not cross NETWORK Subgroup</u>,

Only on <u>SENDING & RECEIVING Device</u> Data Packet <u>can cross all 7 Layers</u>

On Sending device packet cross all 7 layers from top to bottom (Application to Physical)

On Receiving device packet cross all 7 layers from bottom to top (Physical to Application)

On Intermediary device packet cross only 3 layers from top to bottom (Physical to Network & Network to Physical)


Application (7)
SMTP, FTP, Telnet
Presentation (6)
Format Data, Encryption
Session (5)
Start & Stop Sessions
Transport (4)
TCP, UDP, Port Numbers
Network (3)
IP Address, Routers
Data Link (2)
MAC Address, Switches
Physical (1)
Cable, Network Interface Cards, Hubs

Encapsulation/Decapsulation

- At Sender Site, each layer add its own information to the data received from its upper layer (Called as HEADER). (HEADER + DATA= DATA for next lower layer)

- This HEADER can be accessed (add/remove) only by specific layer
- At Receiver Site, This HEADER is removed (on matching certain conditions) only by the layer that has added the HEADER at sender site.

- **Thank You**
- **Discussion & Doubt session will be in lecture.**

Important terms to keep in mind

1. **Network Model**
2. **Encapsulation / Decapsulation**
3. **Peer to Peer process**
4. **OSI model**

OSI Reference Model

- Layer 1 – The Physical Layer
  - Defines the type of media to be used
  - What order are bits transmitted (if serial or parallel)?
  - Data Rate or Transmission Rate
  - Line Configuration (P2P / MP)
  - Physical Topology
  - Transmission Mode (Simplex, Half/ Full Duplex)
  - Defines representation of data on the medium
    - Is a ‘0’ “high” or “low”, “on” or “off”?

Layer 1 – Physical

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

OSI Reference Model

- Layer 2 – The Data Link Layer
  - Defines "right to transmit" rules (Access Control)
  - Provides directly-connected hop-to-hop data transfer (Hop to Hop / Node to Node Delivery)
  - Defines higher-level structure of data (frames)
  - Defines "physical" address structure for hosts (Physical Addressing)
  - Error Control
  - Flow Control

Layer 2 – Data Link
Layer 1 – Physical

The data link layer is responsible for moving frames from one hop (node) to the next.

OSI Reference Model

- Layer 3 – The Network Layer
  - Provides end-host-to-end-host data transfer across multiple data links (host to host/ source to destination delivery)
  - Defines higher-level structure of data (packets)
  - Defines "abstract" address structure for host (Logical Addressing)
  - Routing
  - Delivery and Forwarding

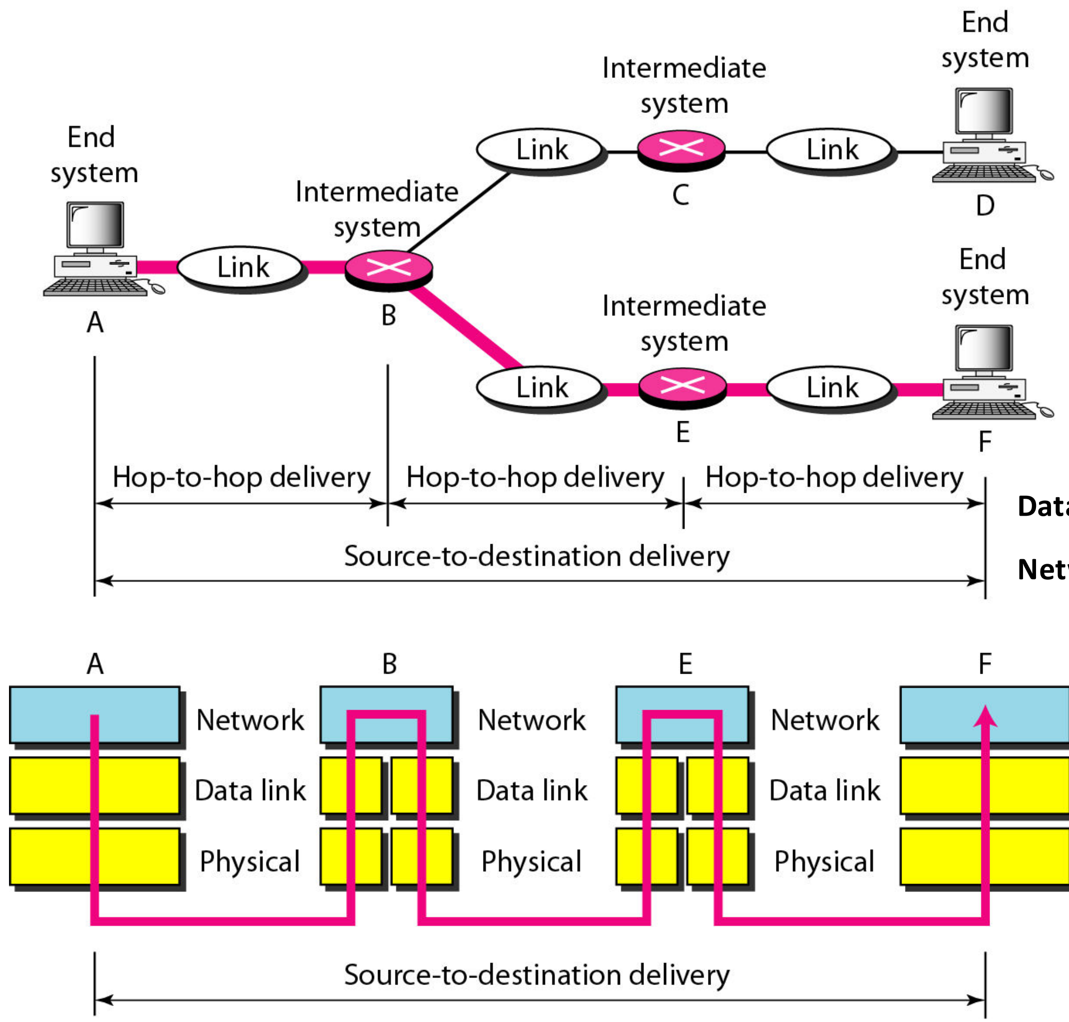
Layer 3 – Network

Layer 2 – Data Link

Layer 1 – Physical

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Figure 2.9 *Source-to-destination delivery*

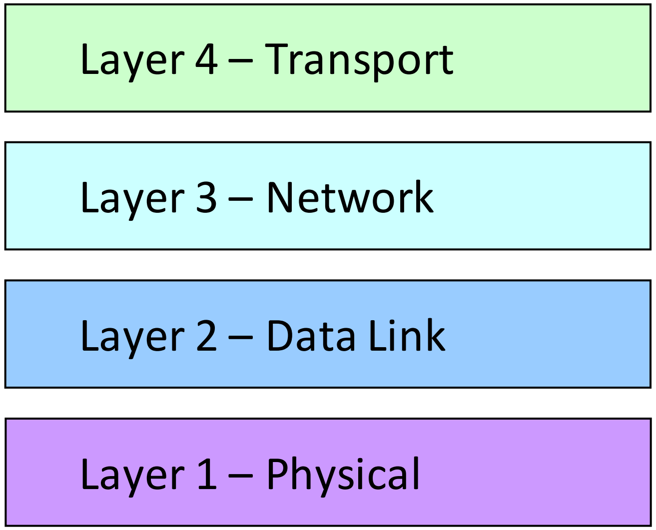


Data Link Layer- Hop to Hop

Network Layer- Source to Destination

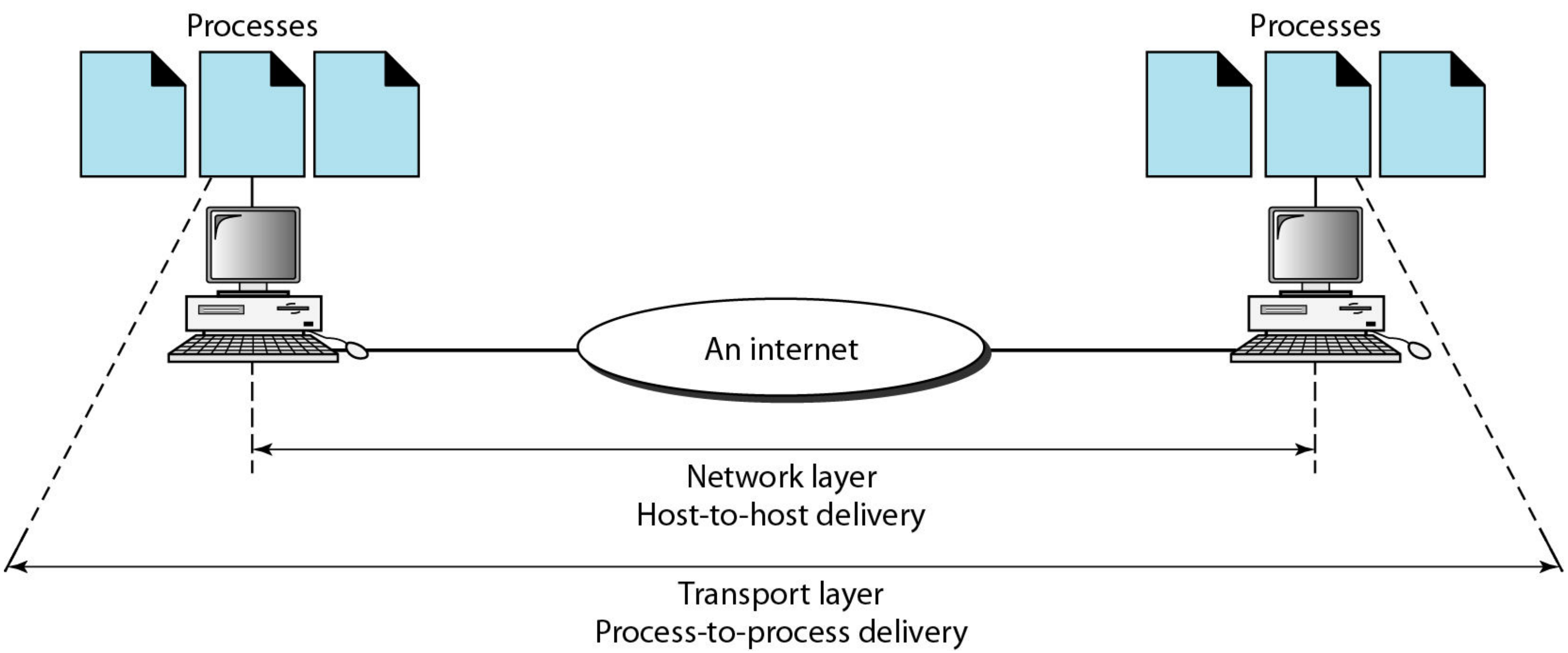
OSI Reference Model

- Layer 4 – The Transport Layer
  - Provides process-to-process data transfer
  - *May* provide for reliable data transfer
  - Defines higher-level structure for data (datagrams, streams, etc.)
  - Defines "port" addresses for services (processes)



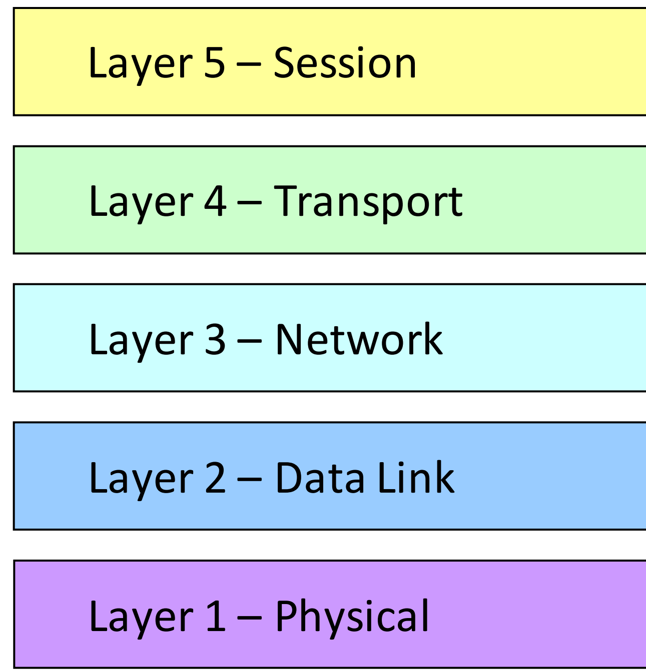
The transport layer is responsible for the delivery of a message from one process to another.

Figure 2.11 *Reliable process-to-process delivery of a message*



OSI Reference Model

- Layer 5 – The Session Layer
  - Provides a logically persistent connection between processes
  - May involve user or host authentication (login), transaction encapsulation (for database access), etc.



The session layer is responsible for dialog control and synchronization.

OSI Reference Model

- Layer 6 – The Presentation Layer
  - Defines the network representation of data
  - Converts between the network and host representations of data (ASCII/EBCDIC, byte order, encryption, compression, etc.)

Layer 6 – Presentation

Layer 5 – Session

Layer 4 – Transport

Layer 3 – Network

Layer 2 – Data Link

Layer 1 – Physical

The presentation layer is responsible for translation, compression, and encryption.

OSI Reference Model

- Layer 7 – The Application Layer
  - Provides a portal for the application to access the network
  - Describes the dialog between two applications communicating across the network.

Layer 7 – Application

Layer 6 – Presentation

Layer 5 – Session

Layer 4 – Transport

Layer 3 – Network

Layer 2 – Data Link

Layer 1 – Physical

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

Summary of OSI Layers

Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1

- **Thank You**
- **Discussion & Doubt session will be in lecture.**

Important terms to keep in mind

1. **OSI model and services of layers**

COMPUTER NETWORKS
(BCSC 0008)

Lecture 4
TCP/IP Model and Addressing

Previous discussed topics:

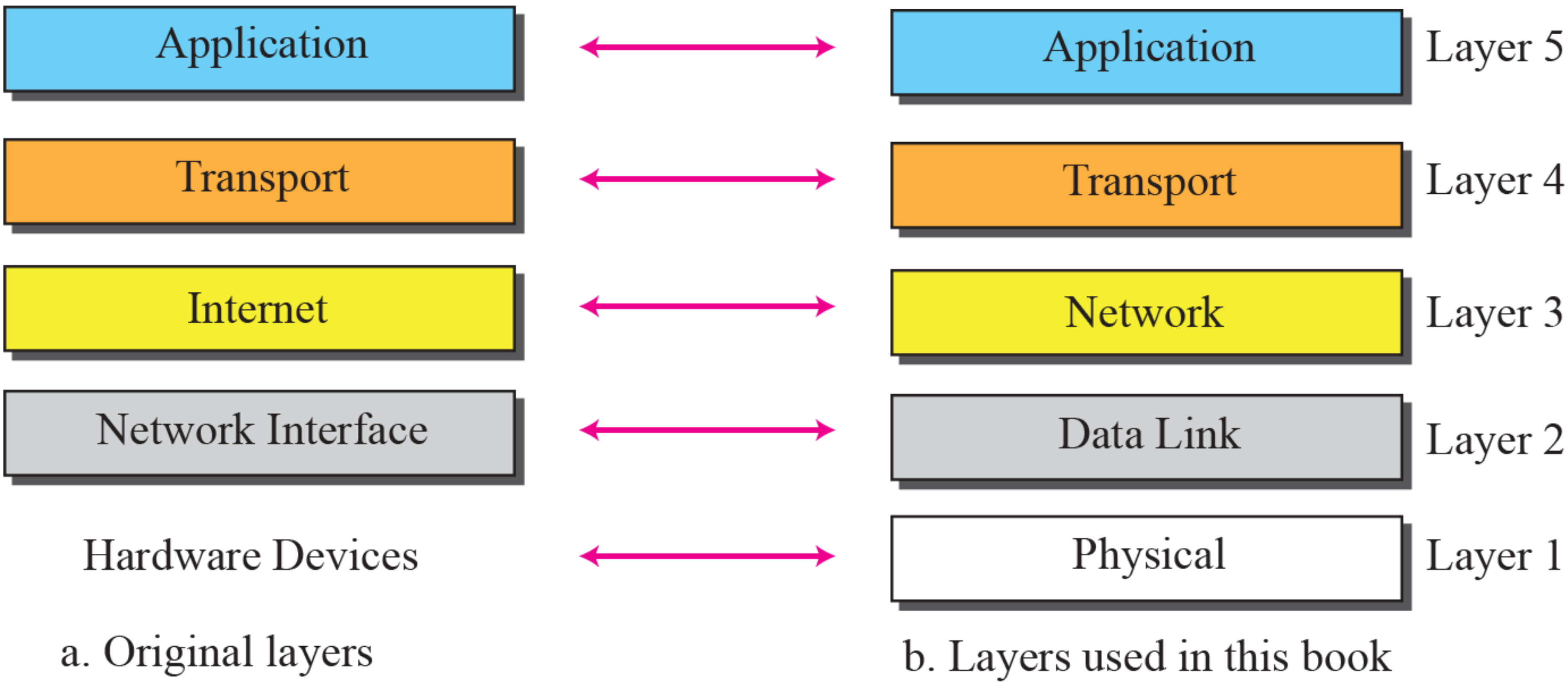
1. **Network Model**
2. **OSI Model**
3. **7 Layers of OSI** (Application, Presentation, Session, Transport, Network, Data Link & Physical)
4. **Encapsulation/Decapsulation, Peer to Peer, Support groups of OSI**

Now we will discuss:

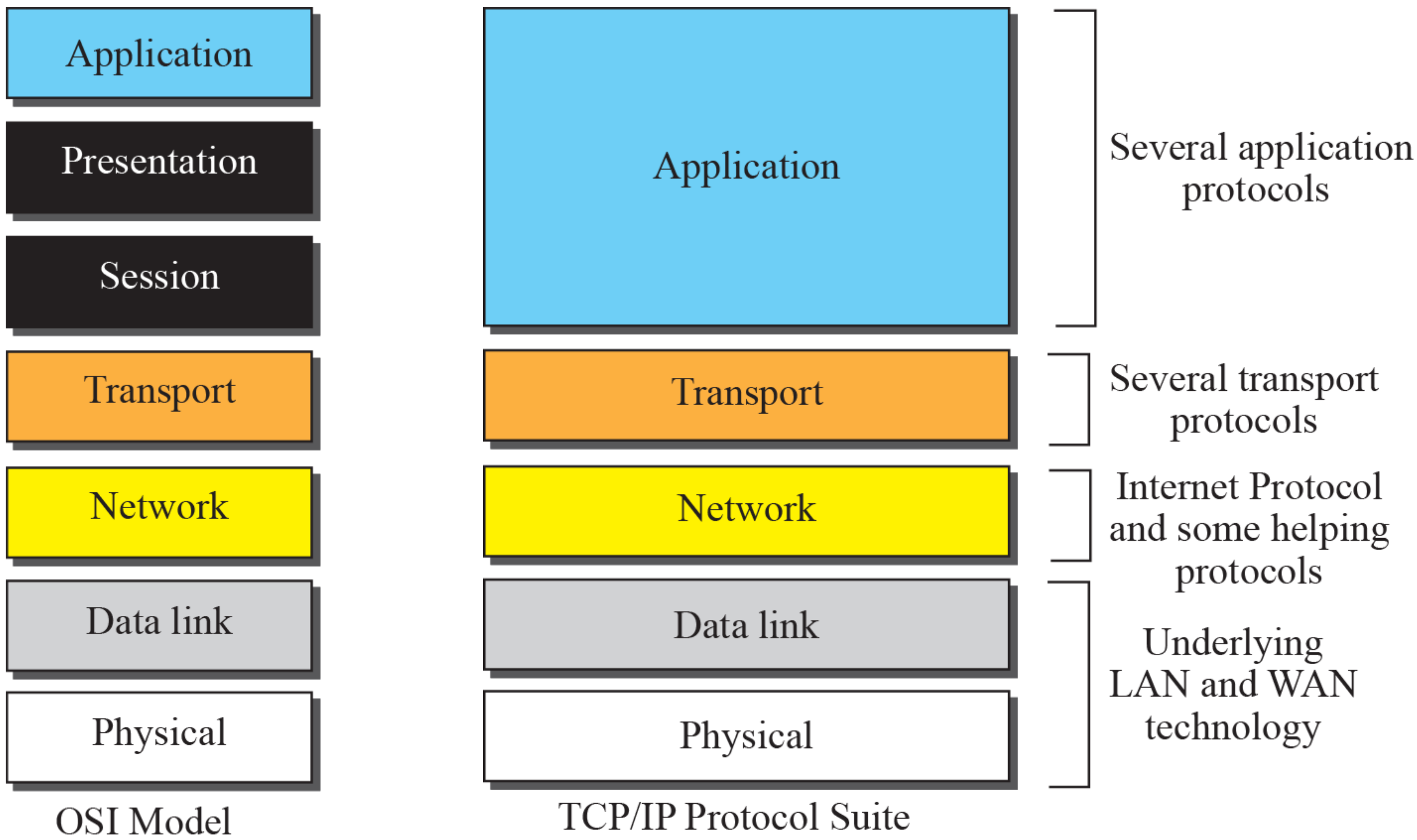
1. **TCP/IP Model**
2. **Comparison OSI vs. TCP/IP**
3. **Different Addresses used in OSI for Communication**

TCP/IP PROTOCOL SUITE

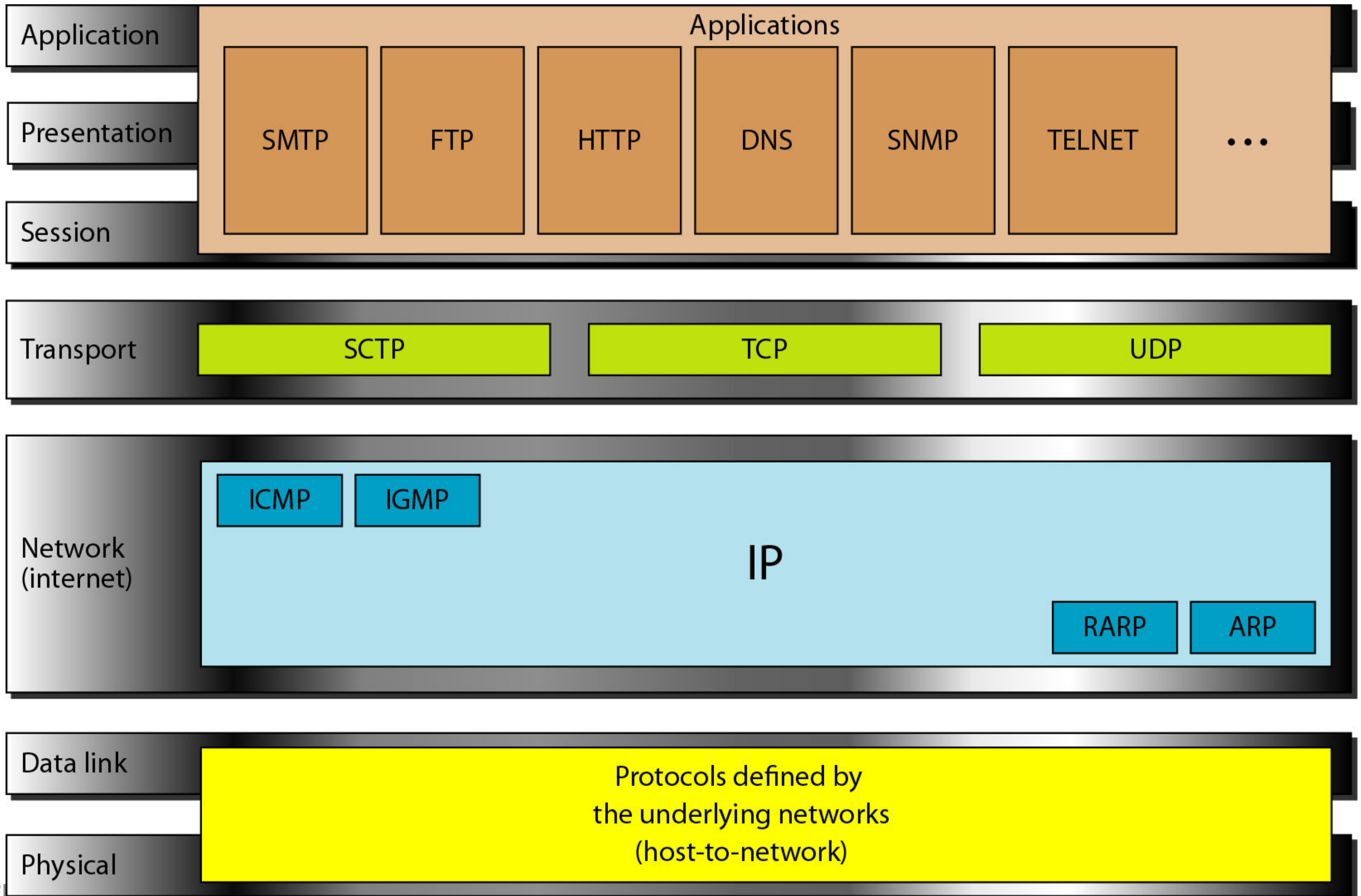
The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not match exactly with those in the OSI model. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model with the layers named similarly to the ones in the OSI model.


Application
Transport
Internet
Network Interface
Hardware Devices
a. Original layers
Application
Transport
Network
Data Link
Physical
Layer 5
Layer 4
Layer 3
Layer 2
Layer 1
b. Layers used in this book

TCP/IP and OSI model Ref: Fourozan 4th Ed.

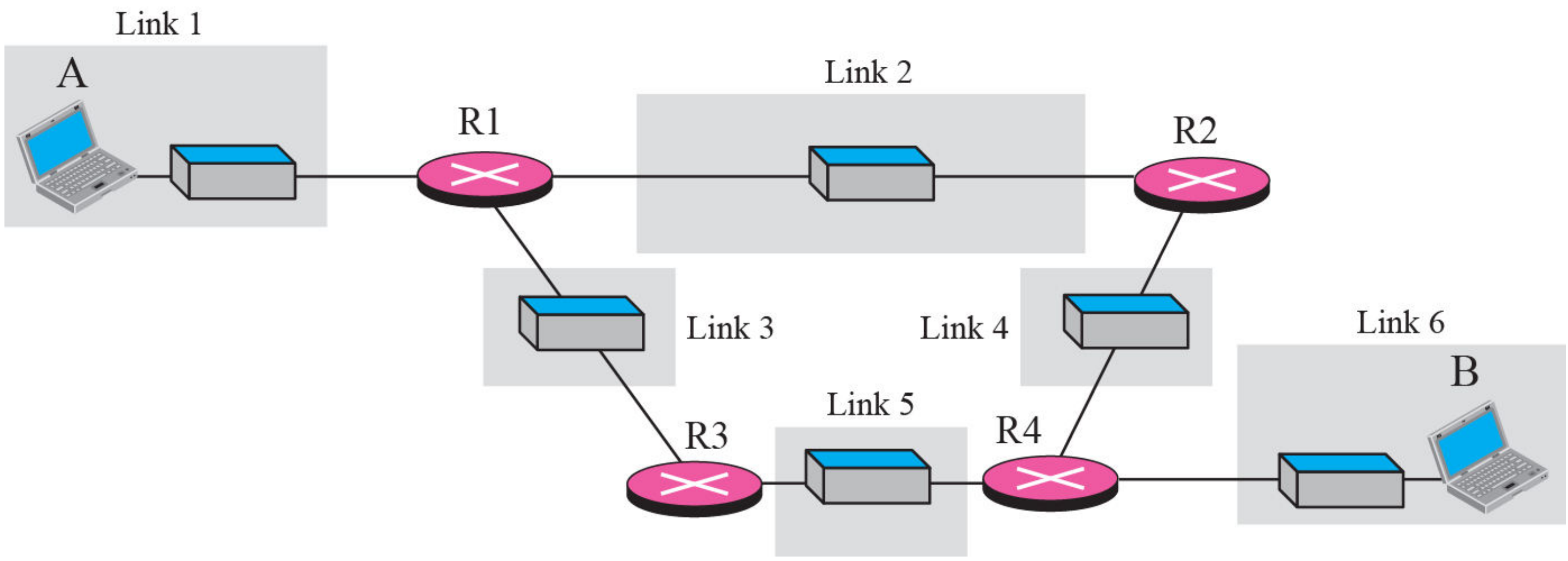


TCP/IP PROTOCOL SUITE

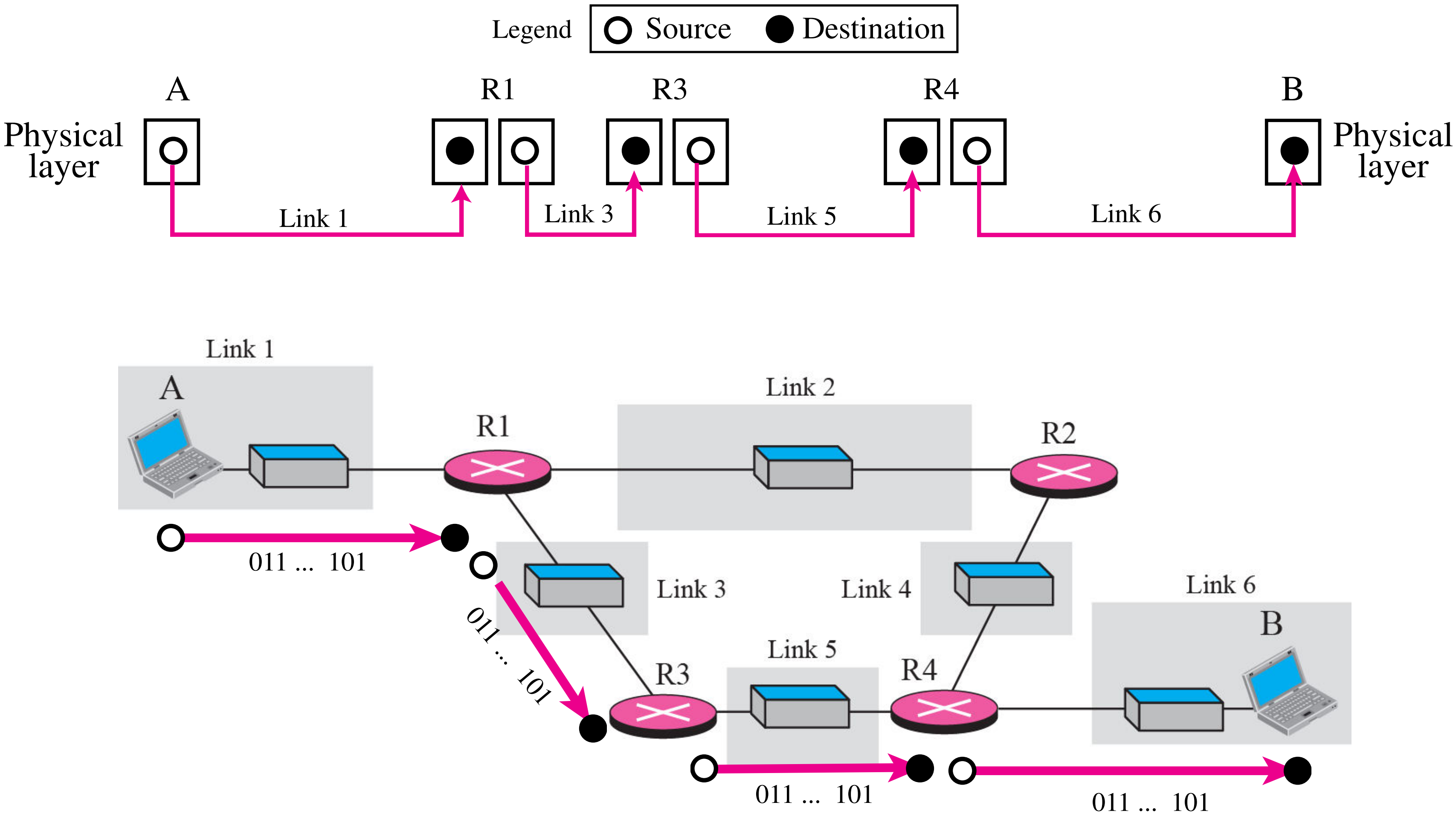


SMTP-Simple Mail Transfer Protocol
FTP-File Transfer Protocol
HTTP-Hyper Text Transfer Protocol
DNS-Domain Name System
SNMP-Simple Network Management Protocol
TELNET-Teletype Network
SCTP-Stream Control Transmission Protocol
TCP-Transmission Control Protocol
UDP-User Datagram Protocol
ICMP-Internet Control Message Protocol
IGMP-Internet Group Management Protocol
RARP-Reverse Address Resolution Protocol
ARP-Address Resolution Protocol

A private internet Ref: Fourozan 4th Ed.



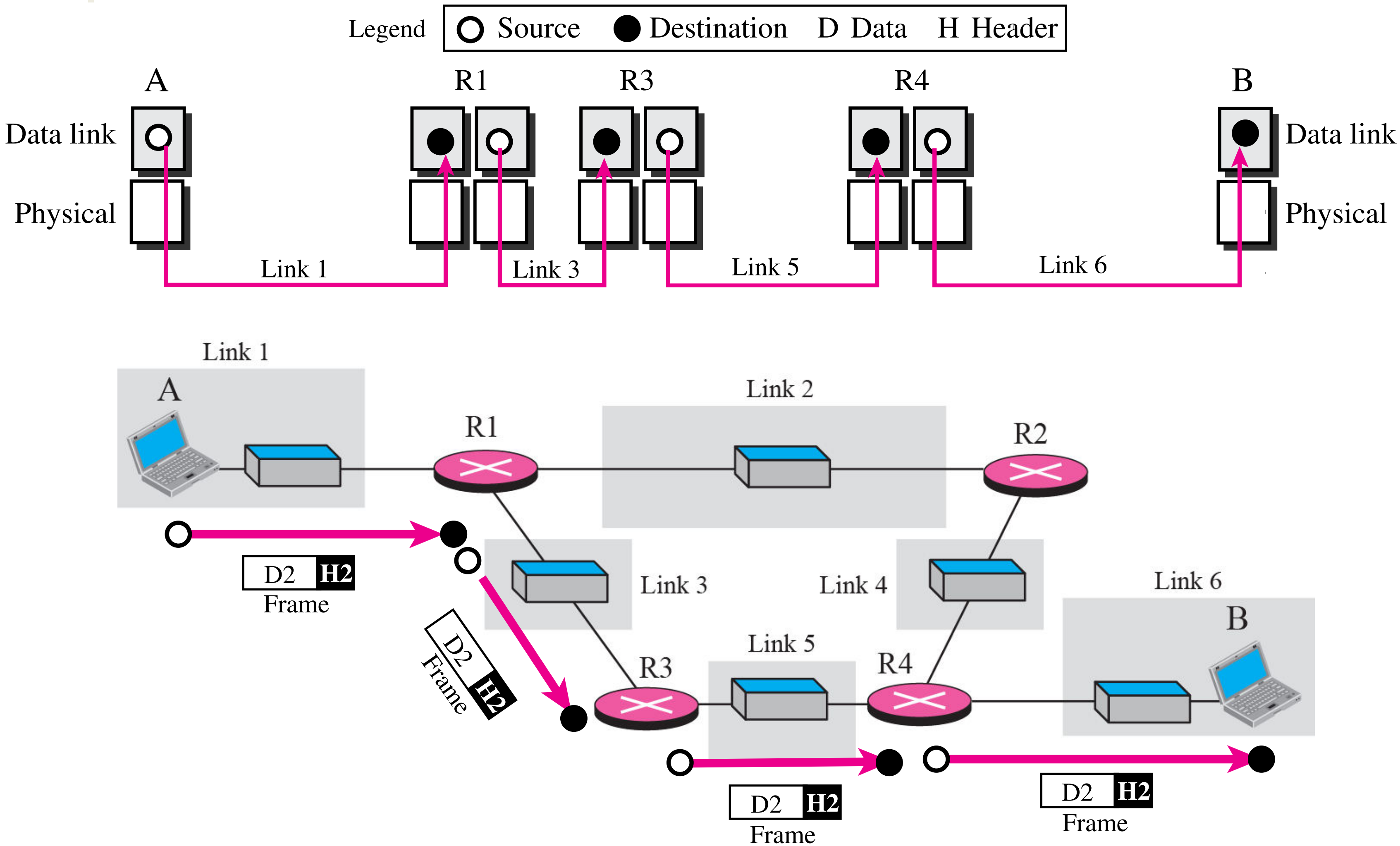
Communication at the physical layer Ref: Fourozan 4th Ed.



Note

The unit of communication at the physical layer is a bit.

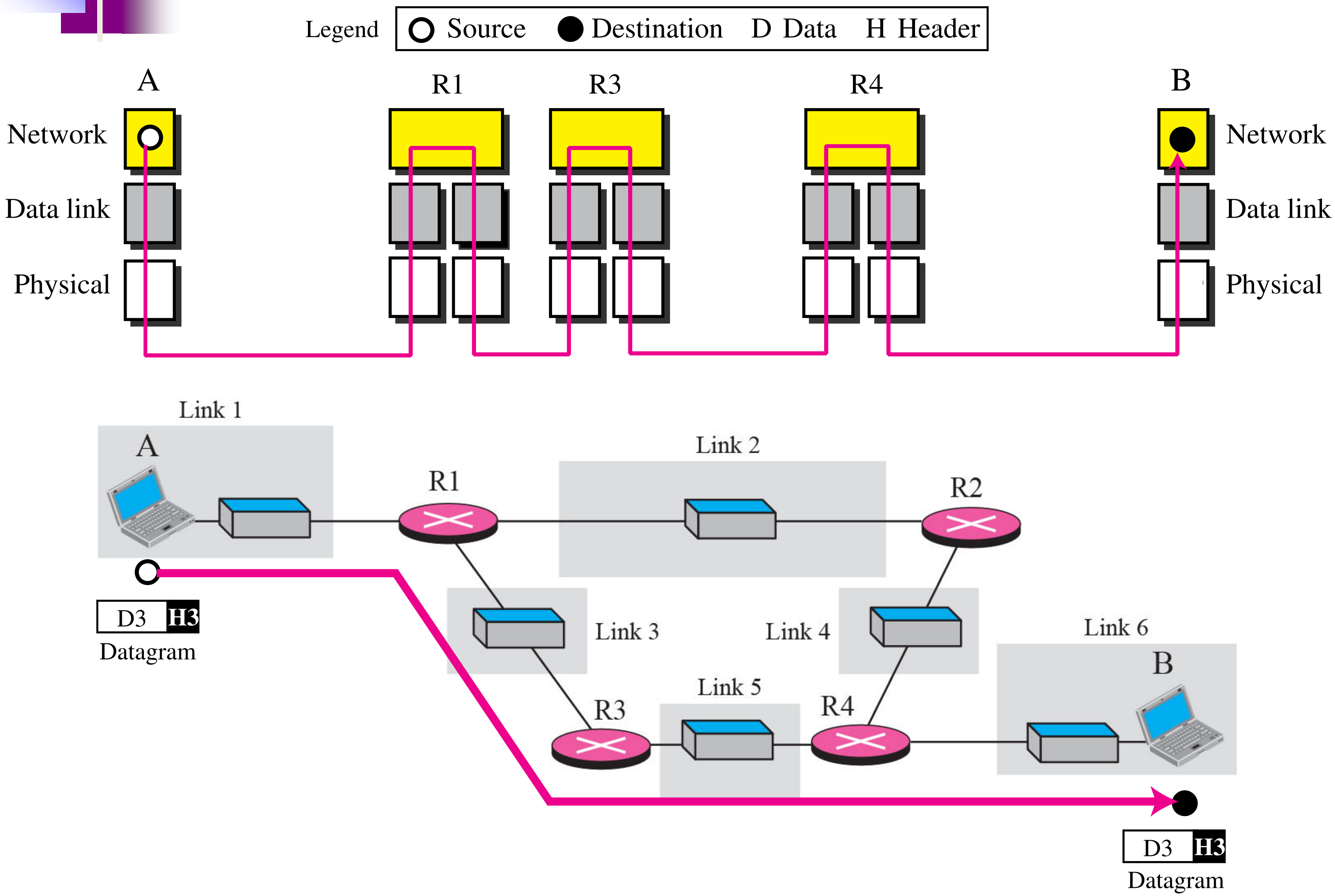
Figure 2.11 *Communication at the data link layer*



Note

The unit of communication at the data link layer is a frame.

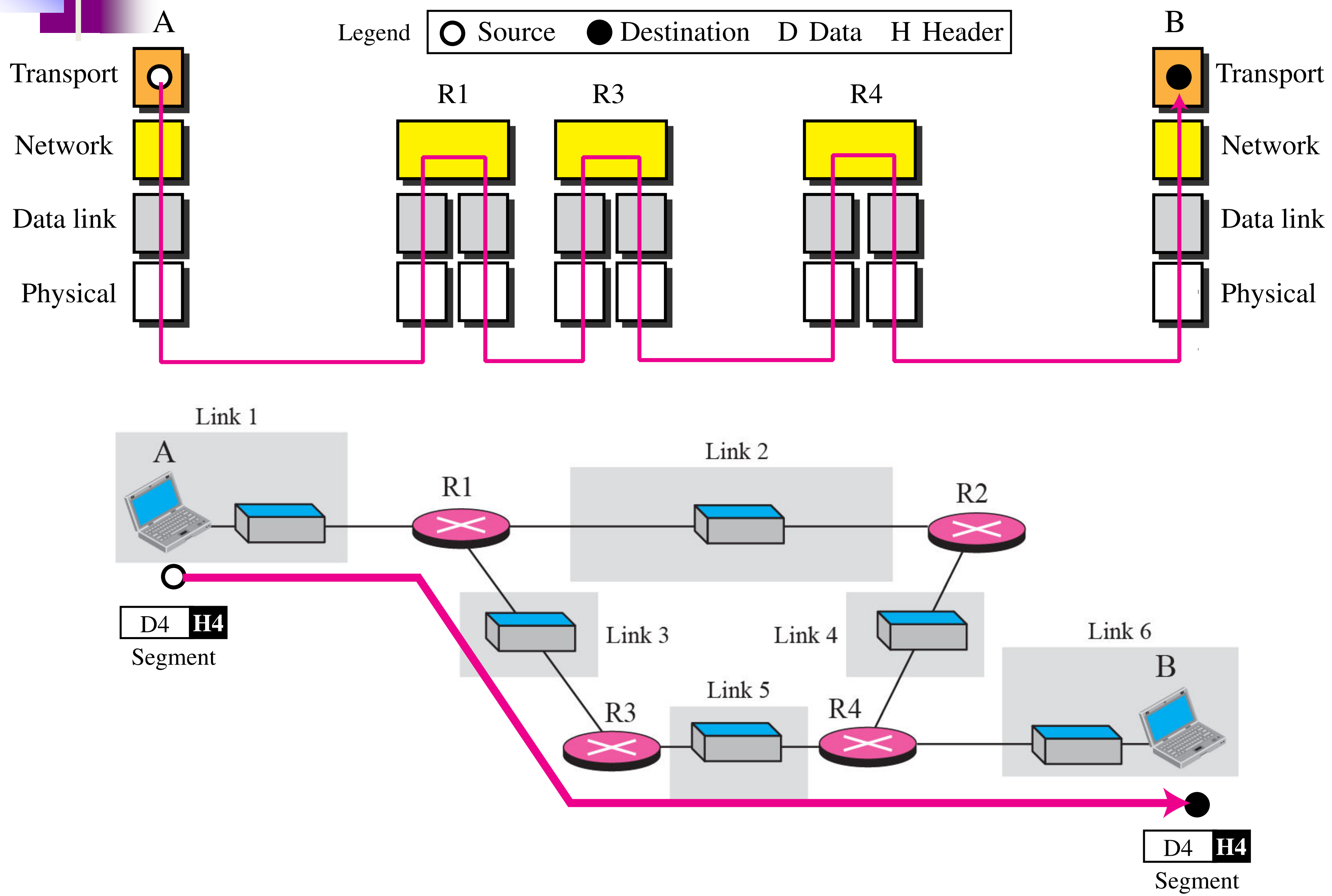
Figure 2.12 *Communication at the network layer*



Note

The unit of communication at the network layer is a datagram or packet.

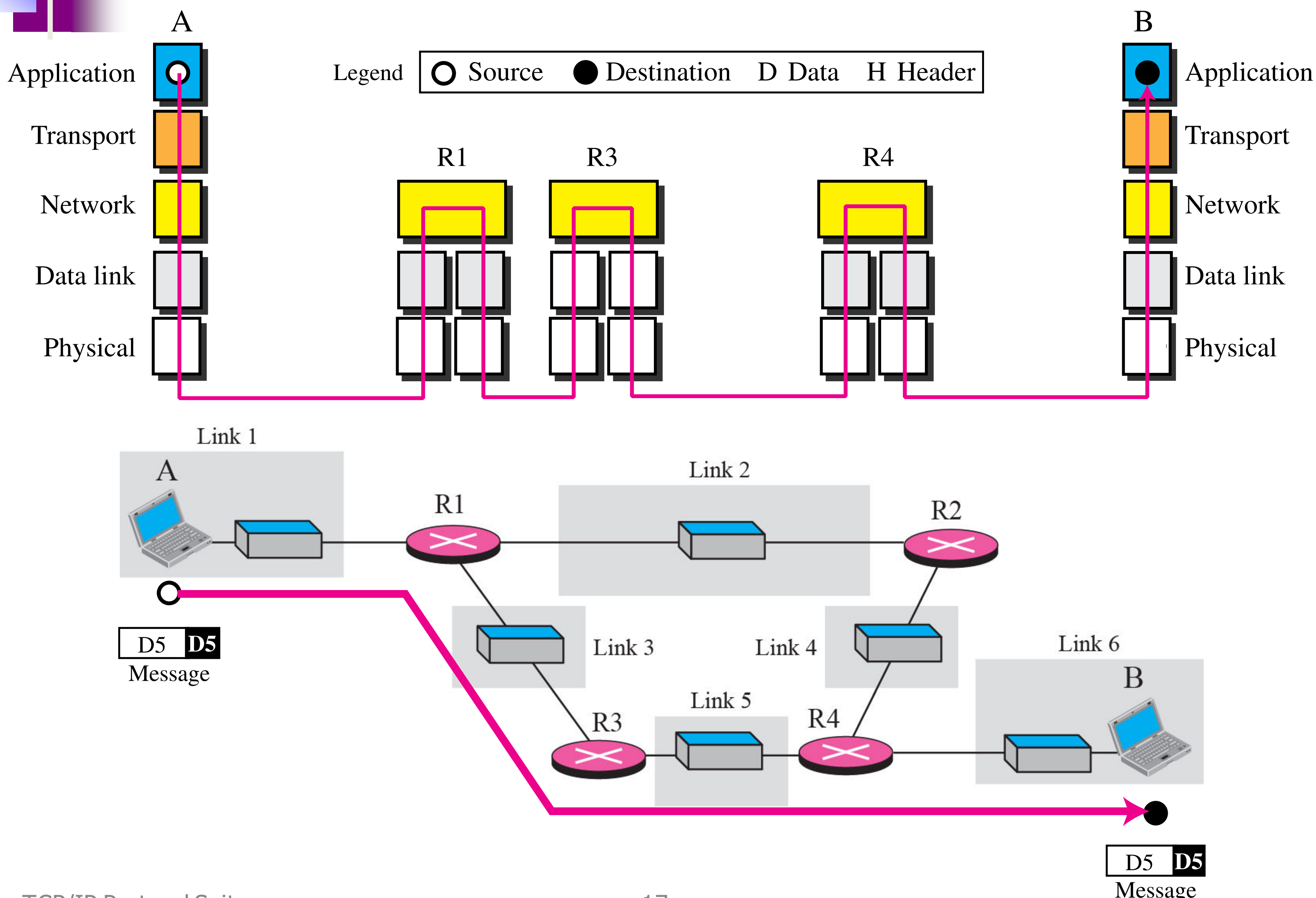
Figure 2.13 *Communication at transport layer*



Note

The unit of communication at the transport layer is a segment, user datagram, or a packet, depending on the specific protocol used in this layer.

Figure 2.14 *Communication at application layer*



Note

The unit of communication at the application layer is a message.

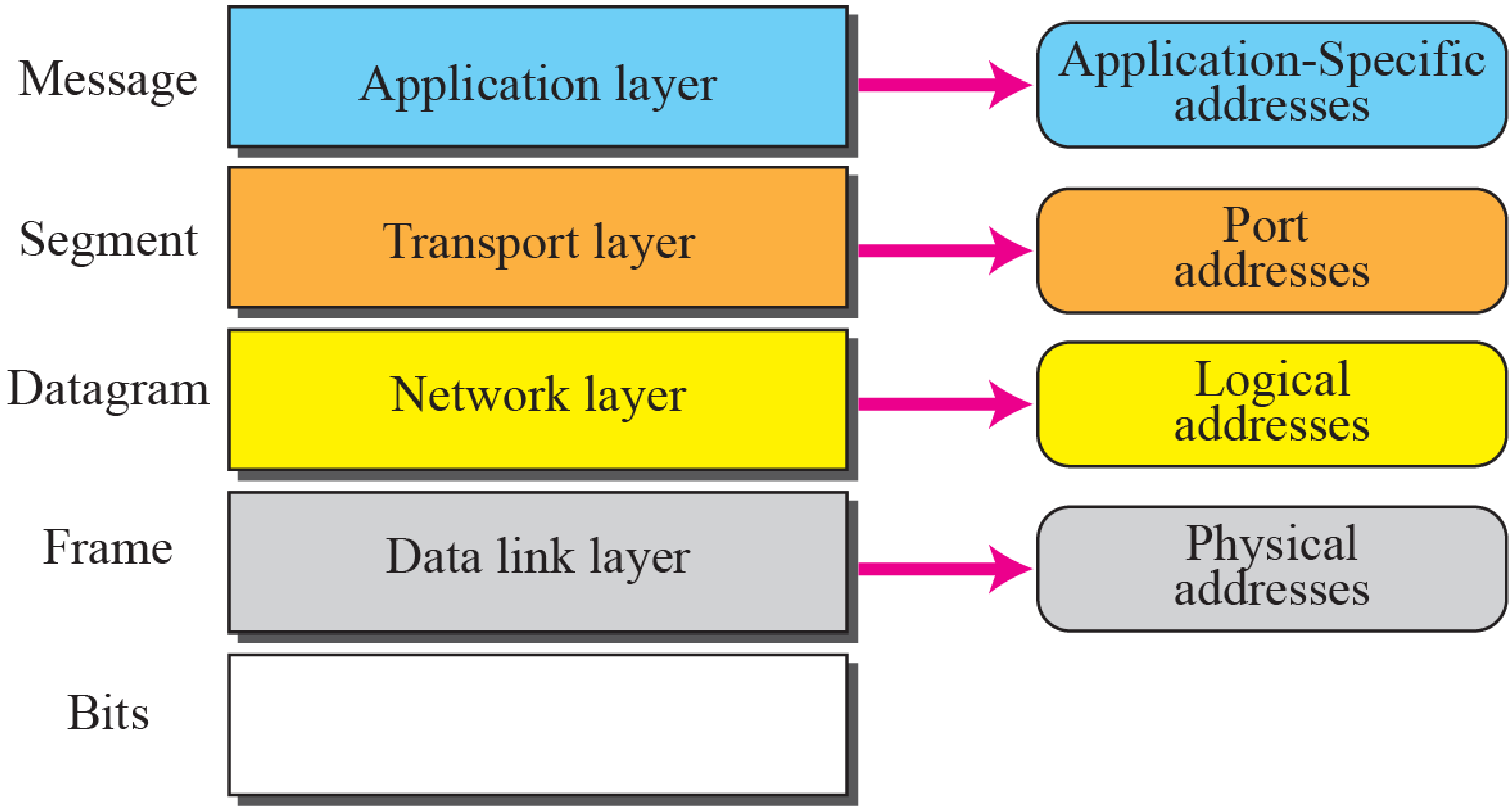
2-4 ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical address, logical address, port address, and application-specific address. Each address is related to a one layer in the TCP/IP architecture, as shown in Figure 2.15.

Topics Discussed in the Section

- ✓ Physical Addresses
- ✓ Logical Addresses
- ✓ Port Addresses
- ✓ Application-Specific Addresses

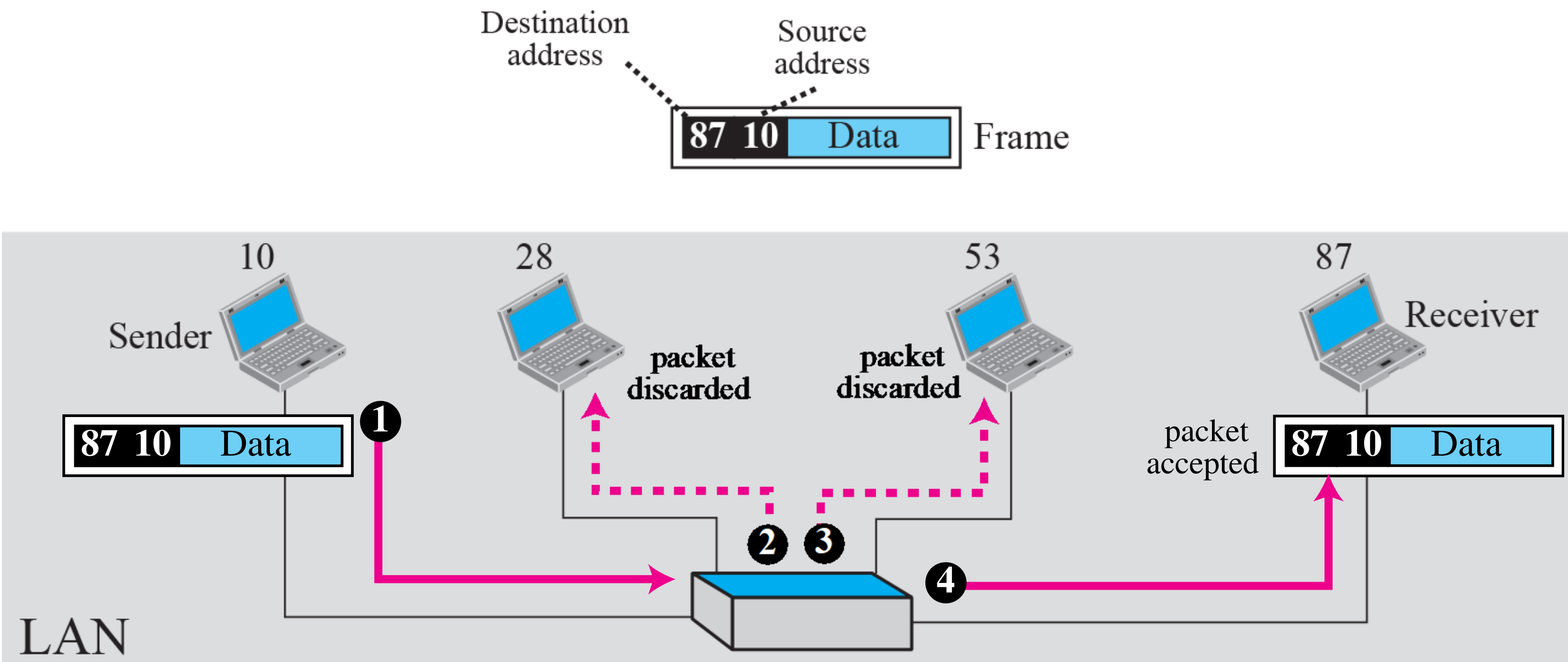
Figure 2.15 *Addresses in the TCP/IP protocol suite*



Example 2.3

In Figure 2.16 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (a LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame. The frame is propagated through the LAN. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address.

