Introduction

Computer Network

- **Computer Network** is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.

- The aim of the computer network is the sharing of resources among various devices.

Networking Elements

- At least two computers
- Transmission medium either wired or wireless
- Protocols or rules that govern the communication
- Network software such as Network Operating System

Components of Computer Network

- Hub
- Repeater
- Switch
- Router
- Cables

Architecture

- Peer-To-Peer network
- Client/Server network

Network Types

- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

Internetworking

- Intranet
- Internet

Transmission Mode

The way in which data is transmitted from one device to another device is known as **transmission mode**.

- Simplex mode
- Half-duplex mode
- Full-duplex mode

Topology

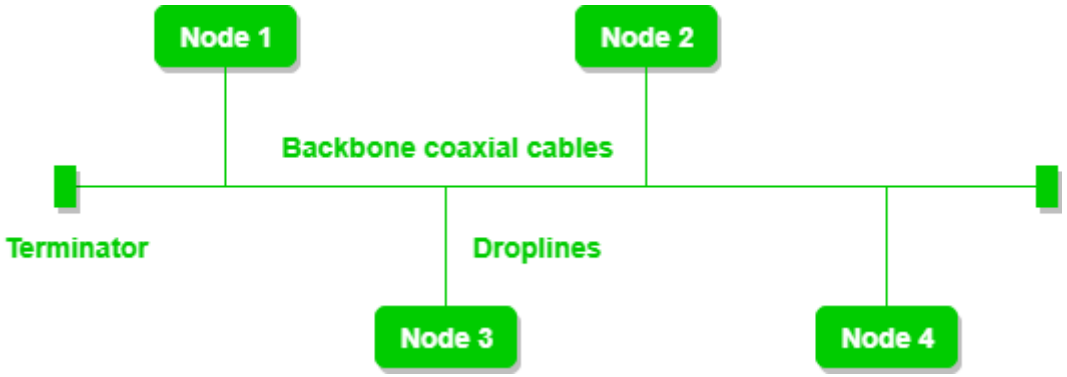
Topology defines the structure of the network of how all the components are interconnected to each other.

Types of Topology

- Bus
- Ring
- Star
- Mesh

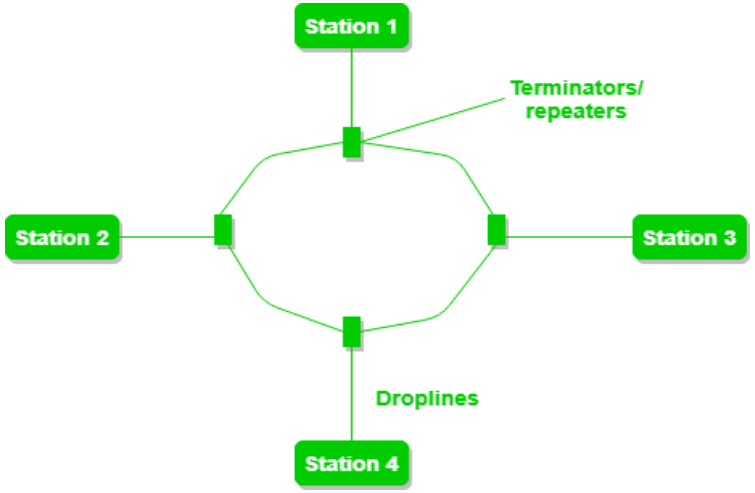
Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable



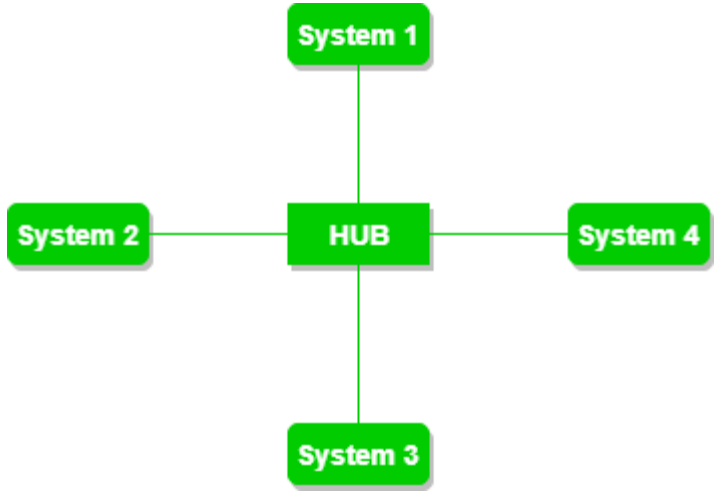
Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.



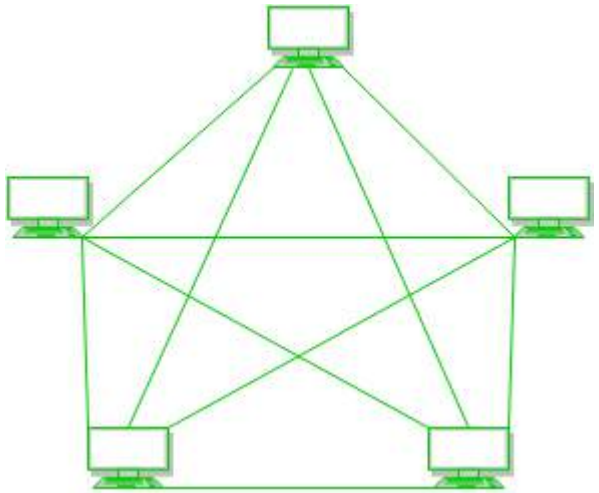
Star Topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.



Mesh Topology

- In a mesh topology, every device is connected to another device via a particular channel.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.

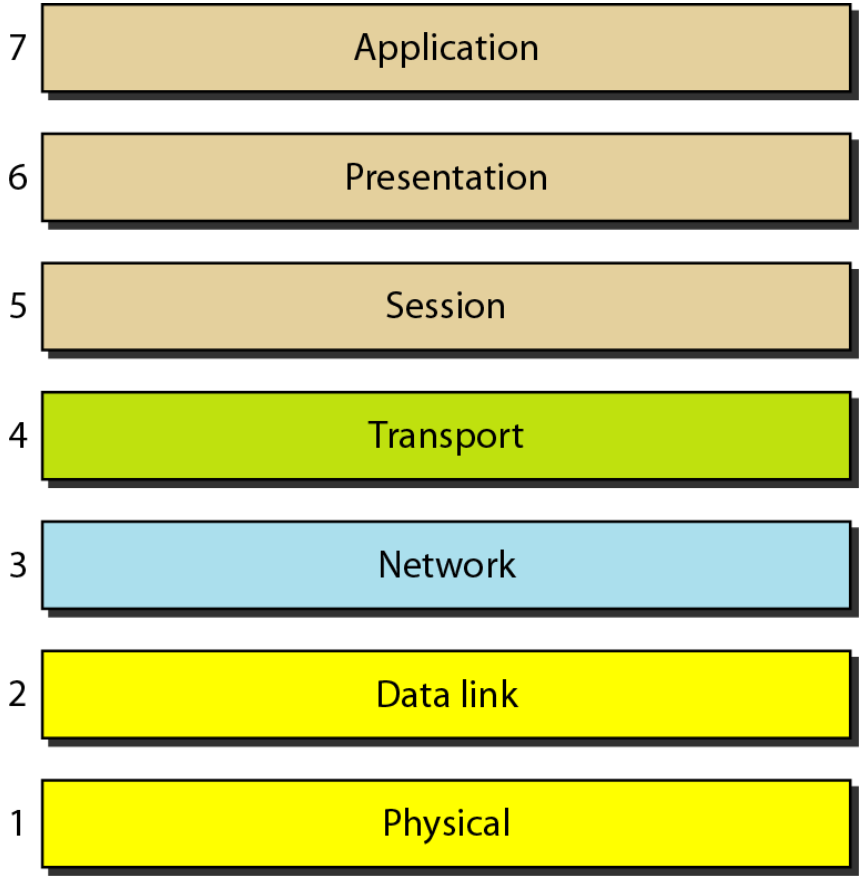


OSI Model

OSI

- OSI stands for **Open Systems Interconnection**.
- It has been developed by ISO – '**International Organization for Standardization**'.
- It is a 7 layer architecture with each layer having specific functionality to perform.
  - Outlines **WHAT** needs to be done to send data from one computer to another.
  - Not **HOW** it should be done.
  - Protocols stacks handle how data is prepared for transmittal (to be transmitted)

Seven Layers of the OSI model

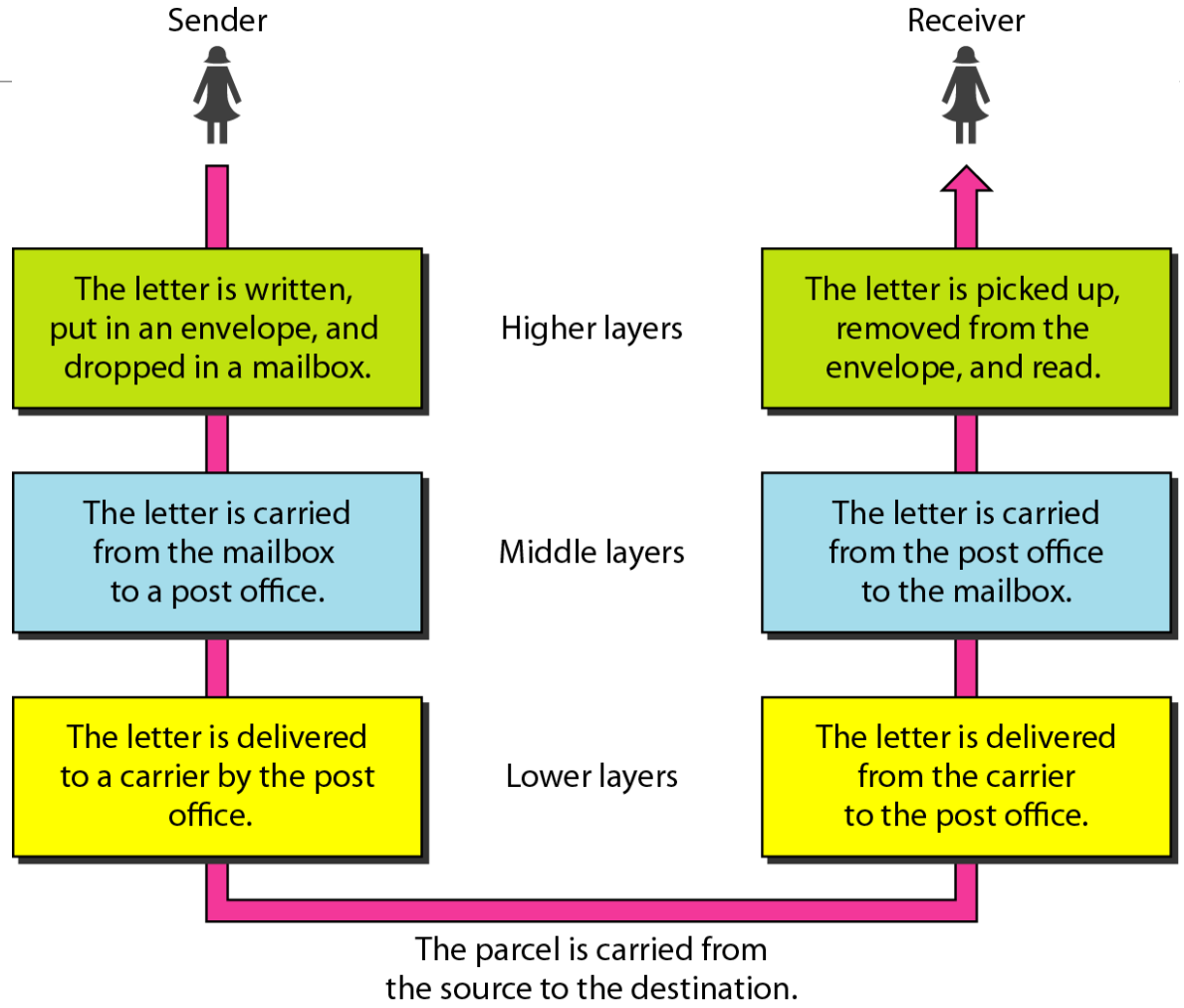


Why a layered model?

- Easier to teach communication process.
- Speeds development, changes in one layer does not affect how the other levels works.
- Standardization across manufactures.
- Allows different hardware and software to work together.
- Reduces complexity

LAYERED TASKS

Tasks involved in sending a letter



What is “THE MODEL?”

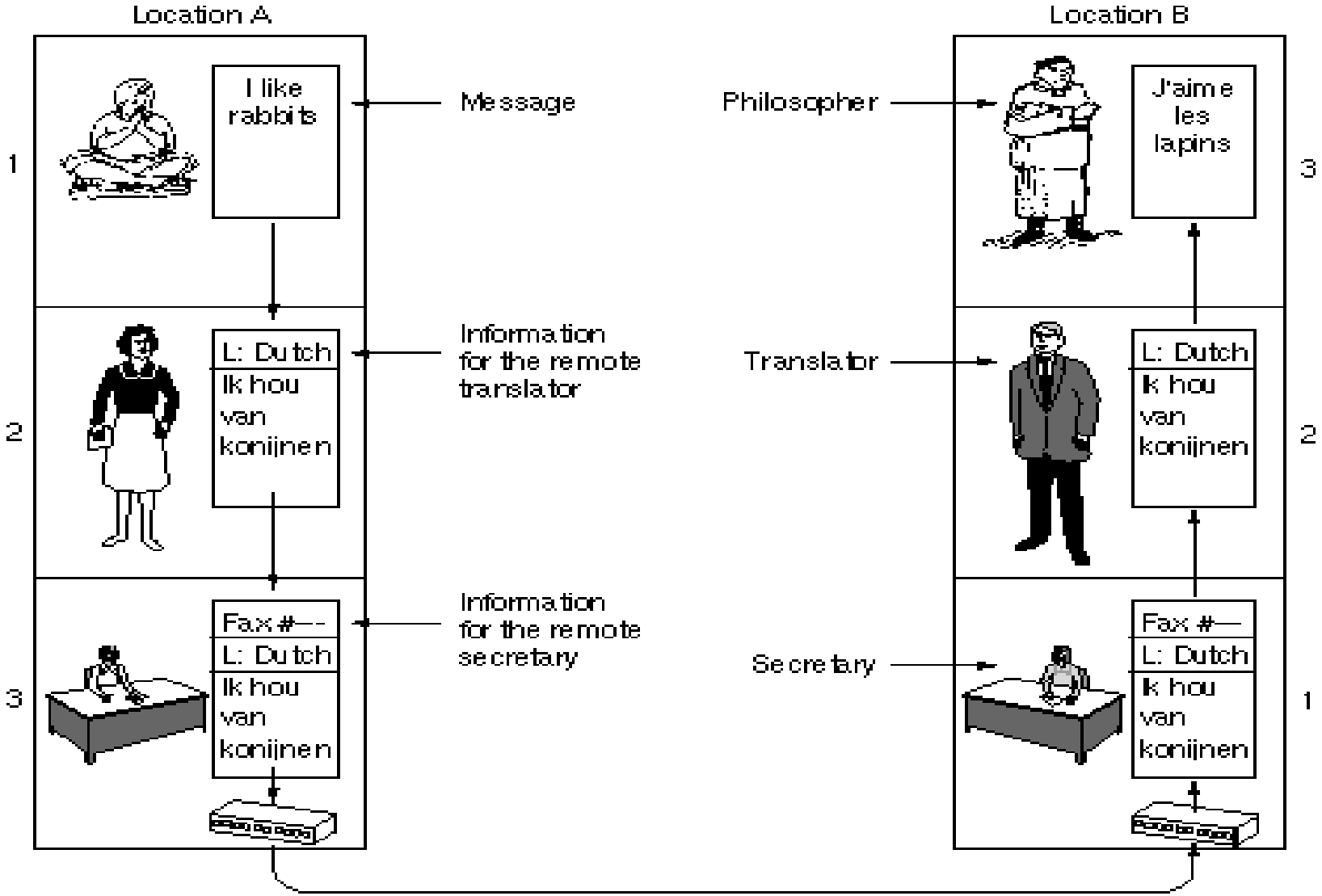
- Commonly referred to as the OSI reference model.

- The OSI model
  - is a theoretical blueprint that helps us understand how data gets from one user’s computer to another.
  - It is also a model that helps develop standards so that all of our hardware and software talks nicely to each other.

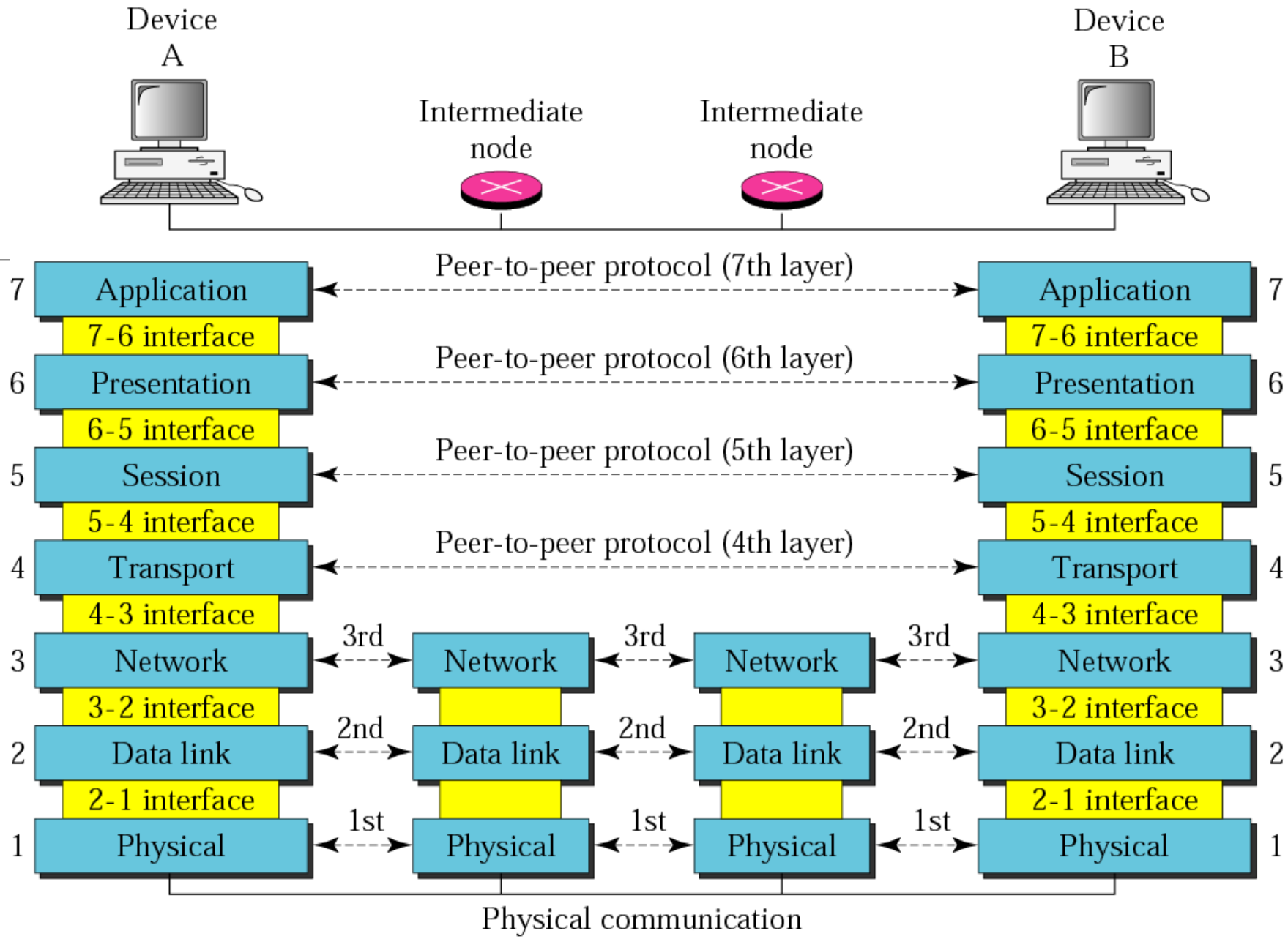
Why use a reference model?

- Serves as an outline of rules for how protocols can be used to allow communication between computers.
- Each layer has its own function and provides support to other layers.

PHILOSOPHER TRANSLATOR SECRETARY ARCHITECTURE



OSI Model


Device A
Intermediate node
Intermediate node
Device B
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

Networking Devices

Networking Devices

- Hub
- Repeater
- Switch
- Router

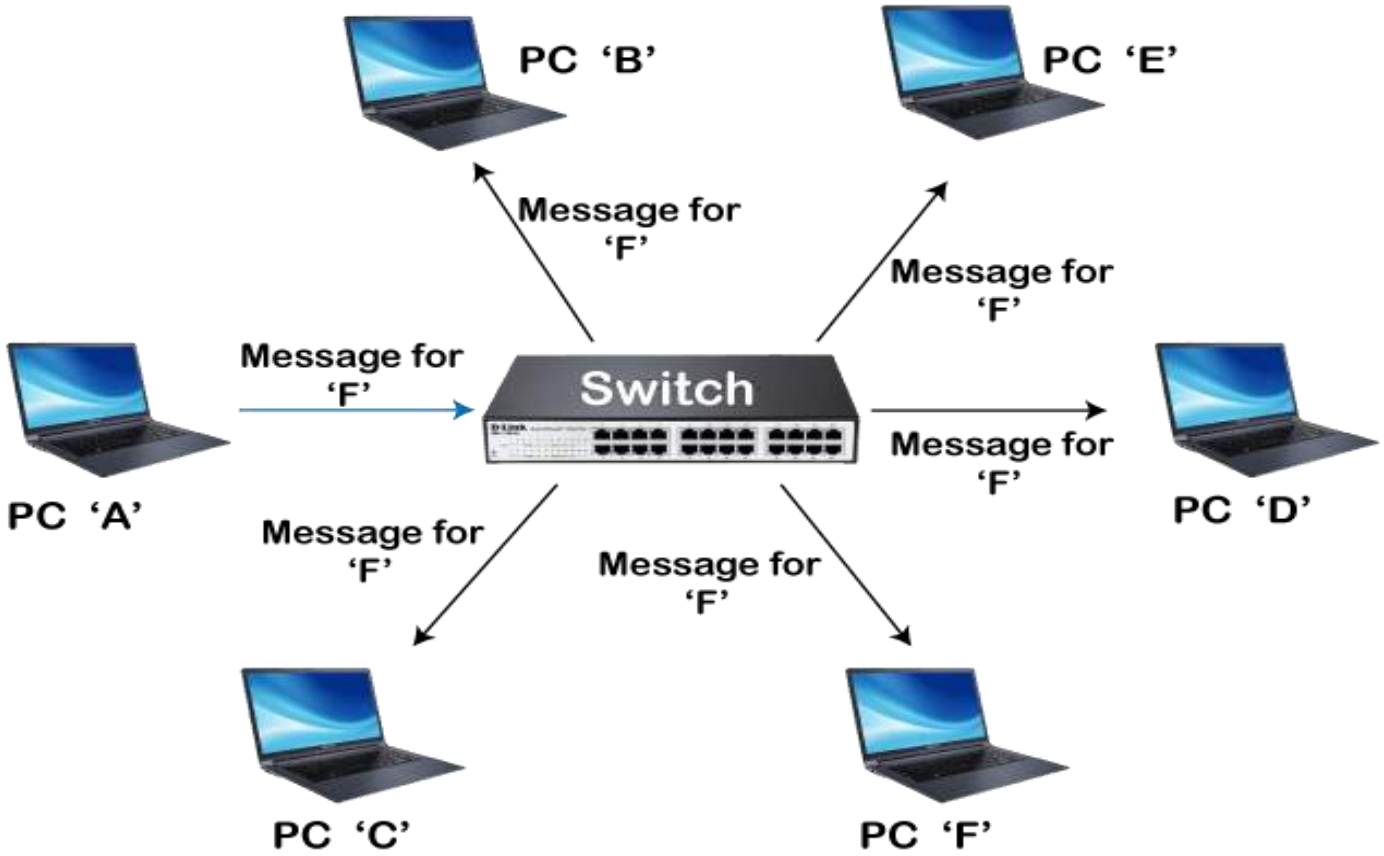
Switch

- A switch is a multicast networking device that works under the Datalink layer of the OSI model and connects a bunch of computers or devices in a network.

- a switch acts as the central interconnecting device that connects all the devices of a network in order to ensure proper resource sharing.

- Basically, in a network, all the end devices like a computer printer, servers, etc. are connected through the switch

Switch


PC 'B'
PC 'E'
Message for 'F'
Message for 'F'
Message for 'F'
Switch
Message for 'F'
PC 'A'
PC 'D'
Message for 'F'
Message for 'F'
PC 'C'
PC 'F'

Router

A Router is a networking device that operates under the network layer of the OSI model and is used to connect two or more networks.

A router is a device that is used to interconnect various switches of different networks to form even a wider network

Switch & Router

Switch works on the data link layer of the OSI model.

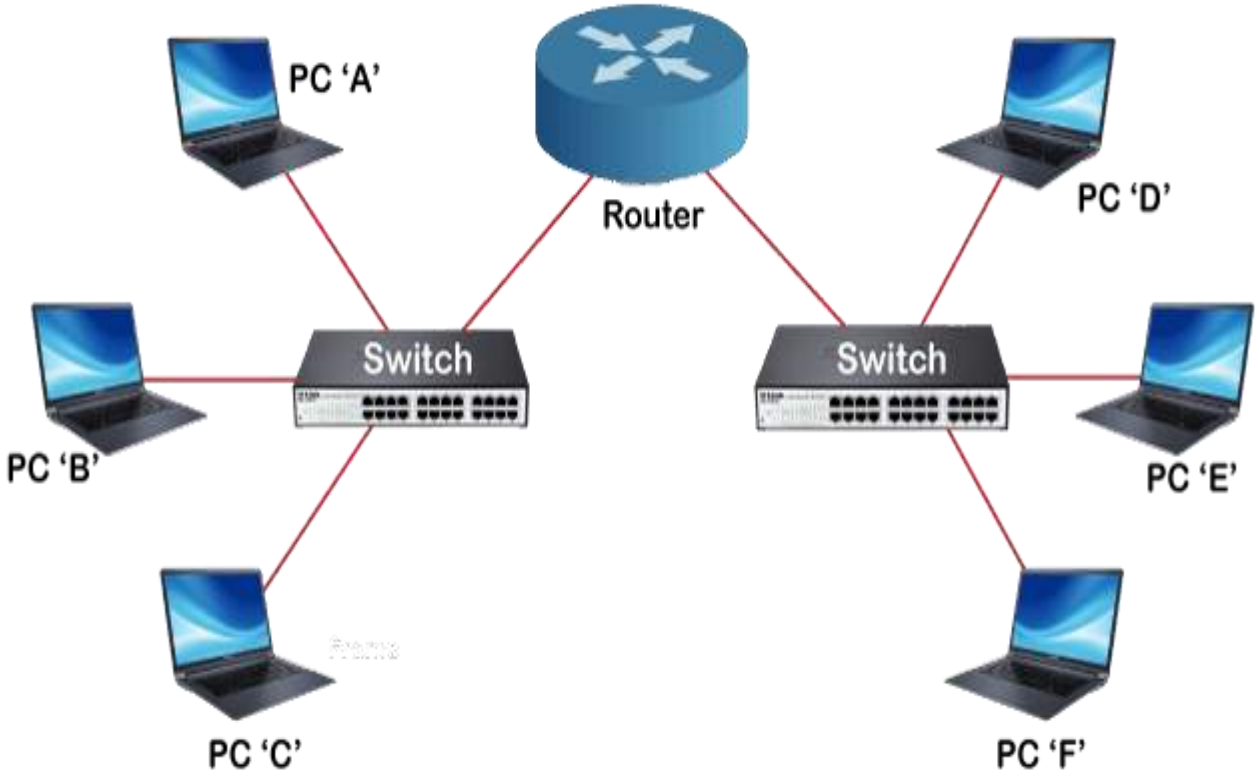
The Router works on the network layer of the OSI model

Switch can join multiple devices within one LAN.

A Router can link both LAN as well as WAN.

Switch works based on the MAC address,

Router works based on IP address.



Connection of networks through Router

Network Addressing

Address

- MAC Address
- IP Address

MAC

A **Media Access Control (MAC)** address is a 48-bit (6 bytes) address that is used for communication between two hosts in an Ethernet environment.

It is a hardware address, which means that it is stored in the firmware of the network card (NIC).

MAC addresses are usually written in the form of 12 hexadecimal digits. For example, consider the following MAC address:

D8-D3-85-EB-12-E3

How to find out your own MAC address?

IP Address

An IP address is a 32-bit number that identifies a host on a network

An IP address is usually written in the form of four decimal numbers separated by periods (.)

Example

10.2.3.4

How to find out your IP address?

- Using CMD
- Using Google

Private IP address of a system is the IP address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

Public IP address of a system is the IP address which is used to communicate outside the network. Public IP address is basically assigned by the ISP.

Private addresses ranges

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Which information can we get from IP Address?

https://viewdns.info/

https://www.whatismyip.com/

https://whois.domaintools.com/

https://www.whois.com/whois/

182.73.197.20 (VIT)

182.72.39.10

182.72.39.9

Network Addressing

Address

- MAC Address
- IP Address

MAC

A **Media Access Control (MAC)** address is a 48-bit (6 bytes) address that is used for communication between two hosts in an Ethernet environment.

It is a hardware address, which means that it is stored in the firmware of the network card (NIC).

MAC addresses are usually written in the form of 12 hexadecimal digits. For example, consider the following MAC address:

D8-D3-85-EB-12-E3

How to find out your own MAC address?

IP Address

An IP address is a 32-bit number that identifies a host on a network

An IP address is usually written in the form of four decimal numbers separated by periods (.)

Example

10.2.3.4

How to find out your IP address?

- Using CMD
- Using Google

Private IP address of a system is the IP address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

Public IP address of a system is the IP address which is used to communicate outside the network. Public IP address is basically assigned by the ISP.

Private addresses ranges

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Which information can we get from IP Address?

https://viewdns.info/

https://www.whatismyip.com/

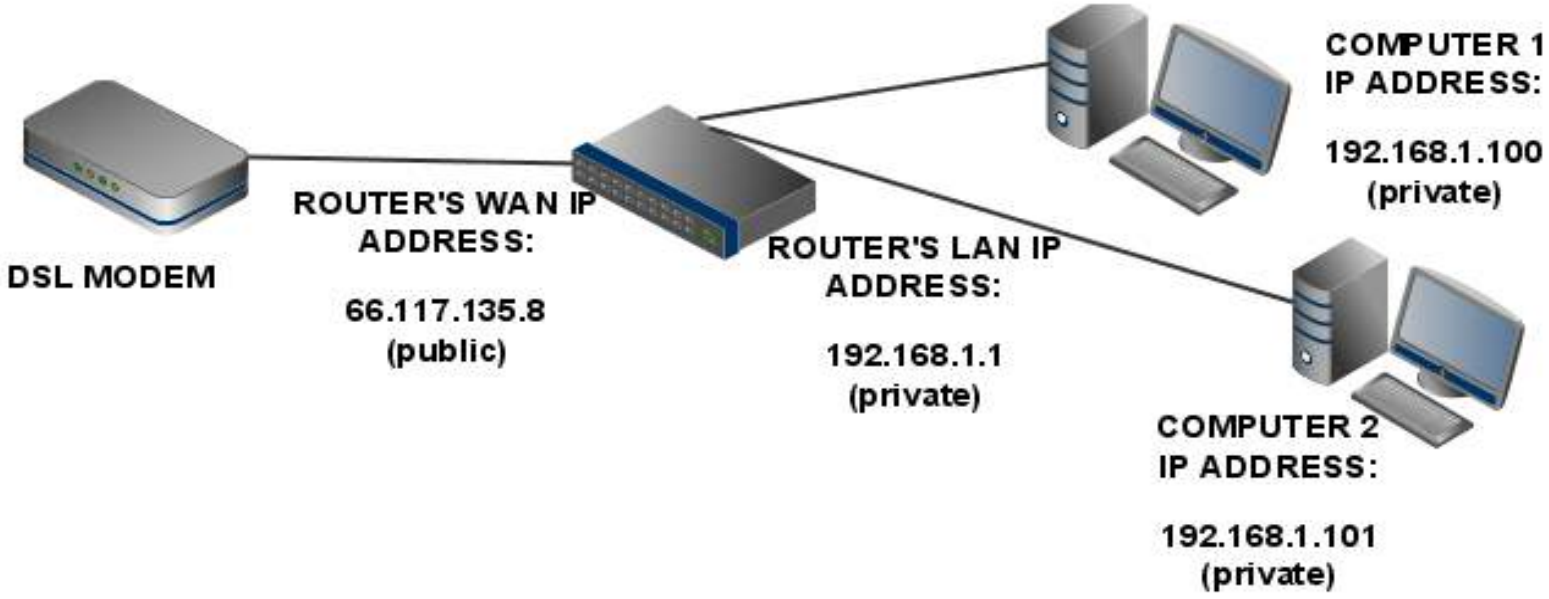
https://whois.domaintools.com/

https://www.whois.com/whois/

182.73.197.20 (VIT)

182.72.39.10

182.72.39.9


DSL MODEM
ROUTER'S WAN IP ADDRESS:
66.117.135.8
(public)
ROUTER'S LAN IP ADDRESS:
192.168.1.1
(private)
COMPUTER 1 IP ADDRESS:
192.168.1.100
(private)
COMPUTER 2 IP ADDRESS:
192.168.1.101
(private)

How to map from Private Address to Public and vice versa?

Network Address Translation (NAT)

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access.

Default Gateway

Default Gateway: is an intermediate device between the local network and Global Network.

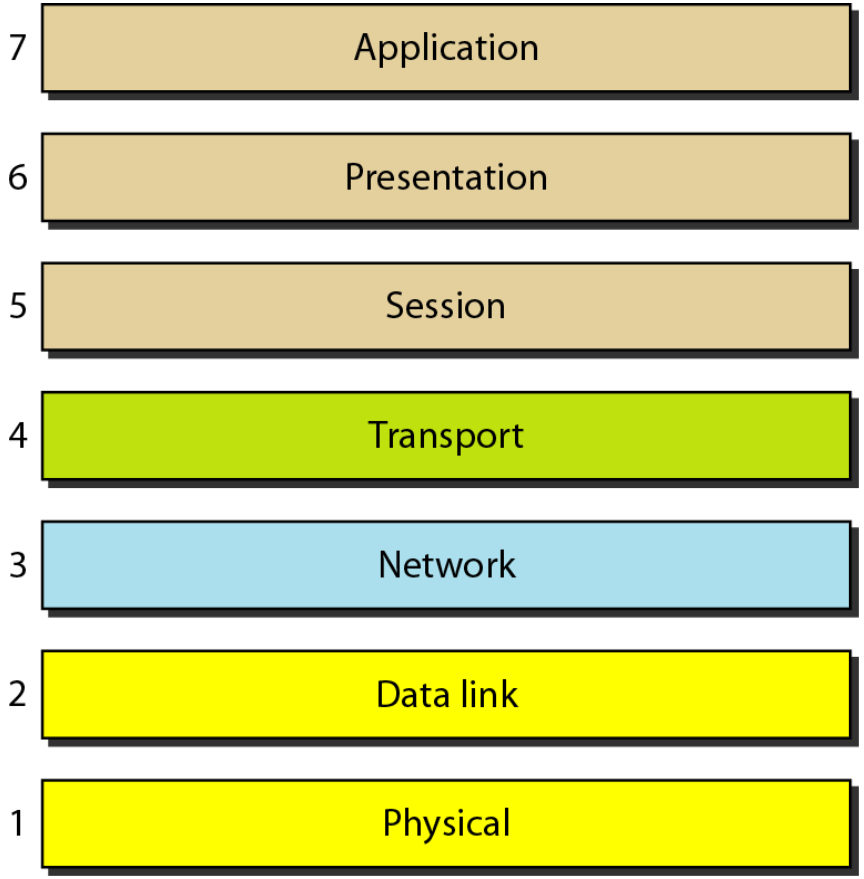
CMD: Tracert <Domain/IP>

OSI Model

OSI

- OSI stands for **Open Systems Interconnection**.
- It has been developed by ISO – '**International Organization for Standardization**'.
- It is a 7 layer architecture with each layer having specific functionality to perform.
  - Outlines **WHAT** needs to be done to send data from one computer to another.
  - Not **HOW** it should be done.
  - Protocols stacks handle how data is prepared for transmittal (to be transmitted)

Seven Layers of the OSI model

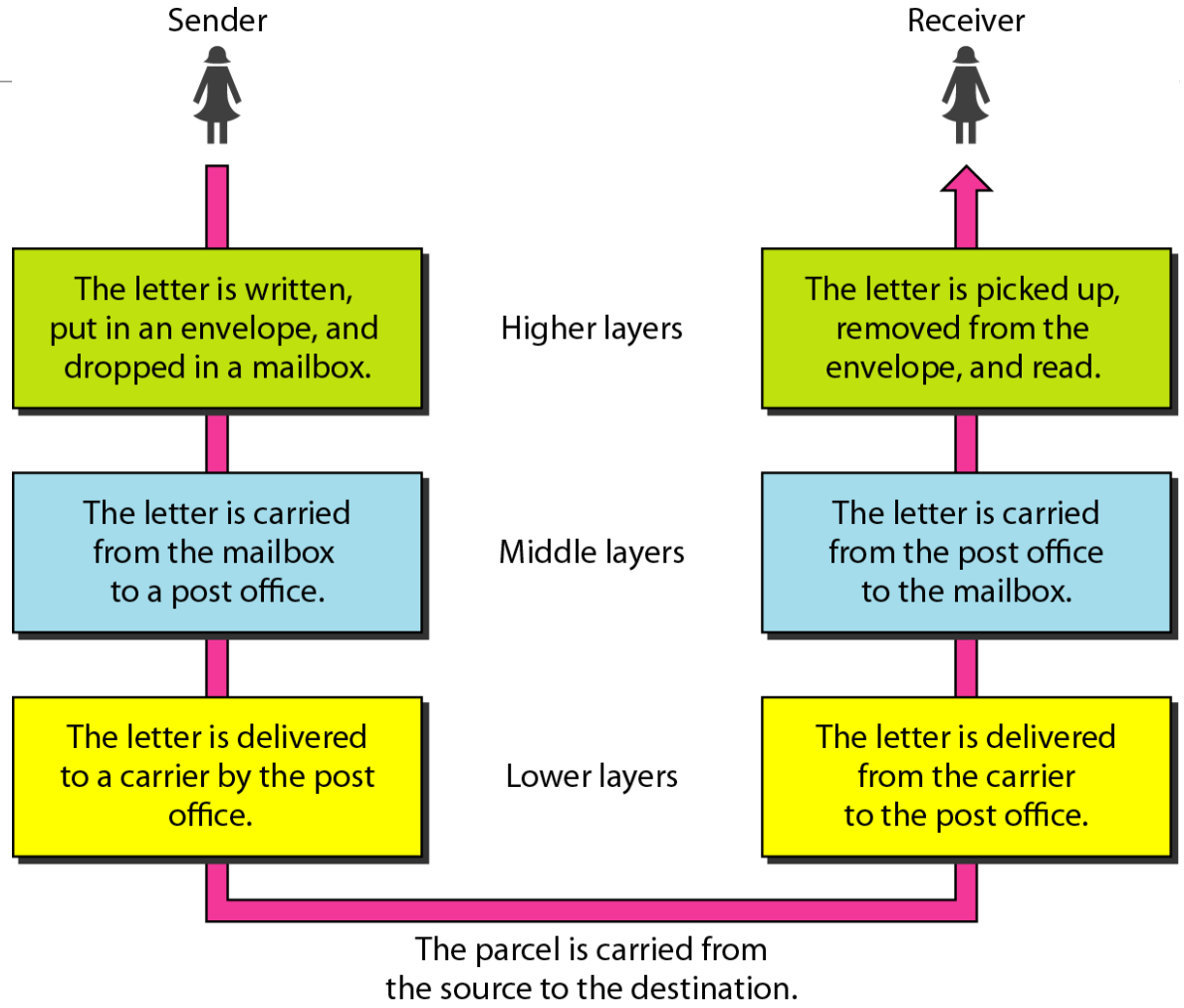


Why a layered model?

- Easier to teach communication process.
- Speeds development, changes in one layer does not affect how the other levels works.
- Standardization across manufactures.
- Allows different hardware and software to work together.
- Reduces complexity

LAYERED TASKS

Tasks involved in sending a letter



What is “THE MODEL?”

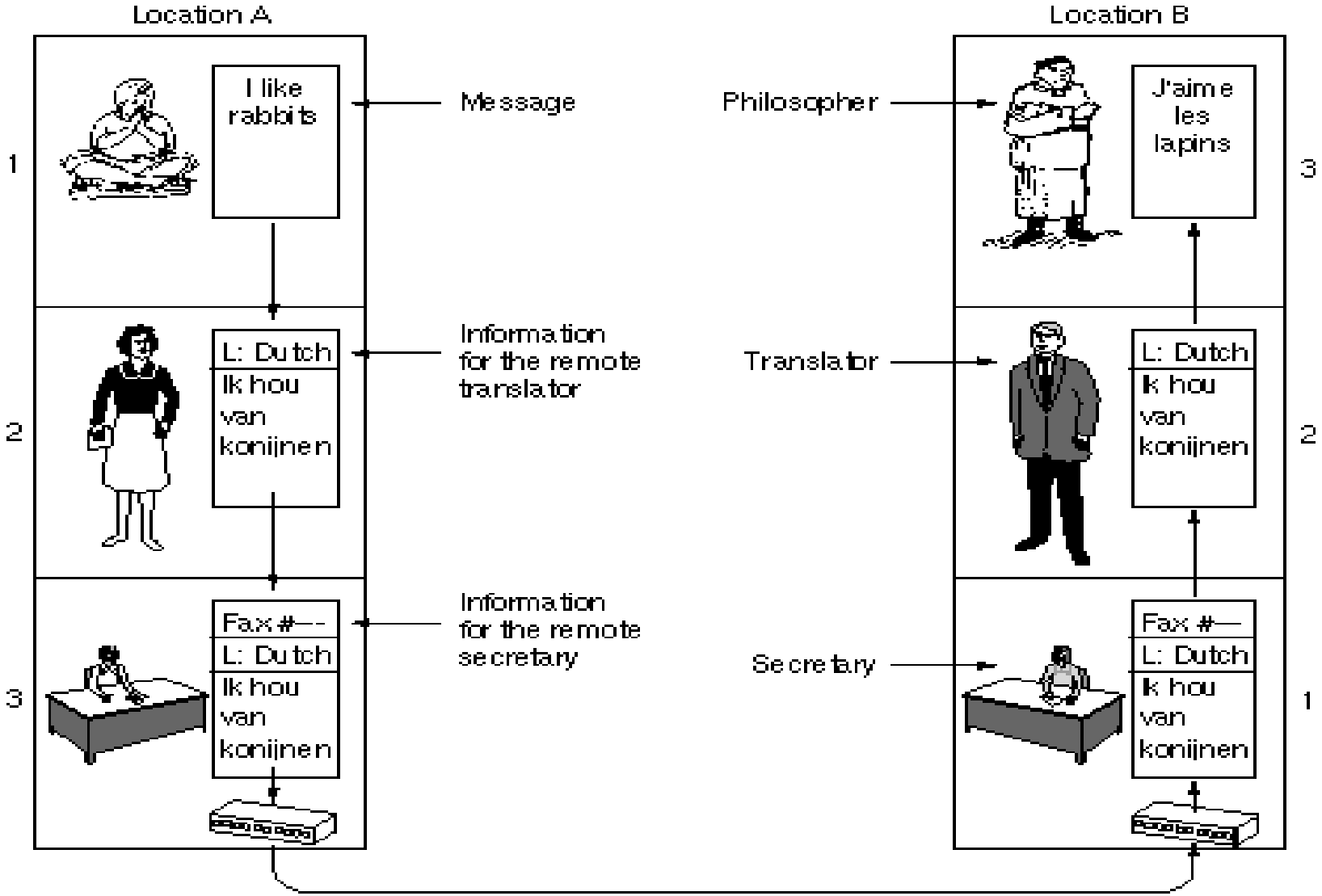
- Commonly referred to as the OSI reference model.

- The OSI model
  - is a theoretical blueprint that helps us understand how data gets from one user’s computer to another.
  - It is also a model that helps develop standards so that all of our hardware and software talks nicely to each other.

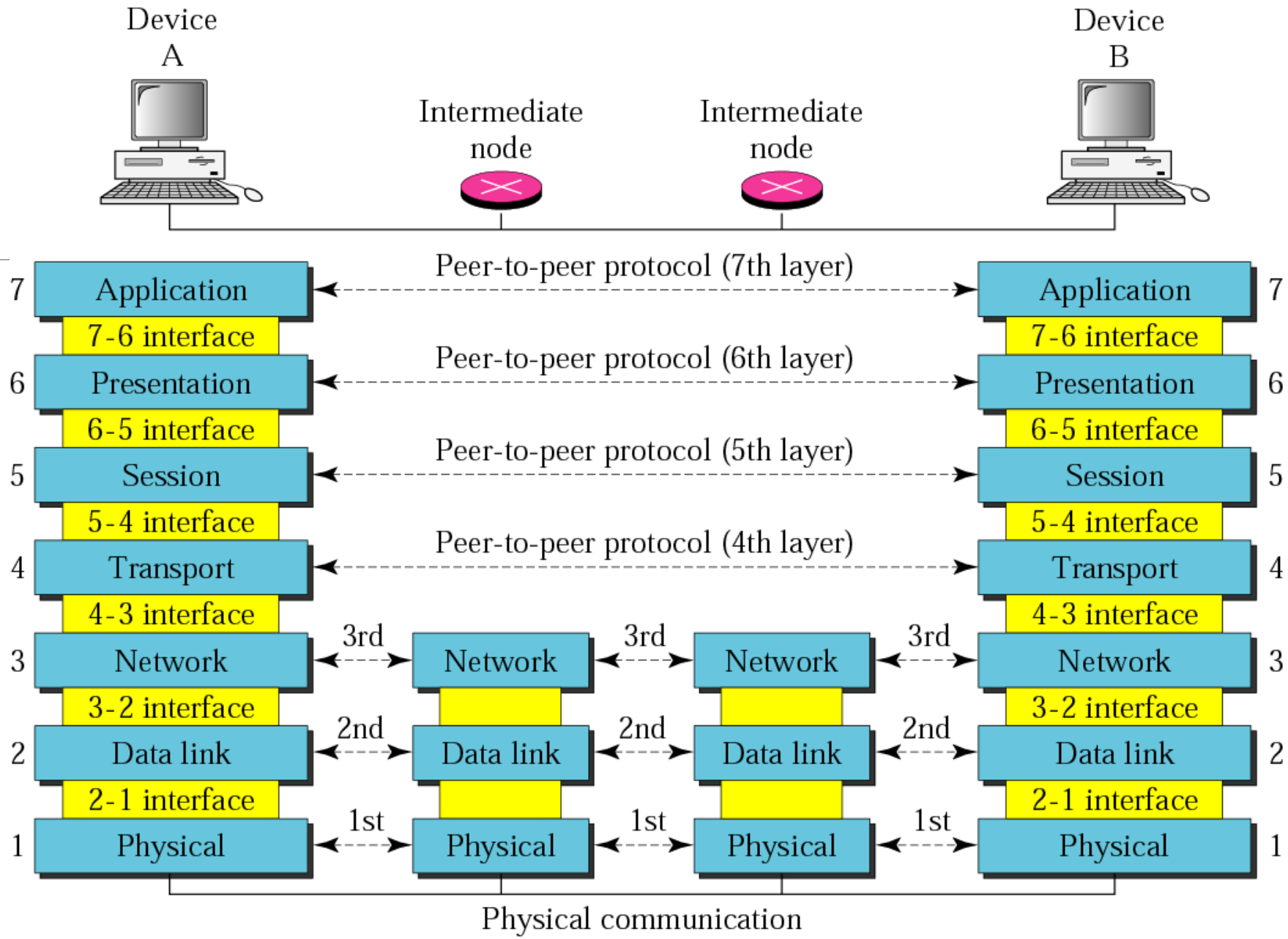
Why use a reference model?

- Serves as an outline of rules for how protocols can be used to allow communication between computers.
- Each layer has its own function and provides support to other layers.

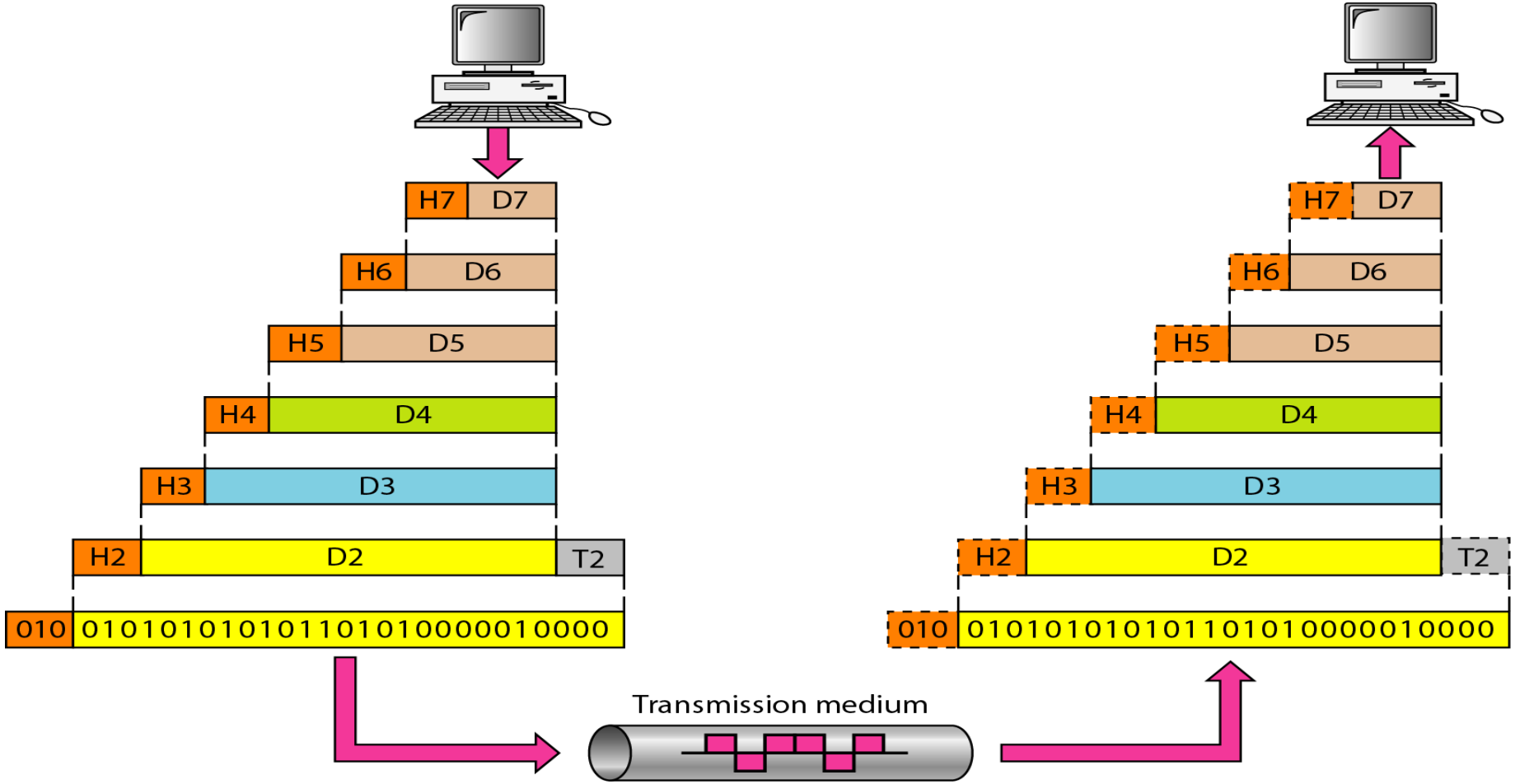
PHILOSOPHER TRANSLATOR SECRETARY ARCHITECTURE



OSI Model


Device A
Intermediate node
Intermediate node
Device B
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

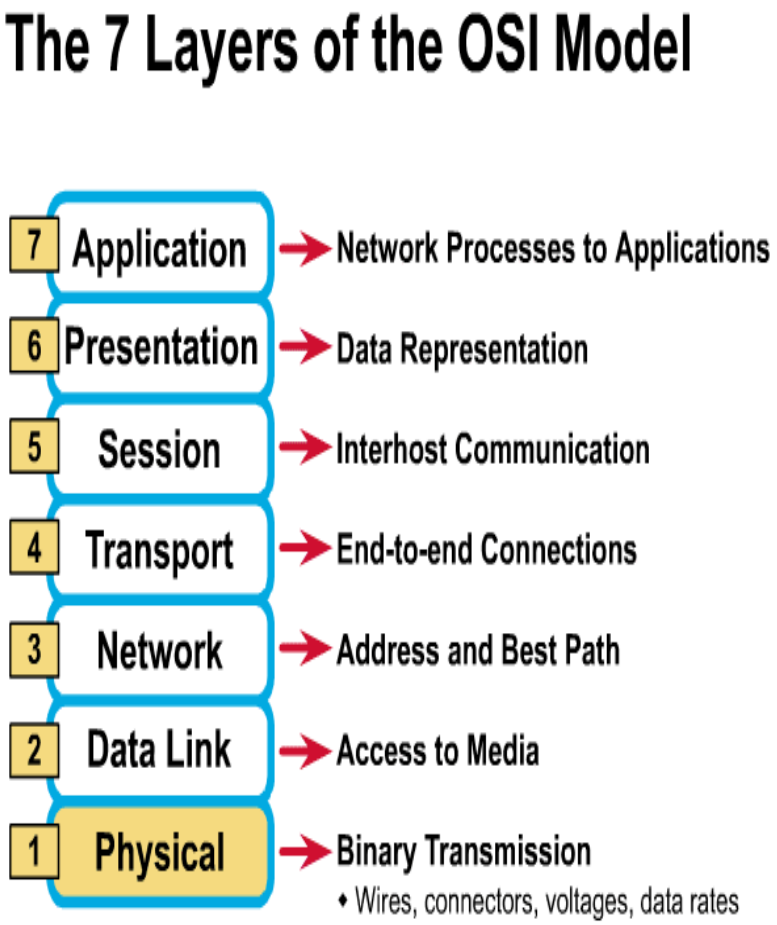
An exchange using the OSI model



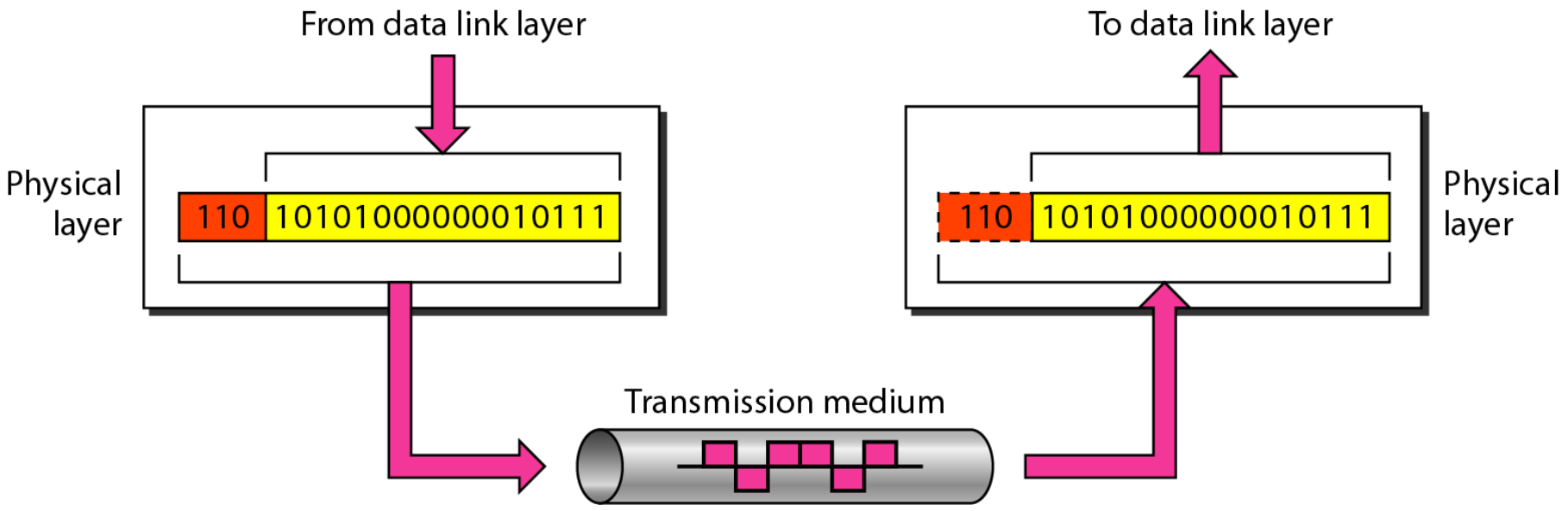
Physical Layer

Determines the specs for all physical components

- Cabling
- Physical topology
- Representation of bits
- Electrical properties
- Transmission mode