Figure 2.16 *Example 2.3: physical addresses*



Example 2.4

As we will see in Chapter 3, most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

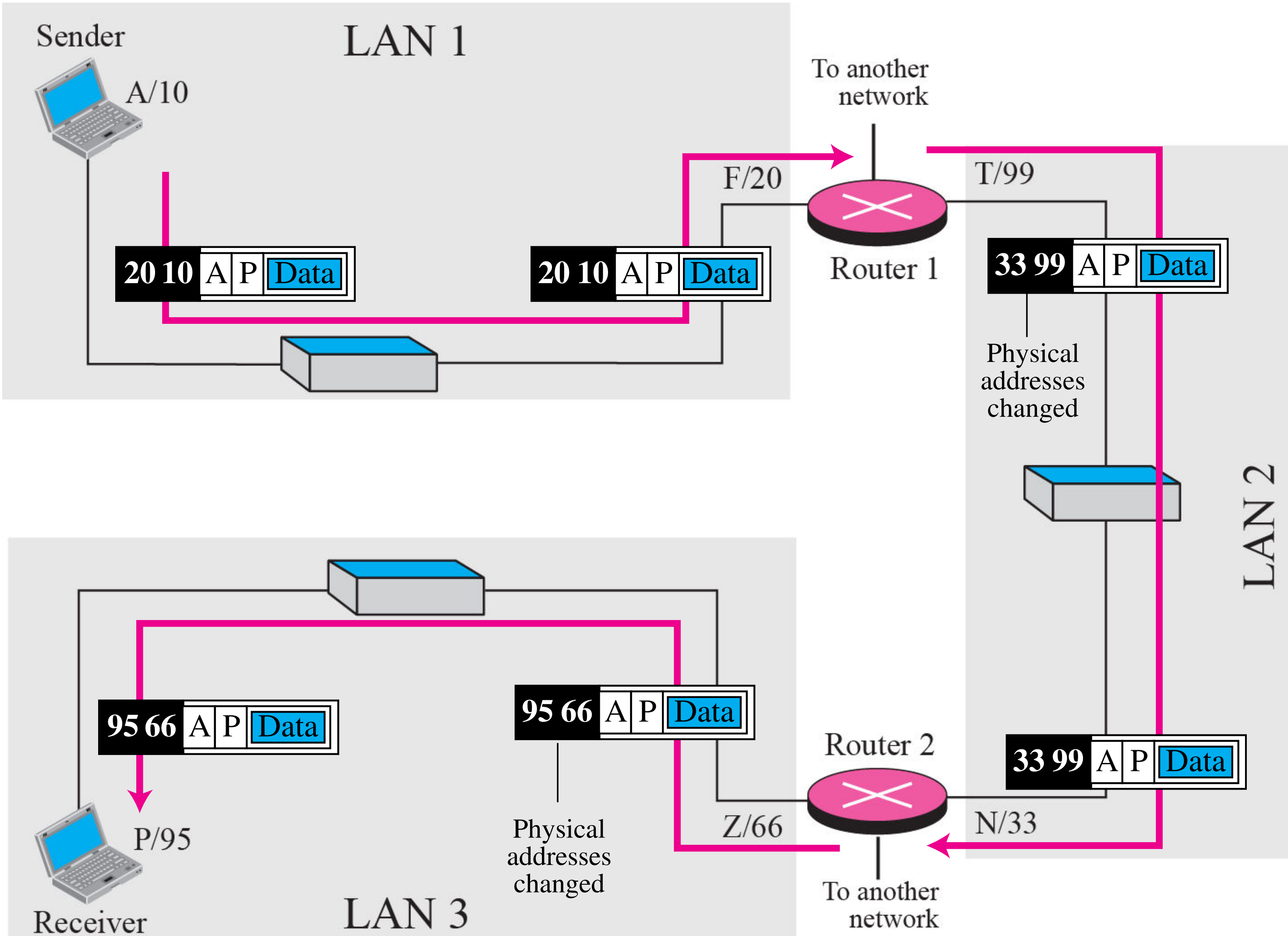
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address

Example 2.5

Figure 2.17 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks. So each router has three pairs of addresses, one for each connection. Although it may be obvious that each router must have a separate physical address for each connection, it may not be obvious why it needs a logical address for each connection. We discuss these issues in Chapters 11 and 12 when we discuss routing. The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95. We use letters to show the logical addresses and numbers for physical addresses, but note that both are actually numbers, as we will see in later chapters.

Figure 2.17 *Example 2.5: logical addresses*



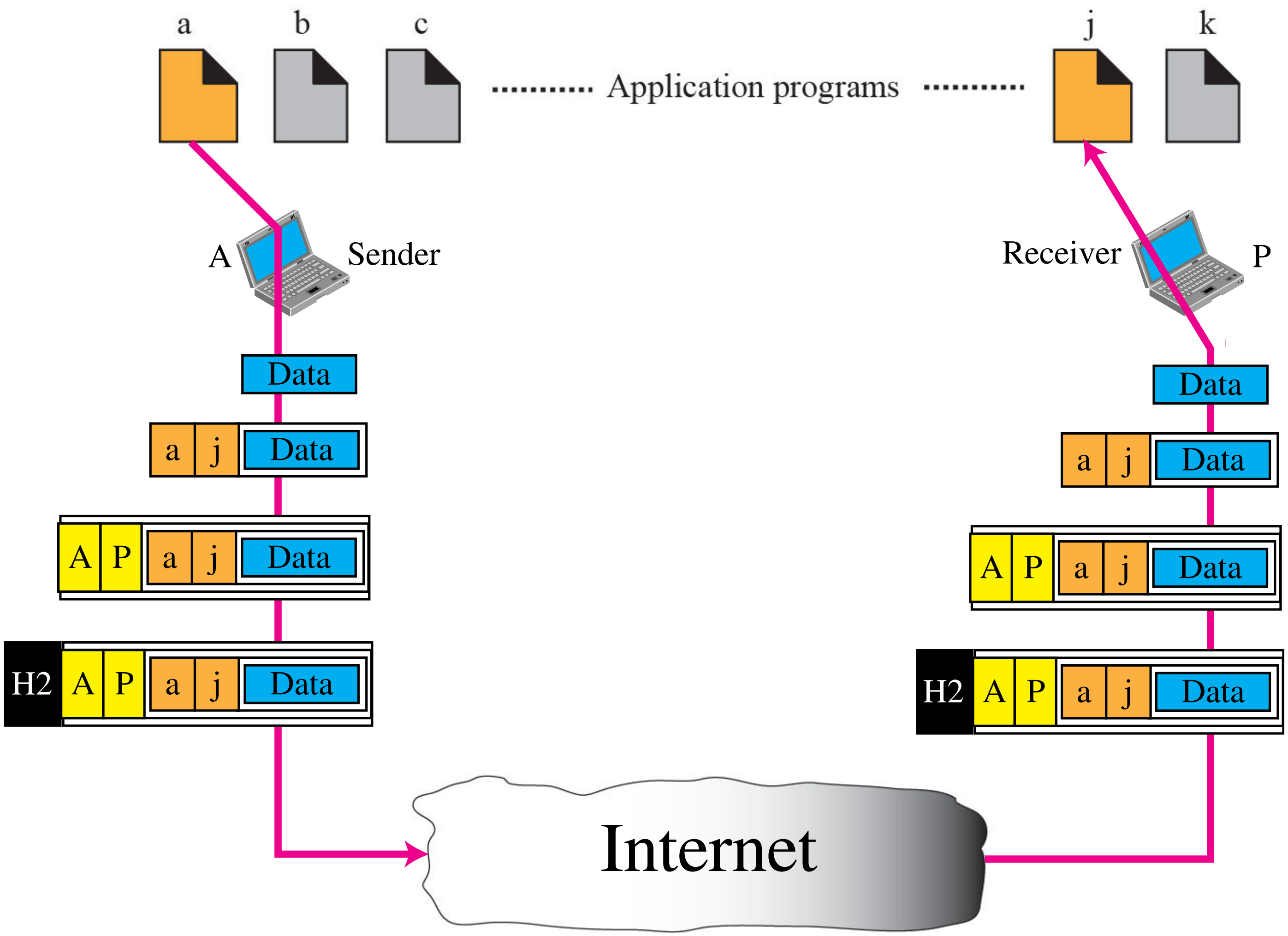
Note

The physical addresses will change from hop to hop, but the logical addresses remain the same.

Example 2.6

Figure 2.18 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program, as we will see in Chapter 17.

Figure 2.18 *Example 2.6: port numbers*



Note

The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.

Example 2.7

As we will see in future chapters, a port address is a 16-bit address represented by one decimal number as shown.

753
A 16-bit port address represented as one single number

- **Thank You**
- **Discussion & Doubt session will be in lecture.**

Important terms to keep in mind.

COMPUTER NETWORKS (BCSC 0008)

DATA & SIGNALS
Chapter 3 (FOUROZAN 4th Edition)

Text and Reference Books

Text Books:

1. Fourouzan B. A. (2004), “Data Communication and Networking”, 4th Edition, McGraw-Hill.

References:

1. Kurose, J. F. and Ross K. W. (2005), “Computer Networking: A Top-Down Approach Featuring the Internet”, 3rd Edition, Addison-Wesley.
2. A. S. Tanenbaum (2006), “Computer Networks”, 2nd Edition, Prentice Hall India.

Previous discussed topics:

1. **OSI Model**
2. **TCP/IP Model**
3. **Addressing**

Now we will discuss:

1. **Data & Signals**
2. **Periodic Analog Signals & Digital Signals**
3. **Transmission Impairments**
4. **Latency**

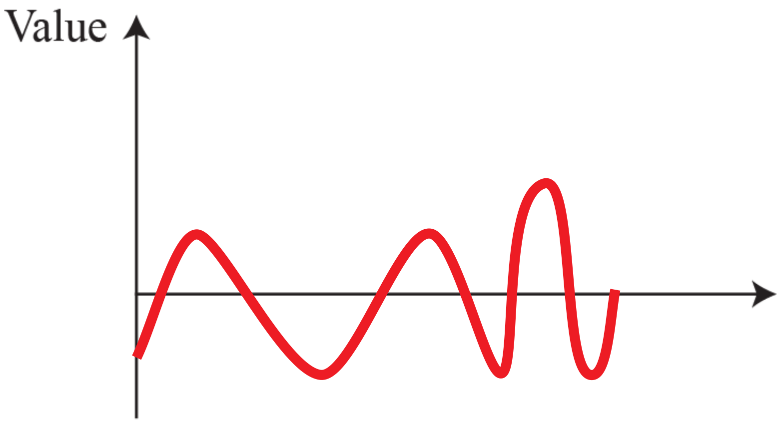
Analog and Digital Data

•Data can be **analog or digital**.

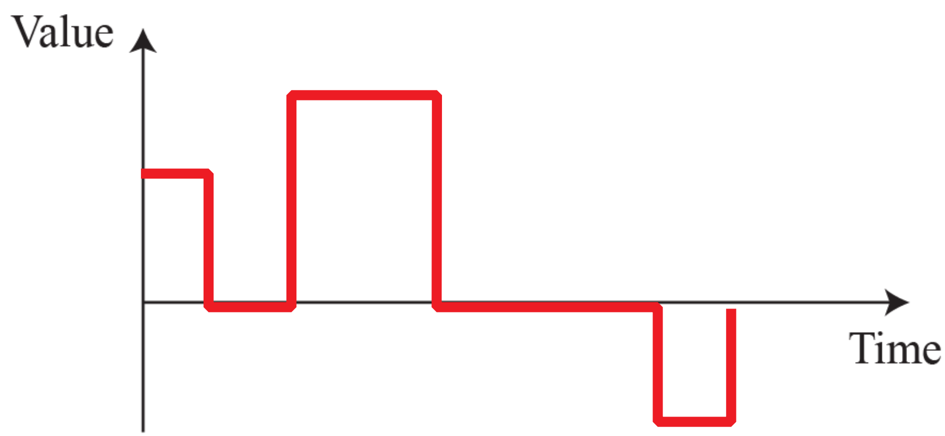
•The term analog data refers to information that is continuous; For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous.

•On the other hand, digital data refers to information that has discrete states. For example, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06.

Comparison of analog and digital signals



a. Analog signal



b. Digital signal

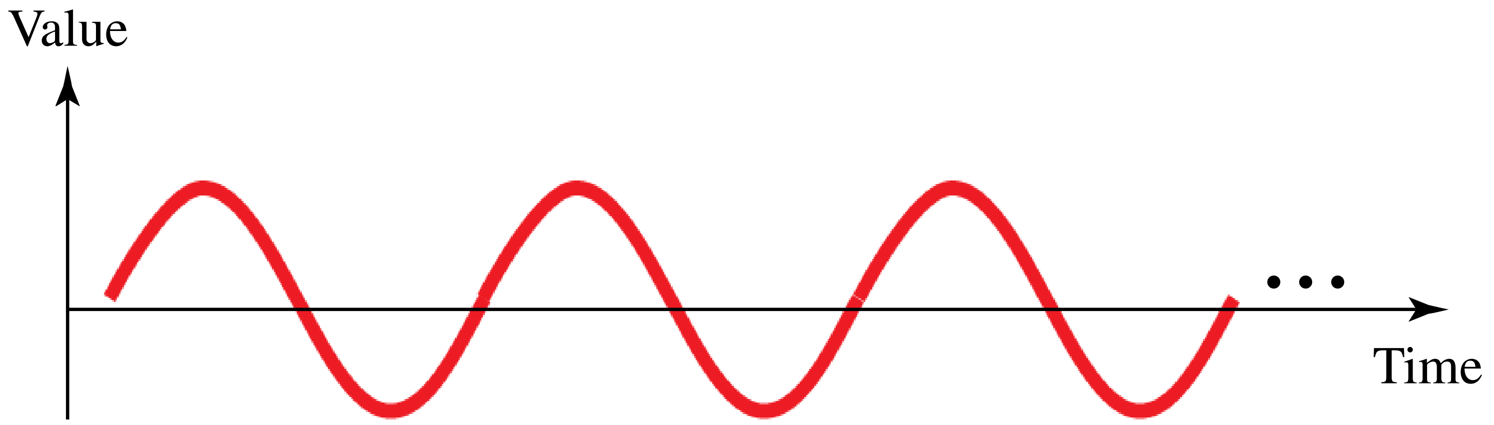
Periodic and Nonperiodic

A **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.

A **non periodic signal** changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals.

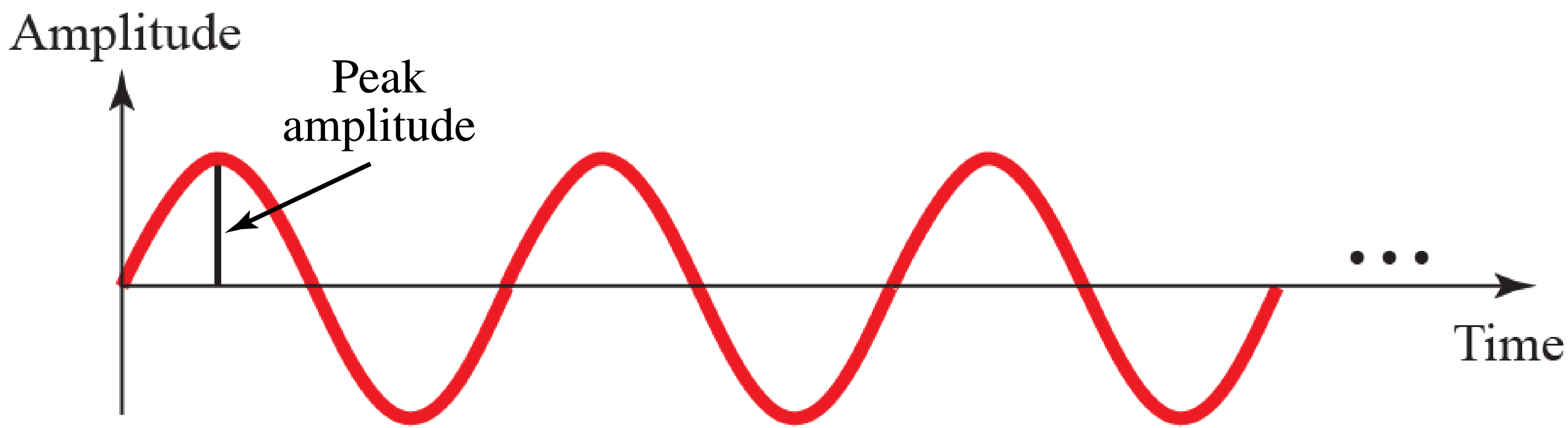
The sine wave is the most fundamental form of a periodic analog signal.

A sine wave

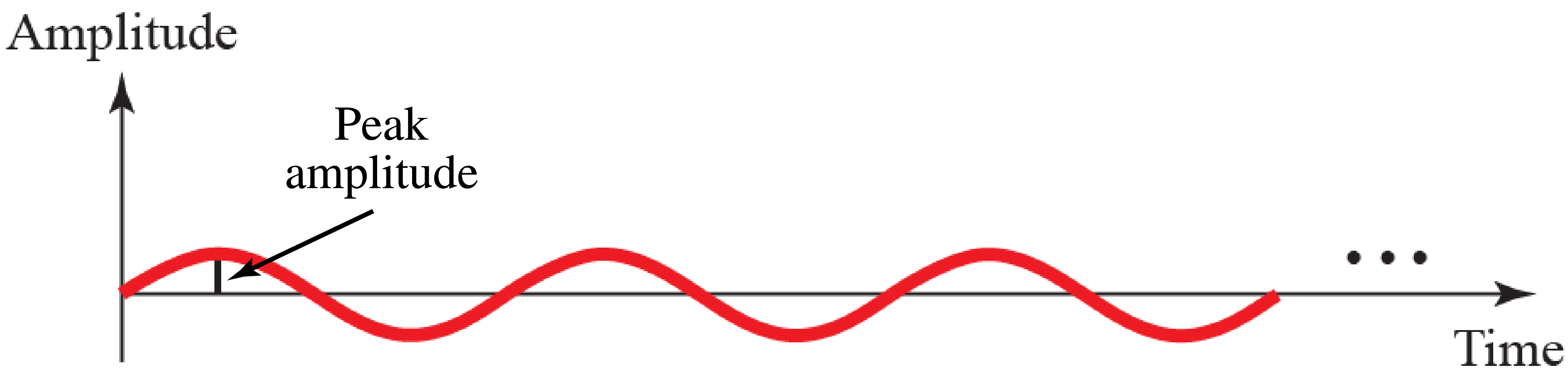


The sine wave is the most fundamental form of a periodic analog signal.

Two signals with two different amplitudes

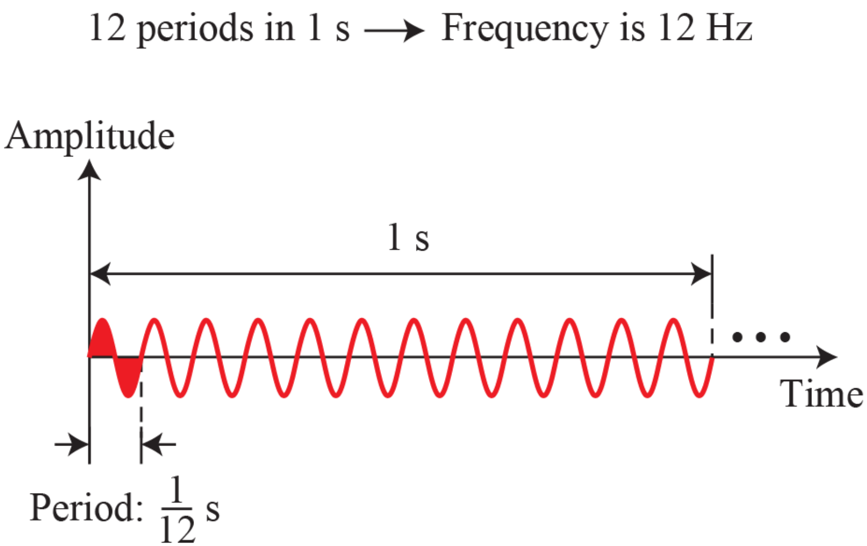


a. A signal with high peak amplitude

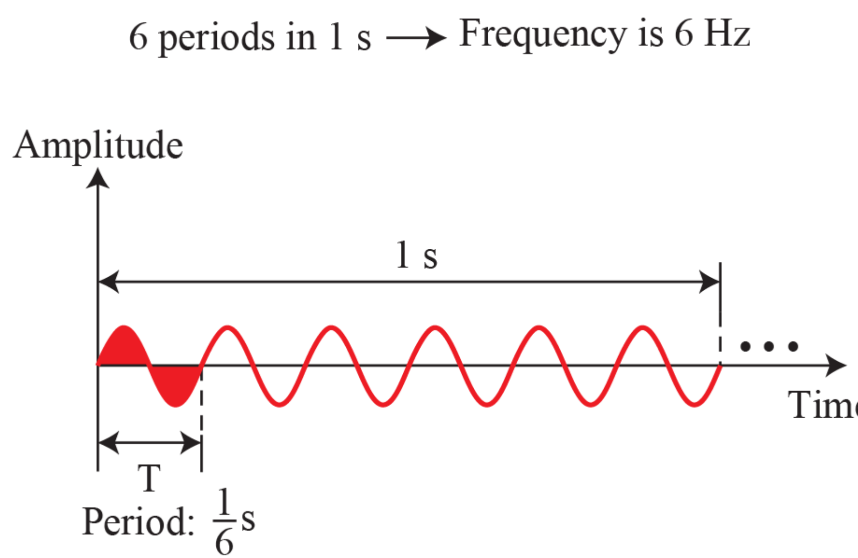


b. A signal with low peak amplitude

Two signals with same phase, different amplitudes and frequency



a. A signal with a frequency of 12 Hz



b. A signal with a frequency of 6 Hz

Units of period and frequency

Period		*Frequency*	
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

Example 1

Express a period of 100 ms in microseconds.

Solution

The equivalents of 1 ms (1 ms is 10–3 s) and 1 s (1 s is 106 μs). We make the following substitutions:

$$100 \text{ ms} = 100 \times 10^{-3} \text{ s} = 100 \times 10^{-3} \times 10^{6} \text{ μs} = 10^{2} \times 10^{-3} \times 10^{6} \text{ μs} = 10^{5} \text{ μs}$$

Example 2

The power we use at home has a frequency of 60 Hz (50 Hz in Europe). The period of this sine wave can be determined as follows:

$$T = \frac{1}{f} = \frac{1}{60} = 0.0166 \text{ s} = 0.0166 \times 10^3 \text{ ms} = 16.6 \text{ ms}$$

This means that the period of the power for our lights at home is 0.0116 s, or 16.6 ms. Our eyes are not sensitive enough to distinguish these rapid changes in amplitude.

Example 3

The period of a signal is 100 ms. What is its frequency in kilohertz?.

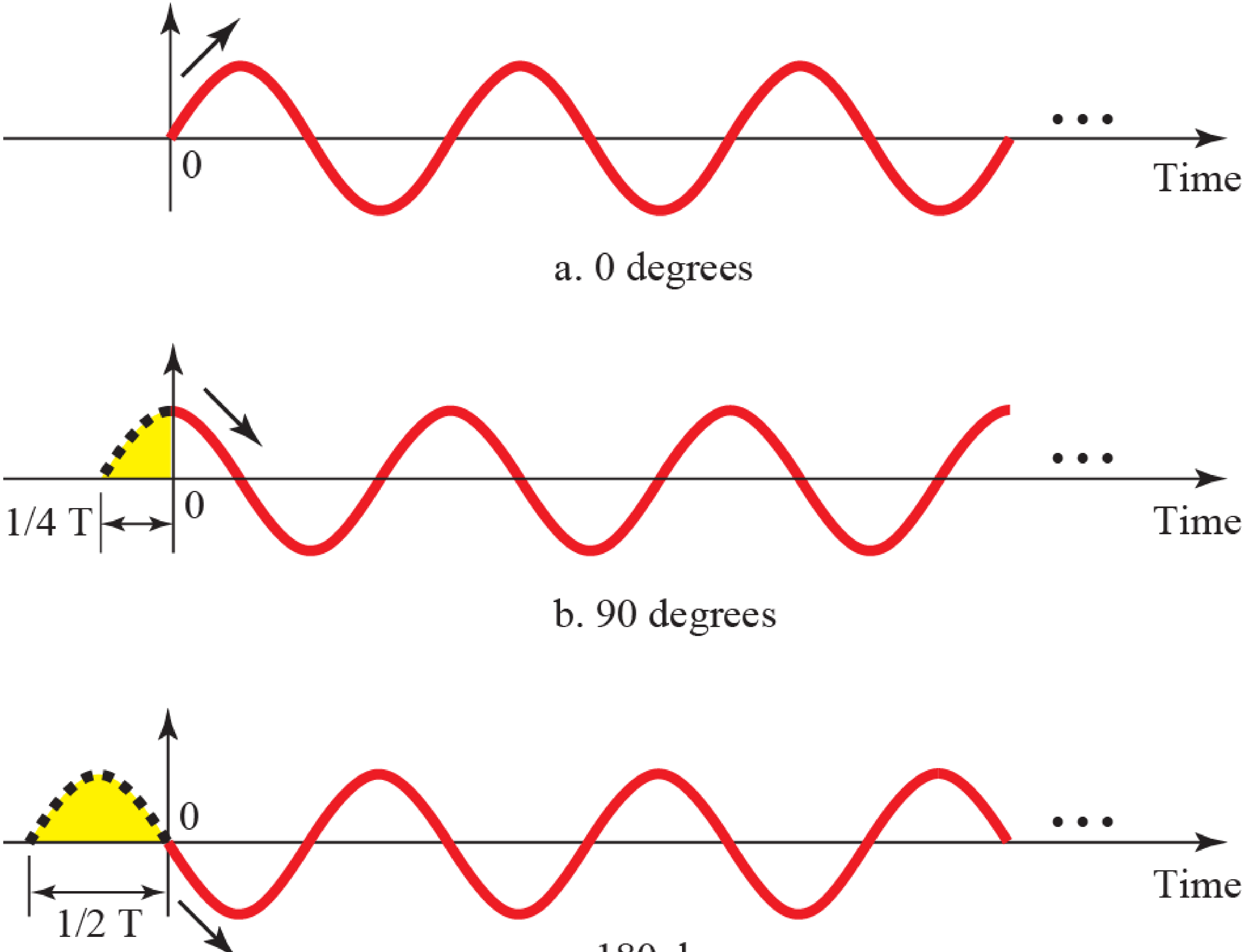
Solution

First we change 100 ms to seconds, and then we calculate the frequency from the period (1 Hz = 10^{-3} kHz).

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

$$f = \frac{1}{T} = \frac{1}{10^{-1}} \text{Hz} = 10 \text{ Hz} = 10 \times 10^{-3} \text{ kHz} = 10^{-2} \text{ kHz}$$

The term <u>PHASE</u>, or <u>PHASE SHIFT</u>, describes the position of the waveform relative to time 0

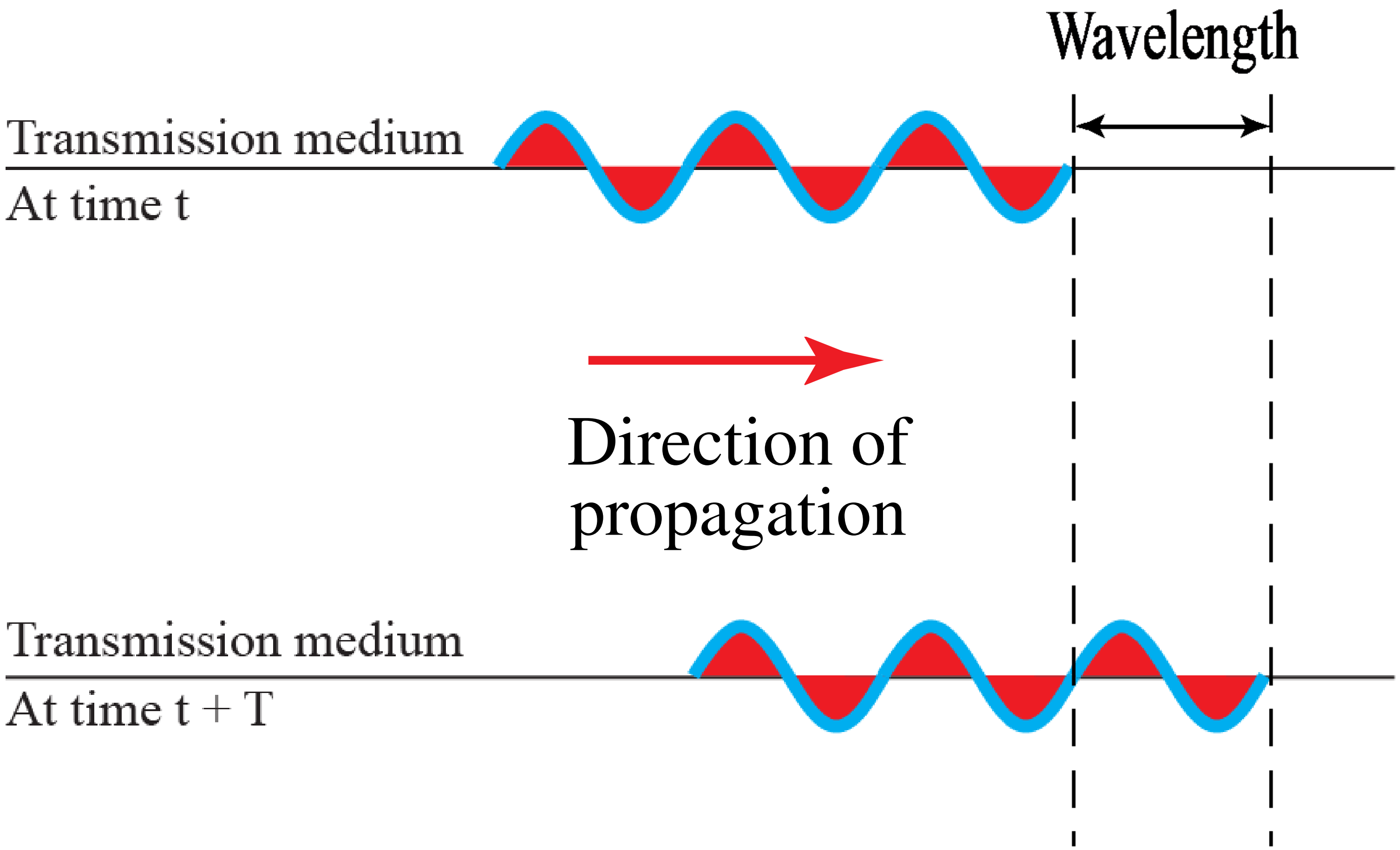


a. 0 degrees

b. 90 degrees

c. 180 degrees

WAVELENGTH binds the period or the frequency of a simple sine wave to the propagation speed of the medium



Application of Simple Signals

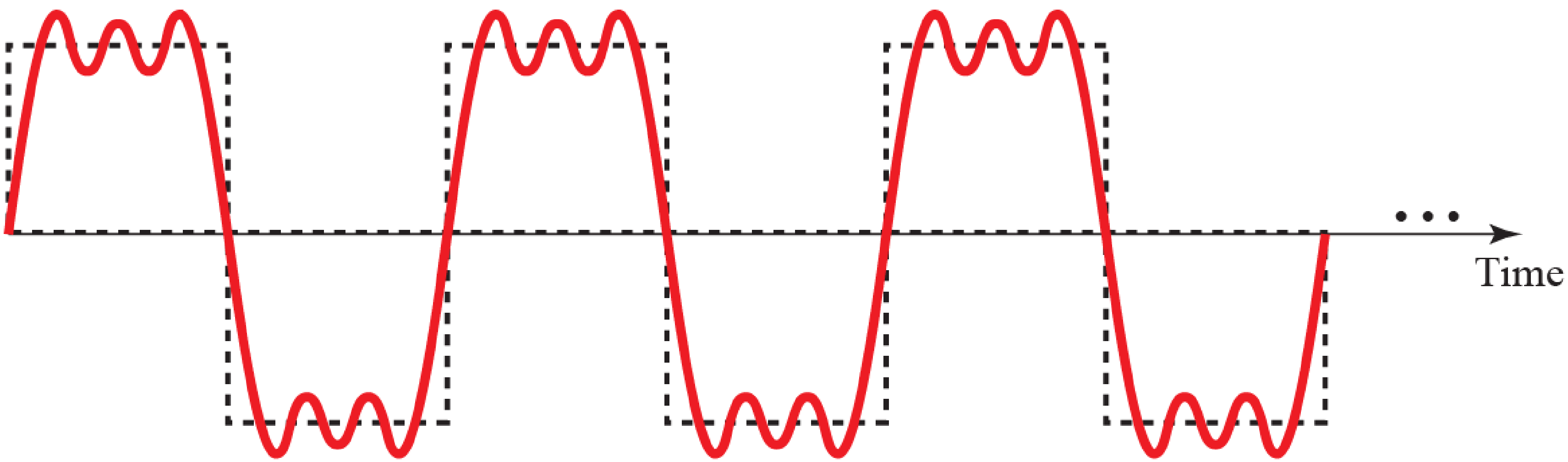
Simple sine waves have many applications in daily life.

We can send a single sine wave to carry electric energy from one place to another. For example, the power company sends a single sine wave with a frequency of 60 Hz to distribute electric energy to houses and businesses.

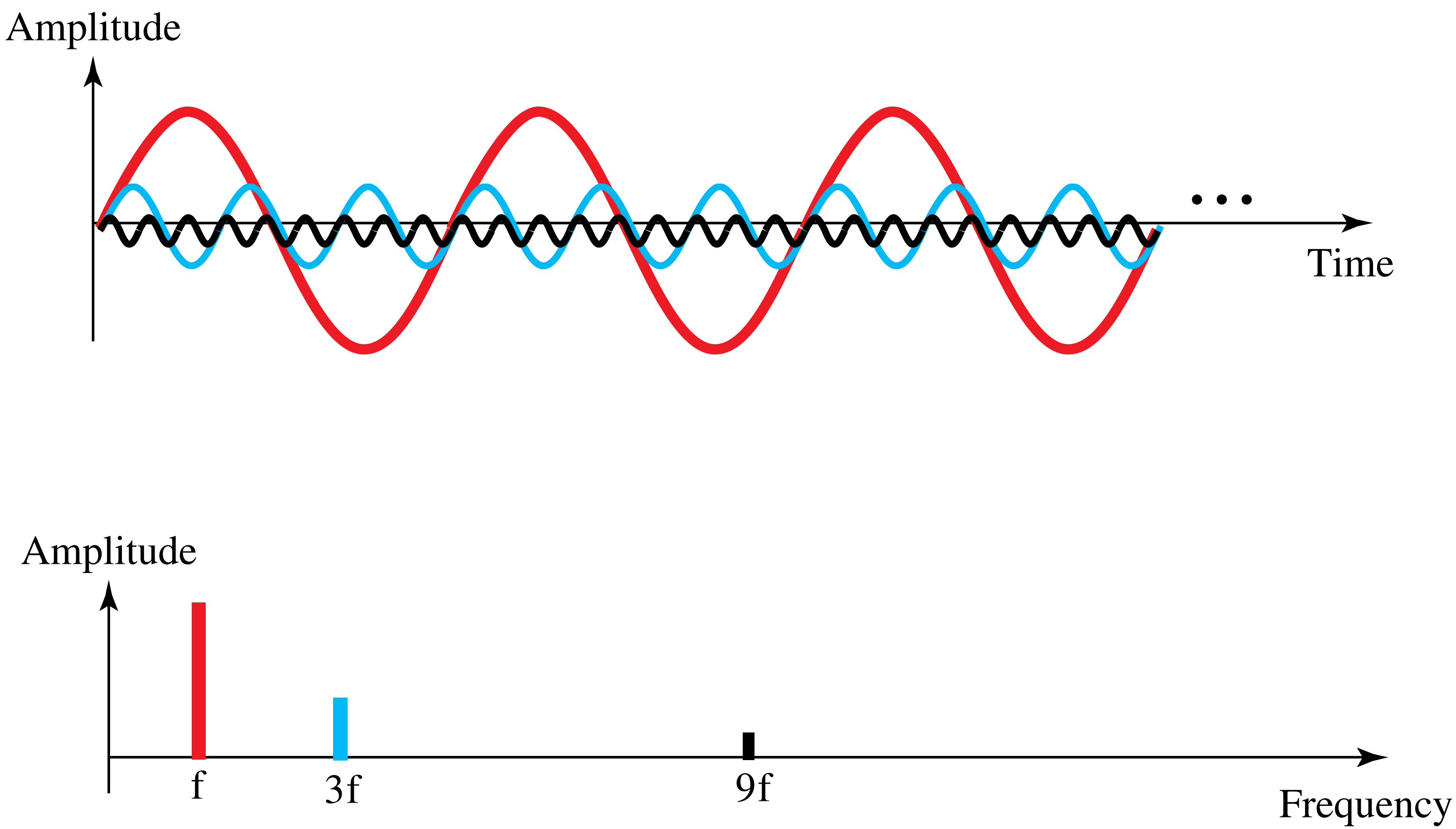
As another example, we can use a single sine wave to send an alarm to a security center when a burglar opens a door or window in the house. In the first case, the sine wave is carrying energy; in the second, the sine wave is a signal of danger.

Composite Period Signal

A **Composite Signal** is collection of multiple signals



Decomposition of a composite periodic signal

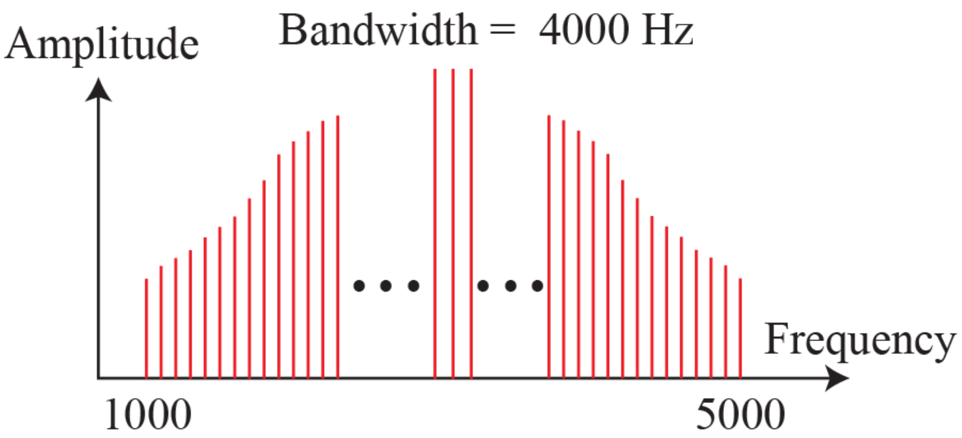


b. Frequency-domain decomposition of the composite signal

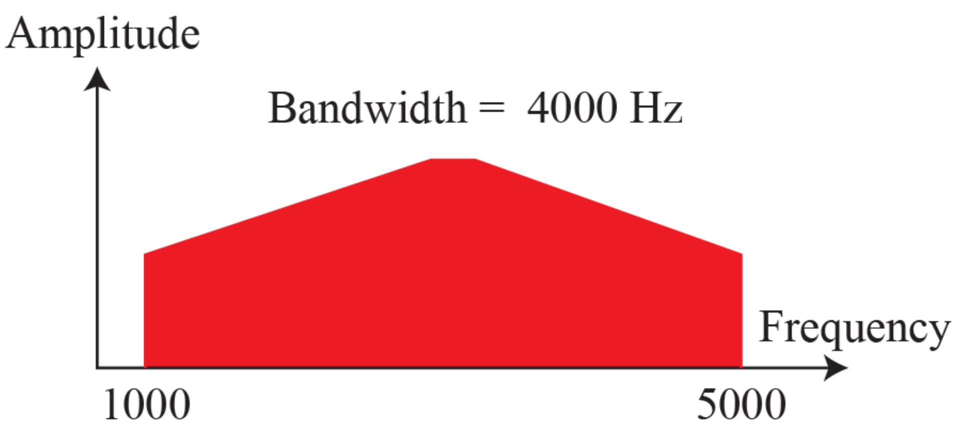
Bandwidth

The range of frequencies contained in a composite signal is its **bandwidth**. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 − 1000, or 4000.

Figure 3.13: The bandwidth of periodic and nonperiodic composite signals



a. Bandwidth of a periodic signal



b. Bandwidth of a nonperiodic signal

Example 4

If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is its bandwidth?

Solution

Let f_h be the highest frequency, f_l the lowest frequency, and B the bandwidth. Then

$$B = f_h - f_l = 900 - 100 = 800 \text{ Hz}$$

Example 5

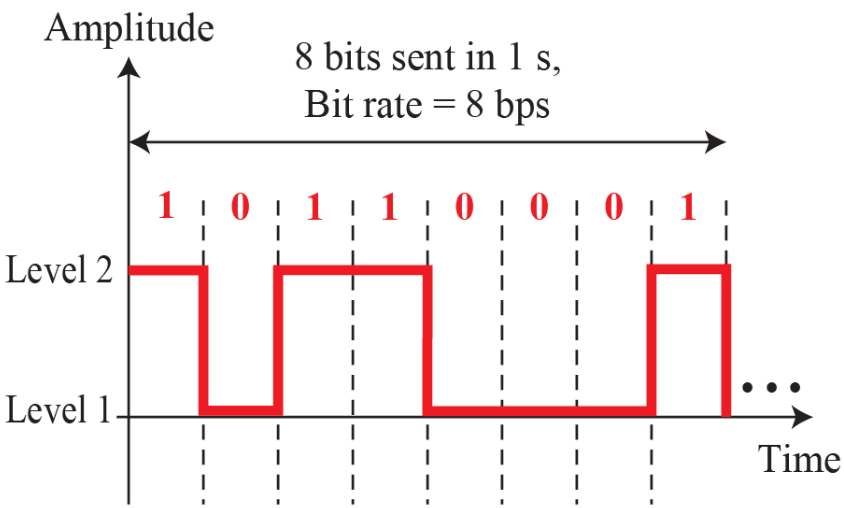
A periodic signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency?

Solution

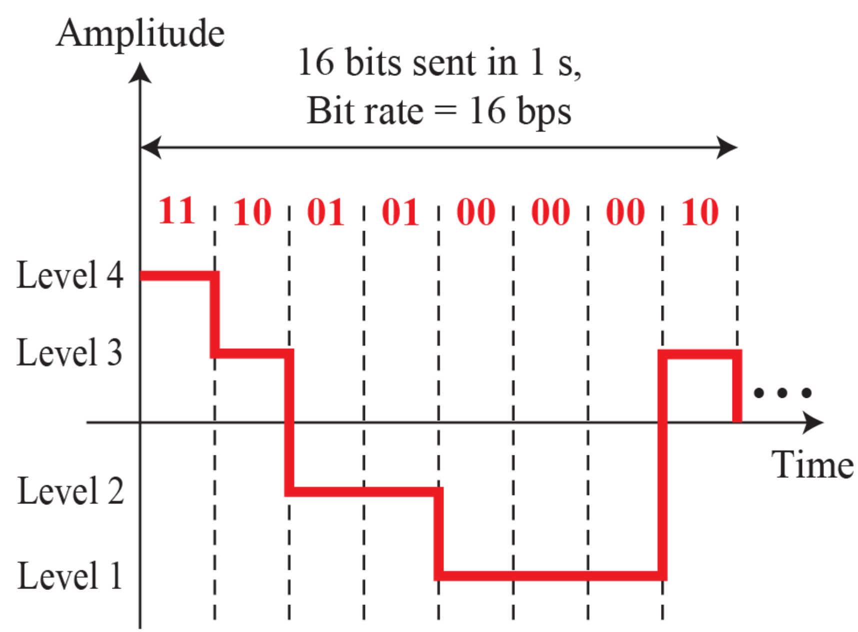
Let f_h be the highest frequency, f_l the lowest frequency, and B the bandwidth. Then

$$B = f_h - f_l \longrightarrow 20 = 60 - f_l \longrightarrow f_l = 60 - 20 = 40 \text{ Hz}$$

Two digital signals: one with two signal levels and the other with four signal levels



a. A digital signal with two levels



b. A digital signal with four levels

Example 6

A digital signal has eight levels. How many bits are needed per level? We calculate the number of bits from the following formula. Each signal level is represented by 3 bits.

$$\text{Number of bits per level} = \log_2 8 = 3$$

Example 7

A digital signal has nine levels. How many bits are needed per level? We calculate the number of bits by using the formula. Each signal level is represented by 3.17 bits. However, this answer is not realistic. The number of bits sent per level needs to be an integer.

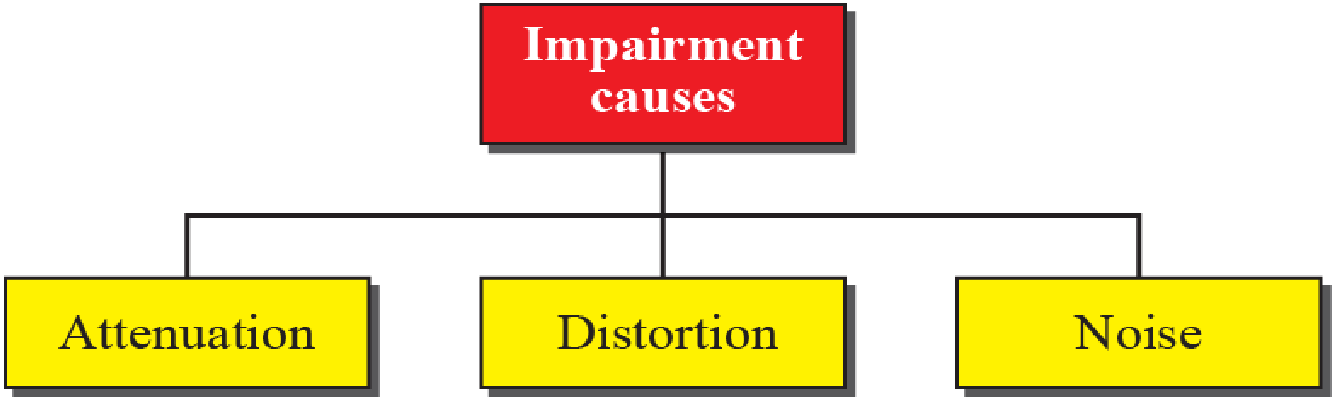
For this example, 4 bits can represent one level.

Bit Rate

Most digital signals are non periodic, and thus period and frequency are not appropriate characteristics. Another term **Bit Rate** (instead of frequency) is used to describe digital signals. **The bit rate is the number of bits sent in 1s, expressed in bits per second (bps)**.

Transmission Impairment

Signals travel through transmission media, which are not perfect. **The imperfection causes signal impairment**. This means that the signal at the beginning of the medium is **not the same** as the signal at the end of the medium. What is sent is not what is received. **Three causes of impairment are attenuation, distortion, and noise**



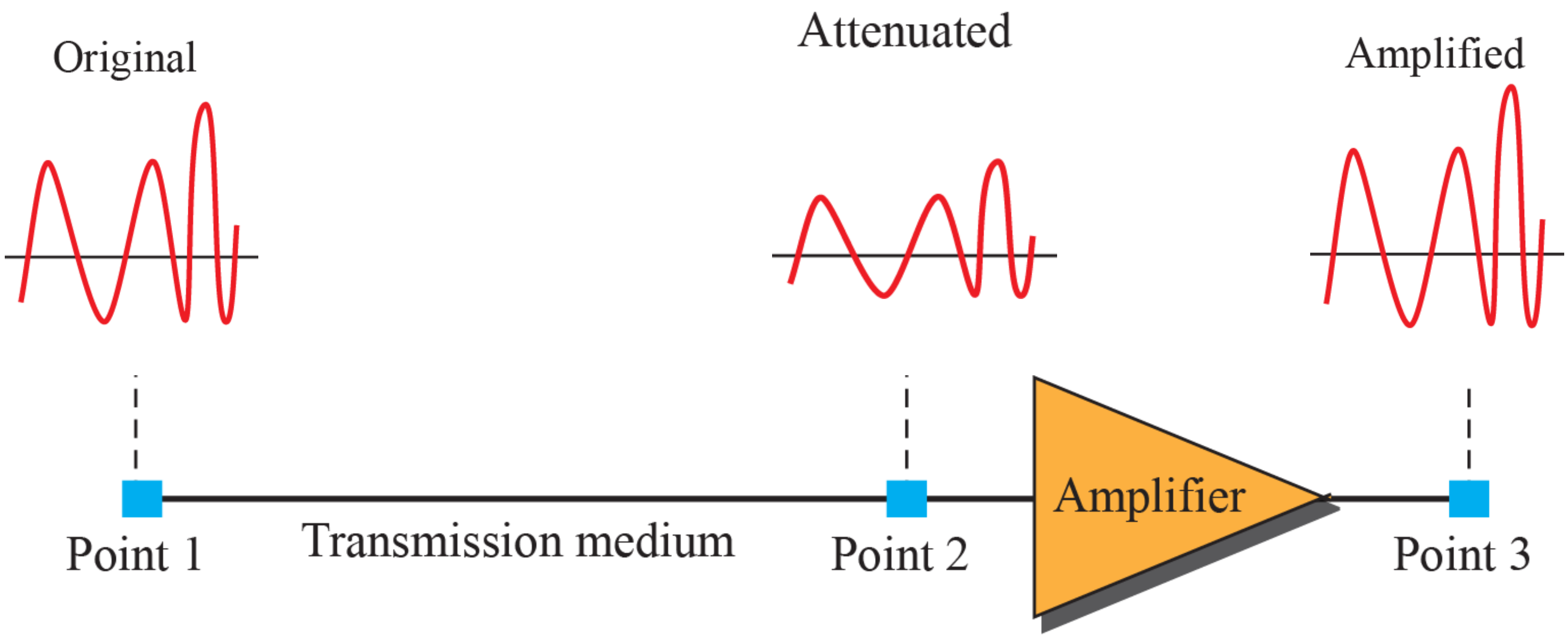
Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it **loses some of its energy** in overcoming the resistance of the medium. *That is why a wire carrying electric signals gets warm*, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. **To compensate for this loss, amplifiers are used to amplify the signa**l. Next figure shows the effect of attenuation and amplification.

Decibel (dB) is used to measure the attenuation.

dB= $10 \log_{10} \frac{P_2}{P_1}$

Attenuation and Amplification



Example 8

Suppose a signal travels through a transmission medium and its power is reduced to one half. This means that P2 = 0.5 P1. In this case, the attenuation (loss of power) can be calculated as

$$\boxed{10 \log_{10} P_2/P_1 = 10 \log_{10} (0.5\ P_1)\ /P_1 = 10 \log_{10} 0.5 = 10 \times (-0.3) = -3 \text{ dB.}}$$

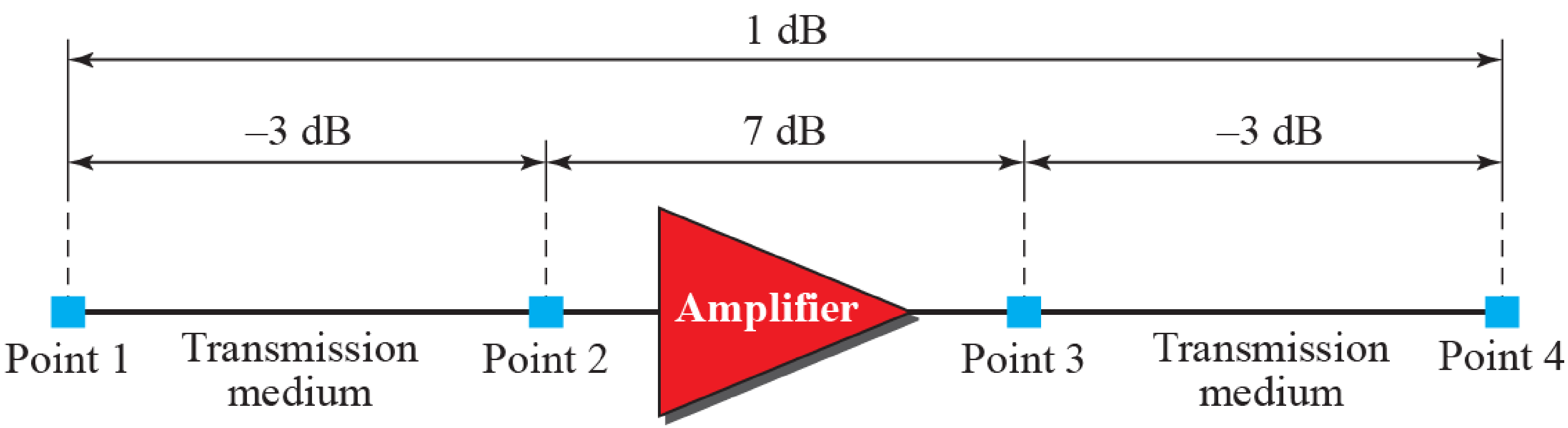
A loss of 3 dB (–3 dB) is equivalent to losing one-half the power.

Example 9

A signal travels through an amplifier, and its power is increased 10 times. This means that $P_2 = 10P_1$. In this case, the amplification (gain of power) can be calculated as

$$10 \log_{10} \frac{P_2}{P_1} = 10 \log_{10} \frac{10P_1}{P_1} = 10 \log_{10} 10 = 10(1) = 10 \text{ dB}$$

Example 10



Question on next slide

One reason that engineers use the decibel to measure the changes in the strength of a signal is that decibel numbers can be added (or subtracted) when we are measuring several points (cascading) instead of just two. In Figure 3.28 a signal travels from point 1 to point 4. The signal is attenuated by the time it reaches point 2. Between points 2 and 3, the signal is amplified. Again, between points 3 and 4, the signal is attenuated. We can find the resultant decibel value for the signal just by adding the decibel measurements between each set of points. In this case, the decibel value can be calculated as

$$dB = -3 + 7 - 3 = +1$$

Sometimes the decibel is used to measure signal power in milliwatts. In this case, it is referred to as dB_m and is calculated as dB_m = 10 log10 Pm, where Pm is the power in milliwatts. Calculate the power of a signal if its $dB_m = -30$.