Physical layer

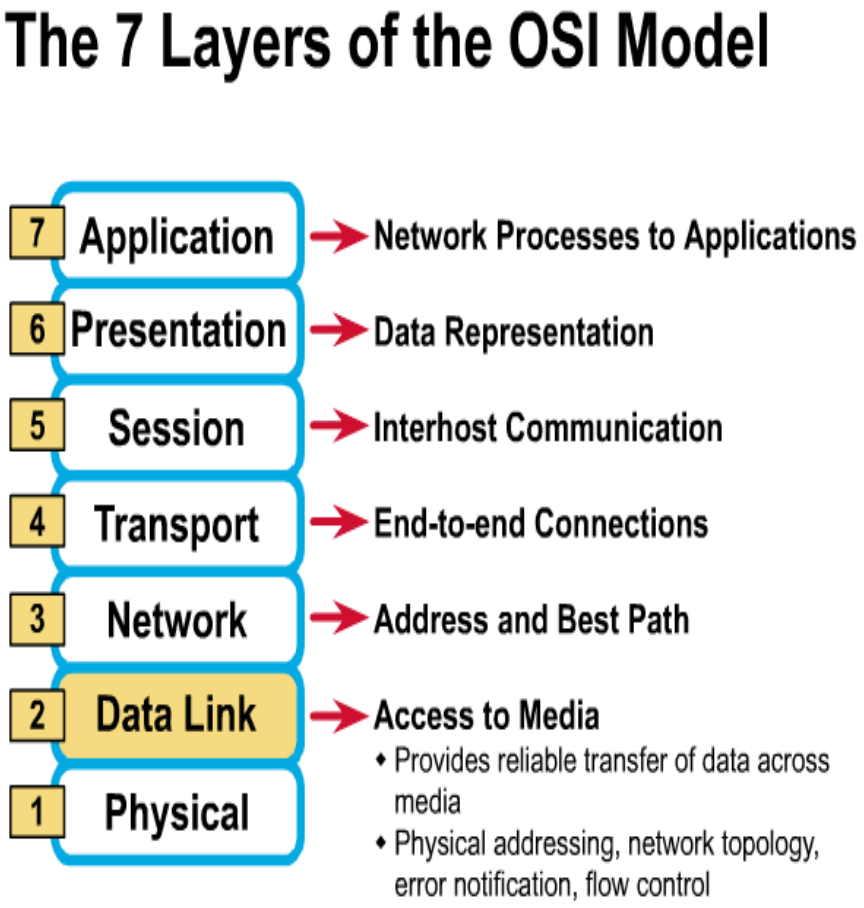


Note

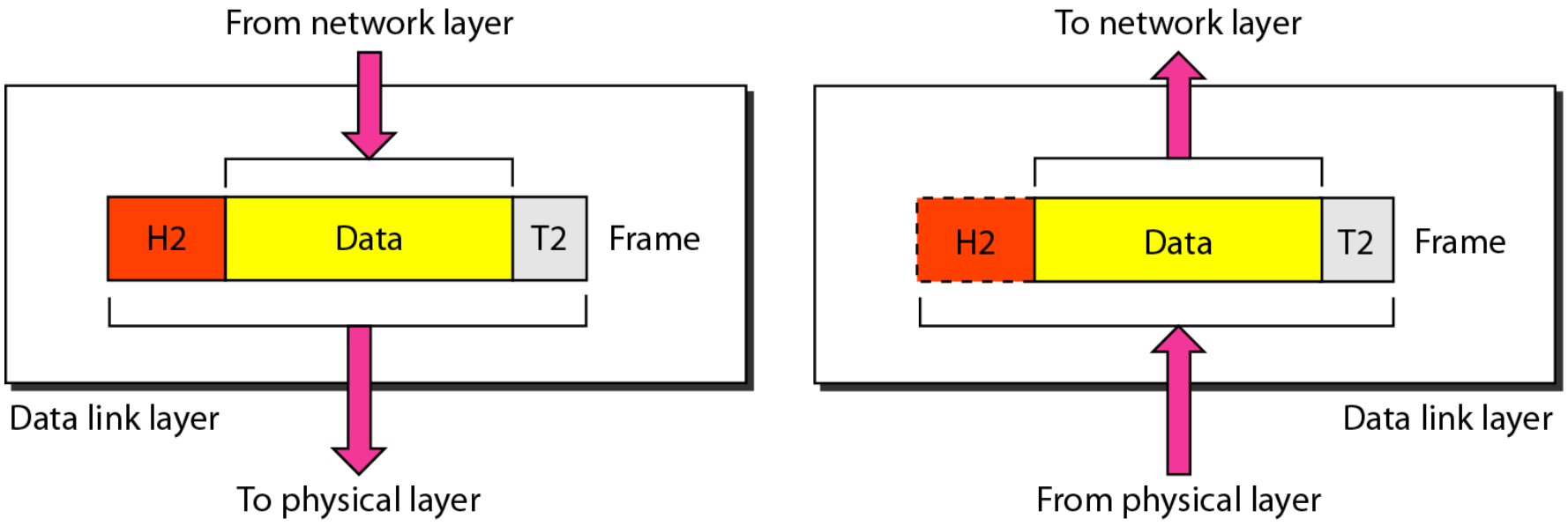
The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Data Link Layer

- Physical Addressing
- Flow control
- Error control



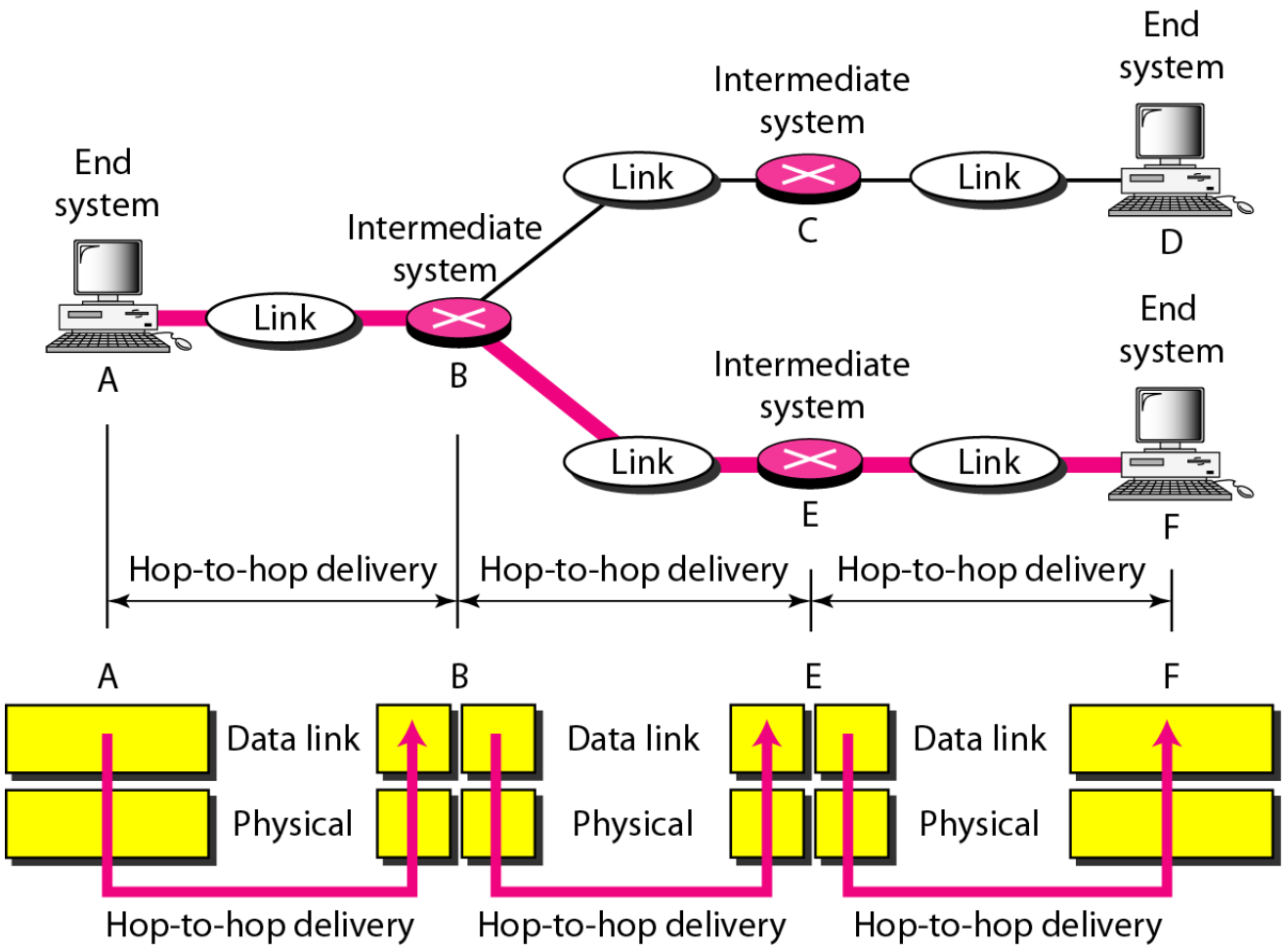
Data link layer



Note

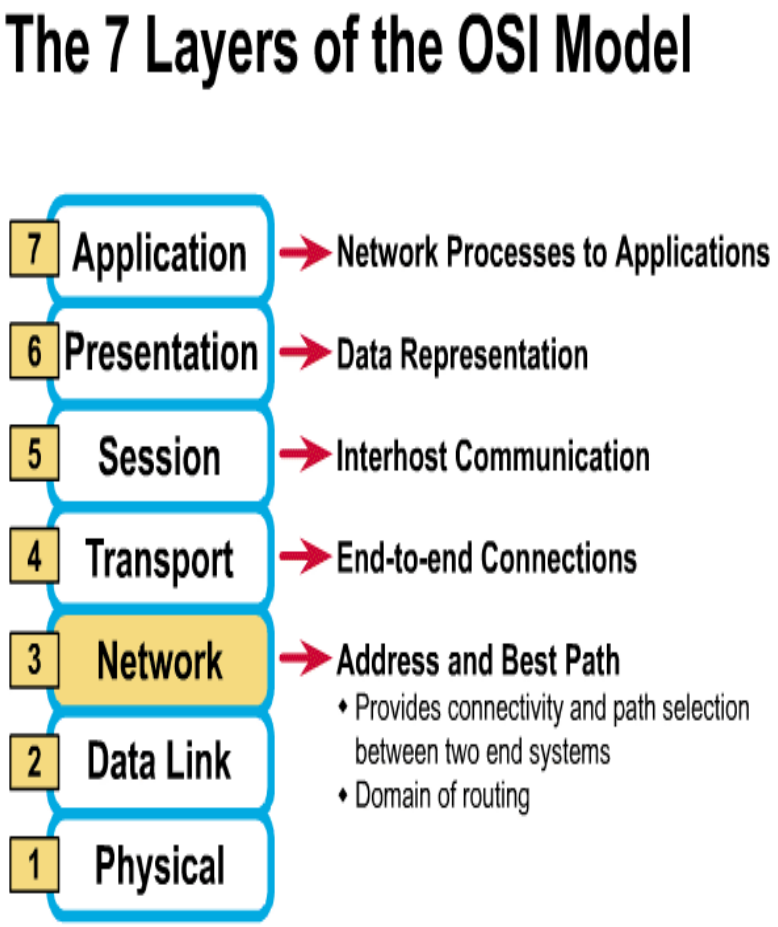
The data link layer is responsible for moving frames from one hop (node) to the next.

Hop-to-hop delivery

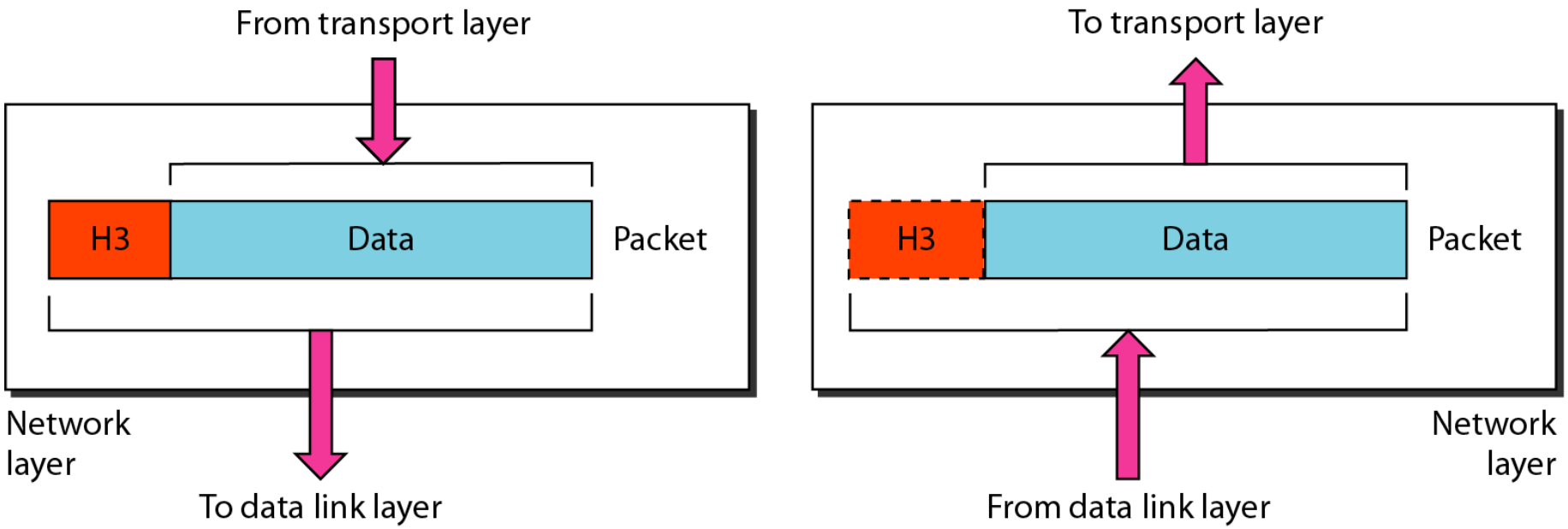


Network Layer

- Logical Addressing
- Routing



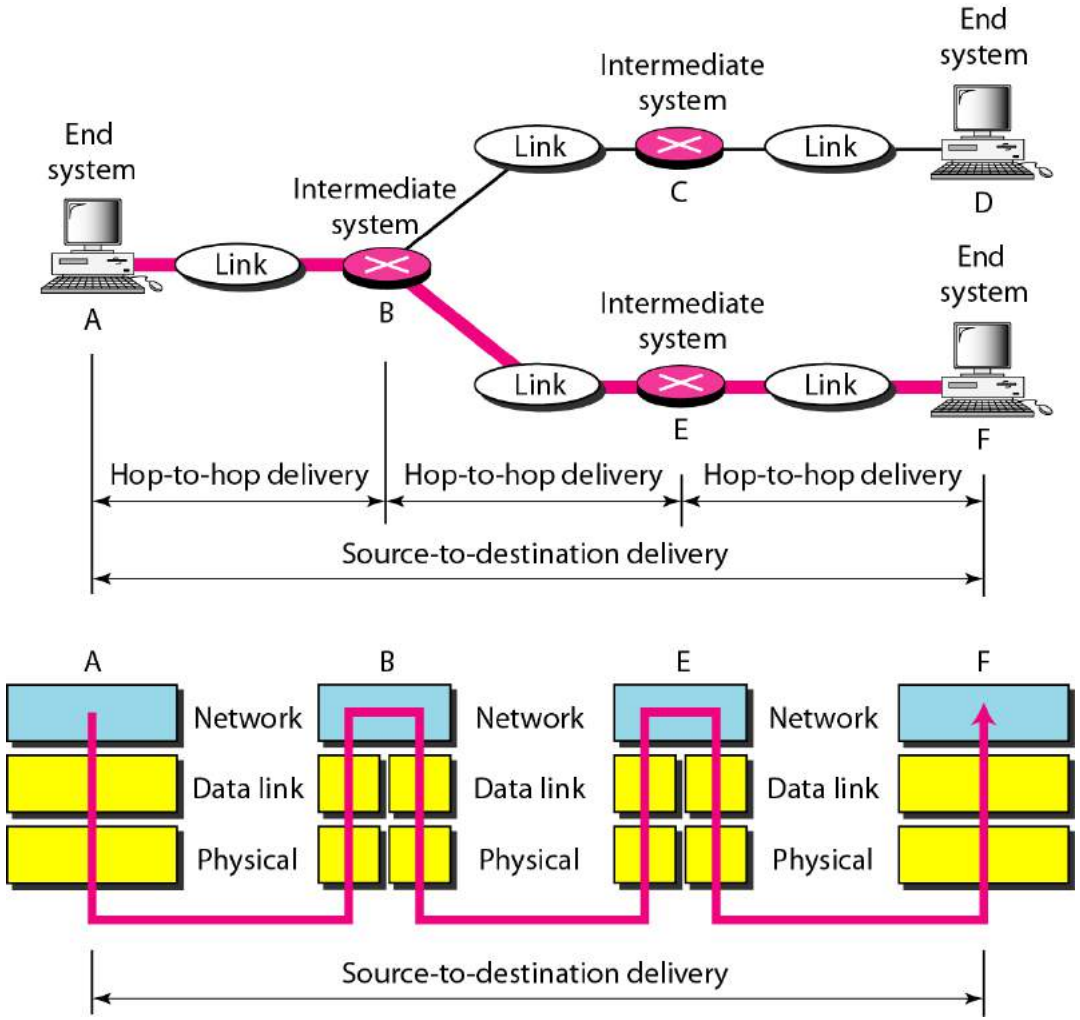
Network layer



Note

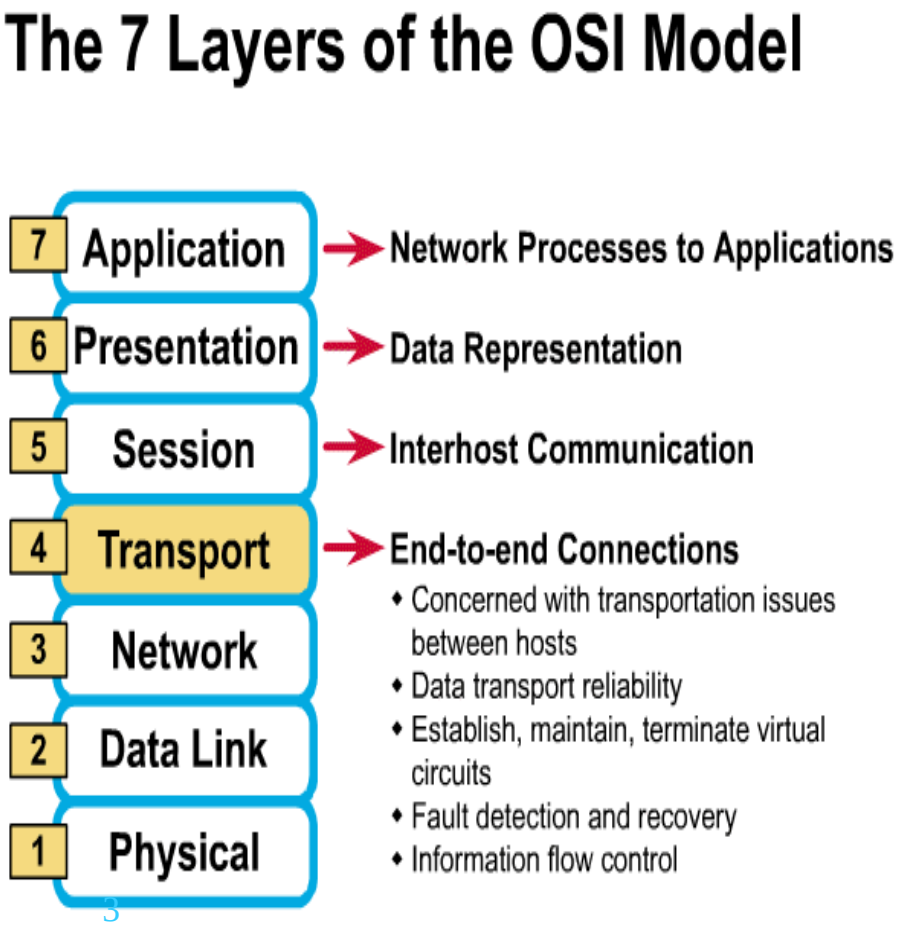
The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Source-to-destination delivery

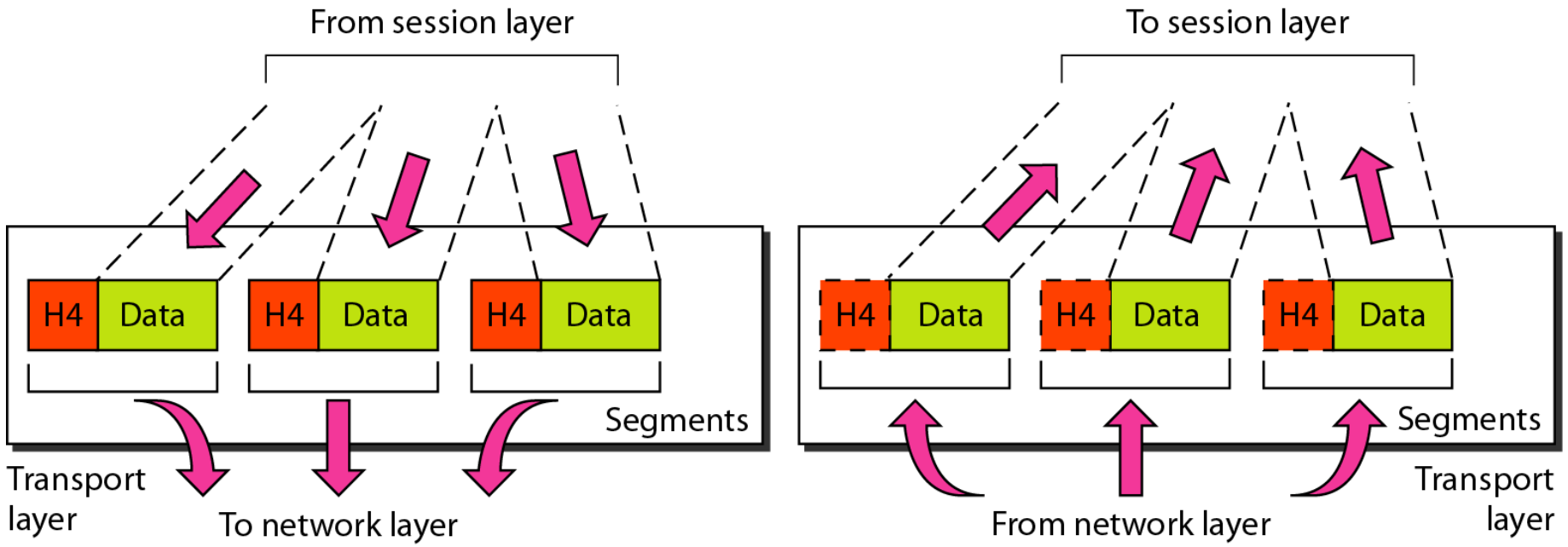


Transport Layer

- Service Point Addressing
- Segment and reassembly
- Flow Control
- Error Control
- Connection Control



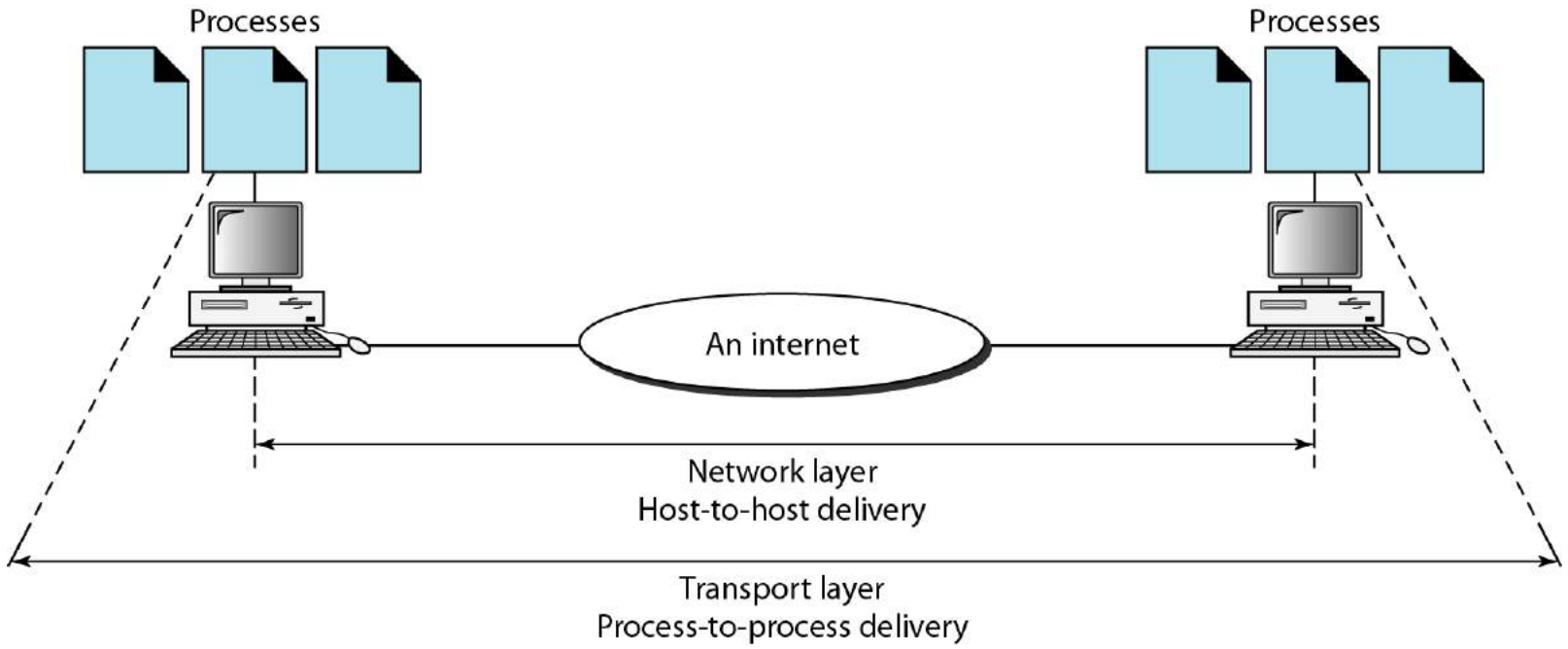
Transport layer



Note

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

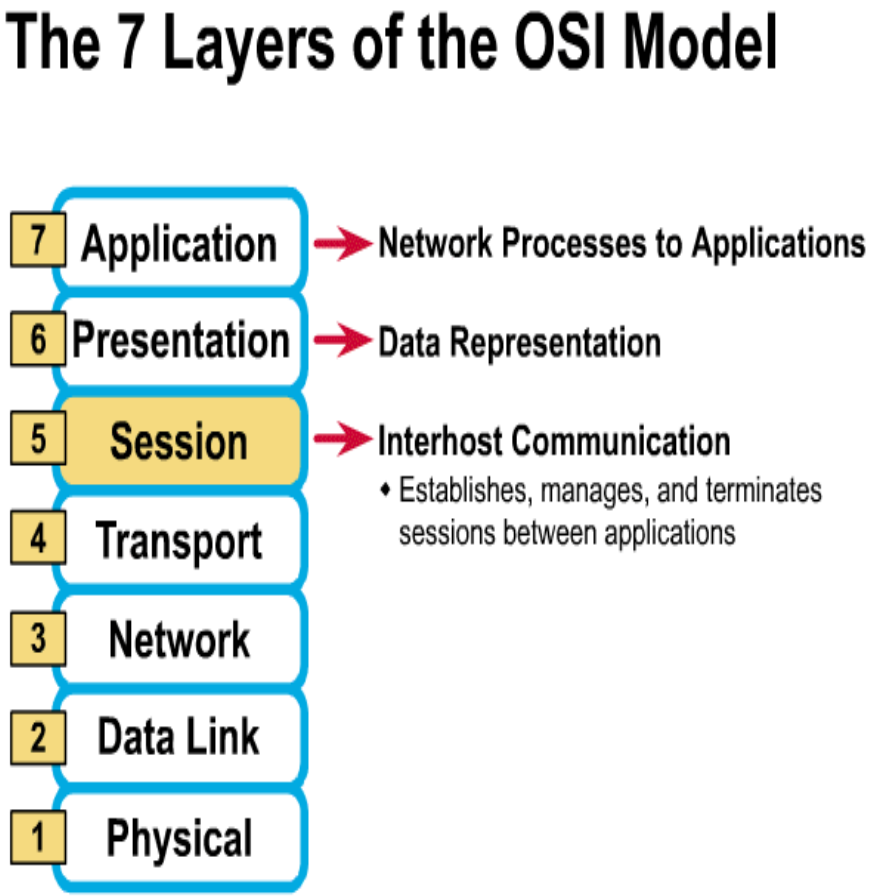
Reliable process-to-process delivery of a message



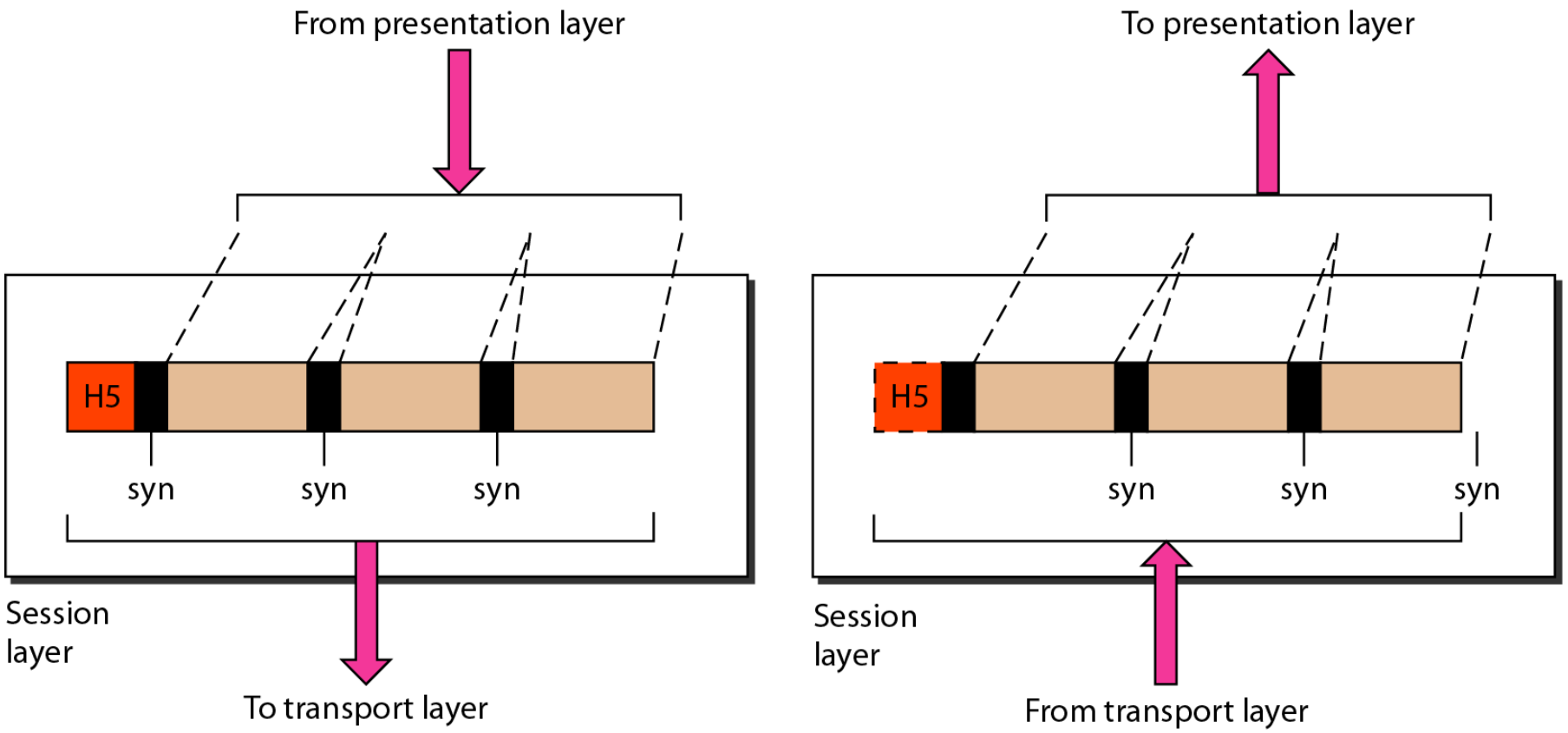
OSI Model

Session Layer

- Allows applications to maintain an ongoing session
- Manages Session
- Synchronization



Session layer

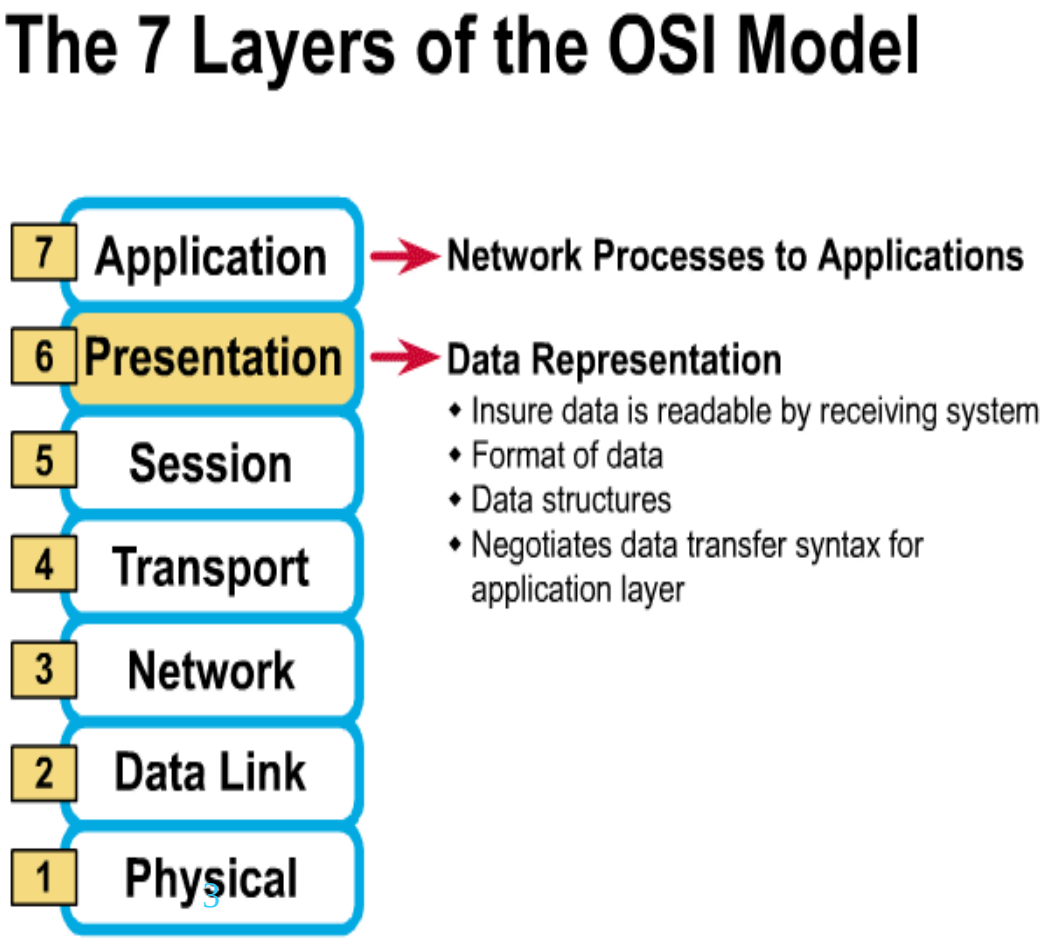


Note

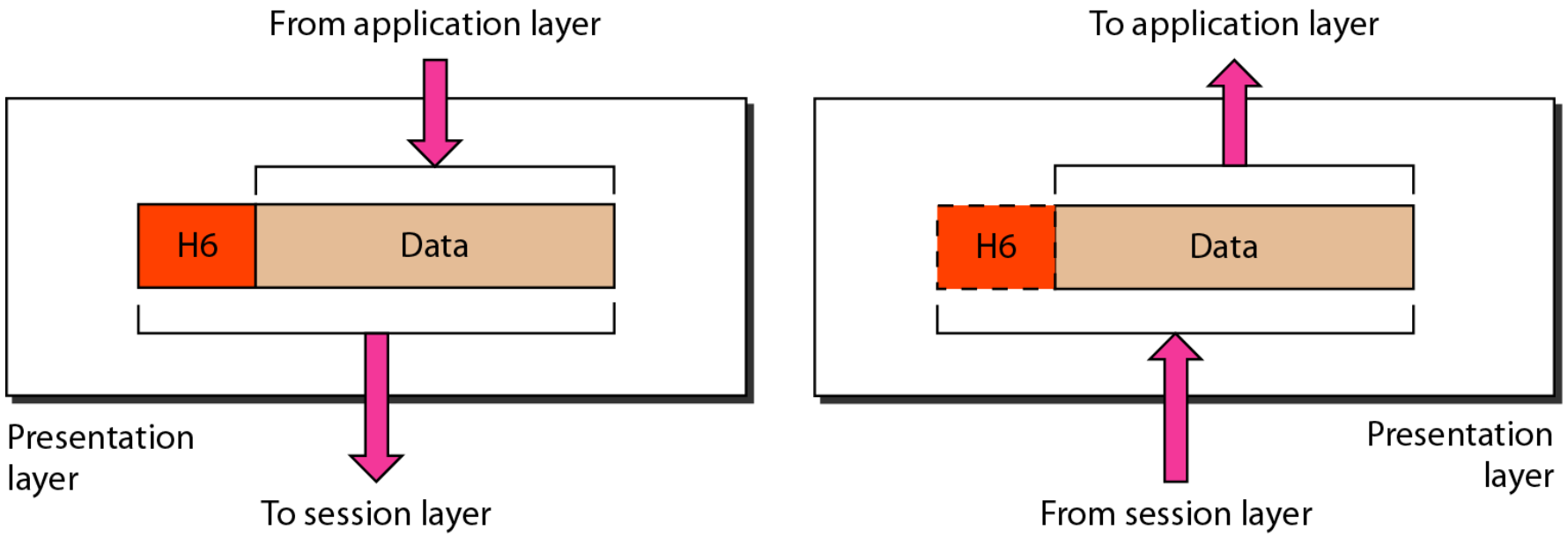
The session layer is responsible for dialog control and synchronization.

Presentation Layer

- Encryption
- Decryption
- Compression



Presentation layer

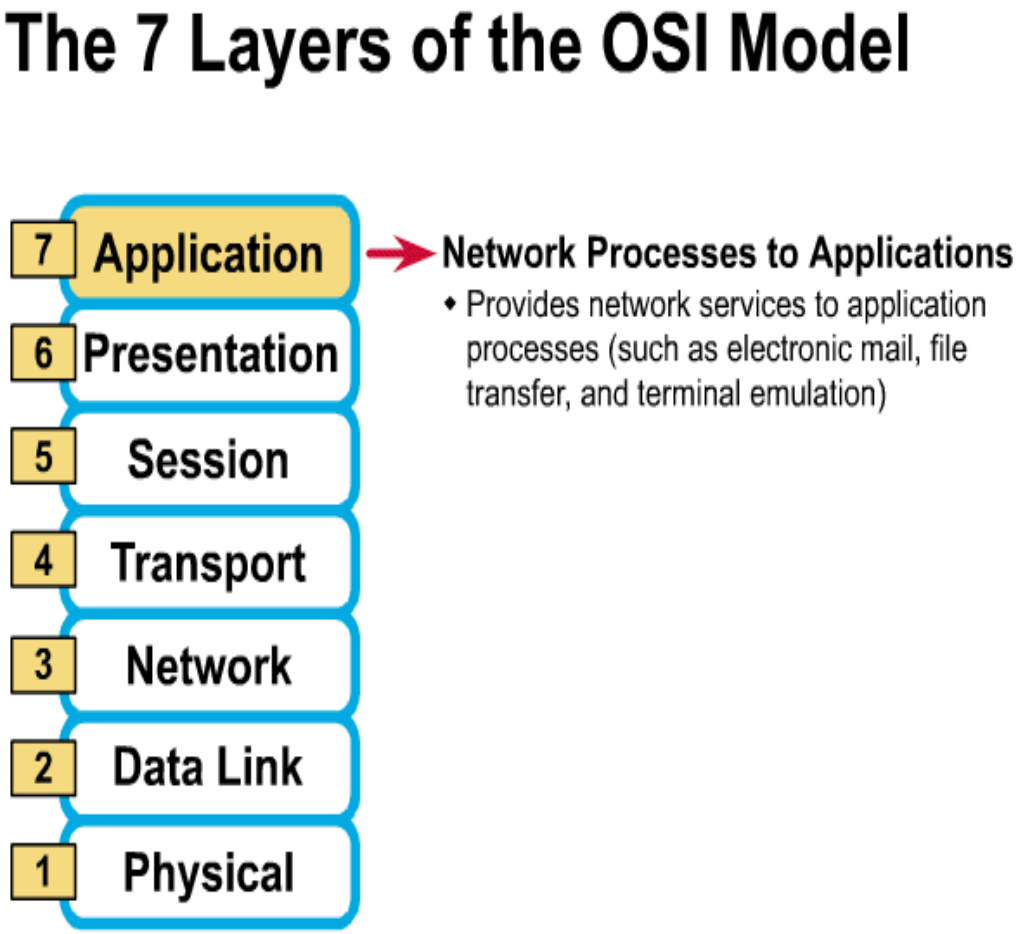


Note

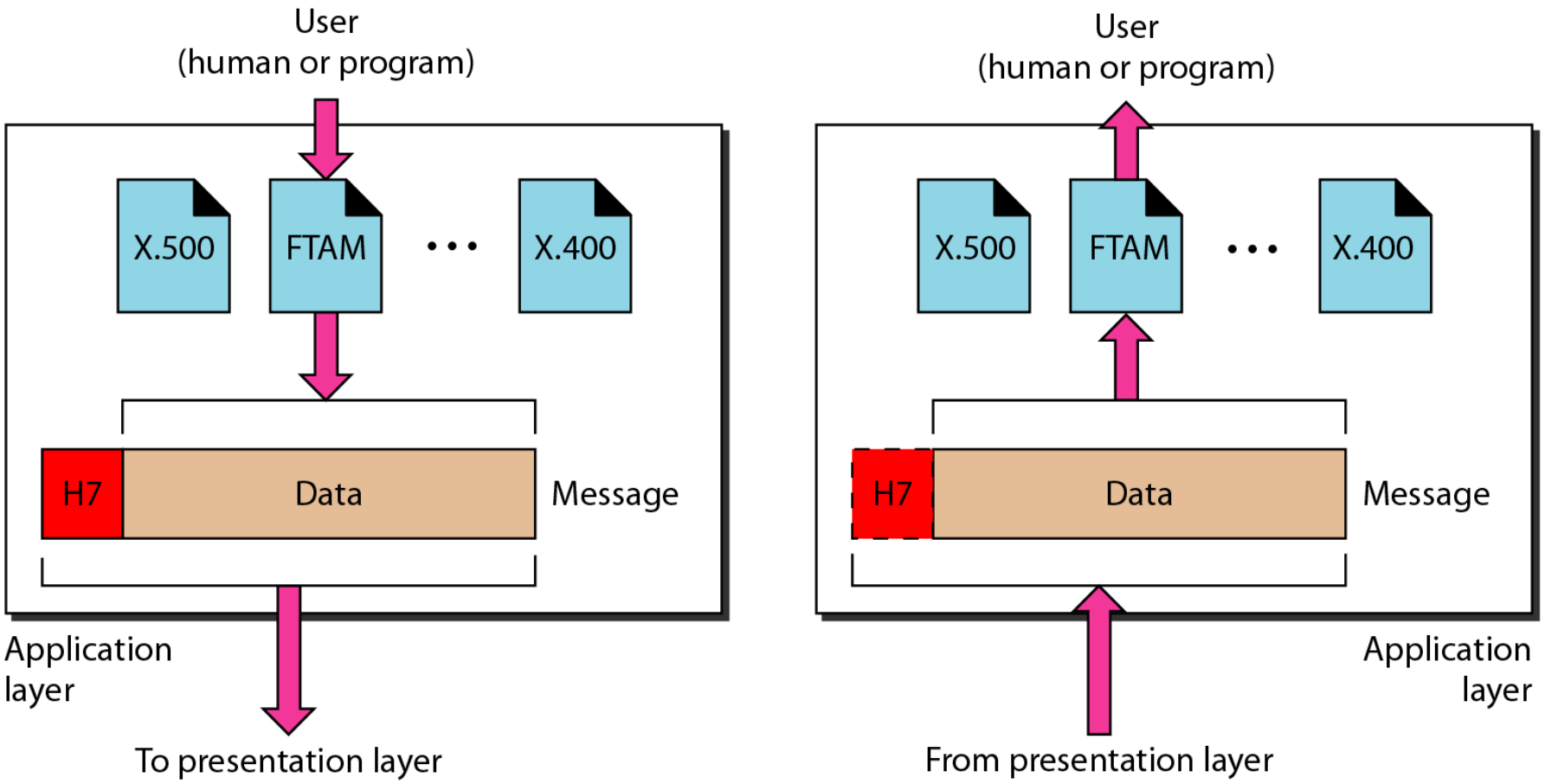
The presentation layer is responsible for translation, compression, and encryption.

Application Layer

- Gives end-user applications access to network resources
- File transfer, access, management
- Mail Services



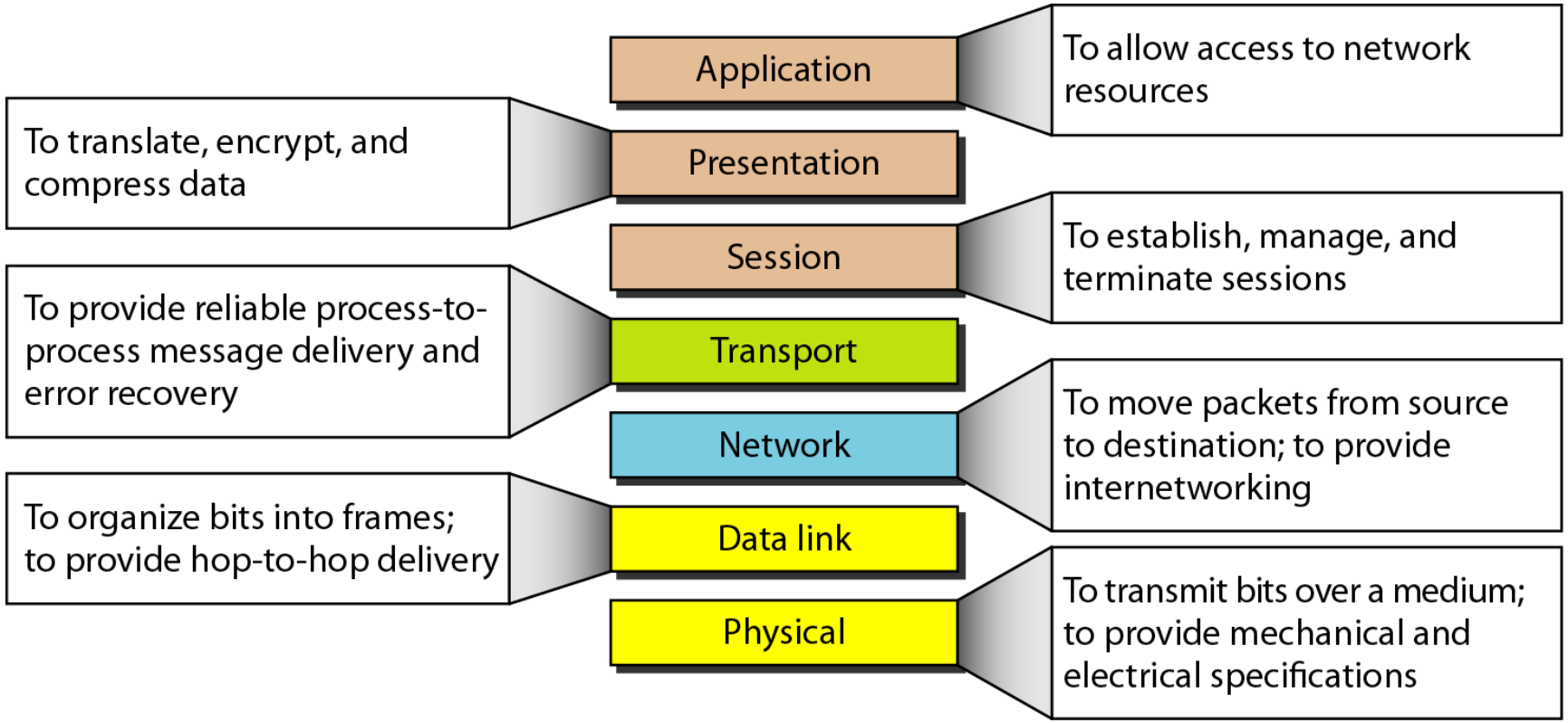
Application layer



Note

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

Summary of layers



How Does It All Work Together

Each layer contains a Protocol Data Unit (PDU)

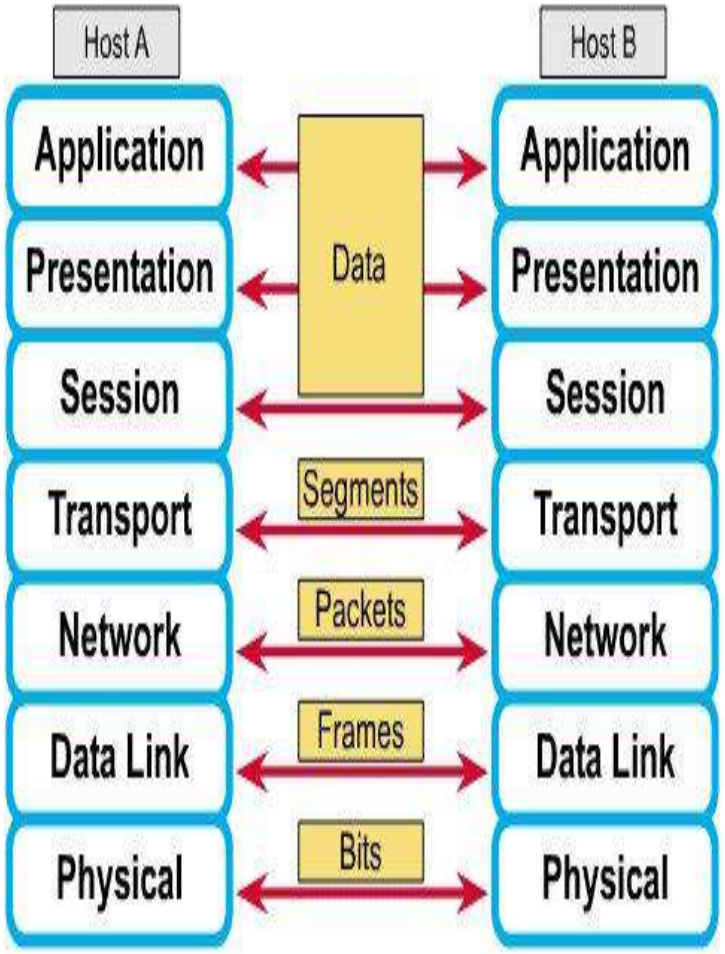
PDU's are used for peer-to-peer contact between corresponding layers.

Data is handled by the top three layers, then Segmented by the Transport layer.

The Network layer places it into packets and the Data Link frames the packets for transmission.

Physical layer converts it to bits and sends it out over the media.

The receiving computer reverses the process using the information contained in the PDU.



The Postal Analogy
How would the OSI compare to the regular Post Office

Application	**A-** Write a 20 page letter to a foreign country.
Presentation	**P-** Translate the letter so the receiver can read it.
Session	**S-** Insure the intended recipient can receive letter.
Transport	**T-** Separate and number pages. Like registered mail, tracks delivery and requests another package if one is “lost” or “damaged” in the mail.
Network	**N-** Postal Center sorting letters by zip code to route them closer to destination.
Data-Link	**D-** Local Post Office determining which vehicles to deliver letters.
Physical	**P-** Physical Trucks, Planes, Rail, autos, etc which carry letter between stations.

TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

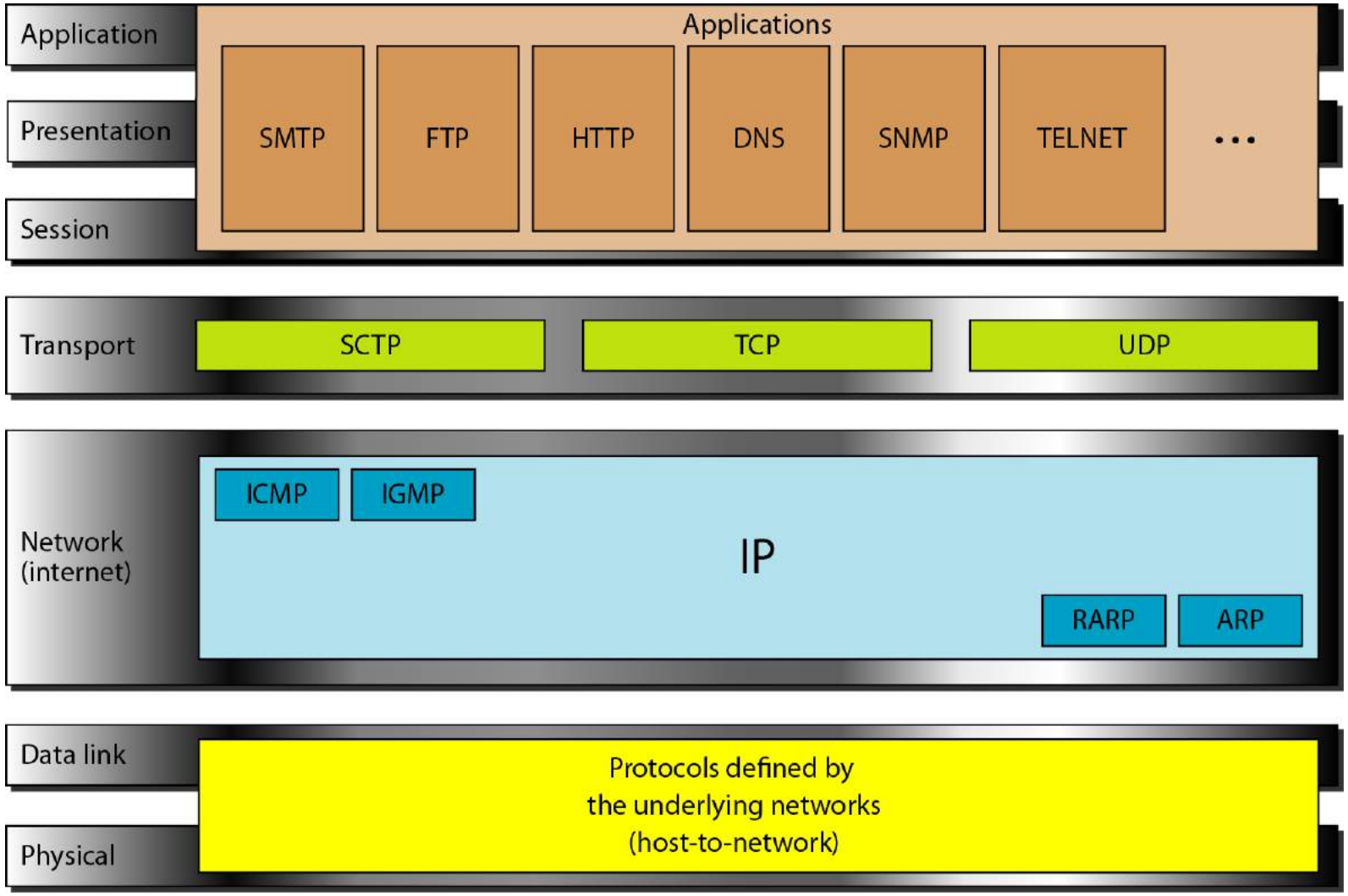
Layer 4: Application

Layer 3: Transport

Layer 2: Internet

Layer 1: Host to network

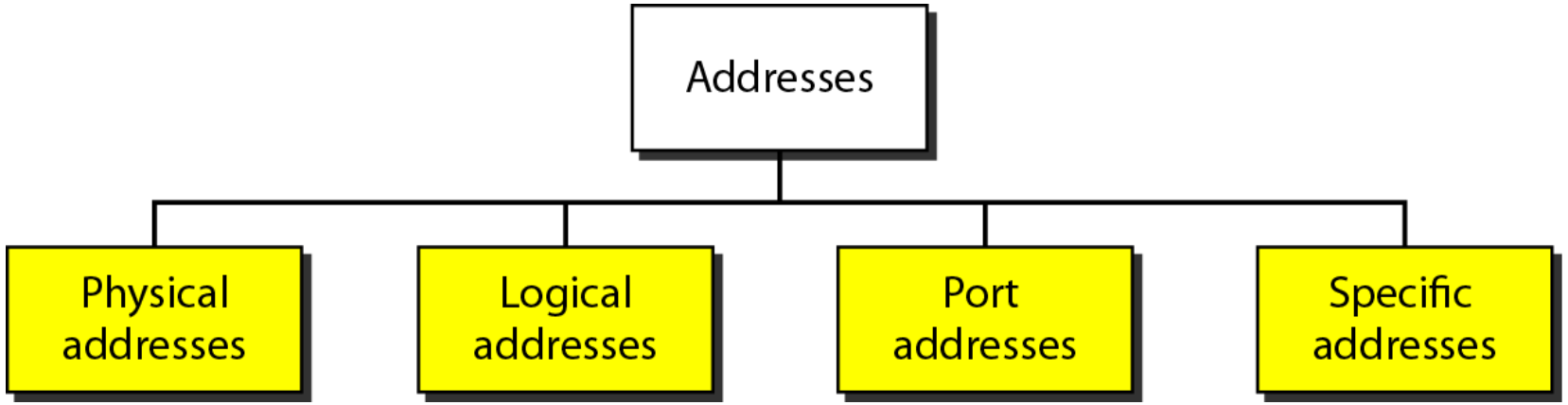
TCP/IP and OSI model



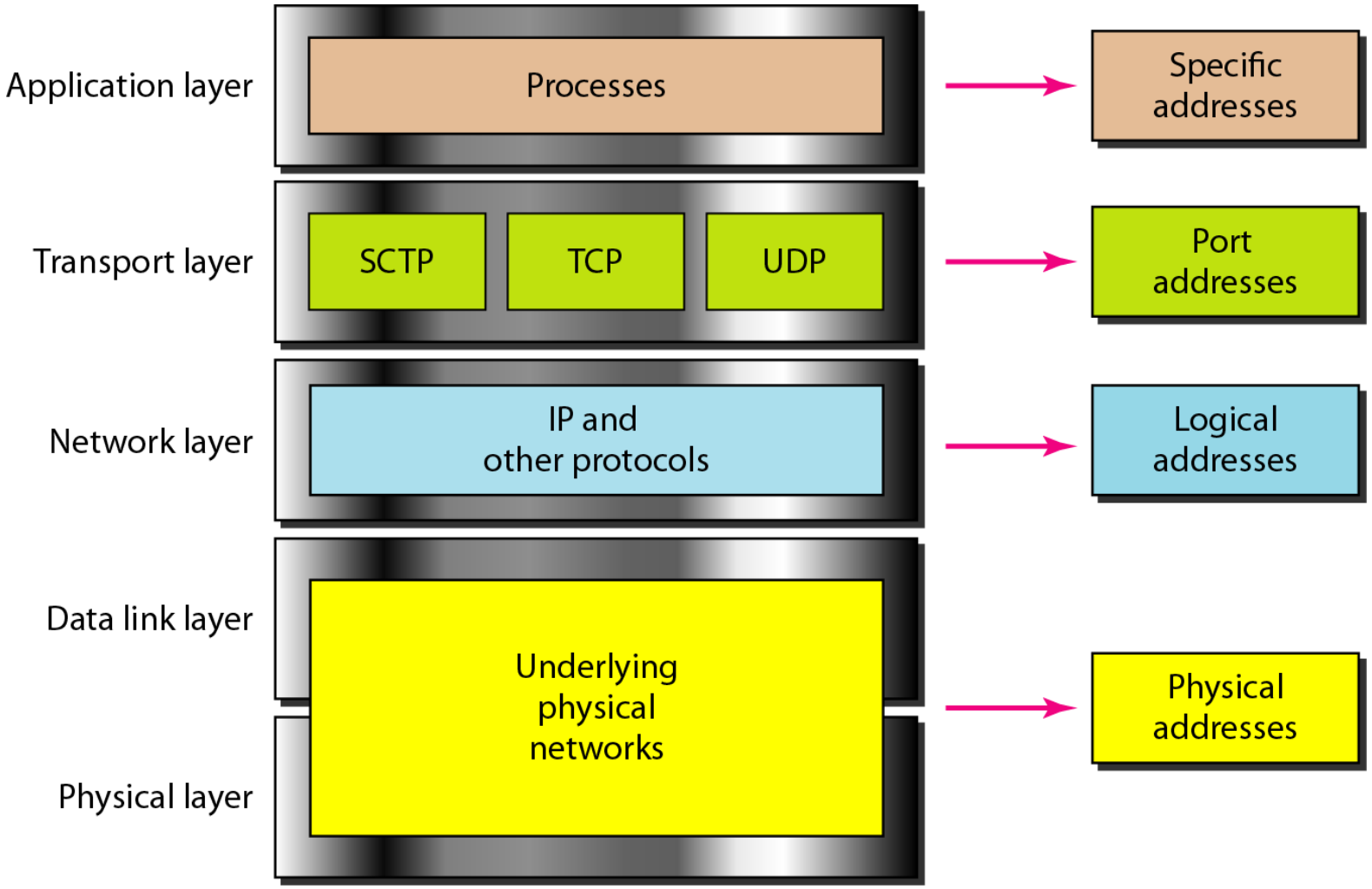
ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

Addresses in TCP/IP



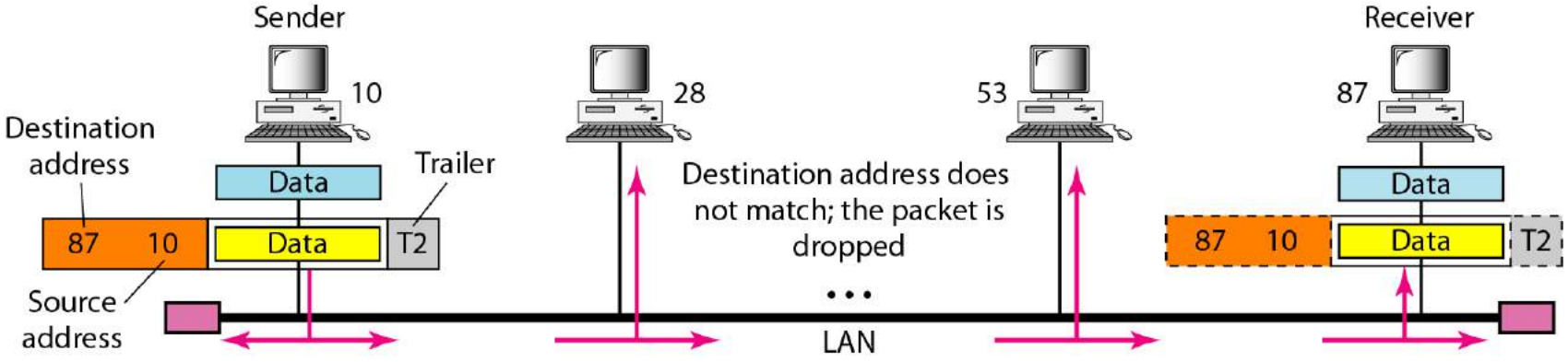
Relationship of layers and addresses in TCP/IP



Example 1

In Figure 1 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

Figure 1 *Physical addresses*



Example 2

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:

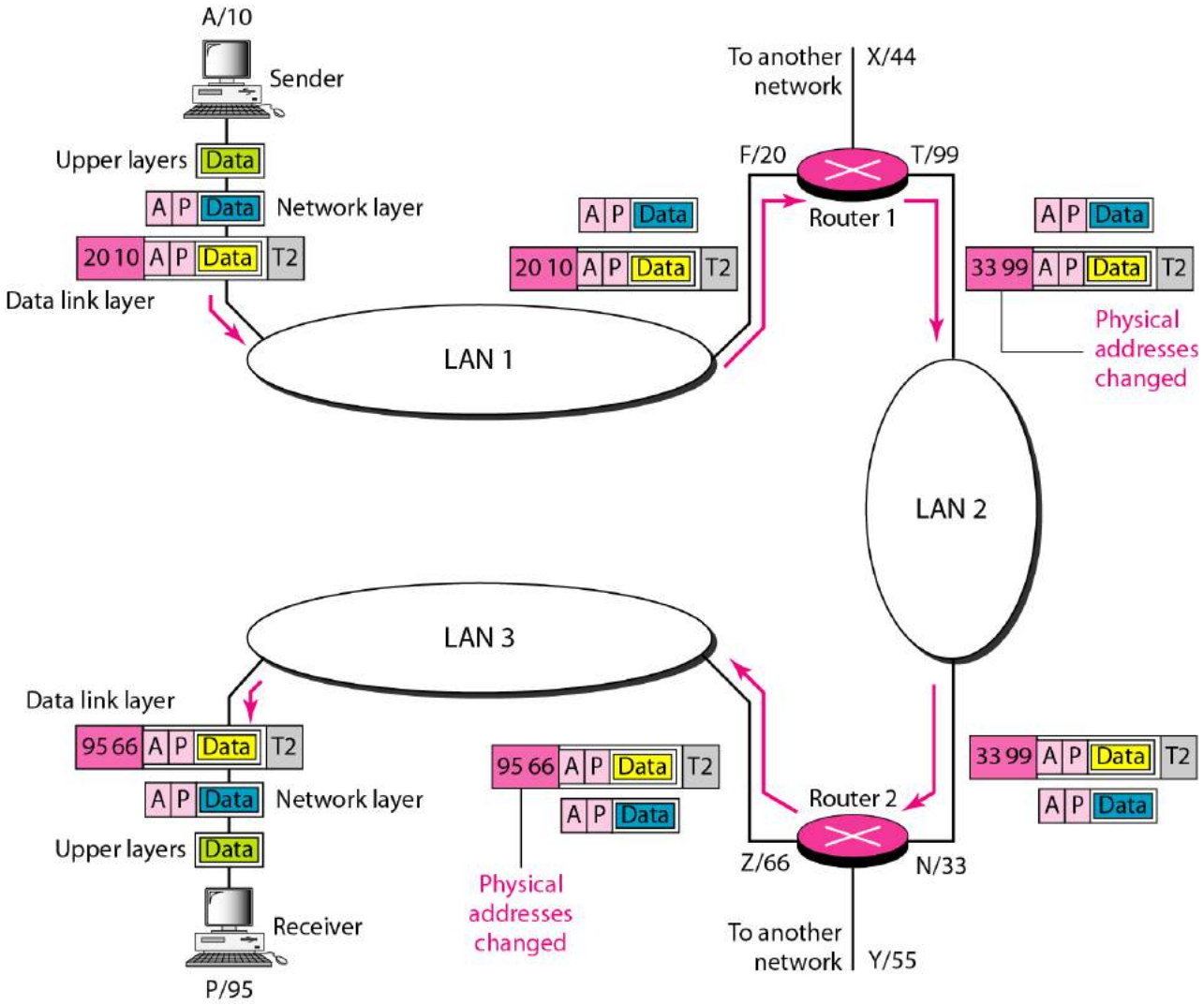
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

Example 3

Figure 2 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 (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

Figure 2 *IP addresses*



Example 4

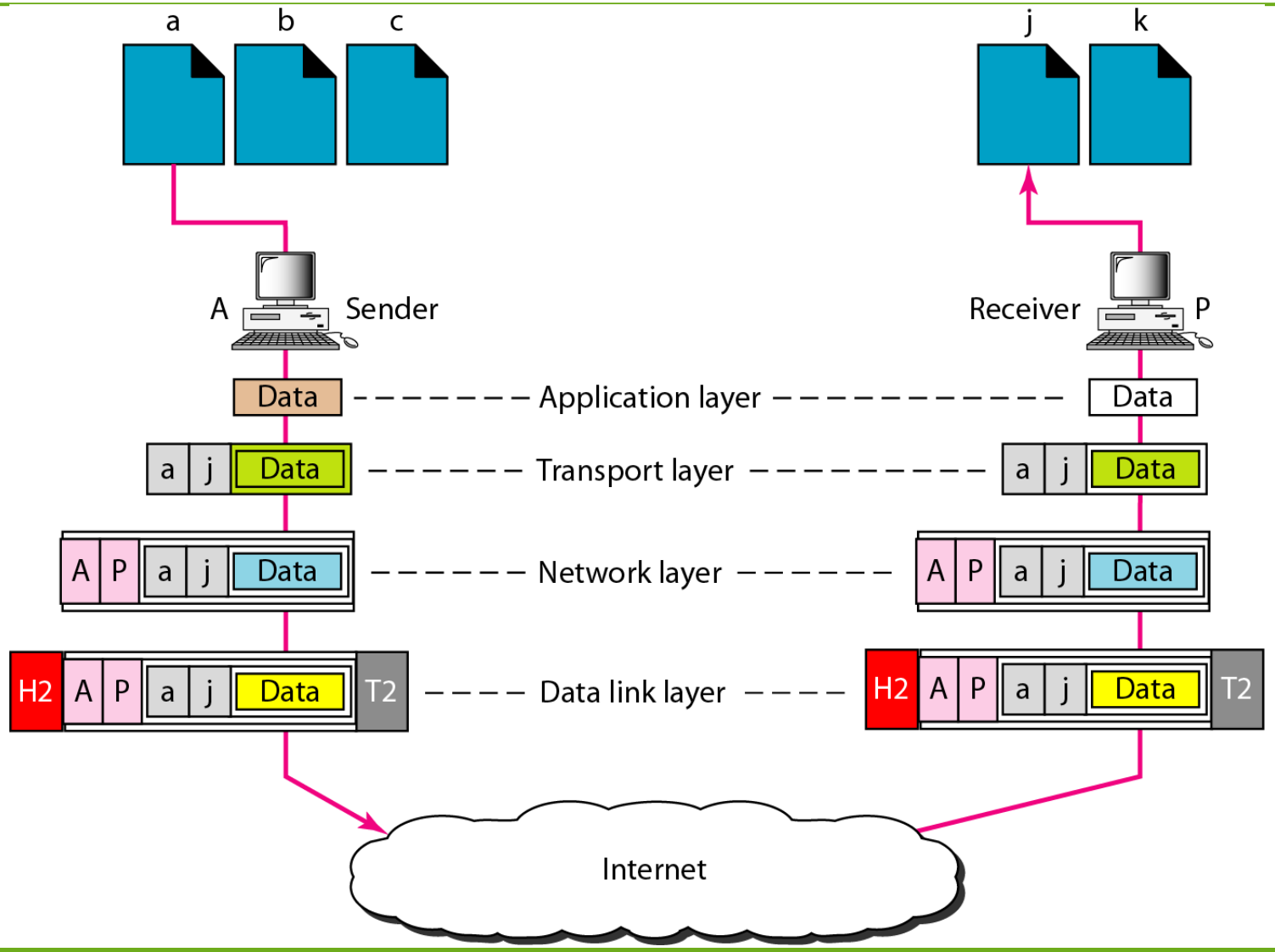
Figure 3 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

OSI Model

Example 4

Figure 3 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 physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Figure 3 *Port addresses*



Note

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

Example 5

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.

Data Encapsulation In TCP/IP

At each layer in the TCP/IP protocol stack

- Outgoing data is packaged and identified for delivery to the layer underneath

PDU – Packet Data Unit – the “envelop” information attached to a packet at a particular TCP/IP protocol

- e.g. header and trailer

Header

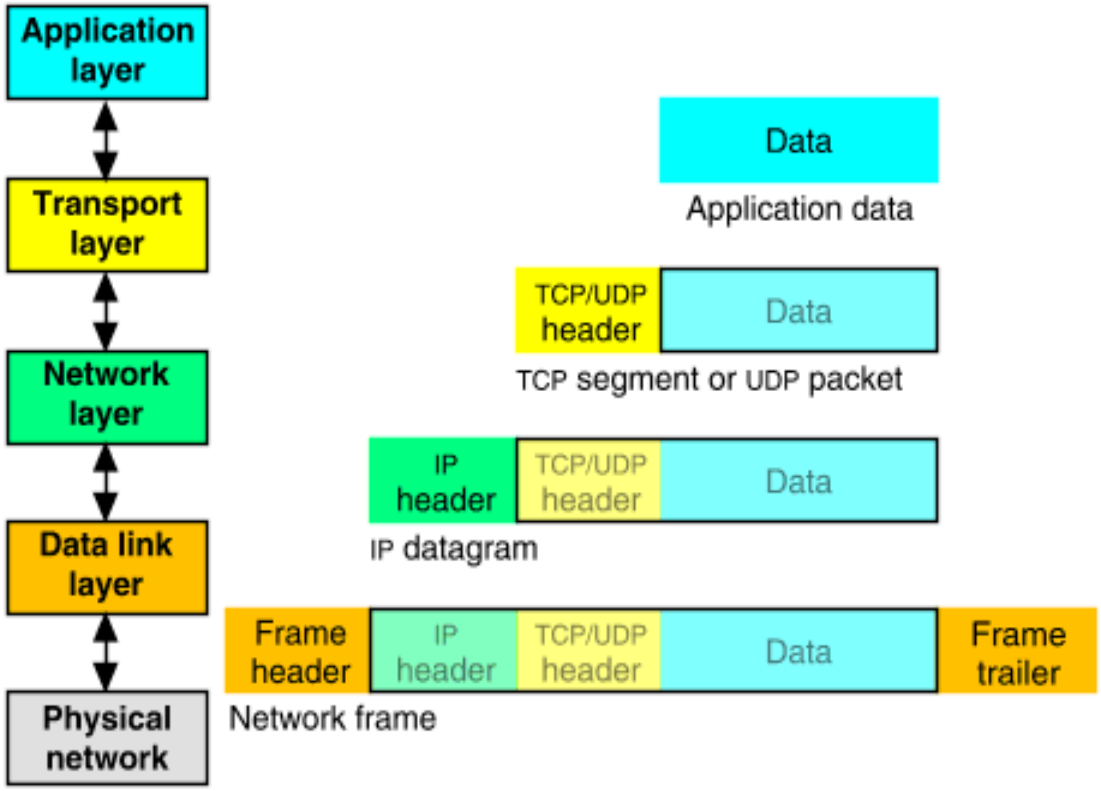
- PDU’s own particular opening component
- Identifies the protocol in use, the sender and intended recipient

Trailer (or packet trailer)

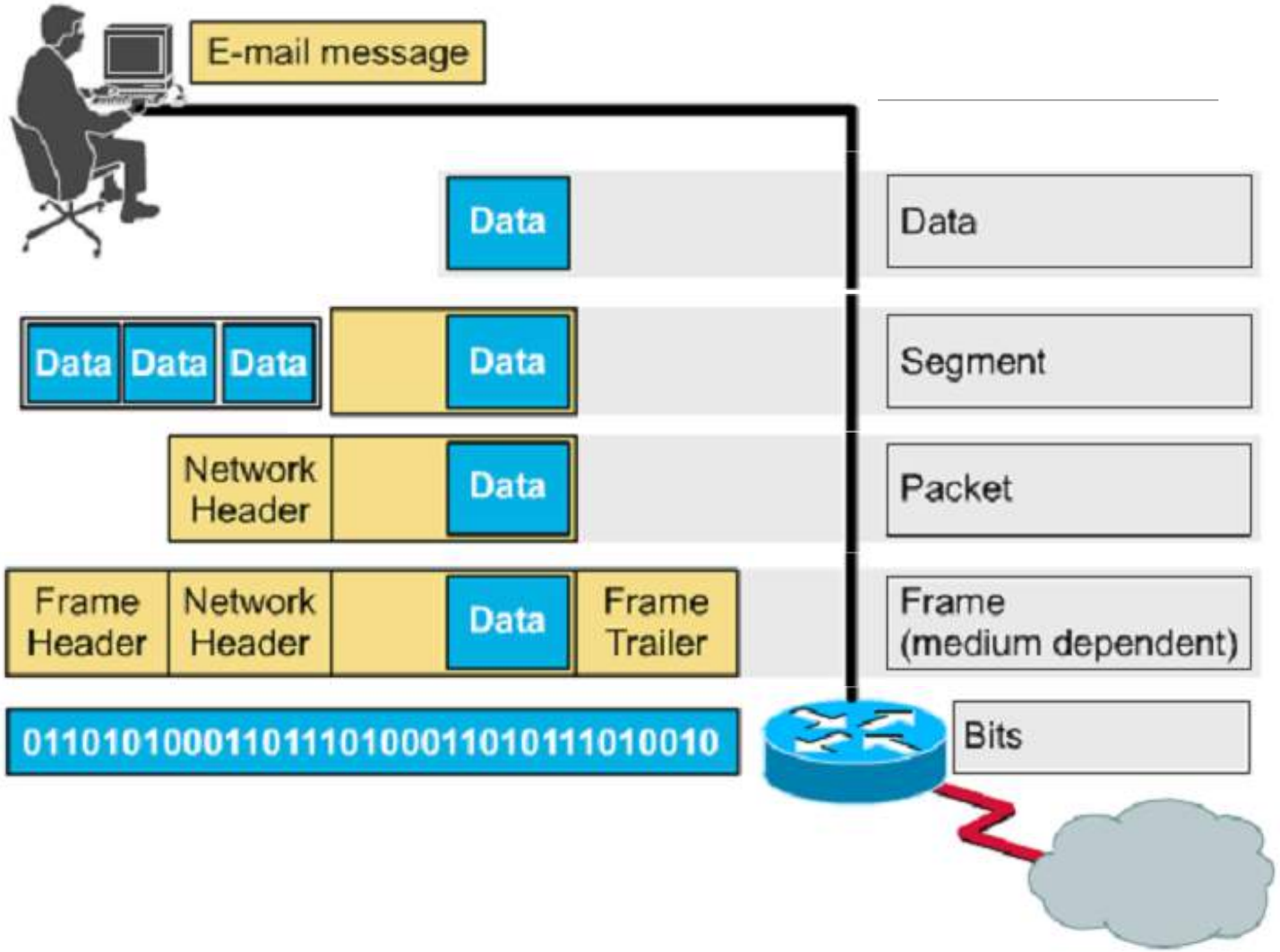
- Provides data integrity checks for the payload

Packet Encapsulation (TCP/IP)

- The data is sent down the protocol stack
- Each layer adds to the data by prepending headers



Encapsulation Example 6: E-mail



How the OSI and TCP/IP Models Relate in a Networking Environment

OSI Model Layer	OSI Model Name	Equipment	PDU	Words to Remember	TCP/IP Model
Layer 7	Application	Computer	Data/Message	Browsers	Application
Layer 6	Presentation			Common Data Format	Application
Layer 5	Session			Dialogues and Conversations	Application
Layer 4	Transport	Computer	Segment	Quality of Service, and Reliability	Transport
Layer 3	Network	Router	Packet	Path Selection, Routing, and Addressing	Internet
Layer 2	Data Link - MAC -LLC	Bridge, Switch	Frame	Frames and Media Access Control (MAC)	Network Access
Layer 1	Physical	Repeater, Hub	Bit	Signals and Media	Network Access

Analog and Digital

Note

To be transmitted, data must be transformed to electromagnetic signals.

ANALOG AND DIGITAL

- The term analog data refers to information that is continuous.
- The term digital data refers to information that has discrete states.
- Analog data take on continuous values.
- Digital data take on discrete values.

Analog and Digital Data

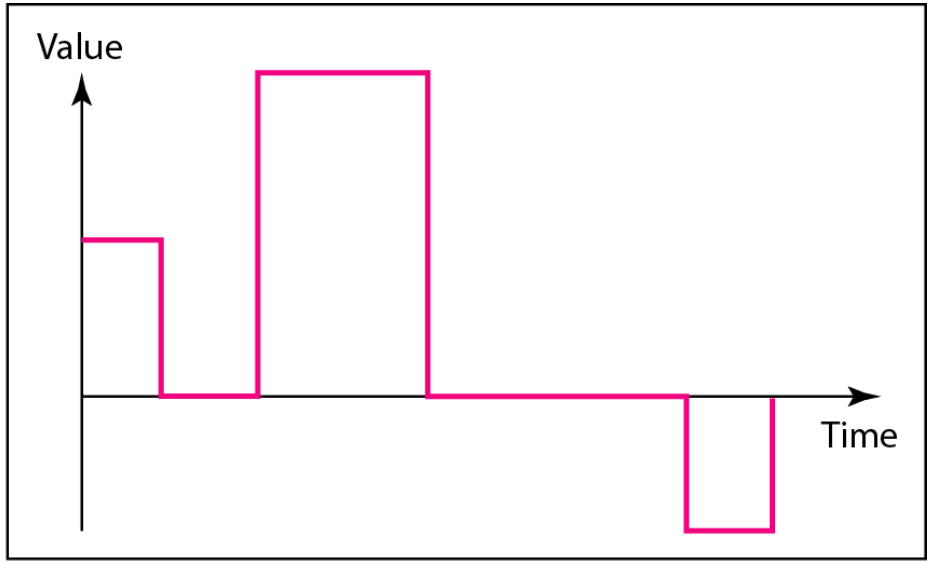
- Data can be analog or digital.
- Analog data are continuous and take continuous values.
- Digital data have discrete states and take discrete values.

Analog and Digital Signals

- Signals can be analog or digital.
- Analog signals can have an infinite number of values in a range.
- Digital signals can have only a limited number of values.

Comparison of analog and digital signals

a. Analog signal

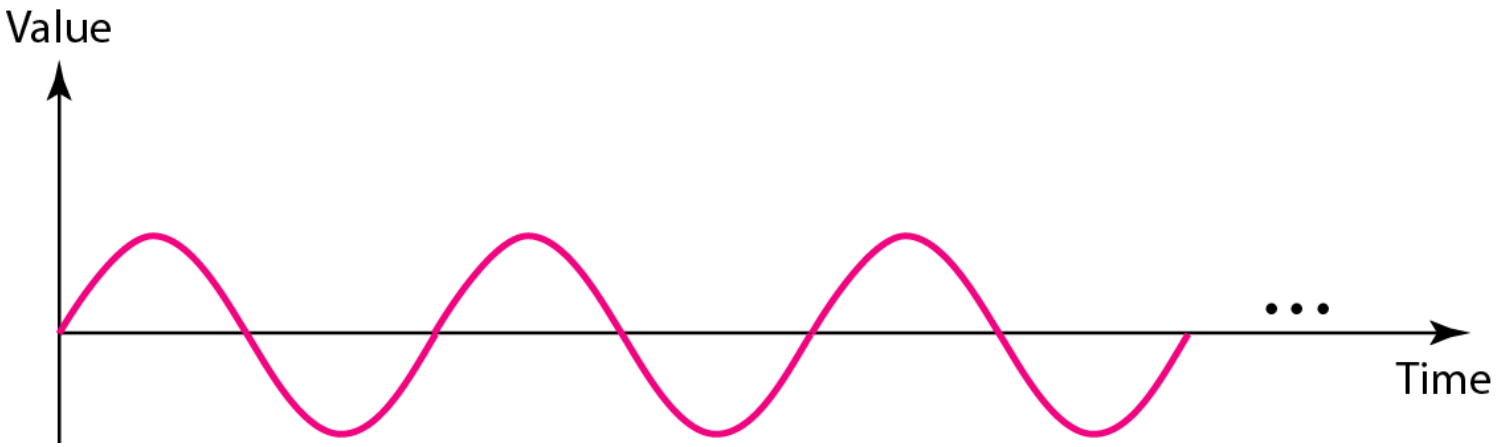


b. Digital signal

ANALOG SIGNALS CHARACTERISTICS

- 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 nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

A sine wave(periodic signal)



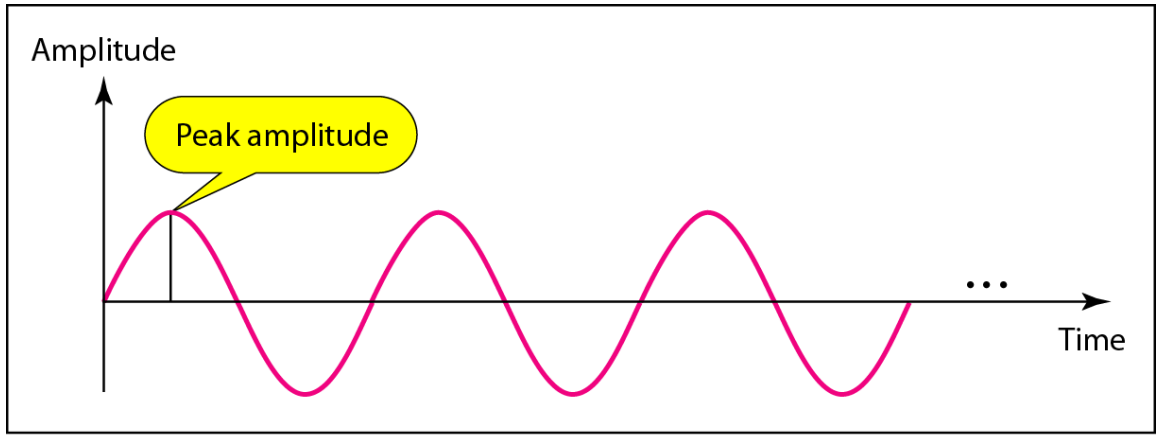
A sine wave(periodic signal)

A sine wave can be represented by three parameters:

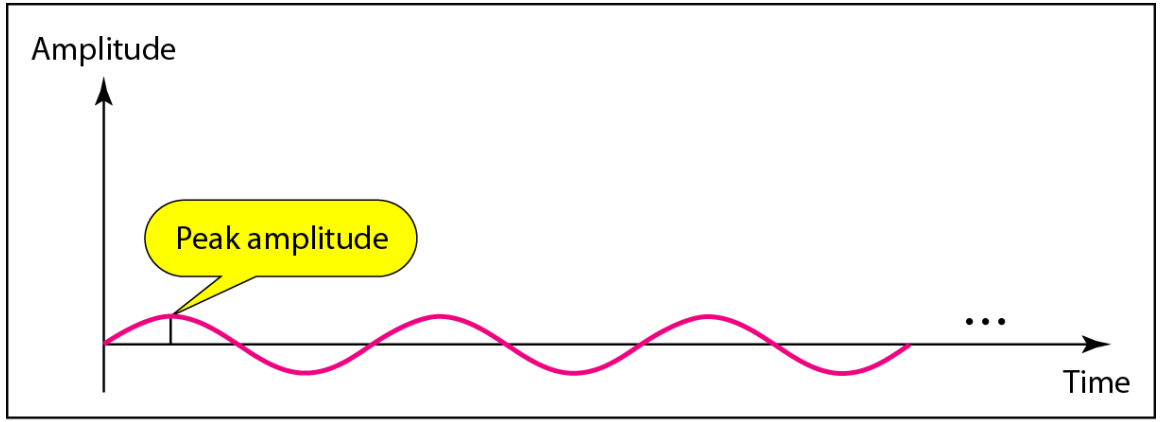
1. the peak amplitude
2. the frequency, and
3. the phase.

These three parameters fully describe a sine wave.

Two signals with the same phase and frequency, but different amplitudes



a. A signal with high peak amplitude



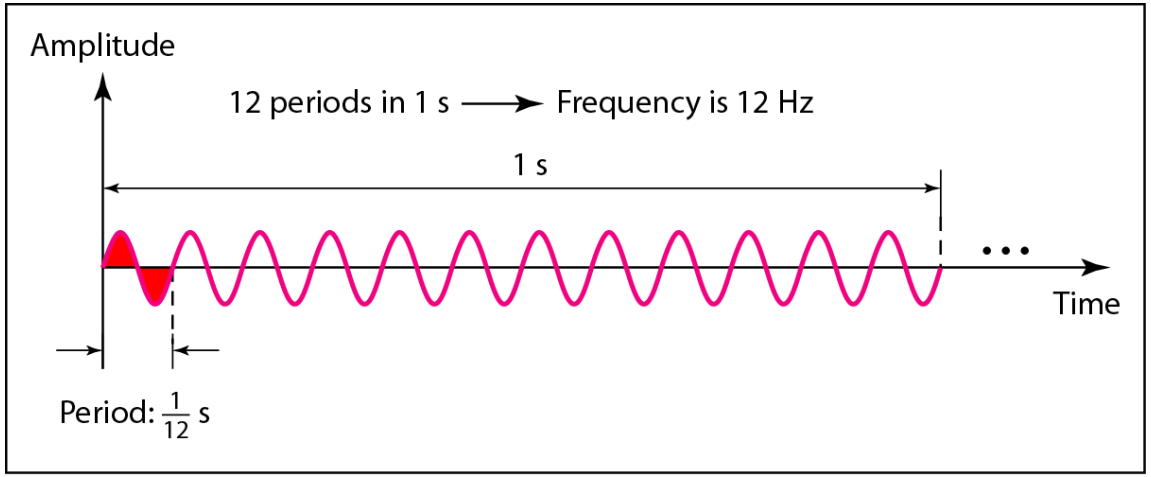
b. A signal with low peak amplitude

Note

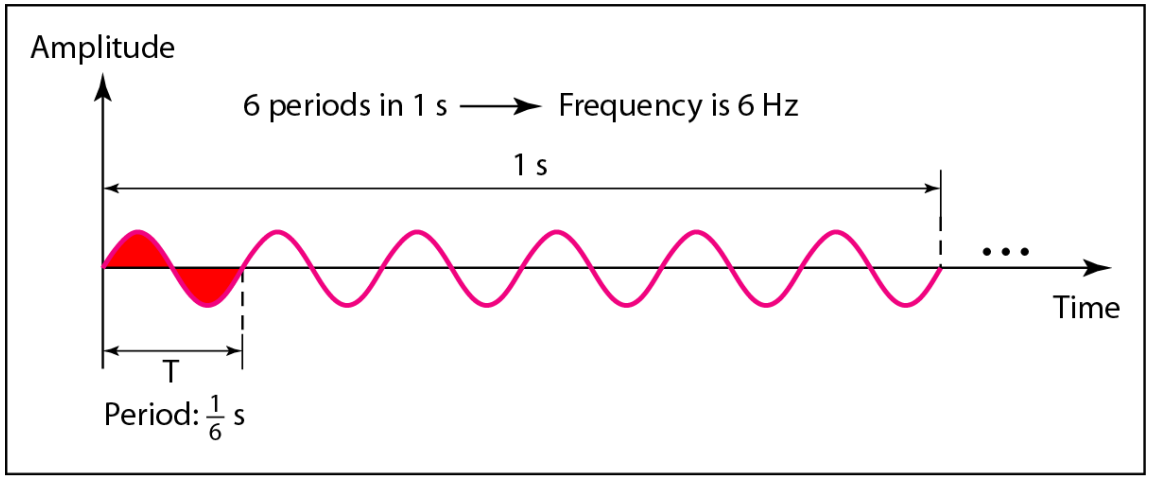
Frequency and period are the inverse of each other.

$$f = \frac{1}{T} \quad \text{and} \quad T = \frac{1}{f}$$

Two signals with the same amplitude and phase, but different frequencies



a. A signal with a frequency of 12 Hz



b. A signal with a frequency of 6 Hz

Units of period and 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

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

Example

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

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

Example

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

Example

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).

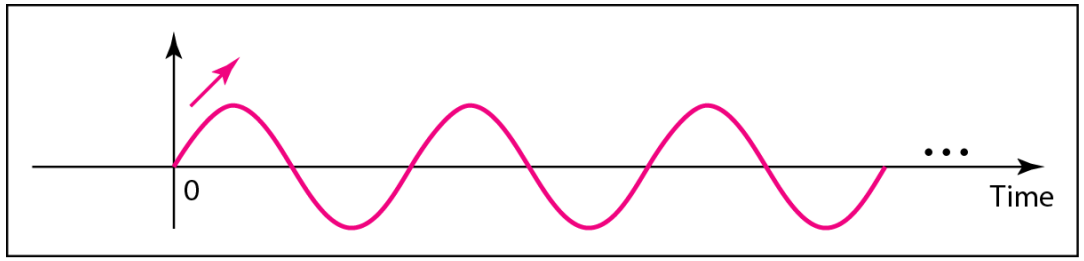
$$100 \text{ ms} = 100 \times 10^{-3} \text{ s} = 10^{-1} \text{ s}$$

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

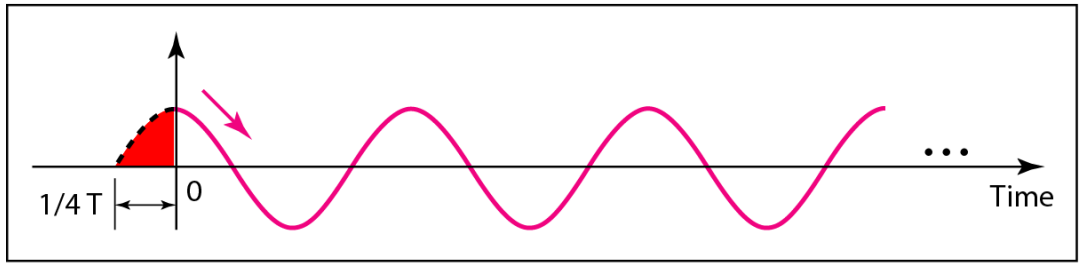
Note

Phase describes the position of the waveform relative to time 0.

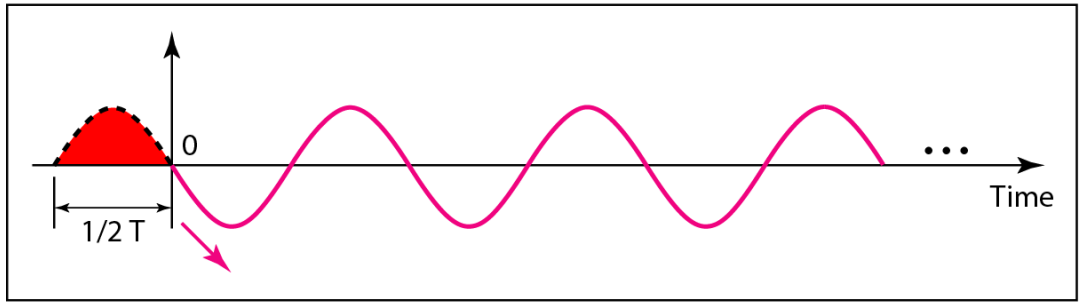
Figure Three sine waves with the same amplitude and frequency, but different phases



a. 0 degrees



b. 90 degrees



c. 180 degrees

Example

A sine wave is offset 1/6 cycle with respect to time 0. What is its phase in degrees and radians?

Solution

We know that 1 complete cycle is 360°. Therefore, 1/6 cycle is

Example

A sine wave is offset 1/6 cycle with respect to time 0. What is its phase in degrees and radians?

Solution

We know that 1 complete cycle is 360°. Therefore, 1/6 cycle is

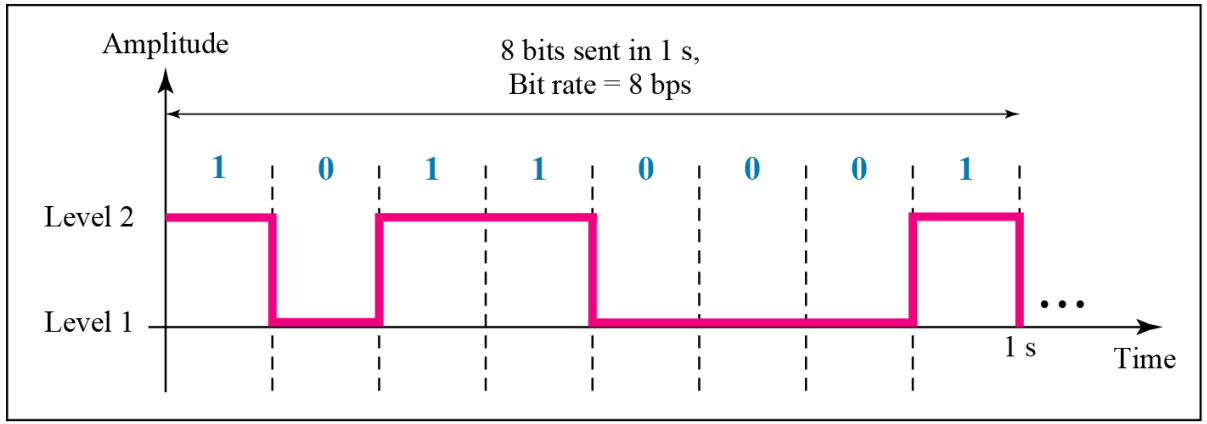
$$\boxed{\frac{1}{6} \times 360 = 60^\circ = 60 \times \frac{2\pi}{360}\ \text{rad} = \frac{\pi}{3}\ \text{rad} = 1.046\ \text{rad}}$$

Digital Signal

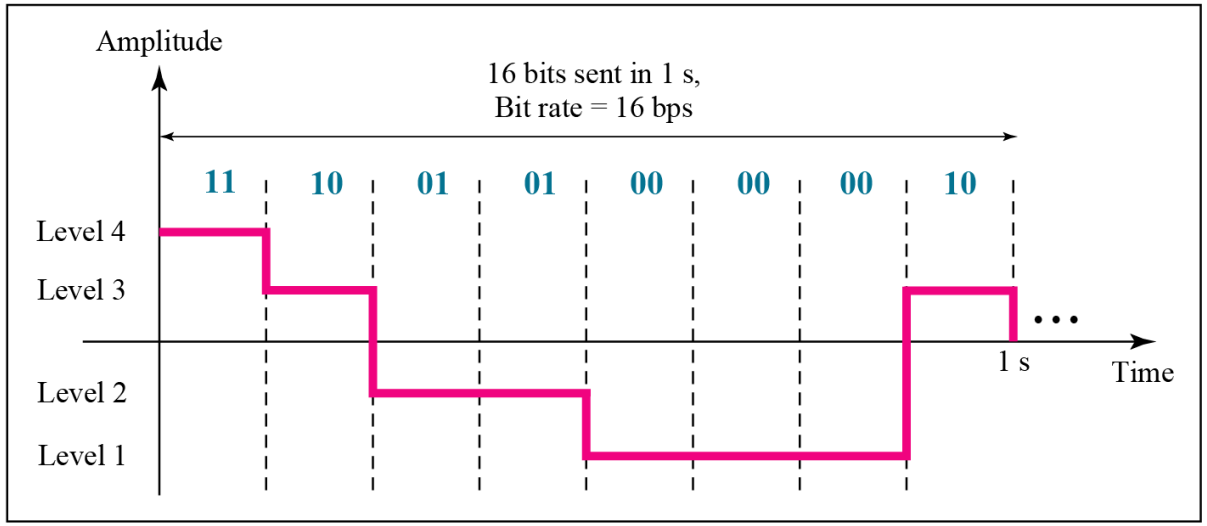
DIGITAL SIGNALS

- In addition to being represented by an analog signal, information can also be represented by a digital signal.
- For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage.
- A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level.

Figure 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

A digital signal has eight levels. How many bits are needed per level? We calculate the number of bits from the formula

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

Each signal level is represented by 3 bits.

Example

A digital signal has nine levels. How many bits are needed per level?

Example

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 as well as a power of 2.

For this example, 4 bits can represent one level.

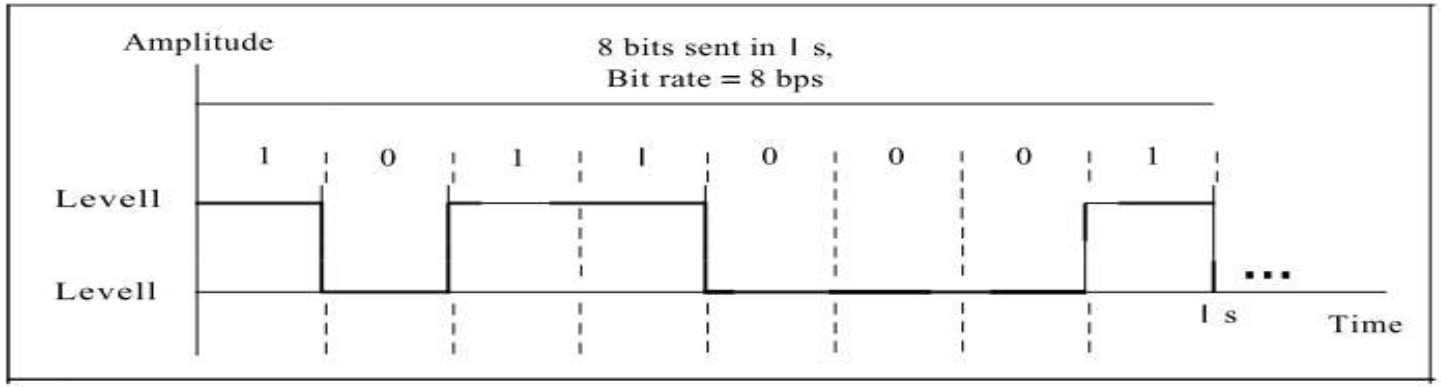
Digital Signal (non periodic signal)

Digital signals are nonperiodic, and thus period and frequency are not appropriate characteristics.

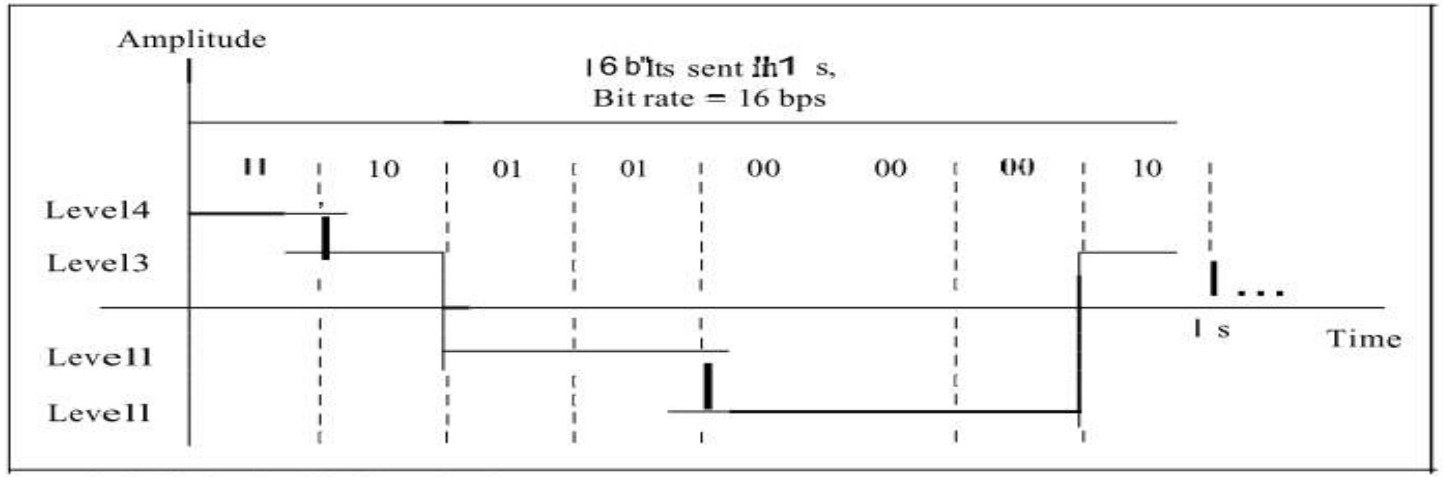
Bit rate is used to describe digital signals.

The bit rate is the number of bits sent in 1 second, expressed in bits per second (bps).

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

Assume we need to download text documents at the rate of 100 pages per sec. What is the required bit rate of the channel?

Solution

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits (ascii), the bit rate is

Example

Assume we need to download text documents at the rate of 100 pages per sec. What is the required bit rate of the channel?

Solution

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits (ascii), the bit rate is

$$100 \times 24 \times 80 \times 8 = 1{,}636{,}000 \text{ bps} = 1.636 \text{ Mbps}$$

Example

A digitized voice channel is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits.

What is the required bit rate?

Solution

The bit rate can be calculated as

Example

A digitized voice channel is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits.

What is the required bit rate?

Solution

The bit rate can be calculated as

$$\boxed{2 \times 4000 \times 8 = 64{,}000 \text{ bps} = 64 \text{ kbps}}$$

Example

What is the bit rate for high-definition TV (HDTV)?

Solution

HDTV uses digital signals to broadcast high quality video signals. The HDTV screen is normally a ratio of 16 : 9. There are 1920 by 1080 pixels per screen, and the screen is renewed 30 times per second. Twenty-four bits represents one color pixel.

Example

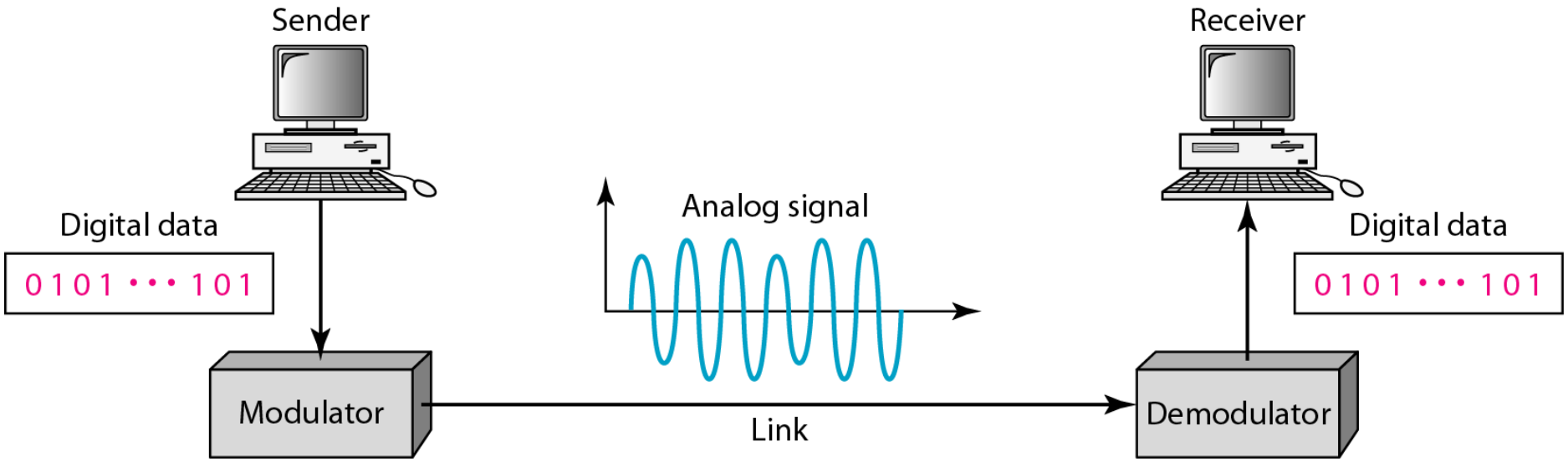
What is the bit rate for high-definition TV (HDTV)?

Solution

HDTV uses digital signals to broadcast high quality video signals. The HDTV screen is normally a ratio of 16 : 9. There are 1920 by 1080 pixels per screen, and the screen is renewed 30 times per second. Twenty-four bits represents one color pixel.

$$1920 \times 1080 \times 30 \times 24 = 1{,}492{,}992{,}000 \text{ or } 1.5 \text{ Gbps}$$

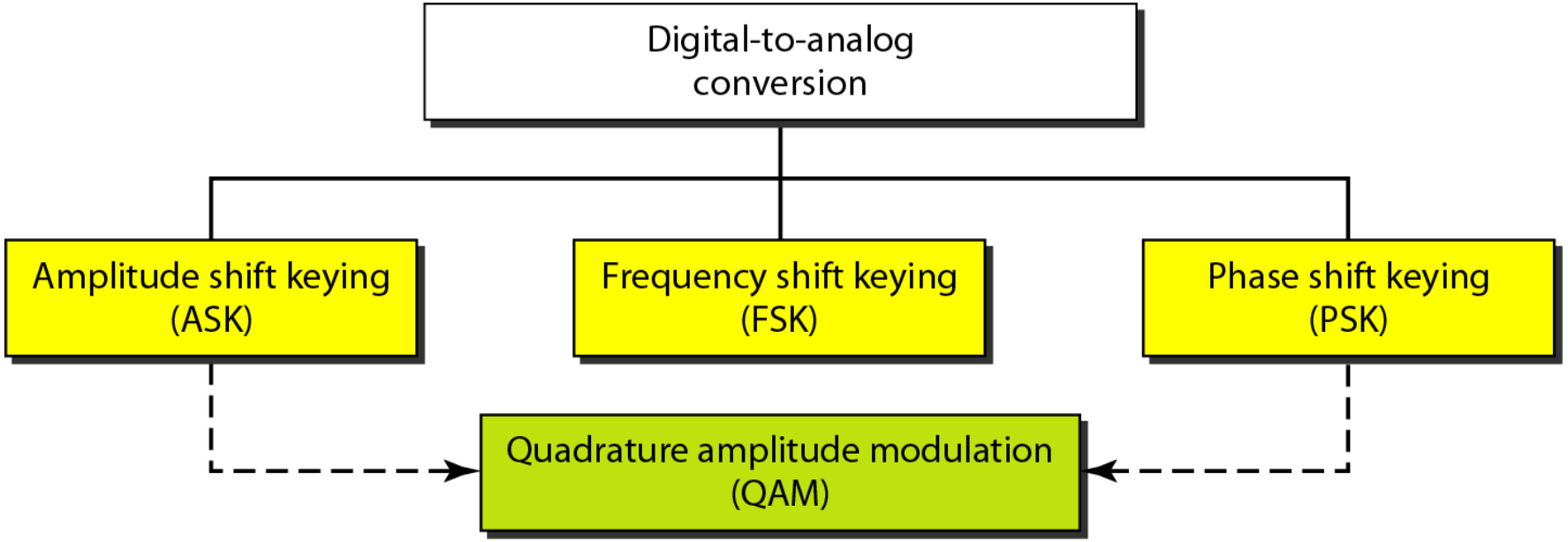
Figure *Digital-to-analog conversion*



Types of digital-to-digital conversion

- Line Coding
- Block Coding
- Scrambling

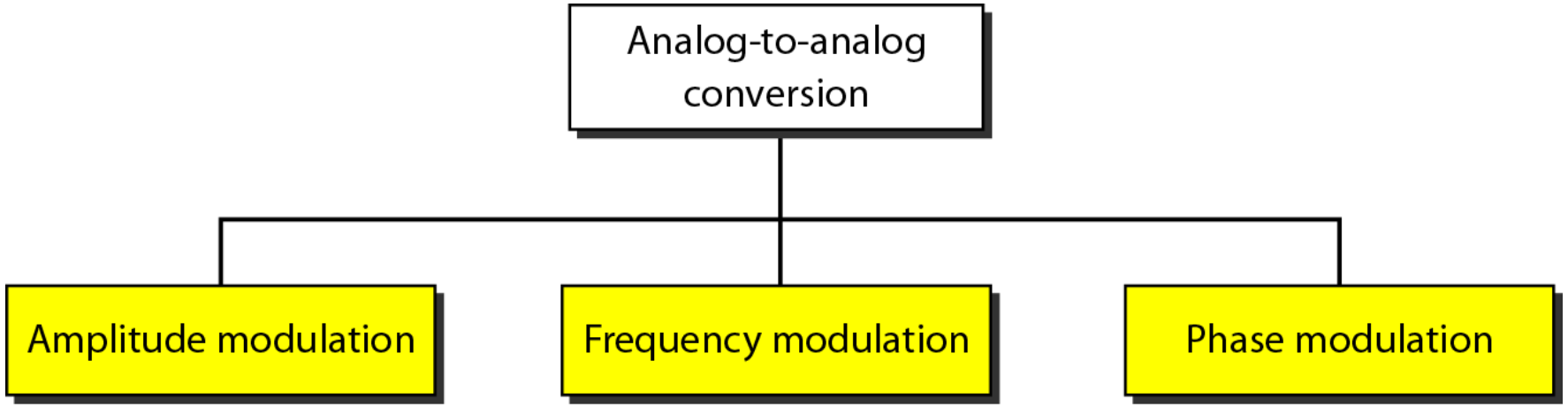
Types of digital-to-analog conversion



Types of analog-to-digital conversion

- Pulse Code Modulation (PCM)
- Delta Modulation (DM)

Types of analog-to-analog conversion

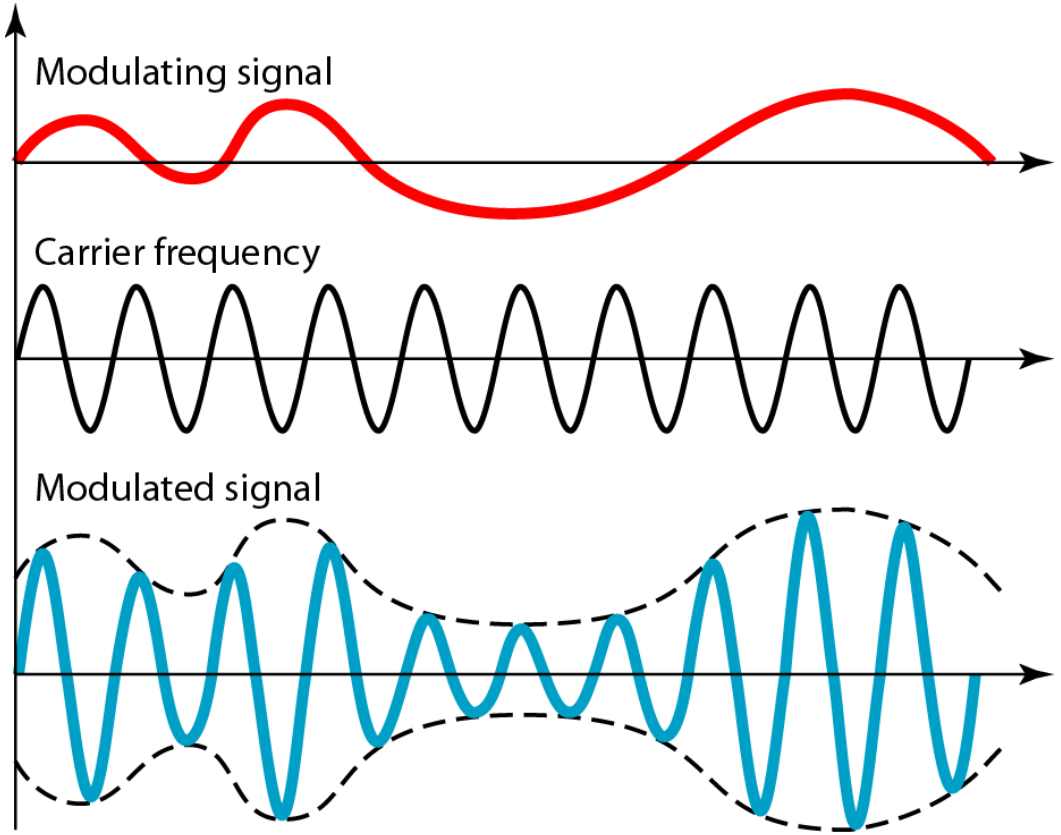


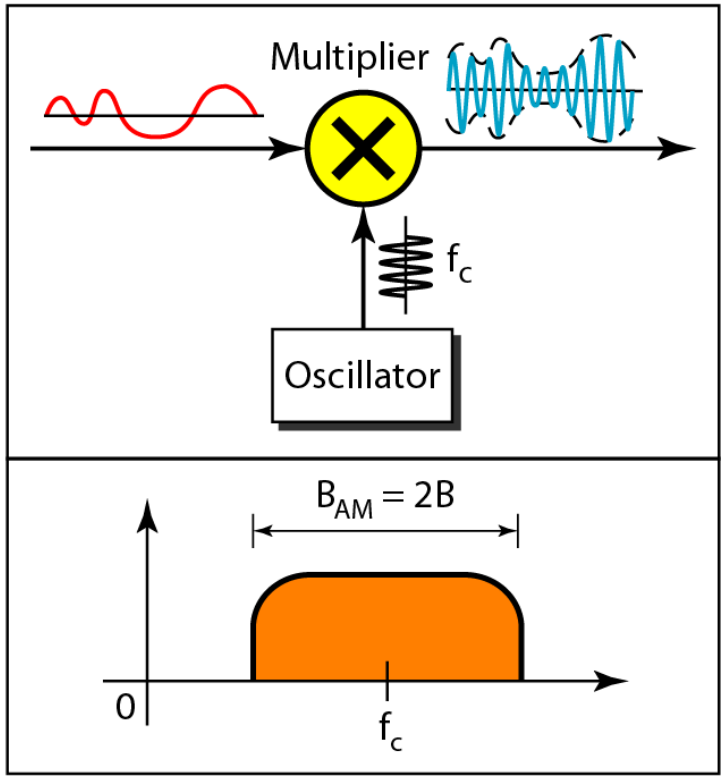
Amplitude Modulation

In AM transmission, the carrier signal is modulated so that its amplitude varies with the changing amplitudes of the modulating signal.