Solution

We can calculate the power in the signal as

$$\mathrm{dB_m} = 10\log_{10} \longrightarrow dB_m = -30 \longrightarrow \log_{10} P_m = -3 \longrightarrow P_m = 10^{-3}\,\mathrm{mW}$$

Example 12

The loss in a cable is usually defined in decibels per kilometer (dB/km). If the signal at the beginning of a cable with −0.3 dB/km has a power of 2 mW, what is the power of the signal at 5 km?

Solution

The loss in the cable in decibels is $5 \times (-0.3) = -1.5$ dB. We can calculate the power as

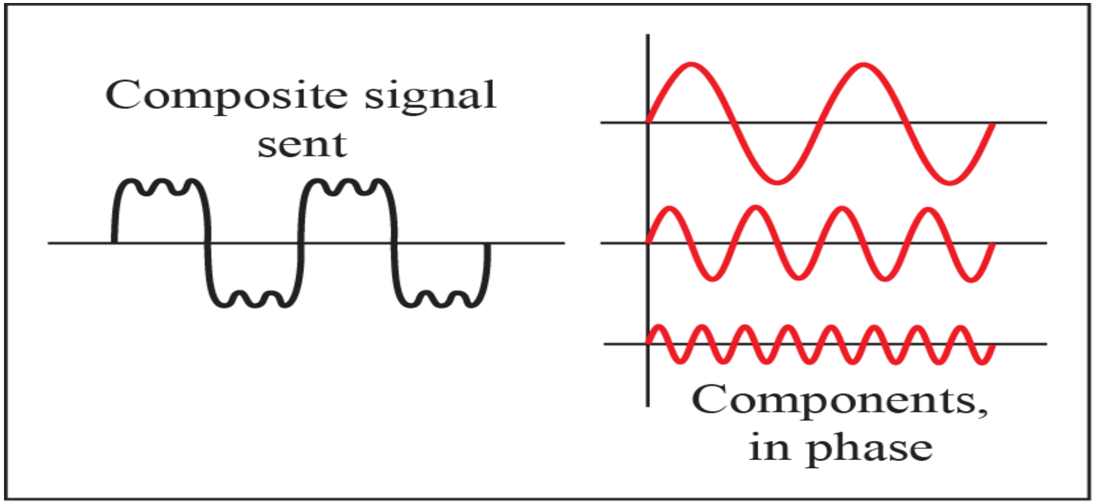
$$\text{dB} = 10 \log_{10} (P_2 / P_1) = -1.5 \quad \longrightarrow \quad (P_2 / P_1) = 10^{-0.15} = 0.71$$

$$P_2 = 0.71 P_1 = 0.7 \times 2 \text{ mW} = 1.4 \text{ mW}$$

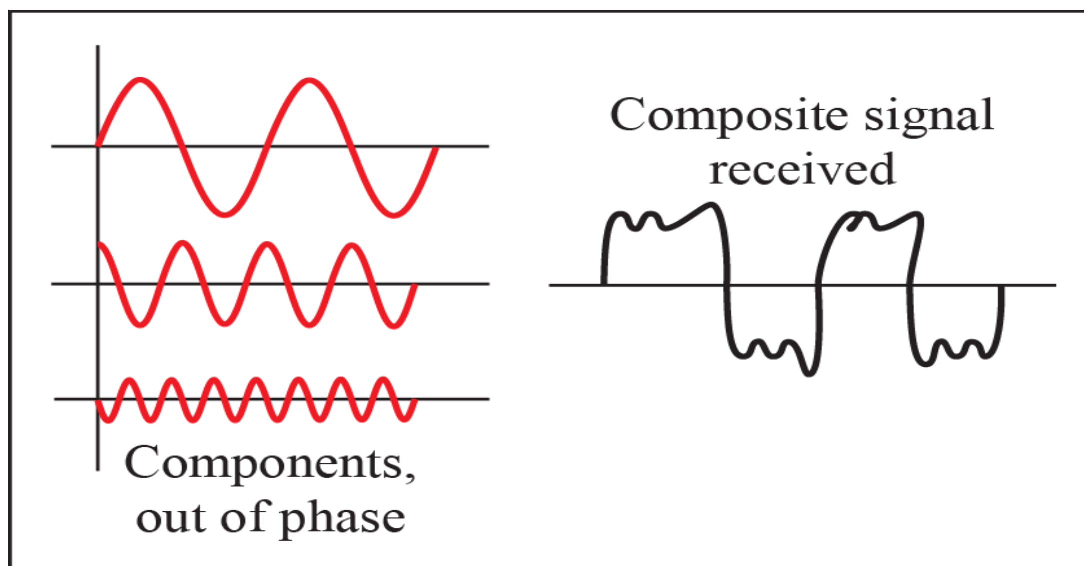
Distortion

Distortion means that the signal changes its form or shape. *Distortion can occur in a composite signal made of different frequencies*. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. *Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration*.

Distortion



At the sender



At the receiver

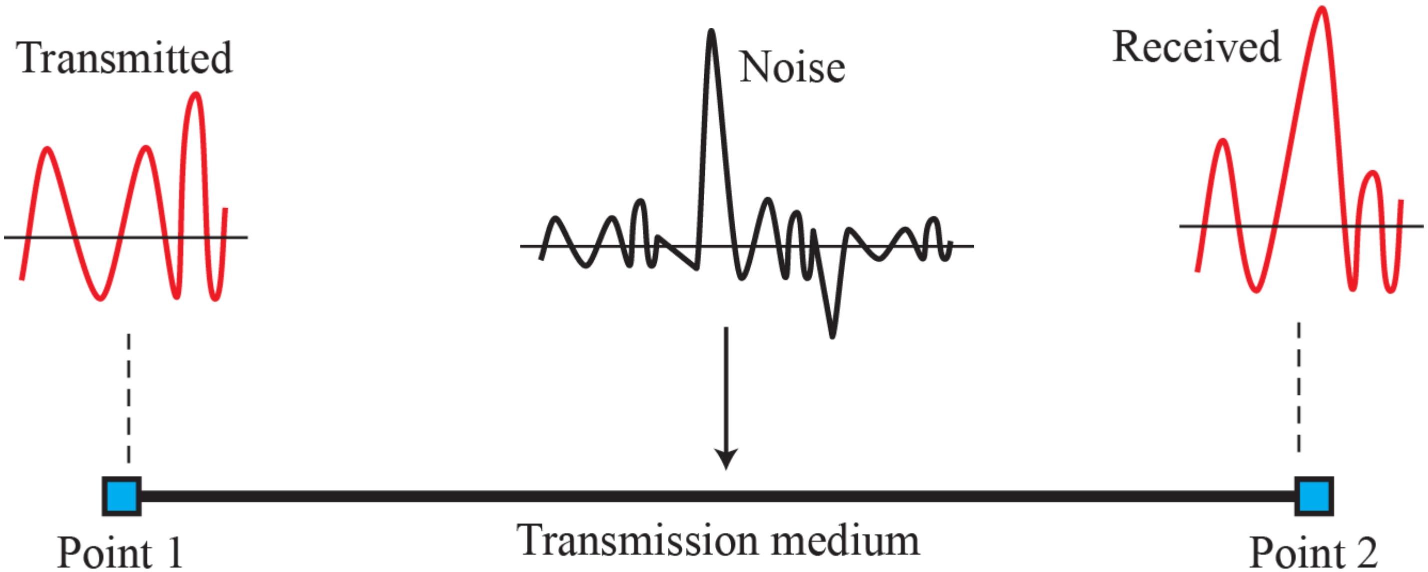
Noise

Noise is another cause of impairment. Several types of noise, such as *thermal noise, induced noise, crosstalk, and impulse noise*, **may corrupt the signal**. Thermal noise is the random motion of electrons in a wire, which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors. Crosstalk is the effect of one wire on the other.

Noise is measured in terms of SNR (Signal to Noise Ratio)

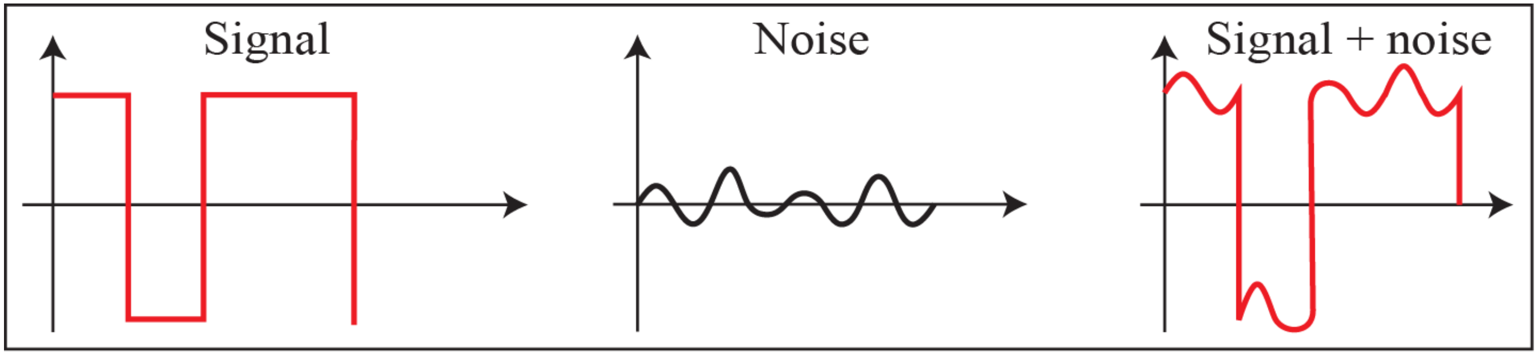
SNR= Average Signal Power / Average Noise Power

Noise

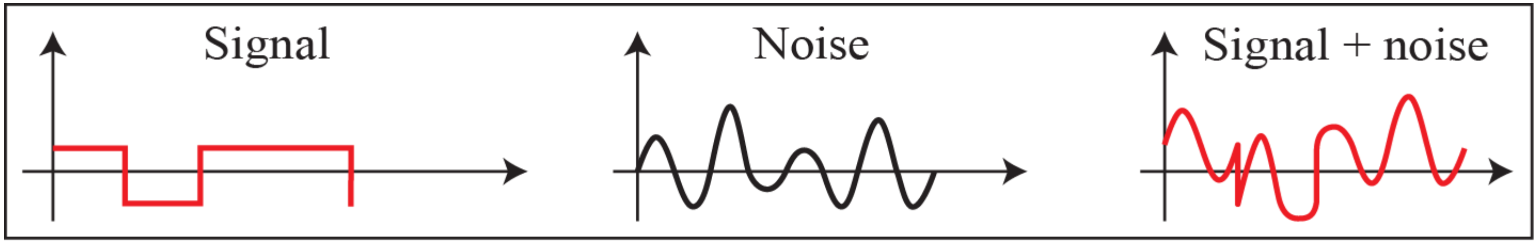


Transmitted
Noise
Received
Point 1
Transmission medium
Point 2

Two cases of SNR: a high SNR and a low SNR



a. High SNR



b. Low SNR

Example 13

The power of a signal is 10 mW and the power of the noise is 1 μW; what are the values of SNR and SNR_{dB}?

Solution

The values of SNR and SNR_{dB} can be calculated as follows:

$$SNR = (10{,}000\ \mu w) / (1\ \mu w) = 10{,}000 \qquad SNR_{dB} = 10 \log_{10} 10{,}000 = 10 \log_{10} 10^4 = 40$$

Example 14

The values of SNR and SNR_{dB} for a noiseless channel are

Solution

The values of SNR and SNRdB for a noiseless channel are

$$SNR = (\text{signal power}) / 0 = \infty \longrightarrow SNR_{dB} = 10 \log_{10} \infty = \infty$$

We can never achieve this ratio in real life; it is an ideal.

Noiseless Channel: Nyquist Rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate.

$$\text{BitRate} = 2 \times \text{bandwidth} \times \log_2 L$$

Example 15

Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \times 3000 \times \log_2 2 = 6000 \text{ bps}$$

Example 16

Consider the same noiseless channel transmitting a signal with four signal levels (for each level, we send 2 bits). The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \times 3000 \times \log_2 4 = 12{,}000 \text{ bps}$$

Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

$$\text{Capacity} = \text{bandwidth} \times \log_2(1 + \text{SNR})$$

Example 17

Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity C is calculated as

$$C = B \log_2 (1 + \text{SNR}) = B \log_2(1 + 0) = B \log_2 1 = B \times 0 = 0$$

This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

Example 18

The signal-to-noise ratio is often given in decibels. Assume that $SNR_{dB} = 36$ and the channel bandwidth is 2 MHz. The theoretical channel capacity can be calculated as

$$SNR_{dB} = 10 \log_{10} SNR \longrightarrow SNR = 10^{SNR_{dB}/10} \longrightarrow SNR = 10^{3.6} = 3981$$

$$C = B \log_2(1 + SNR) = 2 \times 10^6 \times \log_2 3982 = 24 \text{ Mbps}$$

Example 19

We have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. What are the appropriate bit rate and signal level?

Solution

First, we use the Shannon formula to find the upper limit.

$$C = B \log_2(1 + \text{SNR}) = 10^6 \log_2(1 + 63) = 10^6 \log_2 64 = 6 \text{ Mbps}$$

The Shannon formula gives us 6 Mbps, the upper limit. For better performance we choose something lower, 4 Mbps. Then we use the Nyquist formula to find the number of signal levels.

$$4 \text{ Mbps} = 2 \times 1 \text{ MHz} \times \log_2 L \longrightarrow L = 4$$

Note

The Shannon capacity gives us the upper limit; the Nyquist formula tells us how many signal levels we need.

Latency or Delay

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = propagation time + transmission time + queuing time + processing delay

Propagation & Transmission delay

<u>Propagation speed</u> - speed at which a bit travels though the medium from source to destination.

<u>Transmission speed</u> - the speed at which all the bits in a message arrive at the destination. (difference in arrival time of first and last bit)

Propagation Delay = Distance/Propagation speed

Transmission Delay = Message size/bandwidth in bps

<u>Latency</u> = *Propagation delay + Transmission delay + Queuing time + Processing time*

Example 20

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution

We can calculate the throughput as

$$\text{Throughput} = (12{,}000 \times 10{,}000) / 60 = 2 \text{ Mbps}$$

The throughput is almost one-fifth of the bandwidth in this case.

Example 21

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4 × 108 m/s in cable.

Solution

We can calculate the propagation time as

$$\text{Propagation time} = (12{,}000 \times 10{,}000) / (2.4 \times 2^8) = 50 \text{ ms}$$

The example shows that a bit can go over the Atlantic Ocean in only 50 ms if there is a direct cable between the source and the destination.

Example 22

What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4 × 108 m/s.

Solution

We can calculate the propagation and transmission time as

$$\textbf{Propagation time} = (12{,}000 \times 1000) / (2.4 \times 10^8) = 50 \text{ ms}$$

$$\textbf{Transmission time} = (2500 \times 8) / 10^9 = 0.020 \text{ ms}$$

Note that in this case, because the message is short and the bandwidth is high, the dominant factor is the propagation time, not the transmission time.

Example 23

What are the propagation time and the transmission time for a 5-MB (megabyte) message (an image) if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4 × 108 m/s.

Solution

We can calculate the propagation and transmission times as

$$\text{Propagation time} = (12{,}000 \times 1000) / (2.4 \times 10^8) = 50 \text{ ms}$$

$$\text{Transmission time} = (5{,}000{,}000 \times 8) / 10^6 = 40 \text{ s}$$

We can calculate the propagation and transmission times as

Bandwidth

One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: bandwidth in hertz and bandwidth in bits per second..

Bandwidth

In networking, we use the term bandwidth in two contexts.

- The first, **bandwidth in her**tz, refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass.

- The second, **bandwidth in bits per second**, refers to the speed of bit transmission in a channel or link. Often referred to as Capacity.

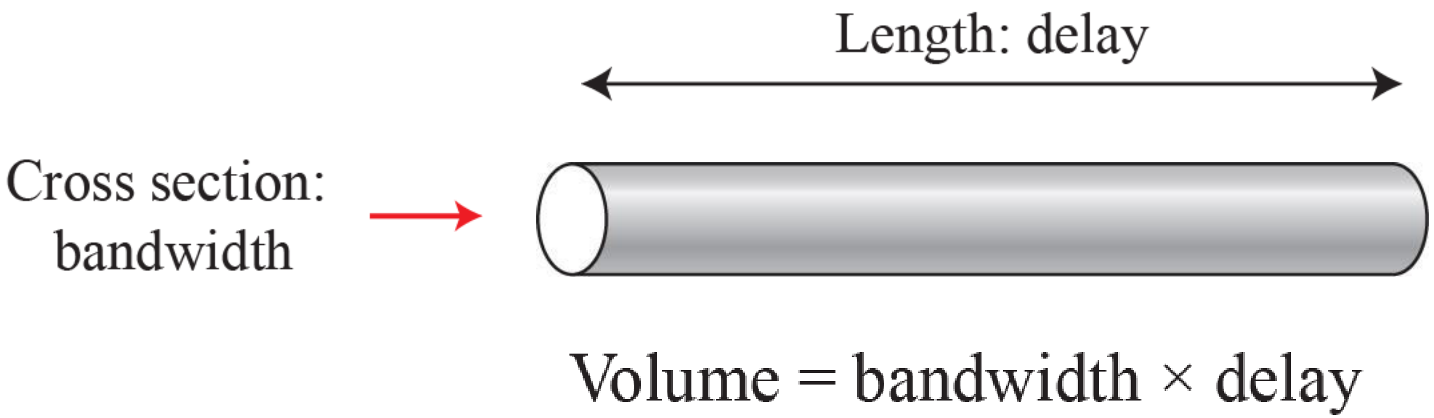
Throughput

The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of B bps, but we can only send T bps through this link with T always less than B.

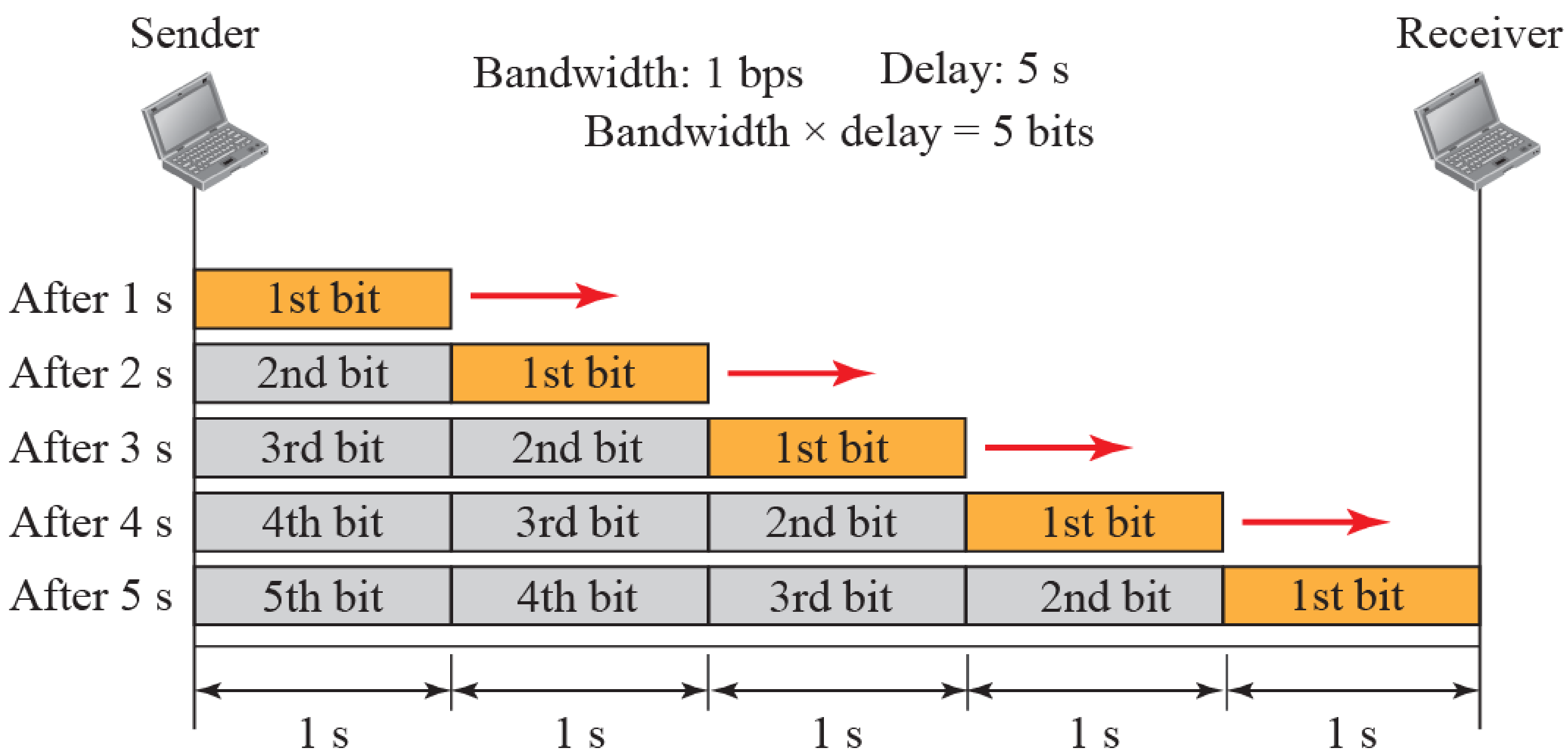
Bandwidth-Delay Product

Bandwidth and delay are two performance metrics of a link. However, as we will see in this chapter and future chapters, what is very important in data communications is the product of the two, the bandwidth-delay product. Let us elaborate on this issue, using two hypothetical cases as examples.

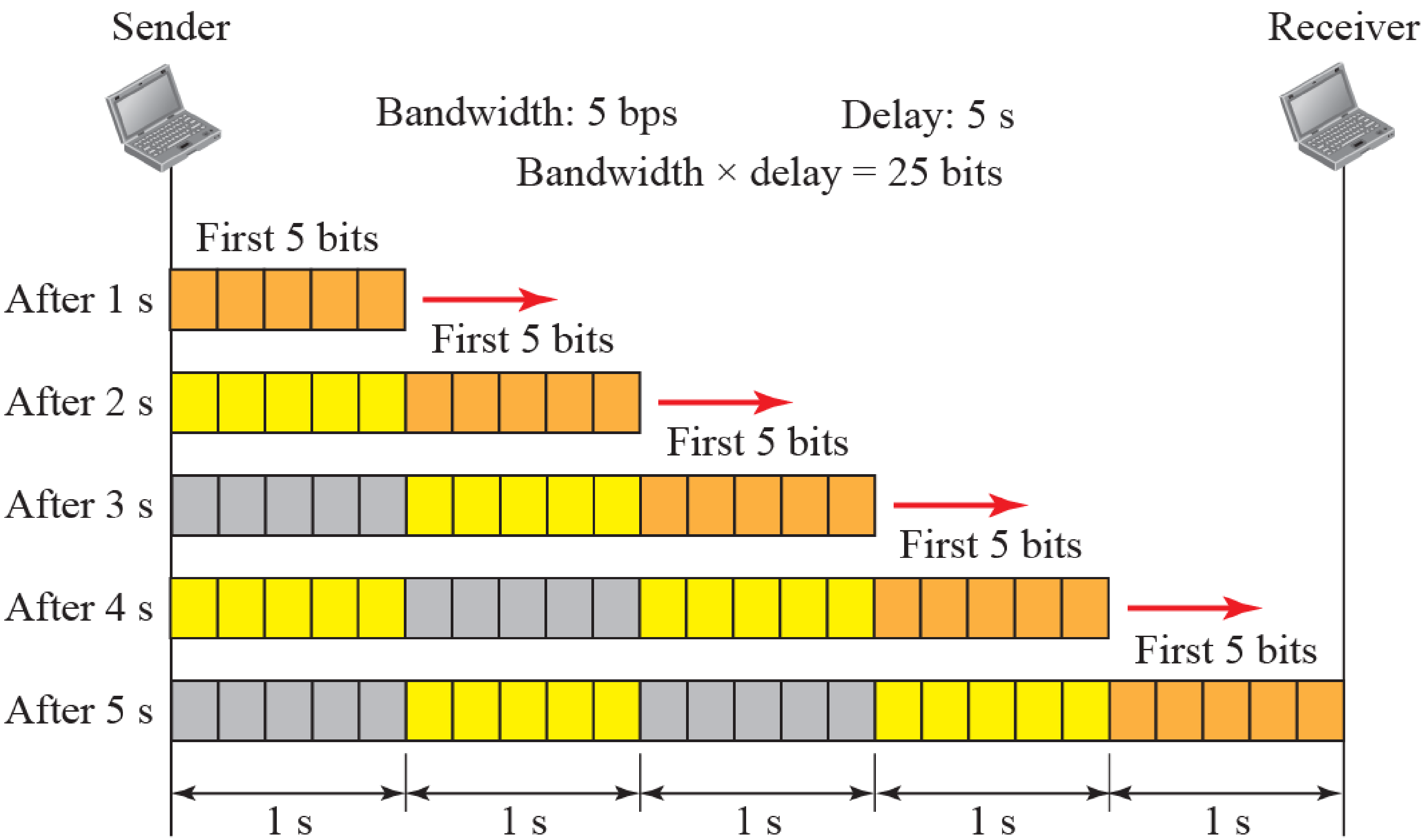
Concept of bandwidth-delay product



Filling the links with bits for Case 1



Filling the pipe with bits for Case 2



- **Thank You**
- **Discussion & Doubt session will be in lecture.**

Important terms to keep in mind

1. **Analog & Digital Signal**
2. **Simple Composite Signal**
3. **Nyquist & Shannon capacity**
4. **Transmission Impairment**
5. **Latency**
6. **Bandwidth (Hz/ bps)**

COMPUTER NETWORKS (BCSC 0008)

DIGITAL SIGNALS
DIGITAL TO DIGITAL CONVERSION
(LINE CODING)
Chapter 4 (FOUROZAN 4th Edition)

Text and Reference Books

Text Books:

1. Fourouzan B. A. (2004), “Data Communication and Networking”, 4th Edition, McGraw-Hill.

References:

1. Kurose, J. F. and Ross K. W. (2005), “Computer Networking: A Top-Down Approach Featuring the Internet”, 3rd Edition, Addison-Wesley.
2. A. S. Tanenbaum (2006), “Computer Networks”, 2nd Edition, Prentice Hall India.

Previous discussed topics:

1. **OSI Model**
2. **TCP/IP Model**
3. **Addressing**
4. **Data & Signals**
5. **Transmission Media**

Now we will discuss:

1. **Data element vs. Signal element**
2. **Baud Rate**
3. **Line Coding Schemes (Unipolar & Polar)**

DIGITAL-TO-DIGITAL CONVERSION

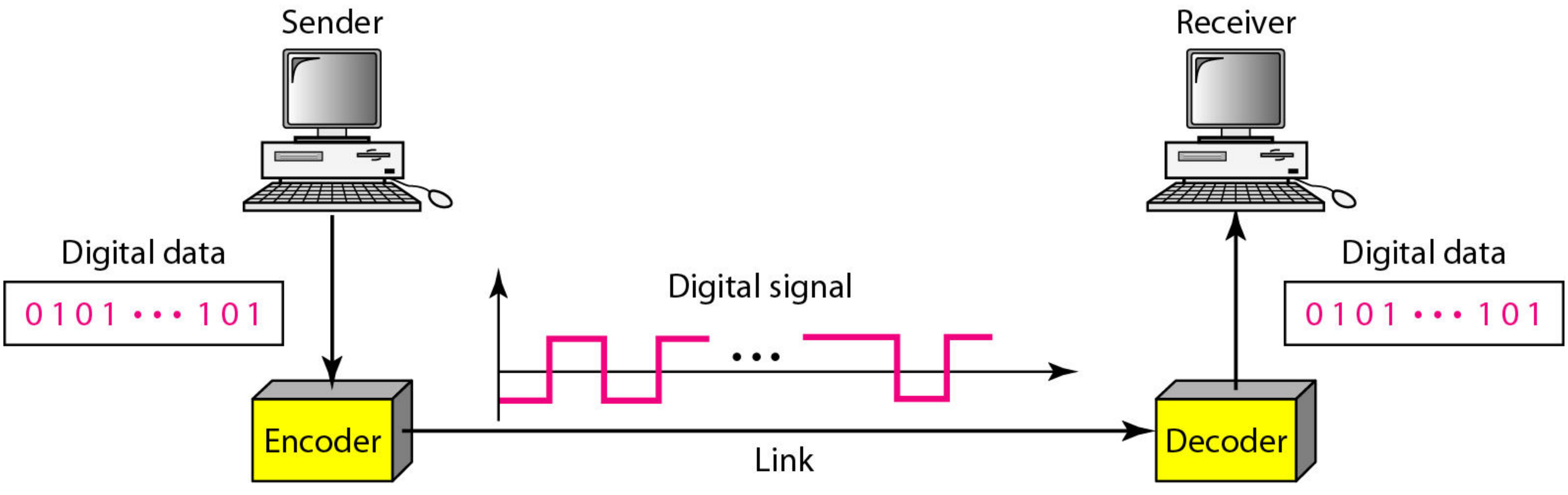
In this section, we see how we can represent digital data by using digital signals. The conversion involves three techniques: line coding, block coding, and scrambling. Line coding is always needed; block coding and scrambling may or may not be needed.

Line Coding

- Converting a string of 1's and 0's (digital data) into a sequence of signals that denote the 1's and 0's.

- For example a high voltage level (+V) could represent a "1" and a low voltage level (0 or -V) could represent a "0".

Line coding and decoding



Mapping Data symbols onto Signal levels

- A data symbol (or element) can consist of a number of data bits:
  - 1 , 0 or
  - 11, 10, 01, ……
- A data symbol can be coded into a single signal element or multiple signal elements
  - 1 -> +V, 0 -> -V
  - 1 -> +V and -V, 0 -> -V and +V
- **The ratio ‘r’ is the number of data elements carried by a signal element.**

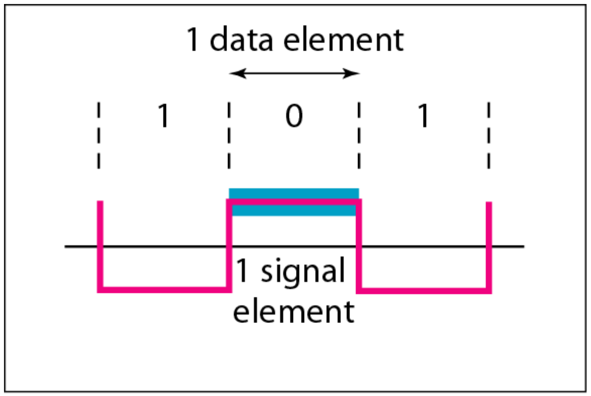
Relationship between data rate and signal rate

- The **data rate defines the number of bits sent per sec - bps**. It is often referred to the bit rate. The signal rate is **the number of signal elements sent in a second** and is measured in bauds. It is also referred to as the modulation rate or baud rate.
- Goal is to increase the data rate whilst reducing the baud rate.

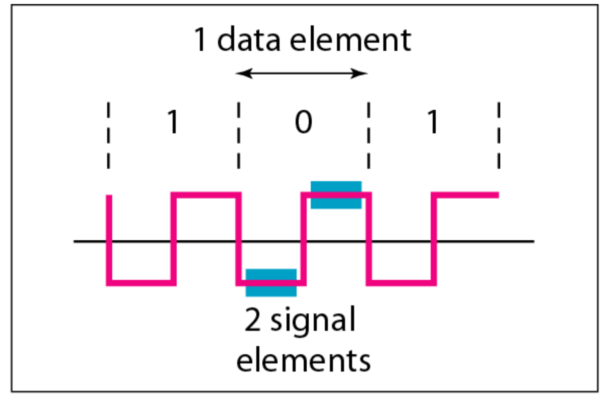
A *data element* is the smallest entity that can represent a piece of information (a bit). A *signal element* is the shortest unit of a digital signal. Data elements are what we need to send; signal elements are what we can send. Data elements are being carried; signal elements are the carriers.

The *data rate* defines the number of data elements (bits) sent in 1s. The unit is bits per second (bps). The *signal rate* is the number of signal elements sent in 1s. The unit is the baud.

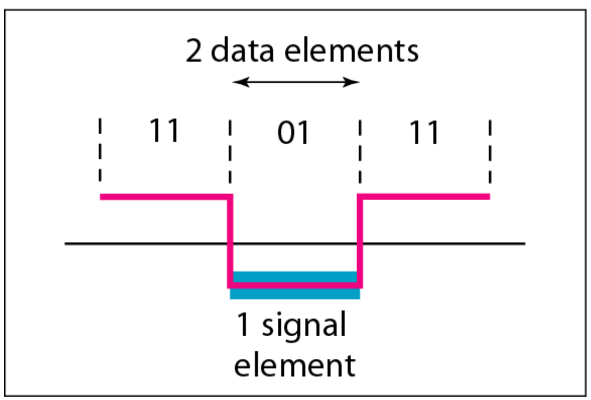
Signal element versus data element



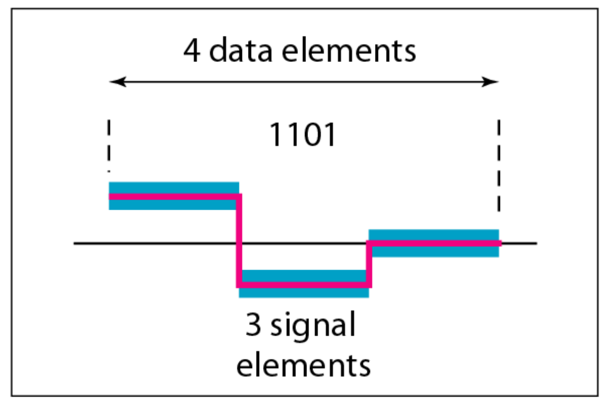
a. One data element per one signal element ($r = 1$)



b. One data element per two signal elements $\left(r = \frac{1}{2}\right)$



c. Two data elements per one signal element ($r = 2$)



d. Four data elements per three signal elements $\left(r = \frac{4}{3}\right)$

Data rate and Baud rate

The baud or signal rate can be expressed as:

$$S = c \times N \times 1/r \text{ bauds}$$

Where,

- N is data rate
- c is the case factor (worst, best & avg.)
- r is the ratio between data element & signal element

Example 1

A signal is carrying data in which one data element is encoded as one signal element (r = 1). If the bit rate is 100 kbps, what is the average value of the baud rate if c is between 0 and 1?

Solution

We assume that the average value of c is 1/2 . The baud rate is then

$$S = c \times N \times \frac{1}{r} = \frac{1}{2} \times 100{,}000 \times \frac{1}{1} = 50{,}000 = 50 \text{ kbaud}$$

Calculate the value of signal rate for each of the cases if data rate is 1 Mbps and c= 1/2

We use the formula $s = c \times N \times (1/r)$ for each case. We let $c = 1/2$.

a. $r = 1 \rightarrow s = (1/2) \times (1\ \text{Mbps}) \times 1/1 = 500$ **kbaud**

b. $r = 1/2 \rightarrow s = (1/2) \times (1\ \text{Mbps}) \times 1/(1/2) = 1$ **Mbaud**

c. $r = 2 \rightarrow s = (1/2) \times (1\ \text{Mbps}) \times 1/2 = 250$ **Kbaud**

d. $r = 4/3 \rightarrow s = (1/2) \times (1\ \text{Mbps}) \times 1/(4/3) = 375$ **Kbaud**

Line Coding

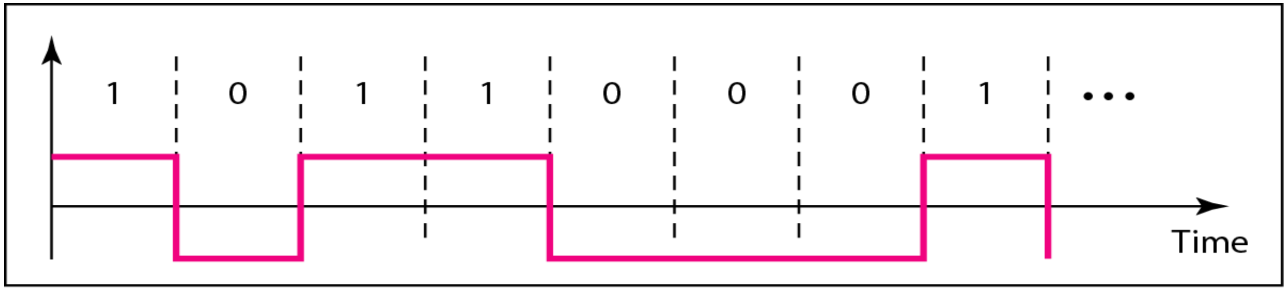
- **Data** as well as **signals** that represents data can either be digital or analog.
- **Line coding** is the process of converting **digital data to digital signals**.
- By this technique we converts a sequence of bits to a digital signal.
- At the sender side digital data are encoded into a digital signal and at the receiver side the digital data are recreated by decoding the digital signal.

We can divide line coding schemes into five categories

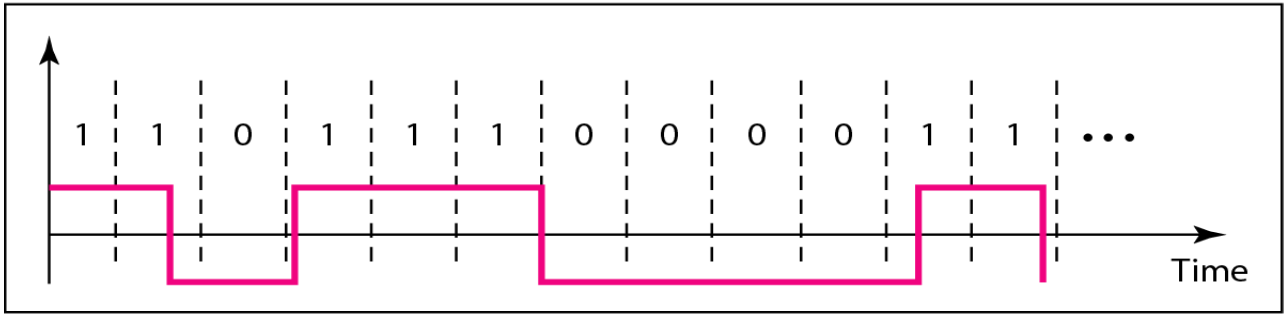
- Unipolar (eg. NRZ scheme).
- Polar (eg. NRZ-L, NRZ-I, RZ, and Biphase – Manchester and differential Manchester).
- Bipolar (eg. AMI and Pseudoternary).
- Multilevel
- Multitransition

Characteristic of line coding techniques

- There should be **self-synchronizing** i.e., both receiver and sender clock should be synchronized.
- There should have some error-detecting capability.
- There should be immunity to noise and interference.
- There should be less complexity.
- There should be no low frequency component (**DC-component**) as long distance transfer is not feasible for low frequency component signal.
- There should be less base line wandering.



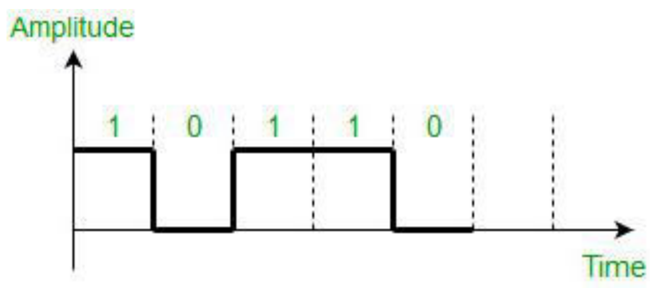
a. Sent



b. Received

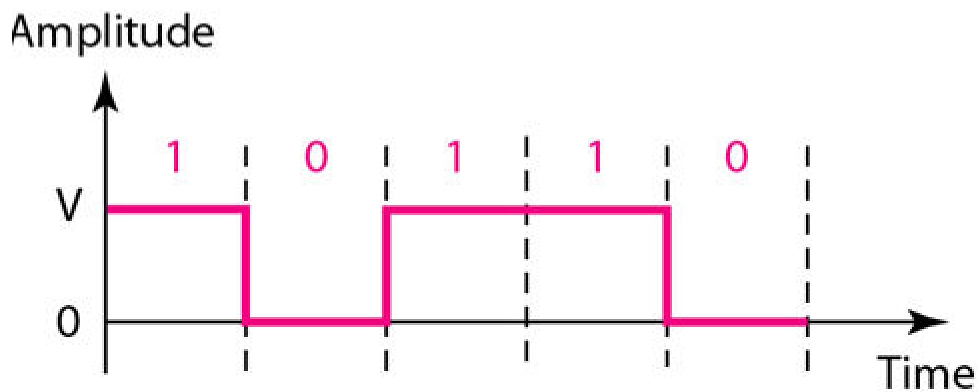
Unipolar scheme

All signal levels are on **one side of the time axis** - either above or below
It is unipolar line coding scheme in which positive voltage defines bit 1 and the zero voltage defines bit 0. Signal does not return to zero at the middle of the bit thus **it is called NRZ**. For example: Data = 10110.



Disadvantages
But this scheme uses more power as compared to polar scheme to send one bit per unit line resistance.
Moreover for continuous set of zeros or ones there will be self-synchronization and base line wandering problem.

Unipolar NRZ scheme



<u>Assumption</u>: data element '1' is on positive side of axis and data element '0' is on the axis.

<u>NOTE:</u> data element '1' is on negative side of axis and data element '0' is on the axis can also be assumed

Polar – NRZ Line Coding Scheme

The voltages are on both sides of the time axis.

The signal level does not return to zero during a symbol transmission **(during bit duration)**.

The signal will change level at the edge of the time interval and not in between.

Polar NRZ scheme can be implemented with two voltages. **E.g. +V for 1 and -V for 0 or vice versa**

There are two versions:

NZR - Level (NRZ-L) - **Positive voltage for one symbol and negative for the other**

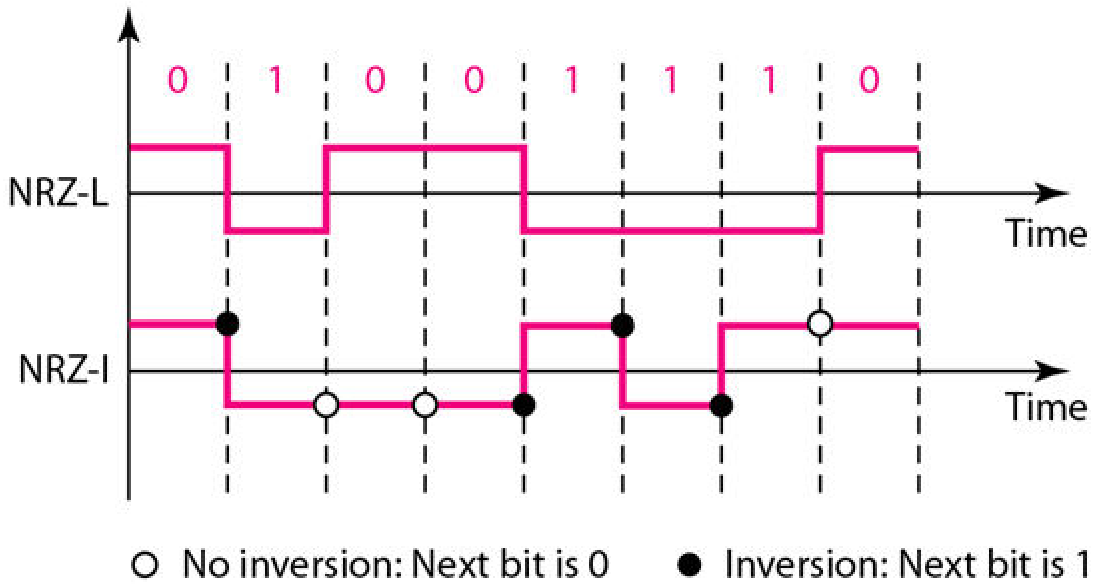
NRZ - Inversion (NRZ-I) - Two-level signal has a transition at a boundary.

If the next bit that we are going to transmit is a logical 1,

Does not have a transition if the next bit that we are going to transmit is a logical 0.

Figure 4.6 *Polar NRZ-L and NRZ-I schemes*

Assumption: +V for 0 and -V for 1

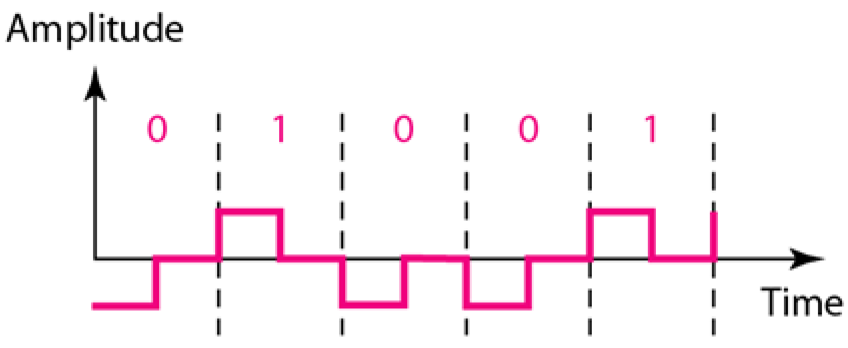


Polar –RZ Line Coding Scheme

- The Return to Zero (RZ) scheme uses **three voltage values.**
- **+, 0, -.**
- **Each symbol has a transition in the middle**.
- Either from high to zero or from low to zero.
- The signal level will return to zero during a symbol transmission **(during bit duration)**.
- The signal will change level in between of the signal element or bit duration.
- This scheme has more signal transitions **(two per symbol)** and therefore requires a wider bandwidth.

Polar RZ scheme

Assumption: +V for 1 and -V for 0



One Bit Duration, Signal is returning to zero axis during the bit i.e., at the middle of the signal element transmission and not at the edge of the interval

Problem-1

In a digital transmission, the receiver clock is 0.1 percent faster than the sender clock. How many extra bits per second does the receiver receive if the data rate is 1 kbps? How many if the data rate is 1 Mbps?

Solution

At 1 kbps, the receiver receives 1001 bps instead of 1000 bps.
Note:1kbps=1000bps

1000 bits sent	1001 bits received	1 extra bps

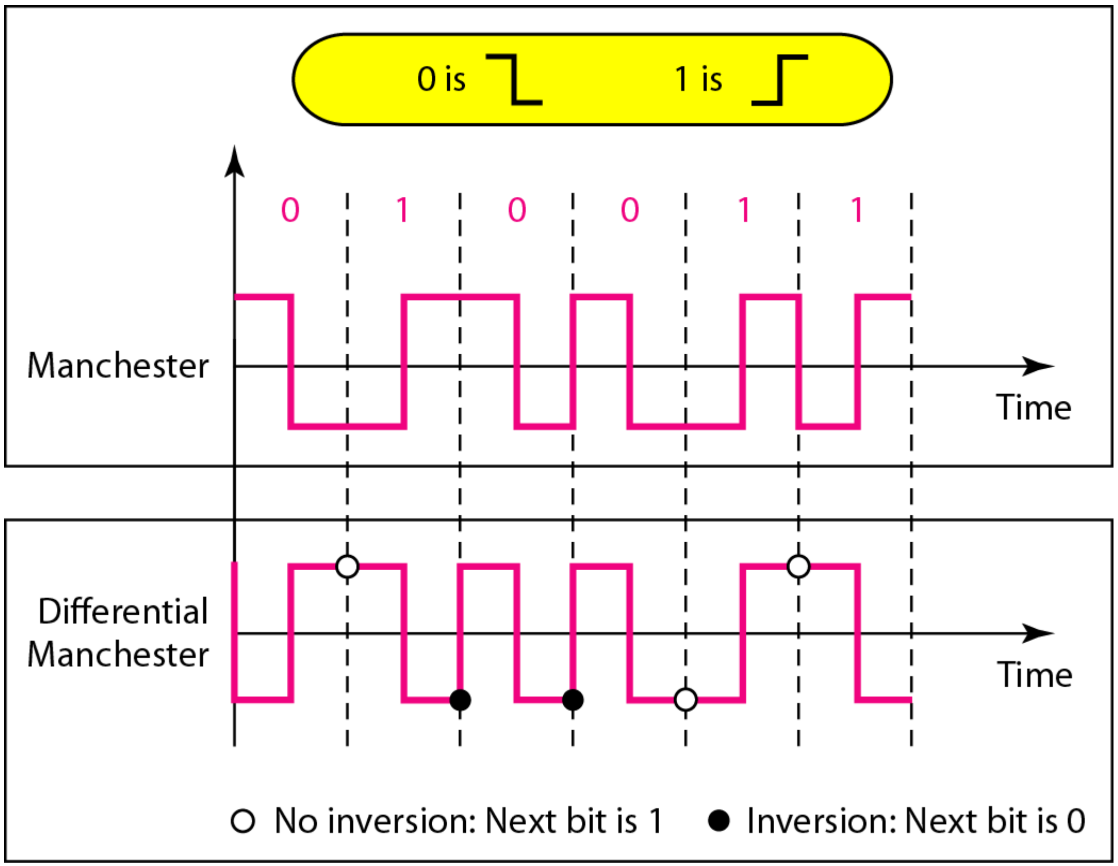
At 1 Mbps, the receiver receives 1,001,000 bps instead of 1,000,000 bps.
Note 1MBPS=1000000bps

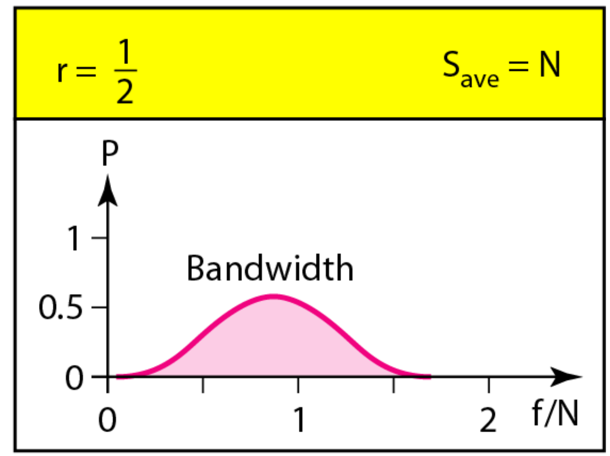
1,000,000 bits sent	1,001,000 bits received	1000 extra bps

Polar Biphase: Manchester and Differential Manchester

- Manchester coding consists of combining the NRZ-L and RZ schemes.
  - **Every symbol has a level transition in the middle: from high to low or low to high. Uses only two voltage levels.**
- Differential Manchester coding consists of combining the NRZ-I and RZ schemes.
  - **Every symbol has a level transition in the middle. But the level at the beginning of the symbol is determined by the symbol value. One symbol causes a level change the other does not.**

Figure 4.8 *Polar biphase: Manchester and differential Manchester schemes*





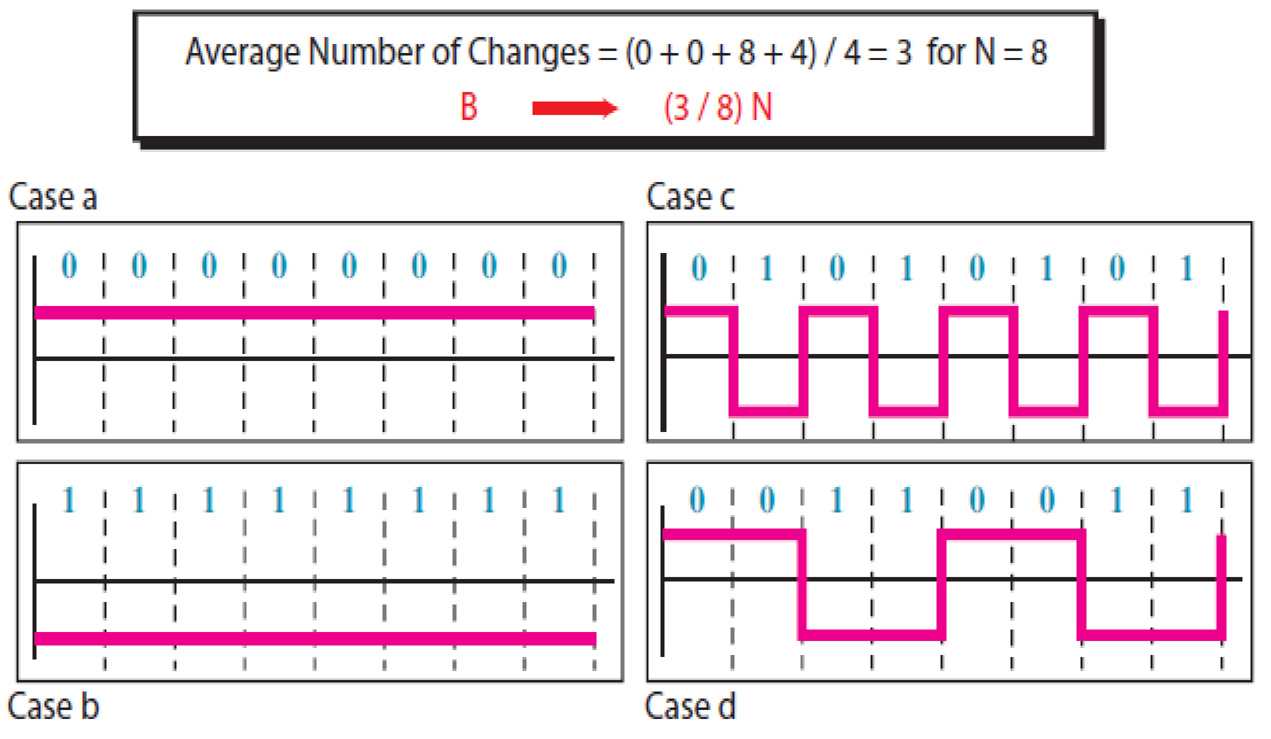
Question

14. In a digital transmission, the sender clock is 0.2 percent faster than the receiver clock. How many extra bits per second does the sender send if the data rate is 1 Mbps?
15. Draw the graph of the NRZ-L scheme using each of the following data streams, assuming that the last signal level has been positive. From the graphs, guess the bandwidth for this scheme using the average number of changes in the signal level. Compare your guess with the corresponding entry in Table 4.1.
    a. 00000000
    b. 11111111
    c. 01010101
    d. 00110011
16. Repeat Exercise 15 for the NRZ-I scheme.
17. Repeat Exercise 15 for the Manchester scheme.
18. Repeat Exercise 15 for the differential Manchester scheme.