The frequency and phase of the carrier remain the same; only the amplitude changes to follow variations in the information

Figure *Amplitude modulation*



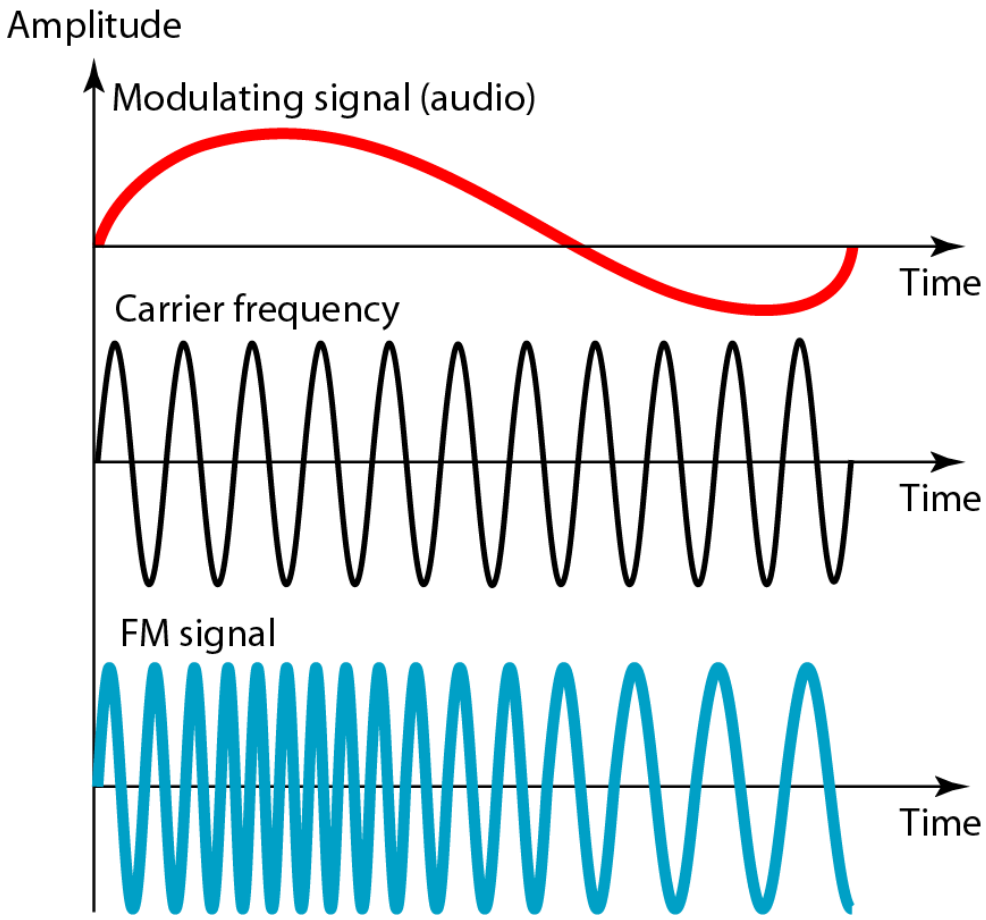


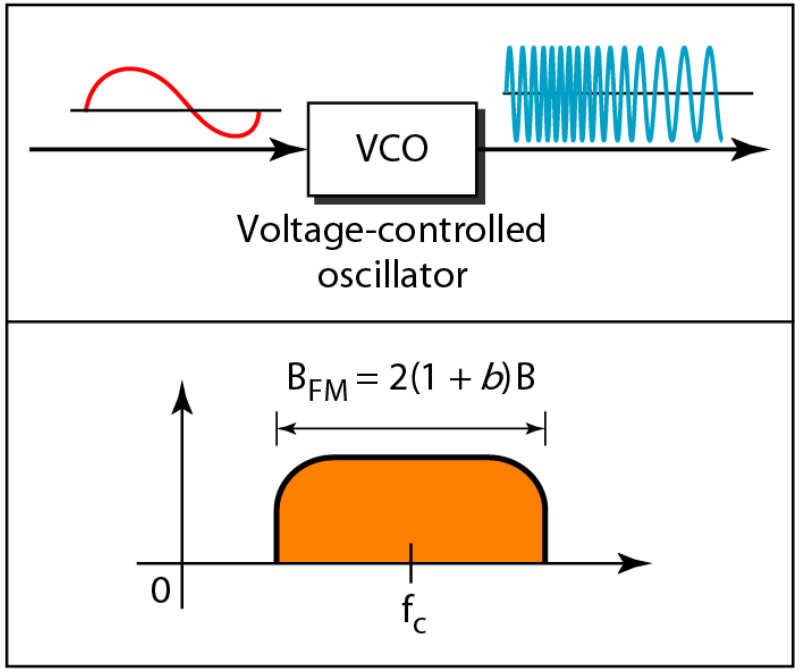
Frequency Modulation

In FM transmission, the frequency of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal.

The peak amplitude and phase of the carrier signal remain constant, but as the amplitude of the information signal changes, the frequency of the carrier changes correspondingly

Figure *Frequency modulation*



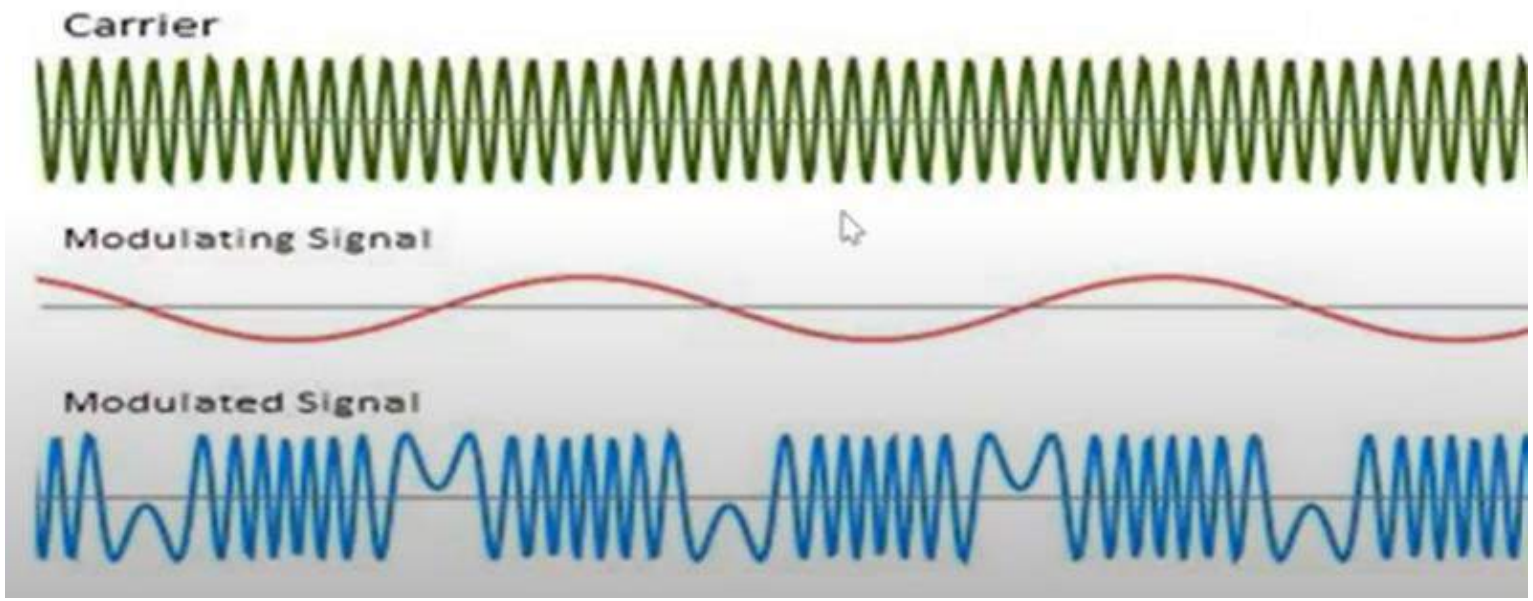


Phase Modulation (PM)

The modulating signal only changes the phase of the carrier signal.

The peak amplitude and frequency of the carrier signal remain constant, but as the amplitude of the information signal changes, the phase of the carrier changes correspondingly.

Figure *Phase modulation*



TRANSMISSION MODES

- The transmission of binary data across a link can be accomplished in either parallel or serial mode.

- Parallel mode, multiple bits are sent with each clock tick.

- Serial mode, 1 bit is sent with each clock tick.

Figure *Data transmission and modes*

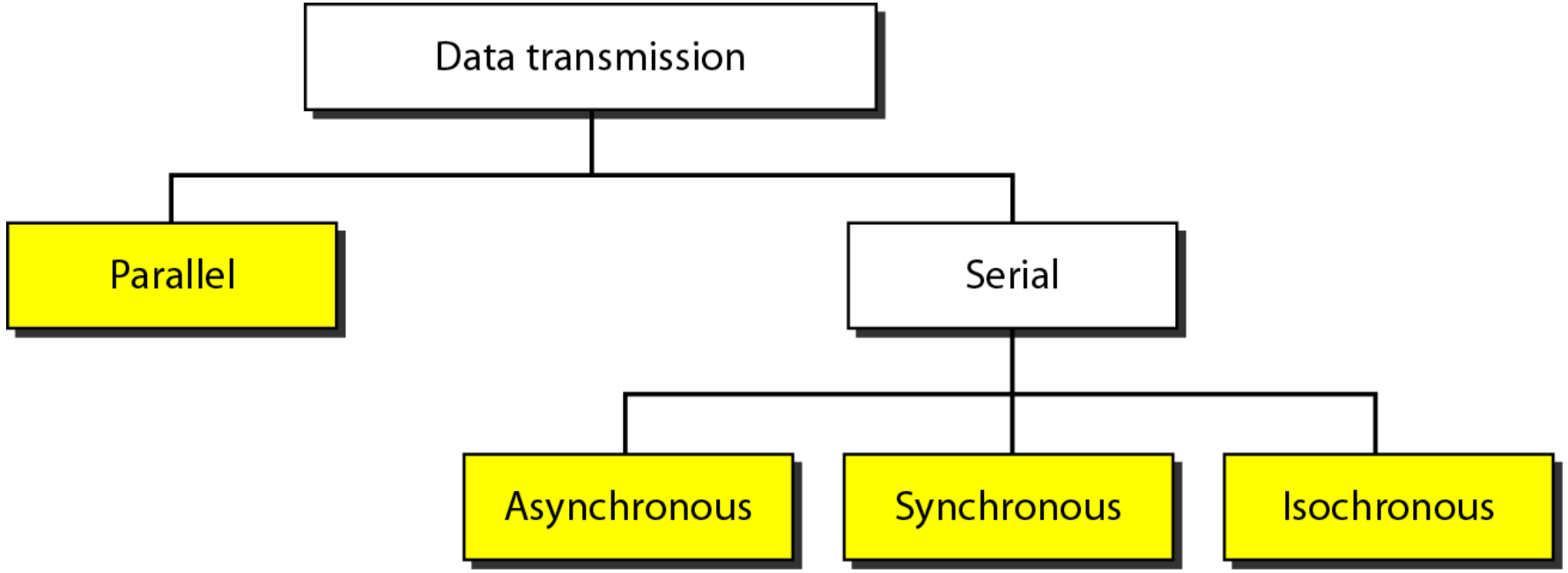


Figure *Parallel transmission*

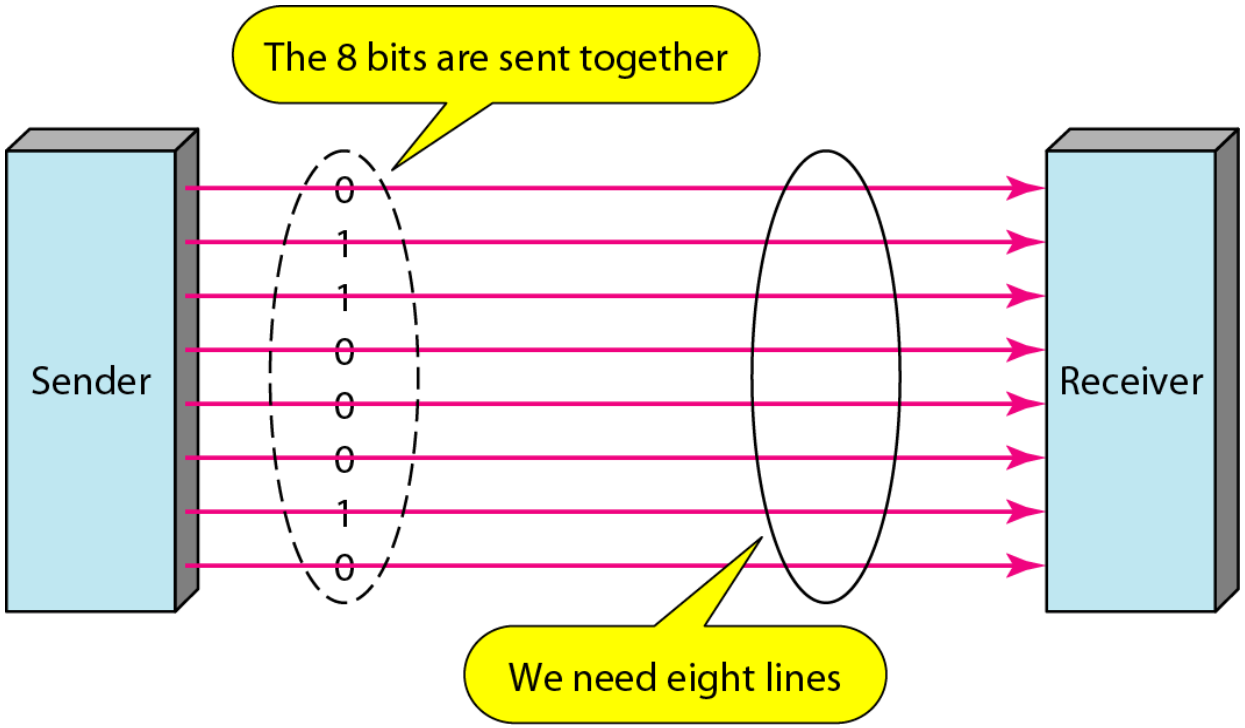
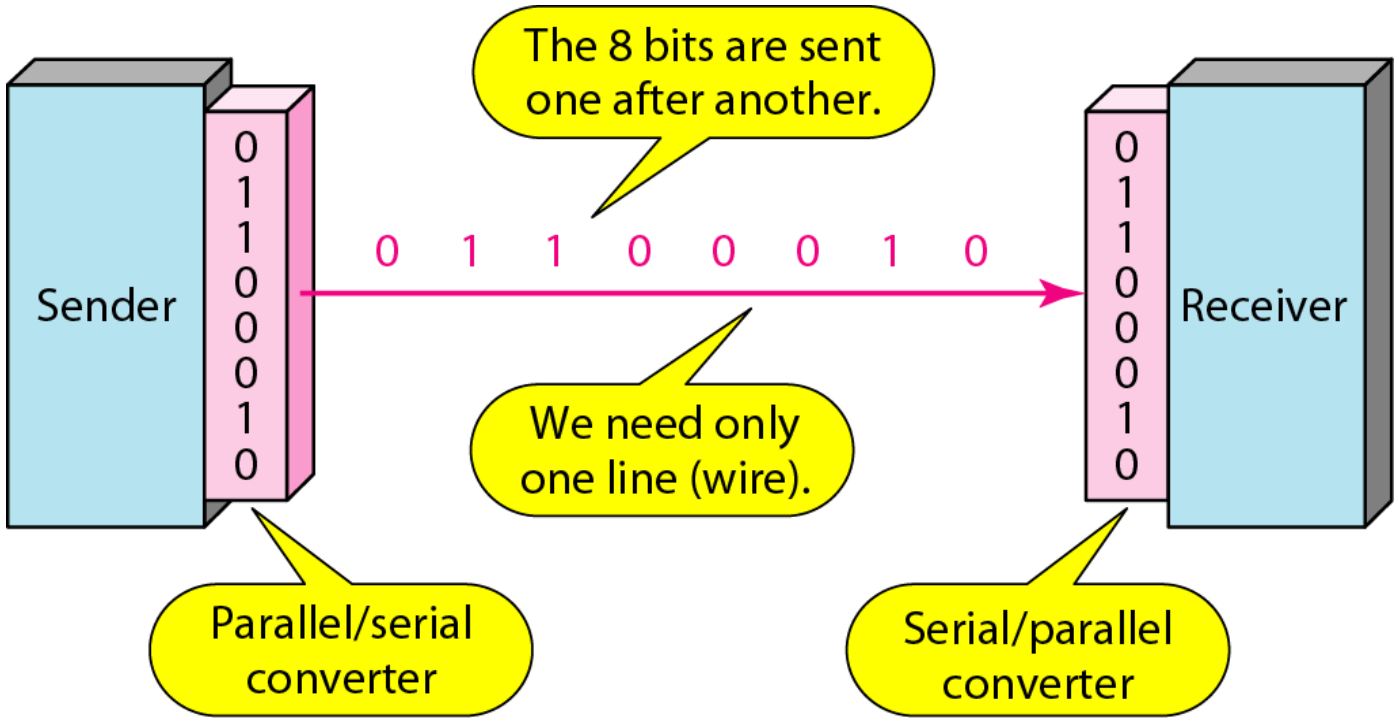


Figure *Serial transmission*



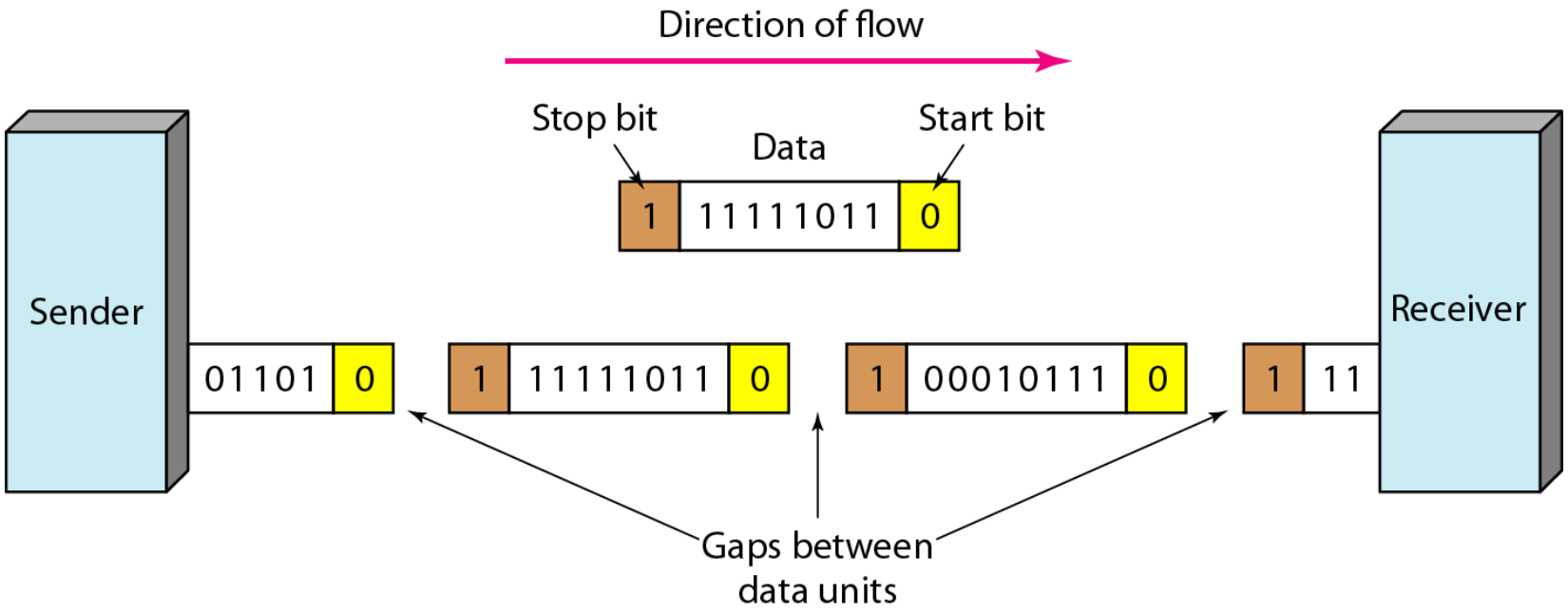
Note

In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte.

Note

Asynchronous here means "asynchronous at the byte level," but the bits are still synchronized; their durations are the same.

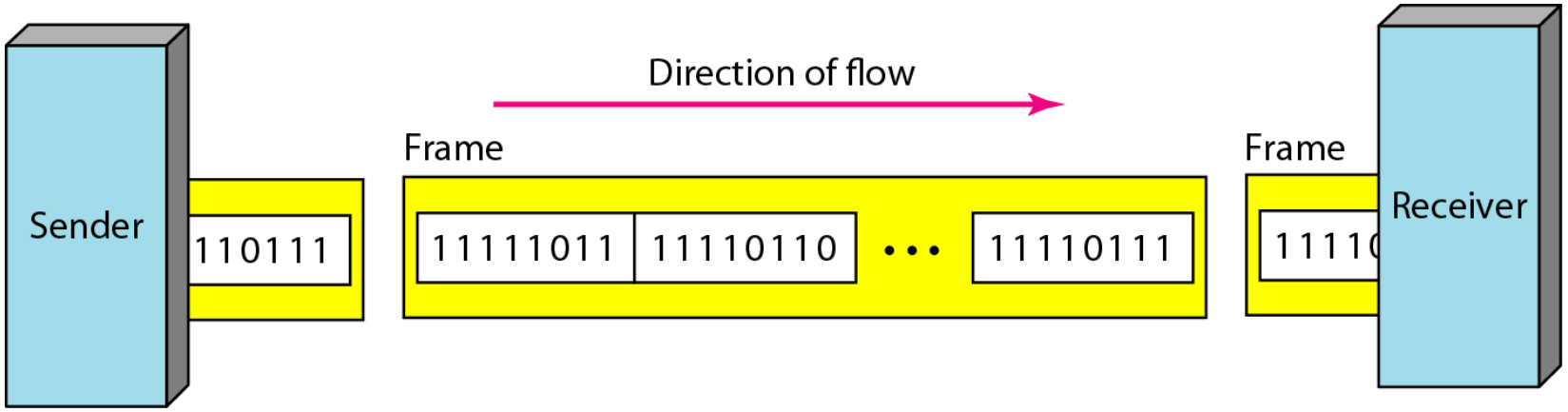
Figure *Asynchronous transmission*



Note

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits. The bits are usually sent as bytes and many bytes are grouped in a frame. A frame is identified with a start and an end byte.

Figure *Synchronous transmission*



Isochronous

- In isochronous transmission we cannot have uneven gaps between frames.

- Transmission of bits is fixed with equal gaps.

PERFORMANCE

One important issue in networking is the performance of the network—how good is it?.

- Bandwidth - capacity of the system
- Throughput - no. of bits that can be pushed through
- Latency (Delay) - delay incurred by a bit from start to finish

Note

Bandwidth

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

For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

Throughput

The throughput is a measure of how fast we can actually send data through a network.

Bandwidth and Throughput

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.

In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

Example

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

Example

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

$$\text{Throughput} = \frac{12{,}000 \times 10{,}000}{60} = 2 \text{ Mbps}$$

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

Latency (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

Latency = Propagation delay + Transmission delay + Queueing time + Processing time

Propagation Delay

Propagation Delay measures the time required for a bit to travel from the source to the destination

Propagation Delay = Distance/Propagation speed

Propagation speed - speed at which a bit travels though the medium from source to destination

For example, in a vacuum, light is propagated with a speed of 3×10^8 mbps

Transmission delay

Transmission Delay :The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

Transmission Delay = Message size/bandwidth bps

Example

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

Example

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

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

Example

What are the propagation time and the transmission time for a 2.5-kbyte message (an e-mail) 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 shown on the next slide:

Example

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

$$\text{Transmission time} = \frac{2500 \times 8}{10^9} = 0.020 \text{ ms}$$

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. The transmission time can be ignored.

Example

What are the propagation time and the transmission time for a 5-Mbyte 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 2.4×10^8 m/s.

Solution

We can calculate the propagation and transmission times as shown on the next slide.

Example

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

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

Note that in this case, because the message is very long and the bandwidth is not very high, the dominant factor is the transmission time, not the propagation time. The propagation time can be ignored.

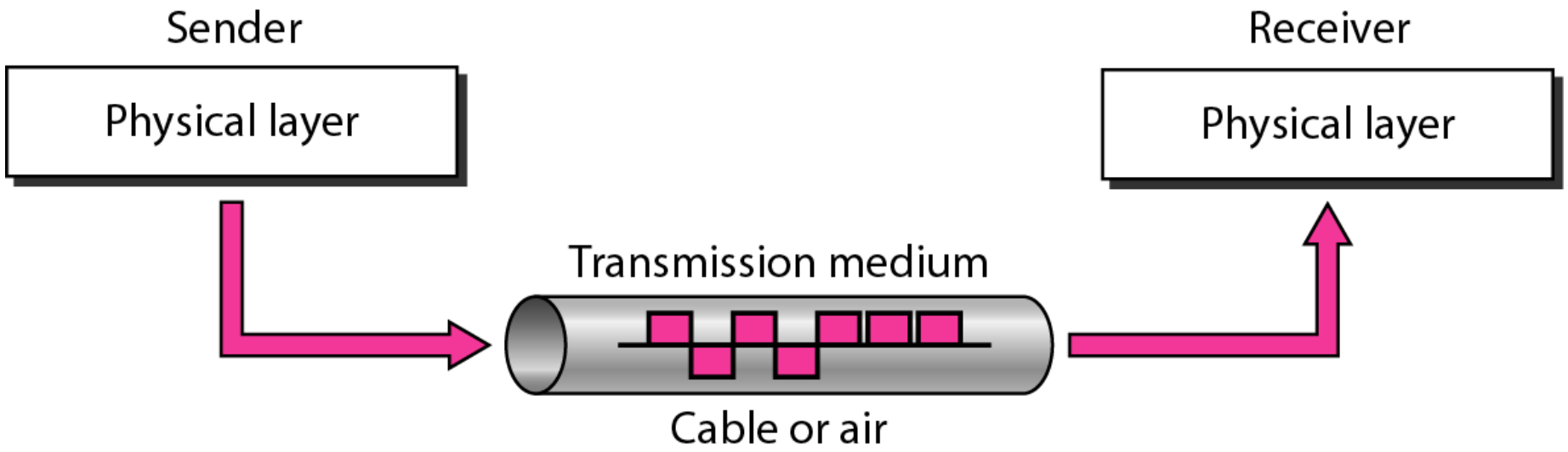
Queuing Time

- The time needed for each intermediate or end device to hold the message before it can be processed.

- The queuing time is not a fixed factor.

Transmission Medium

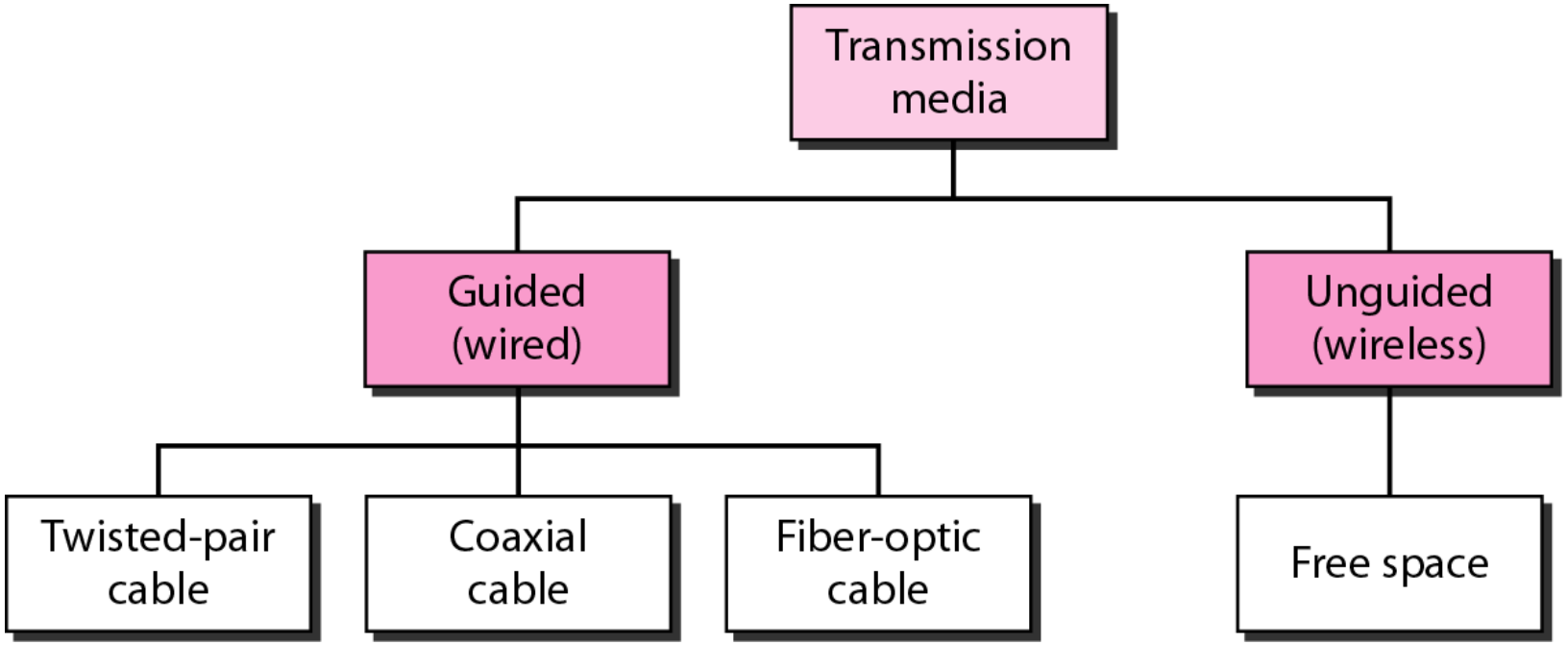
Figure *Transmission medium and physical layer*



Transmission Media

- Transmission media are actually located below the physical layer and are directly controlled by the physical layer.
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable, or fiber-optic cable.
- The information is usually a signal that is the result of a conversion of data from another form.

Figure *Classes of transmission media*



GUIDED MEDIA

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

Figure *Twisted-pair cable*

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference

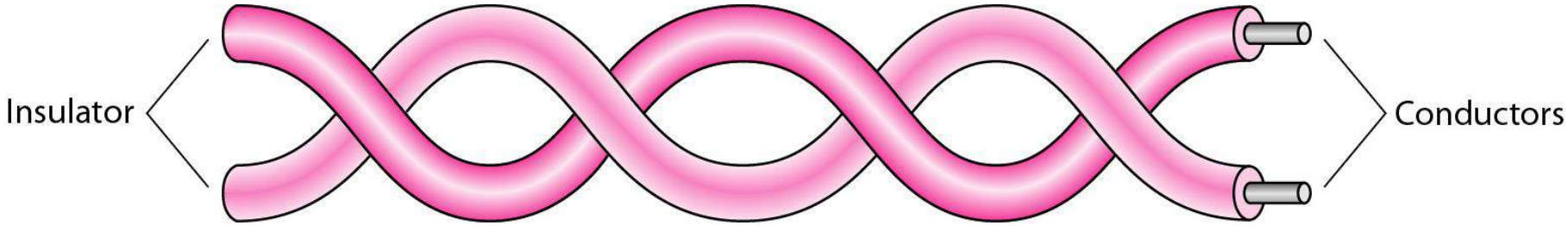
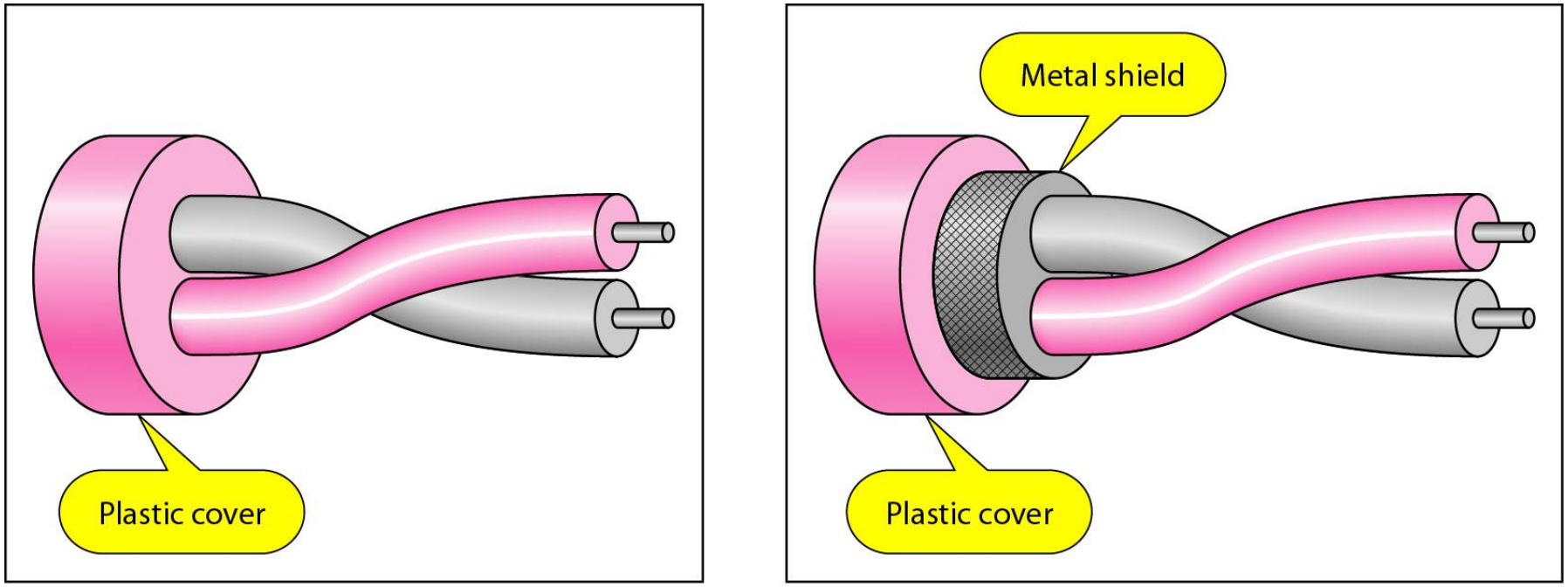


Figure *UTP and STP cables*

STP: Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive



a. UTP b. STP

Categories

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest

Table *Categories of unshielded twisted-pair cables*

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Figure *UTP connector*

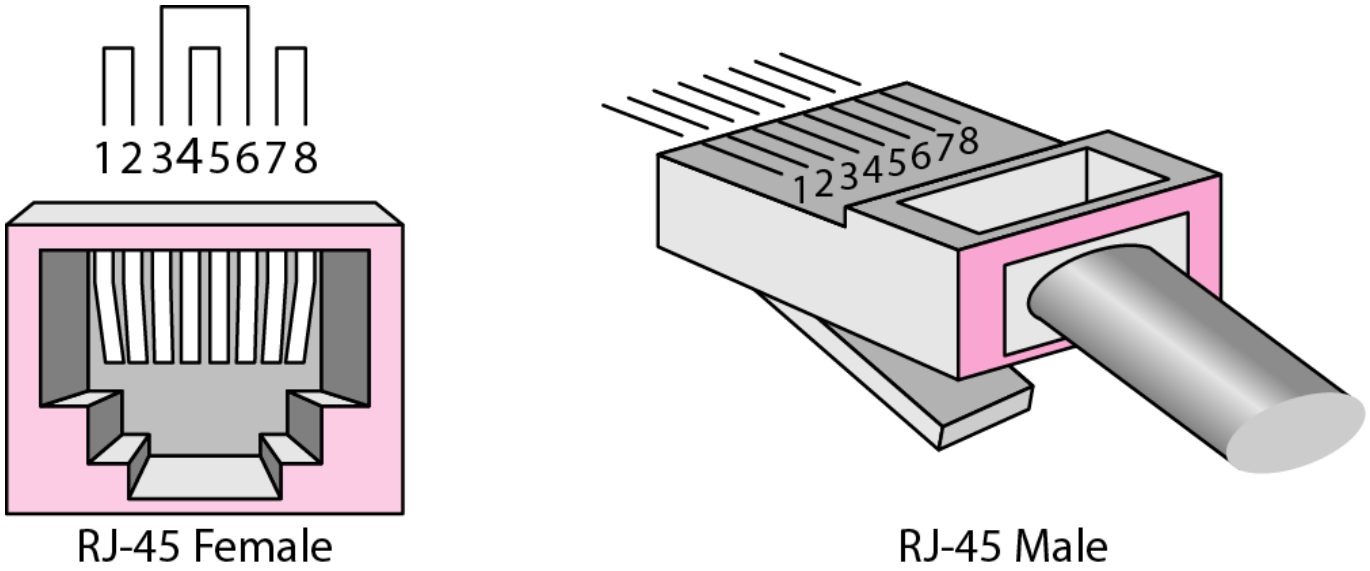
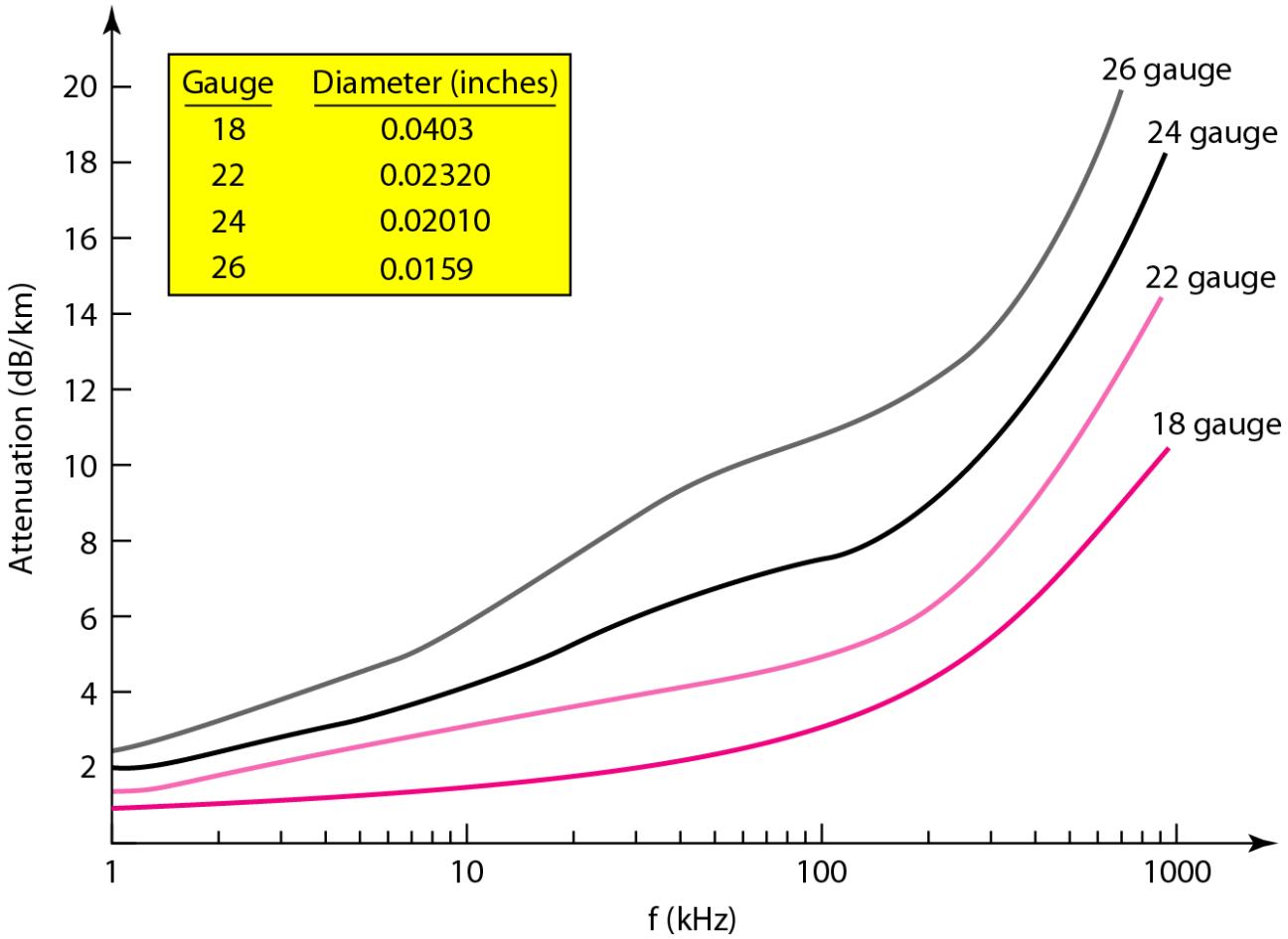


Figure *UTP performance: Performance One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance.*



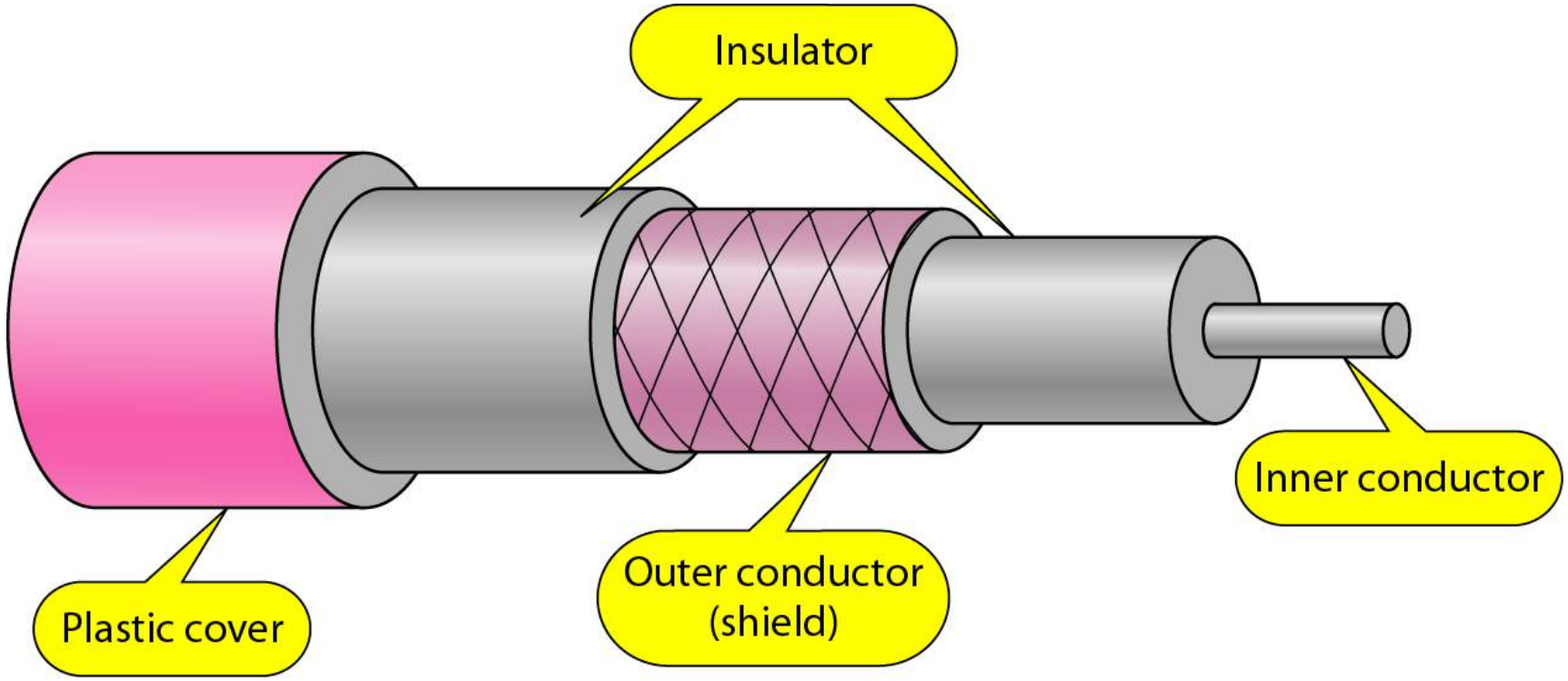
Applications

- Twisted-pair cables are used in telephone lines to provide voice and data channels.
- Local-area networks, such as lOBase-T and lOOBase-T.
- The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables

Coaxial cable

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable.
- TPC having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Figure *Coaxial cable*



Categories of coaxial cables

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Figure *BNC connectors*

The BNC connector is used to connect the end of the cable to a device, such as a TV set.

The BNC T connector is used in Ethernet networks (see Chapter 13) to branch out to a connection to a computer or other device.

The BNC terminator is used at the end of the cable to prevent the reflection of the signal

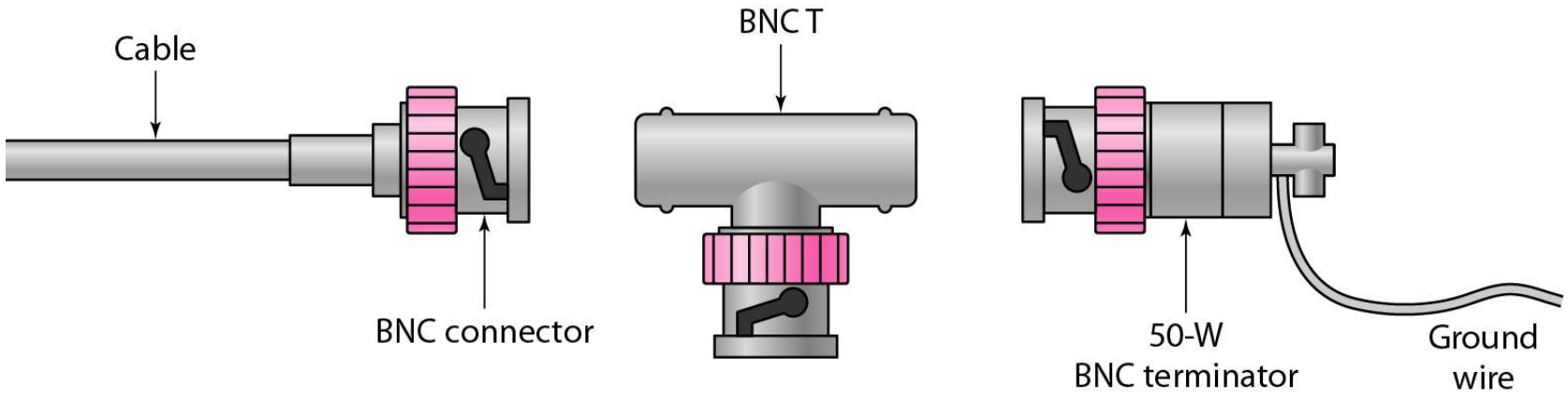
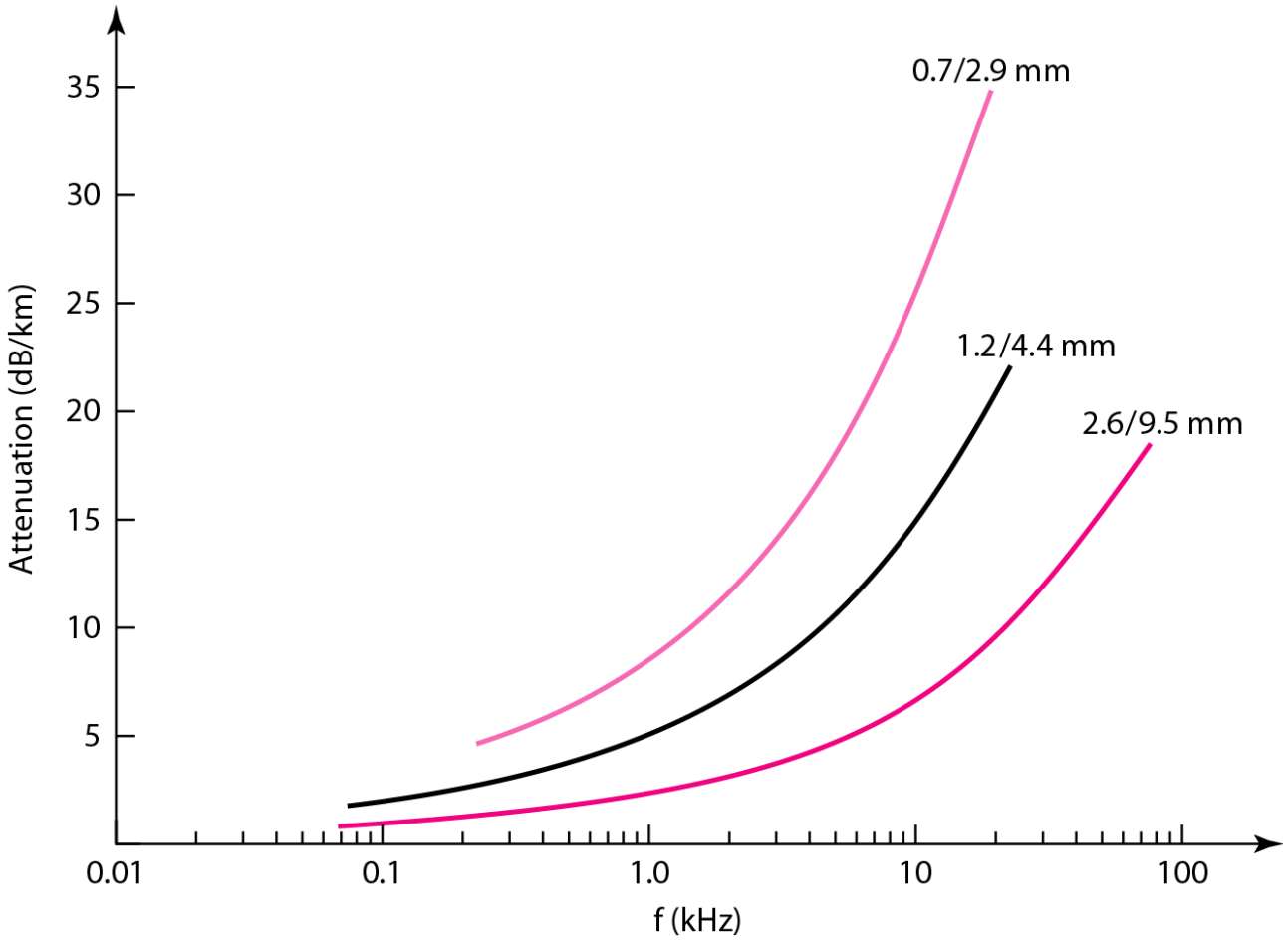


Figure *Coaxial cable performance*



Application

- Coaxial cable was widely used in analog telephone networks
- Cable TV networks also use coaxial cables
- Another common application of coaxial cable is in traditional Ethernet LANs

Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

Figure: Fiber optics: *Bending of light ray*

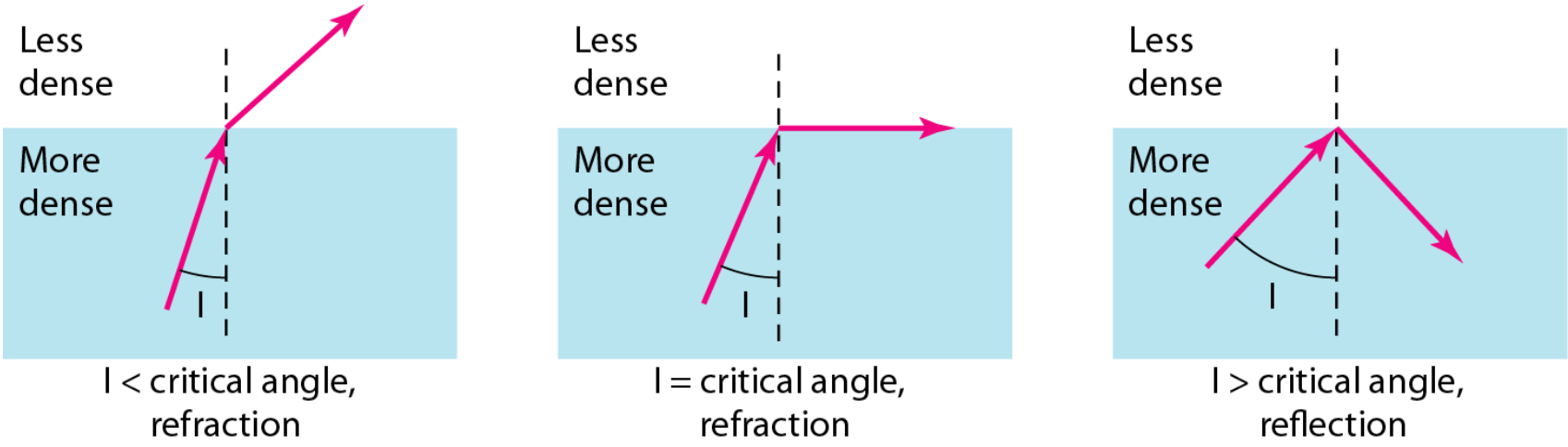


Figure *Optical fiber*

A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it

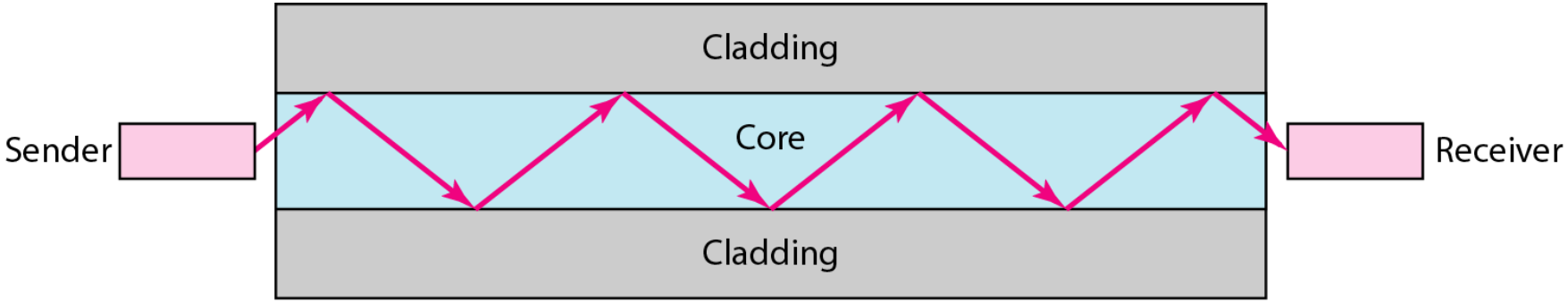
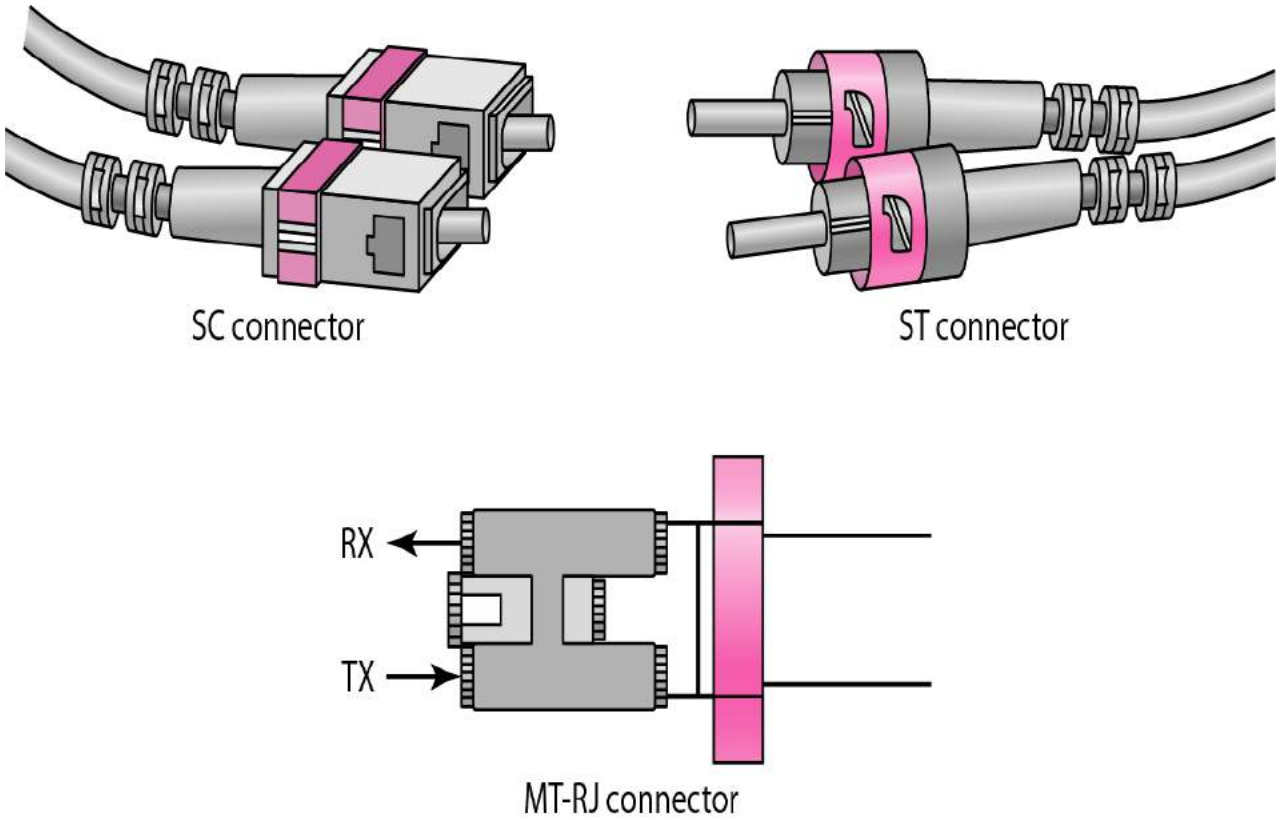


Figure *Fiber-optic cable connectors*



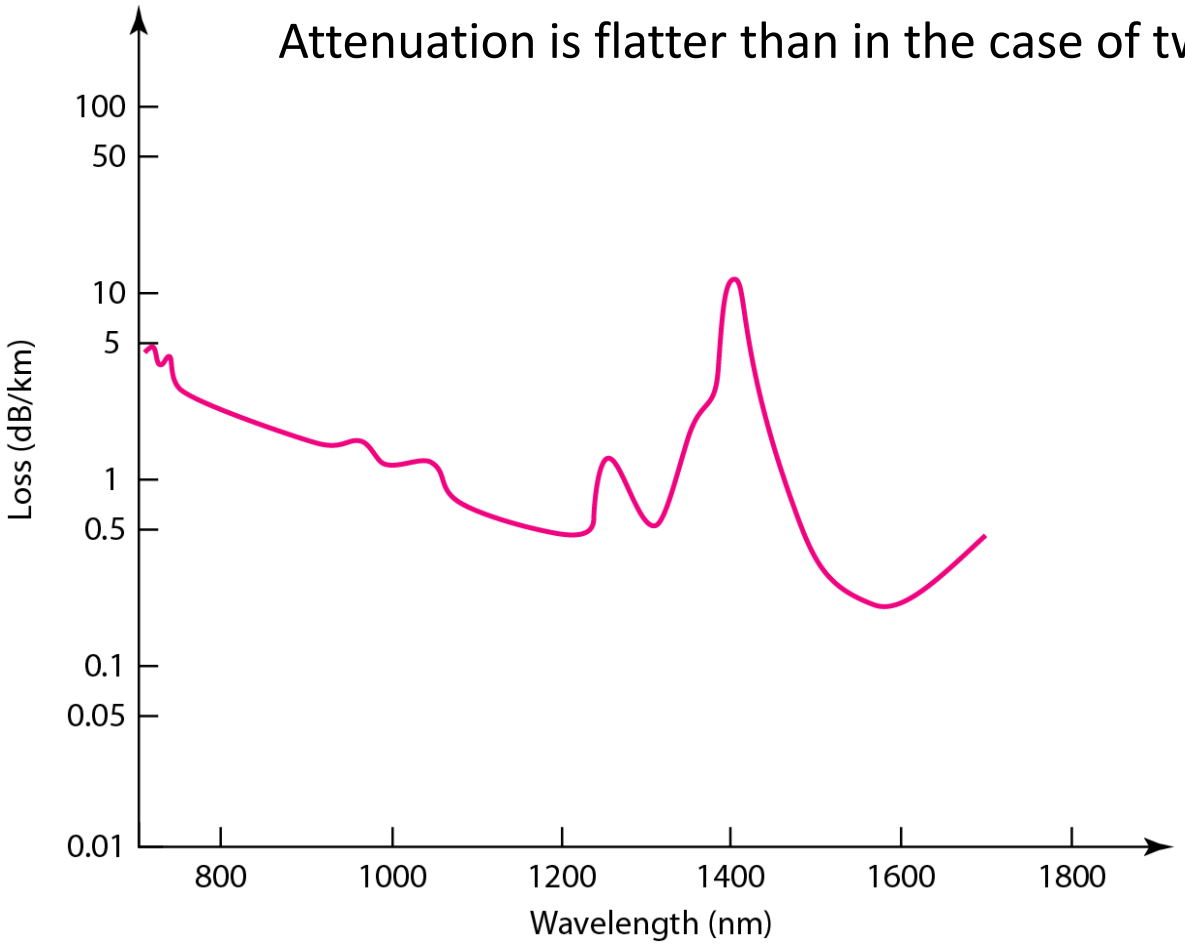
The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system.