14. The number of bits is calculated as $(0.2/100) \times (1\text{ Mbps}) =$ **2000 bits**

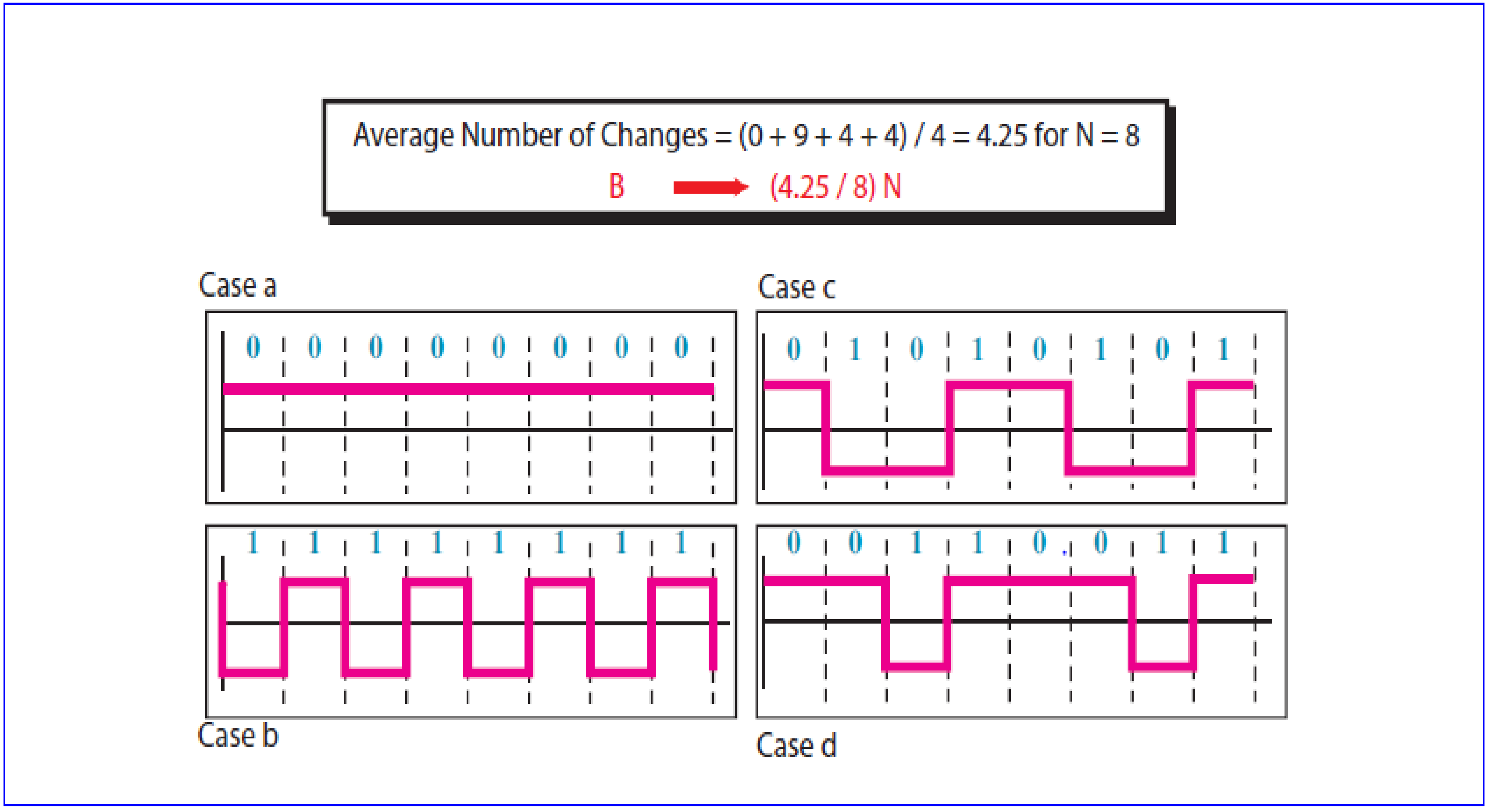
Solution

Figure 4.1 *Solution to Exercise 15*



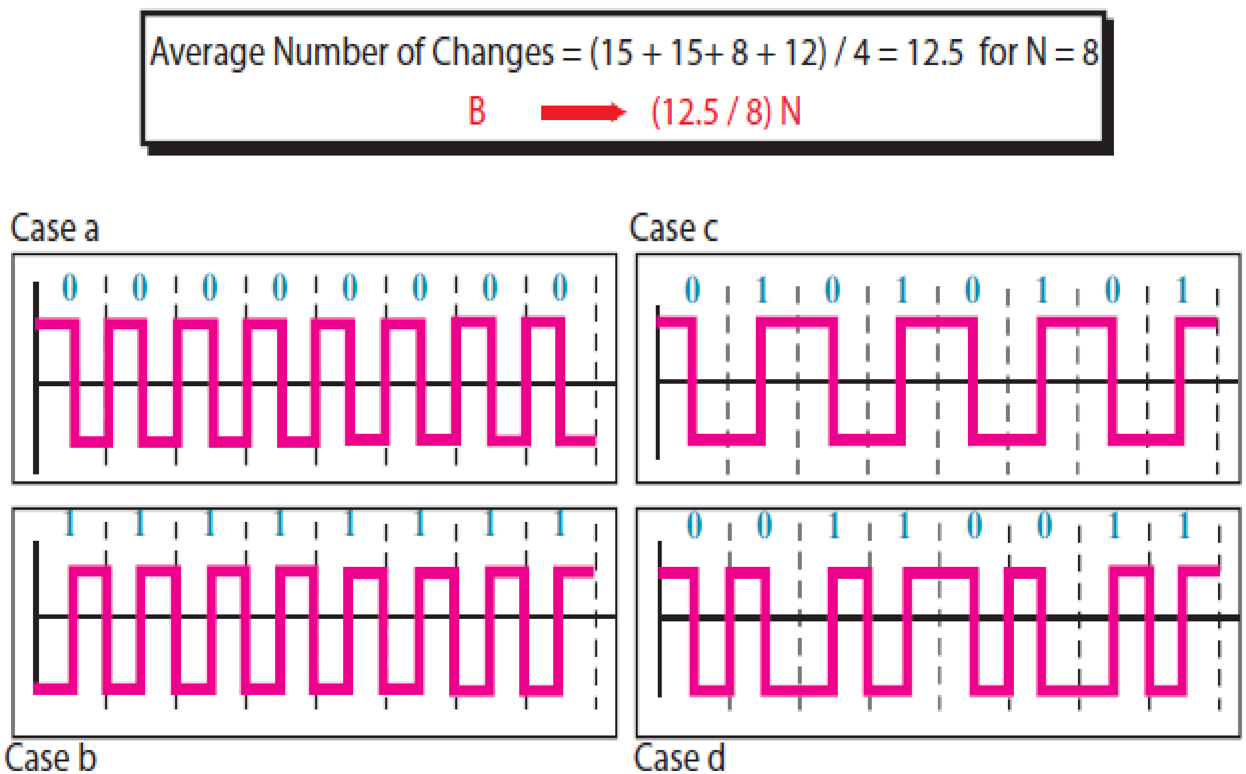
Solution

Figure 4.2 *Solution to Exercise 16*



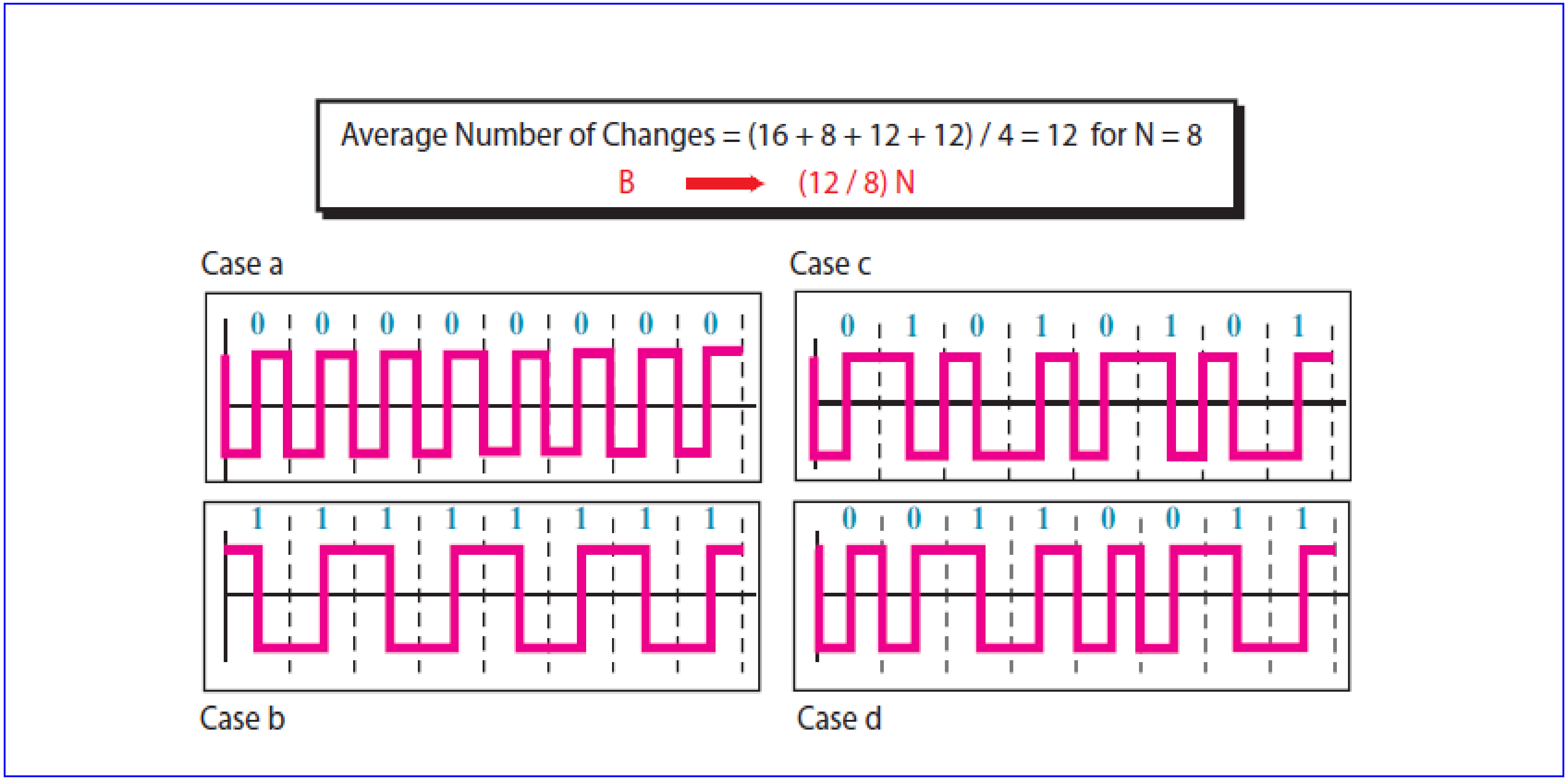
Solution

Figure 4.3 *Solution to Exercise 17*



Solution

Figure 4.4 *Solution to Exercise 18*



COMPUTER NETWORKS (BCSC 0008)

MULTIPLEXING

Text and Reference Books

Text Books:

1. Fourouzan B. A. (2004), "Data Communication and Networking", 4th Edition, McGraw-Hill.

References:

1. Kurose, J. F. and Ross K. W. (2005), "Computer Networking: A Top-Down Approach Featuring the Internet", 3rd Edition, Addison-Wesley.
2. A. S. Tanenbaum (2006), "Computer Networks", 2nd Edition, Prentice Hall India.

Previous discussed topics:

1. **OSI Model**
2. **TCP/IP Model**
3. **Addressing**
4. **Data & Signals**
5. **Transmission Media & Line Encoding**
6. **Switching**

Now we will discuss:

1. **Multiplexing : FDM & TDM**

Bandwidth utilization is the wise use of available bandwidth to achieve specific goals.

Efficiency can be achieved by multiplexing;

MULTIPLEXING

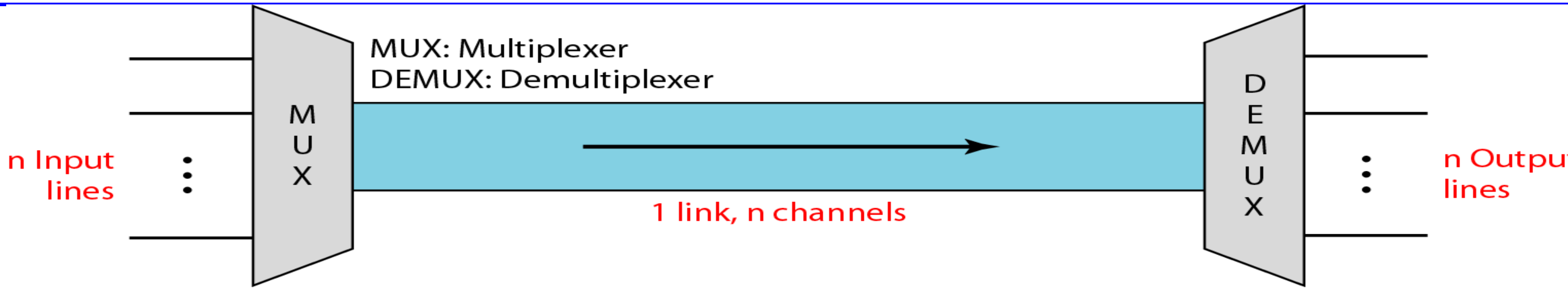
Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared.

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

If the bandwidth of a link is greater than the bandwidth needs of the devices connected to it, the bandwidth is wasted.

An efficient system maximizes the utilization of all resources; bandwidth is one of the most precious resources we have in data communications.

Dividing a link into channels



- ❖ The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream (many-to one).
- ❖ At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines.

MULTIPLEXING

- Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

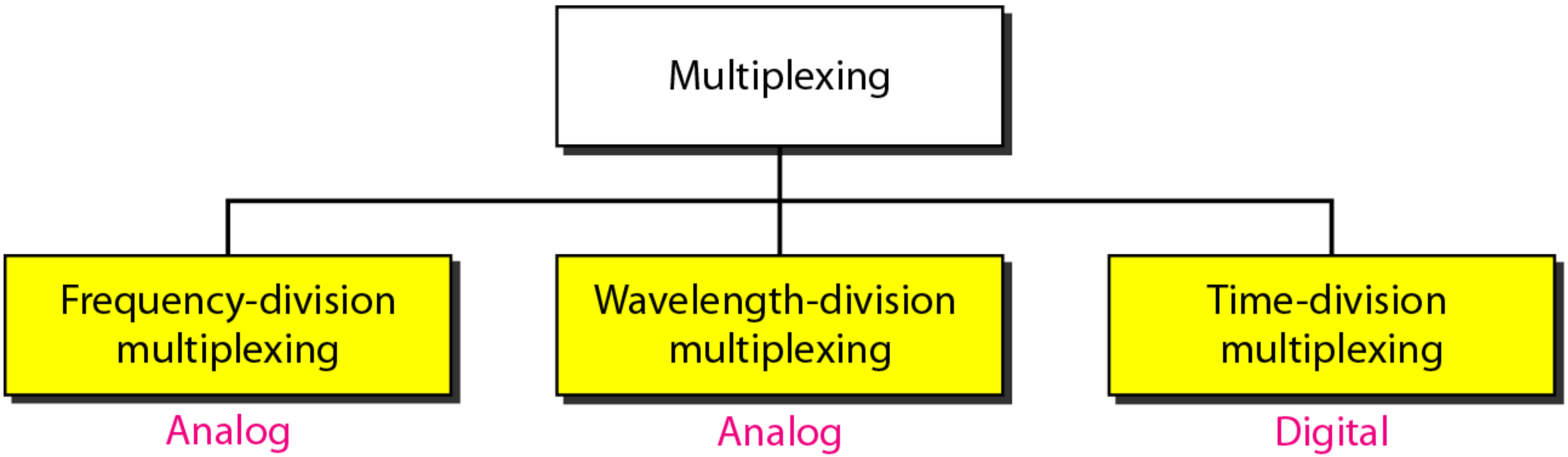
- A **Multiplexer** (MUX) is a device that combines several signals into a single signal. It is a device that selects between several analog or digital input signals and forwards the selected input to a single output line.

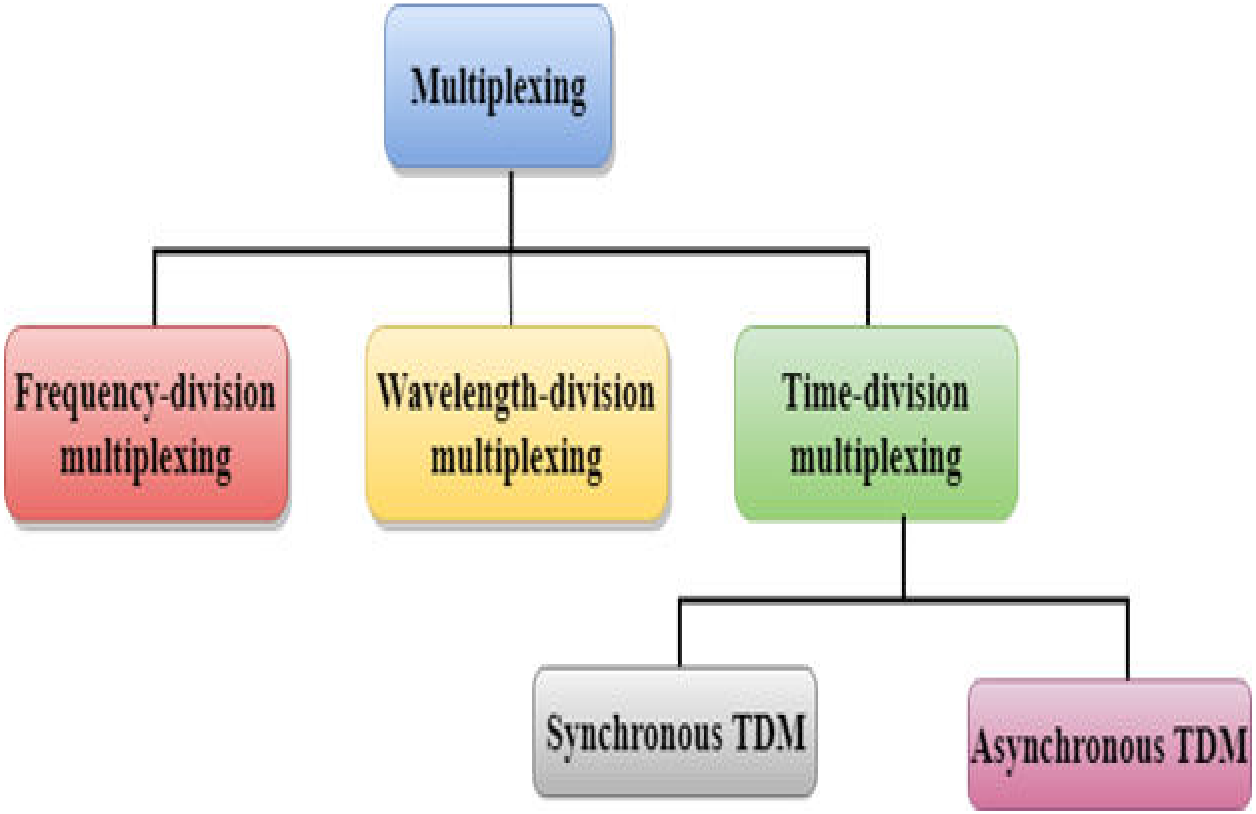
- A **Demultiplexer** (DEMUX) is a device that performs the inverse operation.

Advantages of Multiplexing

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

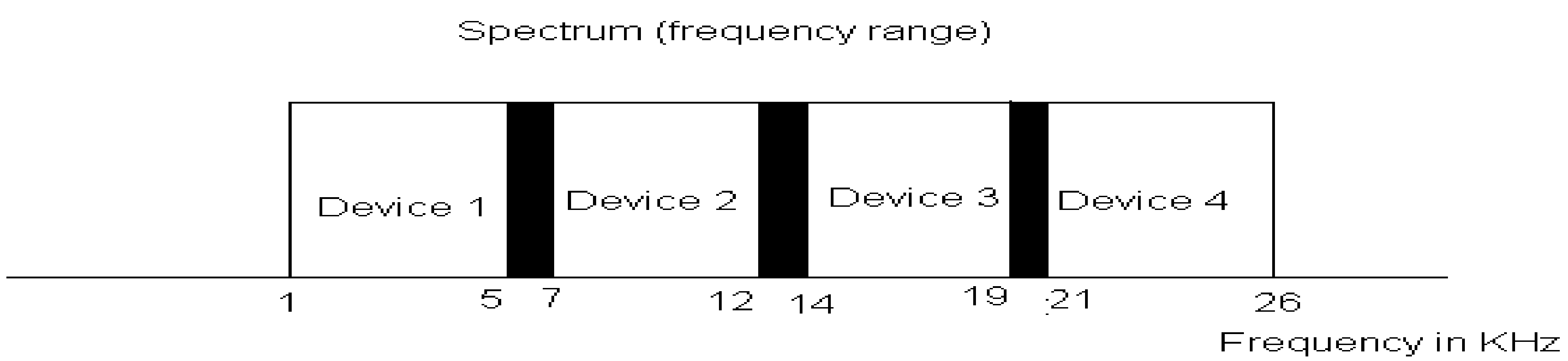
Categories of multiplexing



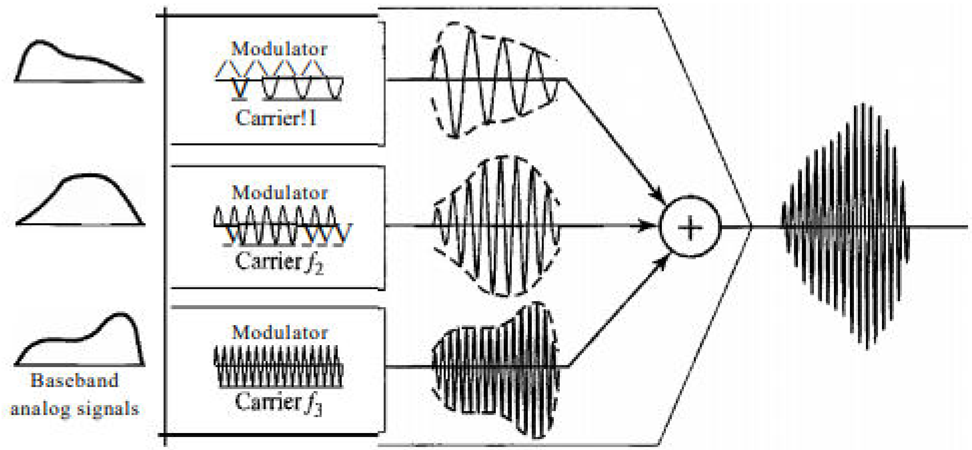

Multiplexing
Frequency-division multiplexing
Wavelength-division multiplexing
Time-division multiplexing
Synchronous TDM
Asynchronous TDM

Frequency-division Multiplexing (FDM)

- Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted.
- Signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link.
- Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal.
- The frequency spectrum is divided into several logical channels, in which every user feels that they possess a particular bandwidth
- There is a suitable frequency gap between the 2 adjacent signals to avoid over-lapping. Since the signals are transmitted in the allotted frequencies so this decreases the probability of collision.



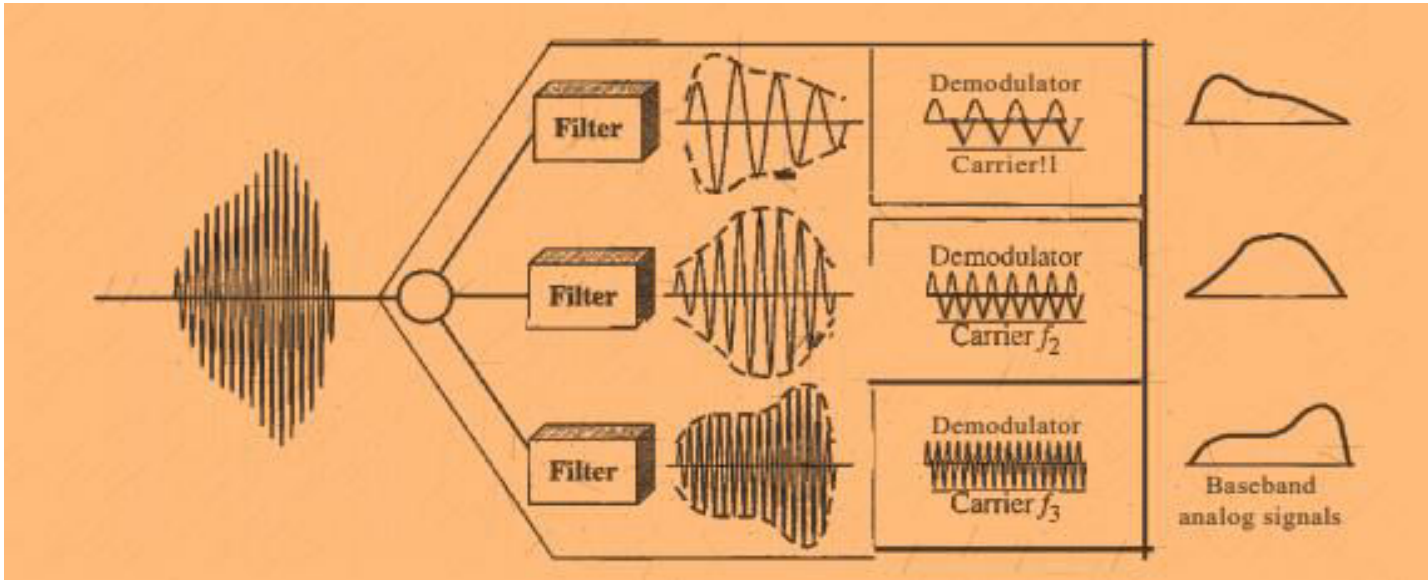
We consider FDM to be an analog multiplexing technique; however, this does not mean that FDM cannot be used to combine sources sending digital signals.
A digital signal can be converted to an analog signal before FDM is used to multiplex them



Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies (f1,f2 and f3).
The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

FDM Demultiplexing Process

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines.



Applications of FDM

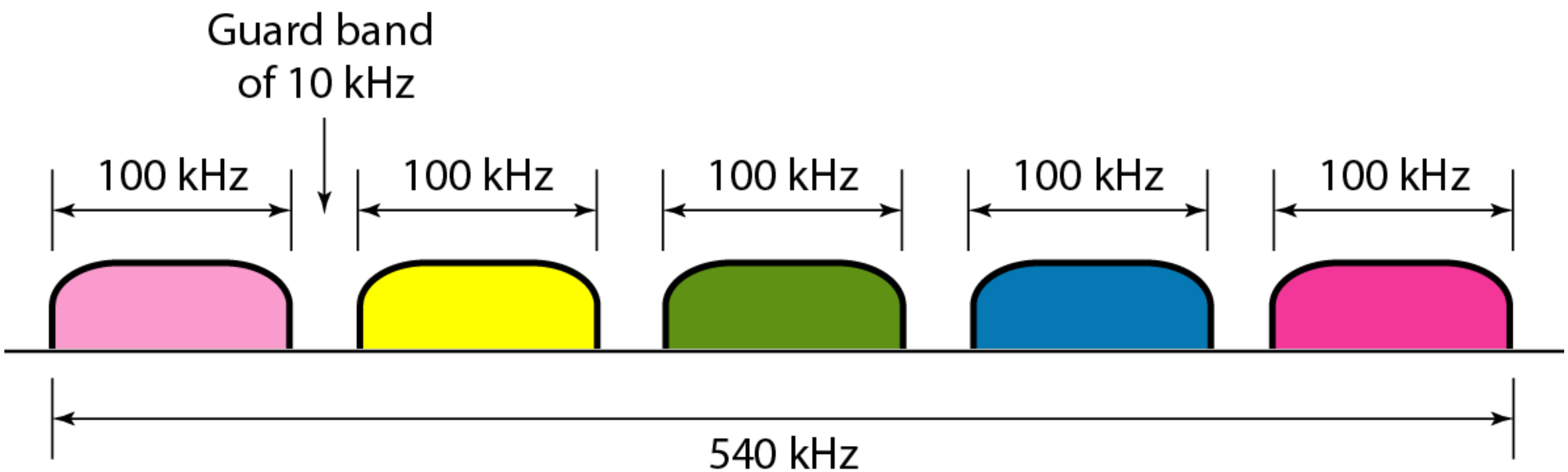
- A very common application of FDM is AM(Amplitude Modulation) and FM radio broadcasting.

- Radio uses the air as the transmission medium

- Another common use of FDM is in television broadcasting. Each TV channel has its own bandwidth of 6 MHz.

- The first generation of cellular telephones (still in operation) also uses FDM. Each user is assigned two 30-kHz channels, one for sending voice and the other for receiving

Five channels, each with a 100-kHz bandwidth, are to be multiplexed together. What is the minimum bandwidth of the link if there is a need for a guard band of 10 kHz between the channels to prevent interference?



Solution

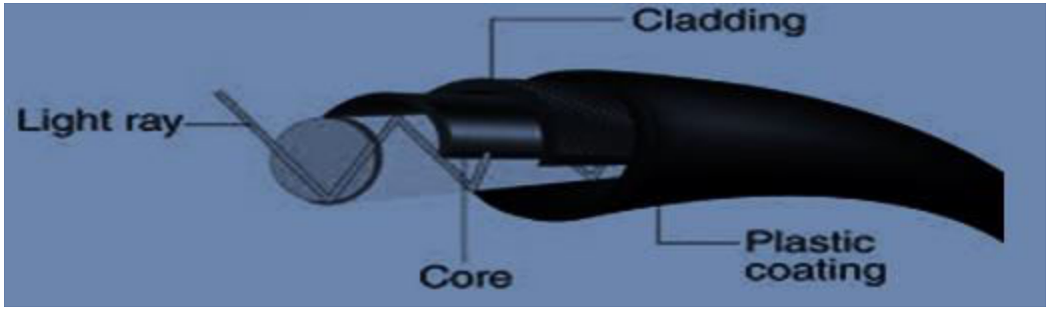
For five channels, we need at least four guard bands. This means that the required bandwidth is at least

$$5 \times 100 + 4 \times 10 = 540 \text{ kHz},$$

FDM is an analog multiplexing technique that combines analog signals.

Wavelength Division Multiplexing (WDM)

Wavelength Division Multiplexing is same as FDM except that the optical signals(**Optical signal** is an electromagnetic **signal**) are transmitted through the fibre optic cable.

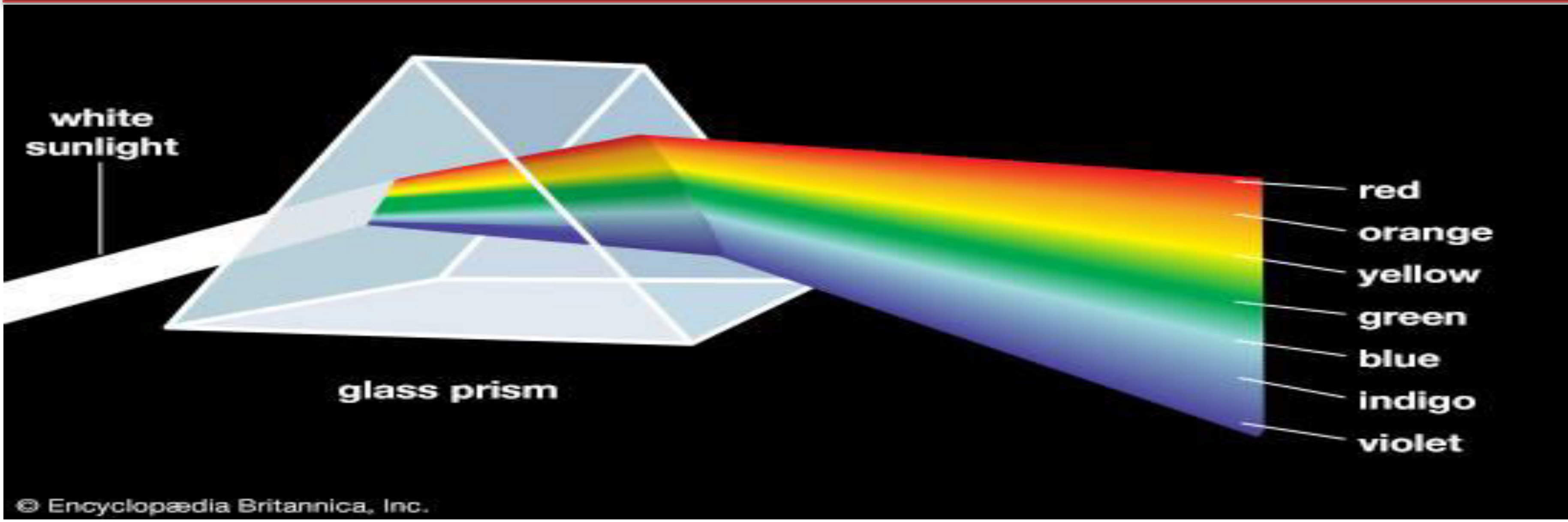


WDM is used on fibre optics to increase the capacity of a single fibre

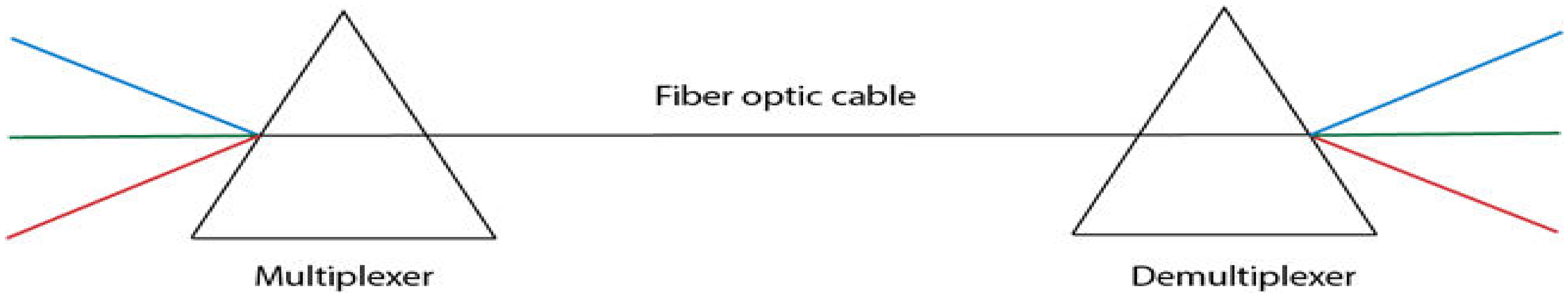
It is an analog multiplexing technique.

Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.

Note: Light has the property that keeps it from mixing and allows it to be separated into its color like this prism.



- ❖ Multiplexing and Demultiplexing can be achieved by using a prism.
- ❖ Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- ❖ Prism also performs a reverse operation, i.e., demultiplexing the signal.



- The technology of WDM is widely used in Optical Transport Networks.
- This technology can be used in Synchronous optical networking. SONET is a communication protocol, developed by Bellcore – that is used to transmit a large amount of data over relatively large distances using optical fibre. With SONET, multiple digital data streams are transfered at the same time over the optical fibre.
- This technology is used for up gradation of broadband

TDMA(Time Division Multiple Access)

An alternative to FDM is TDM(Time Division Multiplexing). Here, the users take turns (in a round-robin fashion),each one periodically getting the entire bandwidth for a little burst of time.

❖This happens when data transmission rate of media is greater than that of the sources(sending and receiving device), and each signal is allotted a definite amount of time.

❖These slots are so small that all transmissions appear to be parallel.

❖In frequency division multiplexing all the signals operate at the same time with different frequencies, but in time division multiplexing all the signals operate with same frequency at different times.

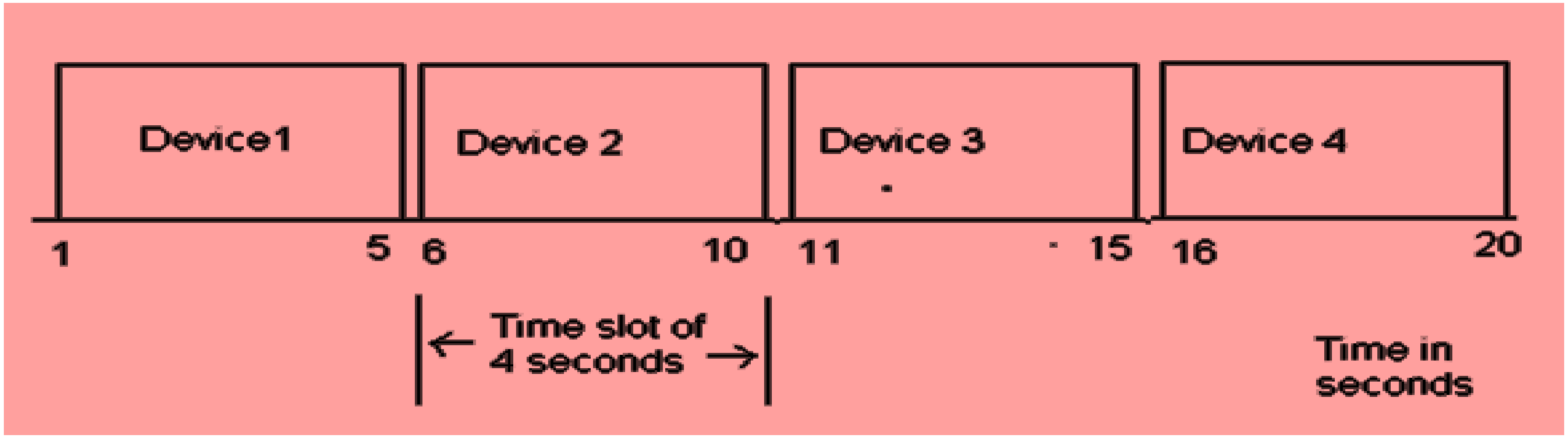
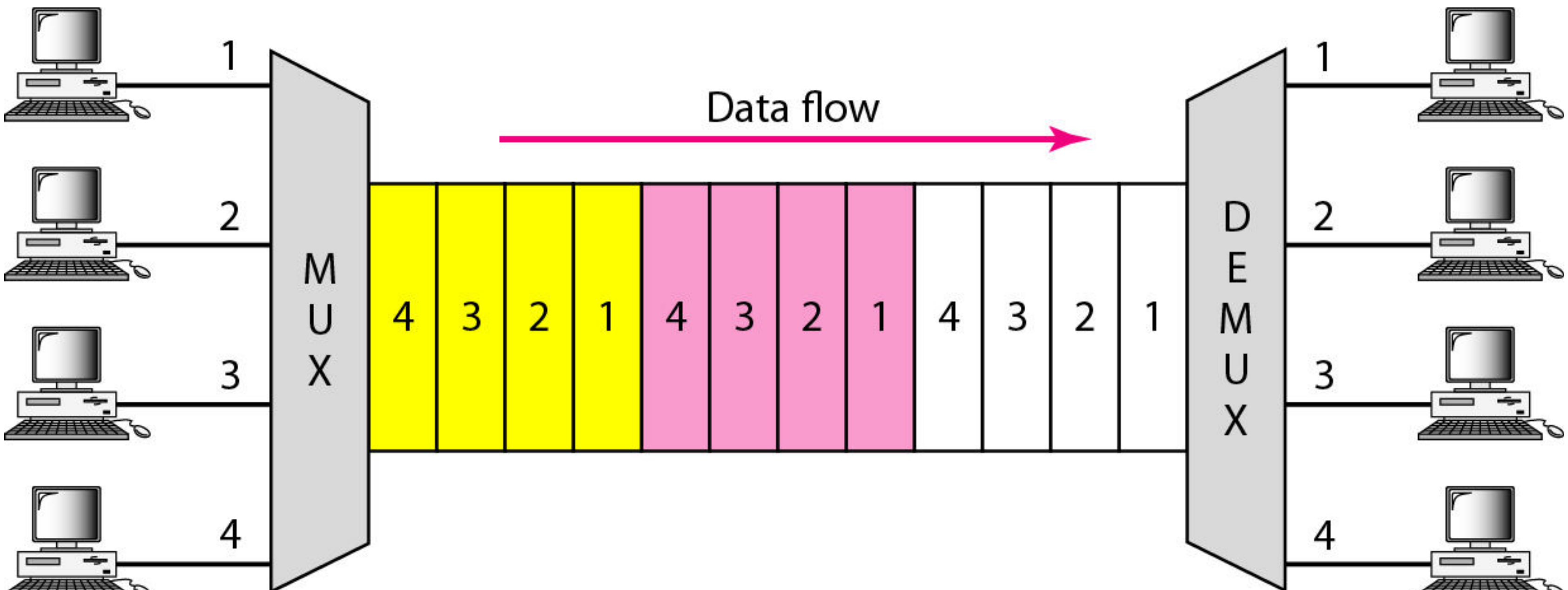


Figure 6.12 *TDM*



TDM is a digital multiplexing technique for combining several low-rate channels into one high-rate one.

Time-division Multiplexing (TDM)

TDM can be implemented in two ways:

- Synchronous TDM
- Asynchronous TDM

Synchronous time-division

- In synchronous TDM, every device which is present in this has given the same time slot to transmit data. It does not consider whether the device contains data or not.
- Time slots are grouped into frames. There are various kinds of time slots that are organized into frames and each frame consist of one or more time slots dedicated to each sending device.

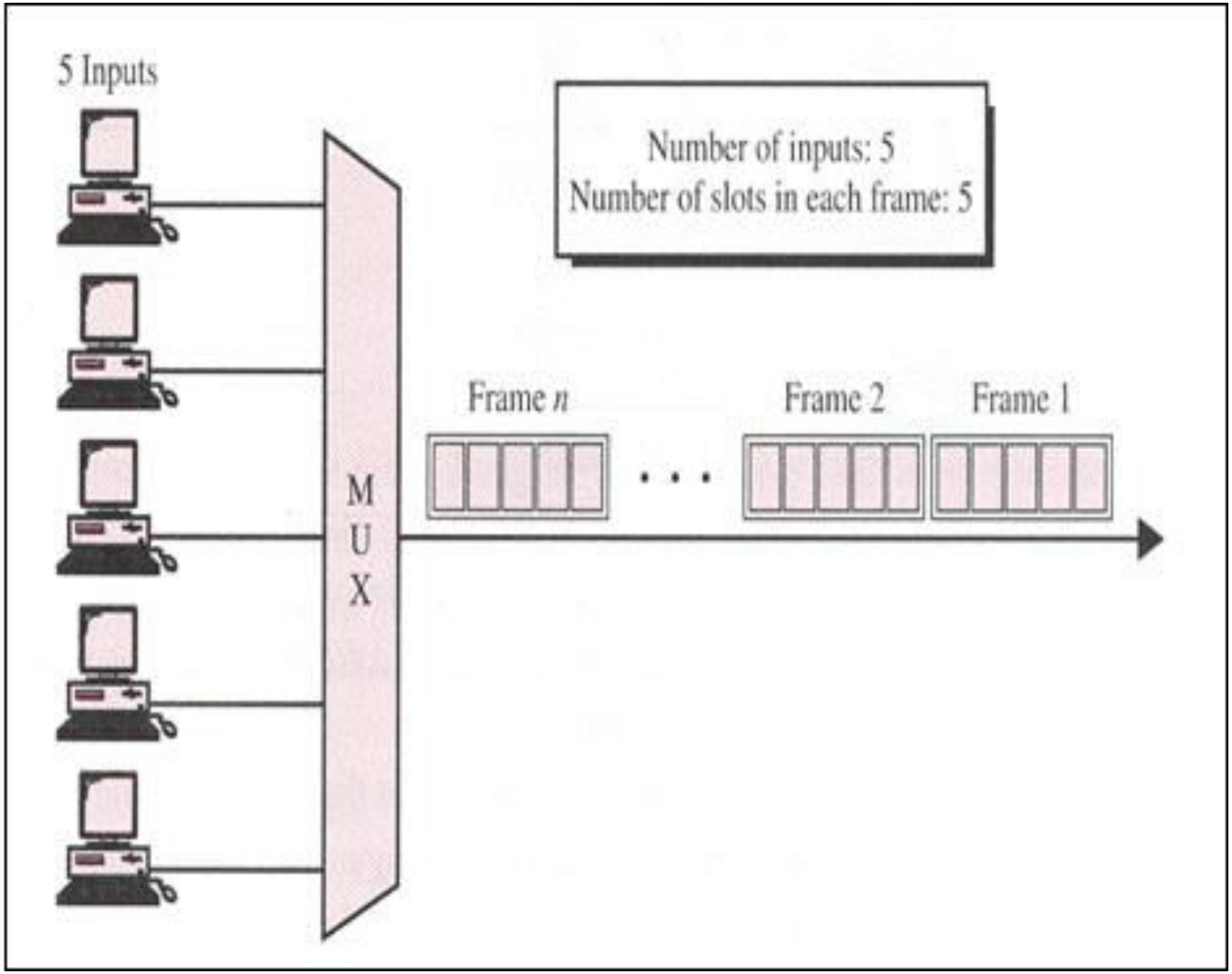
Asynchronous TDM

Other name of asynchronous TDM is statistical division multiplexing. It is called so because time-slots are not fixed i.e. slots are flexible. As slots are not fixed, a device which wants to send data allotted time-slot.

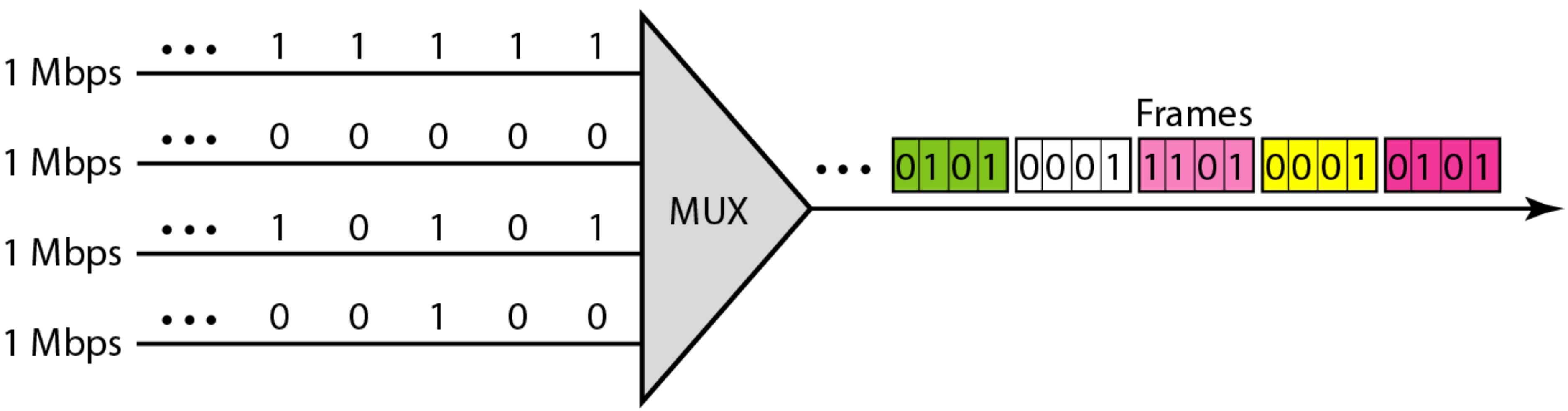
Application of TDMA

It used in ISDN (Integrated Services Digital Network) telephone lines.
It is used in PSTN (public switched telephone network).
It is used for some telephone system.
TDM is used in digital audio mixing system.

Note: It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.


5 Inputs
Number of inputs: 5
Number of slots in each frame: 5
MUX
Frame n
Frame 2
Frame 1
. . .

Given figure shows synchronous TDM with a **data stream for each input** and **one data stream** for the output. The unit of data is 1 bit. Find
(a) the input bit duration,
(b) the output bit duration,
(c) the output bit rate, and
(d) the output frame rate.



Solution

We can answer the questions as follows:

Note:**The input bit duration is the inverse of the bit rate**

Here bit rate =1 MBPS

So the input bit duration=1/1 Mbps = 1 μs.

b. **The output bit duration is one-fourth of the input bit duration(four slot in a frame)**, or ¼ μs.

C. **The output bit rate is the inverse of the output bit duration or** 1/(4μs) or 4 Mbps. This can also be deduced from the fact that the output rate is 4 times as fast as any input rate; so the output rate = 4 × 1 Mbps = 4 Mbps.

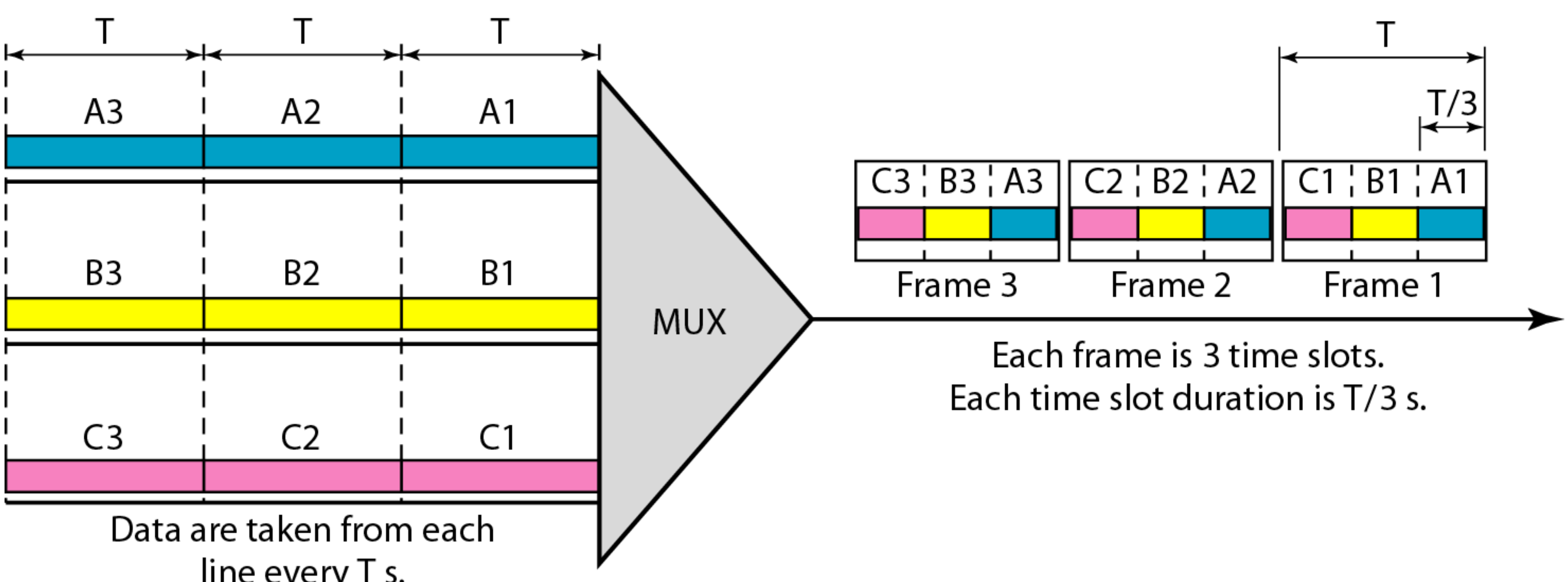
d. The frame rate is always the same as any input rate. So the frame rate is 1,000,000(as 1 MBPS=10power6bps) frames per second.

In given Figure, the data rate for each input connection is 1 kbps. If 1 bit at a time is multiplexed (a unit is 1 bit), what is the duration of

(a) Each input slot,

(b) Each output slot, and

(c) Each frame?



Solution

- **Each input slot**

a. The input bit duration is the inverse of the bit rate The data rate of each input connection is 1 kbps. This means that the bit duration is 1/1000 s or 1ms(1000 **milliseconds** in a **second**). The duration of the input time slot is 1 ms (same as bit duration).

- **Each output slot**

b.

The duration of each output time slot is one-third of the input time slot. This means that the duration of the output time slot is 1/3 ms.

c. Each frame carries three output time slots. So the duration of a frame is 3 × 1/3 ms, or 1 ms. The duration of a frame is the same as the duration of an input unit.

Example 6.7

Four 1-kbps connections are multiplexed together. A unit is 1 bit. Find

(a) The duration of 1 bit before multiplexing,
(b) The transmission rate of the link,
(c) The duration of a time slot, and
(d) The duration of a frame.

Solution

We can answer the questions as follows:

a. The duration of 1 bit before multiplexing is 1 / 1 kbps, or 0.001 s (1 ms).

b. The rate of the link is 4 times the rate of a connection, or 4 kbps.

c. The duration of each time slot is one-fourth of the duration of each bit before multiplexing, or 1/4 ms or 250 μs. Note that we can also calculate this from the data rate of the link, 4 kbps. The bit duration is the inverse of the data rate, or 1/4 kbps or 250 μs.

d. The duration of a frame is always the same as the duration of a unit before multiplexing, or 1 ms. We can also calculate this in another way. Each frame in this case has four time slots. So the duration of a frame is 4 times 250 μs, or 1 ms.

COMPUTER NETWORKS (BCSC 0008)

Lecture 8
Transmission Media

Lecture Presented by: Prof. Diwakar Bharadwaj, Mr. Saurabh Anand, Mr. Akhilesh Kumar Singh

Media

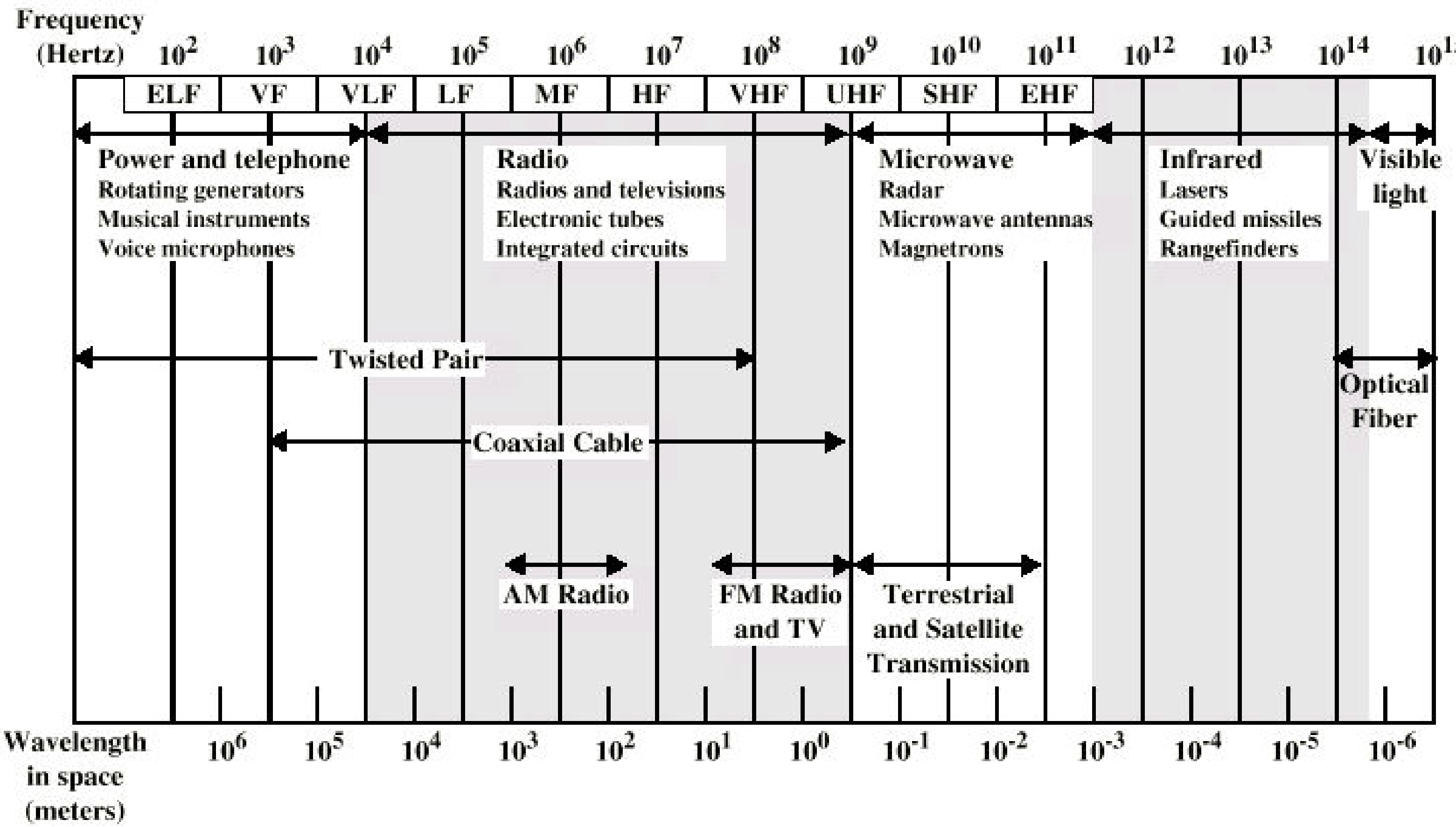
- Basic function of media – carry flow of information in form of bits through a LAN
  - In a copper based network, bits will be electrical signals
  - In a fiber based network, bits will be light pulses
  - Media considered to be Layer 1 component of a LAN
- Physical path between transmitter and receiver
- Wired and Wireless
- Communication is in the form of electromagnetic waves
- Characteristics and quality of data transmission are determined by characteristics of medium and signal
- In wired media, medium characteristics is more important, whereas in wireless media, signal characteristics is more important

Transmission Media

- Physical path between transmitter and receiver
- Wired and Wireless
- Communication is in the form of electromagnetic waves
- Characteristics and quality of data transmission are determined by characteristics of medium and signal
- In wired media, medium characteristics is more important, whereas in wireless media, signal characteristics is more important

Some Typical Media	Maximum Theoretical Bandwidth	Maximum Physical Distance
50-Ohm Coaxial Cable (Ethernet 10Base2, ThinNet)	10-100 Mbps	200m
75-Ohm Coaxial Cable (Ethernet 10Base5, ThickNet)	10-100 Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 10BaseT, 100Base-TX)	10 Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 100Base-TX)(Fast Ethernet)	100 Mbps	100m
Multimode (62.5/125um) Optical Fiber 100Base-FX	100 Mbps	2000m
Singlemode (10um core) Optical Fiber 1000Base-LX	1000Mbps (1.000 Gbps)	3000m
Other technologies being researched	2400 Mbps (2.400 Gbps)	40km = 40,000m
Wireless	2.0 Mbps	100m

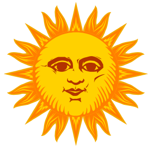
Electromagnetic Spectrum



ELF = Extremely low frequency
VF = Voice frequency
VLF = Very low frequency
LF = Low frequency
MF = Medium frequency
HF = High frequency
VHF = Very high frequency
UHF = Ultrahigh frequency
SHF = Superhigh frequency
EHF = Extremely high frequency

Basic limitations

- Attenuation
- Delay Distortion
- Noise
  - Thermal/White Noise
  - Intermodulation Noise
  - Crosstalk
  - Echo
  - Impulse Noise

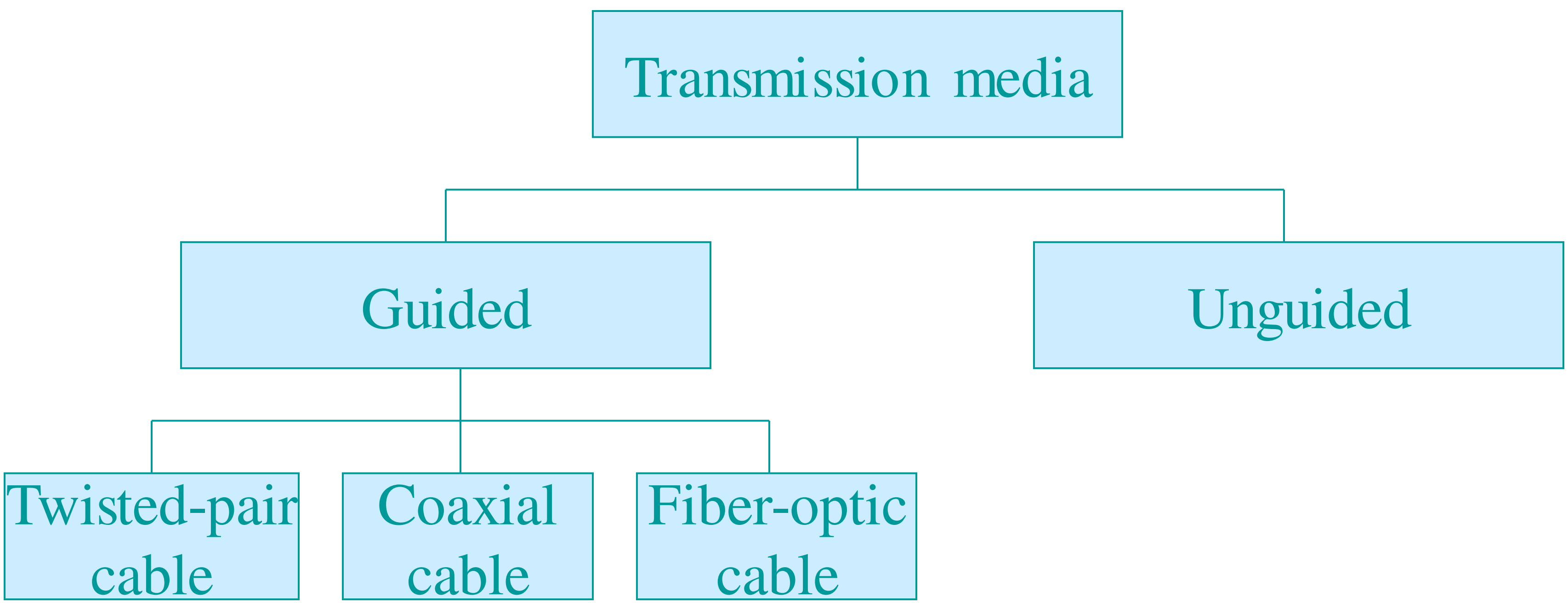


Design Factors for Transmission Media

- Bandwidth: All other factors remaining constant, the greater the band-width of a signal, the higher the data rate that can be achieved.
- Transmission impairments. Limit the distance a signal can travel.
- Interference: Competing signals in overlapping frequency bands can distort or wipe out a signal.
- Number of receivers: Each attachment introduces some attenuation and distortion, limiting distance and/or data rate.

Classes of Transmission Media

- Conducted or guided media
  - use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver
- Wireless or unguided media
  - use radio waves of different frequencies and do not need a wire or cable conductor to transmit signals



Wire Conductors

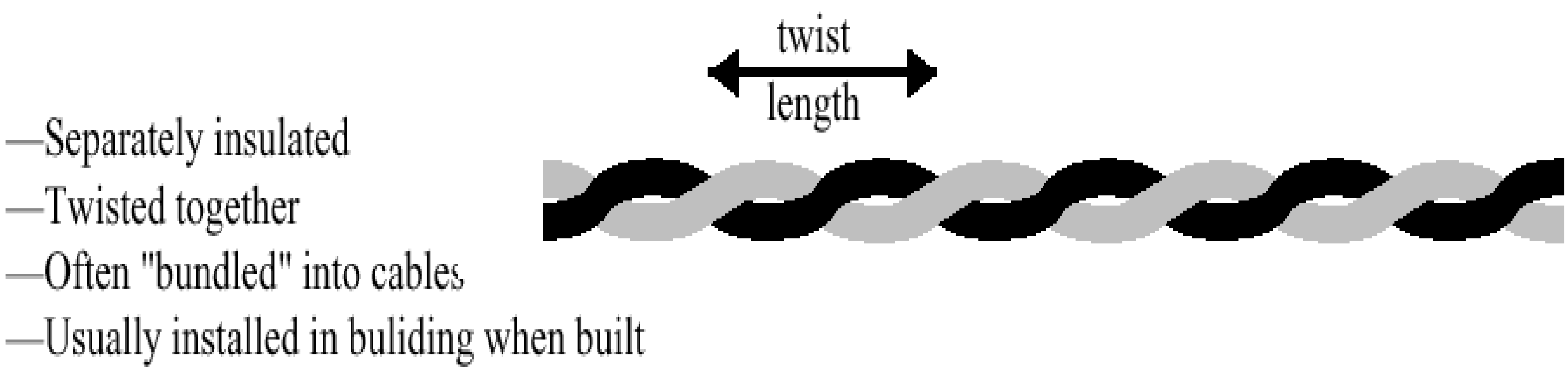
- Wire types: *single conductor*, *twisted pair*, & *shielded multiconductor bundles.*
- Large installed base.
- Reasonable cost.
- Relatively low bandwidth, however, recent LAN speeds in the 100 Mbps range have been achieved.
- Susceptible to external interference.
- Shielding can reduce external interference.
- Can transmit both analog and digital signals. Amplifier required every 5 to 6 km for analog signals. For digital signals, repeaters required every 2 to 3 km.

Wired - Twisted Pair

- The oldest, least expensive, and most commonly used media
- Pair of insulated wires twisted together to reduce susceptibility to interference : ex) capacitive coupling, crosstalk
- Skin effect at high frequency
- Up to 250 kHz analog and few Mbps digital signaling (for long-distance point-to-point signaling)
- Need repeater every 2-3 km (digital), and amplifier every 5-6 km (analog)

Twisted Pair

- Consists of two insulated copper wires arranged in a regular spiral pattern to minimize the electromagnetic interference between adjacent pairs
- Often used at customer facilities and also over distances to carry voice as well as data communications
- Low frequency transmission medium
- Telephone (subscriber loop: between house and local exchange)
- High-speed (10 - 100 Mbps) LAN :
    - token ring, fast - Ethernet



(a) Twisted pair

Types of Twisted Pair

- STP (shielded twisted pair)
  - the pair is wrapped with metallic foil or braid to insulate the pair from electromagnetic interference
- UTP (unshielded twisted pair)
  - each wire is insulated with plastic wrap, but the pair is encased in an outer covering

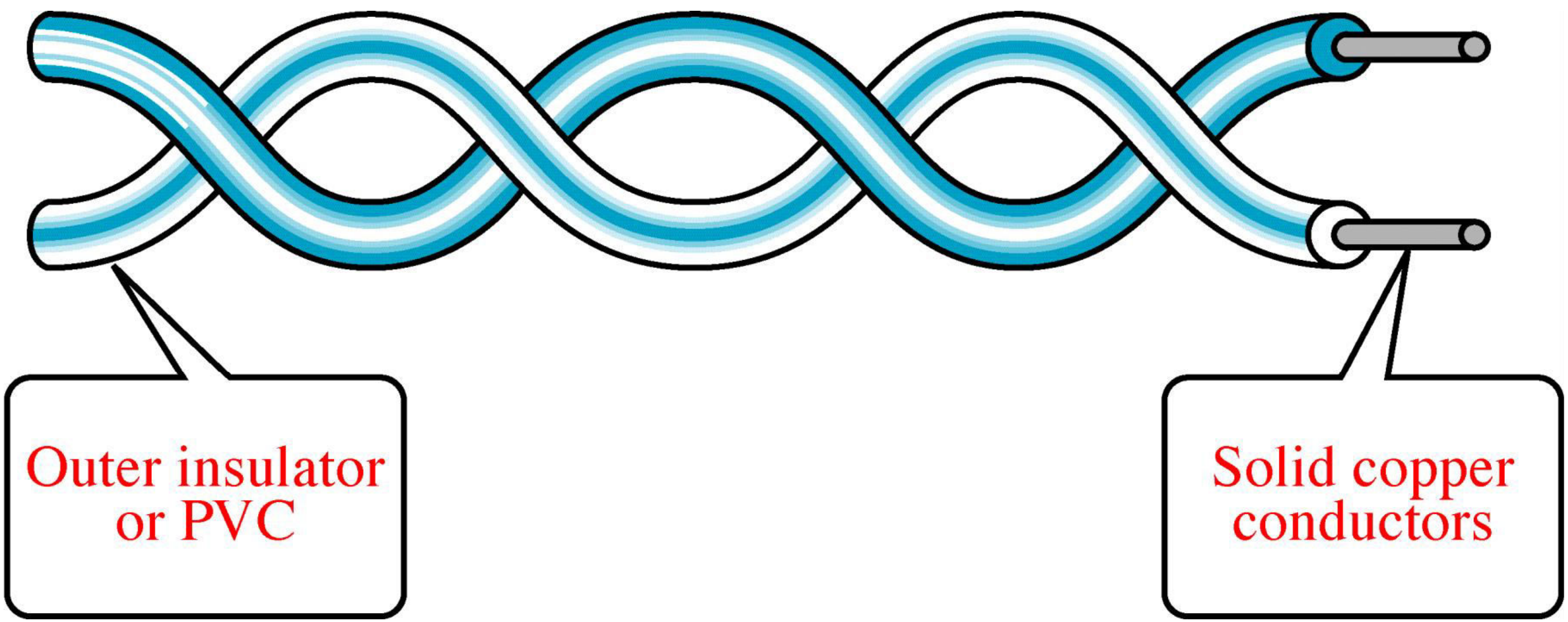
Ratings of Twisted Pair

- Category 3
  - UTP cables and associated connecting hardware whose transmission characteristics are specified up to 16 MHZ.
  - data rates of up to 16mbps are achievable
- Category 4
  - UTP cables and associated connecting hardware whose transmission characteristics are specified up to 20 MHz.
- Category 5
  - UTP cables and associated connecting hardware whose transmission characteristics are specified up to 100 MHz.
  - data rates of up to 100mbps are achievable
  - more tightly twisted than Category 3 cables
  - more expensive, but better performance
- Category 5 enhanced, Cat 6, cat 7
  - Fast and giga-ethernet
- STP
  - More expensive, harder to work with

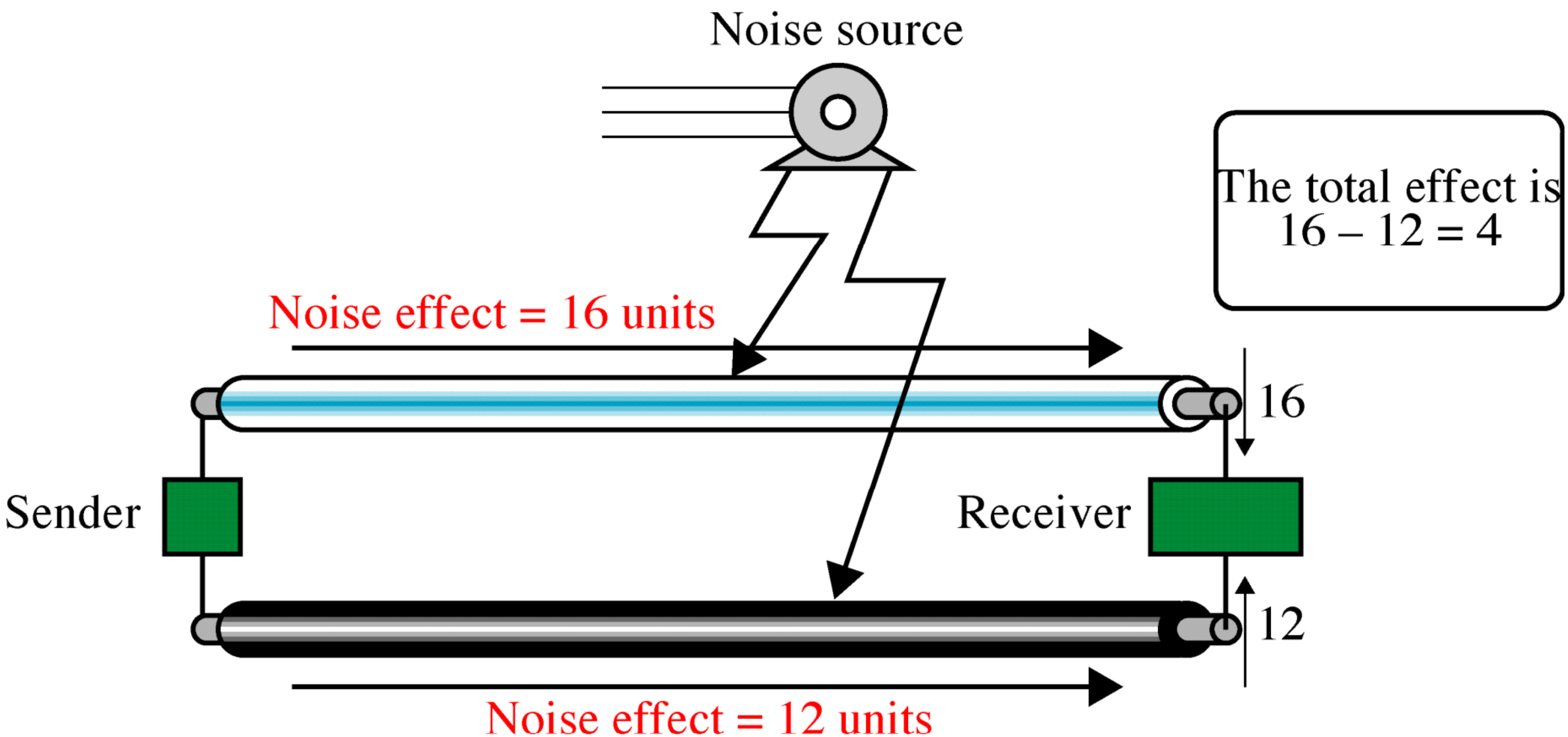
Twisted Pair Advantages

- Advantages
  - Inexpensive and readily available
  - Flexible and light weight
  - Easy to work with and install
- Disvantages
  - Susceptibility to interference and noise
  - Attenuation problem
    - For analog, repeaters needed every 5-6km
    - For digital, repeaters needed every 2-3km
  - Relatively low bandwidth (MHz)

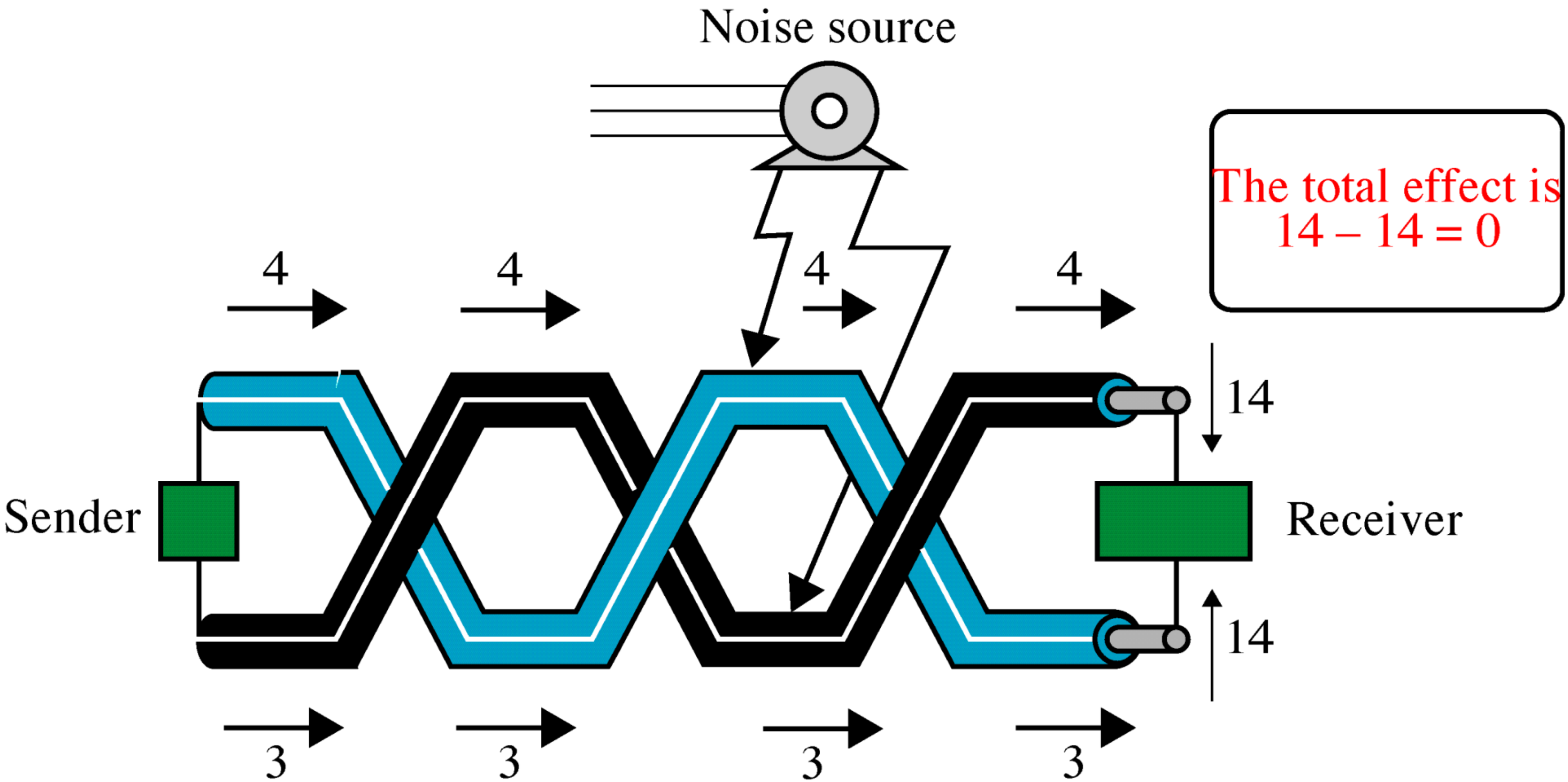
Twisted-Pair Cable



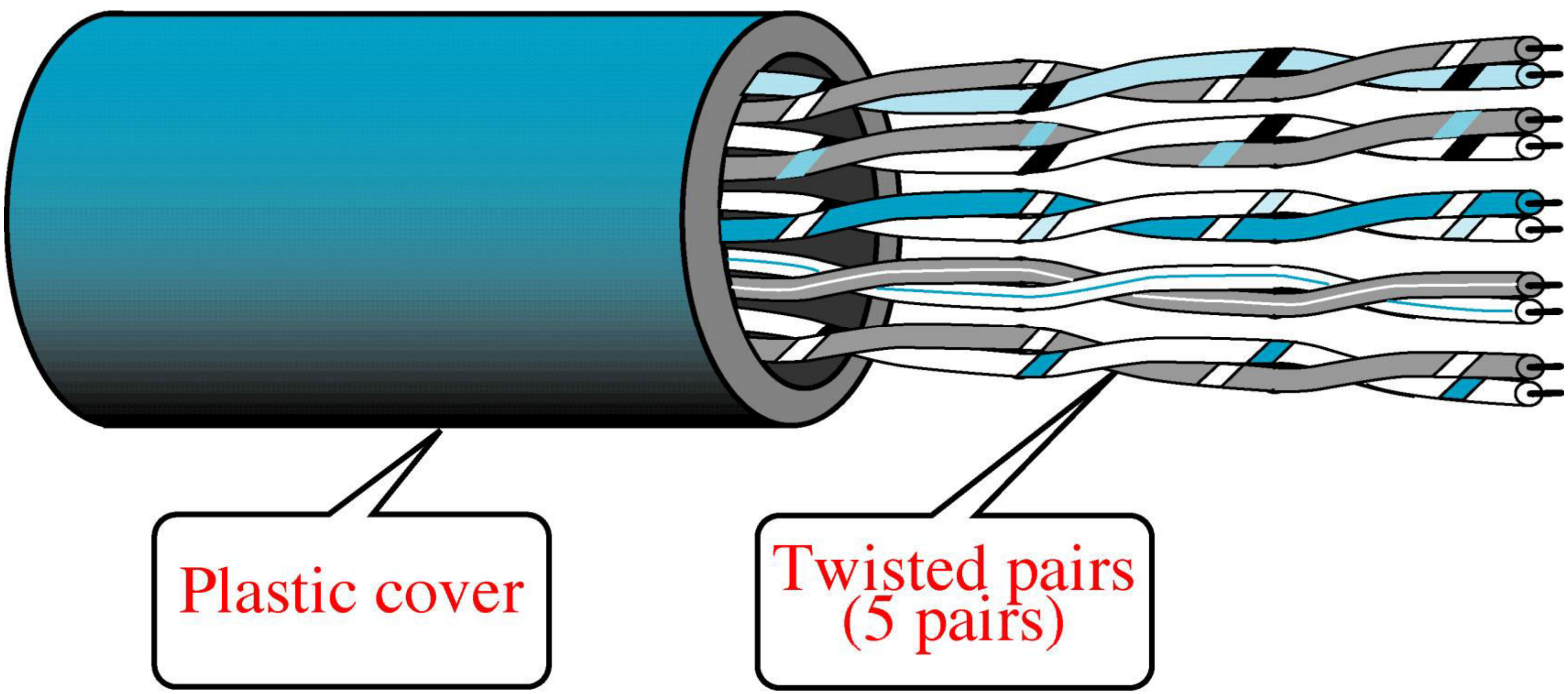
Effect of Noise on Parallel Lines



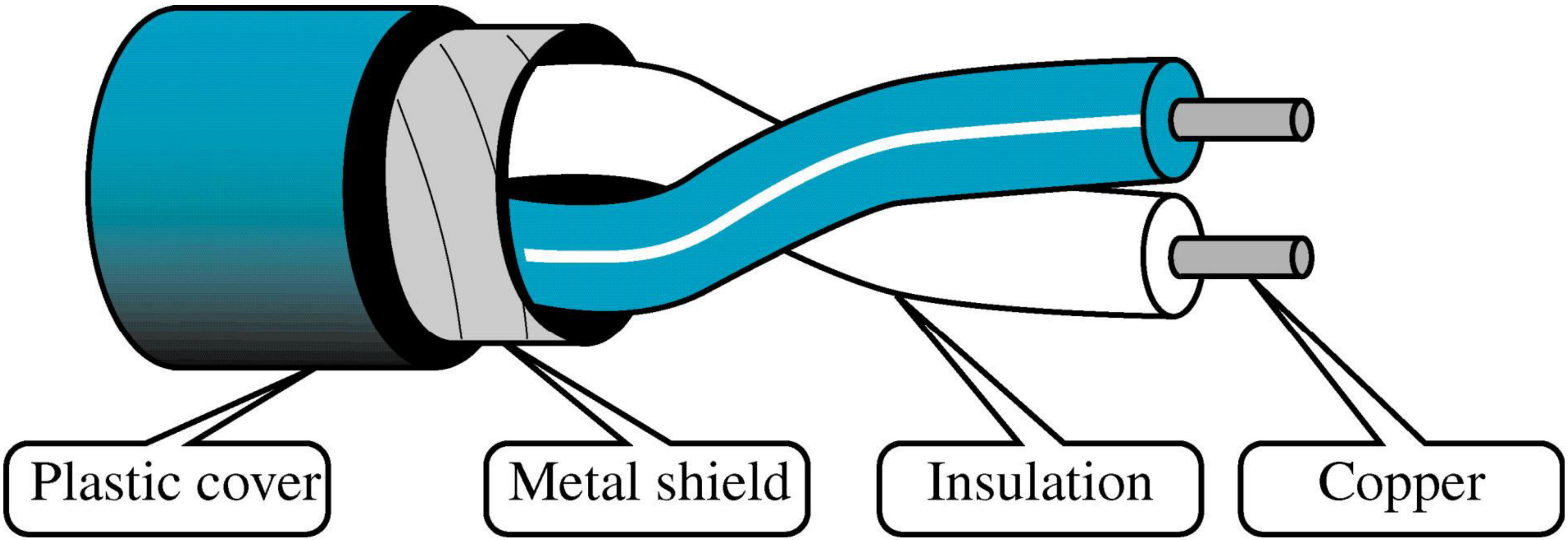
Noise on Twisted-Pair Lines



Unshielded Twisted-Pair Cable



Shielded Twisted-Pair Cable



Wired Transmission Media

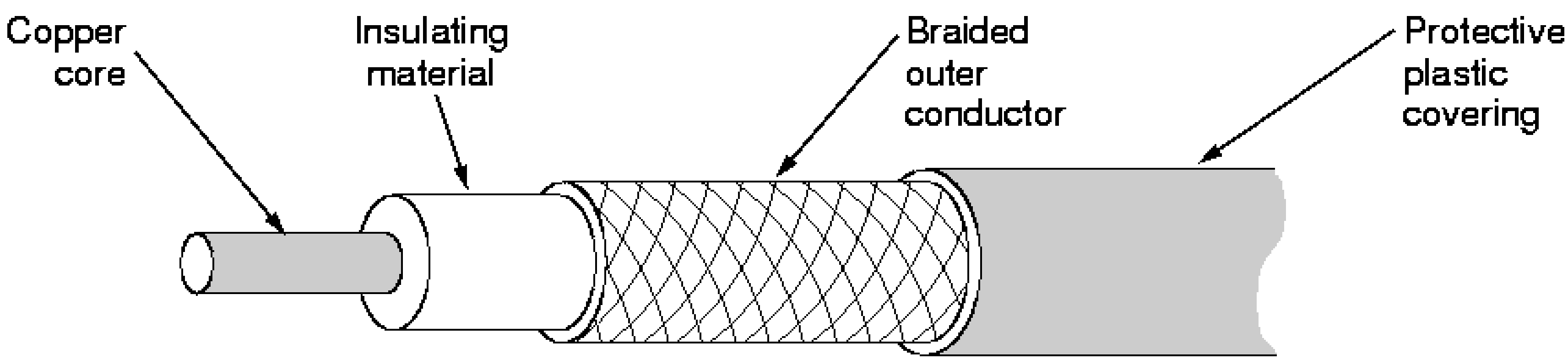
- <u>Coaxial Cable</u>
  - Most versatile medium

    => LANs, Cable TV, Long-distance telephones, VCR-to-TV connections
  - Noise immunity is good
  - Very high channel capacity

    => few 100 MHz / few 100 Mbps
  - Need repeater/amplifier every few kilometer or so (about the same as with twisted pair)
- Has an inner conductor surrounded by a braided mesh
- Both conductors share a common center axial, hence the term "co-axial"

Coaxial cable

- Signal and ground wire
  - Solid center conductor running coaxially inside a solid (usually braided) outer circular conductor.
  - Center conductor is shielded from external interference signals.



Properties of coaxial cable

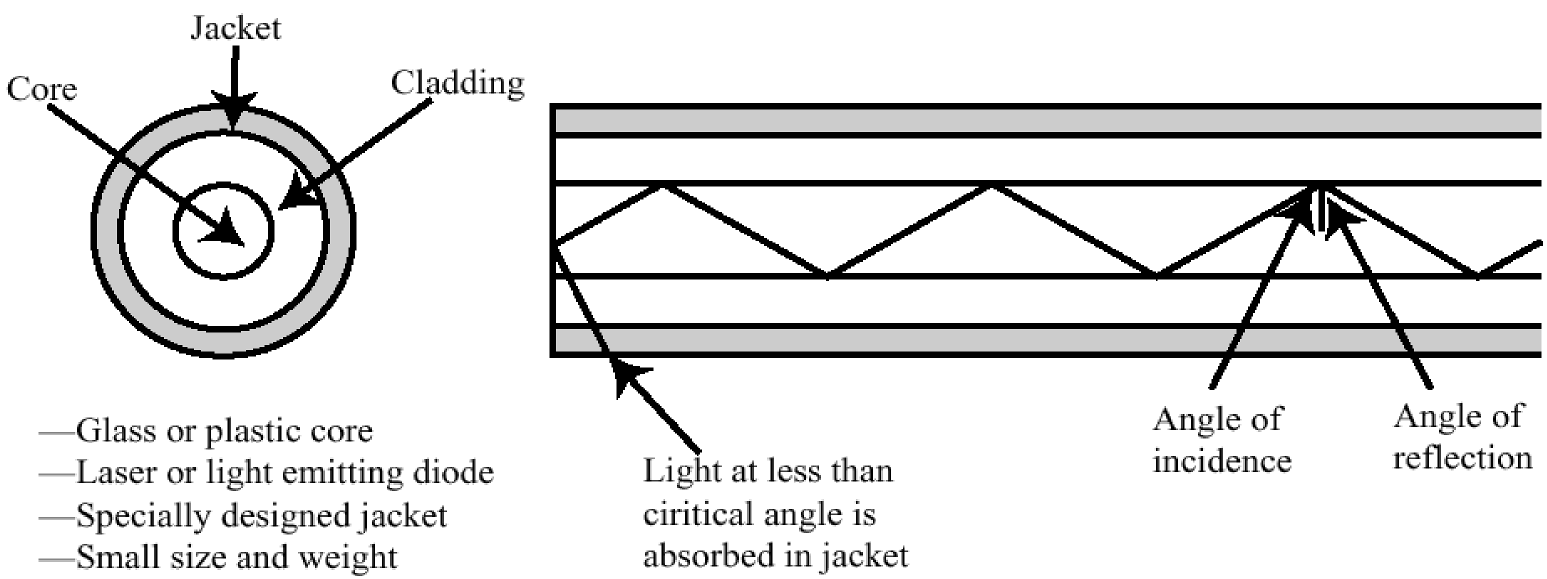
- Better shielding allows for longer cables and higher transfer rates.
- 100 m cables
  - 1 to 2 Gbps feasible (modulation used)
  - 10 Mbps typical
- Higher bandwidth
  - 400 to 600Mhz
  - up to 10,800 voice conversations
- Can be tapped easily: stations easily added (pros and cons)
- Much less susceptible to interference than twisted pair
- Used for long haul routes by Phone Co.
  - Mostly replaced now by optical fiber.
- High attenuation rate makes it expensive over long distance
- Bulky
- *Baseband* vs. *broadband* coax.

Wired Transmission Media

- <u>Optical Fiber</u>
  - Flexible, thin (few to few hundred μm), very pure glass/plastic fiber capable of conducting optical rays
  - Extremely high bandwidth : capable of ≥ 2 Gbps
  - Very high noise immunity, resistant to electromagnetic interference
  - Does not radiate energy/cause interference
  - Very light
  - Need repeaters only 10's or 100 km apart
  - Very difficult to tap : Better security but multipoint not easy
  - Require a light source with injection laser diode (ILD) or light-emitting diodes (LED)

Wired Transmission Media

- Optical Fiber (Cont'd)
  - Need optical-electrical interface (more expensive than electrical interface)

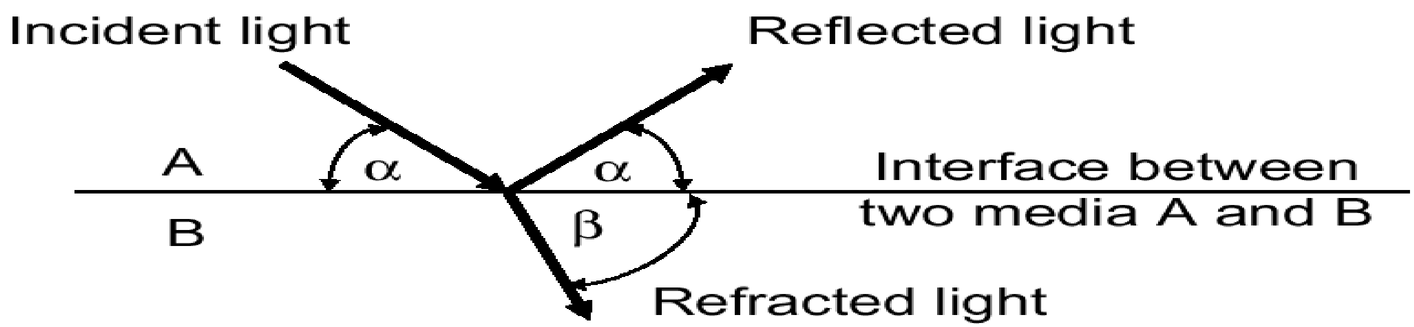


(c) Optical Fiber

Wired Transmission Media

Optical Fiber

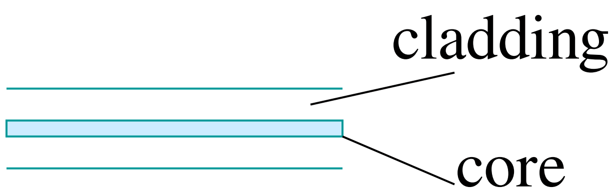
- Principle of optical fiber transmission: Based on the principle of total internal reflection



- If β>α, medium B (water) has a higher optical density than medium A (air)
- In case the index of refraction<1 (α>β), if α is less than a certain critical angle, there is no refracted light i.e., all the light is reflected. This is what makes fiber optics work.

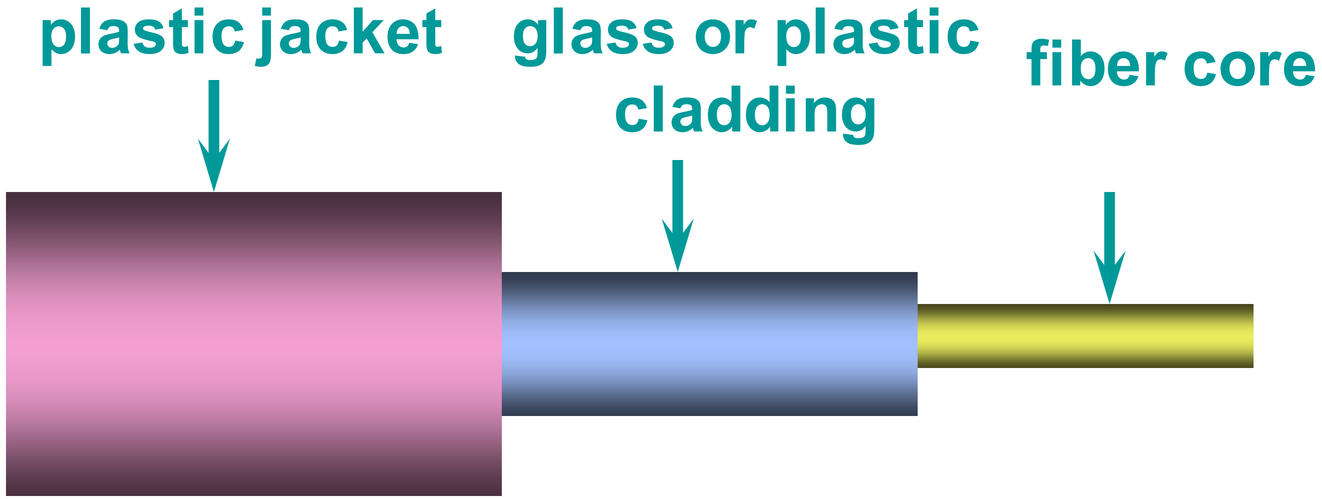
Fiber optics & Physics 101

- Refractive $\text{index}_{\text{material}}$ = (Speed of light in vacuum)/(Speed of light in material)
- Light is bent as it passes through a surface where the refractive index changes. This bending depends on the angle and refractive index. Frequency does not change, but because it slows down, the wave length gets shorter, causing wave to bend.
- In case of fiber optic media, refractive index of core > refractive index of cladding thereby causing internal reflection.



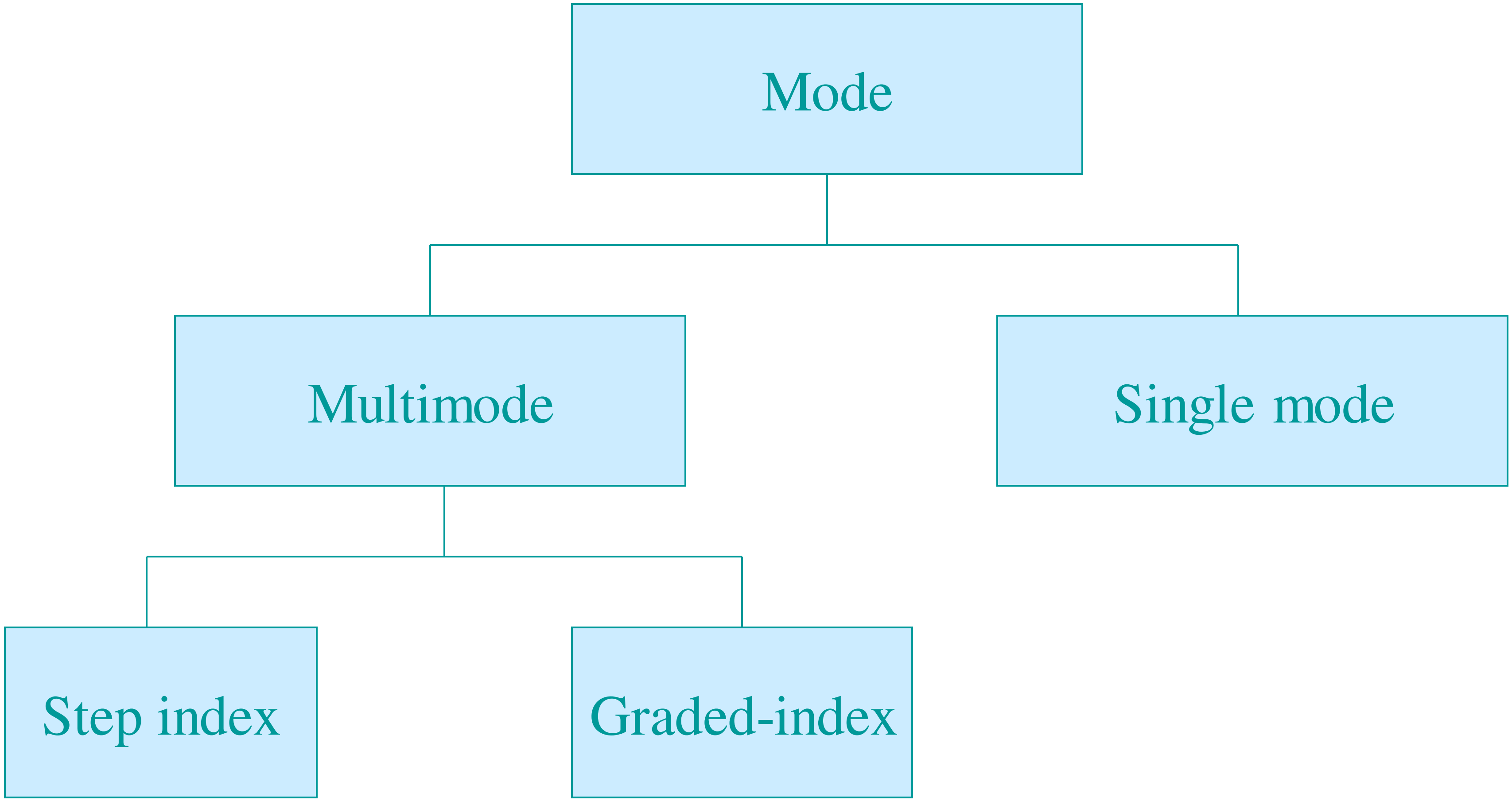
Fiber Optic Layers

- consists of three concentric sections



Modes of fiber

- Fiber consists of two parts: the *glass core* and *glass cladding* with a lower refractive index.
- Light propagates in 1 of 3 ways depending on the type and width of the core material.
  - **Multimode stepped index fiber**
    - Both core and cladding have different but uniform refractive index.
    - Relies on total internal reflection; Wide pulse width.
  - **Multimode graded index fiber**
    - Core has variable refractive index (light bends as it moves away from core).
    - Narrow pulse width resulting in higher bit rate.
  - **Singlemode fiber (> 100 Mbs)**
    - Width of core diameter equal to a single wavelenth.

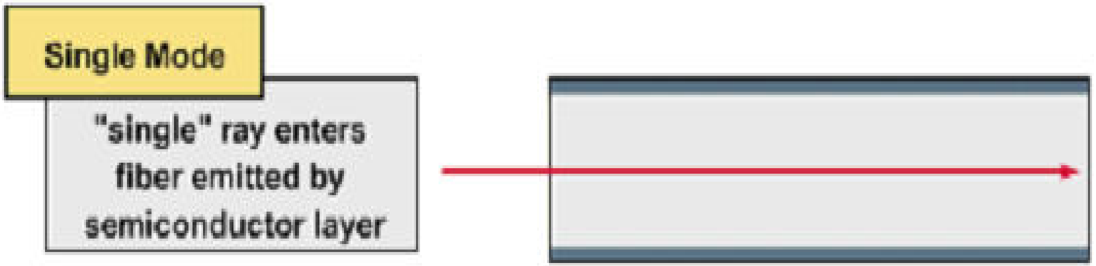

Mode
Multimode
Single mode
Step index
Graded-index

Fiber Optic Types

- multimode step-index fiber
  - the reflective walls of the fiber move the light pulses to the receiver
- multimode graded-index fiber
  - acts to refract the light toward the center of the fiber by variations in the density
- single mode fiber
  - the light is guided down the center of an extremely narrow core

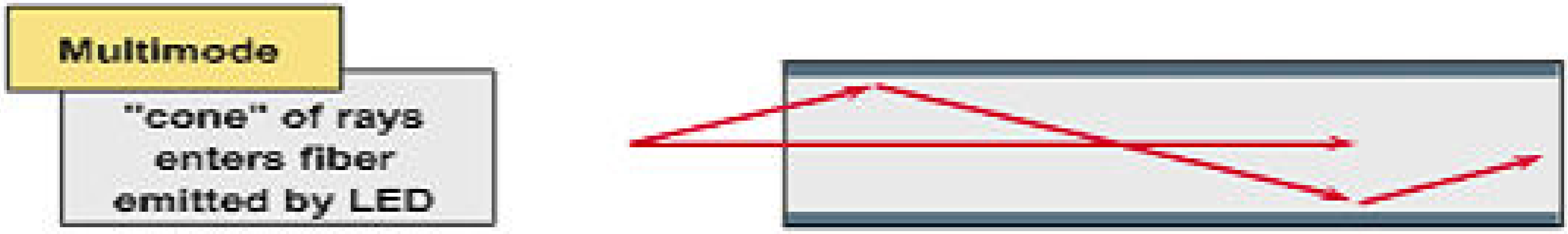
Types of optical fiber

- Modes, bundles of light rays enter the fiber at a particular angle
- Single-mode
  - Also known as mono-mode
  - Only one mode propagates through fiber
  - Higher bandwidth than multi-mode
  - Longer cable runs than multi-mode
  - Lasers generate light signals
  - Used for inter-building connectivity

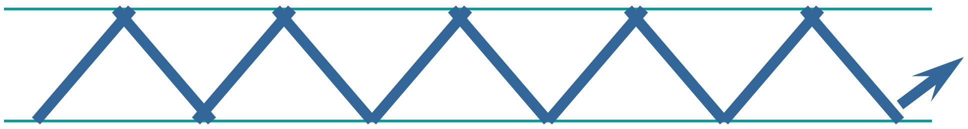


Types of optical fiber

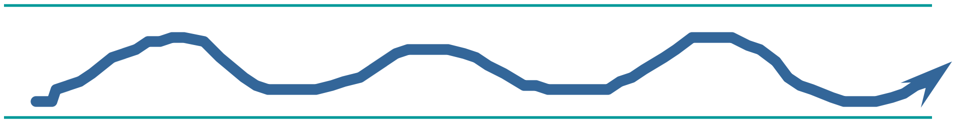
- Multi-mode
  - Multiple modes propagate through fiber
  - Different angles mean different distances to travel
    - Transmissions arrive at different times
    - Modal dispersion
  - LEDs as light source
  - Used for intra-building connectivity



Fiber Optic Signals



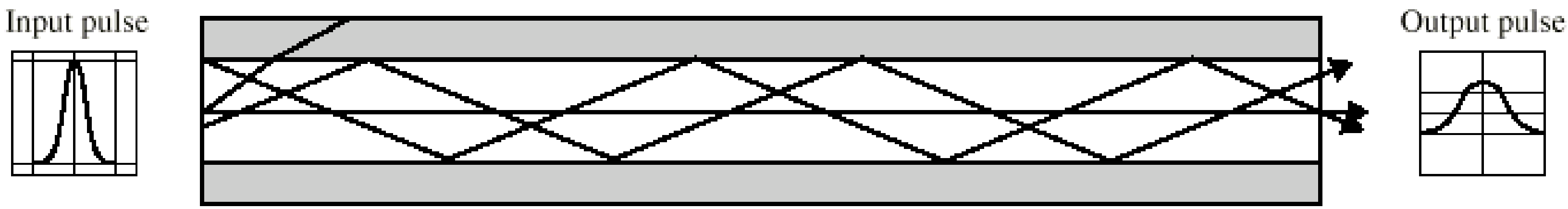
fiber optic multimode step-index



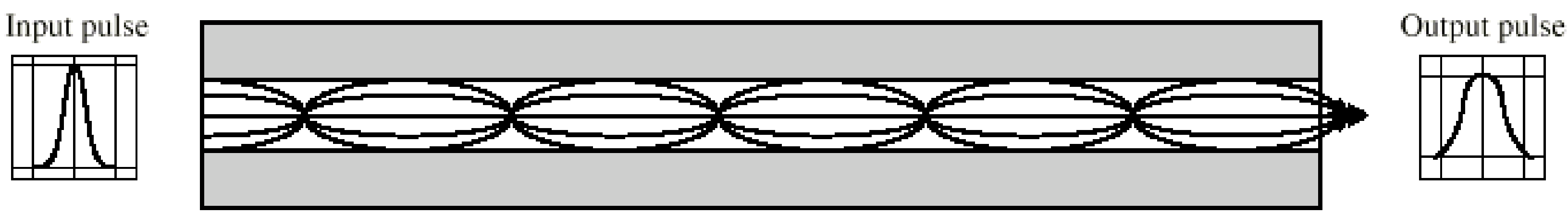
fiber optic multimode graded-index

fiber optic single mode

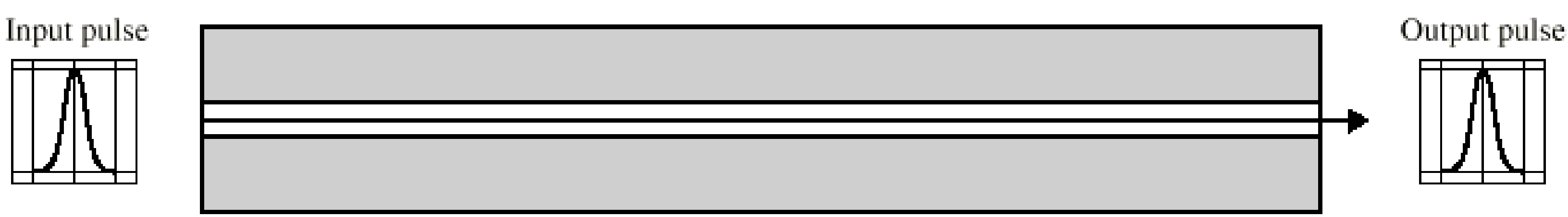
Optical Fiber Transmission Mode



(a) Step-index multimode



(b) Graded-index multimode



(c) Single mode

Fiber Optic

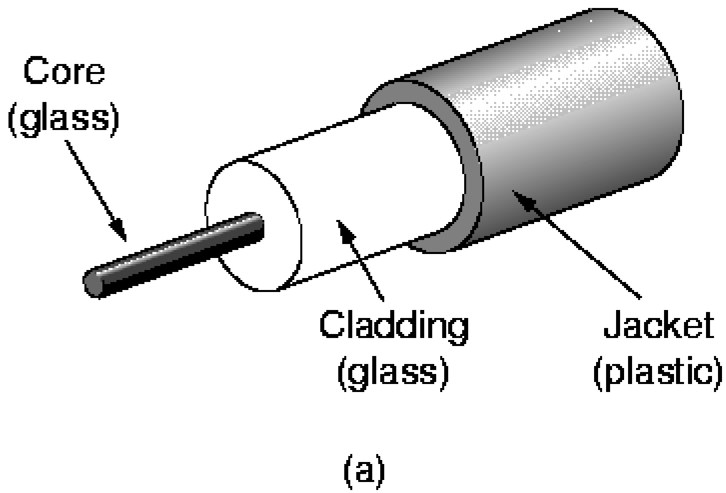
Advantages

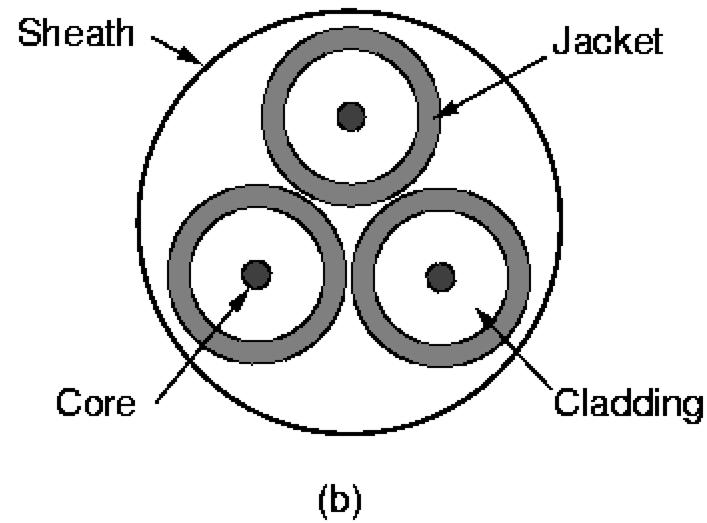
- greater capacity (bandwidth Gbps)
- smaller size and lighter weight
- lower attenuation
- immunity to environmental interference
- highly secure due to tap difficulty and lack of signal radiation

Disvantages

- expensive over short distance
- requires highly skilled installers
- adding additional nodes is difficult

Fiber cables





- Multimode: diameter of core is ~50 microns.
  - About the same as a human hair.
- Single mode: diameter of core 8-10 microns.
- They can be connnected by connectors, or by splicing, or by fusion.

Fiber vs. copper

- Fiber (pros)
  - Higher bandwidth,
  - Lower attenuation,
  - Immune to electromagnetic noise and corrosive chemicals,
  - Thin and lightweight,
  - Security (does not leak light, difficult to tap).
- Fiber (cons)
  - Not many skilled “fiber engineers,”
  - Inherently unidirectional,
  - Fiber interfaces are expensive.