The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.

MT-RJ is a connector that is the same size as RJ45

Figure *Optical fiber performance*

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable



Application

Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network

Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber

- **Adv:**
- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Light weight

- **Dis:**
- Unidirectional light propagation
- Cost.

UNGUIDED MEDIA: WIRELESS

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Figure *Electromagnetic spectrum for wireless communication*

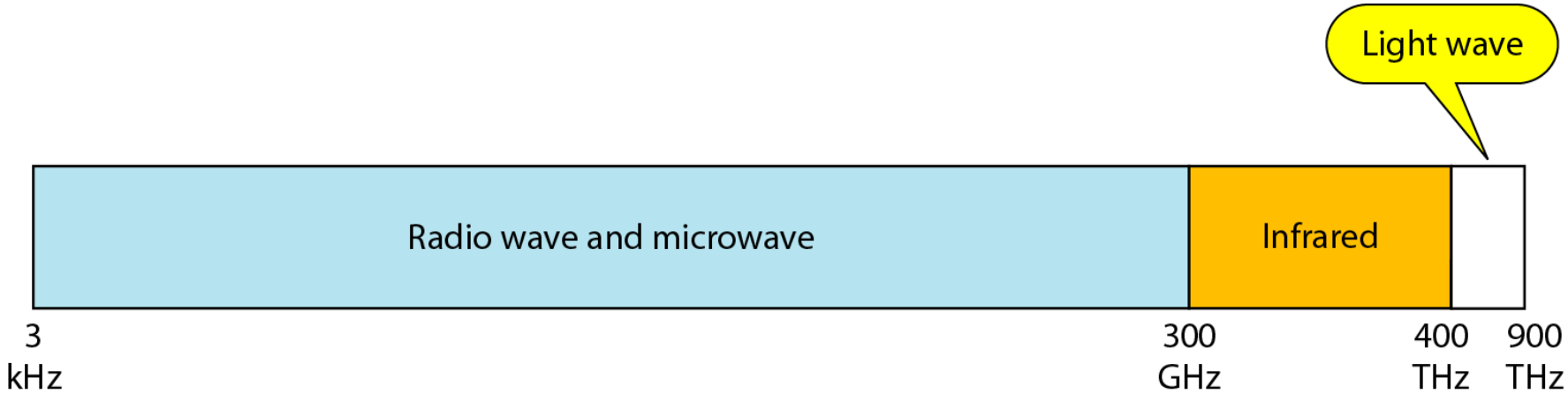


Figure *Propagation methods*

Unguided signals can travel from the source to destination in several ways

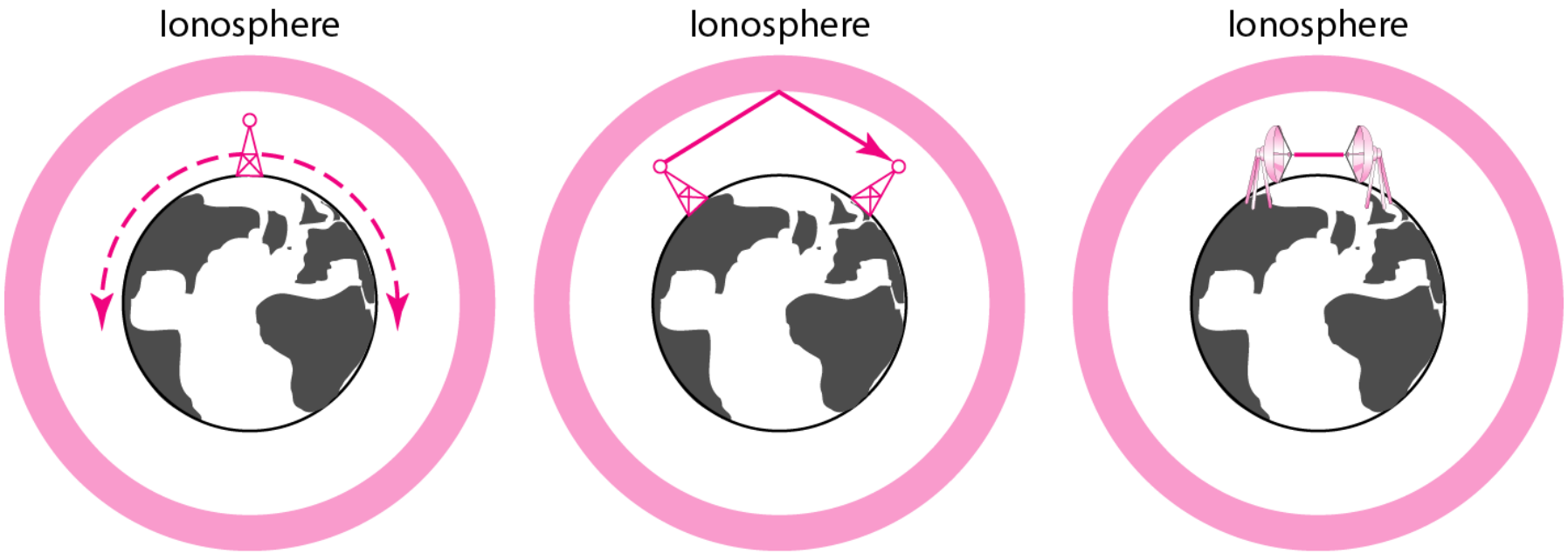
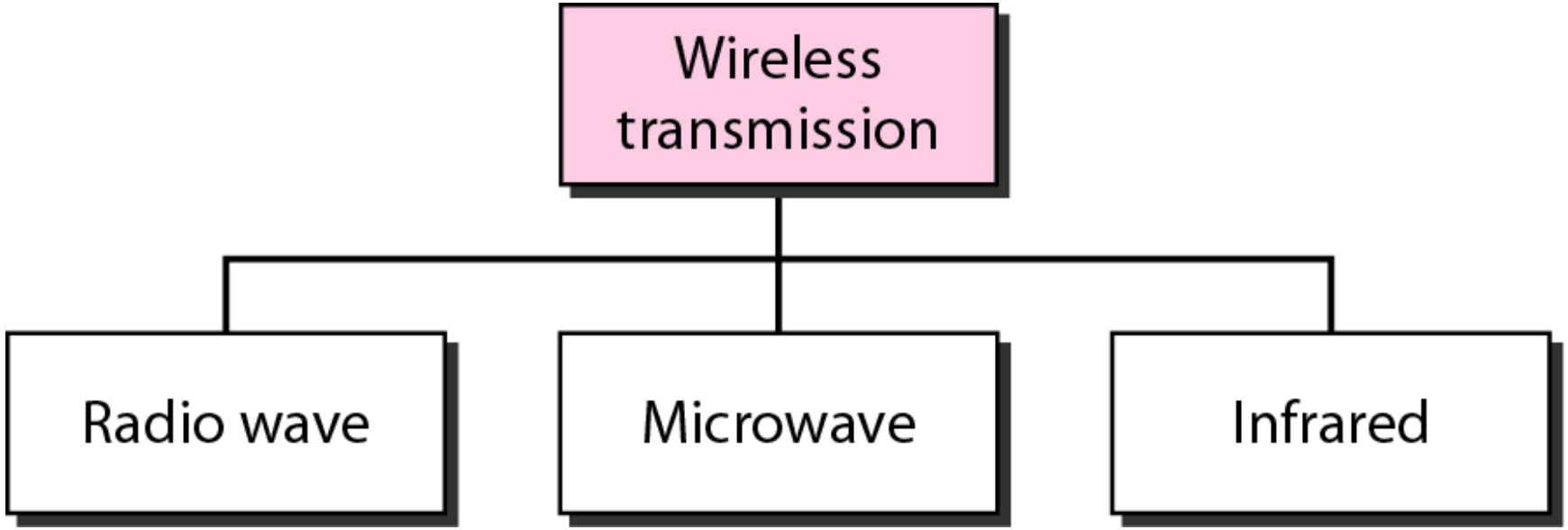


Table *Bands*

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite

Figure *Wireless transmission waves*

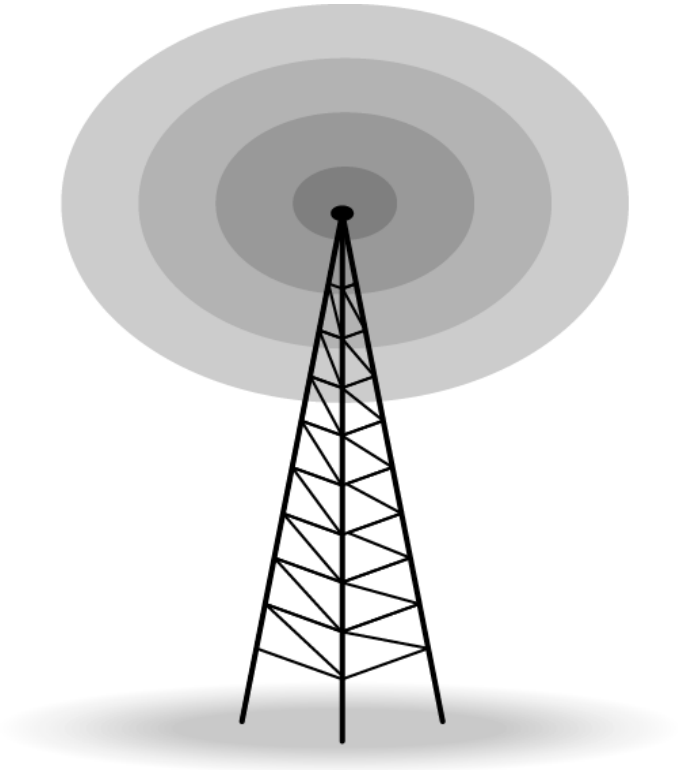


Note

Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls.
Highly regulated. Use omni directional antennas

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves

Figure *Omnidirectional antenna*



Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission

Application

- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.

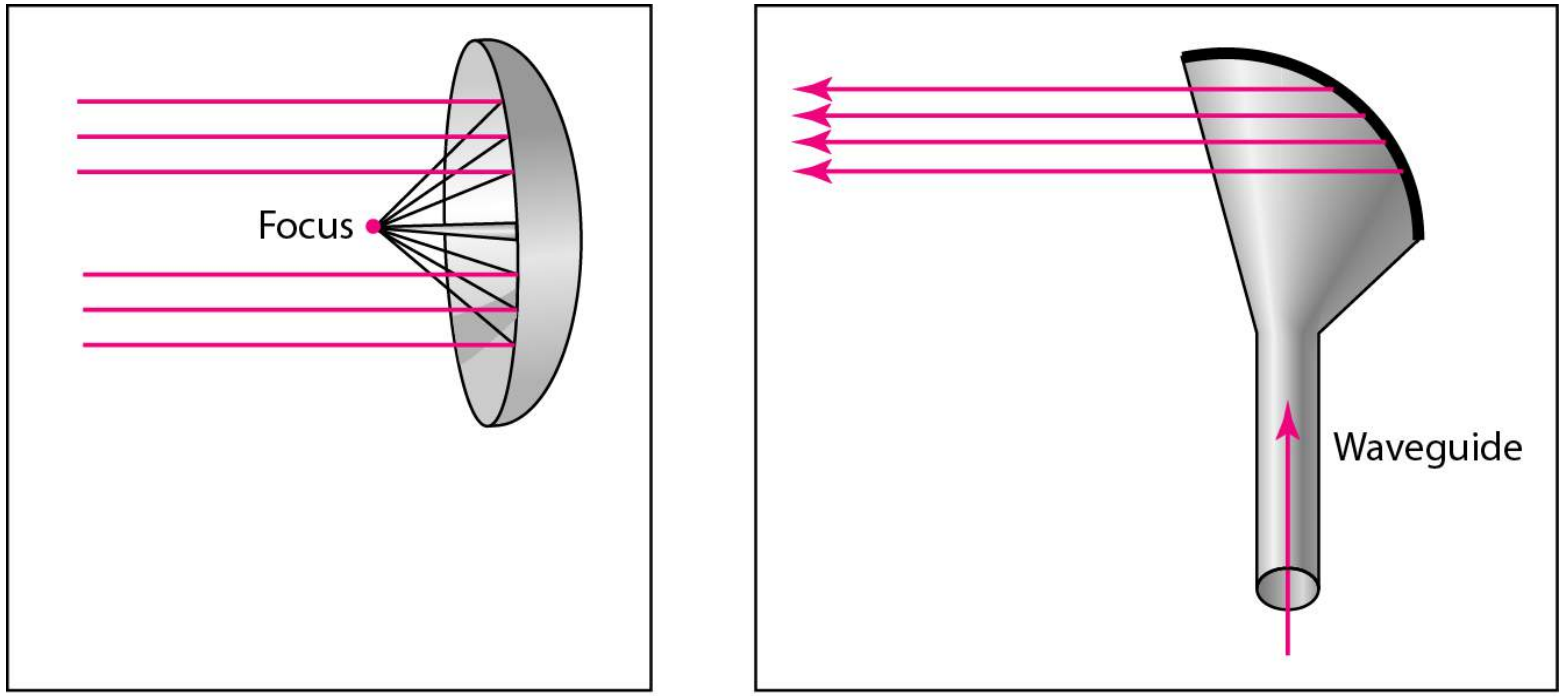
- AM and FM radio, television, maritime radio, cordless phones are examples of multicasting.

Note

Microwaves are used for unicast communication such as cellular telephones, satellite networks,
and wireless LANs.
Higher frequency ranges cannot penetrate walls.
Use directional antennas - point to point line of sight communications.

Electromagnetic waves having frequencies between I and 300 GHz are called microwaves.

Figure *Unidirectional antennas*



a. Dish antenna

b. Horn antenna

Note

Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

SWITCHING

Switching

- A switched network consists of a series of interlinked nodes, called switches.
- Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
- In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

Figure *Switched network*

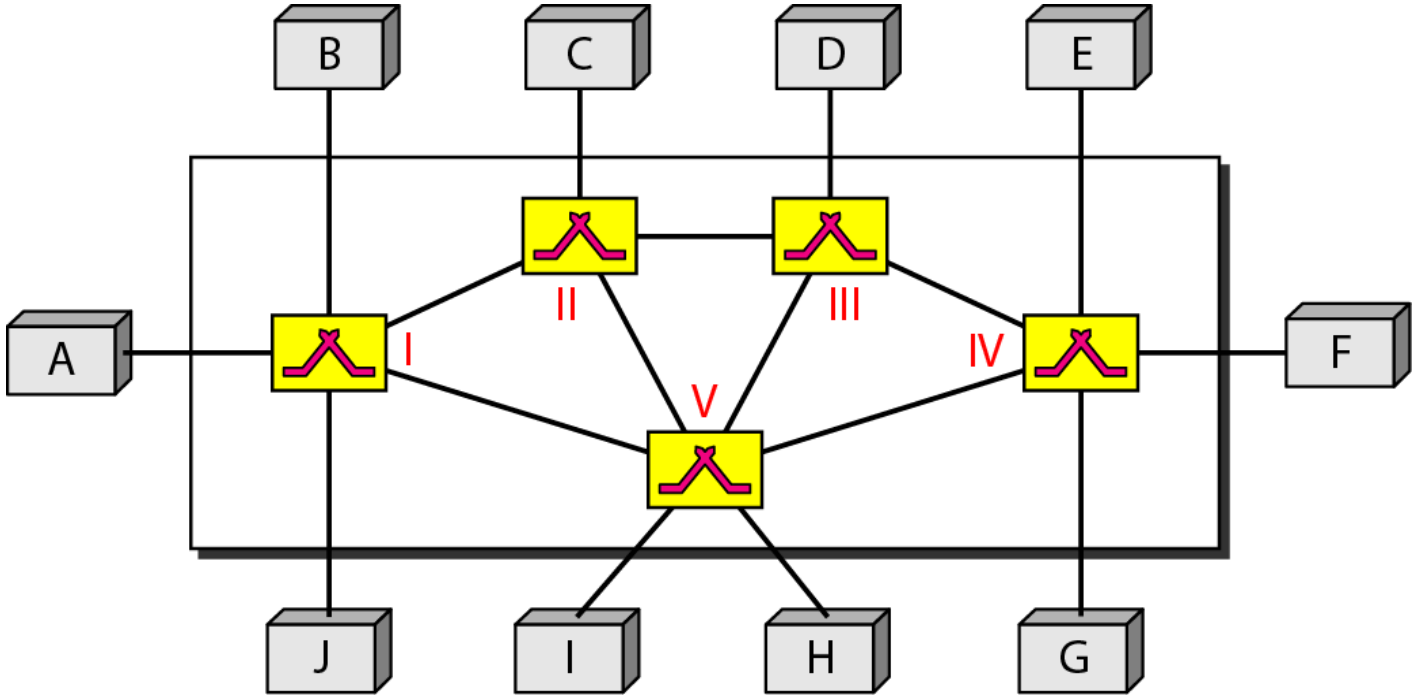
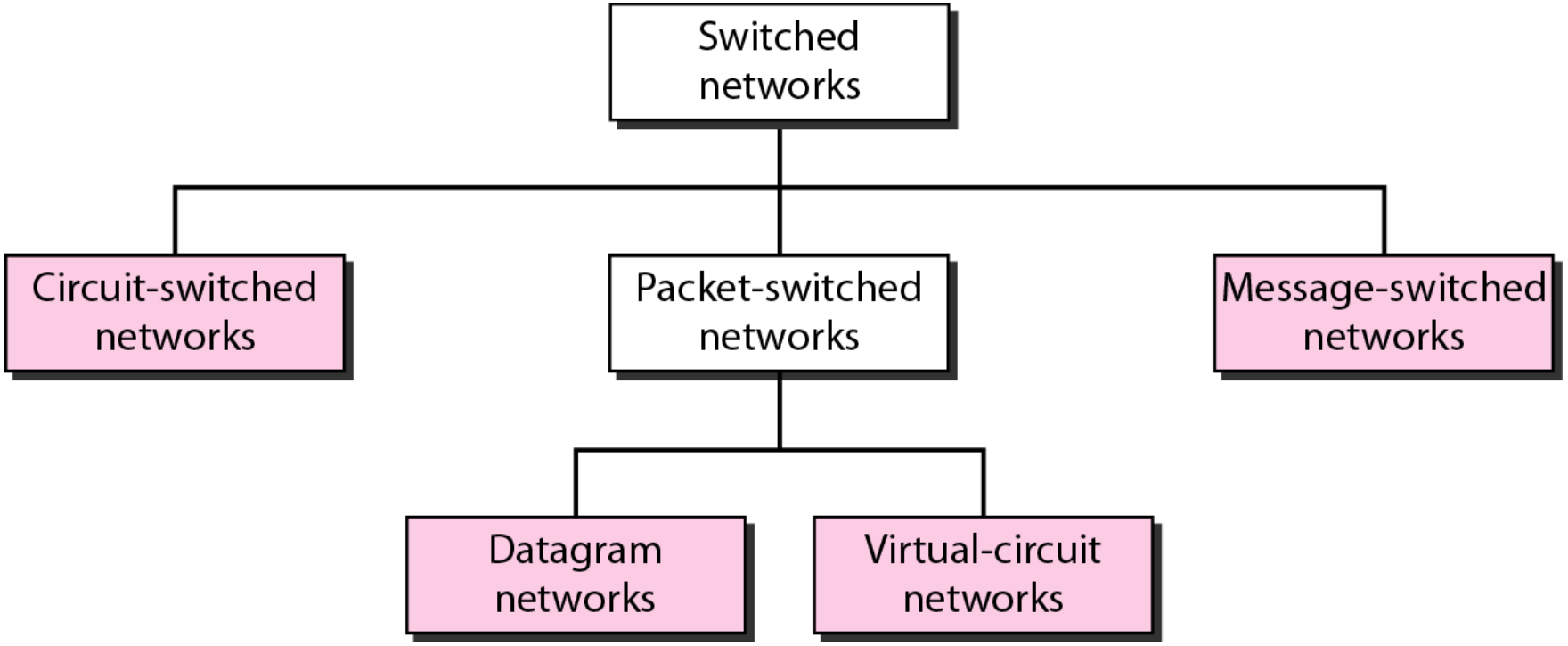


Figure *Taxonomy of switched networks*



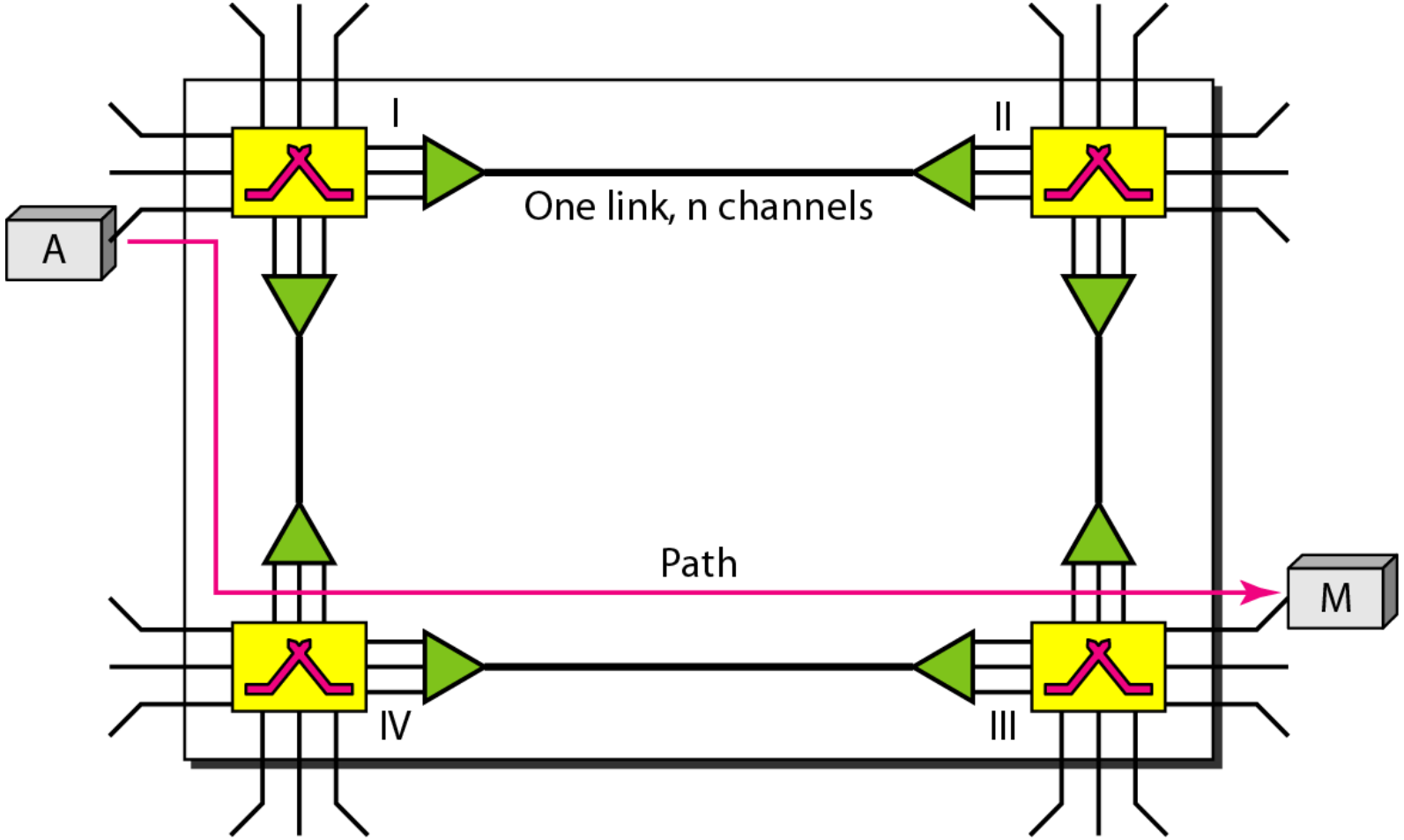
CIRCUIT-SWITCHED NETWORKS

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.

Note

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

Figure: *A trivial circuit-switched network*



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 tear down.

Circuit switching takes place at the physical layer.

Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as, switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.

Data transferred between the two stations are not packetized. The data are a continuous flow sent by the source station and received by the destination station,

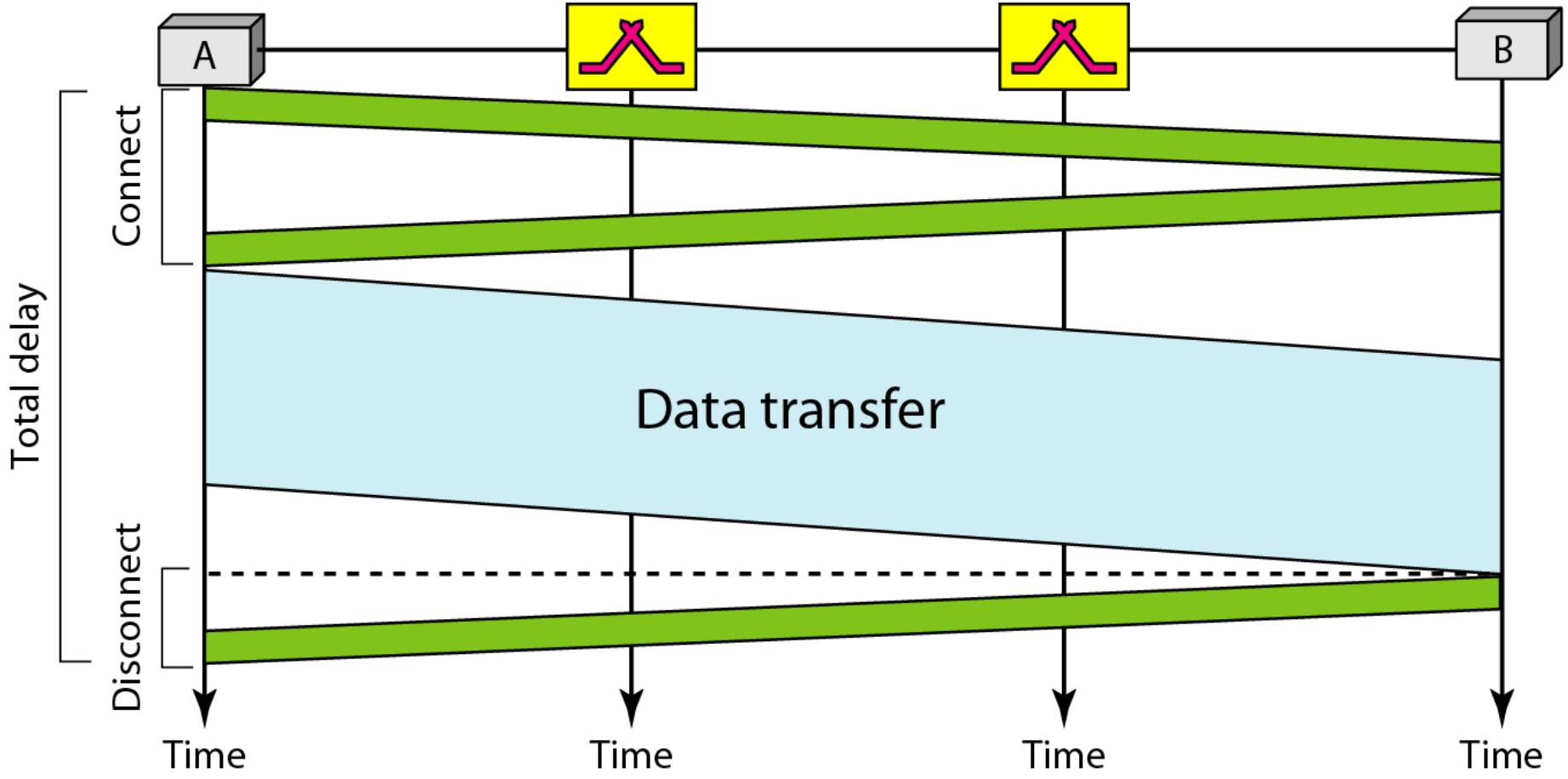
Note

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.

Three Phases

1. Setup Phase
2. Data Transfer Phase
3. Teardown Phase

Figure: *Delay in a circuit-switched network*



Efficiency and Delay

Circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection.

These resources are unavailable to other connections.

The delay in this type of network is minimal.

The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit

Note

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

DATAGRAM NETWORKS

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.

- In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet.
- Resources are allocated on demand.
- In a datagram network, each packet is treated independently of all others.
- Packets in this approach are referred to as datagrams.
- Datagram switching is normally done at the network layer

The datagram networks are sometimes referred to as connectionless networks.

The term connectionless here means that the switch (packet switch) does not keep information about the connection state.

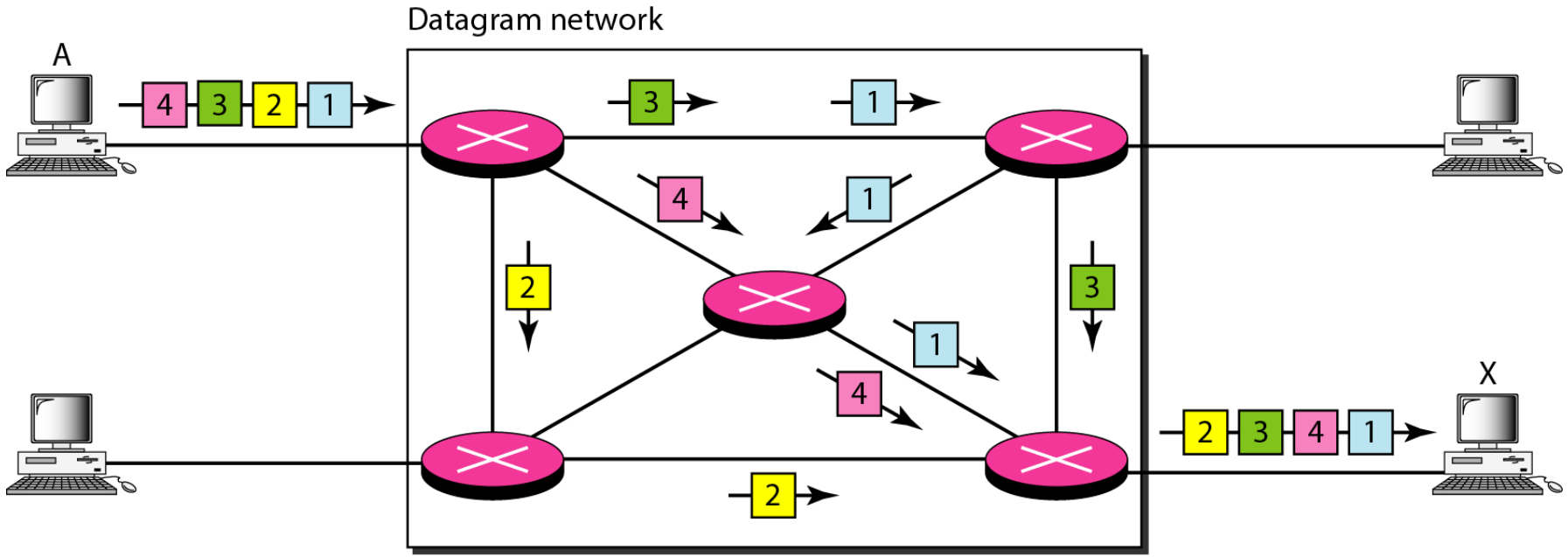
There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

Note

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

Figure: *A datagram network with four switches (routers)*

how the datagram approach is used to deliver four packets from station A to station X



Routing Table

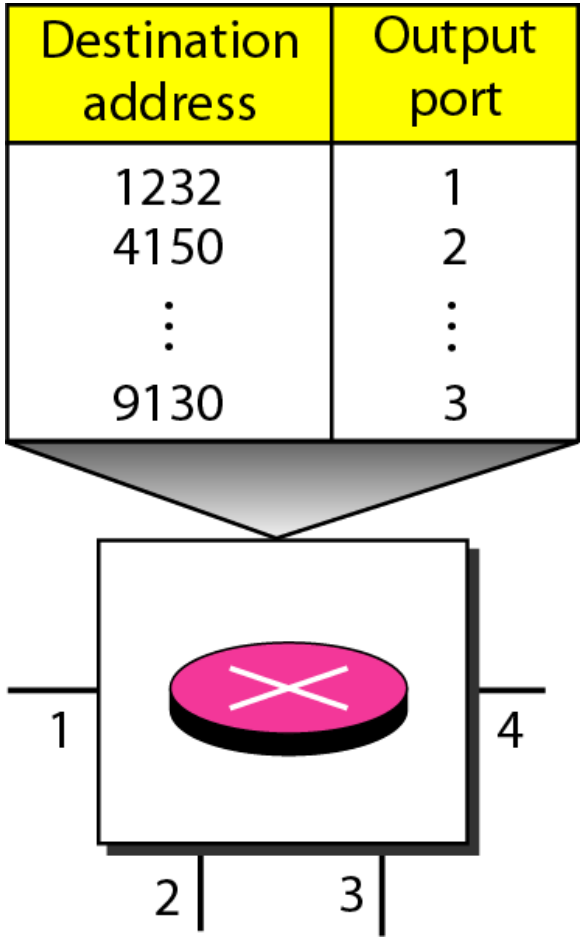
If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network?

each switch has a routing table which is based on the destination address.

The routing tables are dynamic and are updated periodically.

The destination addresses and the corresponding forwarding output ports are recorded in the tables.

Figure: *Routing table in a datagram network*



Note

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

Note

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

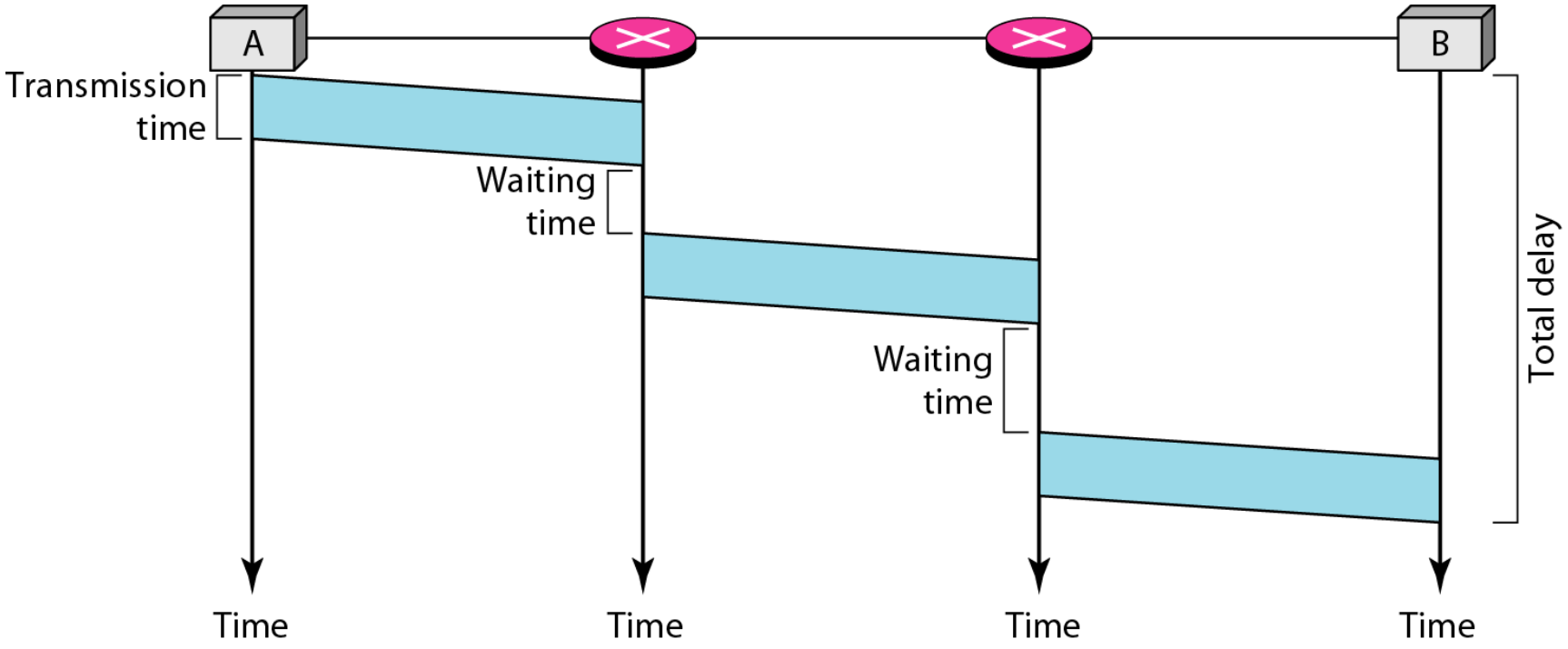
Efficiency and Delay

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred.

There may be greater delay in a datagram network than in a circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded.

Figure :*Delay in a datagram network*

Total delay =3T+ 3t +WI + W2



Note

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

VIRTUAL-CIRCUIT NETWORKS

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

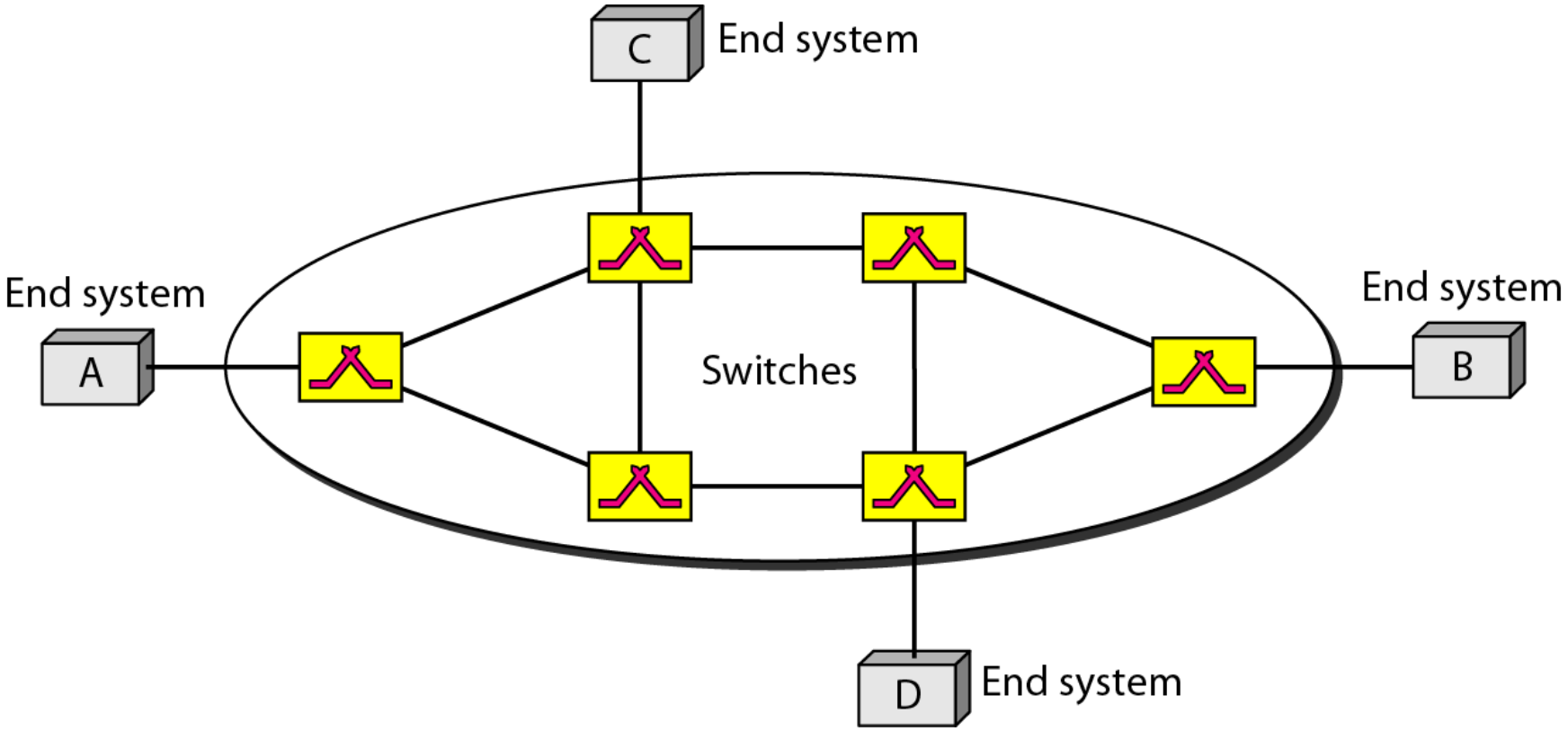
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction ,not end-to-end jurisdiction.

4. As in a circuit-switched network, all packets follow the same path established during the connection.

5. A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is Physical

Figure: *Virtual-circuit network*



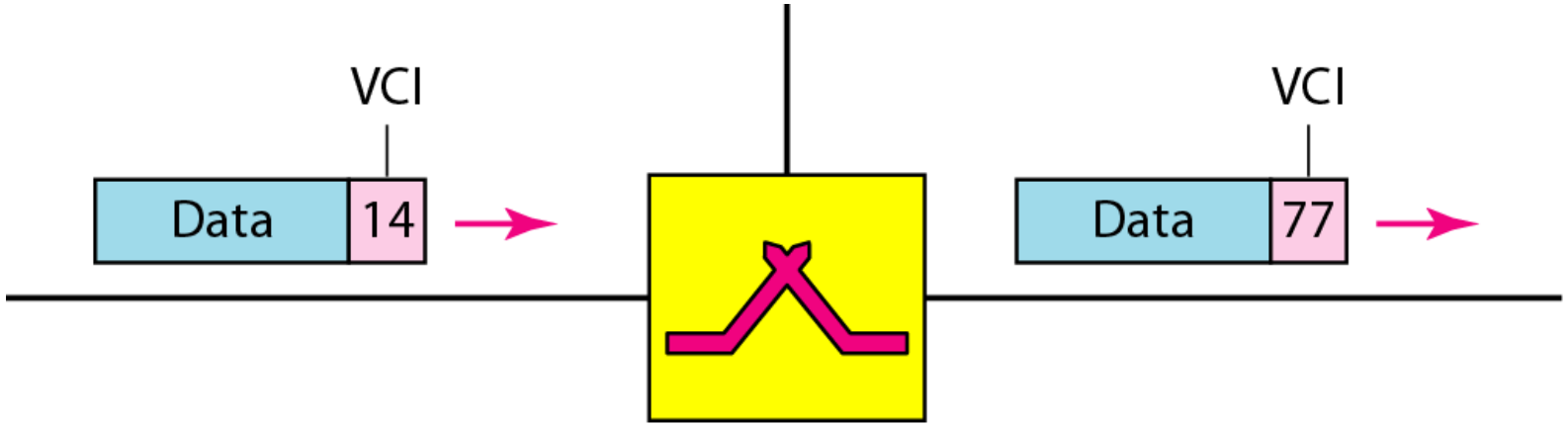
Addressing

Global Addressing A source or a destination needs to have a global address-an address that can be unique.

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

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 VCl.

Figure: *Virtual-circuit identifier*



Three Phase

Setup

Data transfer

Teardown

Figure: *Switch and tables in a virtual-circuit network*

Data Transfer Phase

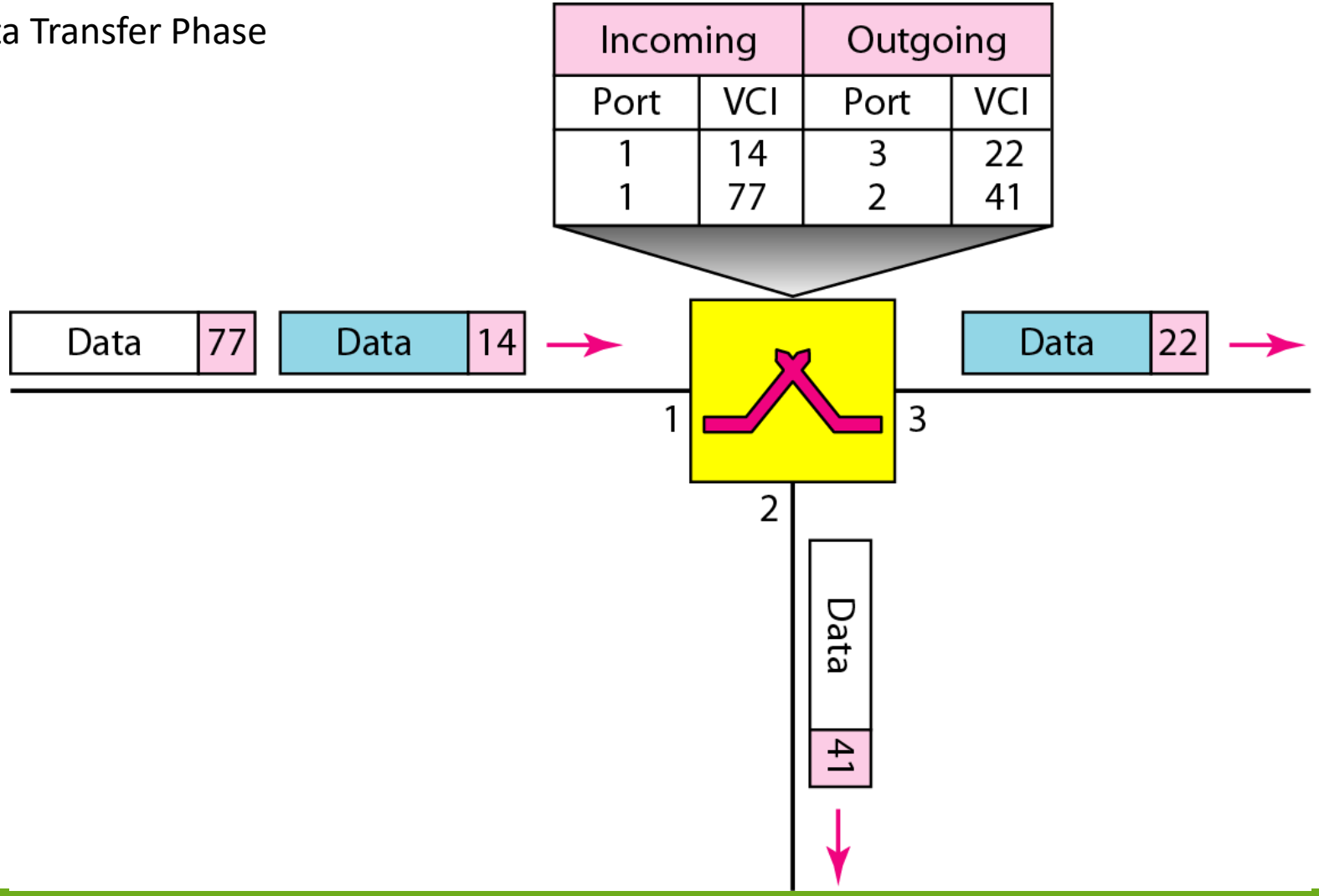
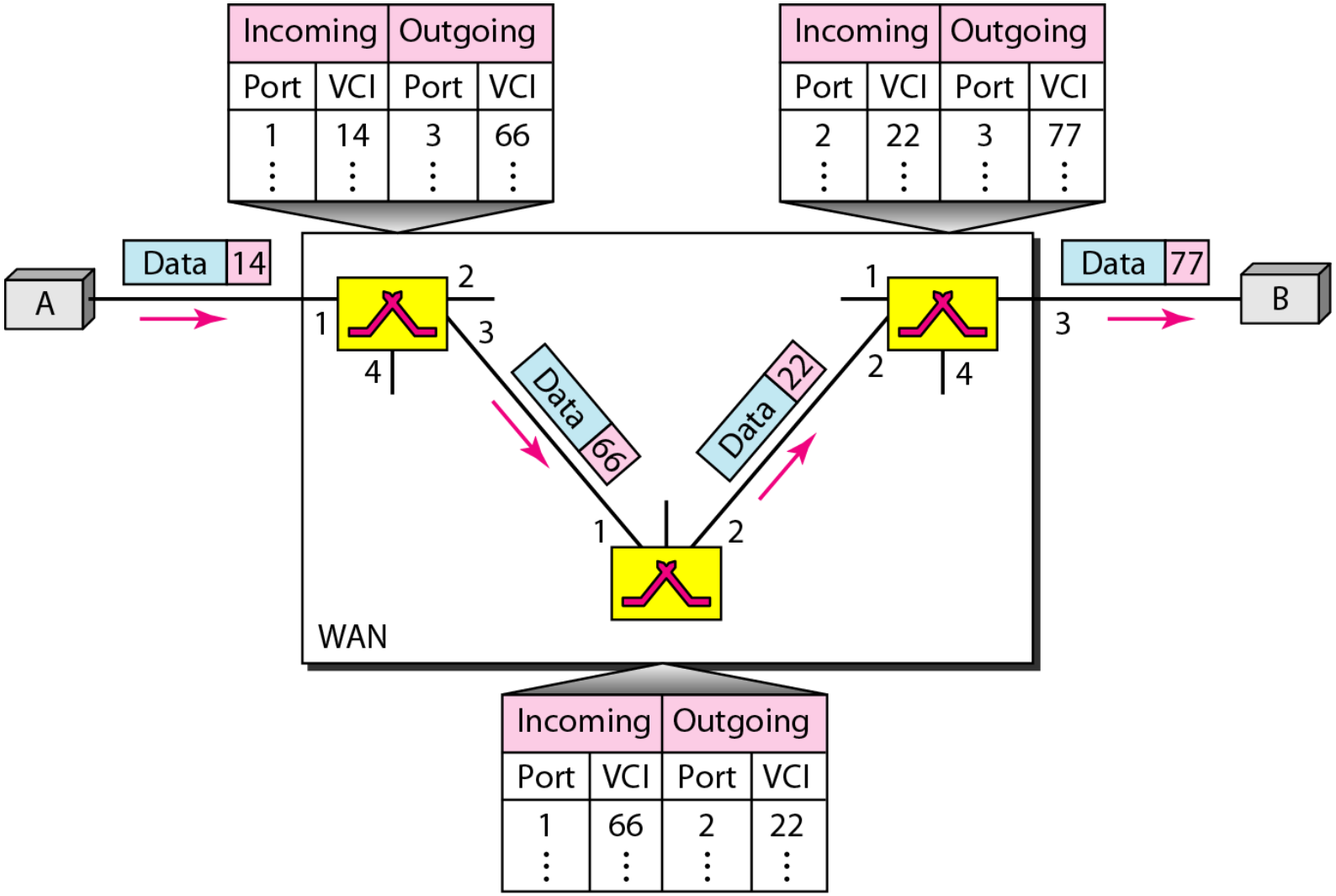


Figure :*Source-to-destination data transfer in a virtual-circuit network*

how a frame from source A reaches destination B and

how its VCI changes during the trip. Each switch changes the VCI and routes the frame.



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:

1. the setup request and
2. the acknowledgment

Figure: *Setup request in a virtual-circuit network*

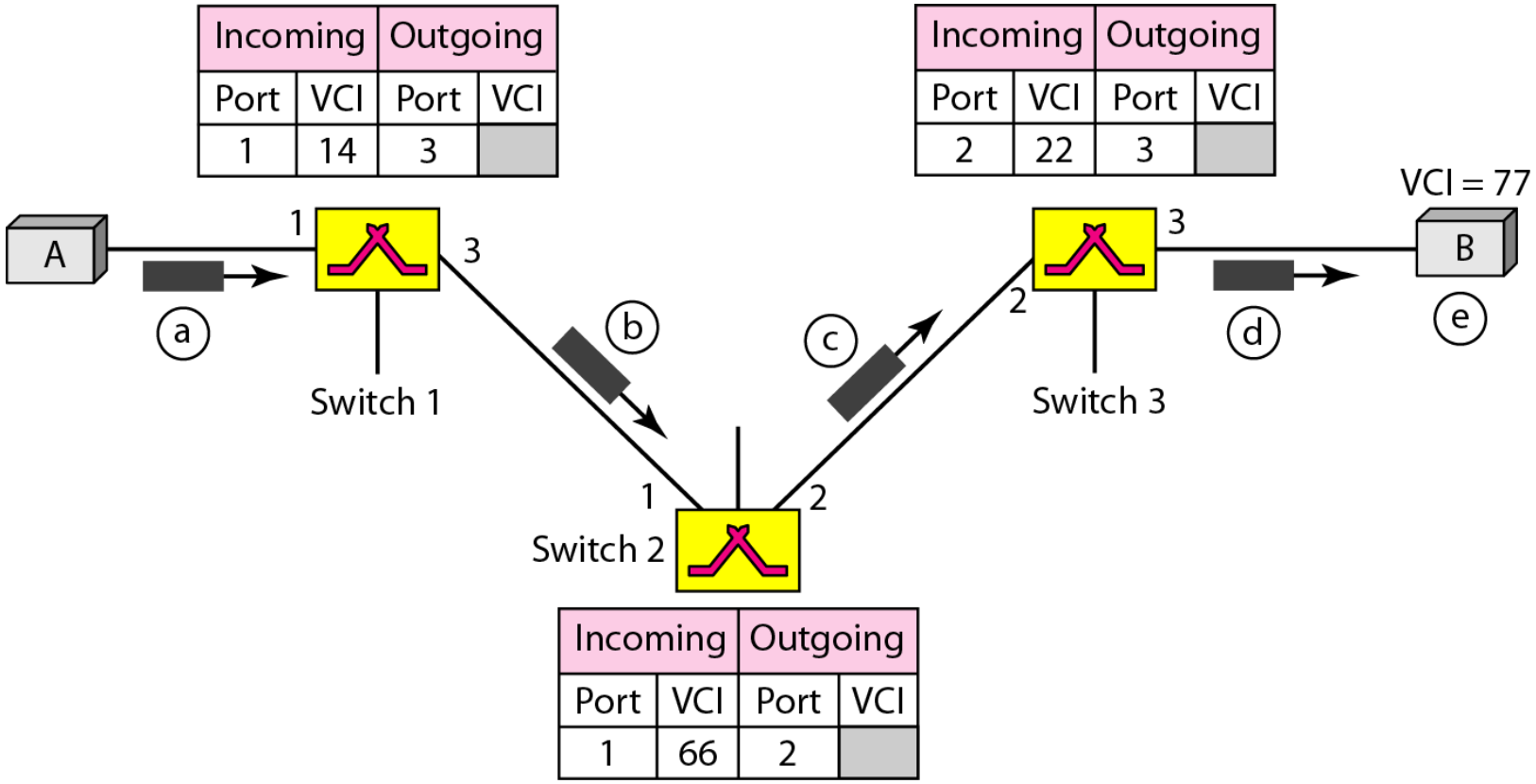
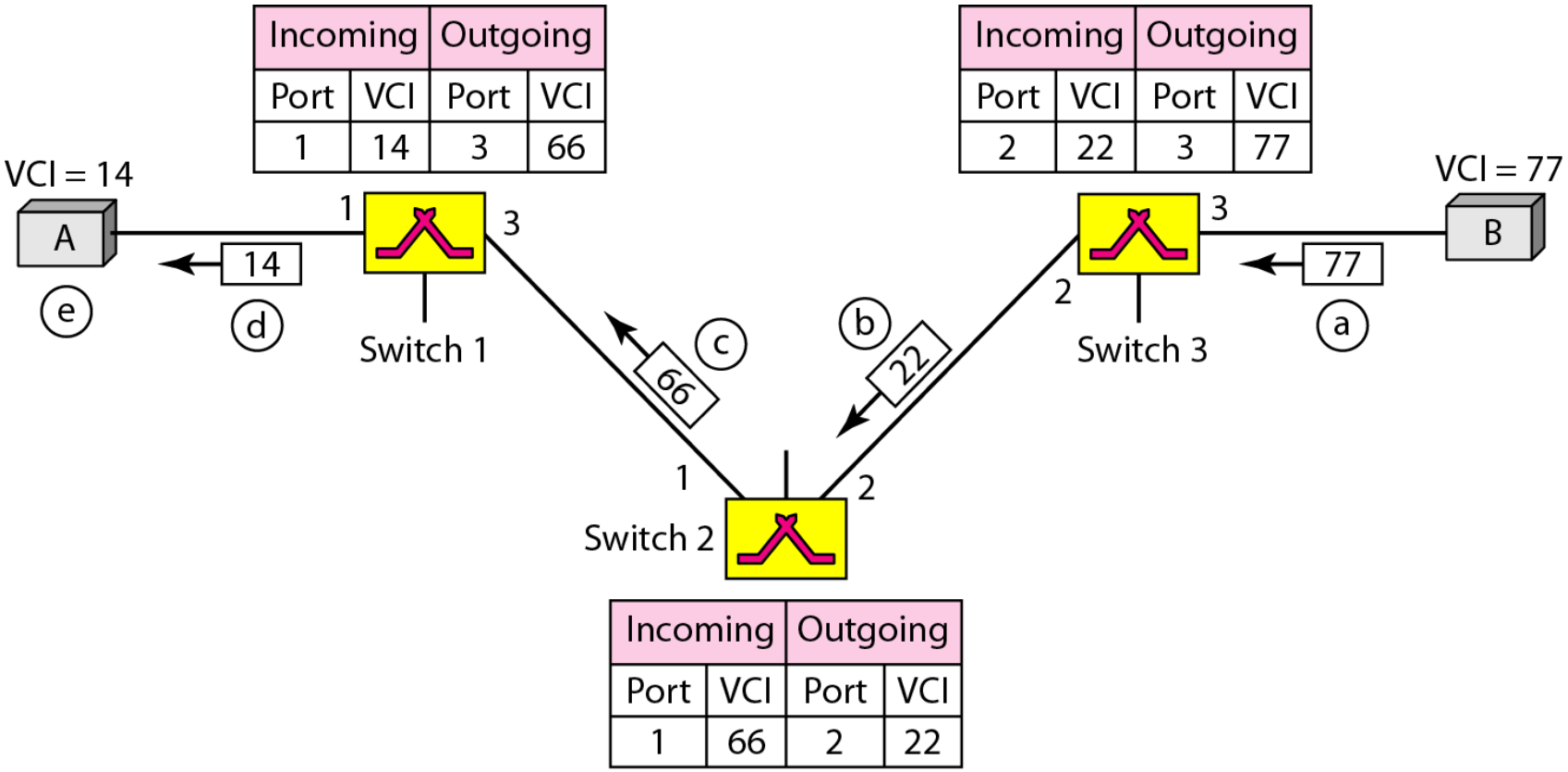


Figure: *Setup acknowledgment in a virtual-circuit network*



Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a teardown request. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables

Note

In virtual-circuit switching, all packets belonging to the same source and destination travel the same path;
but the packets may arrive at the destination with different delays if resource allocation is on demand.

Efficiency and Delay

Resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data transfer phase.

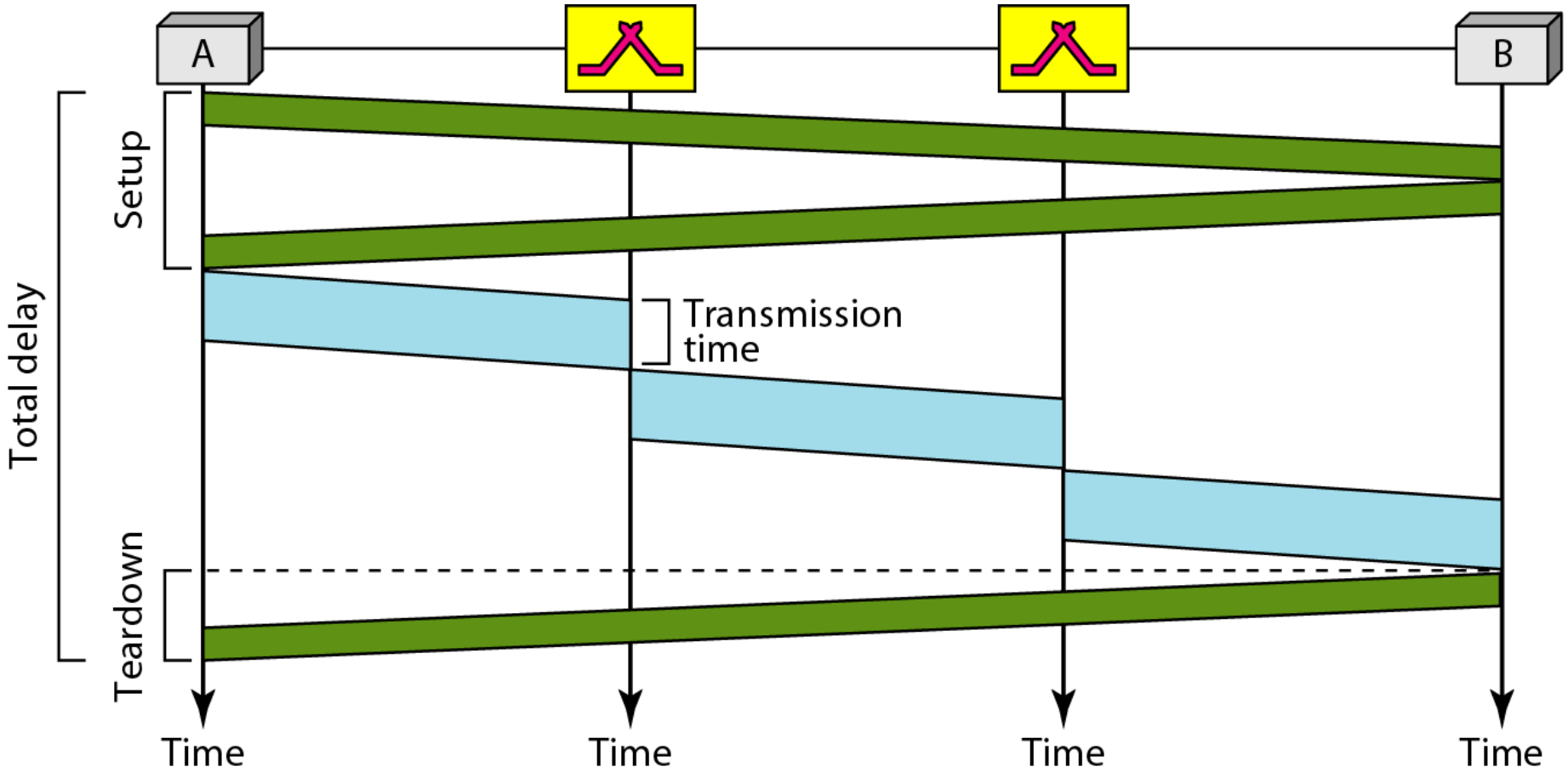
In the first case, the delay for each packet is the same;

in the second case, each packet may encounter different delays.

There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it.

Figure :*Delay in a virtual-circuit network*

Total delay = 3T+ 3't + setup delay + teardown delay



Note

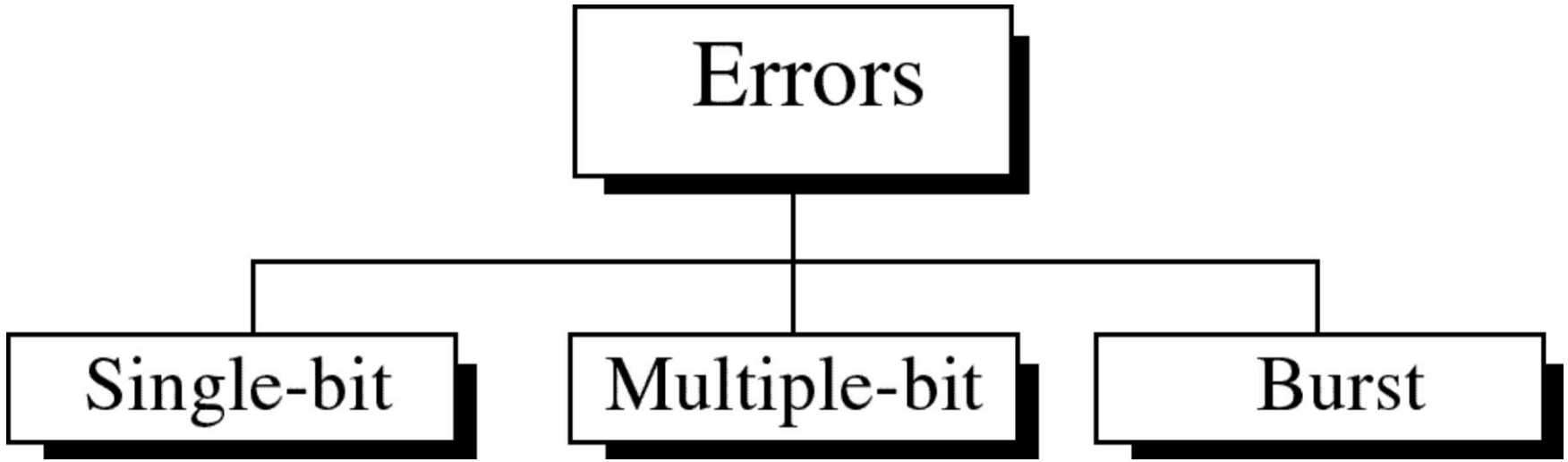
Switching at the data link layer in a switched WAN is normally implemented by using virtual-circuit techniques.

Error Detection and Correction

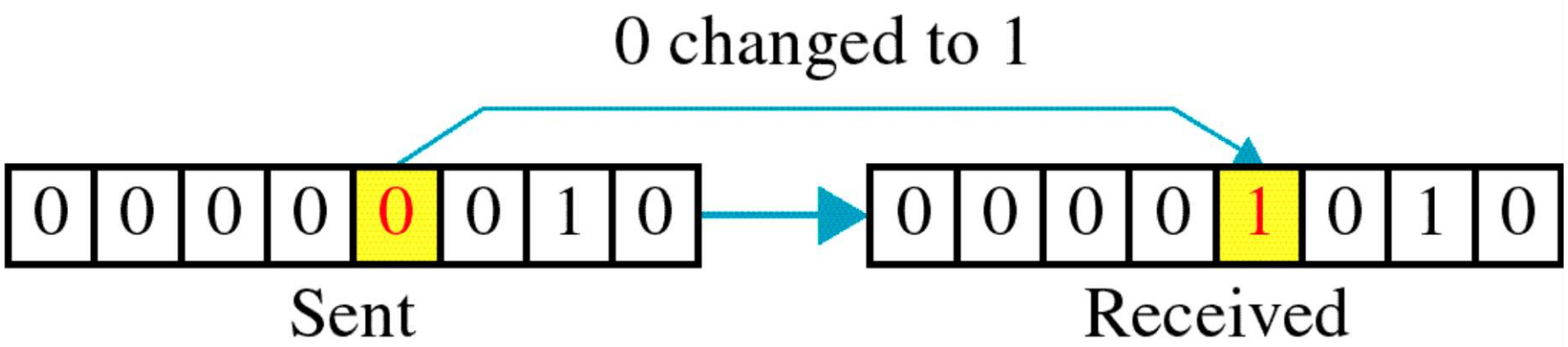
Why

- Networks must be able to transfer data from one device to another with complete accuracy.
- Data can be corrupted during transmission.
- For reliable communication, errors must be detected and corrected.
- Error detection and correction are implemented either at the data link layer or the transport layer of the OSI model.

Types of Errors



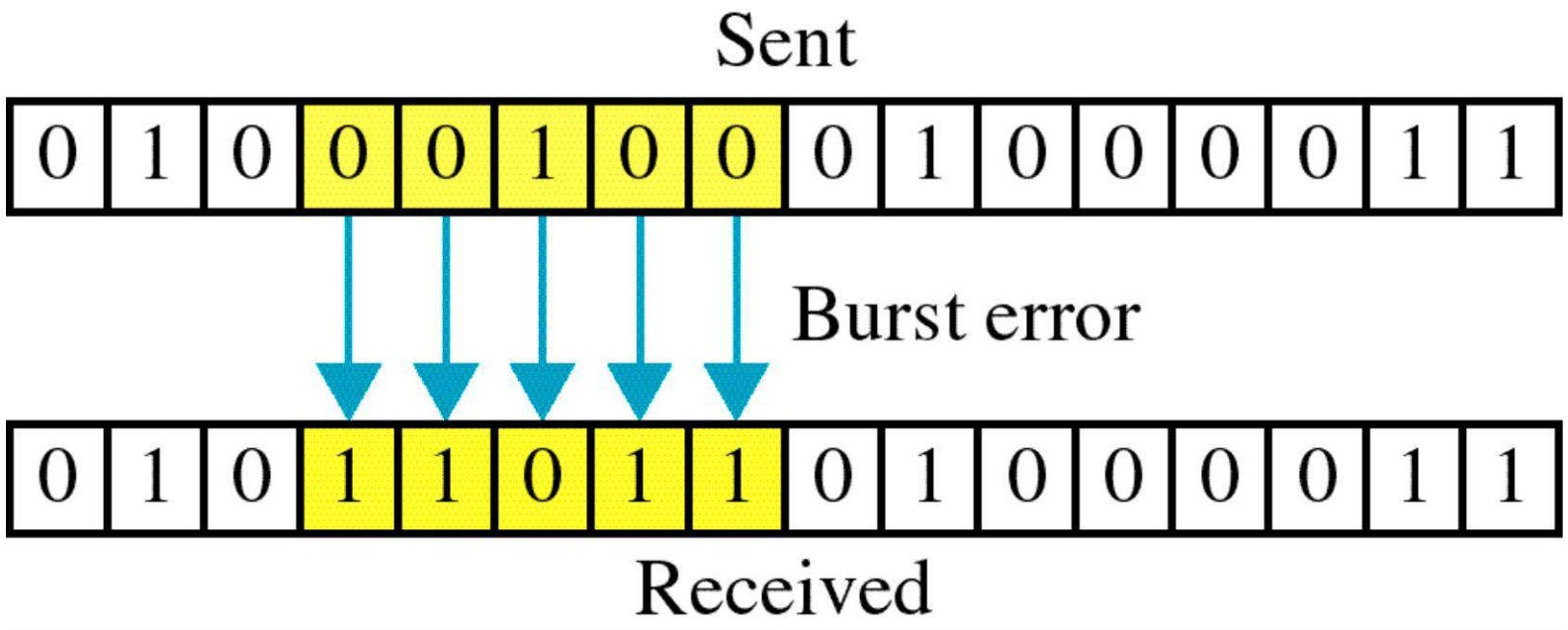
Single-bit error

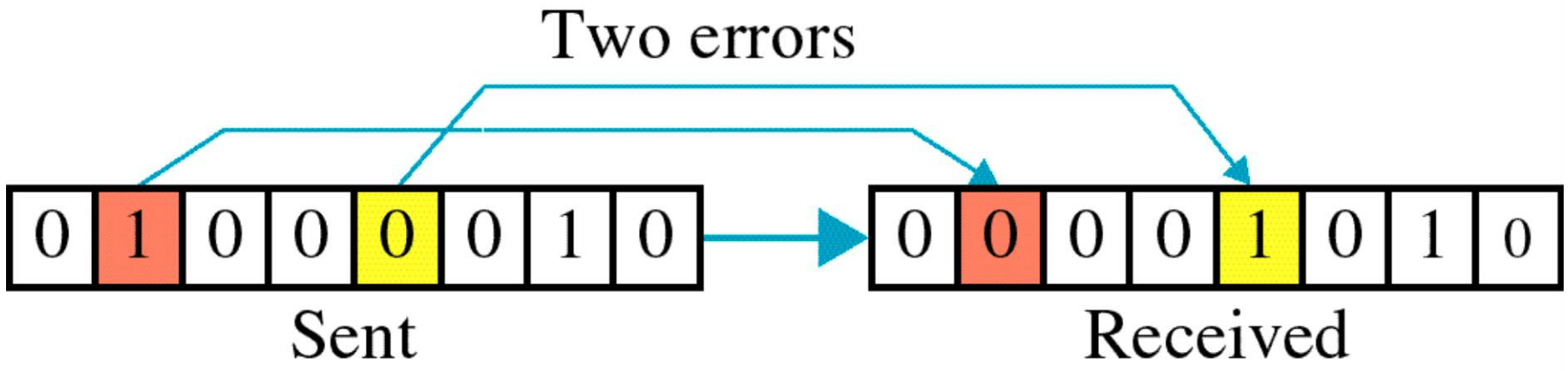


- **Single bit errors** are the **least likely** type of errors in serial data transmission because the noise must have a very short duration which is very rare.

- However this kind of errors can happen in parallel transmission.

Burst error


Sent
0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1
Burst error
0 1 0 1 1 0 1 1 0 1 0 0 0 0 1 1
Received


Two errors
0 1 0 0 0 0 1 0
0 0 0 0 1 0 1 0
Sent
Received

- The term burst error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

- Burst errors does not necessarily mean that the errors occur in consecutive bits, the length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.

- Burst error is most likely to happen in serial transmission since the duration of noise is normally longer than the duration of a bit.

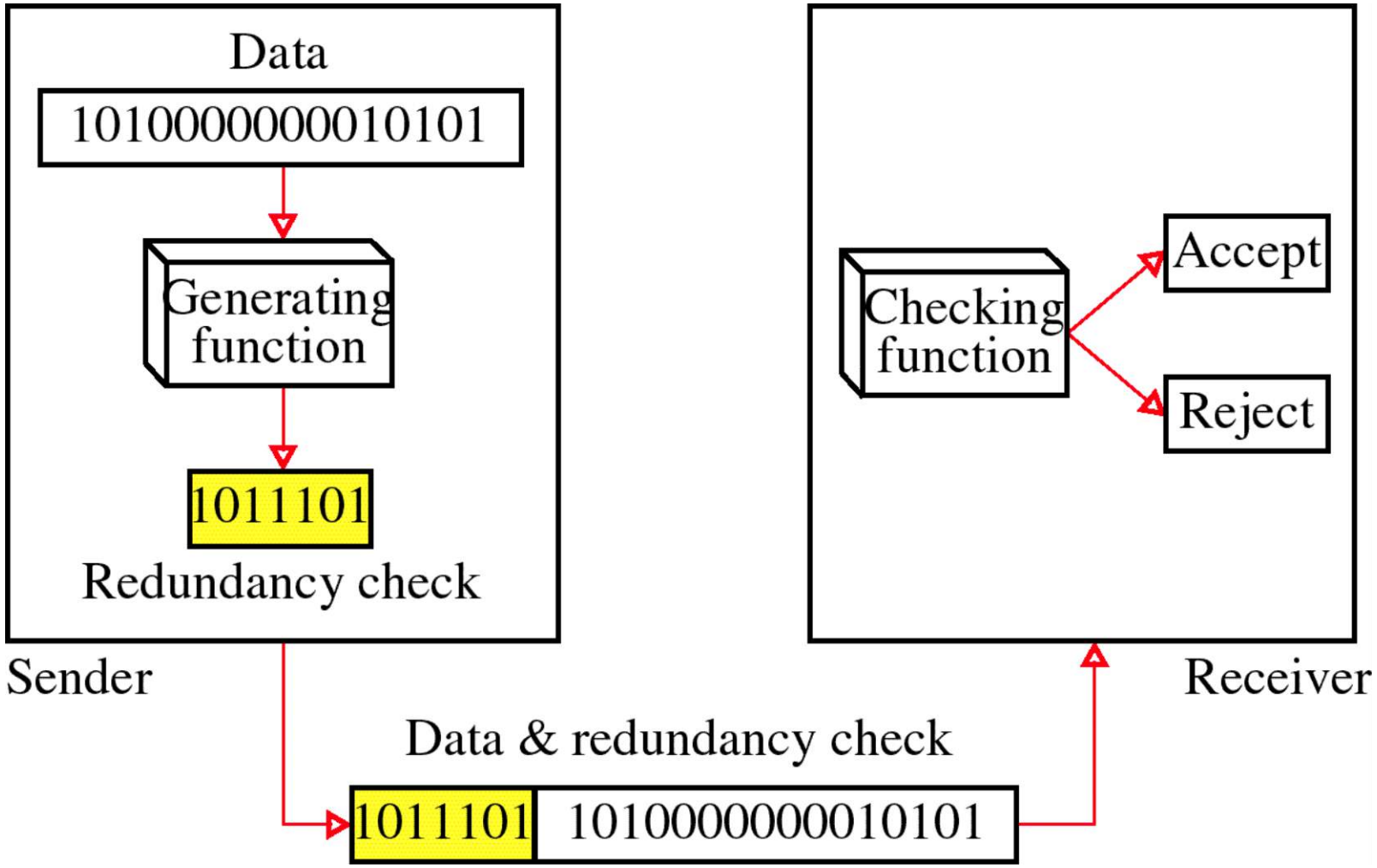
- The number of bits affected depends on the data rate and duration of noise.

Error detection

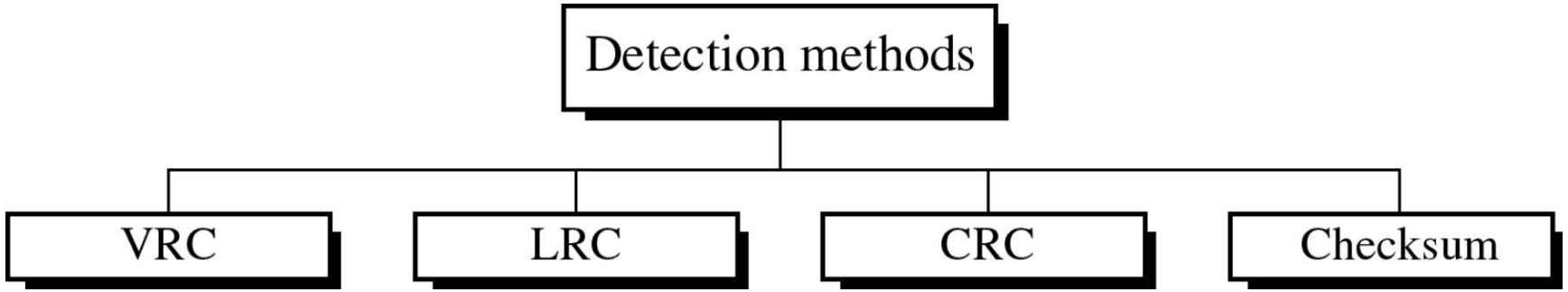
Error detection means to decide whether the received data is correct or not without having a copy of the original message.

Error detection **uses the concept of redundancy**, **which means** adding extra bits for detecting errors at the destination.

Redundancy


Data
1010000000010101
Generating function
1011101
Redundancy check
Sender
Checking function
Accept
Reject
Receiver
Data & redundancy check
1011101
1010000000010101

Four types of redundancy checks are used in data communications



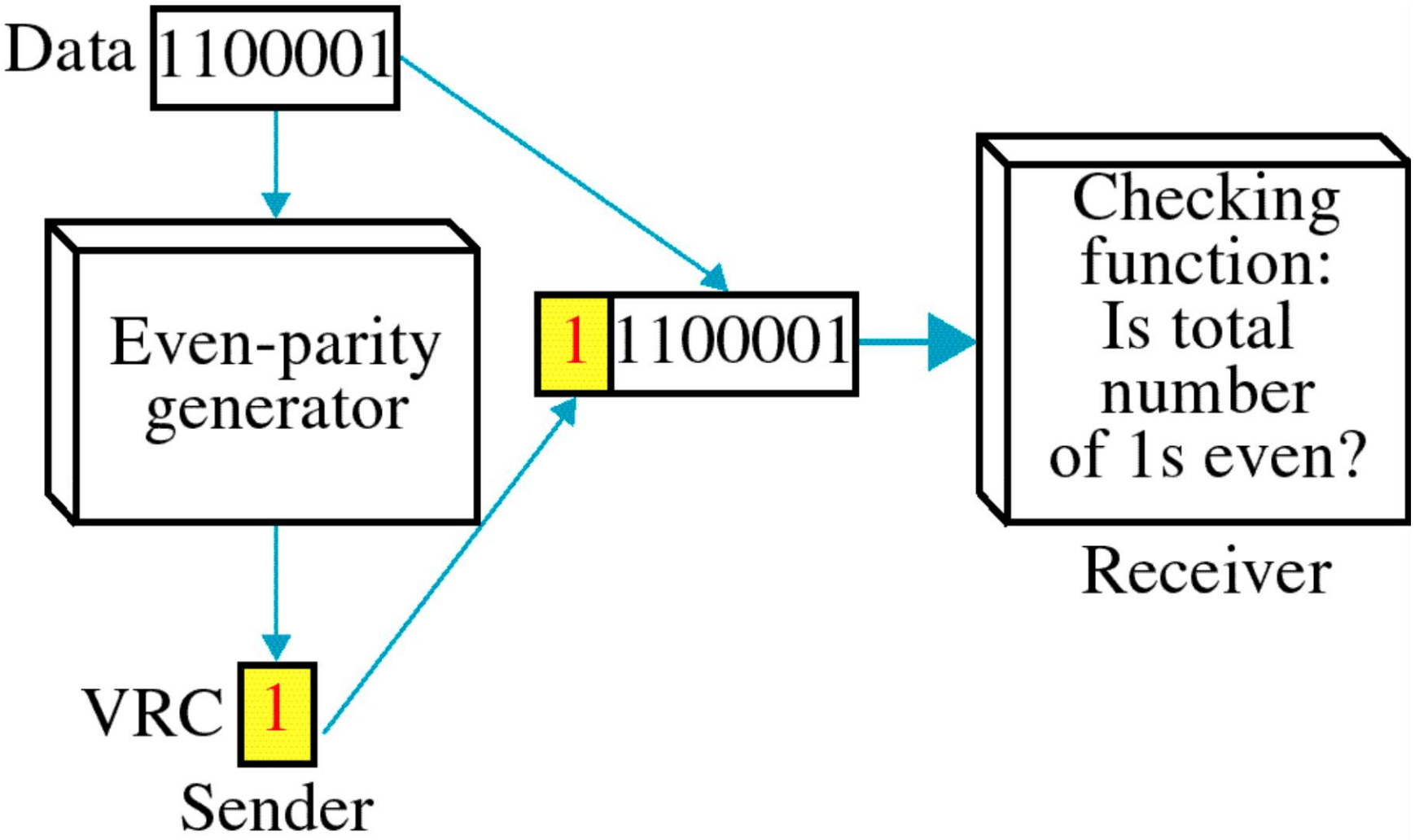
Vertical Redundancy Check (VRC)

Another name of vertical redundancy check is parity check.

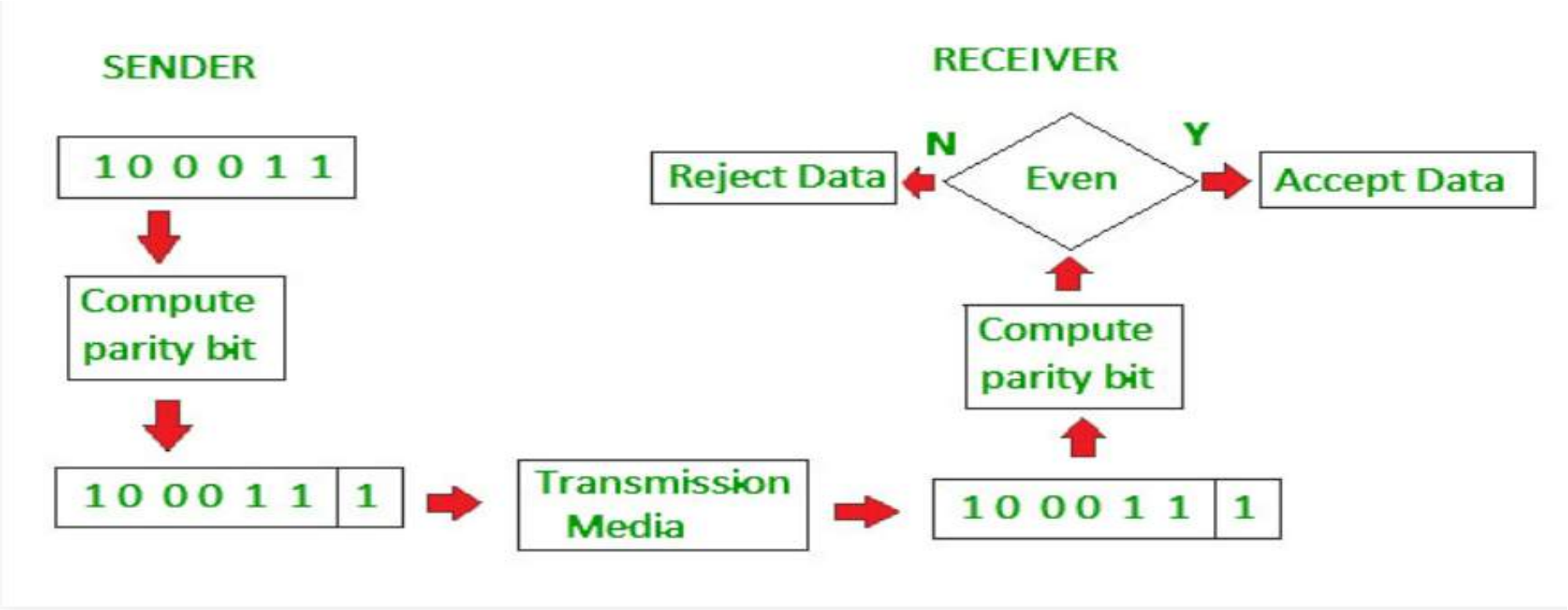
Least Expensive Mechanism.

So in this mechanism when an error detected by this mechanism a parity bit is append to the data unit so the total number of bits becomes **even** including parity bit.

Vertical Redundancy Check



Vertical Redundancy Check



Performance

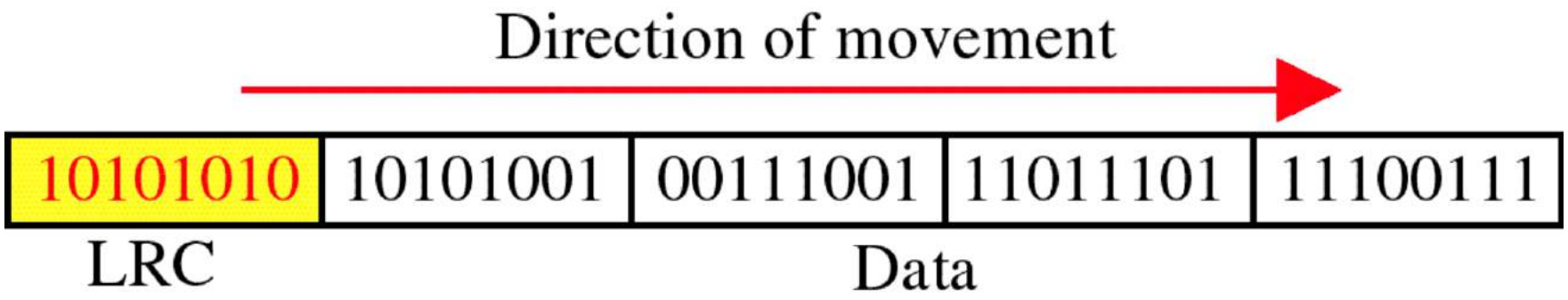
- It can detect single bit error.
- It can detect burst errors only if the total number of errors is odd.

Longitudinal Redundancy Check (LRC)

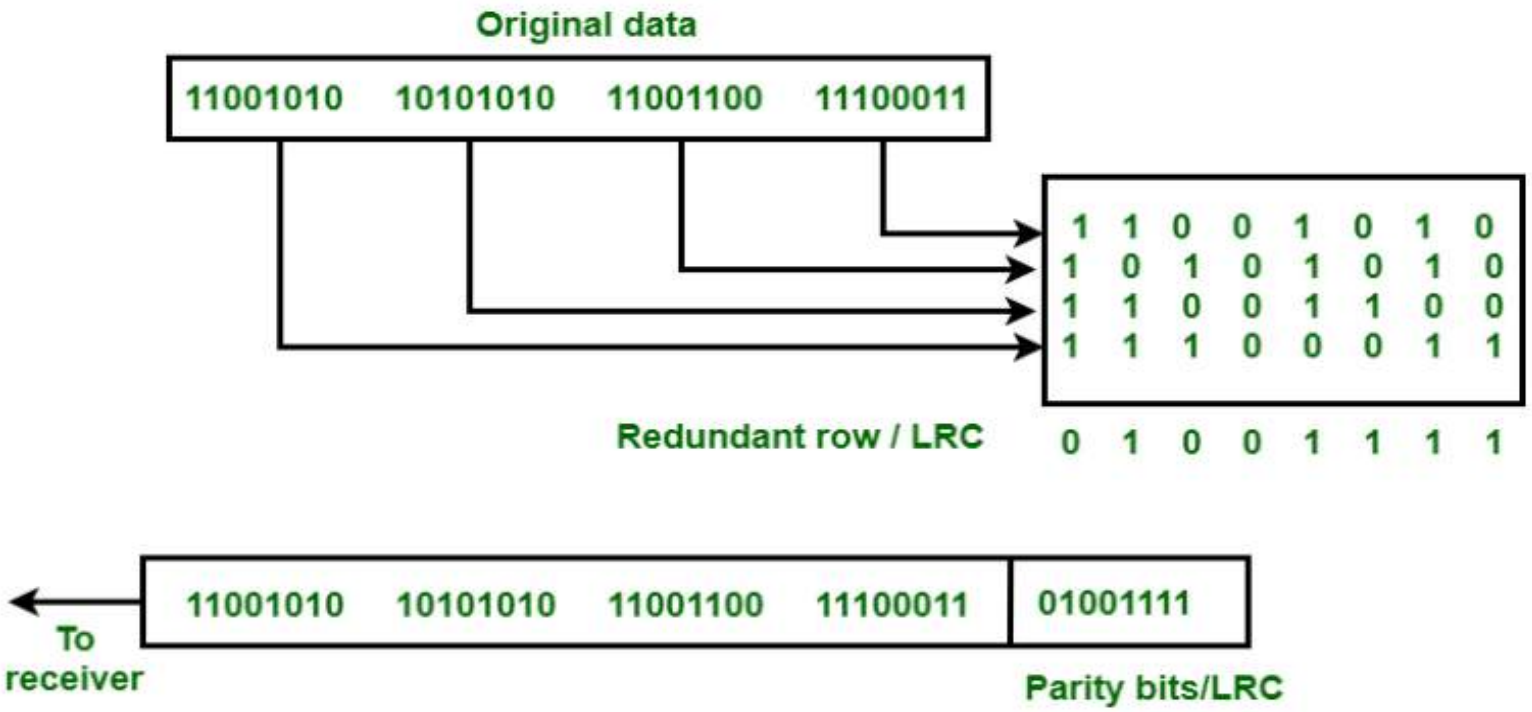
In this method Block of bits organized in tables e.g rows and columns.

calculate the parity bit for each column and the set of this parity bit is also sending with original data

Longitudinal Redundancy Check (LRC)



Longitudinal Redundancy Check (LRC)



Performance

- LRC increases the likelihood of detecting burst errors.
- If two bits in one data units are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error.

Example : If data 110011 010101 is changed to 010010110100.

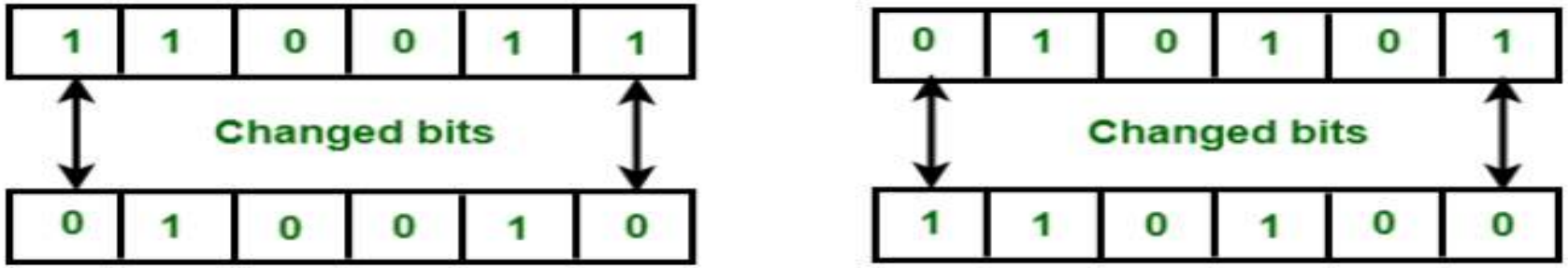


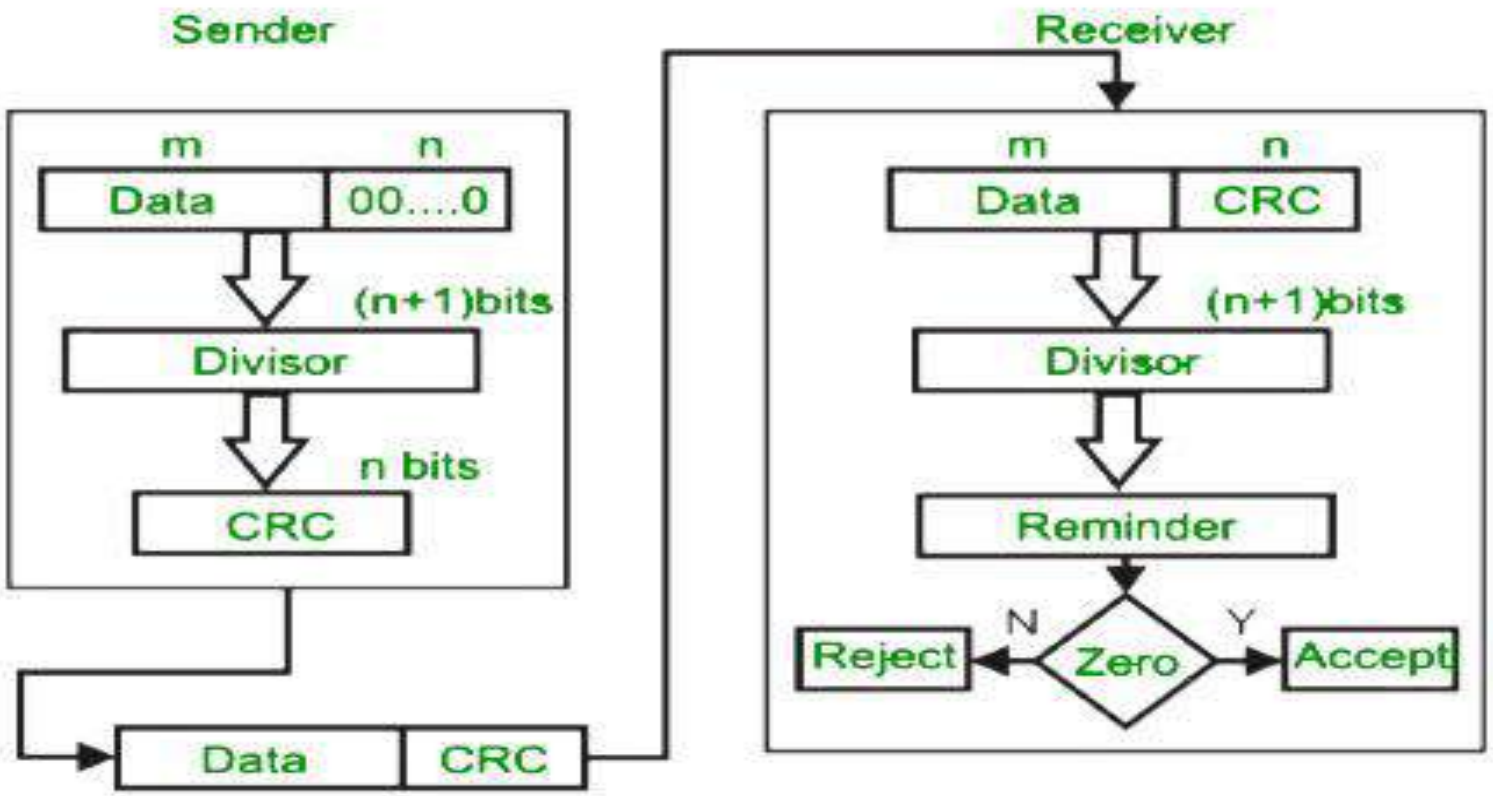
Figure : *Two bits at same bit position damaged in 2 data units*

In this example 1st and 6th bit in one data unit is changed . Also the 1st and 6th bit in second unit is changed.

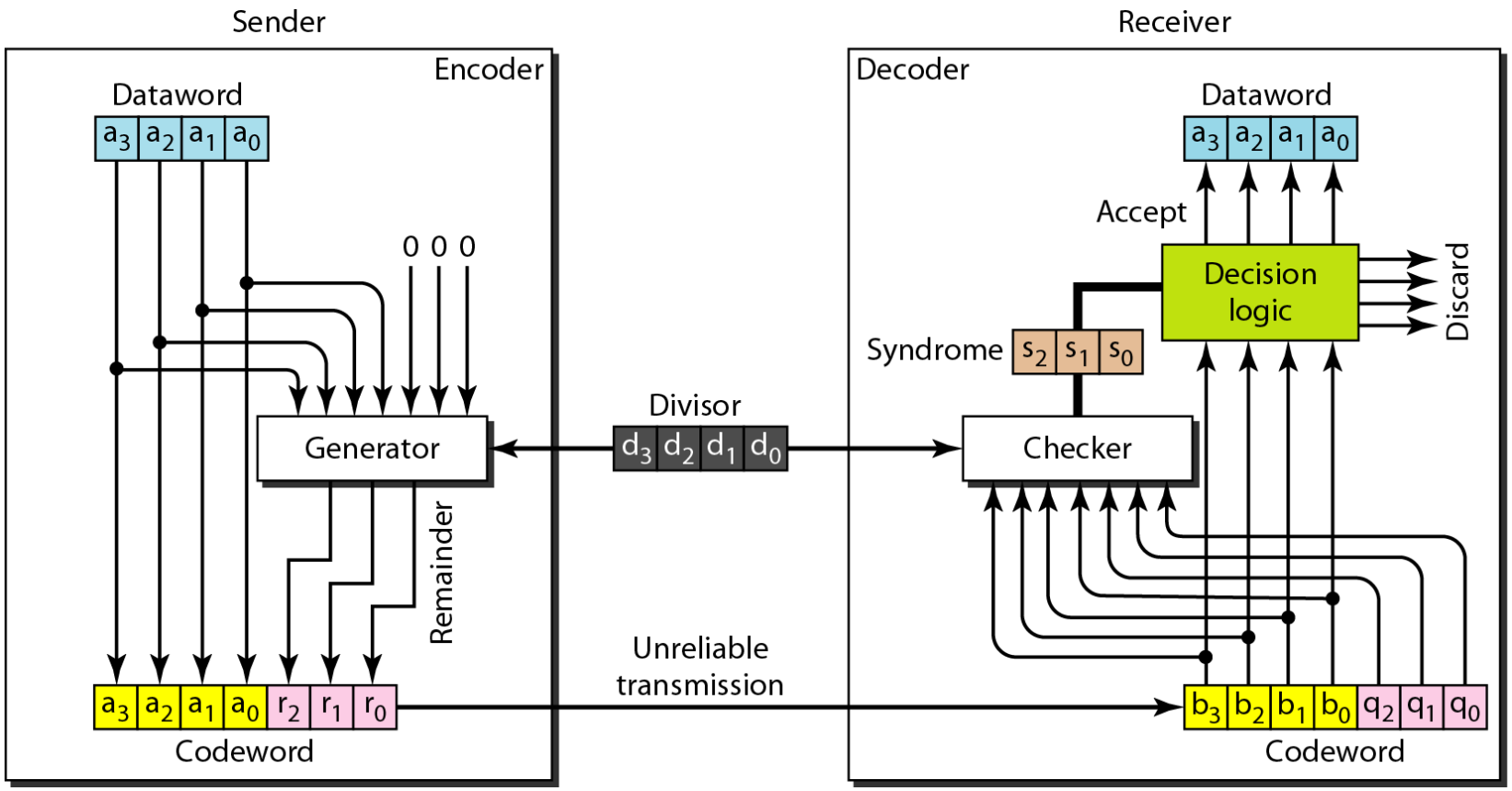
Cyclic redundancy check (CRC)

- CRC is based on binary division.
- CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

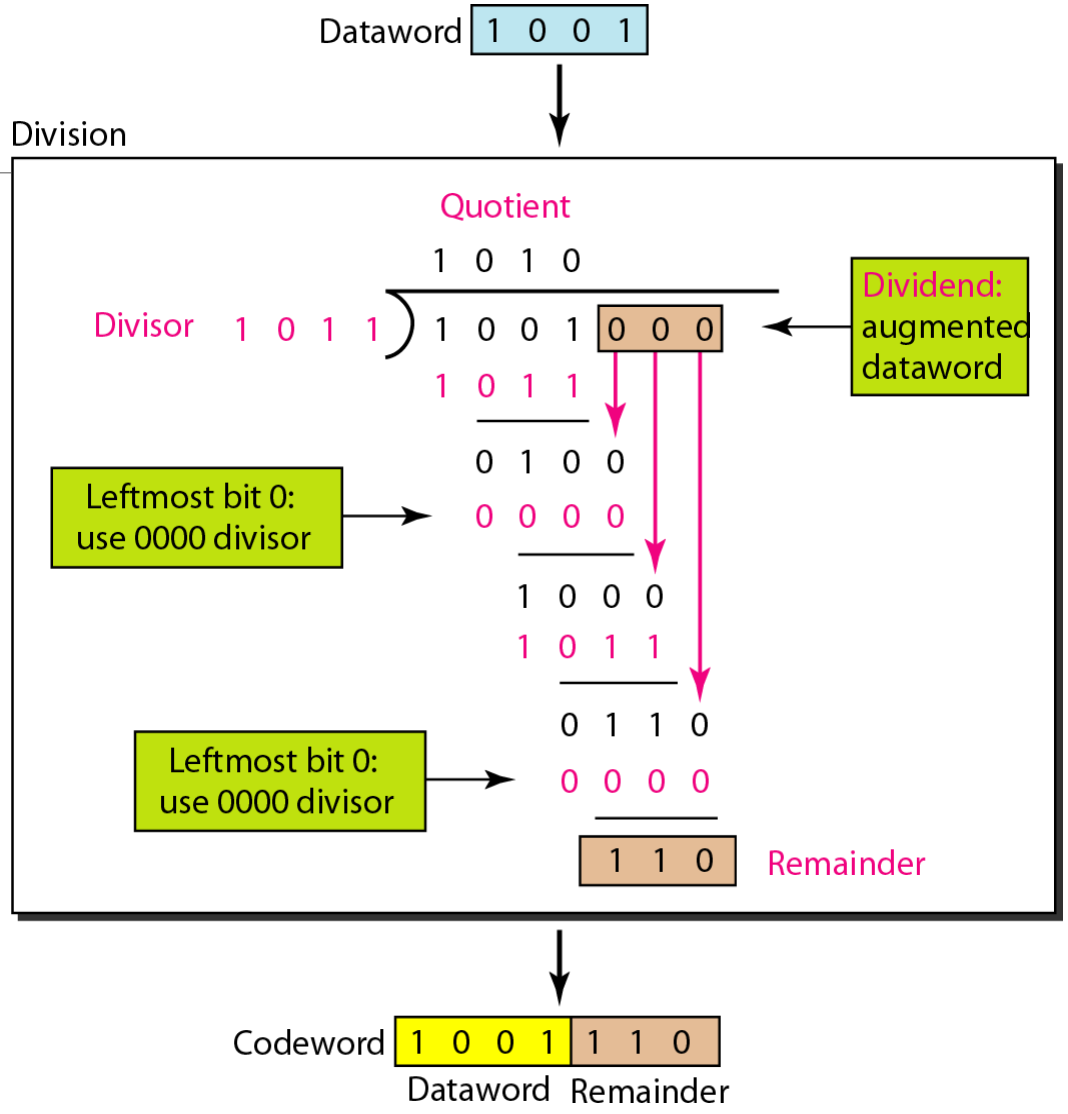
CRC


Sender
m
n
Data
00....0
(n+1)bits
Divisor
n bits
CRC
Data
CRC
Receiver
m
n
Data
CRC
(n+1)bits
Divisor
Reminder
N
Y
Reject
Zero
Accept

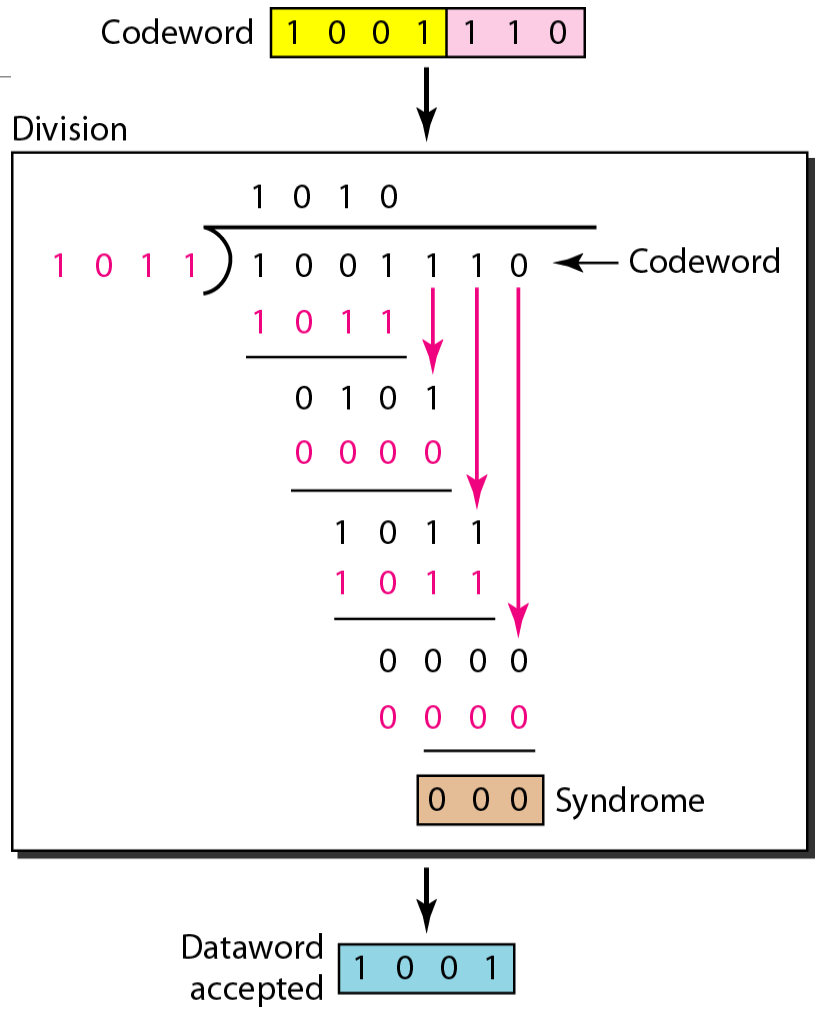
CRC encoder and decoder

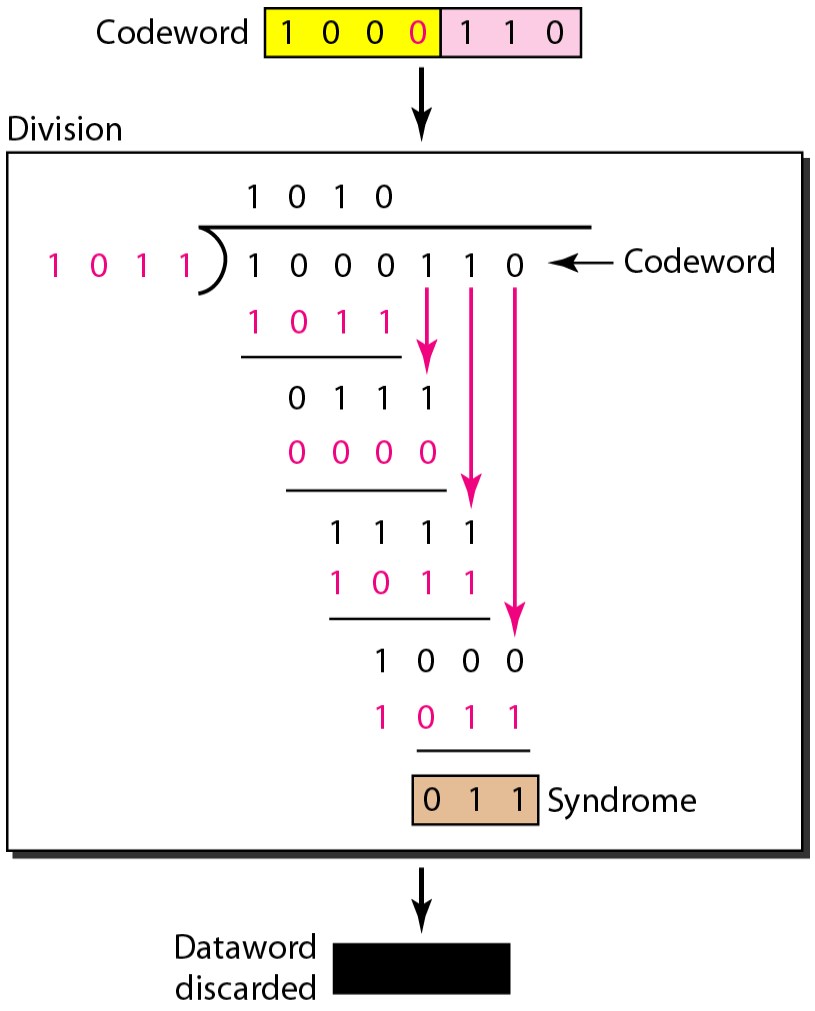


Division in CRC encoder



Division in the CRC decoder for two cases





Example

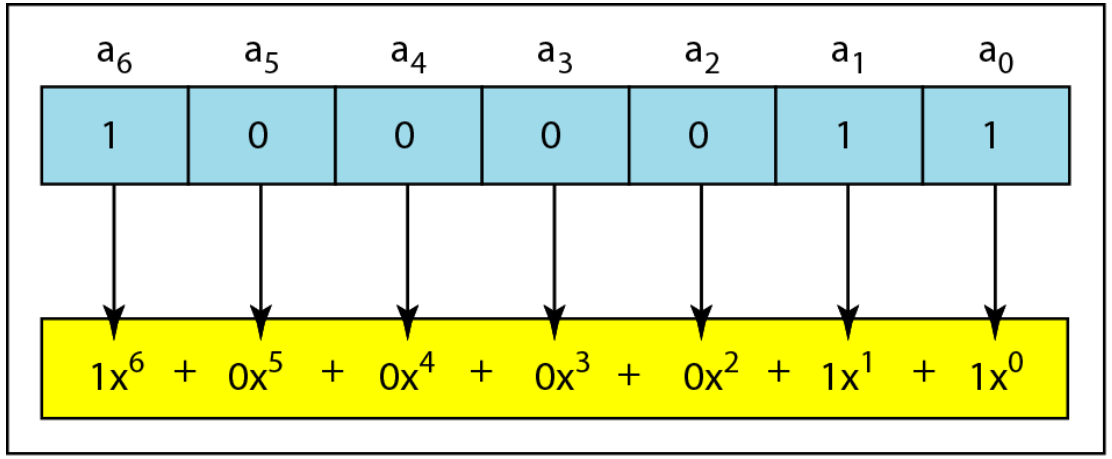
```
Frame:       1 1 0 1 0 1 1 1 1 1
Generator:   1 0 0 1 1

                     1 1 0 0 0 0 1 1 1 0   ← Quotient (thrown away)
1 0 0 1 1 / 1 1 0 1 0 1 1 1 1 1 0 0 0 0   ← Frame with four zeros appended
            1 0 0 1 1
              1 0 0 1 1
              1 0 0 1 1
                0 0 0 0 1
                0 0 0 0 0
                  0 0 0 1 1
                  0 0 0 0 0
                    0 0 1 1 1
                    0 0 0 0 0
                      0 1 1 1 1
                      0 0 0 0 0
                        1 1 1 1 0
                        1 0 0 1 1
                          1 1 0 1 0
                          1 0 0 1 1
                            1 0 0 1 0
                            1 0 0 1 1
                              0 0 0 1 0
                              0 0 0 0 0
                                    1 0   ← Remainder

Transmitted frame:  1 1 0 1 0 1 1 1 1 1 0 0 1 0   ← Frame with four zeros appended
                                                    minus remainder
```

Figure: *A polynomial to represent a binary word*

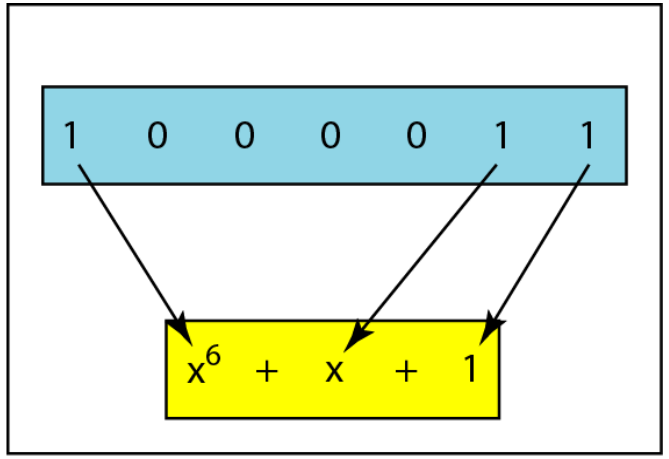
A pattern of 0s and 1s can be represented as a polynomial with coefficients of 0 and 1.