Wireless (Unguided Media) Transmission

- transmission and reception are achieved by means of an antenna
- directional
  - transmitting antenna puts out focused beam
  - transmitter and receiver must be aligned
- omnidirectional
  - signal spreads out in all directions
  - can be received by many antennas

Physical media: radio

- signal carried in electromagnetic spectrum
- no physical “wire”
- bidirectional
- propagation environment effects:
  - reflection
  - obstruction by objects
  - interference

Radio link types:

- microwave
  - e.g. up to 45 Mbps channels
- LAN (e.g., waveLAN)
  - 2Mbps, 11Mbps, 54 Mbps
- wide-area (e.g., cellular)
  - e.g. CDPD, 10’s Kbps
- satellite
  - up to 50Mbps channel (or multiple smaller channels)
  - 270 msec end-end delay
  - geosynchronous versus LEOS

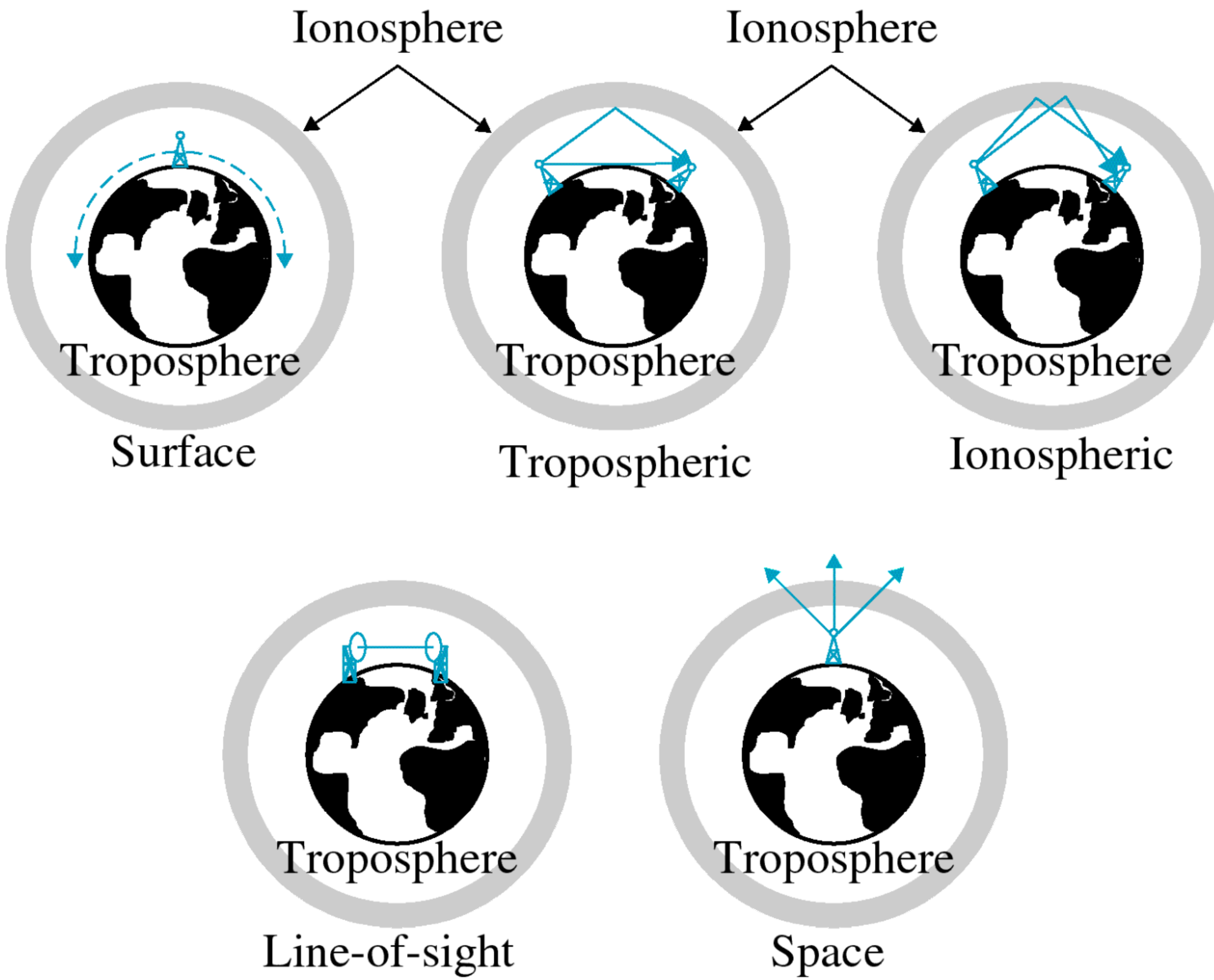
Infrared

- Transceivers must be within line of sight of each other (directly or via reflection)
- Unlike microwaves, infrared does not penetrate walls
- Fairly low bandwidth (4 Mbps).
- Uses wavelengths between microwave and visible light.
- Uses transmitters/receivers (transceivers) that modulate noncoherent infrared light.
- No frequency allocation issue since not regulated.
- Uses include local building connections, wireless LANs, and new wireless peripherals.

Radio Transmission

- Radio waves
  - Easy to generate, travel long distances, and penetrate buildings easily.
  - Omnidirectional.
  - Low frequencies
    - Pass through obstacles well,
    - Quick power drop off (e.g. 1/r3 in air).
  - High frequencies
    - Travel in straight lines and bounce off obstacles.
    - Absorbed by rain.
  - Subject to electrical interference

Propagation Types



Encoding

- Goal: Send bits from one node to another node on the ***same*** physical media
- Problem: Specify a *robust* and *efficient* encoding scheme to achieve this goal

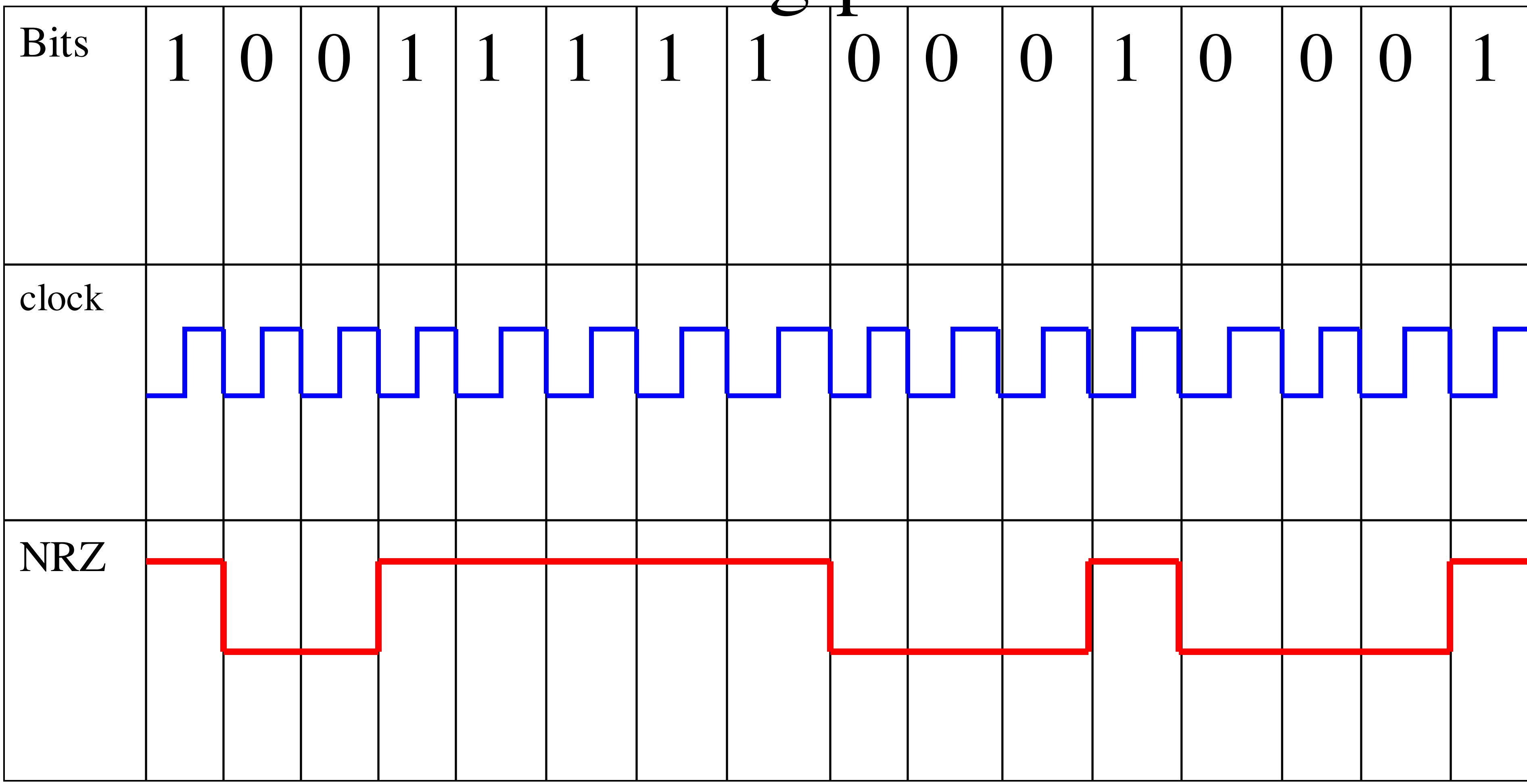
Encoding Schemes

- Non Return to Zero (NRZ)
- Non Return to Zero Inverted (NRZI)
- Manchester Encoding
- 4B/5B Encoding

Modulation

- Non-Return to Zero (NRZ)
  - Used by Synchronous Optical Network (SONET)
  - 1=high signal, 0=low signal
  - Long sequence of same bit cause difficulty
    - DC bias hard to detect – low and high detected by difference from average voltage
    - Clock recovery difficult

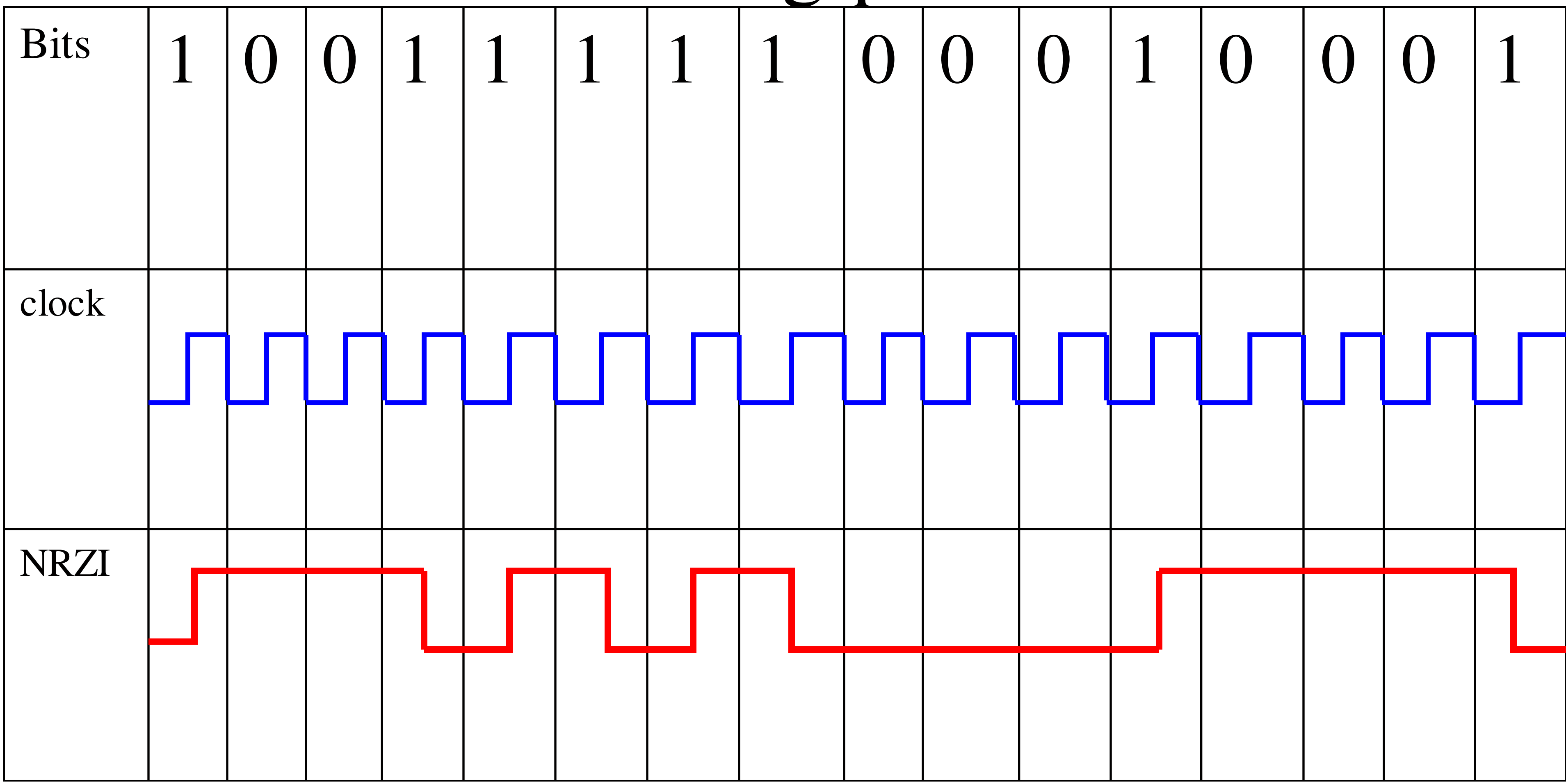
Show the NRZ encoding for the following pattern



Modulation

- Non-Return to Zero Inverted (NRZI)
  - 1=inversion of current value, 0=same value
  - No problem with string of 1’s
  - NRZ-like problem with string of 0’s

Show the NRZI encoding for the following pattern



Modulation

- Manchester
  - Used by ***Ethernet***
  - 1=low to high transition, 0=high to low transition
  - Transition for every bit simplifies clock recovery
  - Not very efficient
    - Doubles the number of transitions
    - Circuitry must run twice as fast

Chapter Summary

- Information can be transmitted via analog or digitally
- Both signals suffer attenuation
- Throughput is the amount of data a medium can transmit during a given period of time
- Costs depend on many factors
- Three specifications dictating networking media
- Length of a network segment is limited due to attenuation
- Connectors connect wire to the network device
- Coaxial cable consists of central copper core surrounded by an insulator and a sheath
- In baseband transmission, digital signals are sent through direct current pulse applied to the wire

Chapter Summary

- Twisted-pair cable consists of color-coded pairs of insulated copper wires, twisted around each other and encased in plastic coating
- The more twists per inch in a pair of wires, the more resistant to noise
- STP cable consists of twisted pair wires individually insulated and surrounded by a shielding
- UTP cabling consists of one or more insulated wire pairs encased in a plastic sheath
- UTP comes in a variety of specifications
- Fiber-optic cable contains one or several glass fibers in its core
- On today’s networks, fiber is used primarily as backbone cable

Chapter Summary

- Best practice for installing cable is to follow the TIA/EIA 568 (see "structured cabling") specifications and manufacturer's recommendations
- Wireless LANs can use radio frequency (RF) or infrared transmission
- Infrared transmission can be indirect or direct
- RF transmission can be narrowband or spread spectrum
- To make correct media transmission choices, consider, throughput, cabling, noise resistance, security/flexibility, and plans for growth

COMPUTER NETWORKS (BCSC 0008)

SWITCHING TECHNIQUES

Text and Reference Books

Text Books:

1. Fourouzan B. A. (2004), “Data Communication and Networking”, 4th Edition, McGraw-Hill.

References:

1. Kurose, J. F. and Ross K. W. (2005), “Computer Networking: A Top-Down Approach Featuring the Internet”, 3rd Edition, Addison-Wesley.
2. A. S. Tanenbaum (2006), “Computer Networks”, 2nd Edition, Prentice Hall India.

Previous discussed topics:

1. **<u>OSI Model</u>**
2. **<u>TCP/IP Model</u>**
3. **<u>Addressing</u>**
4. **<u>Data & Signals</u>**
5. **<u>Transmission Media & Line Encoding</u>**

Now we will discuss:

1. **<u>Concept of Switch</u>**
2. **<u>Circuit, Packet and Message Switching Techniques</u>**

Q:A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. List Possible solutions.

Sol:1-One solution is to make a point-to-point connection between each pair of devices (a mesh topology).

Sol:2-Point-to-point connection between a central device and every other device (a star topology).

Issues with these methods:

- These methods, however, are impractical and wasteful when applied to very large networks.
- The number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time

Sol:3-Other topologies employing multipoint connections, such as a bus

Issues with these methods:

the distances between devices and the total number of devices increase beyond the capacities of the media and equipment

Optimal Solution

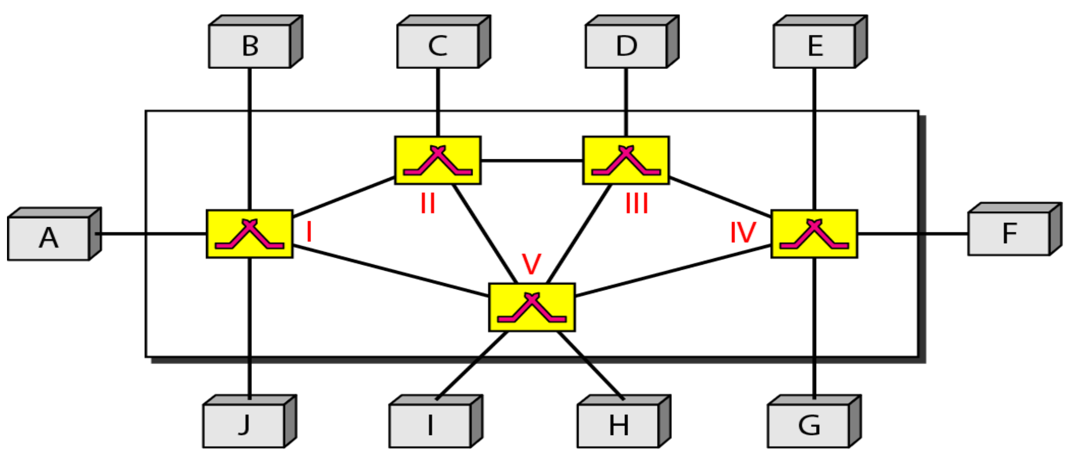
Switching.

SWITCH

- We use switches in circuit-switched and packet-switched networks.
- A **switch** is a **device** in a computer network that connects other **devices** together. Multiple data cables are plugged into a **switch** to enable communication between different networked **devices.**
- A **switch** is a device that is used at the Access or OSI Layer 2; a **switch** can be used to connect multiple hosts (PCs) to the network.

Switching Technique

- How 2 devices communicate when there are many devices?
- **One alternative** is to establish Point to Point connection between each pair of devices using mesh topology (which is highly complex)
- **The other alternative** is to use switching techniques leading to switched connection network.



Switched network

Switching Technique – Beyond Simple Topology

Important Points:

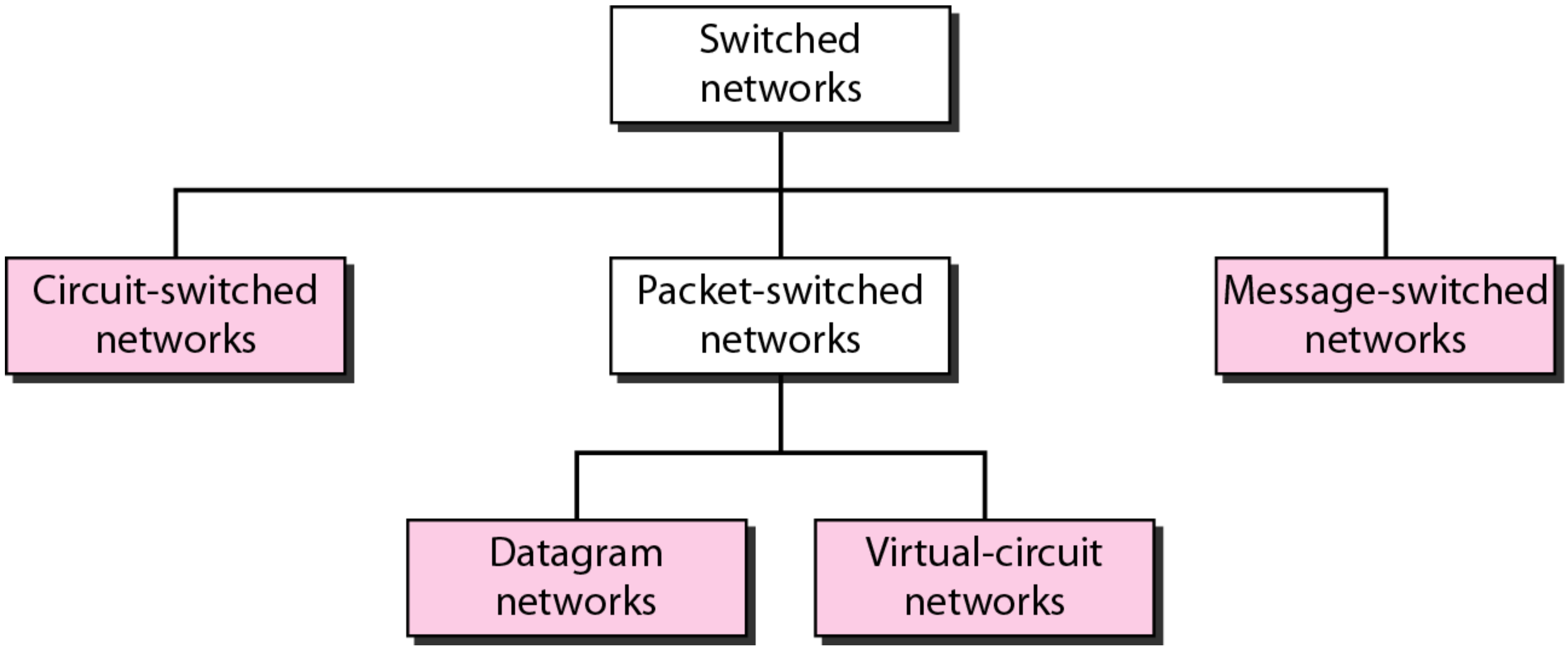
1. The end devices that wish to communicate are called **stations**.
2. The switching devices are called as **nodes**.
3. Some node connects to other nodes and other nodes are attached to stations.
4. There exist **multiple paths** between source to destination pair for better network reliability.
5. Switching nodes have **no concerned with content of data** and hence **provides routing facility** that will move data from node to node until they reach destination.

Switching Technique – Beyond Simple Topology

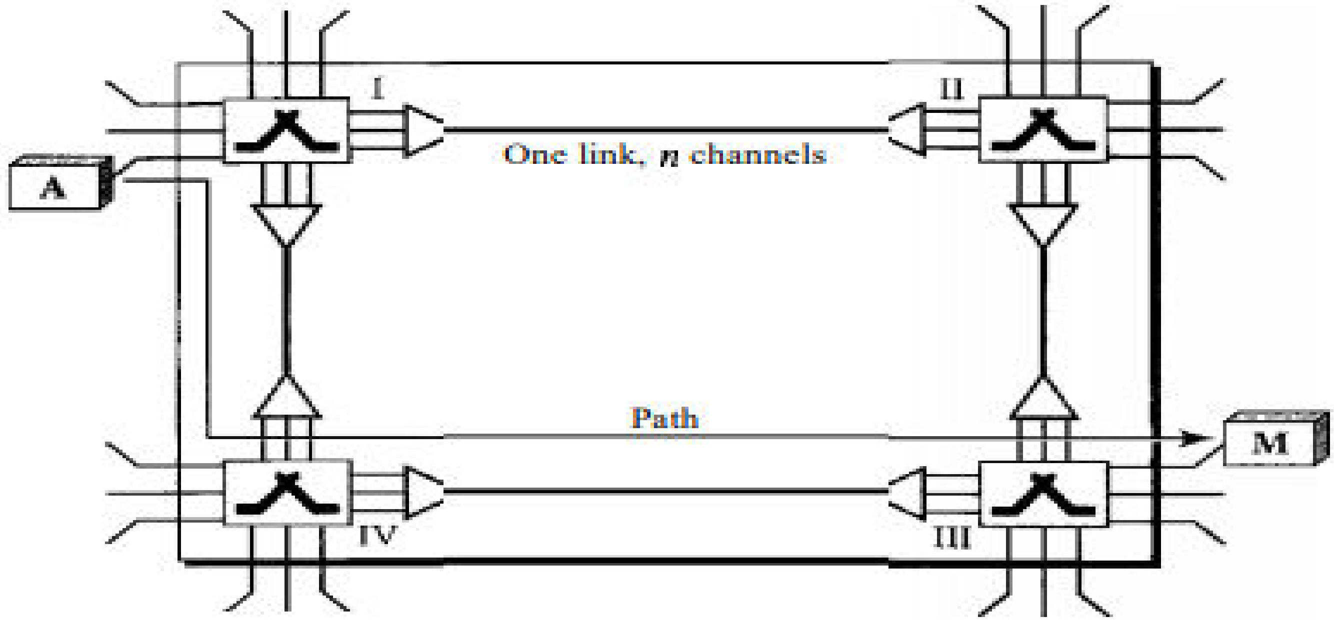
There are three typical switching techniques available for digital traffic.

- ❖ **Circuit Switching (on physical layer)**
- ❖ **Message Switching (on network layer)**
- ❖ **Packet Switching**

Taxonomy of switched networks



Basics of Circuit Switching

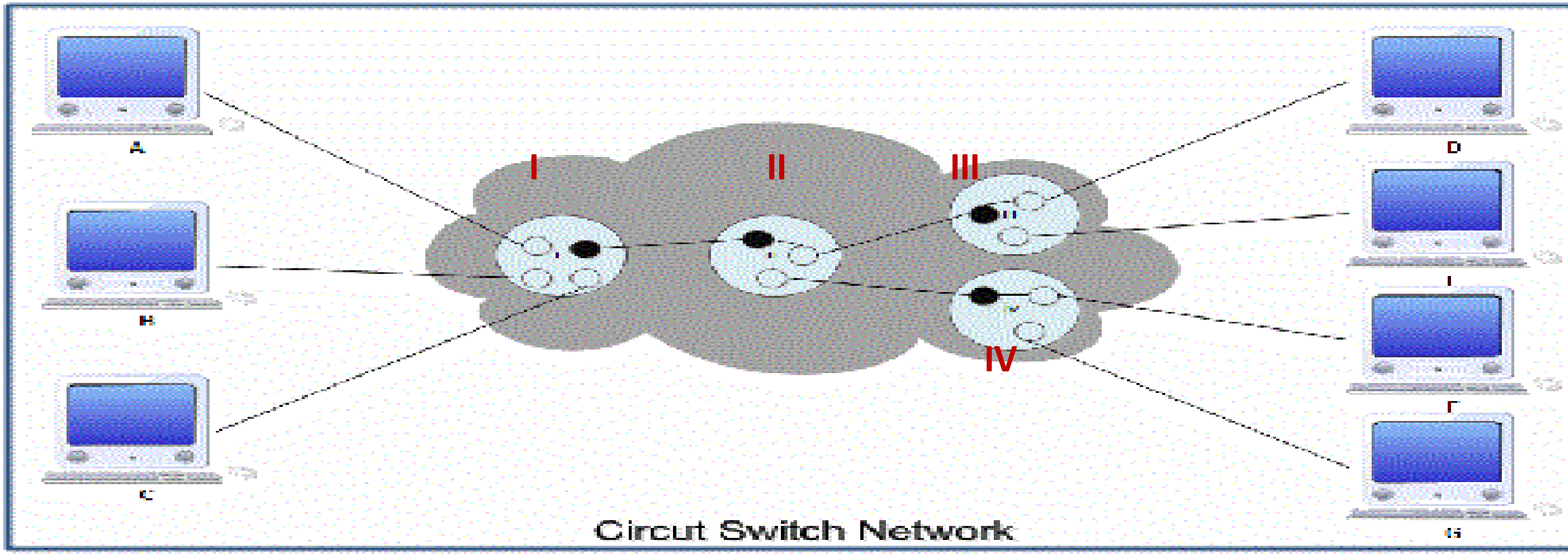


- The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity.
- When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself.
- **This is called the setup phase;** a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path.
- After the dedicated path made of connected circuits (channels) is established, **data transfer can take place.** After all data have been transferred, **the circuits are set down**

CIRCUIT-SWITCHED NETWORKS

- A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM.

- **Circuit switching was designed in 1878 in order to send telephone calls through a dedicated channel.**
- **This channel remains open and in use throughout the whole call and cannot be used by any other data or phone calls.**



- ❖ It is the simplest method of data communication in which a dedicated physical connection or path is established between the sending and receiving device.

- ❖ In circuit switched networks, a set of switches are connected by physical links. A connection between two stations is a dedicated path made of one or more links.

- ❖ Figure shows a circuit switched network in which computer A, B and C are connected to computer D, E, F and G via four switches. If these computers are to be connected with a point-to-point connections, 12 dedicated lines are required which will incur high line cost.

- The four switches connecting these computers thus provide dedicated links by reducing the line cost. Here I, II, III and IV are the circuit switches or nodes. Nodes I, III, IV are connected to computers while II is only routing node.

- In circuit switching the routing decision is made when path is set up across the network. After the link has been set between the sender and receiver, the information is forwarded continuously over the link.

- The dedicated path established between the sender and the receiver is maintained for entire duration of conversation.

- This link or path is released only when data transmission between sender and receiver is over.

- Circuit switching takes place at the physical layer.

- Before starting communication, the stations must make a reservation of resources to be used during the communication. These resources can be switch buffers, switch processing time, switch input/output ports.

- These resources remain dedicated during the entire duration of data transfer.

- **Data transferred** between the two stations are **not packetized** (*i.e.* in form of packets).

- The data are a continuous flow· sent by the source station and received by the destination station and there may be periods of silence.

- There is **no addressing involved** in data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). However, there is end-to-end addressing used during set up phase.

- In telephone systems circuit switching is used.

- The communication in a circuit switched network takes place in three phases:

- A.Circuit establishment or setup phase.
- B.Data transfer phase.
- C.Circuit disconnects or tears down phase.

Circuit establishment or setup phase.

- In circuit switched network, before actual data transfer takes place, a dedicated circuit or path is established between the sender and receiver.

- **For example**, if station A is willing to send a message to station C, it first sends a message to node 2, requesting a connection to station C, using the dedicated link between station A and node 2.
- Node 2 must find the next link in a route, leading to node 4. Based on routing information and availability, node 2 selects the circuit to node 5 and sends a message, requesting connection to station C.

- So far, a dedicated path has been established from station A through node 2 to node 5. Node 5 now gets a channel to node 4 and internally connects it to the previously established path.

- Node 4 completes the connection to station C. After completing the connection, a test is made to check whether station C is busy to accept the connection or not. That completes the circuit establishment phase.

Data transfer phase.

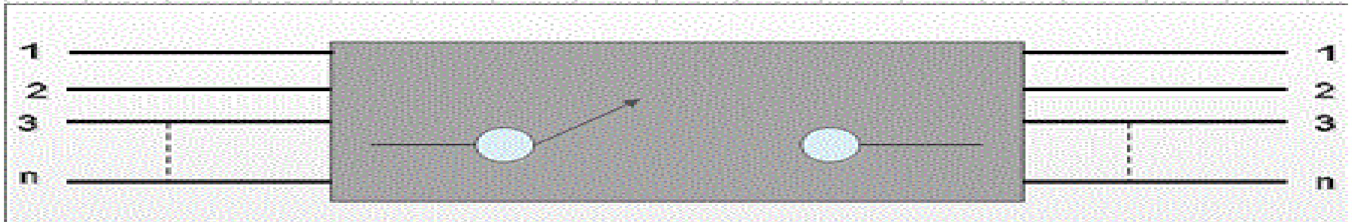
- Actual data transfer between the source and destination takes place after the dedicated path is set up between them.

- The data flows are continuous between sender and receiver.

- There may be periods of silence in between. Generally all the internal connections are duplex.

Circuit disconnects or tears down phase.

- After the completion of data transfer, the established connection is terminated, and notification signal is propagated to all the nodes in the established path to release the dedicated resources.
- Circuit switching can be an inefficient technique if the channel capacity is not used properly.
- However, once the connection is established, data can be transmitted at full speed, supported by the channel.
- This makes the complete utilization of the channel capacity.



A circuit switch

Advantages of Circuit Switching

- The advantages of circuit switching are:

- The dedicated path/circuit established between sender and receiver provides a guaranteed data rate.

- Once the circuit is established, data is transmitted without any delay as there is no waiting time at each switch.

- Since a dedicated continuous transmission path is established, the method is suitable for long continuous transmission.

- **Disadvantages of Circuit Switching**
- The various disadvantages of circuit switching are:

- As the connection is dedicated it cannot be used to transmit any other data even if the channel is free.

- It is inefficient in terms of utilization of system resources.

- As resources are allocated for the entire duration of connection, these are not available to other connections.

- Dedicated channels require more bandwidth.

- Prior to actual data transfer, the time required to establish a physical link between the two stations is too long.

Note

In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until the teardown phase.

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into *n* channels.

Switching at the physical layer in the traditional telephone network uses the circuit-switching approach.

Packet Switched Networks

- In **packet switched** data networks all data to be transmitted is first assembled into one or more message units, called packets.

- Packet switching is a connectionless network switching technique.

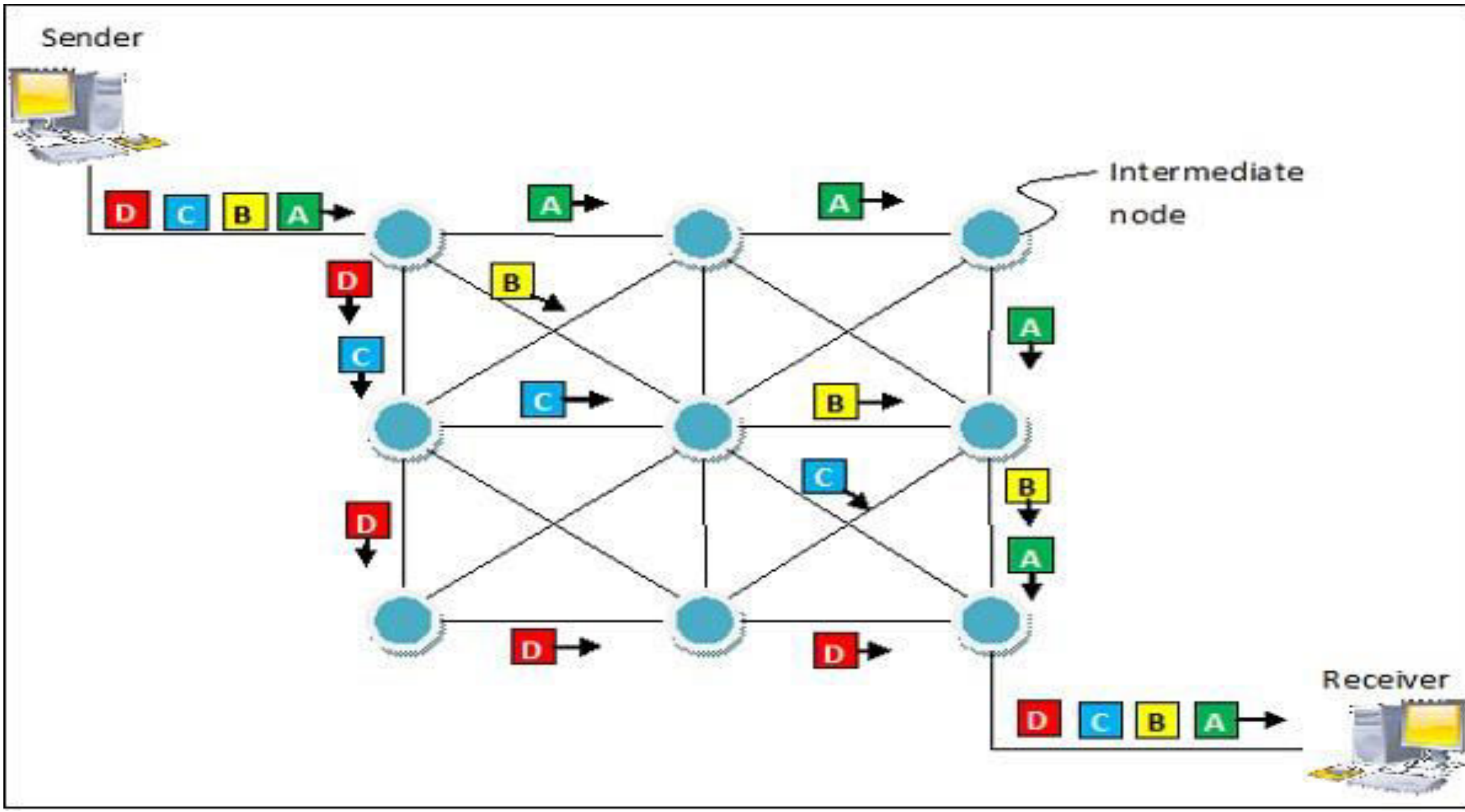
- Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination.

- There is no need to establish a dedicated circuit for communication.

Process

- ❖ Each packet in a packet switching technique has two parts: a header and a payload.
- ❖ The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination.
- ❖ The payload carries the actual data.
- ❖ A packet is transmitted as soon as it is available in a node, based upon its header information.
- ❖ The packets of a message are not routed via the same path. So, the packets in the message arrives in the destination out of order.
- ❖ It is the responsibility of the destination to reorde the packets in order to retrieve the original message.

The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver.



Advantages

- ❖ Delay in delivery of packets is less, since packets are sent as soon as they are available.
- ❖ Switching devices don't require massive storage, since they don't have to store the entire messages before forwarding them to the next node.
- ❖ Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via other paths.
- ❖ It allows simultaneous usage of the same channel by multiple users.
- ❖ It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

Disadvantages

- Packet switching high installation costs.
- They require complex protocols for delivery.
- Network problems may introduce errors in packets, delay in delivery of packets or loss of packets.
- If not properly handled, this may lead to loss of critical information.

DATAGRAM NETWORKS
An Approach of Packet Switching

- In data communications, we need to send messages from one end system to another.

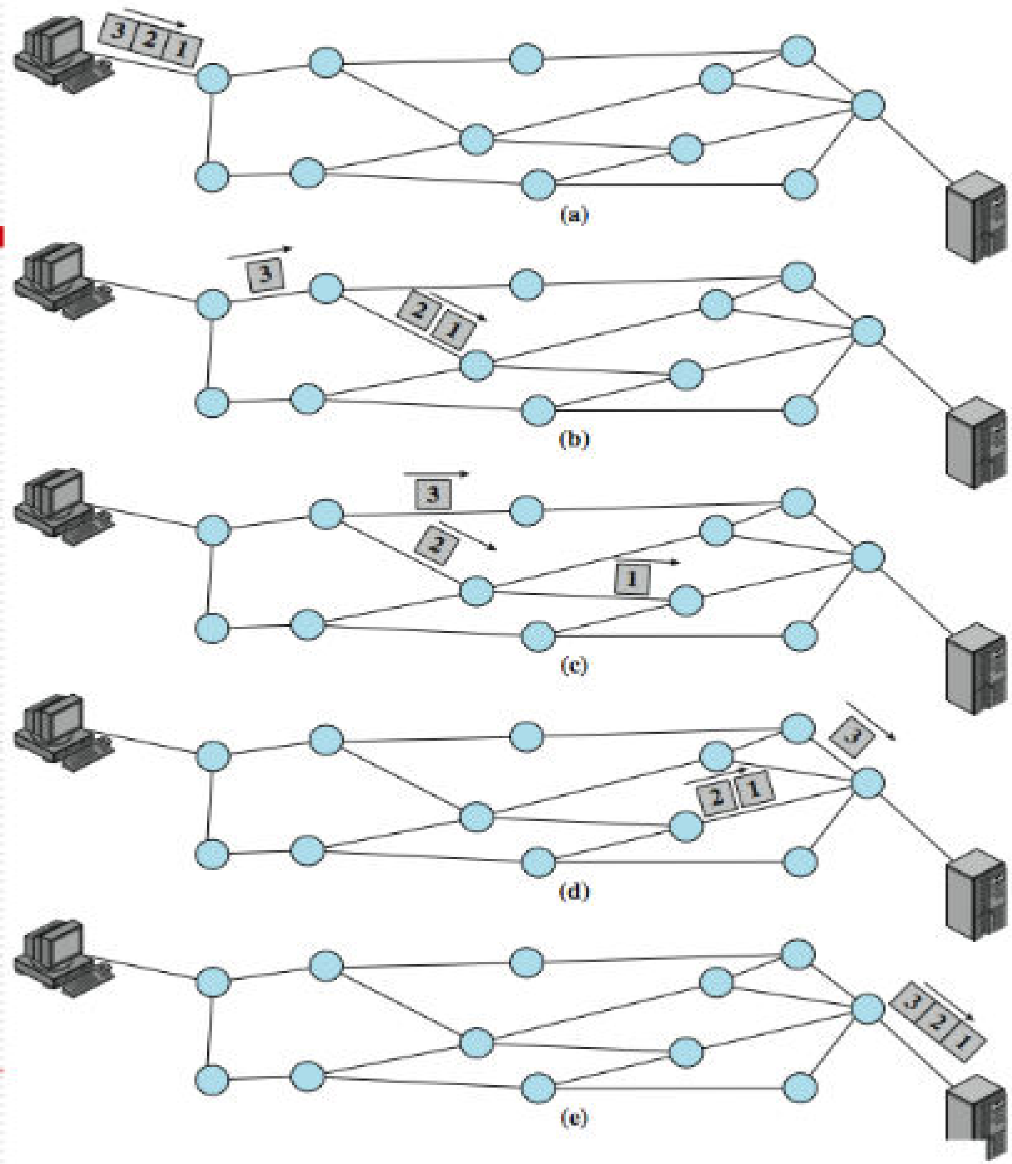
- If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size.

- The size of the packet is determined by the network and the governing protocol.

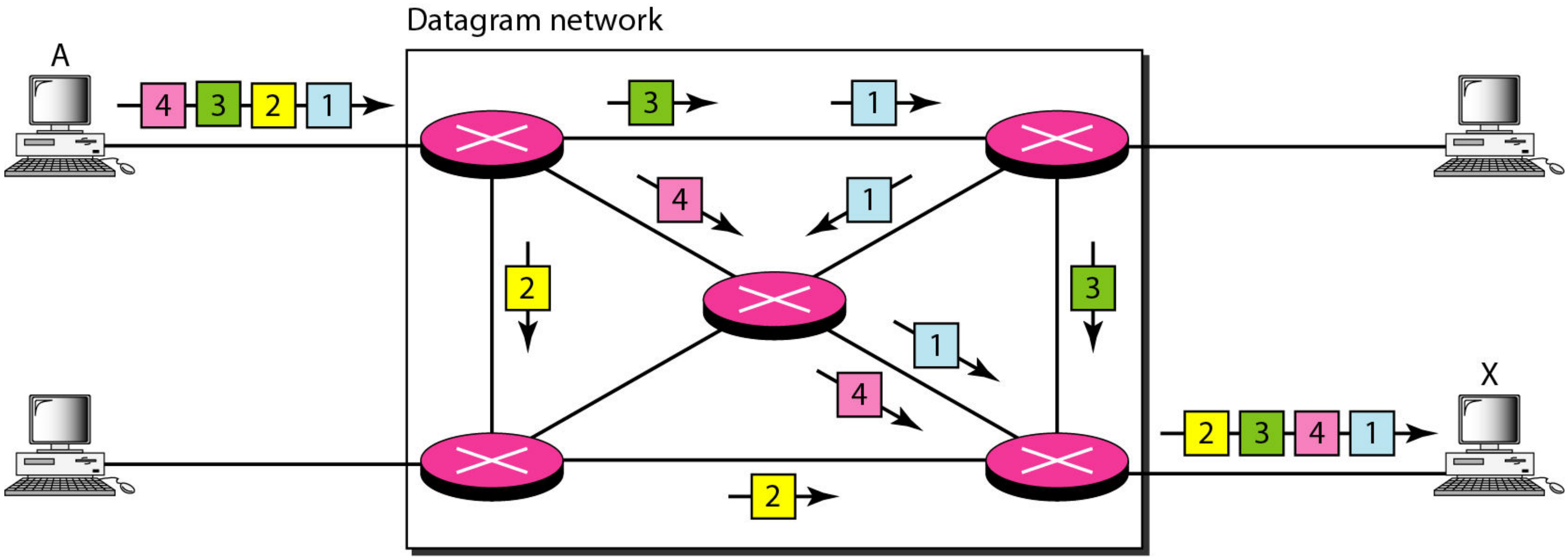
Packet Switching Datagram Approach –Connectionless

Datagram Diagram

- No pre-planned route → fast (no circuit)
- Each packet can pass through a separate path
- Reassembly is required
- Packets may experience jitter (delay variation)
- Network can provide error control
- More flexible (more primitive)
- More reliable (if a node fails circuit fails)

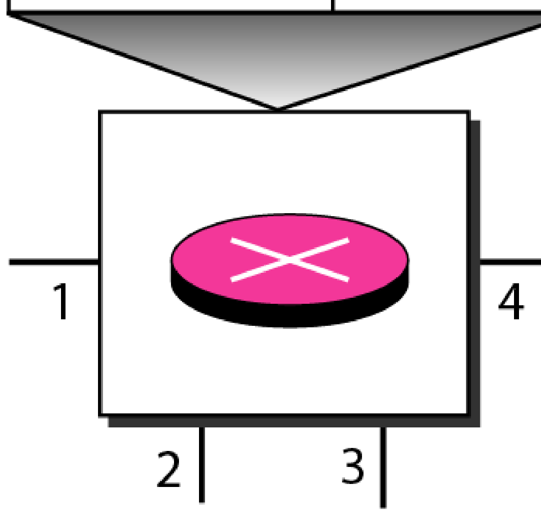


A datagram network



Routing table in a datagram network

Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3



Note

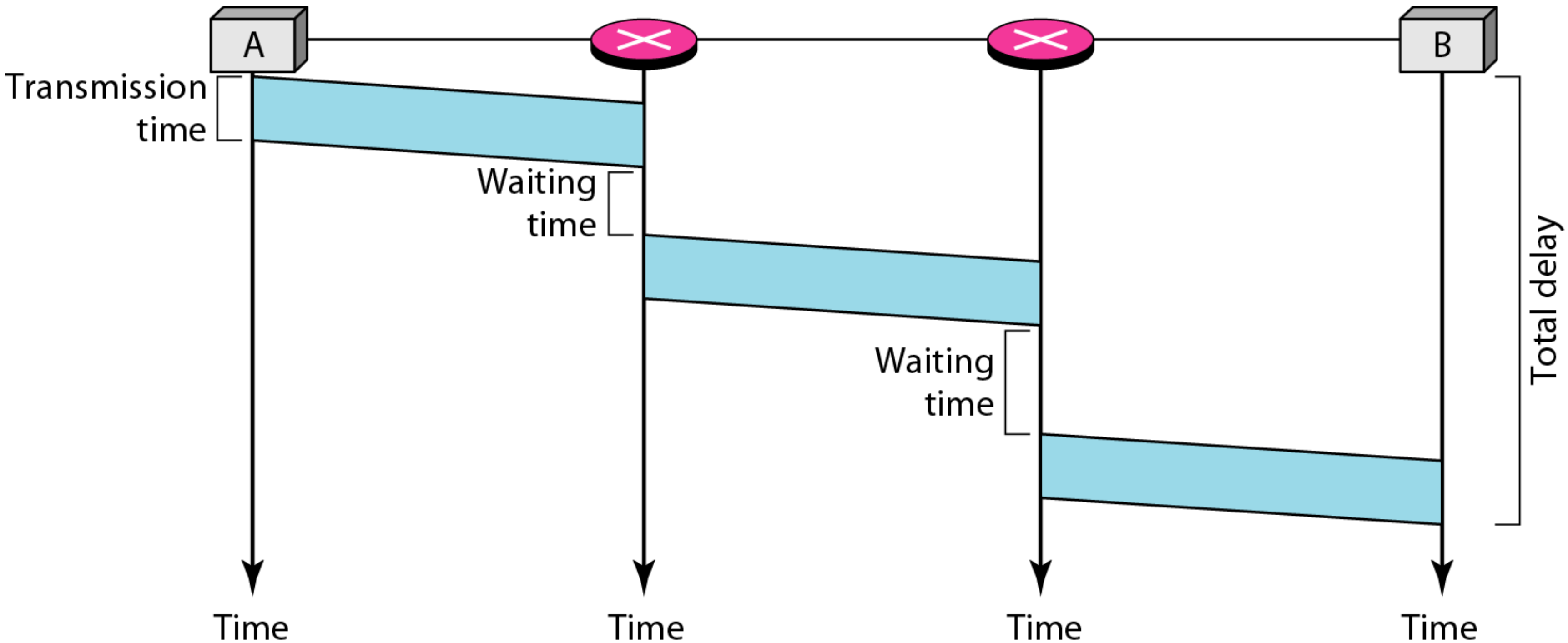
In a packet-switched network, there is no resource reservation; resources are allocated on demand.

A switch in a datagram network uses a routing table that is based on the destination address.

The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.

Switching in the Internet is done by using the datagram approach to packet switching at the network layer.

Delay in a datagram network

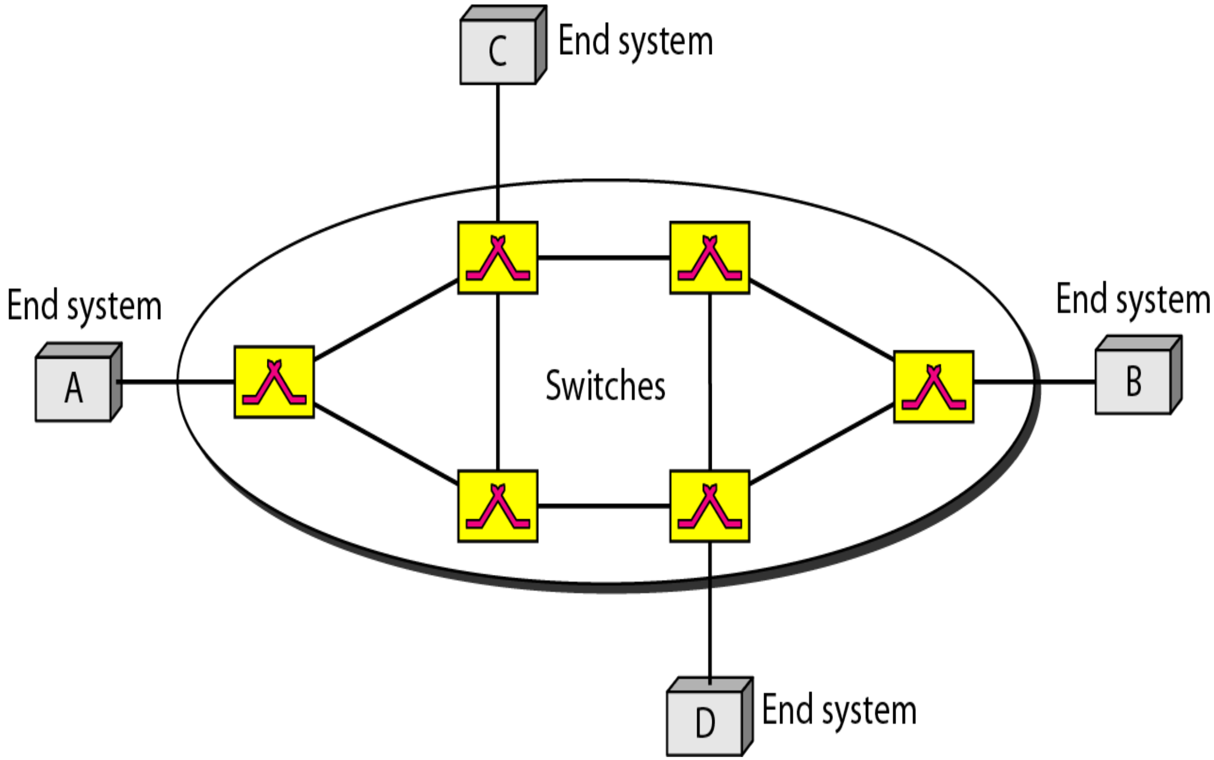


The packet travels through two switches. There are three transmission times ($3T$), three propagation delays (slopes 3τ of the lines), and two waiting times ($w_1 + w_2$). We ignore the processing time in each switch. The total delay is

$$\text{Total delay} = 3T + 3\tau + w_1 + w_2$$

VIRTUAL CIRCUIT-SWITCHED NETWORKS
(An Approach of Packet Switching)

- A virtual-circuit network is a cross between a circuit-switched network and a datagram network.
- It has some characteristics of both.
- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
- However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being carried), not end-to-end jurisdiction
- As in a circuit-switched network, all packets follow the same path established during the connection.
- A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.



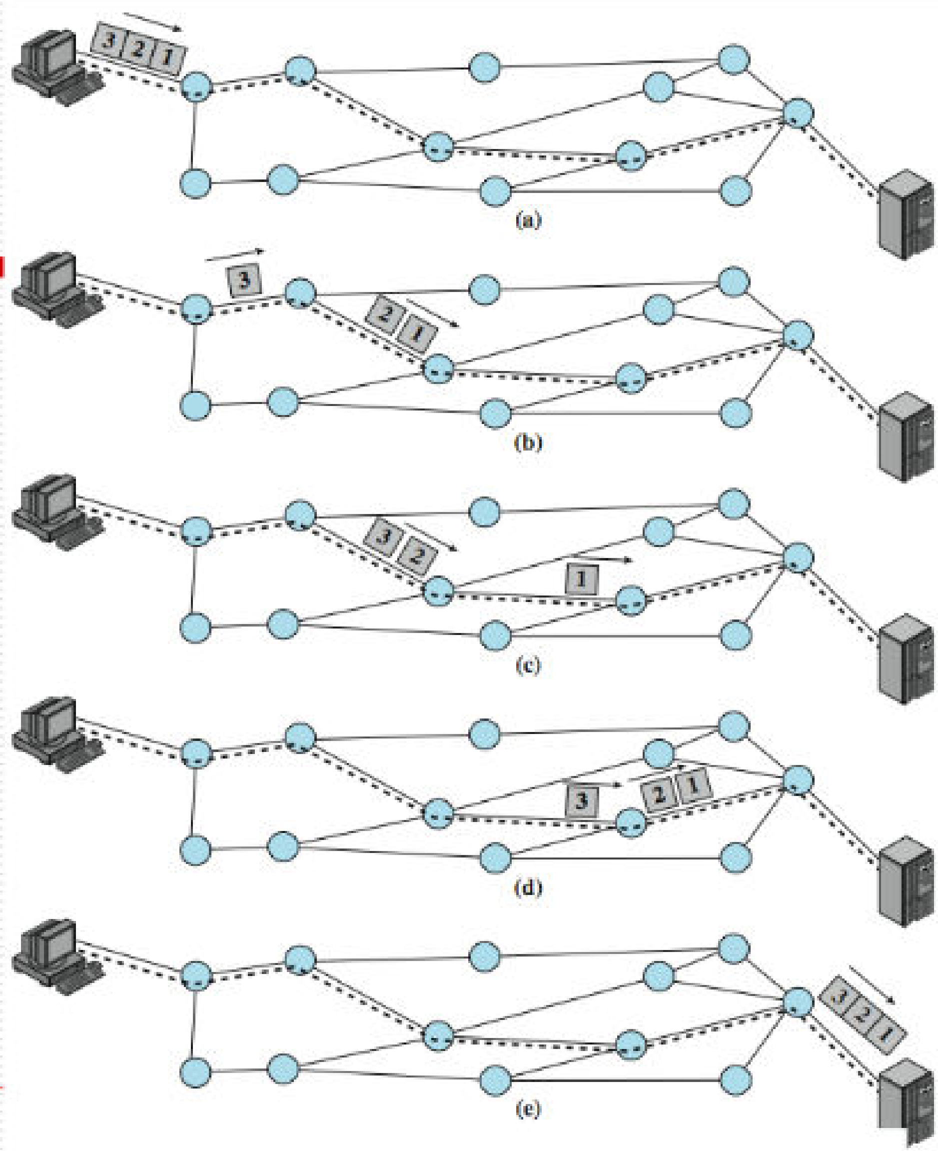
VIRTUAL CIRCUIT-SWITCHED

Packet Switching Virtual Circuit Approach

Connection Oriented

Virtual Circuit Diagram

- call setup phase is required
- Fixed route (circuit switching)
- Each packet has VC ID
- No routing decisions at the intermediate nodes --> fast delivery



Packet Switching
Virtual Circuit Approach
How it is implemented ?