The power of each term shows the position of the bit;

the coefficient shows the value of the bit.

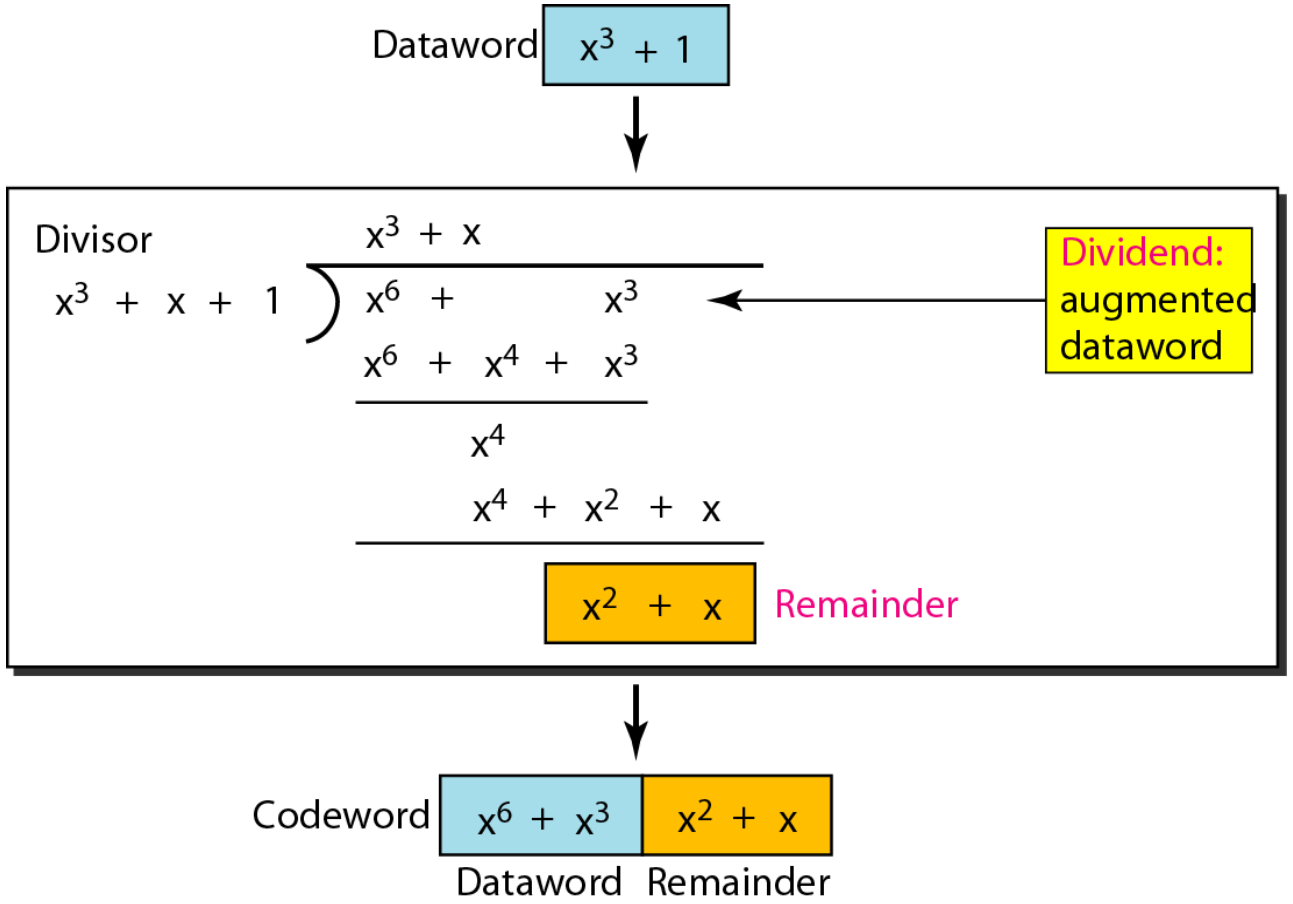


a. Binary pattern and polynomial



b. Short form

Figure *CRC division using polynomials*



Degree of a Polynomial

The degree of a polynomial is the highest power in the polynomial. For example, the degree of the polynomial x6 + x + 1 is 6.

Note that the degree of a polynomial is 1 less that the number of bits in the pattern.

Note

The divisor in a cyclic code is normally called the generator polynomial or simply the generator.

A bit stream 1101011011 is transmitted using the standard CRC method. The generator polynomial is x^4+x+1. What is the actual bit string transmitted?

Benefit of Polynomial

The benefit is even more when we have a polynomial such as x23 + X3 + 1. Here the bit pattern is 24 bits in length (three Is and twenty-one Os) while the polynomial is just three terms.

Checksum

The checksum is used in the Internet by several protocols although not at the data link layer.

Example

Suppose our data is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the data are not accepted.

Example

We can make the job of the receiver easier if we send the negative (complement) of the sum, called the checksum. In this case, we send (7, 11, 12, 0, 6, −36). The receiver can add all the numbers received (including the checksum). If the result is 0, it assumes no error; otherwise, there is an error.

Example

How can we represent the number 21 in one's complement arithmetic using only four bits?

Solution

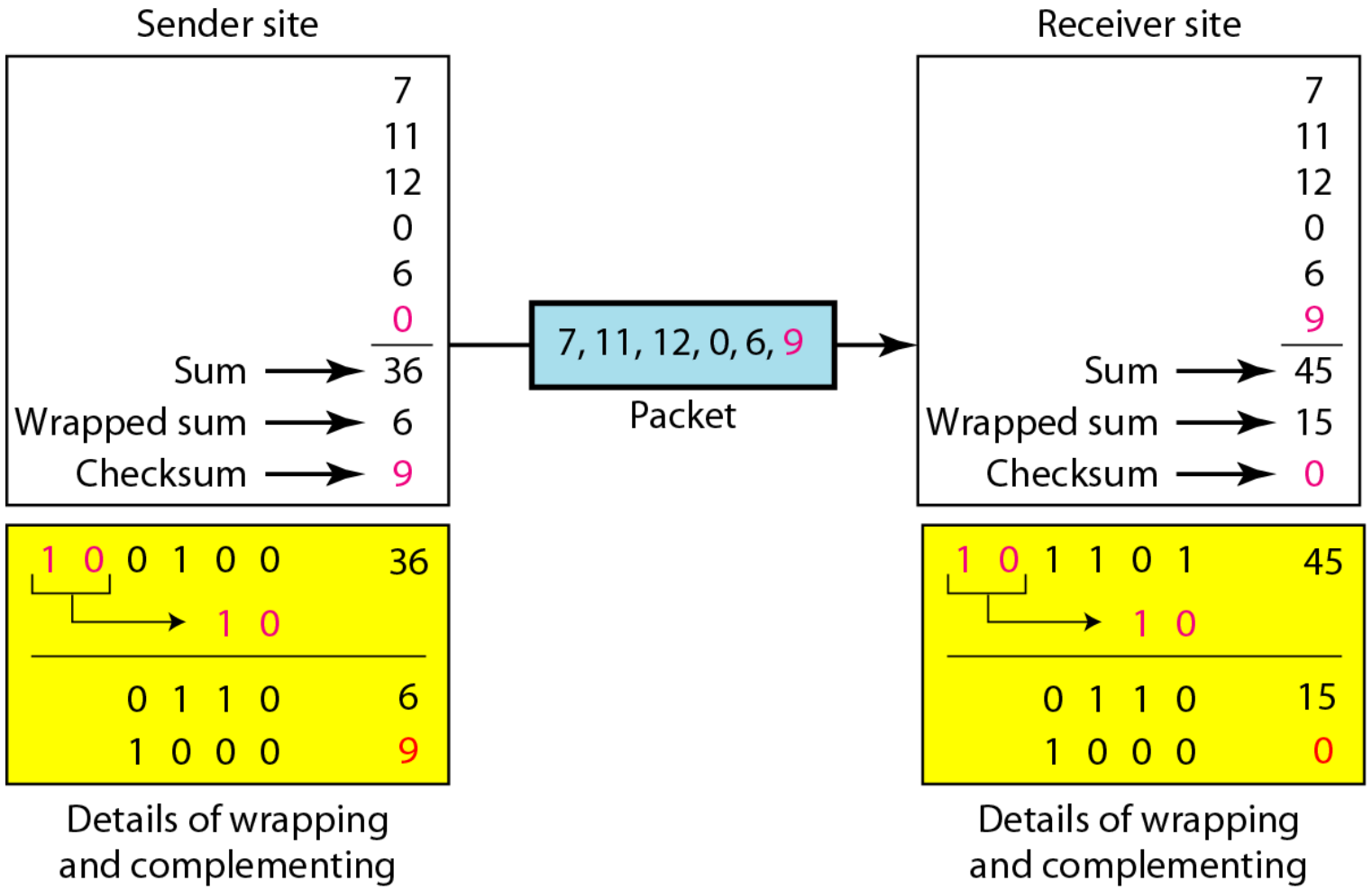
The number 21 in binary is 10101 (it needs five bits). We can wrap the leftmost bit and add it to the four rightmost bits. We have (0101 + 1) = 0110 or 6.

the process at the sender and at the receiver. The sender initializes the checksum to 0 and adds all data items and the checksum (the checksum is considered as one data item and is shown in color). The result is 36. However, 36 cannot be expressed in 4 bits. The extra two bits are wrapped and added with the sum to create the wrapped sum value 6. In the figure, we have shown the details in binary. The sender now sends six data items to the receiver including the checksum 9.

Example

The receiver follows the same procedure as the sender. It adds all data items (including the checksum); the result is 45. The sum is wrapped and becomes 15. The wrapped sum is complemented and becomes 0. Since the value of the checksum is 0, this means that the data is not corrupted. The receiver drops the checksum and keeps the other data items. If the checksum is not zero, the entire packet is dropped.

Figure Process



Note

Sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

Note

Receiver site:

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

Example

Let us calculate the checksum for a text of 8 characters ("Forouzan"). The text needs to be divided into 2-byte (16-bit) words. We use ASCII to change each byte to a 2-digit hexadecimal number. For example, F is represented as 0x46 and o is represented as 0x6F. Figure shows how the checksum is calculated at the sender and receiver sites. In part a of the figure, the value of partial sum for the first column is 0x36. We keep the rightmost digit (6) and insert the leftmost digit (3) as the carry in the second column. The process is repeated for each column. Note that if there is any corruption, the checksum recalculated by the receiver is not all 0s. We leave this an exercise.

Figure

1	0	1	3	Carries
4	6	6	F	(Fo)
7	2	6	7	(ro)
7	5	7	A	(uz)
6	1	6	E	(an)
0	0	0	0	Checksum (initial)
8	F	C	6	Sum (partial)
			1	
8	F	C	7	Sum
7	0	3	8	Checksum (to send)

a. Checksum at the sender site

1	0	1	3	Carries
4	6	6	F	(Fo)
7	2	6	7	(ro)
7	5	7	A	(uz)
6	1	6	E	(an)
7	0	3	8	Checksum (received)
F	F	F	E	Sum (partial)
			1	
8	F	C	7	Sum
0	0	0	0	Checksum (new)

a. Checksum at the receiver site

Performance

- The checksum detects all errors involving an odd number of bits.
- It detects most errors involving an even number of bits.
- If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem.

FLOW AND ERROR CONTROL

The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.

Note

Flow control refers to a set of procedures used to restrict the amount of data
that the sender can send before
waiting for acknowledgment.

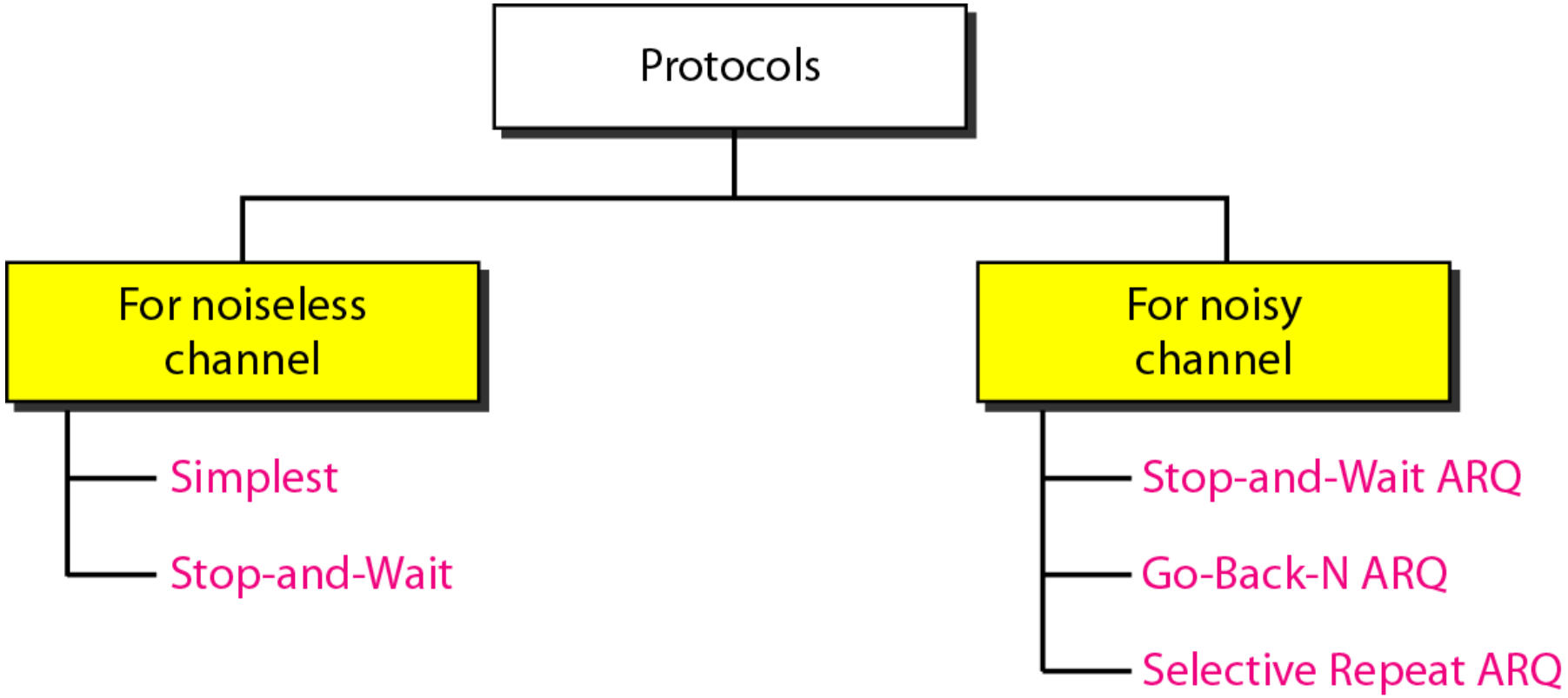
Note

Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

PROTOCOLS

Now let us see how the data link layer can combine framing, flow control, and error control to achieve the delivery of data from one node to another. The protocols are normally implemented in software by using one of the common programming languages.

Figure *Taxonomy of protocols*



NOISELESS CHANNELS

Let us first assume we have an ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel.

Figure *The design of the simplest protocol with no flow or error control*

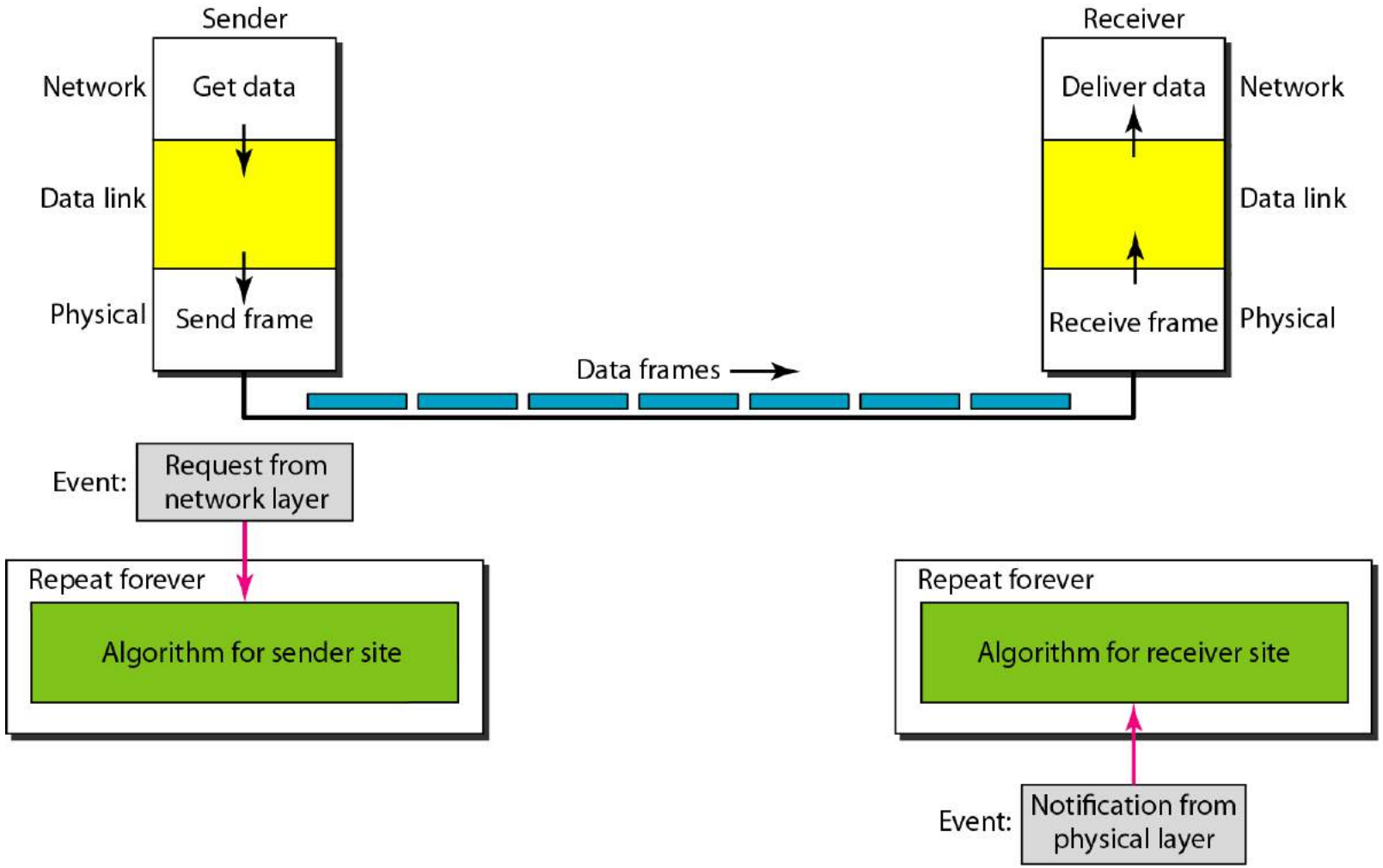


Figure 11.7 shows an example of communication using this protocol. It is very simple. The sender sends a sequence of frames without even thinking about the receiver. To send three frames, three events occur at the sender site and three events at the receiver site. Note that the data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.

Figure *Flow diagram for Example*

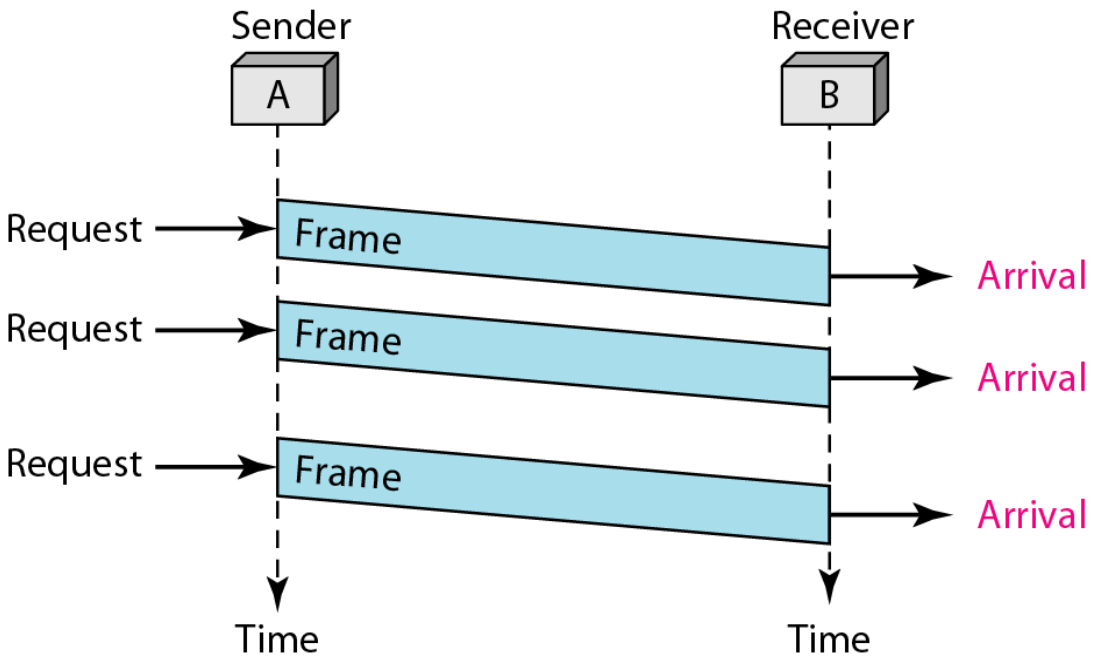


Figure *Design of Stop-and-Wait Protocol*

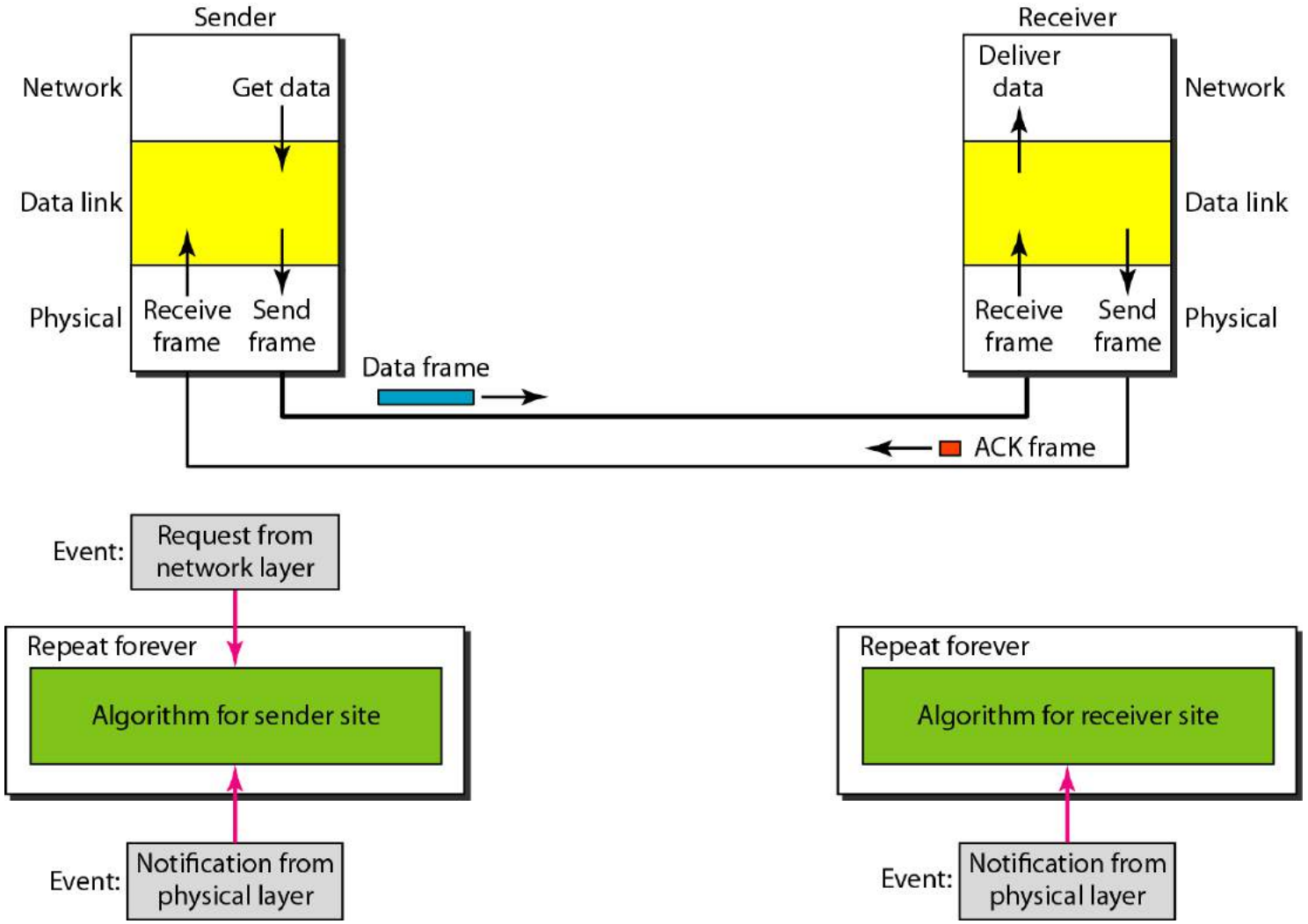
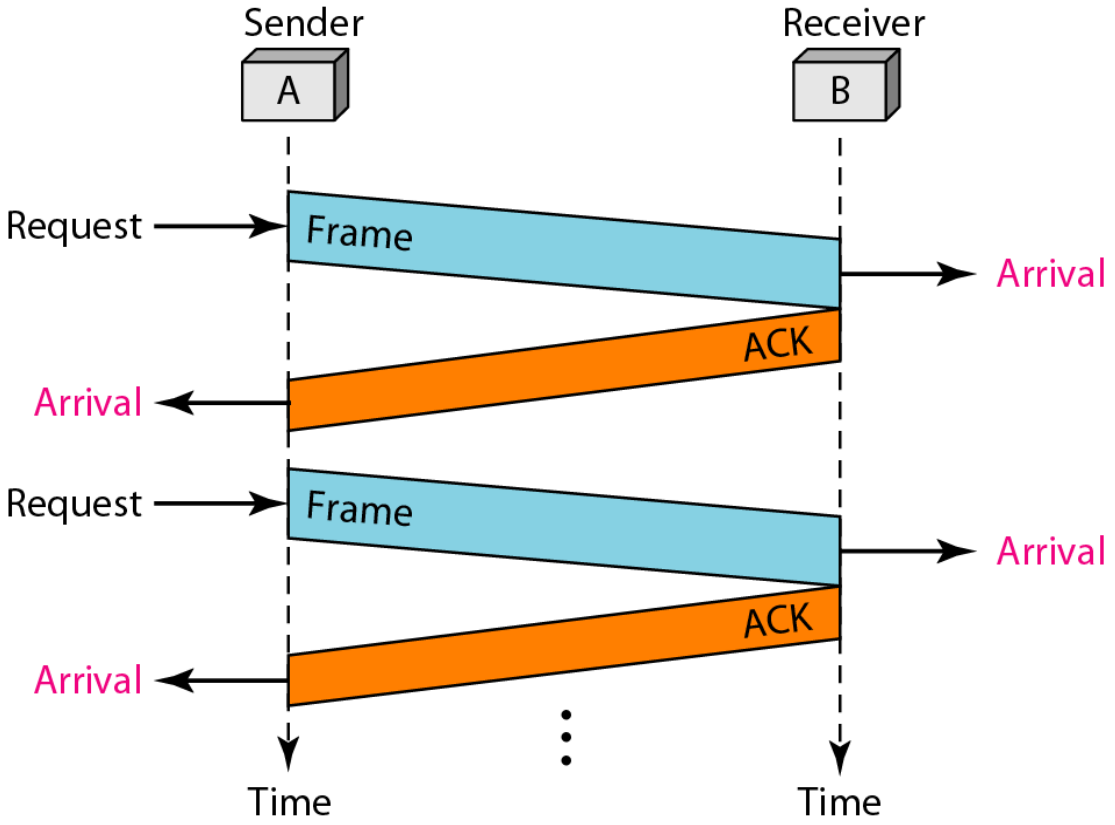
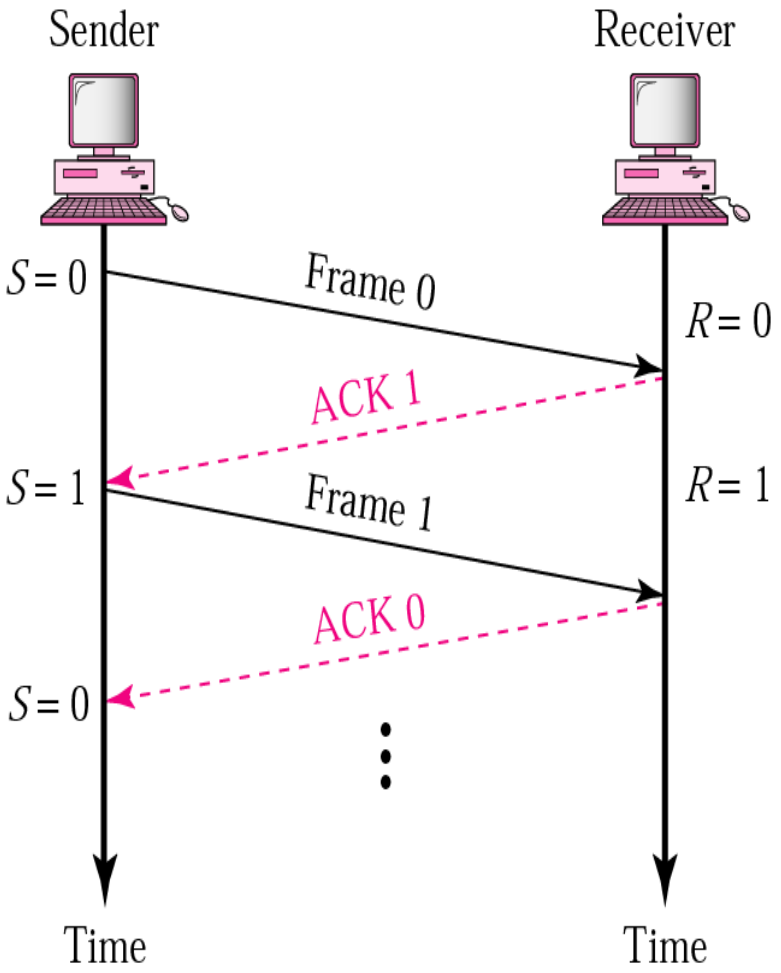


Figure shows an example of communication using this protocol. It is still very simple. The sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.

Figure *Flow diagram for Example*

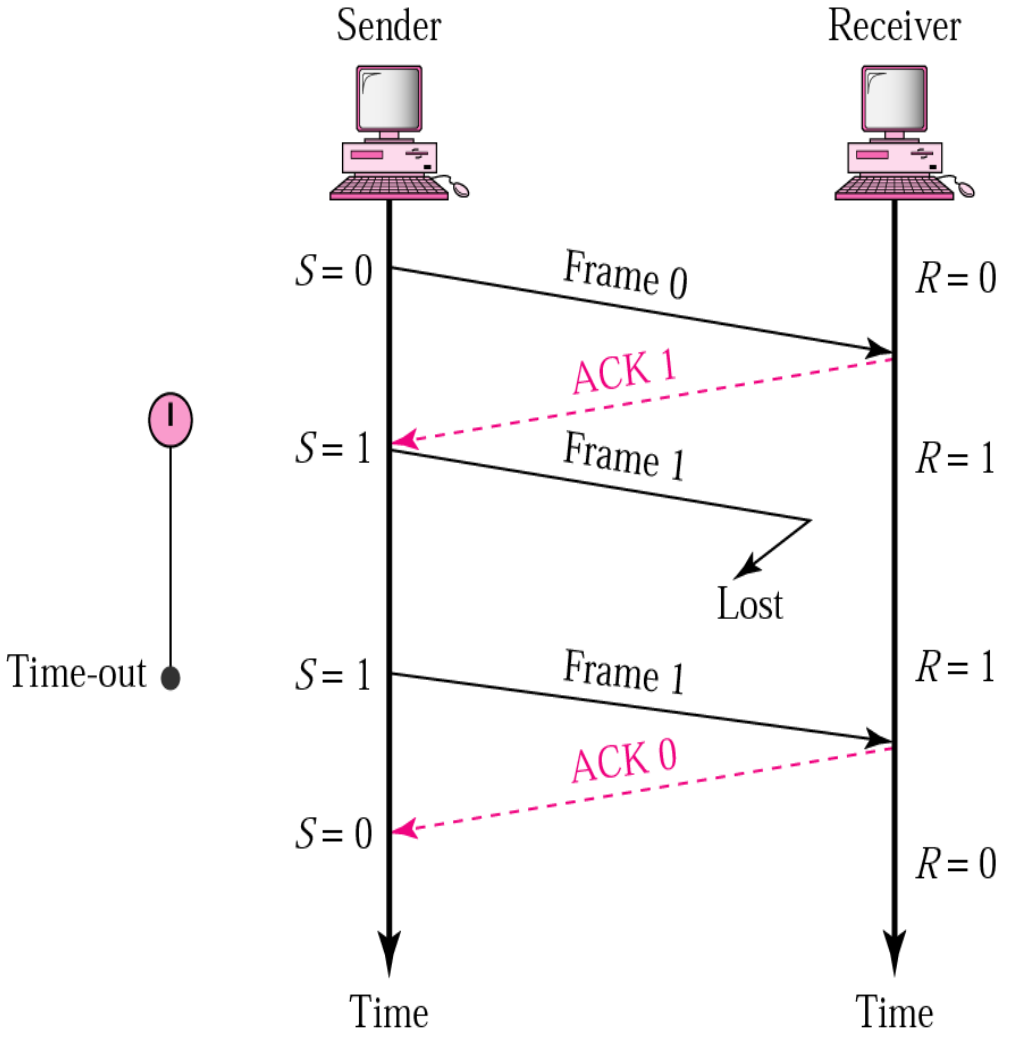


Stop-and-Wait



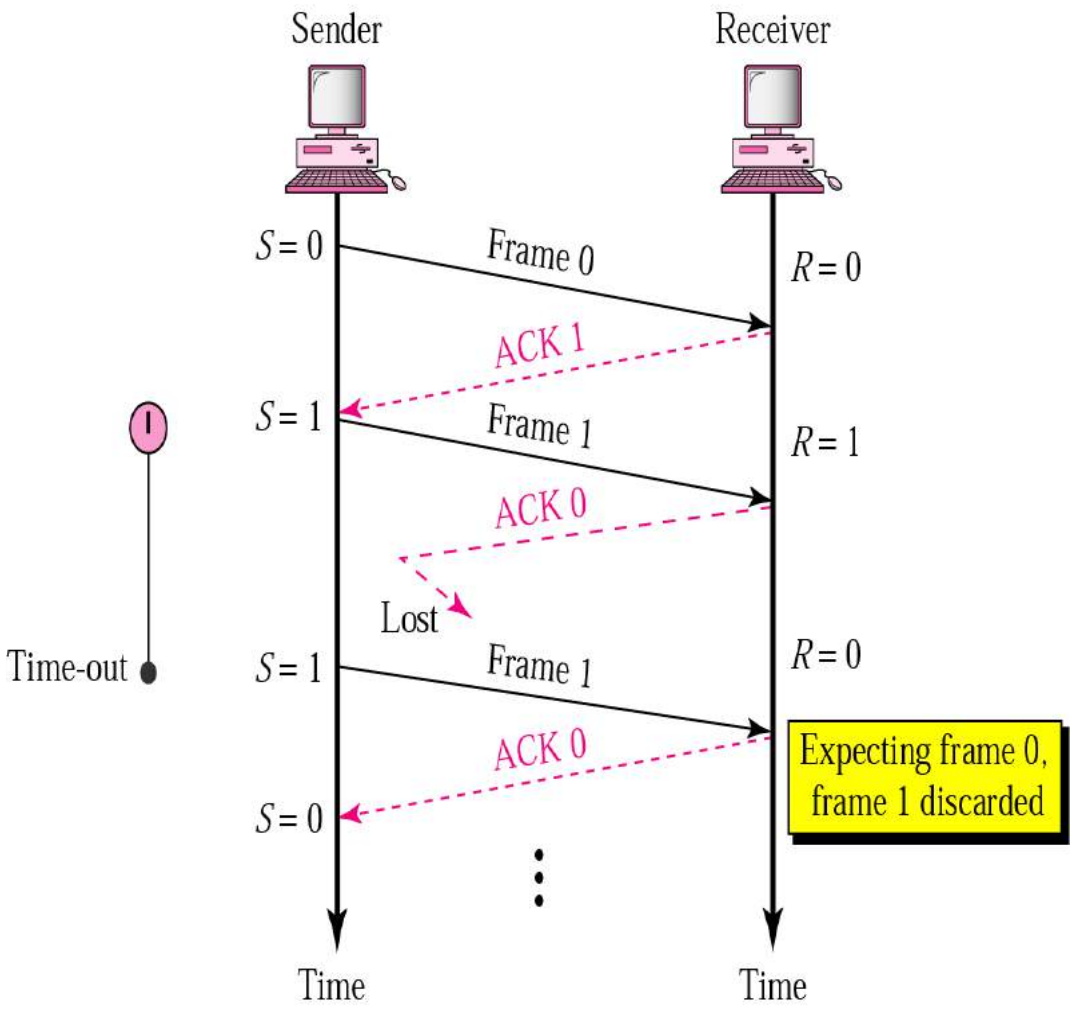
- Sender keeps a copy of the last frame until it receives an acknowledgement.
- For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.
- Sender has a control variable (S) that holds the number of the recently sent frame. (0 or 1)
- Receiver has a control variable ® that holds the number of the next frame expected (0 or 1).
- Sender starts a timer when it sends a frame. If an ACK is not received within a allocated time period, the sender assumes that the frame was lost or damaged and resends it
- Receiver send only positive ACK if the frame is intact.
- ACK number always defines the number of the next expected frame

Stop-and-Wait ARQ, lost frame



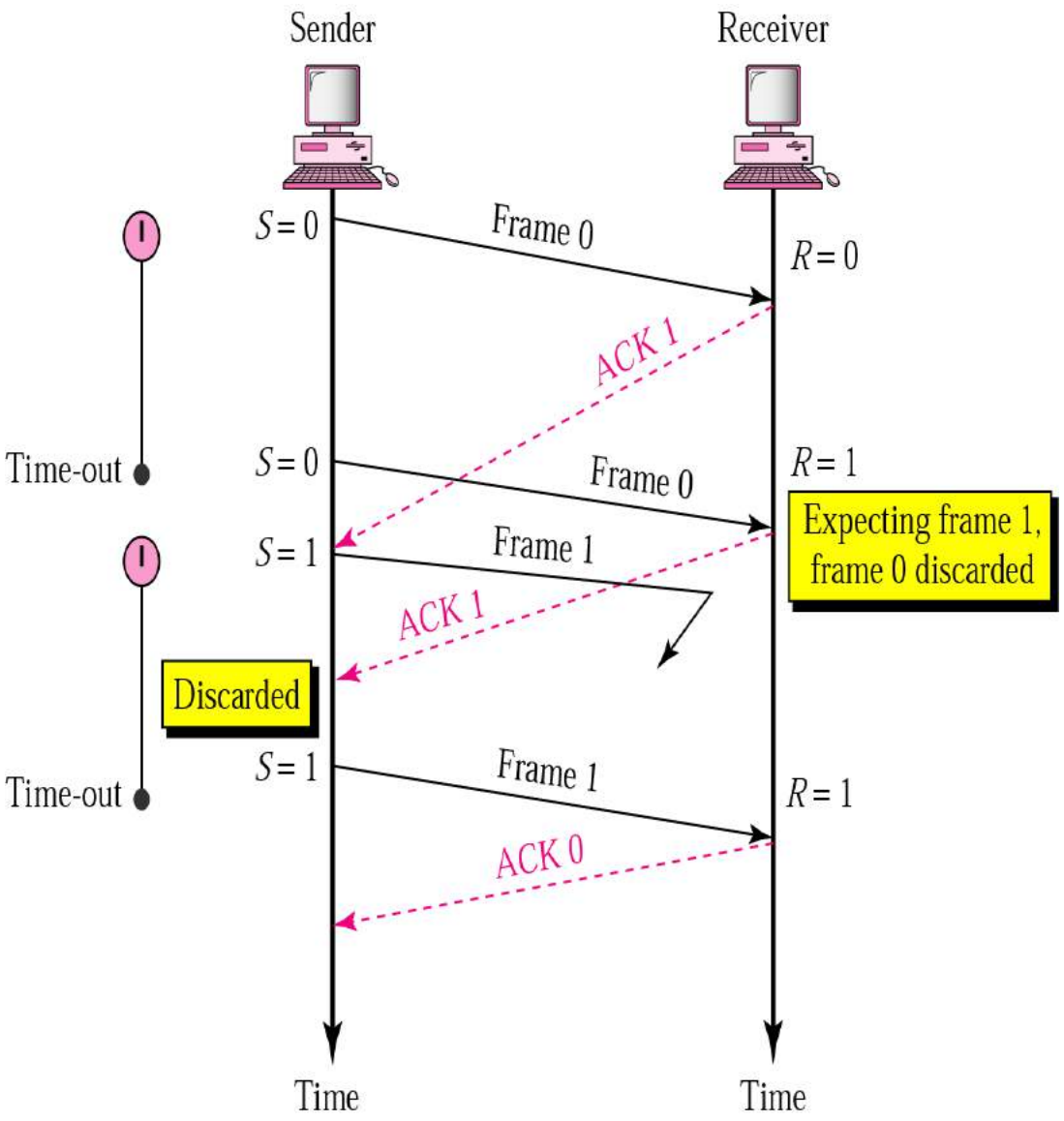
- When a receiver receives a damaged frame, it discards it and keeps its value of R.
- After the timer at the sender expires, another copy of frame 1 is sent.

Stop-and-Wait, lost ACK frame



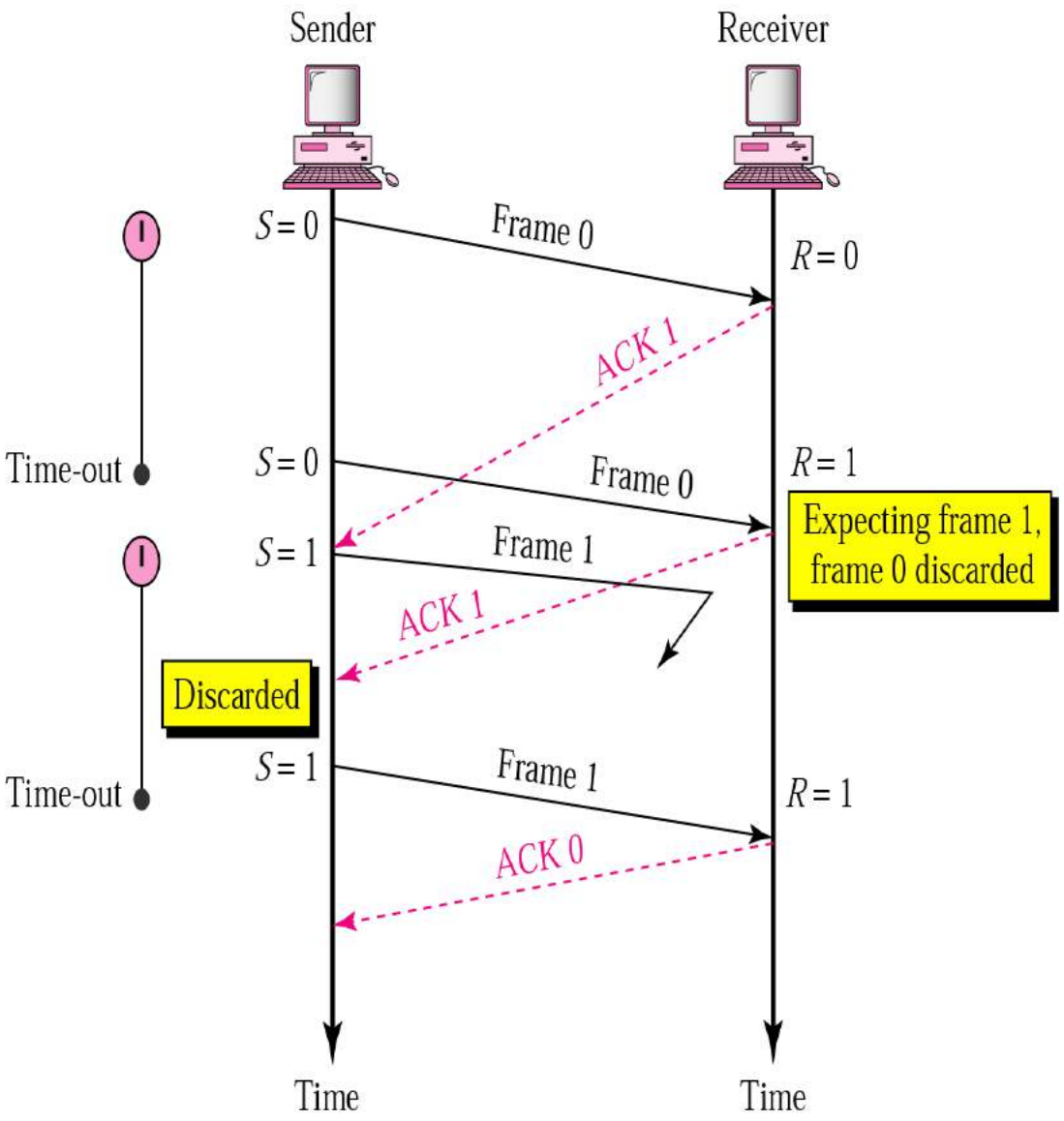
- If the sender receives a damaged ACK, it discards it.
- When the timer of the sender expires, the sender retransmits frame 1.
- Receiver has already received frame 1 and expecting to receive frame 0 (R=0). Therefore it discards the second copy of frame 1.

Stop-and-Wait, delayed ACK frame



- The ACK can be delayed at the receiver or due to some problem
- It is received after the timer for frame 0 has expired.
- Sender retransmitted a copy of frame 0. However, R =1 means receiver expects to see frame 1. Receiver discards the duplicate frame 0.
- Sender receives 2 ACKs, it discards the second ACK.

Stop-and-wait, delayed ACK frame



- The ACK can be delayed at the receiver or due to some problem
- It is received after the timer for frame 0 has expired.
- Sender retransmitted a copy of frame 0. However, R =1 means receiver expects to see frame 1. Receiver discards the duplicate frame 0.
- Sender receives 2 ACKs, it discards the second ACK.

Disadvantage of Stop-and-Wait

- In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged.
- This is not a good use of transmission medium.
- To improve efficiency, multiple frames should be in transition while waiting for ACK.
- Two protocol use the above concept,
  - **Go-Back-N ARQ**
  - **Selective Repeat ARQ**

Problems

1. If the bandwidth of the line is 1.5 Mbps, RTT is 45 msec and packet size is 1 KB, then find the link utilization in stop and wait.

2. A channel has a bit rate of 4 Kbps and one way propagation delay of 20 msec. The channel uses stop and wait protocol. The transmission time of the acknowledgement frame is negligible. To get a channel efficiency of at least 50%, the minimum frame size should be:

3. Consider a MAN with average source and destination 20 Km apart and one way delay of 100 µsec. At what data rate does the round trip delay equals the transmission delay for a 1 KB packet?

4. If the packet size is 1 KB and propagation time is 15 msec, the channel capacity is 10^9 b/sec, then find the transmission time and utilization of sender in stop and wait protocol.

Go-Back-N ARQ

We can send up to W frames before worrying about ACKs.

We keep a copy of these frames until the ACKs arrive.

This procedure requires additional features to be added to Stop-and-Wait ARQ.

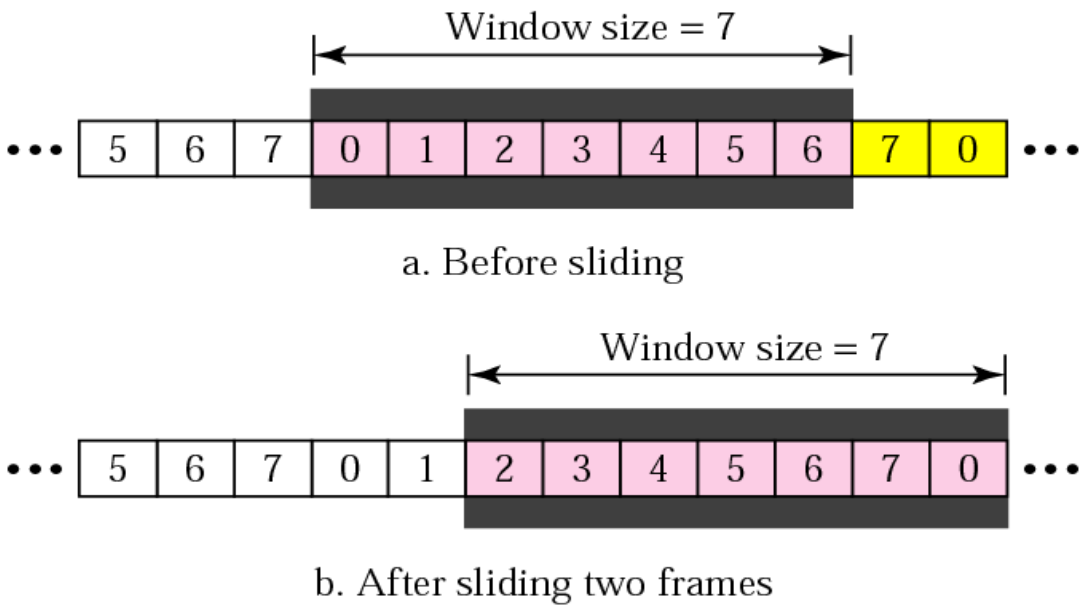
Sequence Numbers

- Frames from a sender are numbered sequentially.
- We need to set a limit since we need to include the sequence number of each frame in the header.
- If the header of the frame allows m bits for sequence number, the sequence numbers range from 0 to $2^m - 1$. for m = 3, sequence numbers are: 1, 2, 3, 4, 5, 6, 7.
- We can repeat the sequence number.
- Sequence numbers are:

0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, …

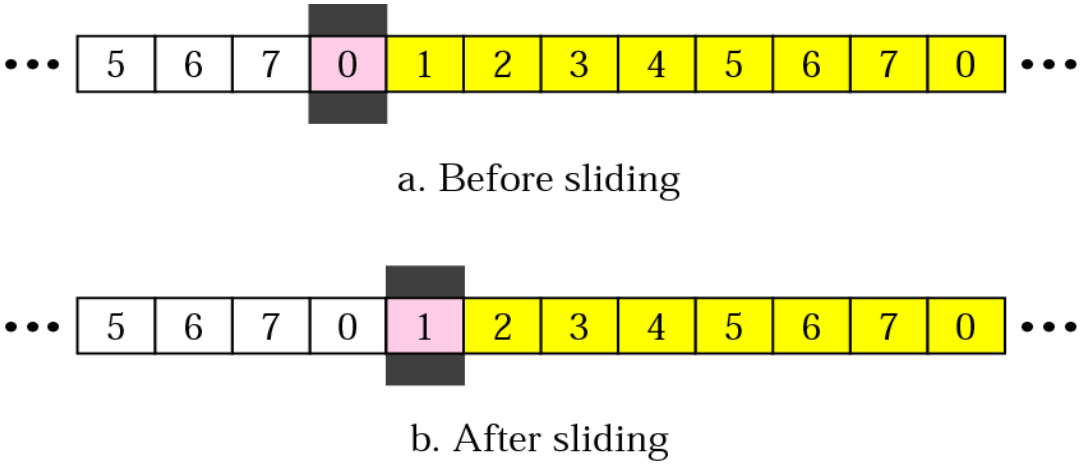
Sender Sliding Window

- At the sending site, to hold the outstanding frames until they are acknowledged, we use the concept of a window.
- The size of the window is at most 2^m -1 where m is the number of bits for the sequence number.
- Size of the window can be variable, e.g. TCP.
- The window slides to include new unsent frames when the correct ACKs are received



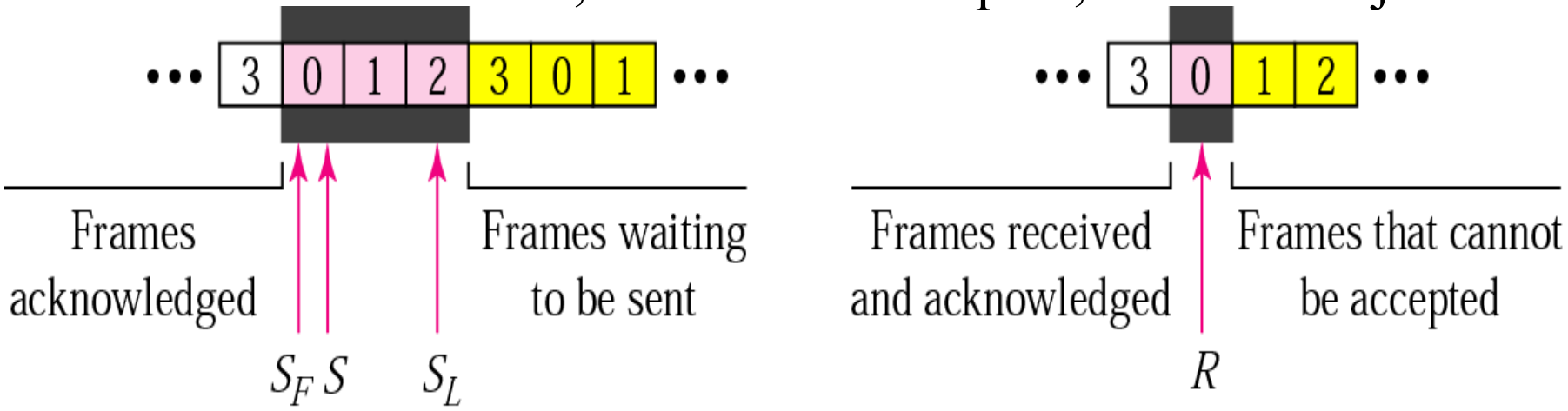
Receiver Sliding Window

- Size of the window at the receiving site is always 1 in this protocol.
- Receiver is always looking for a specific frame to arrive in a specific order.
- Any frame arriving out of order is discarded and needs to be resent.
- Receiver window slides as shown in fig. Receiver is waiting for frame 0 in part a.