Addressing: In a virtual-circuit network, two types of addressing are involved:

- Global
- Local (VCI)

Global Addressing: A source or a destination IP address is considered to be global address.

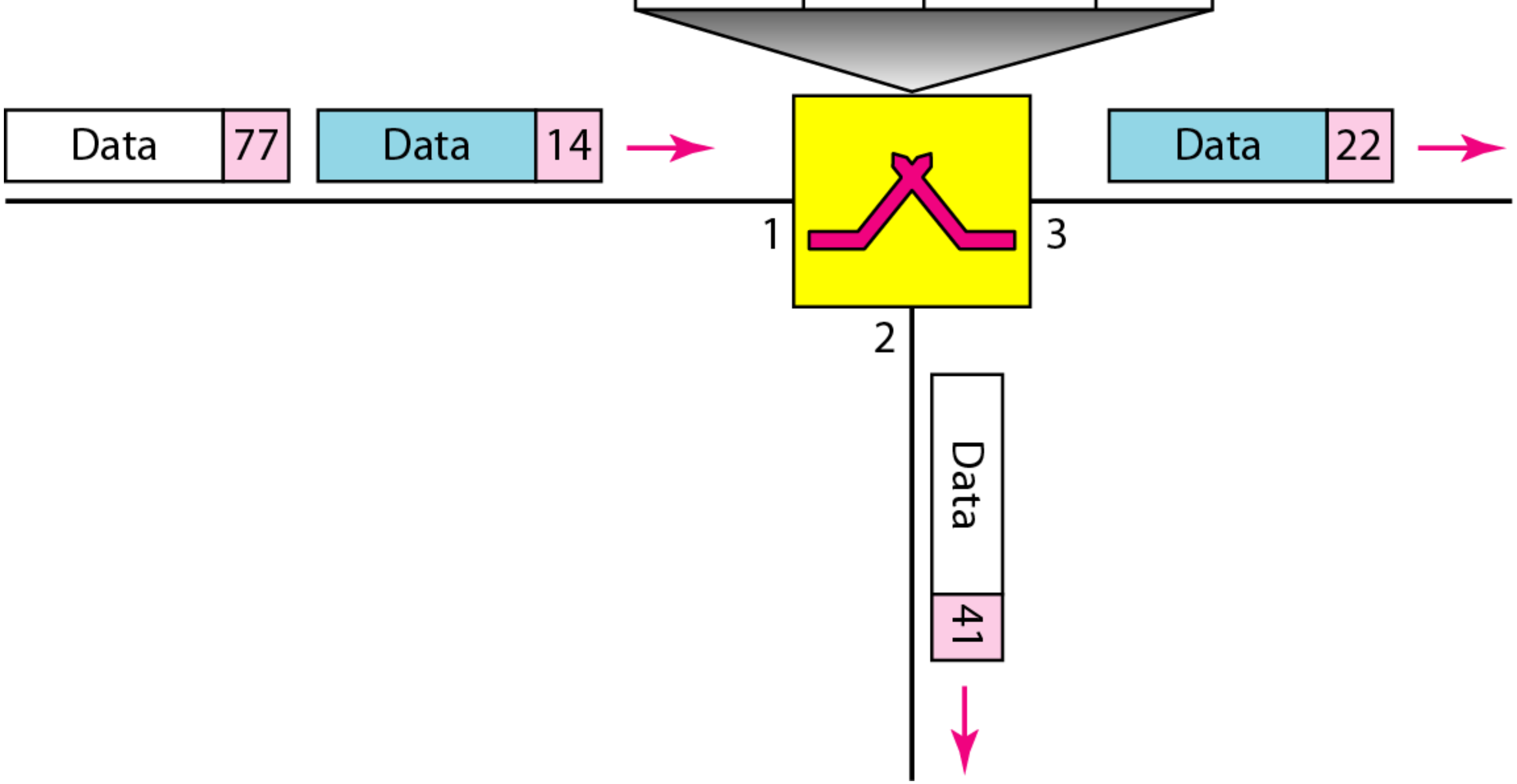
Virtual-Circuit Identifier: The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI).

A VCI, unlike a global address, is a small number that has only switch scope.

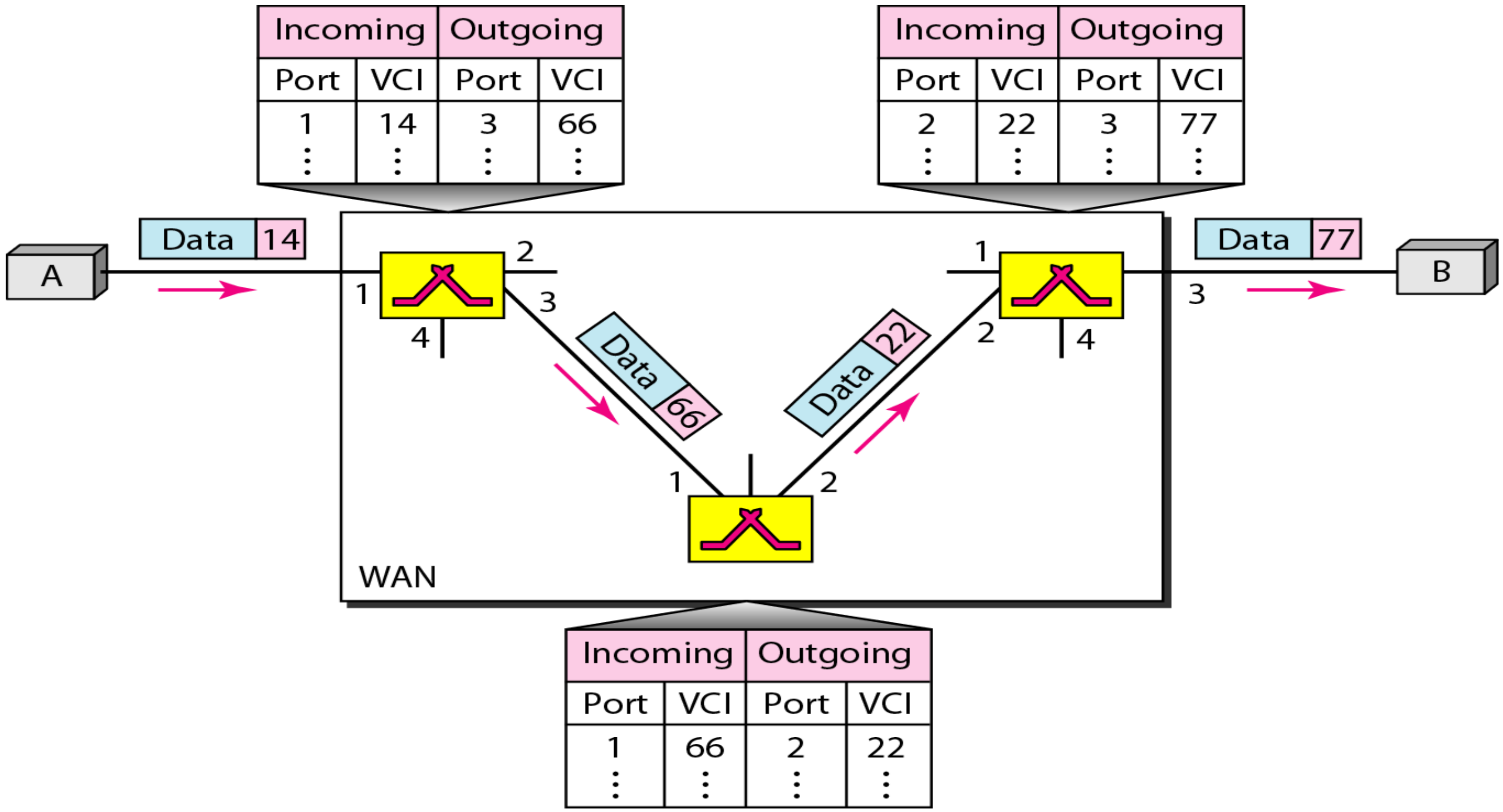
It is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.

Switch and tables in a virtual-circuit network

Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
1	77	2	41



Source-to-destination data transfer in a virtual-circuit network



Packet Switching Virtual Circuit Approach
How Virtual Circuit is Established ?

Three Phases:

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.

Setup phase, the source and destination use their global addresses to help switches make table entries for the connection.

In the **teardown phase**, the source and destination inform the switches to delete the corresponding entry.

Data transfer occurs between these two phases.

Packet Switching Virtual Circuit Approach
How Virtual Circuit is Established ?

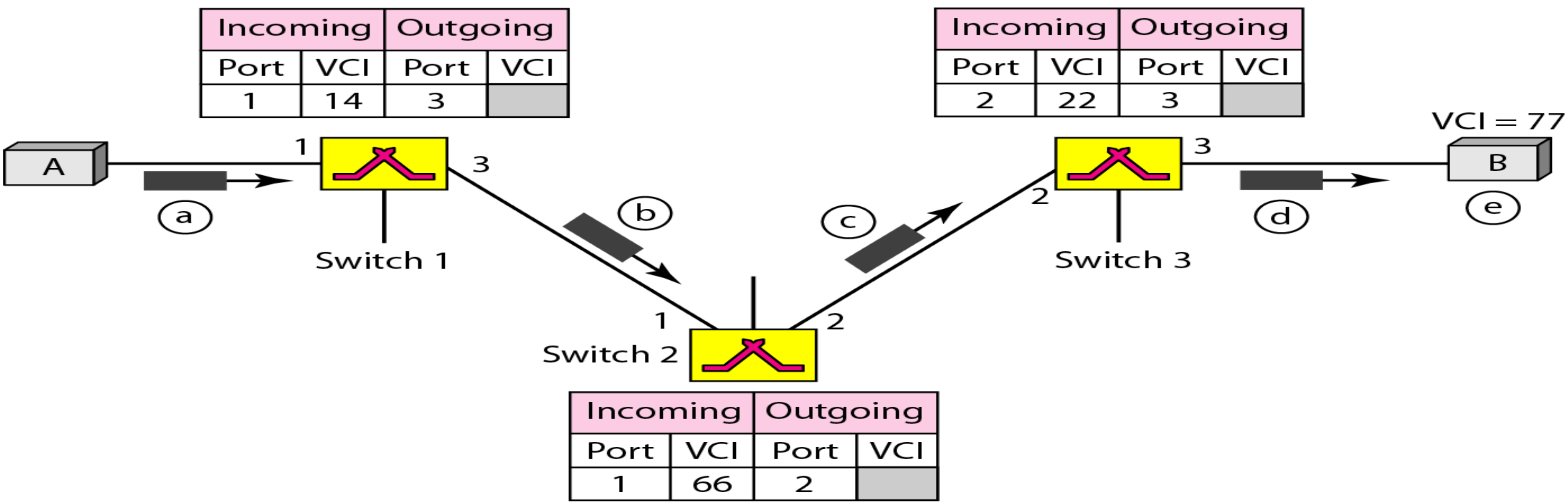
Setup Phase:

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.

Setup Request: A setup request frame is sent from the source to the destination.

Acknowledgment: A special frame, called the acknowledgment frame, completes the entries in the switching tables.

How Virtual Circuit is established



Source A sends a setup frame to switch 1

Switch 1 receives the setup request frame

It knows that a frame going from A to B goes out through port 3

The switch, in the setup phase, acts as a packet switch and it has a routing table which is different from the switching table

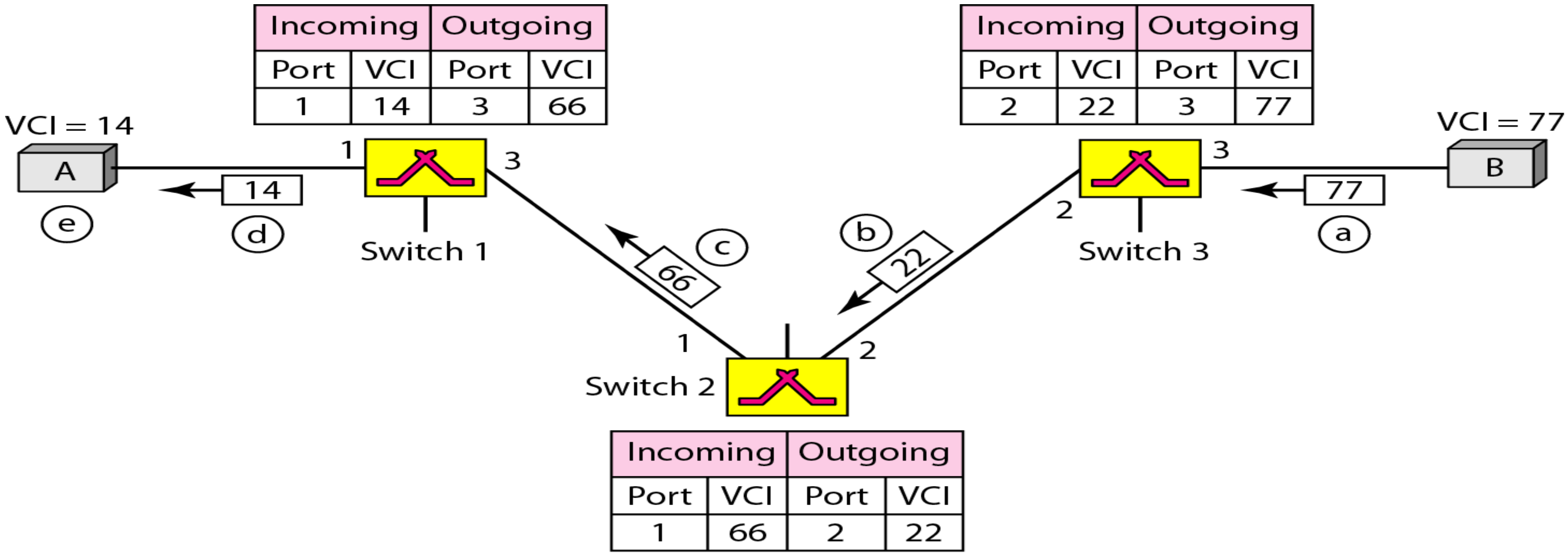
The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step.

Switch 2 receives the setup request frame. The same events happen here as at switch 1 and three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port (2).

Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).

Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and no other sources.

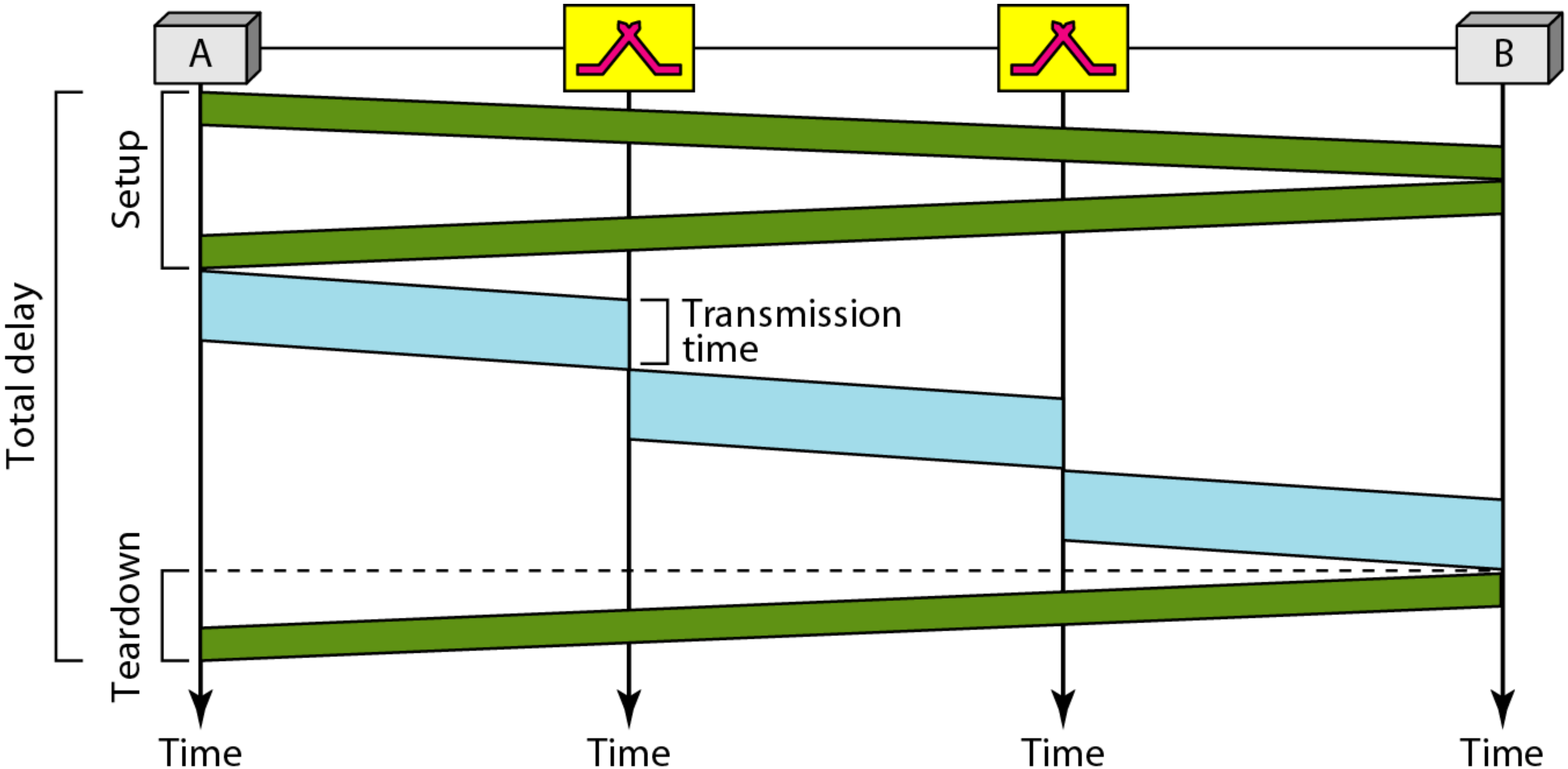
Setup acknowledgment in a virtual-circuit network



A. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch

B. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.
C. Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.
D. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.
E. The source uses this as the outgoing VCI for the data frames to be sent to destination B.

Delay in a virtual-circuit network

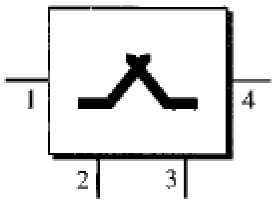


Total delay = $3T + 3\tau$ + setup delay + teardown delay

Virtual Circuit switching-Question Solution

Figure 8.28 *Exercise 18*

Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
2	71	4	41
2	92	1	45
3	58	2	43
3	78	2	70
4	56	3	11



Find the output port and the output VCI for packets with the following input port and input VCI addresses:
Packet 1: 3, 78
Packet 2: 2, 92
Packet 3: 4, 56
Packet 4: 2, 71

Figure 8.28 shows a switch in a virtual circuit network.

Packet 1: **2, 70**
Packet 2: **1, 45**
Packet 3: **3, 11**
Packet 4: **4, 41**

Datagram switching-Question Solution

Five equal-size datagram belonging to the same message leave for the destination one after another. However, they travel through different paths as shown in Table

Datagram	Path Length	Visited Switches
1	3200Km	1,3,5
2	11,700 Km	1,2,5
3	12,200 Km	1,2,3,5
4	10,200 Km	1,4,5
5	10,700 Km	1,4,3,5

We assume that the delay for each switch (including waiting and processing) is 3,10, 20, 7, and 20 ms respectively. Assuming that the propagation speed is 2×10^8 m, find the order the datagram arrive at the destination and the delay for each. Ignore any other delays in transmission.

We assume that the transmission time is negligible in this case. This means that we suppose all datagrams start at time 0. The arrival timed are calculated as:

First:	$(3200 \text{ Km}) / (2 \times 10^8 \text{ m/s})$	$+ (3 + 20 + 20)$	= **59.0 ms**
Second:	$(11700 \text{ Km}) / (2 \times 10^8 \text{ m/s})$	$+ (3 + 10 + 20)$	= **91.5 ms**
Third:	$(12200 \text{ Km}) / (2 \times 10^8 \text{ m/s})$	$+ (3 + 10 + 20 + 20)$	= **114.0 ms**
Fourth:	$(10200 \text{ Km}) / (2 \times 10^8 \text{ m/s})$	$+ (3 + 7 + 20)$	= **81.0 ms**
Fifth:	$(10700 \text{ Km}) / (2 \times 10^8 \text{ m/s})$	$+ (3 + 7 + 20 + 20)$	= **103.5 ms**

The order of arrival is: **3** $\rightarrow$ **5** $\rightarrow$ **2** $\rightarrow$ **4** $\rightarrow$ **1**

Datagram switching-Question Solution

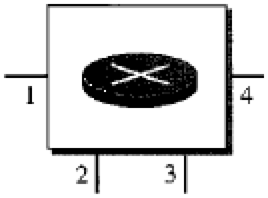
Figure 8.27 shows a switch (router) in a datagram network.

Find the output port for packets with the following destination addresses:

Packet 1: 7176
Packet 2: 1233
Packet 3: 8766
Packet 4: 9144

Figure 8.27 *Exercise 17*

Destination address	Output port
1233	3
1456	2
3255	1
4470	4
7176	2
8766	3
9144	2



Packet 1: **2**
Packet 2: **3**
Packet 3: **3**
Packet 4: **2**

Advantages of packet switching

1. Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.
2. Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
3. Packet can be rerouted if there is any problem, such as, busy or disabled links.
4. The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages of packet switching

1. Protocols for packet switching are typically more complex.
2. It can add some initial costs in implementation.
3. If packet is lost, sender needs to retransmit the data.
4. Another disadvantage is that packet-switched systems still can’t deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

Comparative Analysis

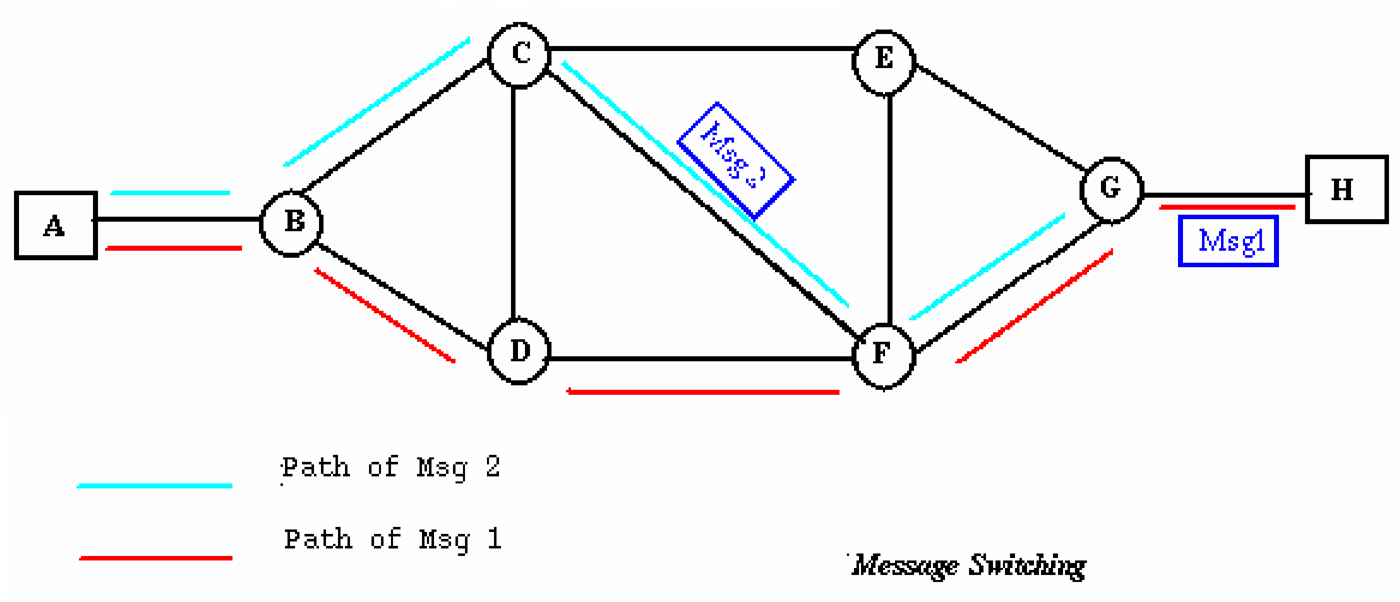
Circuit, Datagram & Virtual Circuit Switching

Circuit Switching	Packet Switching(Datagram type)	Packet Switching(Virtual Circuit type)
Dedicated path	No Dedicated path	No Dedicated path
Path is established for entire conversation	Route is established for each packet	Route is established for entire conversation
Call setup delay	packet transmission delay	call setup delay as well as packet transmission delay
Overload may block call setup	Overload increases packet delay	Overload may block call setup and increases packet delay
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call setup	overhead bits in each packet	overhead bits in each packet

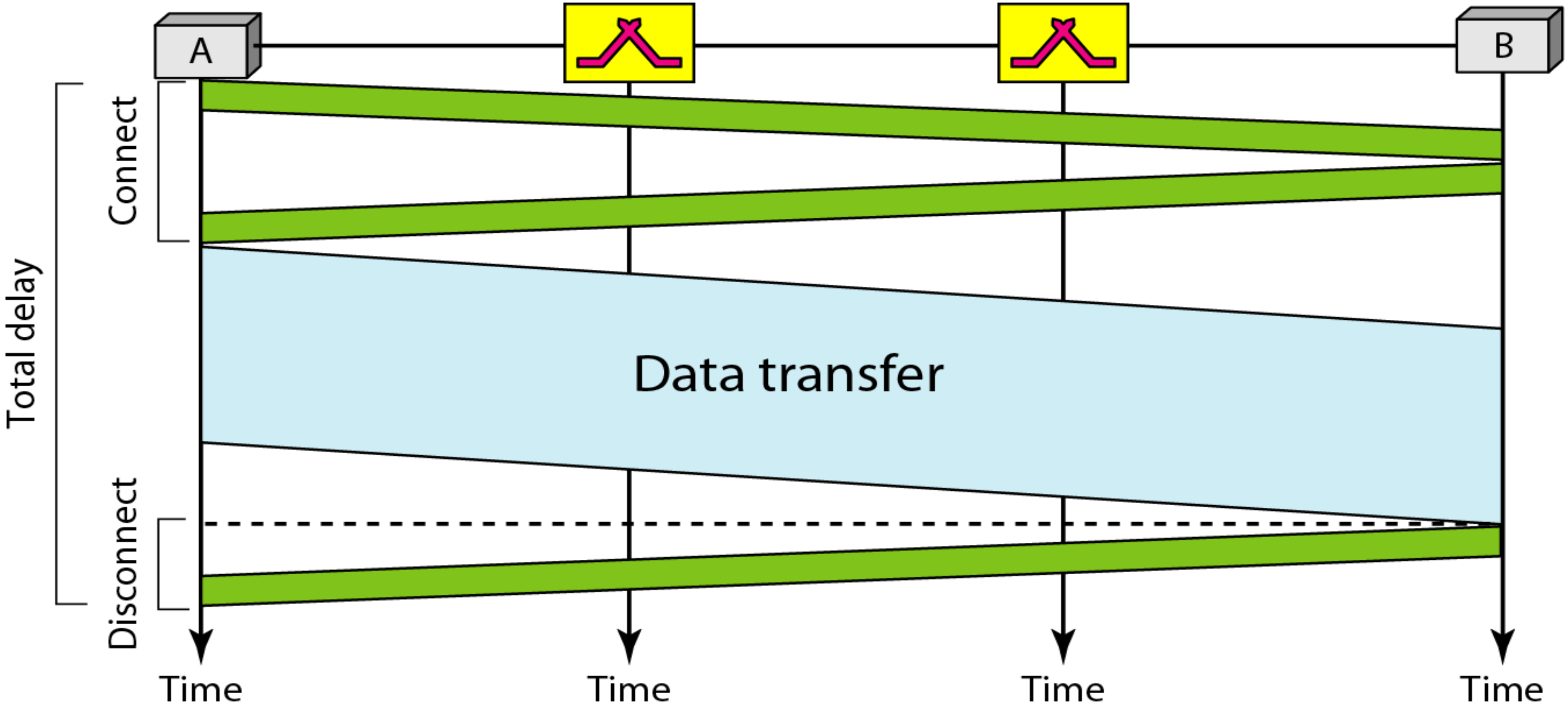
Message Switching

- With message switching there is **no need to establish a dedicated path** between two stations.
- When a station sends a message, the destination address is appended to the message.
- The message is then transmitted through the network, in its **entirety, from node to node**.
- Each node receives the entire message, **stores it in its entirety on disk**, and then transmits the message to the next node.
- This type of network is called **a store-and-forward network**.
- **A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.**

Message Switching



Delay in a circuit-switched network

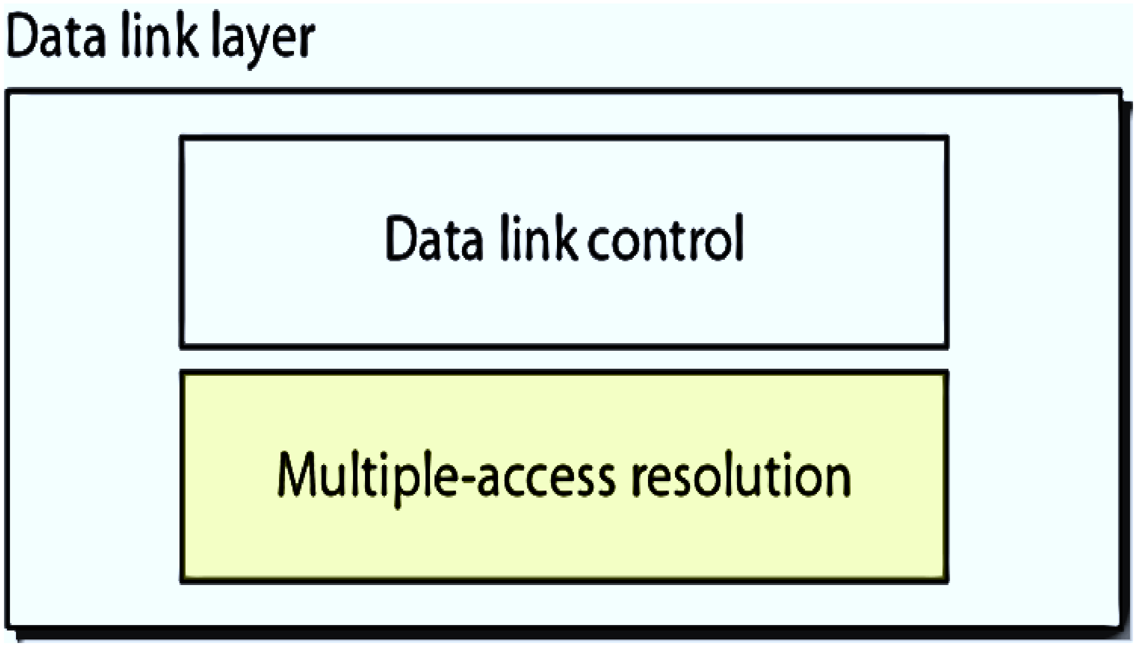


Total Delay in a circuit-switched network will be delay for setup and tear down + Propagation delay + Transmission delay i.e.

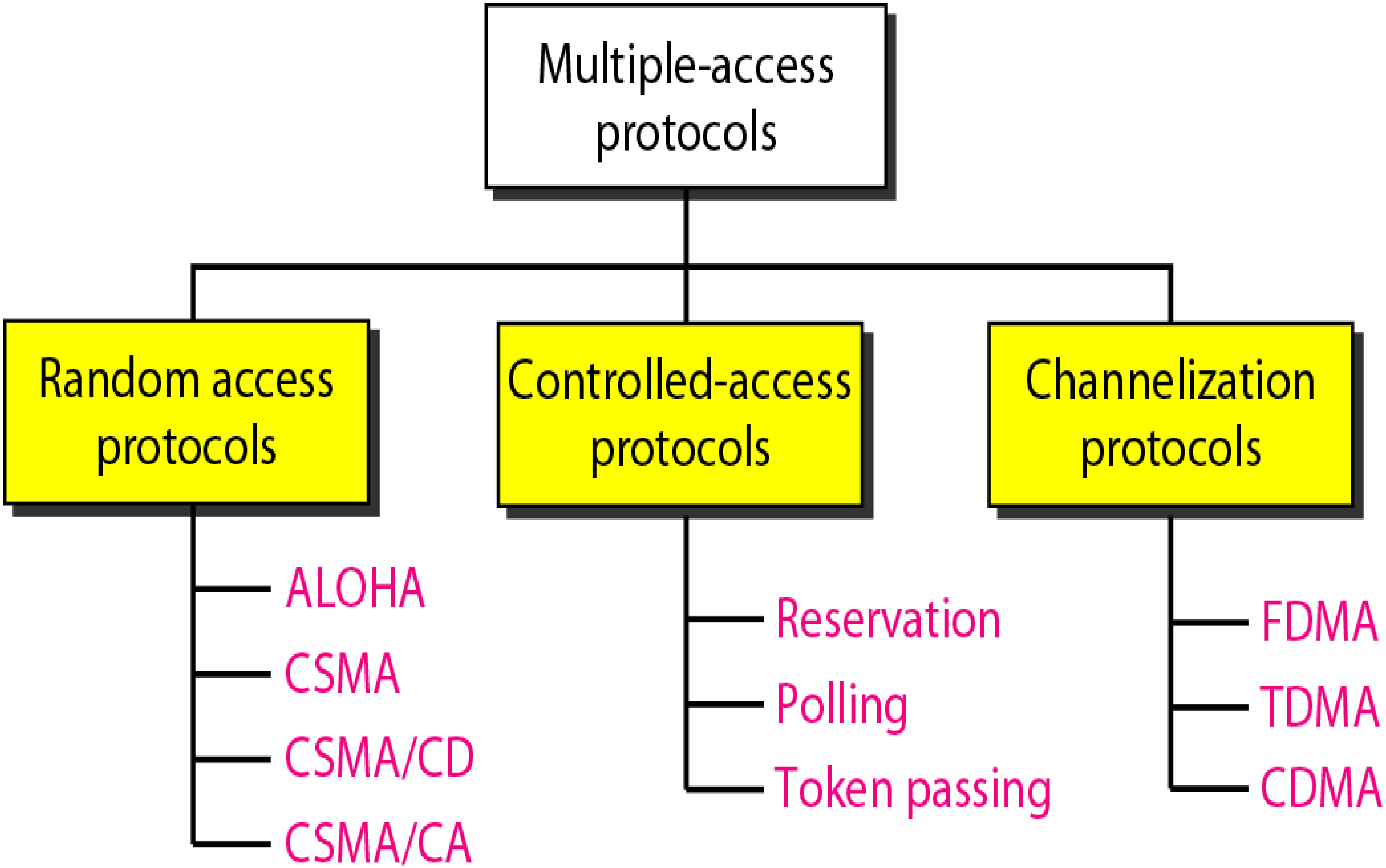
Total Delay= 3 * Propagation time + 3 * Transmission time + Data Transfer time

MULTIPLE ACCESS

Data link layer divided into two functionality-oriented sublayers



- The upper sublayer is responsible for data link control, and the lower sublayer is responsible for resolving access to the shared media.
- If the channel is dedicated, we do not need the lower sublayer.


Multiple-access protocols
Random access protocols
Controlled-access protocols
Channelization protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token passing
FDMA
TDMA
CDMA

RANDOM ACCESS

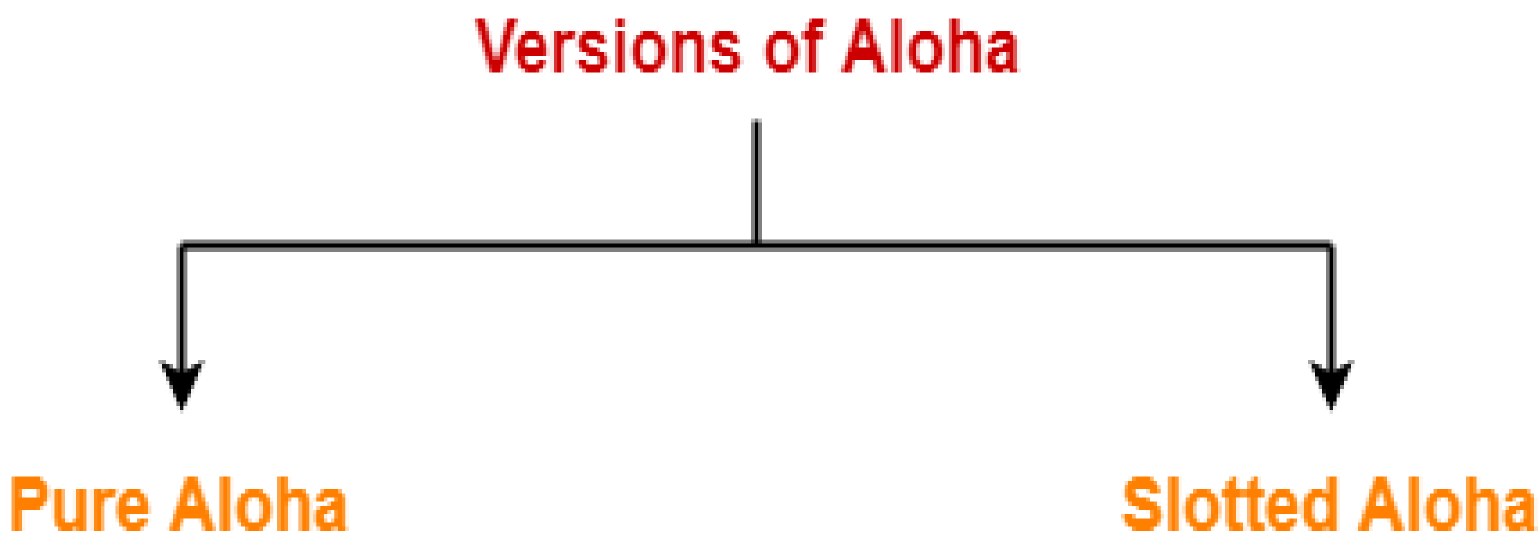
In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

Topics discussed in this section:

ALOHA
Carrier Sense Multiple Access
Carrier Sense Multiple Access with Collision Detection
Carrier Sense Multiple Access with Collision Avoidance

Aloha

There are two different versions of Aloha-



Pure Aloha-

- It allows the stations to transmit data at any time whenever they want.
- After transmitting the data packet, station waits for some time.

- Then, following 2 cases are possible-

Case-01:

- Transmitting station receives an acknowledgement from the receiving station.
- In this case, transmitting station assumes that the transmission is successful.

Case-02:

- Transmitting station does not receive any acknowledgement within specified time from the receiving station.
- In this case, transmitting station assumes that the transmission is unsuccessful.

Frame **time:**The **time** required to send a frame is called frame **time.**

Vulnerable time for Pure Aloha: It is the **time** during which no transmission should be done to avoid any collision.

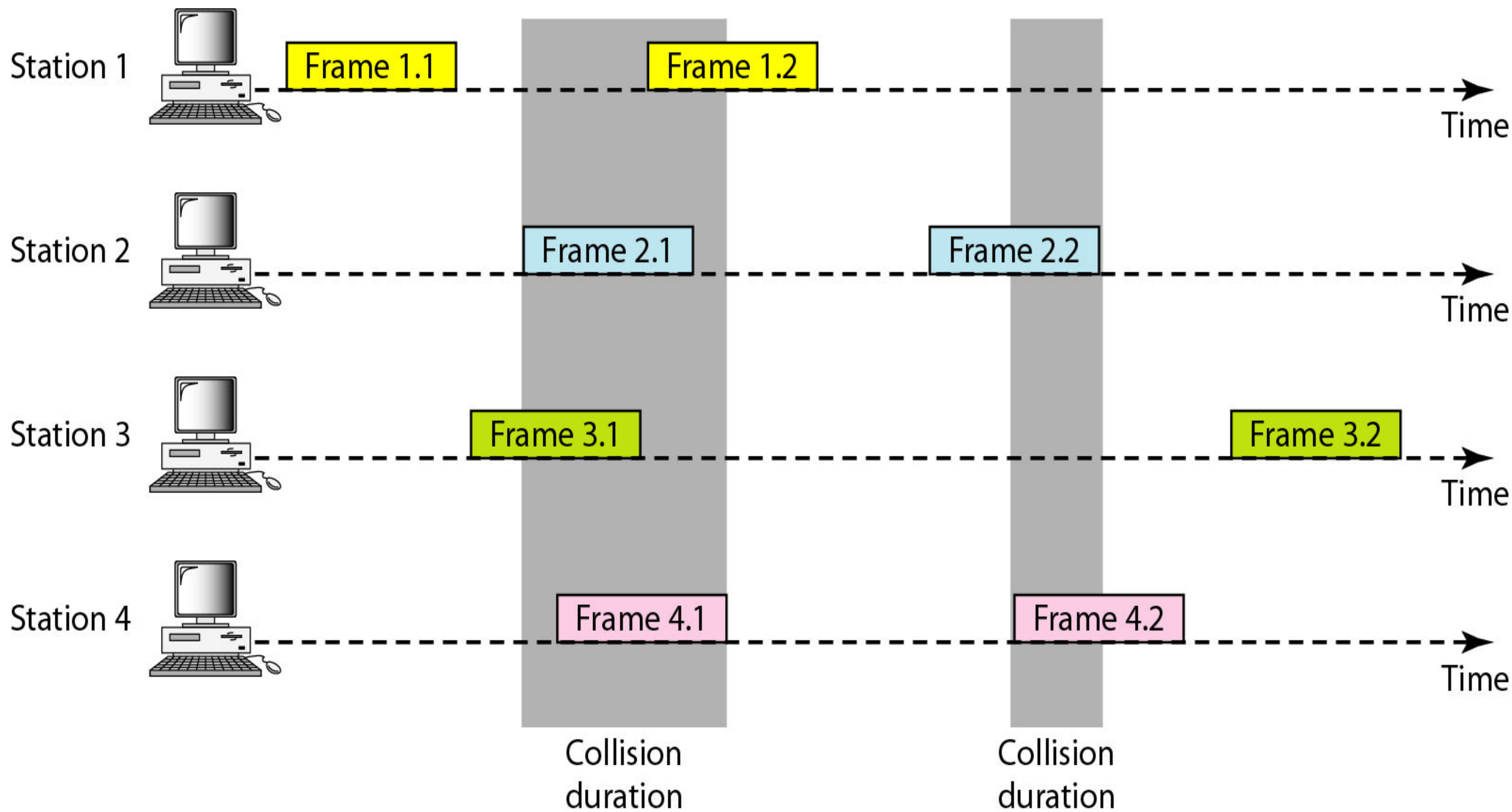
In case of Pure Aloha vulnerable time is 2T.

Throughput Let us call G the average number of frames generated by the system during one frame transmission time. Then it can be proved that the average number of successful transmissions for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput S_{max} is 0.184, for $G = \frac{1}{2}$. In other words, if one-half a frame is generated during one frame transmission time (in other words, one frame during two frame transmission times), then 18.4 percent of these frames reach their destination successfully. This is an expected result because the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other stations generate a frame during this time), the frame will reach its destination successfully.

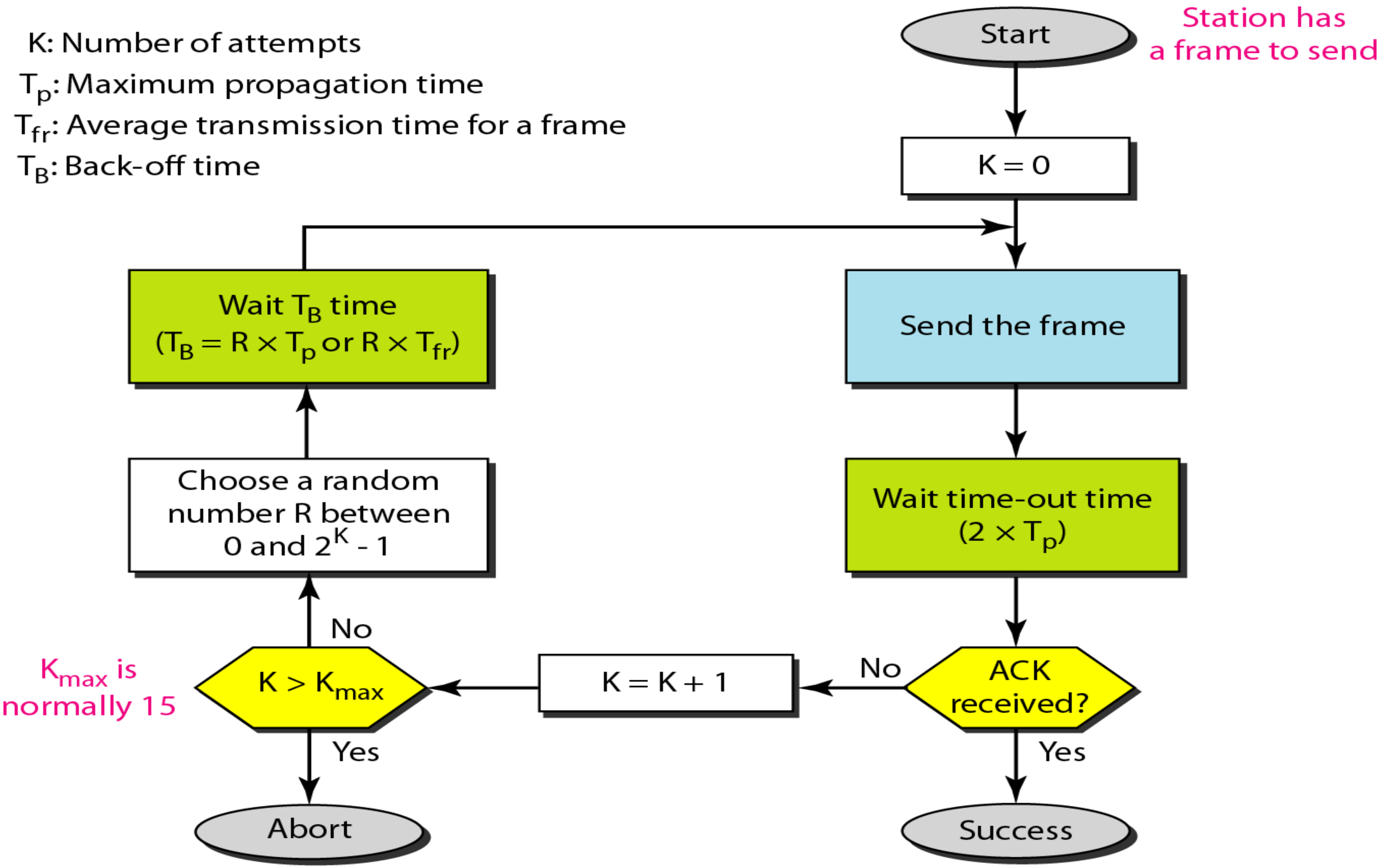
The throughput for pure ALOHA is $S = G \times e^{-2G}$.

The maximum throughput $S_{max} = 0.184$ when $G = (1/2)$.

Frames in a pure ALOHA network



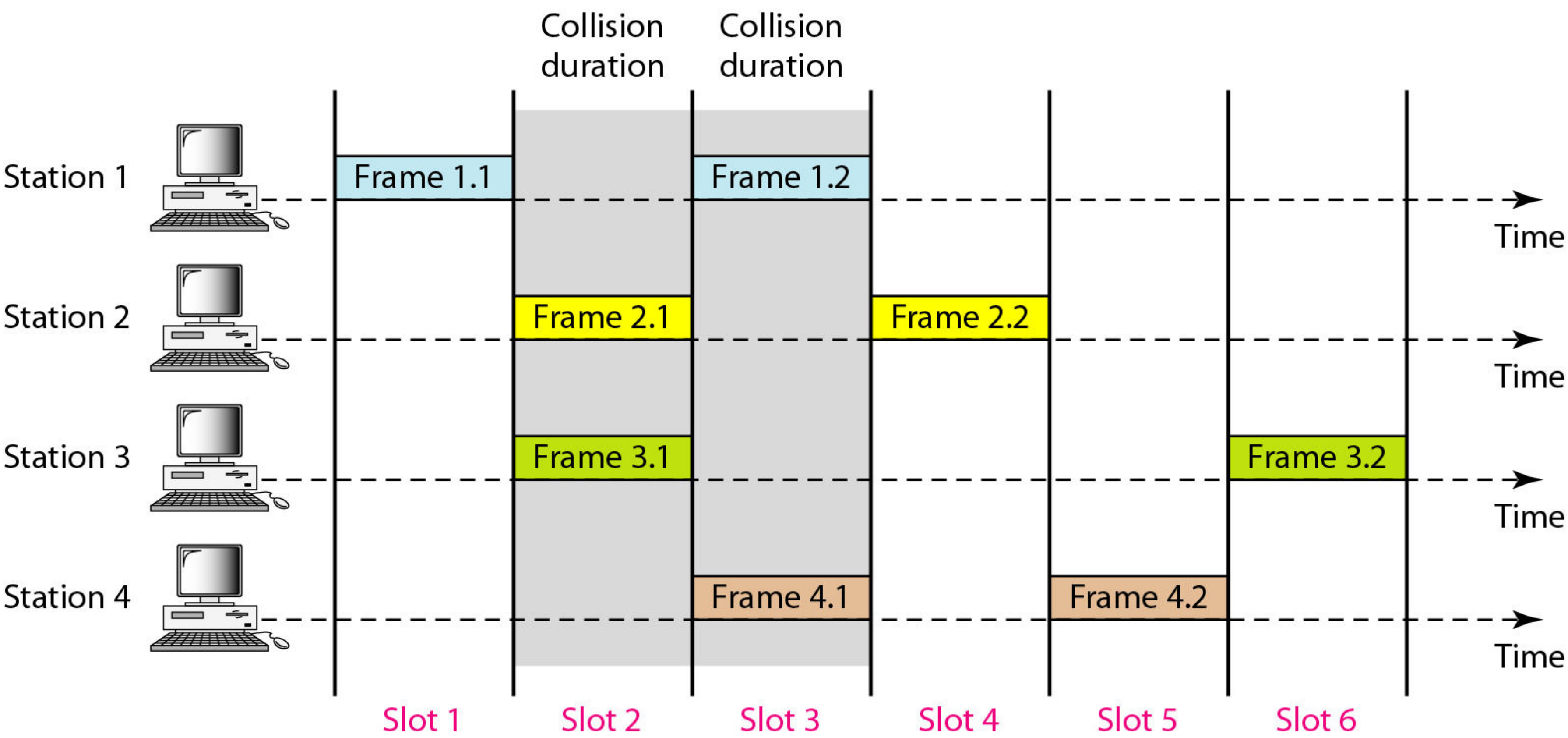
Procedure for pure ALOHA protocol



Slotted Aloha

- Slotted Aloha divides the time of shared channel into discrete intervals called as **time slots**.
- Any station can transmit its data in any time slot.
- The only condition is that station must start its transmission from the beginning of the time slot.
- If the beginning of the slot is missed, then station has to wait until the beginning of the next time slot.
- A collision may occur if two or more stations try to transmit data at the beginning of the same time slot.

Frames in a slotted ALOHA network



Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot.

Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot.
However, the vulnerable time is now reduced to one-half, equal to Tf

Throughput It can be proved that the average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$. The maximum throughput S_{max} is 0.368, when $G = 1$. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other station generates a frame during this time), the frame will reach its destination successfully.

The throughput for slotted ALOHA is $S = G \times e^{-G}$.
The maximum throughput $S_{max} = 0.368$ when $G = 1$.

Problems on Pure and Slotted Aloha

Q:1. A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision free.

Sol:

Average frame transmission time Tfr is 200 bits/200 kbps or 1 ms. The vulnerable time is 2 x 1 ms =2 ms.

Q:2.A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second

Solution

The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case S =G x e-2G or S =0.135 (13.5 percent). This means that the throughput is 1000 X 0.135 =135 frames. Only 135 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (112). In this case S = G x e-2G or S = 0.184 (18.4 percent). This means that the throughput is 500 x 0.184 =92 and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case S = G x e-2G or S =0.152 (15.2 percent). This means that the throughput is 250 x 0.152 = 38. Only 38 frames out of 250 will probably survive.

Q:2.A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces

a. 1000 frames per second

b. 500 frames per second

c. 250 frames per second Solution

The frame transmission time is 200/200 kbps or 1 ms. a. In this case G is 1. So S =G x e-G or S =0.368 (36.8 percent). This means that the throughput is 1000 x 0.0368 =368 frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.

b. Here G is ~. In this case S =G x e-G or S =0.303 (30.3 percent). This means that the throughput is 500 x 0.0303 =151. Only 151 frames out of 500 will probably survive.

c. Now G is 1. In this case S =G x e-G or S =0.195 (19.5 percent). This means that the throughput4 is 250 x 0.195 = 49. Only 49 frames out of 250 will probably survive.

Carrier Sense Multiple Access (CSMA)

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer.

Carrier Sense multiple access requires that each station first check the state of the medium before sending.

CSMA is based on the principle

"sense before transmit"

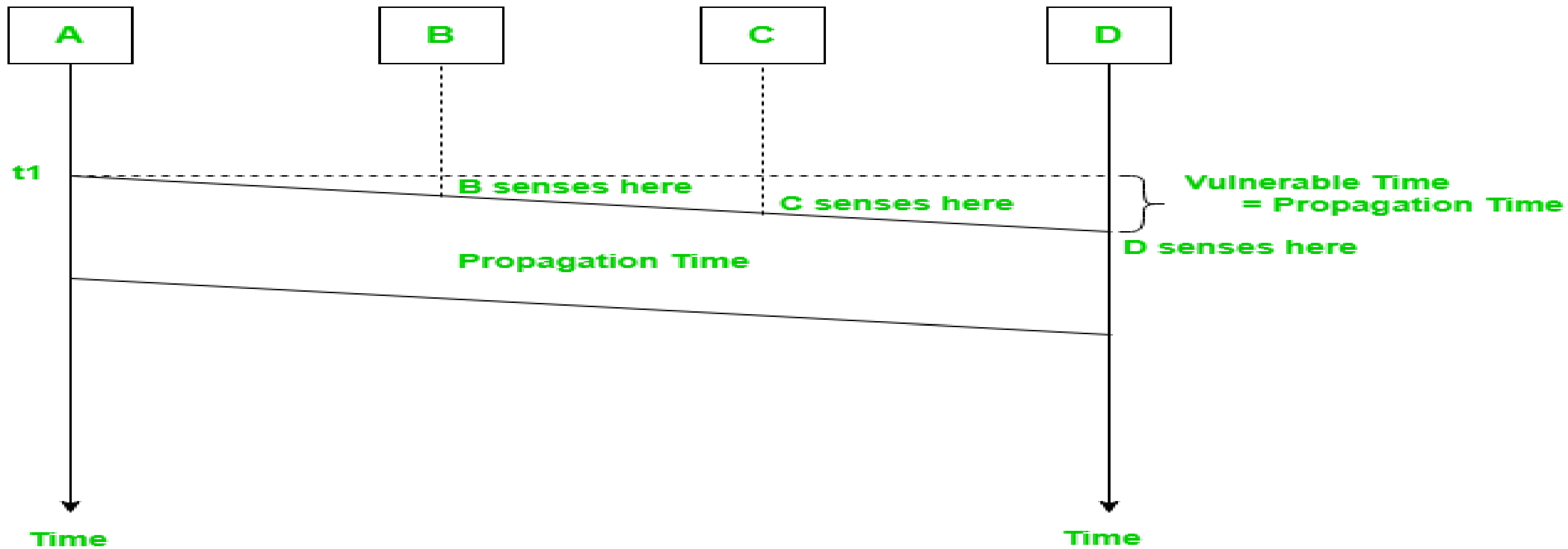
or

"listen before talk"

CSMA can reduce the possibility of collision, but it cannot eliminate it

The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station

Vulnerable time in CSMA



The vulnerable time for CSMA is the propagation time Tp

This is the time needed for a signal to propagate from one end of the medium to the other.

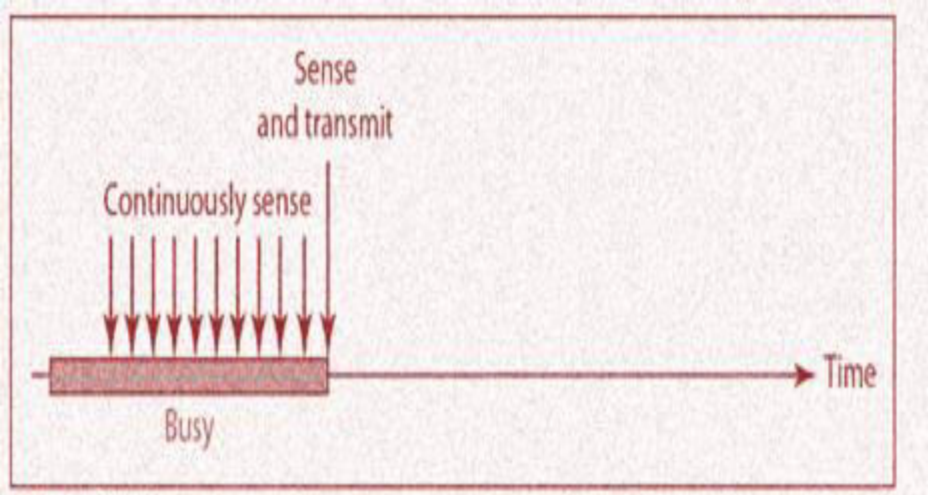
When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.

But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.

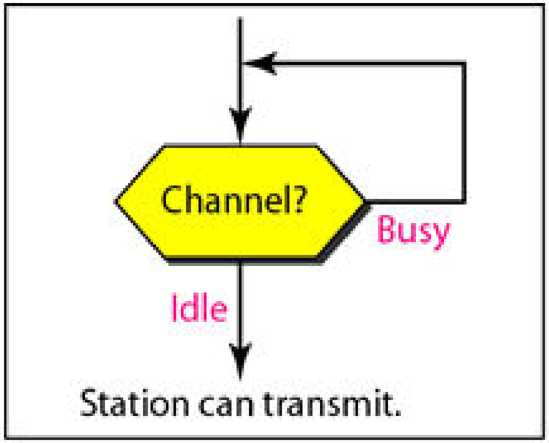
Types of CSMA Protocols

- 1-Persistent CSMA
- Non-Persistent CSMA
- P-Persistent CSMA

1-Persistent CSMA



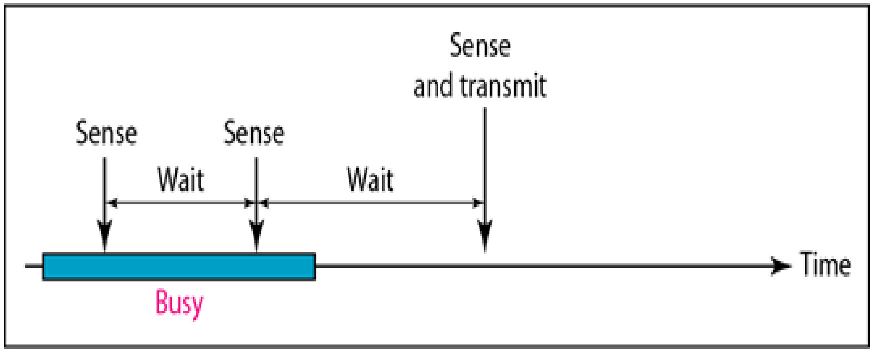
a. 1-persistent



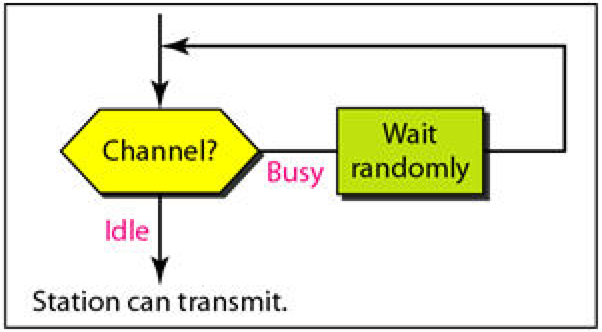
a. 1-persistent

- In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called 1-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start all over again.

Non-Persistent CSMA



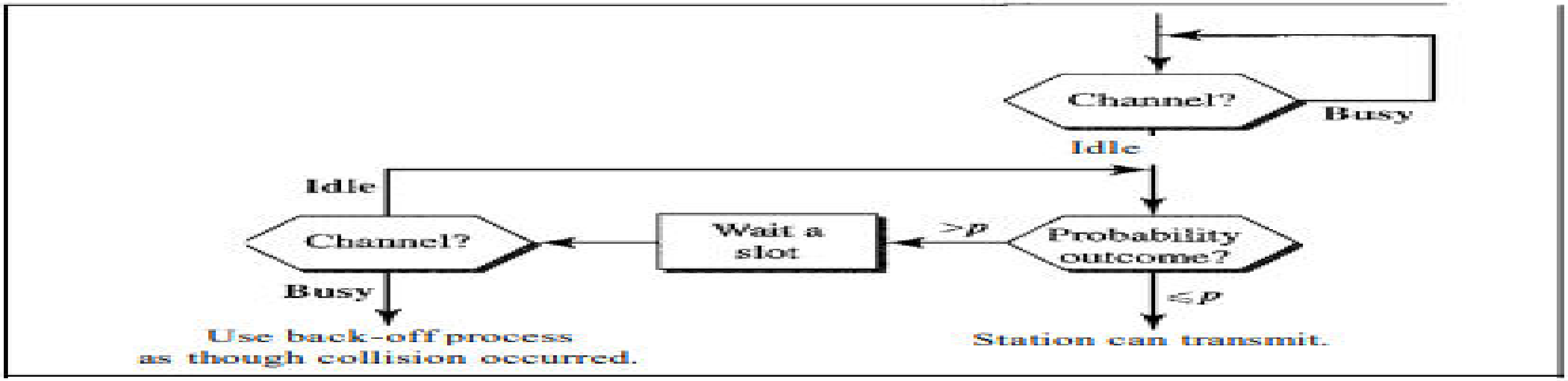
b. Nonpersistent



b. Nonpersistent

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
- After this time, it again checks the status of the channel and if the channel is free it will transmit.
- A station that has a frame to send senses the channel.
- If the channel is idle, it sends immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

P-Persistent CSMA



c. p-persistent

The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.

In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.
2. The station waits for the beginning of the next time slot and checks the line again.
3. a. If the line is idle, it goes to step 1.
4. b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

Collision Detection in CSMA/CD

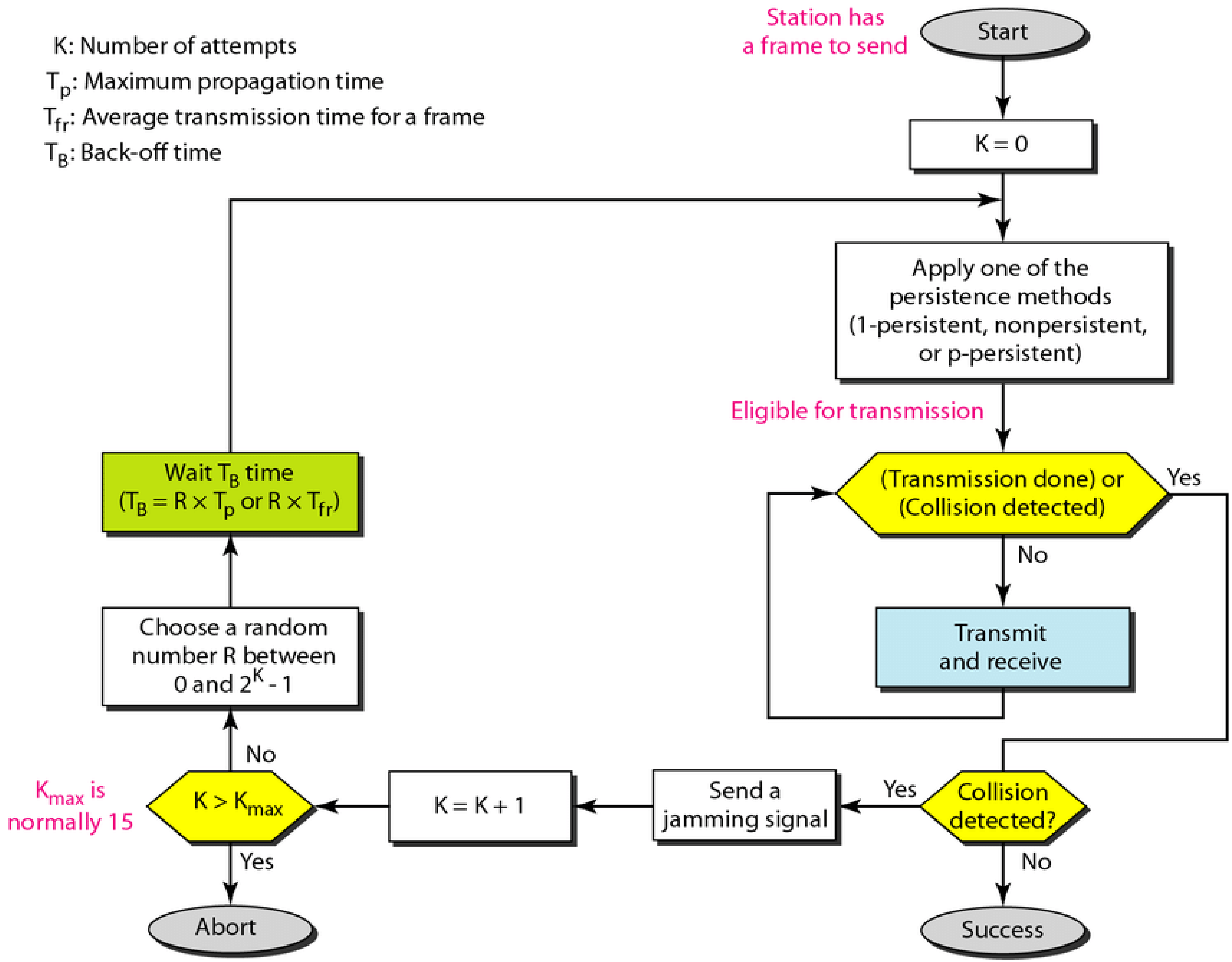
CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media-access control method that was widely used in Early Ethernet technology/LANs.

Consider a scenario where there are ‘n’ stations on a link and all are waiting to transfer data through that channel. In this case all ‘n’ stations would want to access the link/channel to transfer their own data. Problem arises when more than one station transmits the data at the moment. In this case, there will be collisions in the data from different stations.

CSMA/CD is one such technique where different stations that follow this protocol agree on some terms and collision detection measures for effective transmission. This protocol decides which station will transmit when so that data reaches the destination without corruption.

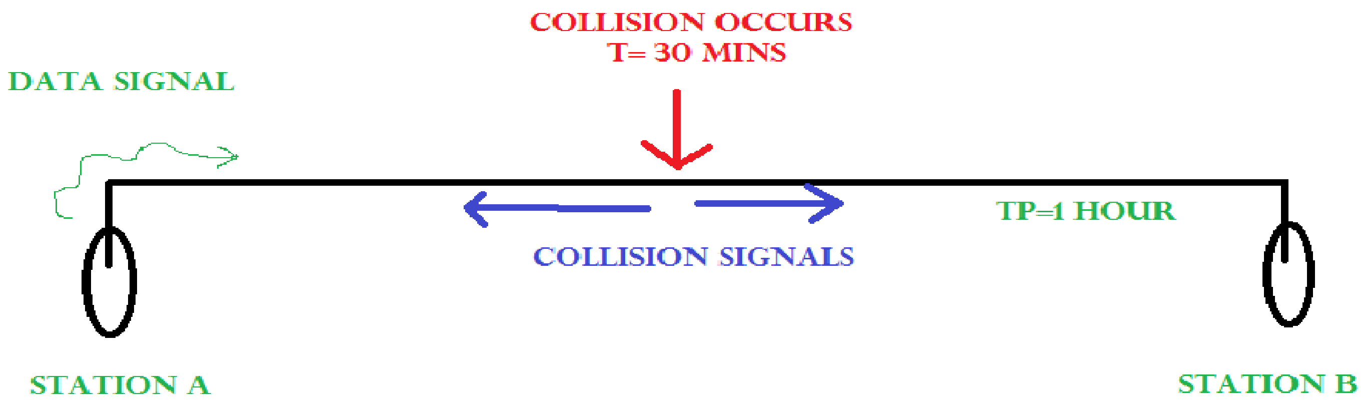
How CSMA/CD works?

- **Step 1:** Check if the sender is ready for transmitting data packets.
- **Step2:**Check if the transmission link is idle?
  Sender has to keep on checking if the transmission link/medium is idle. For this it continuously senses transmissions from other nodes. Sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise it refrains from sending data.
- **Step 3:** Transmit the data & check for collisions.
  Sender transmits its data on the link. CSMA/CD does not use 'acknowledgement' system. It checks for the successful and unsuccessful transmissions through collision signals. During transmission, if collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time interval before it resends the frame. After some random time, it again attempts to transfer the data and repeats above process.
- **Step 4:** If no collision was detected in propagation, the sender completes its frame transmission.



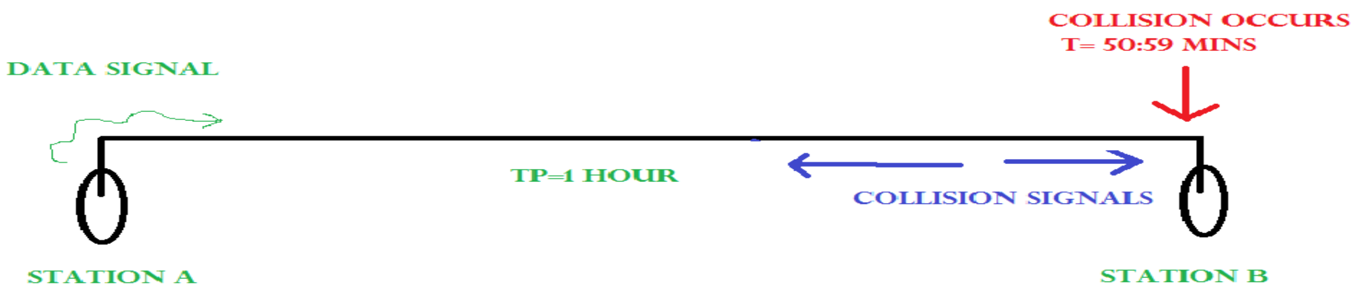
K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
K = 0
Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)
Eligible for transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)
Choose a random number R between 0 and $2^K - 1$
No
K_{max} is normally 15
$K > K_{max}$
Yes
Abort
K = K + 1
Send a jamming signal
Yes
Collision detected?
No
Success

How a station knows if its data collides?



Consider the above situation. Two stations, A & B.
Propagation Time: Tp = 1 hr (Signal takes 1 hr to go from A to B)
At time t=0, A transmits its data.
At t= 30 mints. : Collision occurs.
After collision occurs, a collision signal is generated and sent to both A & B to inform the stations about collision. Since the collision happened midway, the collision signal also takes 30 minutes to reach A & B.
Therefore, t=1 hr: A & B receive collision signals. This collision signal is received by all the stations on that link.

Consider the above system again.



At time t=0, A transmits its data.
At t= 59:59 mins : Collision occurs .
This collision occurs just before the data reaches B. Now the collision signal takes 59:59 minutes again to reach A. Hence, A receives the collision information approximately after 2 hours, that is, after **2 x Tp**. This is the maximum collision time that a system can take to detect if the collision was of its own data.

Length of the packet = 2 X Tp X Bandwidth of the link

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. In contrast to CSMA/CD (Carrier Sense Multiple Access/Collision Detection) that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if a collision occurs. It can’t be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

These are three types of strategies:

Inter Frame Space (IFS) – The concept of an interframe space allows wireless systems to implement a simple priority system. Systems with high priority data to send have shorter IFS times, so whenever the medium is clear they will be the first to

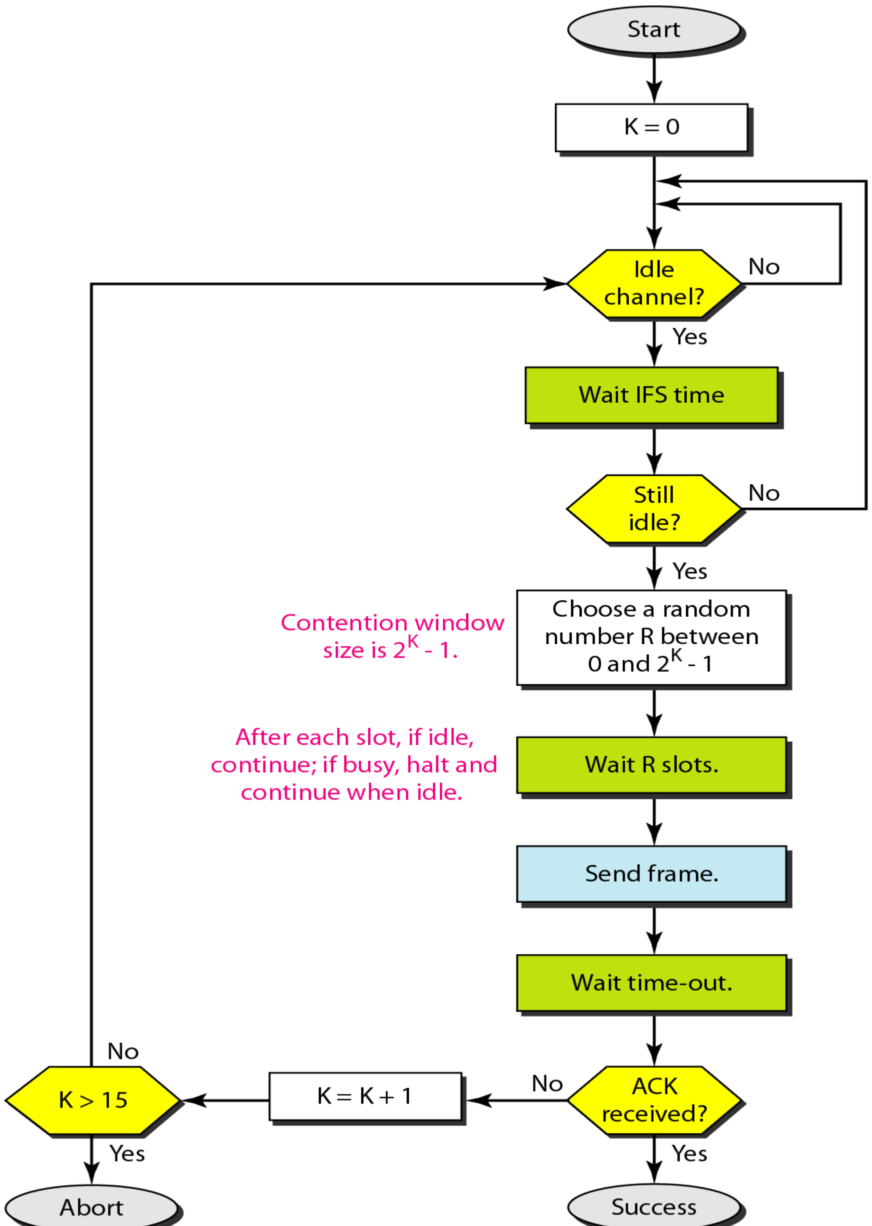
Contention Window – It is the amount of time divided into slots. A station which is ready to send frames chooses random number of slots as **wait time**.

Acknowledgements – The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

ALGORITHM FOR CSMA/CA

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- After sending the frame, it sets a timer.
- The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
- Otherwise, it waits for a back-off time period and restarts the algorithm.

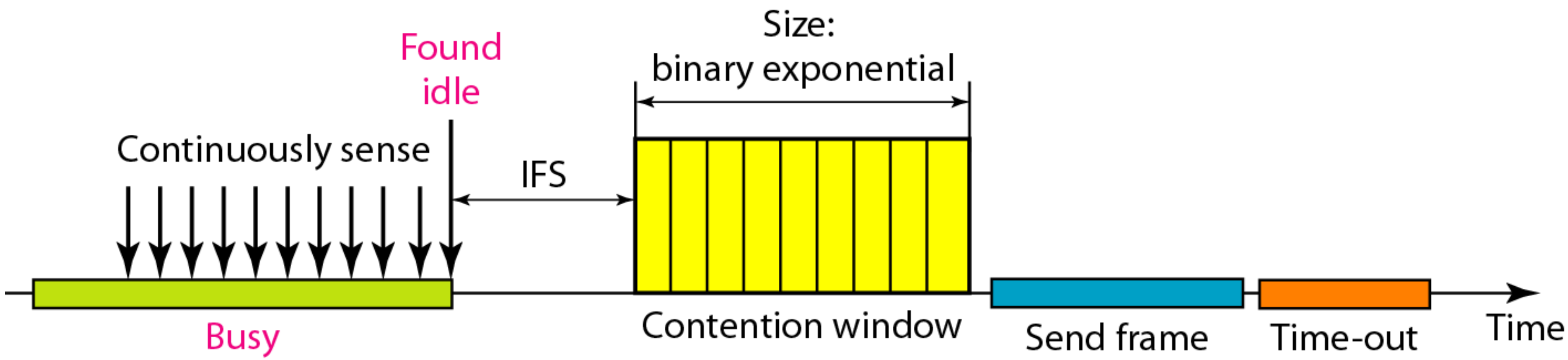
Figure 12.17 *Flow diagram for CSMA/CA*



Channel idle? Don't transmit yet!
Wait IFS time.

Still idle after IFS? Don't transmit yet!
Now in Contention Window.
Choose random number and wait that many slots.

Timing in CSMA/CA



A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal,) is 25.6 μs, what is the minimum size of the frame?

Solution

Minimum size of frame=2 x propagation delay x bandwidth

=2 x 25.6 x 10=512bits or 64 bytes

Q:1.In a CSMA / CD network running at 1 Gbps over 1 km cable with no repeaters, the signal speed in the cable is 200000 km/sec. What is minimum frame size?

Solution-

Given-
- Bandwidth = 1 Gbps
- Distance = 1 km
- Speed = 200000 km/sec

Calculating Propagation Delay-

Propagation delay (T_p)
= Distance / Propagation speed
= 1 km / (200000 km/sec)
= 0.5×10^{-5} sec
= 5×10^{-6} sec

Minimum frame size

= 2 x Propagation delay x Bandwidth
= $2 \times 5 \times 10^{-6}$ sec $\times 10^{9}$ bits per sec
= 10000 bits

A 2 km long broadcast LAN has 10^7 bps bandwidth and uses CSMA / CD. The signal travels along the wire at 2×10^8 m/sec. What is the minimum packet size that can be used on this network?
50 B
100 B
200 B
None of the above

Given-
Distance = 2 km
Bandwidth = 10^7 bps
Speed = 2×10^8 m/sec

Calculating Propagation Delay-

Propagation delay (T_p)
= Distance / Propagation speed
= 2 km / (2×10^8 m/sec)
= 2×10^3 m / (2×10^8 m/sec)
= 10^{-5} sec

Calculating Minimum Frame Size-

Minimum frame size
= 2 x Propagation delay x Bandwidth
= 2×10^{-5} sec x 10^7 bits per sec
= 200 bits or 25 bytes

A and B are the only two stations on Ethernet. Each has a steady queue of frames to send. Both A and B attempts to transmit a frame, collide and A wins **first back off race**. At the end of this successful transmission by A, both A and B attempt to transmit and collide. The probability that A wins the **second back off** race is ___ .

0.5

0.625

0.75

1.0

<u>1st Transmission Attempt-</u>

Both the stations A and B attempts to transmit a frame.
A collision occurs.
Back Off Algorithm runs.
Station A wins and successfully transmits its 1st data packet.

<u>2nd Transmission Attempt-</u>

Station A attempts to transmit its 2nd data packet.
Station B attempts to retransmit its 1st data packet.
A collision occurs.

Now,
We have been asked the probability of station A to transmit its 2nd data packet successfully after 2nd collision.
After the 2nd collision occurs, we have-

At Station A-

2nd data packet of station A undergoes collision for the 1st time.
So, collision number for the 2nd data packet of station A = 1.
Now, station A randomly chooses a number from the range $[0,2^1-1] = [0,1]$.
Then, station A waits for back off time and then attempts to retransmit its data packet.

At Station B-

1st data packet of station B undergoes collision for the 2nd time.
So, collision number for the 1st data packet of station B = 2.
Now, station B randomly chooses a number from the range $[0,2^2-1] = [0,3]$.
Then, station B waits for back off time and then attempts to retransmit its data packet.

Following 8 cases are possible-

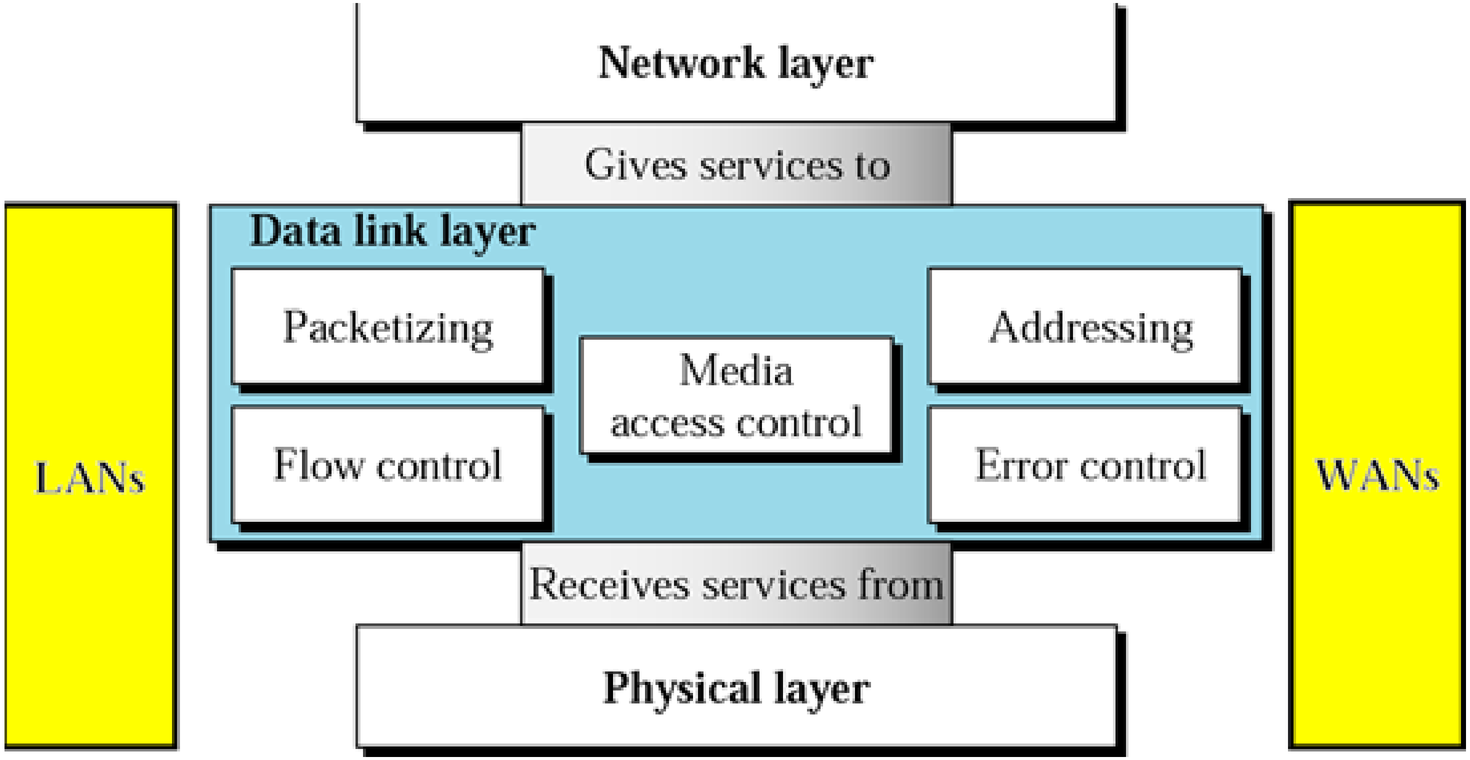
Station A	Station B	Remark
0	0	Collision
0	1	A wins
0	2	A wins
0	3	A wins
1	0	B wins
1	1	Collision
1	2	A wins
1	3	A wins

From here,

- Probability of A winning the 2^{nd} back off race = 5 / 8 = 0.625.
- Thus, Option (B) is correct.

Overview of DLL

The data link layer transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node (hop-to-hop) communication. Specific responsibilities of the data link layer include *framing, addressing, flow control, error control, and media access control.*



Design Issues in Data Link Layer

- **Services provided to the network layer**
- The data link layer act as a service interface to the network layer.
- The principle service is transferring data from network layer on sending machine to the network layer on destination machine.
- **Frame Synchronization:**
  The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine . .

Flow control –

Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

Error control –

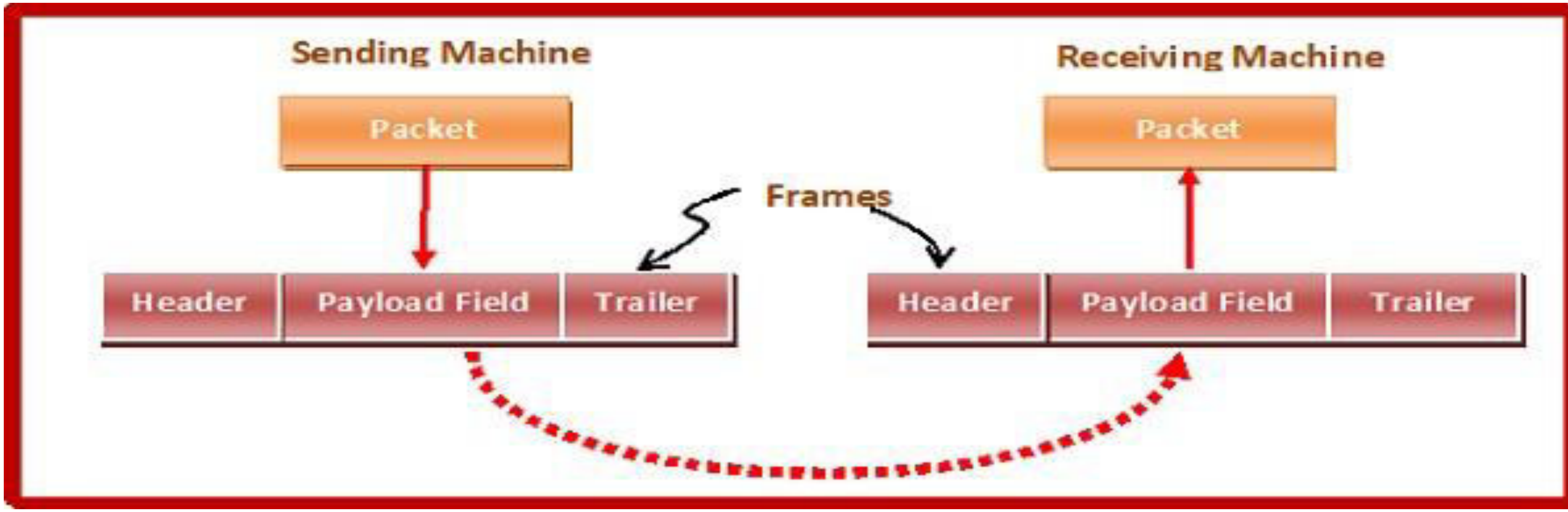
Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Framing

- ❖ Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination.
- ❖ The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing.
- ❖ The data link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another.
- ❖ The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.
- ❖ In addition, each envelope defines the sender and receiver addresses since the postal system is a many-to-many carrier facility.

Why whole message is not packed in single frame?

- Although the whole message could be packed in one frame, that is not normally done.
- One reason is that a frame can be very large, making flow and error control very inefficient.
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole message.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.



Parts of a Frame

A frame has the following parts –

- **Frame Header** – It contains the source and the destination addresses of the frame.
- **Payload field** – It contains the message to be delivered.
- **Trailer** – It contains the error detection and error correction bits.
- **Flag** – It marks the beginning and end of the frame.

Types of Framing

Fixed size – Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells

Drawback: It suffers from internal fragmentation if data size is less than frame size

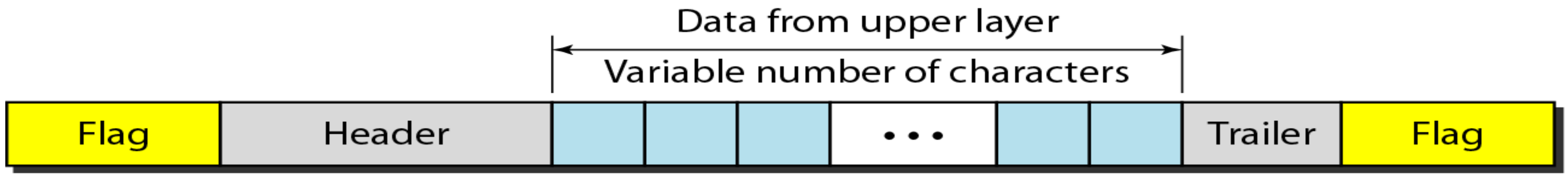
Types of Framing

Variable-Size Framing: In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose:

- ❖ A character-oriented approach
- ❖ A bit-oriented approach.

A character-oriented approach

- To separate one frame from the next, an 8-bit (I-byte) flag is added at the beginning and the end of a frame.
- The flag, composed of protocol-dependent special characters, signals the start or end of a frame.
- To use special characters to indicate the beginning and the end of a frame

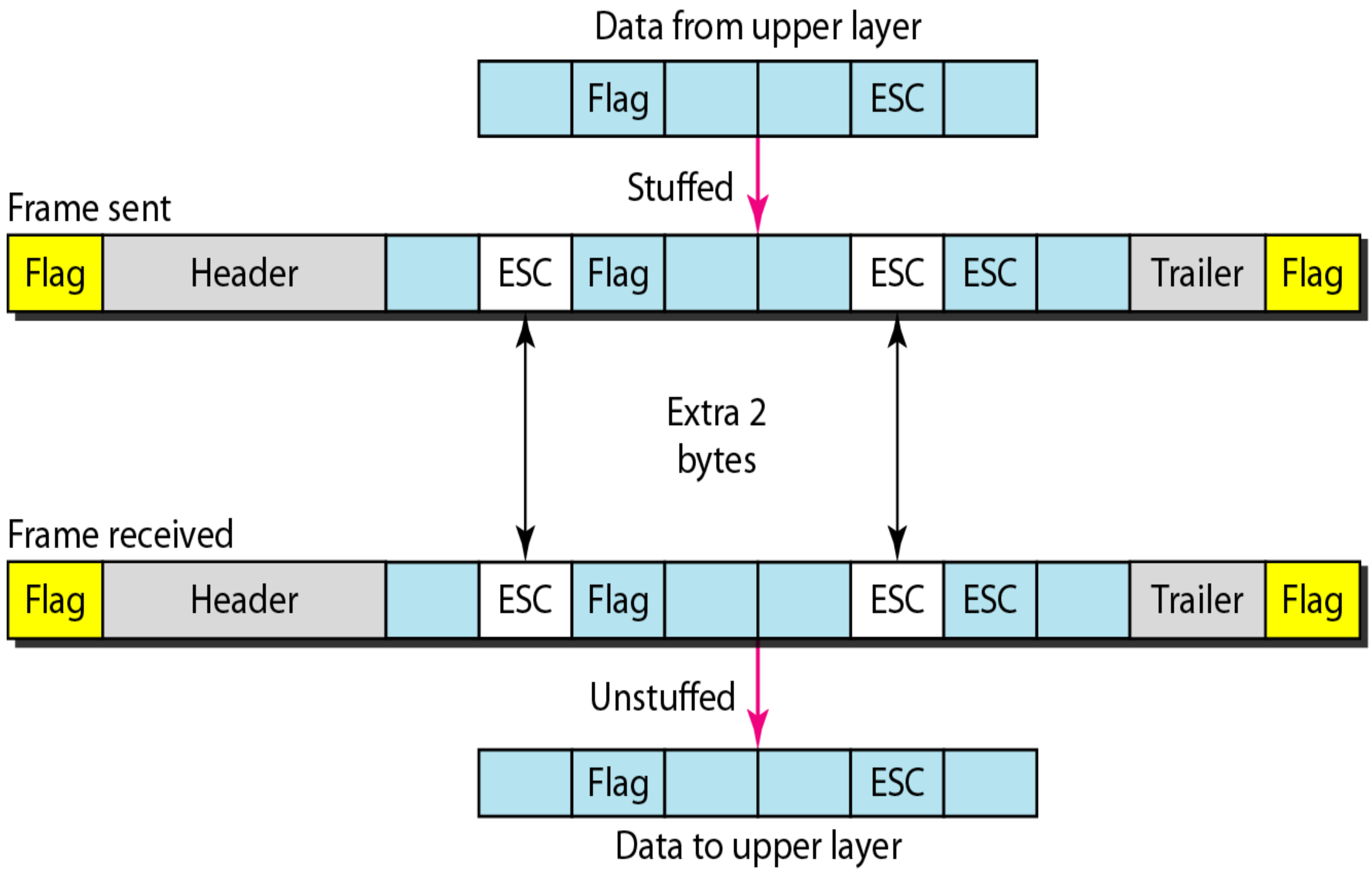


- Good for exchanging text messages, but what if other type of information (graph, audio, video) that can carry any character pattern even same as the special character.
- . If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame. To fix this problem, a **byte-stuffing strategy** was added to character-oriented framing.

Byte stuffing (or character stuffing),

- In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte.
- This byte is usually called the escape character (ESC), which has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

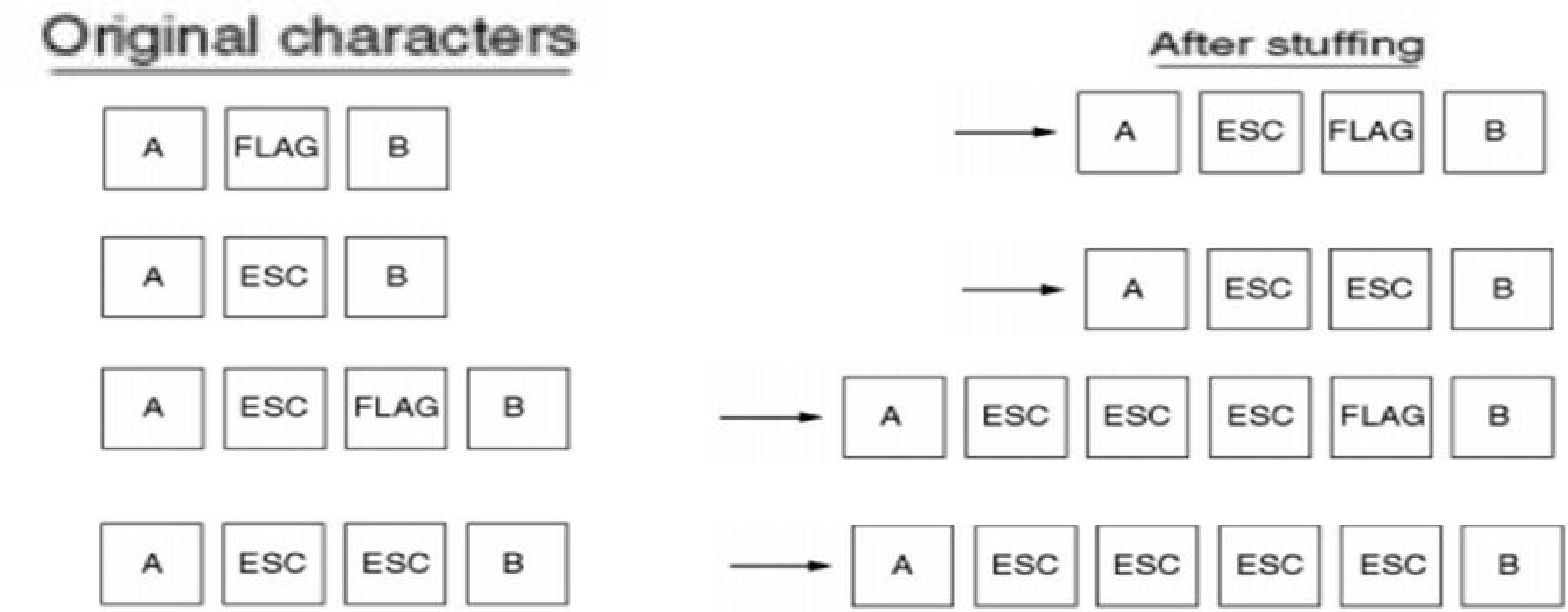
Character-Oriented Protocols-Byte Stuffing



Character-Oriented Protocols

Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.

Do stuffing for following frame



Q:1

Considering “f” as flag delimiter and “e” as DLE (escape) character, Apply the byte stuffing on the single frame data

five apples and four pears

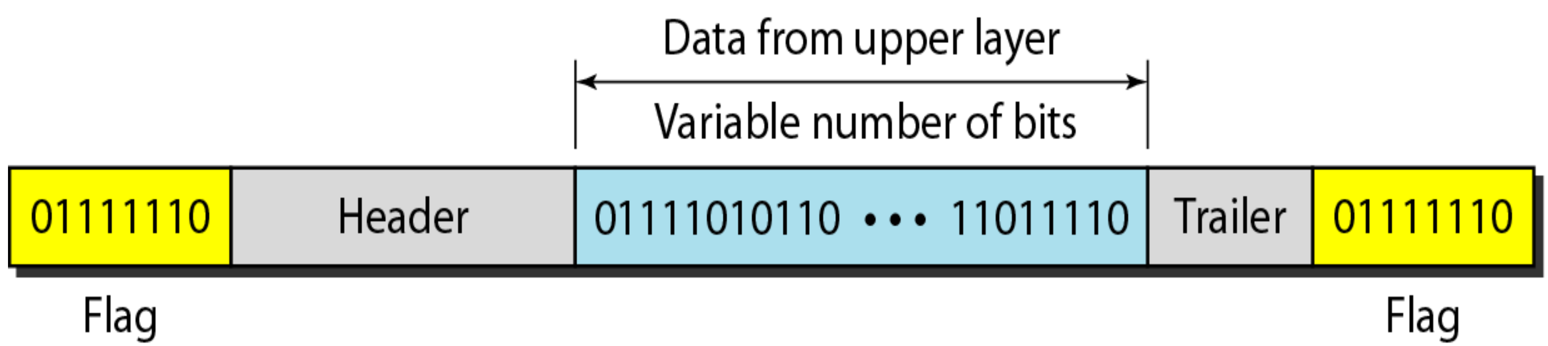
Ans:

fefivee applees and efour peearsf

Bit-Oriented Protocols

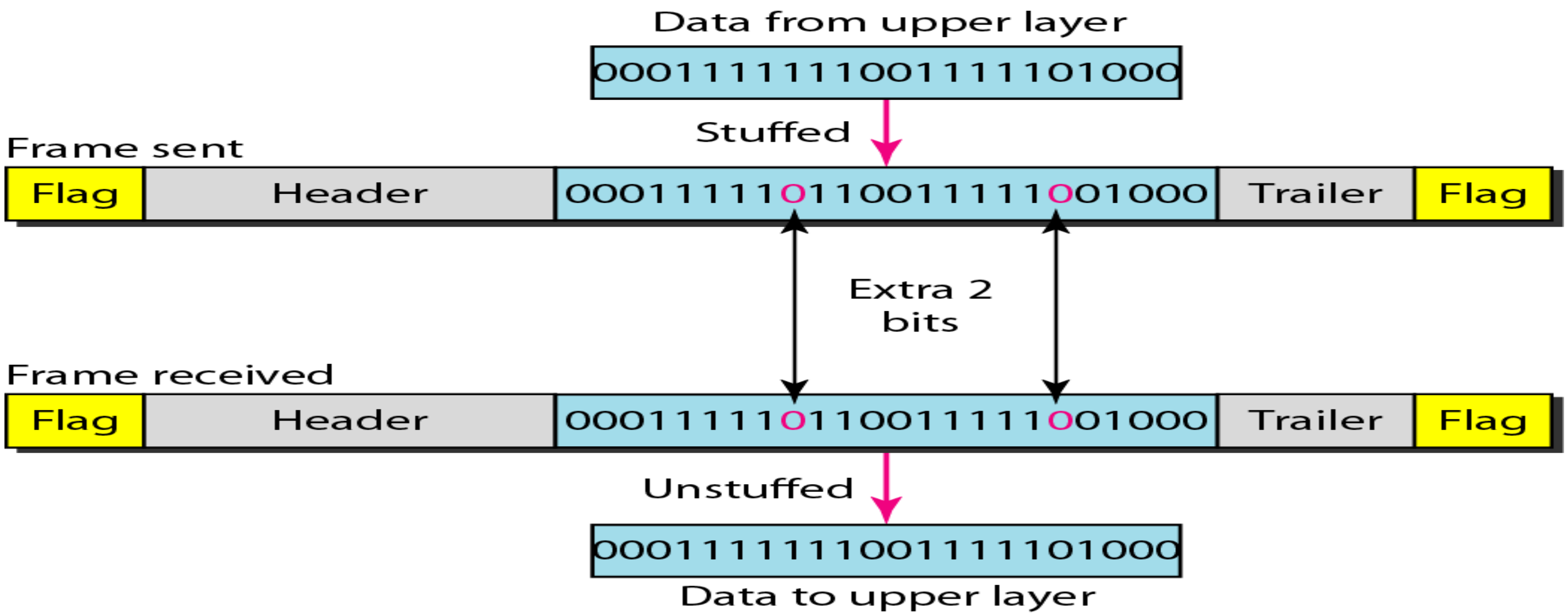
In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.

However, in addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other. Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame.



Bit-Oriented Protocols

- The data may contain the special bit-pattern from the upper layer.
- **Bit stuffing** is the process of adding one extra 0 whenever five(5) consecutive 1's, so that the receiver does not mistake the pattern 0111110 for a flag.



Bit-Oriented Protocols

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

Assume we send a frame of 2 8-bit characters:

01111111 01111101
char 1 char 2

sender rule is - if 5 1s in data add (stuff) a zero

On the line we will send:

Flag

start of frame end of frame

01111110 011111011 011111001 01111110 Flag
char 1 char 2

01111110 011111-11 011111-01 01111110
char 1 char 2

receiver rule is - if a zero occurs after 5 1s remove it

A bit-stuffing based framing protocol uses an 8-bit delimiter pattern of 01111110. If the output bit-string after stuffing is 01111100101, then the input bit-string is

(A) 0111110100

(B) 0111110101

(C) 0111111101

(D) 0111111111

The given delimiter pattern is 01111110. Delimiters are used to define the beginning and end of data.

Since delimiters are special bit-patterns used for special purposes, they must be avoided in the encoded form of the input data. To achieve this, Bit Stuffing is used.

On the sending side, any time five consecutive 1's have been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 delimiter sequence), the sender inserts a 0 before transmitting the next bit.

If the receiver gets five consecutive 1's, it makes its decision based on the next bit it sees (i.e., the bit following the five 1s).

If the next bit is a 0, it must have been stuffed, and so the receiver removes it.

If the next bit is a 1, then one of two things is true: Either this is the end-of-frame marker or an error has been introduced into the bit stream.

Going further and reading the next bit distinguishes these two cases. If the next bit is 0, then it is the end of frame marker (delimiter 01111110), and if the next bit is a 1 then there is must be an error in the frame and it is discarded.

So, For the data sequence 0111111101

Encoding would be – 011111**0**1101

Here the bold 0 is stuffed to distinguish it from the delimiter sequence.

Coming back to the question, the encoded string is – 01111100101 and when the receiver senses that it has received 5 consecutive 1's then

If the next bit is 0, then it is stuffed

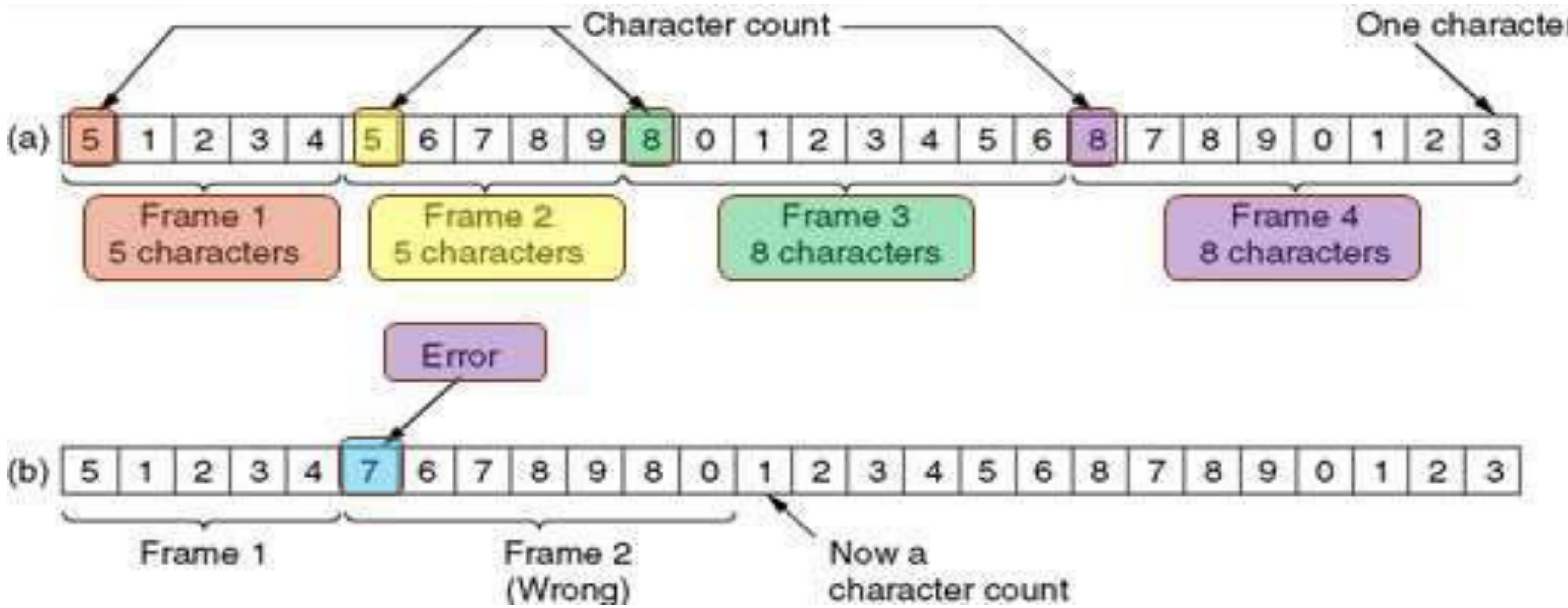
If the next bit is 1, then next to next bit would tell if the frame has ended or there is an error.

In this case, the next bit is 0 which means it was stuffed, so the corresponding input sequence is- 0111110101.

Therefore, option (B) is correct.

FRAMING – CHARACTER COUNT/Byte Count (Character Oriented)

- The framing method that uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is.



The trouble with this algorithm is that the count can be garbled by a transmission error.

Q:1 The following character encoding is used in a data link protocol:

A: 01000111;

B: 11100011;

FLAG: 01111110;

ESC: 11100000

A. Flag bytes with byte stuffing.

The following character encoding is used in a data link protocol:
A: 11010101; B: 10101001;
FLAG: 01111110;
ESC: 10100011

Show the bit sequence transmitted (in binary) for the five-character frame:
A ESC B ESC FLAG
when each of the following framing methods are used:
(a) Flag bytes with byte stuffing.
(b) Starting and ending flag bytes, with bit stuffing.

Ans: A **01111110** 11010101 10100011 10100011 10101001 10100011 10100011 10100011 01111110 **01111110**

Ans:B **01111110** 11010101 10100011 10101001 10100011 011111**0**10 **01111110**