Control Variables

- Sender has 3 variables: S, S_F, and S_L
- S holds the sequence number of recently sent frame
- S_F holds the sequence number of the first frame
- S_L holds the sequence number of the last frame
- Receiver only has the one variable, R, that holds the sequence number of the frame it expects to receive. If the seq. no. is the same as the value of R, the frame is accepted, otherwise rejected.



a. Sender window

b. Receiver window

Acknowledgement

Receiver sends positive ACK if a frame arrived safe and in order.

If the frames are damaged/out of order, receiver is silent and discard all subsequent frames until it receives the one it is expecting.

The silence of the receiver causes the timer of the unacknowledged frame to expire.

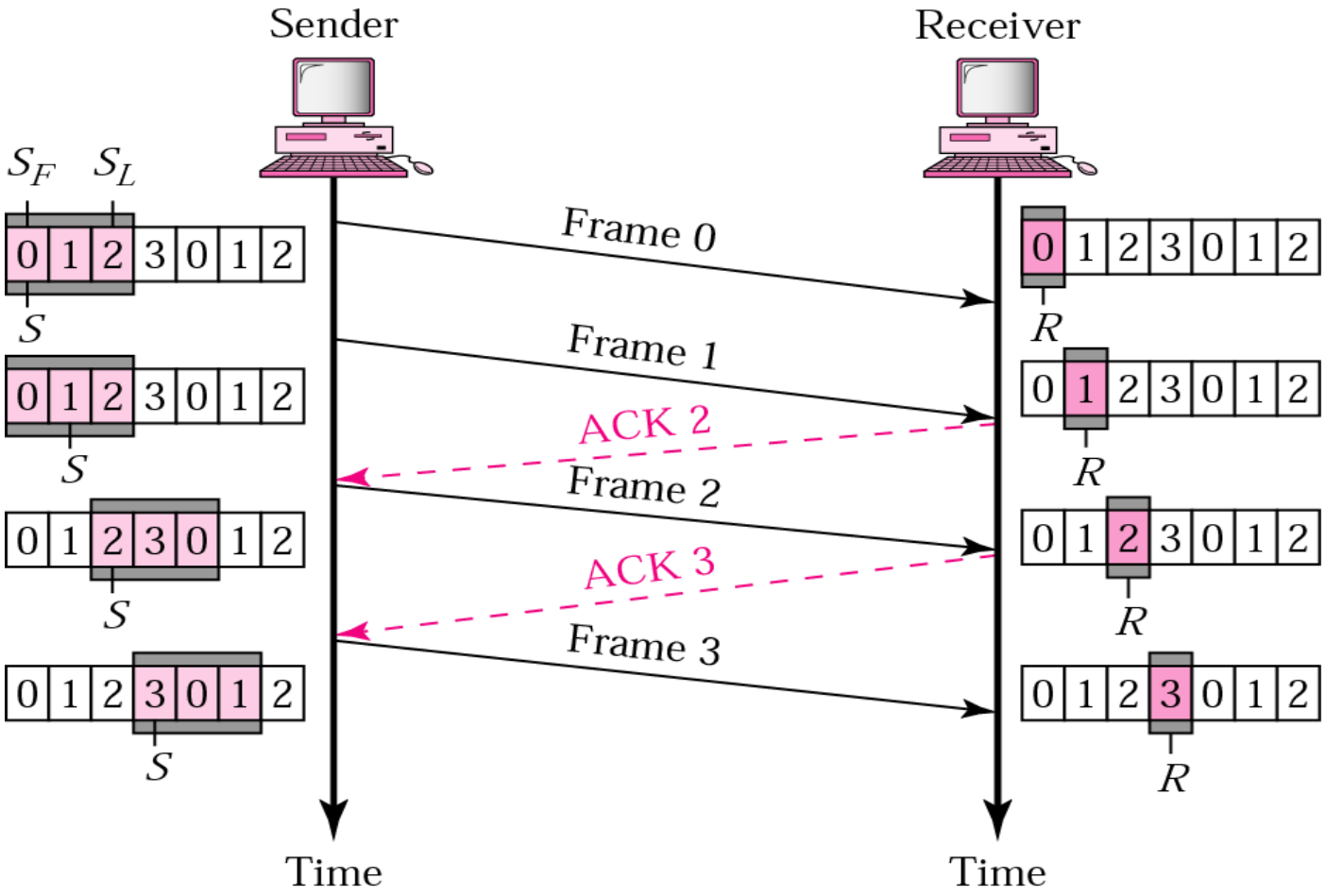
Then the sender resends all frames, beginning with the one with the expired timer.

For example, suppose the sender has sent frame 6, but the timer for frame 3 expires (i.e. frame 3 has not been acknowledged), then the sender goes back and sends frames 3, 4, 5, 6 again. Thus it is called Go-Back-N-ARQ

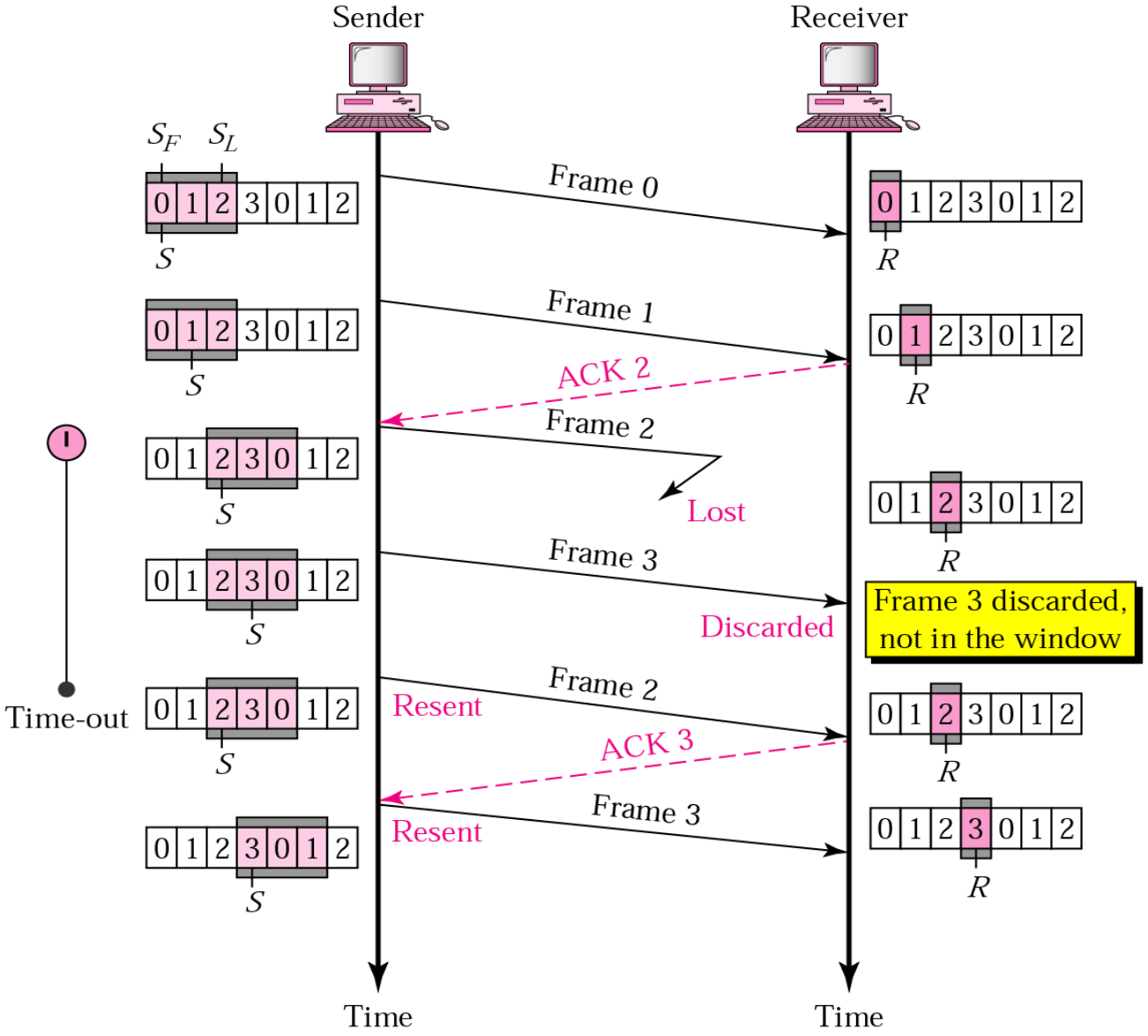
The receiver does not have to acknowledge each frame received, it can send one cumulative ACK for several frames.

Go-Back-N ARQ, normal operation

- The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.



Go-Back-N ARQ, lost frame



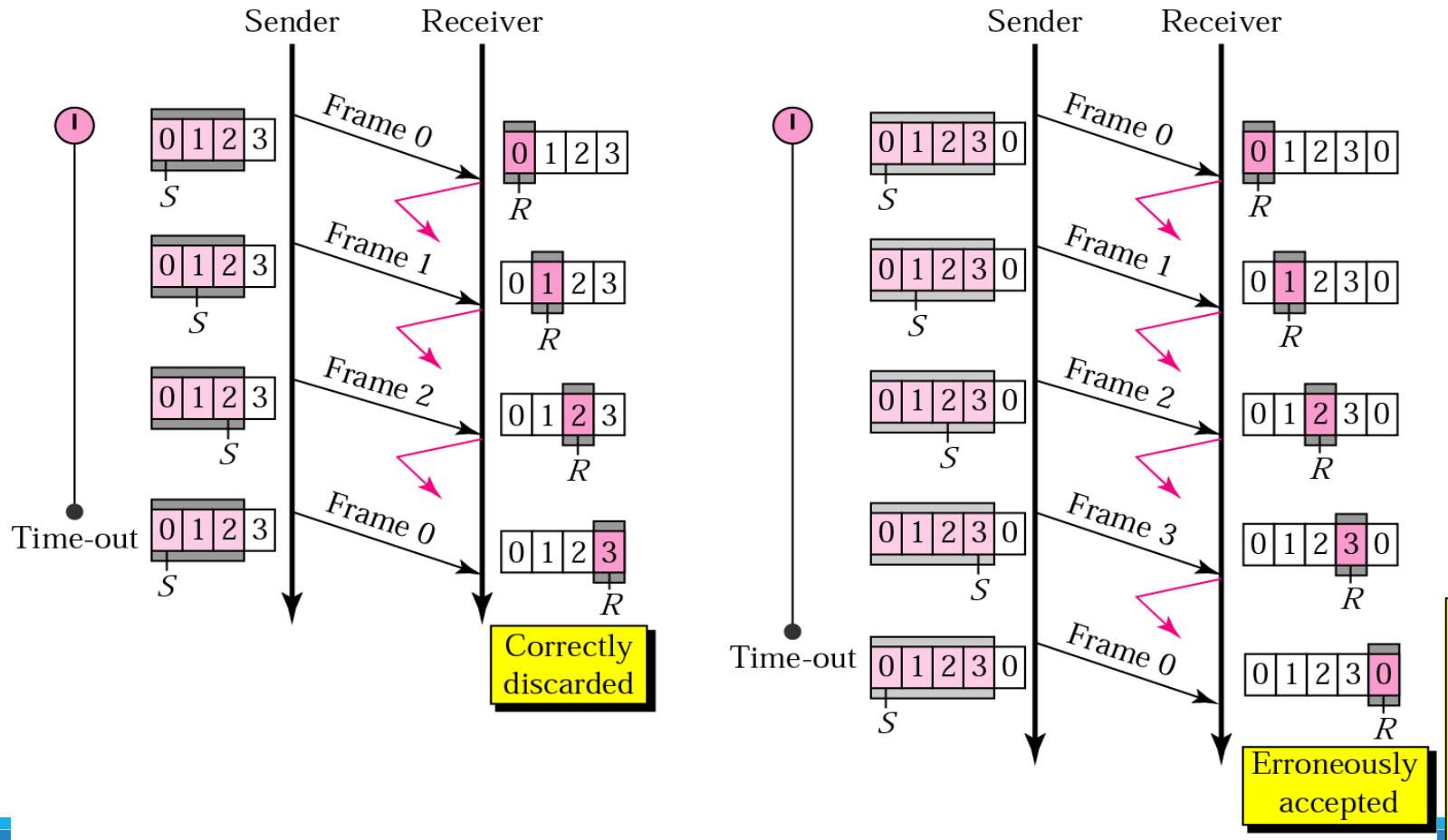
- Frame 2 is lost
- When the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window).
- After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (go back to 2)

Go-Back-N ARQ, damaged/lost/delayed ACK

- If an ACK is damaged/lost, we can have two situations:
- If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames because ACKs are cumulative in this protocol.
- If ACK1, ACK2, and ACk3 are lost, ACK4 covers them if it arrives before the timer expires.
- If ACK4 arrives after time-out, the last frame and all the frames after that are resent.
- Receiver never resends an ACK.
- A delayed ACK also triggers the resending of frames

Go-Back-N ARQ, sender window size

- Size of the sender window must be less than 2^m. Size of the receiver is always 1. If m = 2, window size = $2^m - 1 = 3$.
- Fig compares a window size of 3 and 4.



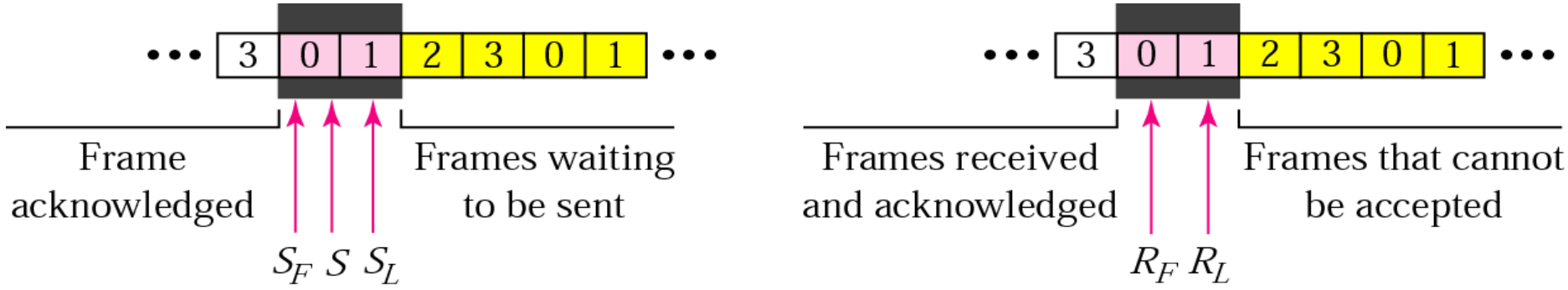
a. Window size < 2^m

b. Window size = 2^m

Accepts as the 1st frame in the next cycle-an **error**

Selective Repeat ARQ, sender and receiver windows

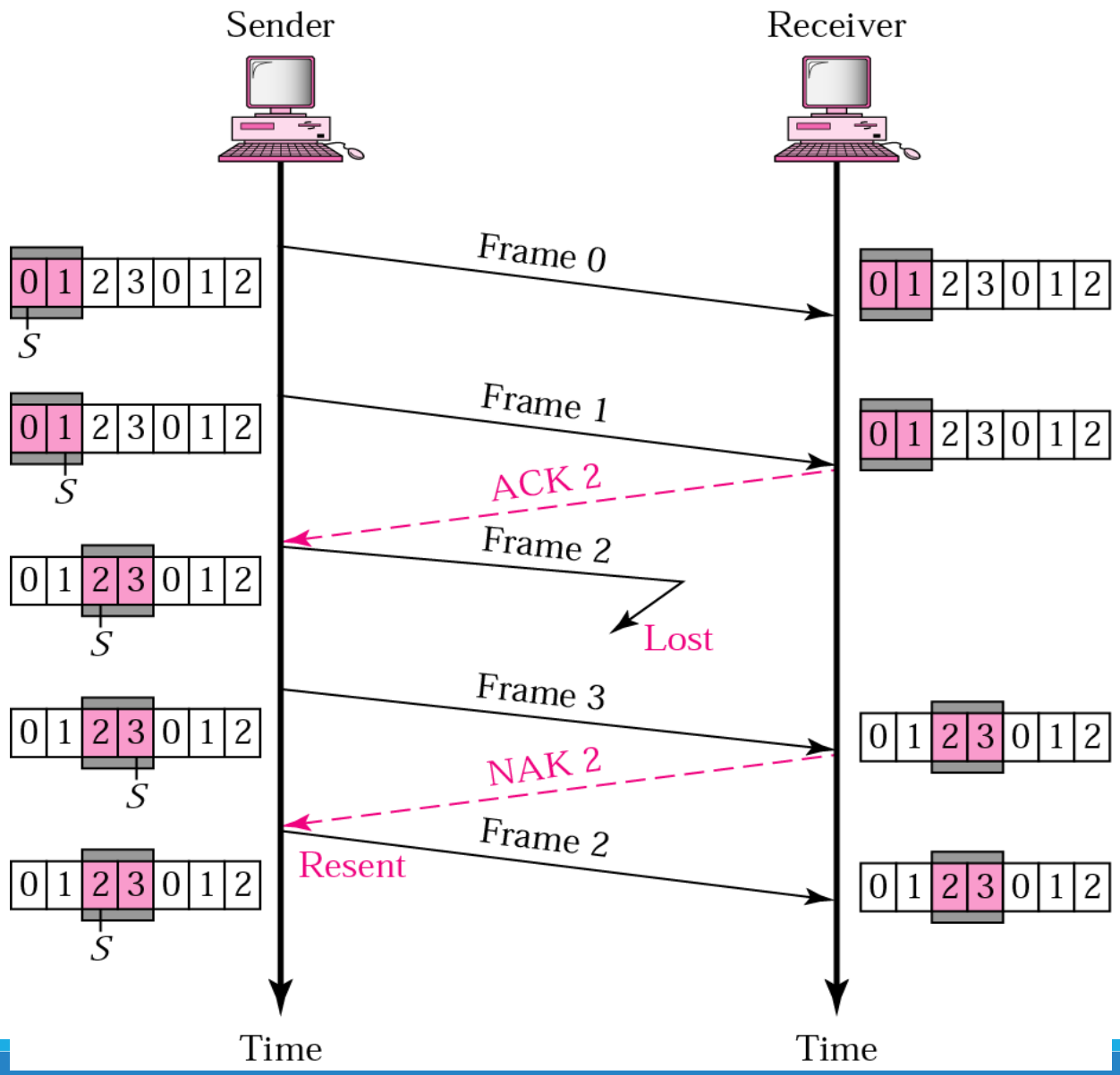
- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission.
- In Selective Repeat ARQ, only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.



a. Sender window

b. Receiver window

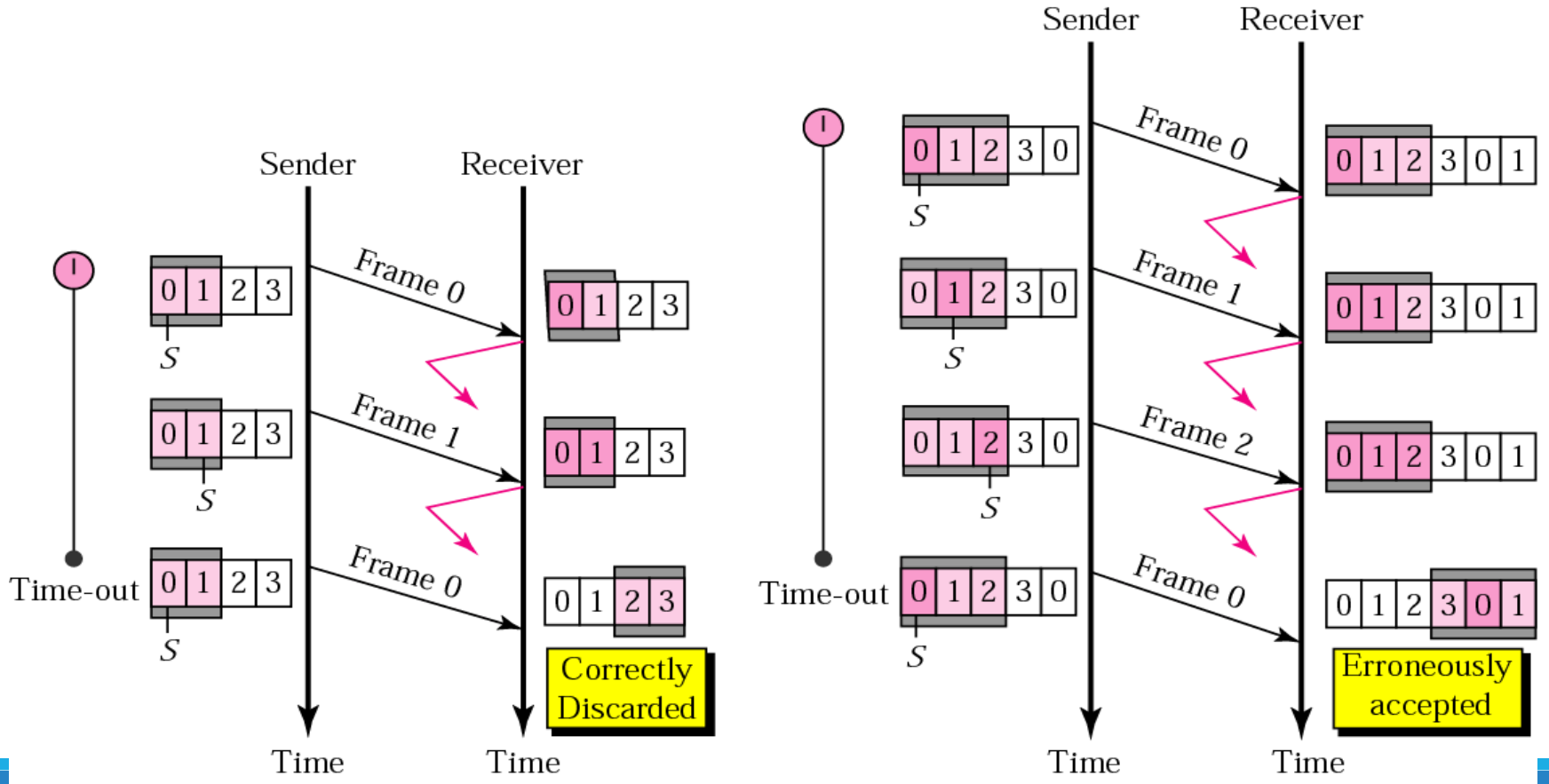
Selective Repeat ARQ, lost frame



- Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3.
- Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

size

- Size of the sender and receiver windows must be at most one-half of 2^m. If m = 2, window size should be $2^m/2 = 2$. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an **error**.



a. Window size = 2^{m-1}

b. Window size > 2^{m-1}

Problems

In SR protocol, suppose frames through 0 to 4 have been transmitted. Now, imagine that 0 times out, 5 (a new frame) is transmitted, 1 times out, 2 times out and 6 (another new frame) is transmitted.

At this point, what will be the outstanding packets in sender’s window?

	Stop and Wait ARQ	Go back N	Selective Repeat	Remarks
Efficiency	1 / (1+2a)	N / (1+2a)	N / (1+2a)	Go back N and Selective Repeat gives better efficiency than Stop and Wait ARQ.
Window Size	Sender Window Size = 1 Receiver Window Size = 1	Sender Window Size = N Receiver Window Size = 1	Sender Window Size = N Receiver Window Size = N	Buffer requirement in Selective Repeat is very large. If the system does not have lots of memory, then it is better to choose Go back N.
Minimum number of sequence numbers required	2	N+1	2 x N	Selective Repeat requires large number of bits in sequence number field.
Retransmissions required if a packet is lost	Only the lost packet is retransmitted	The entire window is retransmitted	Only the lost packet is retransmitted	Selective Repeat is far better than Go back N in terms of retransmissions required.
Bandwidth Requirement	Bandwidth requirement is Low	Bandwidth requirement is high because even if a single packet is lost, entire window has to be retransmitted. Thus, if error rate is high, it wastes a lot of bandwidth.	Bandwidth requirement is moderate	Selective Repeat is better than Go back N in terms of bandwidth requirement.
CPU usage	Low	Moderate	High due to searching and sorting required at sender and receiver side	Go back N is better than Selective Repeat in terms of CPU usage.
Level of difficulty in			Complex as it requires extra logic	Go back N is better than Selective

[Type here]

Multiple Access

Data link layer divided into two functionality-oriented sublayers

Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

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

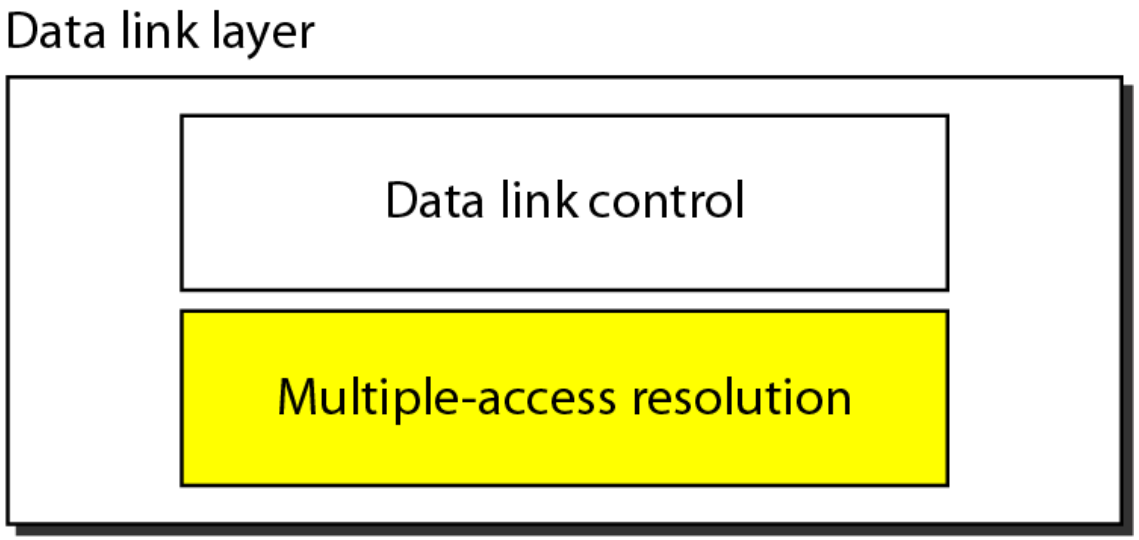
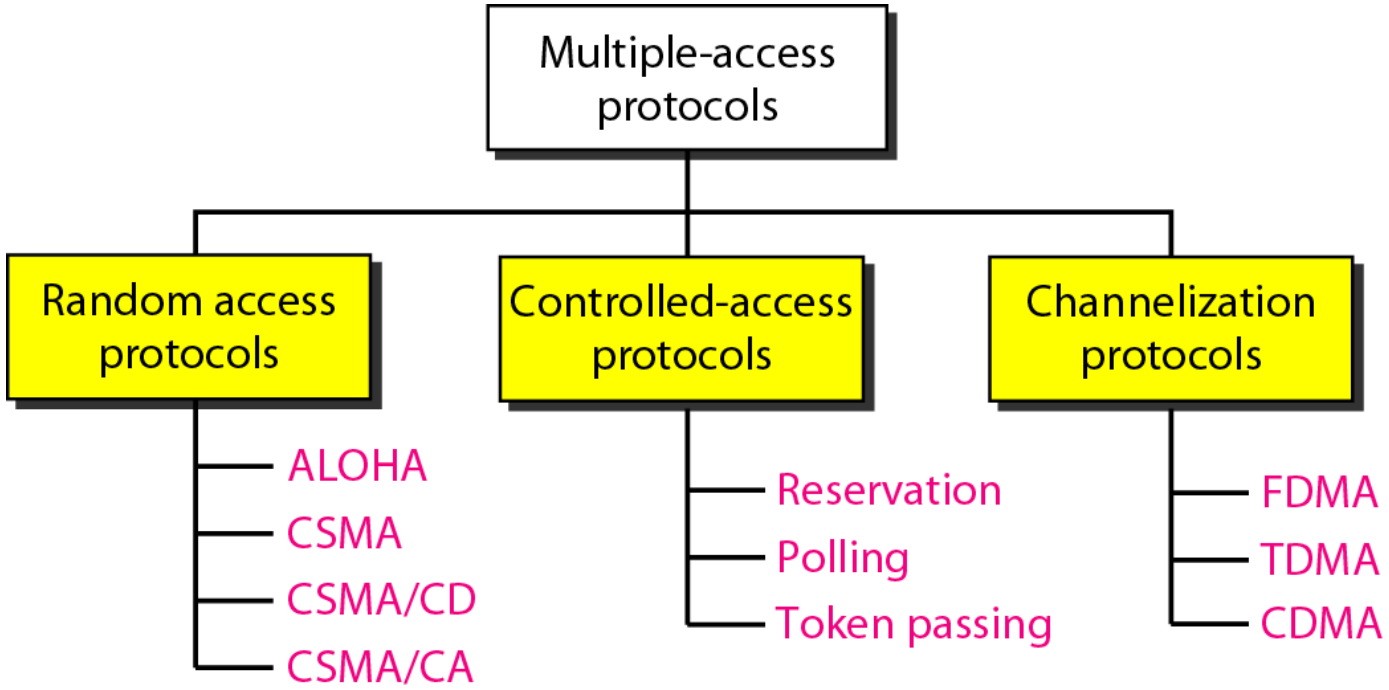


Figure: Taxonomy of multiple-access protocols discussed in this chapter



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.

Each station follows a procedure that answers the following questions:

o When can the station access the medium?

o What can the station do if the medium is busy?

o How can the station determine the success or failure of the transmission?

o What can the station do if there is an access conflict?

ALOHA

There are two different versions of Aloha-

1. Pure Aloha
2. Slotted Aloha

1. 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.

Then,

- Transmitting station uses a **Back Off Strategy** and waits for some random amount of time.
- After back off time, it transmits the data packet again.
- It keeps trying until the back off limit is reached after which it aborts the transmission.

Figure Procedure for pure ALOHA protocol

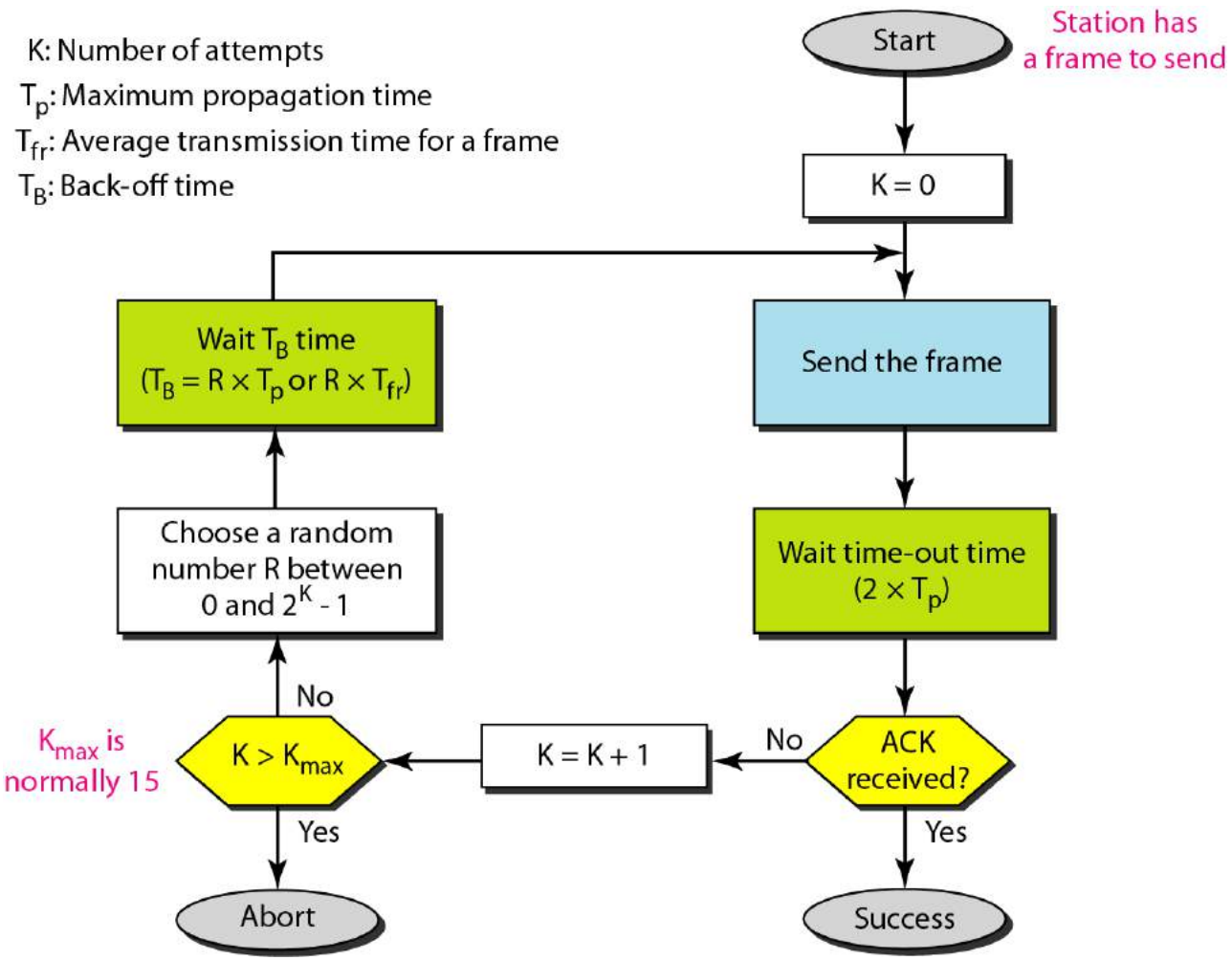
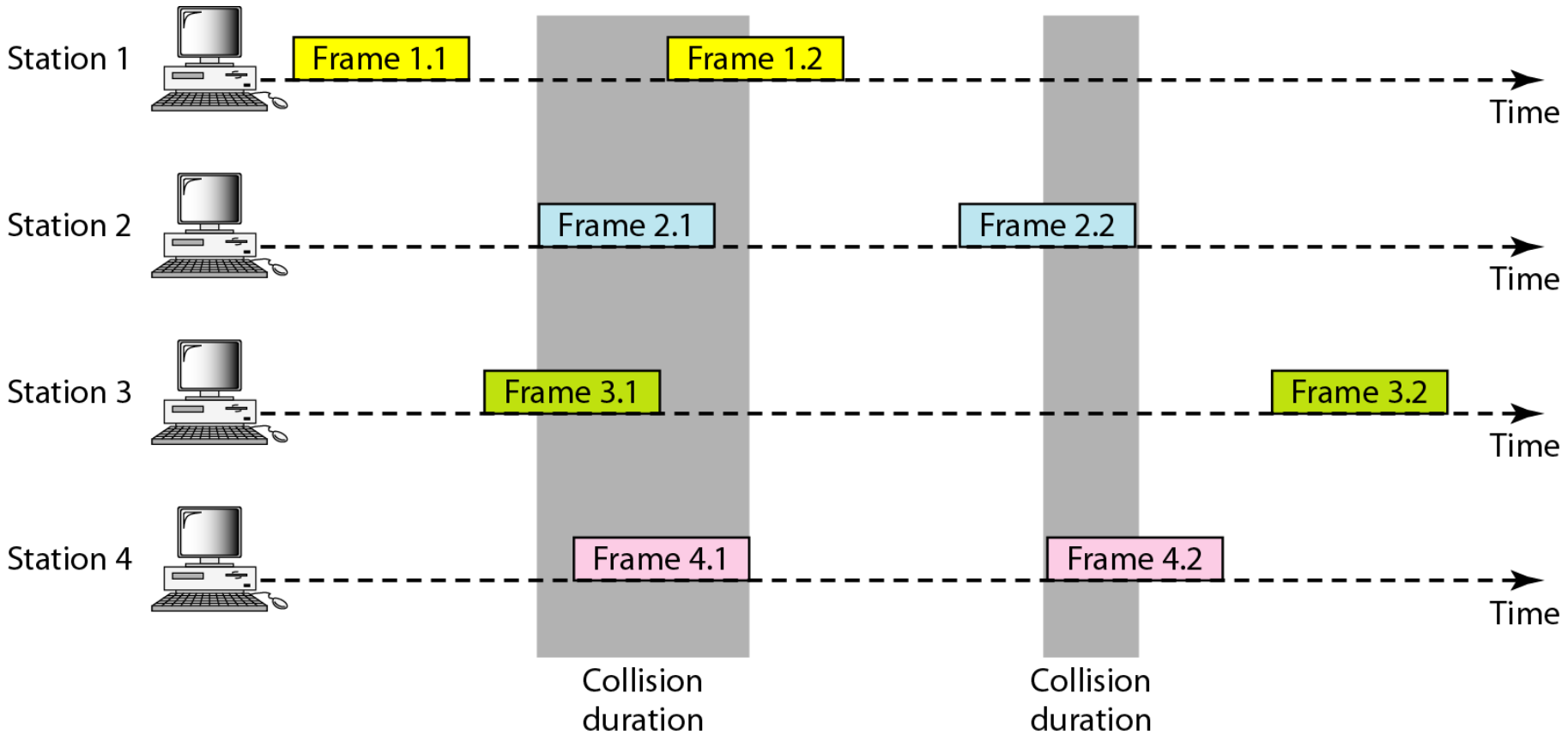


Figure Frames in a pure ALOHA network



Example

The stations on a wireless ALOHA network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s, we find

$$T_p = (600 \times 10^5) / (3 \times 10^8) = 2 \text{ ms.}$$

Now we can find the value of T_B for different values of K .

a. For K = 1, the range is {0, 1}. The station needs to generate a random number with a value of 0 or 1. This means that T_B is either 0 ms (0 × 2) or 2 ms (1 × 2), based on the outcome of the random variable.

Example (continued)

b. For K = 2, the range is {0, 1, 2, 3}. This means that T_B can be 0, 2, 4, or 6 ms, based on the outcome of the random variable.

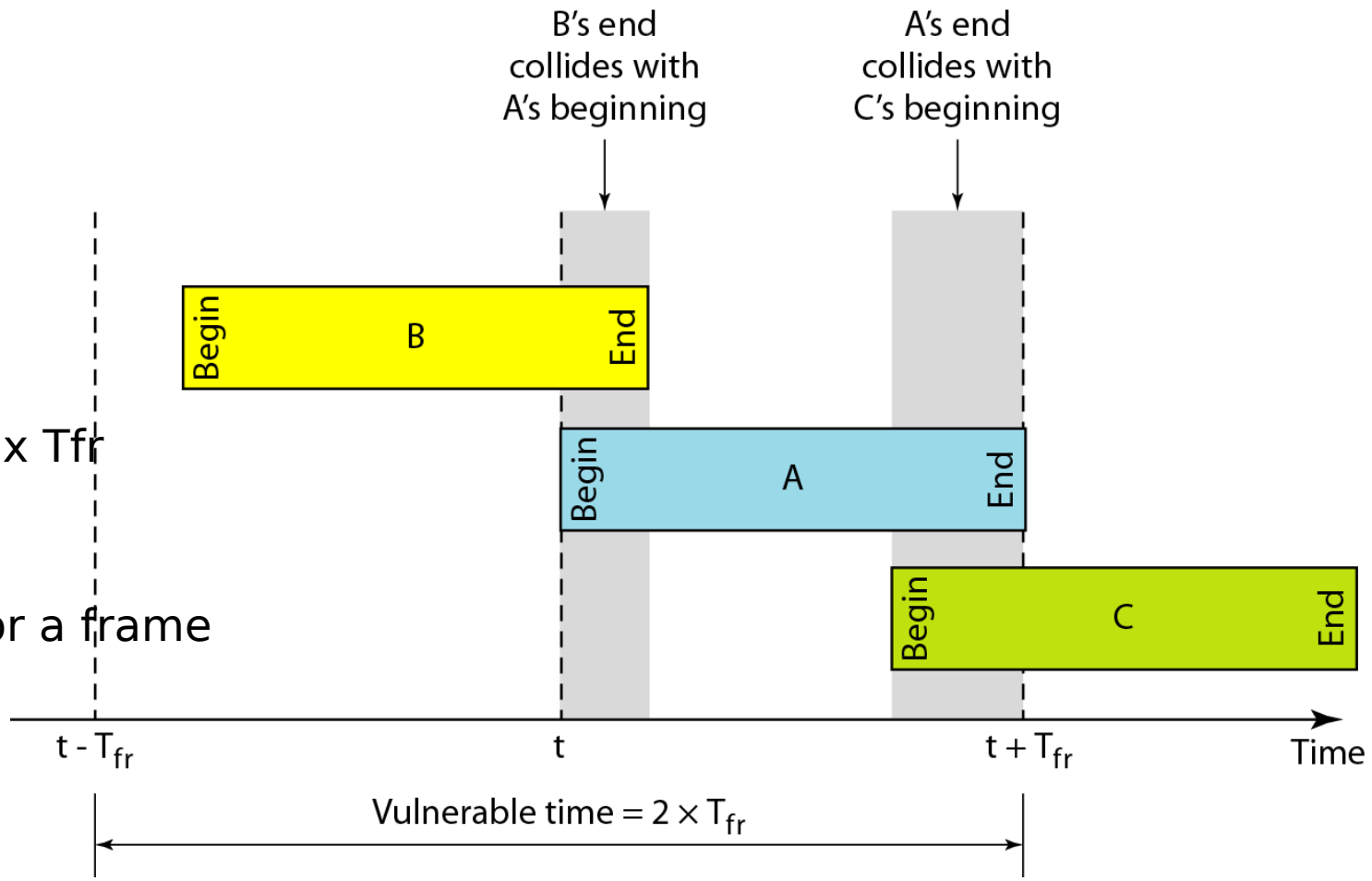
c. For K = 3, the range is {0, 1, 2, 3, 4, 5, 6, 7}. This means that T_B can be 0, 2, 4, . . . , 14 ms, based on the outcome of the random variable.

Figure Vulnerable time for pure ALOHA protocol

The vulnerable time, in which there is a possibility of collision

Pure ALOHA vulnerable time = 2 x Tfr

Tfr: Average transmission time for a frame



Example

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?

Example

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?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the one 1-ms period that this station is sending.

Efficiency-

Efficiency of Pure Aloha (η) = $G \times e^{-2G}$

G the average number of frames generated by the system during one frame transmission time.

Maximum Efficiency-

Maximum Efficiency of Pure Aloha (η) = 18.4%

Note

The throughput for pure ALOHA is

$S = G \times e^{-2G}$.

The maximum throughput

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

Example

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.

Example

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 $S = G \times e^{-2G}$ or $S = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

Example (continued)

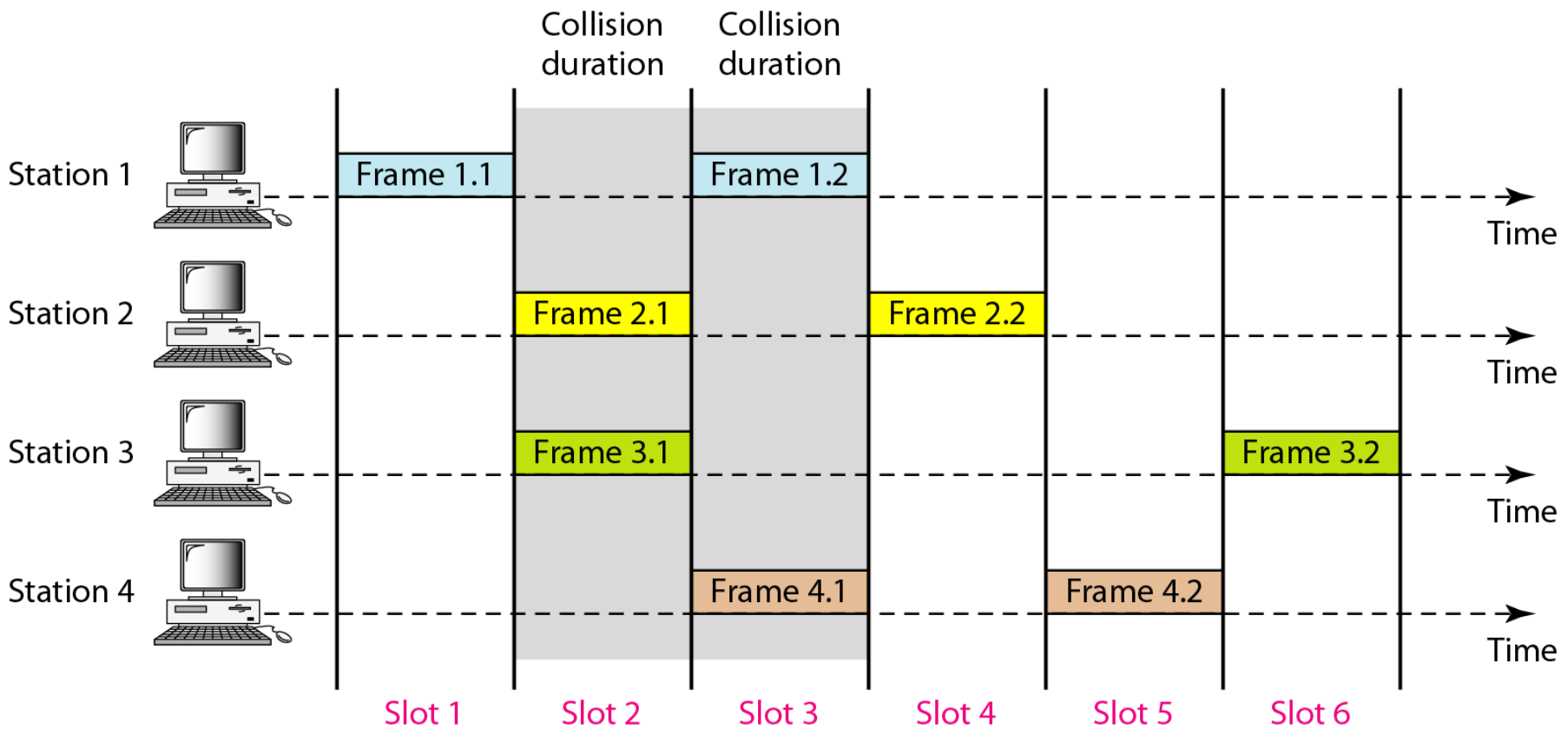
b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or $S = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this 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 $S = G \times e^{-2G}$ or $S = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

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.

Figure Frames in a slotted ALOHA network



Note

The throughput for slotted ALOHA is

$S = G \times e^{-G}$.

The maximum throughput

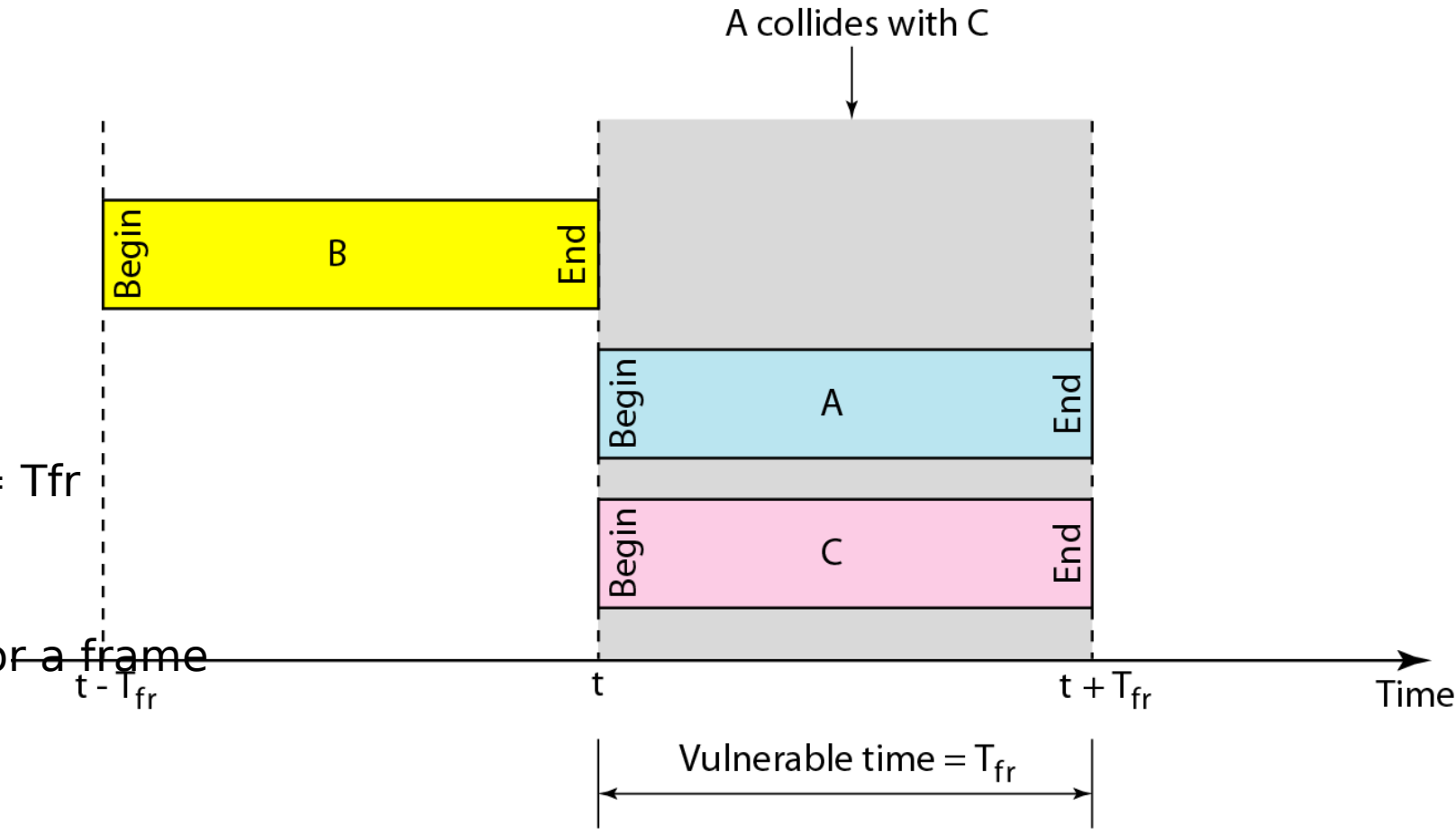
$S_{max} = 0.368$ when $G = 1$.

Figure Vulnerable time for slotted ALOHA protocol

The vulnerable time, in which there is a possibility of collision

Slotted ALOHA vulnerable time = Tfr

Tfr: Average transmission time for a frame



Example

A slotted 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.

Example

A slotted 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 $S = G \times e^{-G}$ or $S = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 386 frames out of 1000 will probably survive.

Example (continued)

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-G}$ or $S = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-G}$ or $S = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

Problems

A group of N stations share 100 Kbps slotted ALOHA channel. Each station output a 500 bits frame on an average of 5000 ms even if previous one has not been sent. What is the required value of N?

CSMA

Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

Sensing the Carrier-

•Any station willing to transmit the data senses the carrier.
•If it finds the carrier free, it starts transmitting its data packet otherwise not.

How?

•Each station can sense the carrier only at its point of contact with the carrier.
•It is not possible for any station to sense the entire carrier.
•Thus, there is a huge possibility that a station might sense the carrier free even when it is actually not.

Figure Space/time model of the collision in CSMA

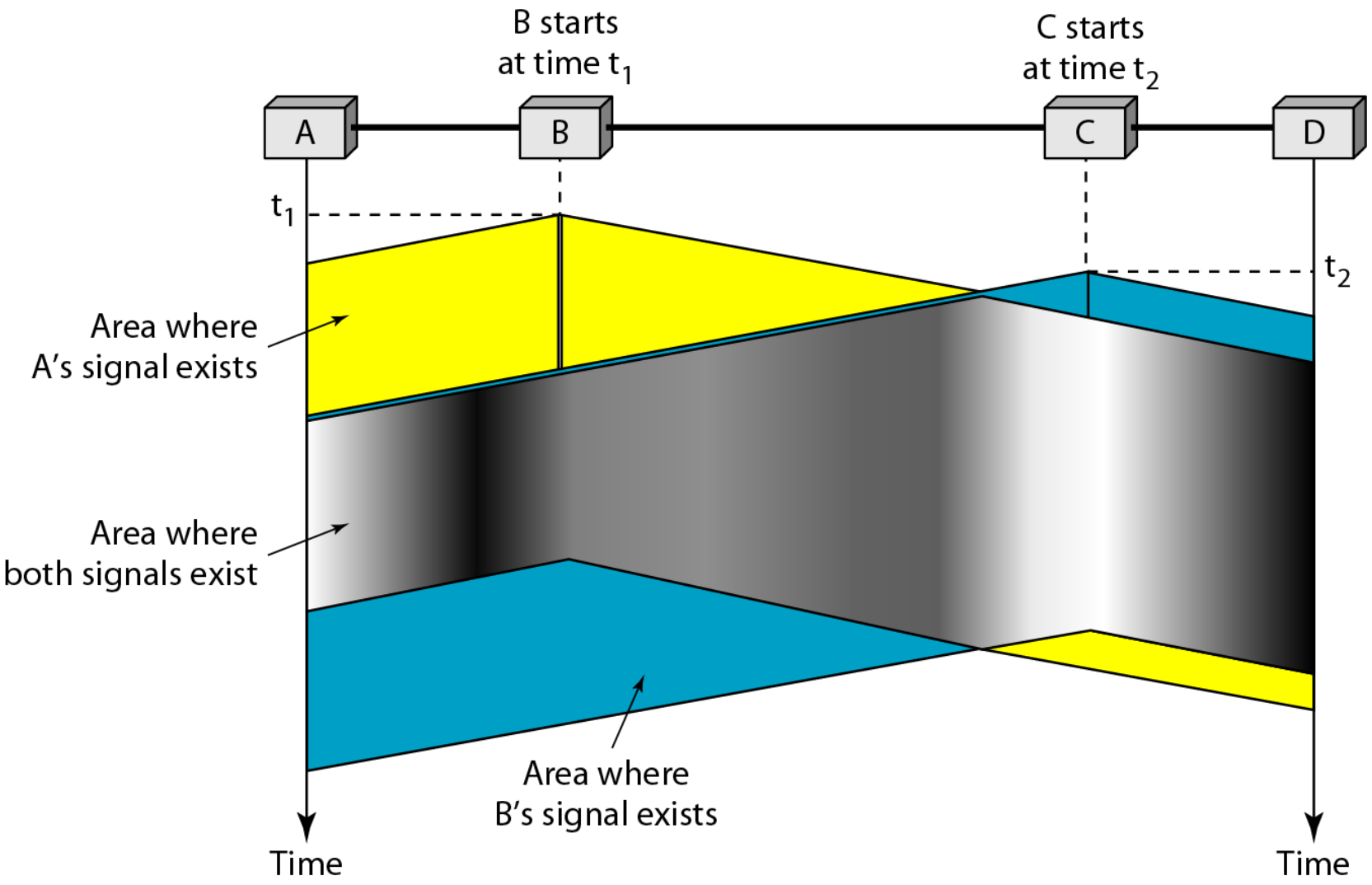


Figure Vulnerable time in CSMA

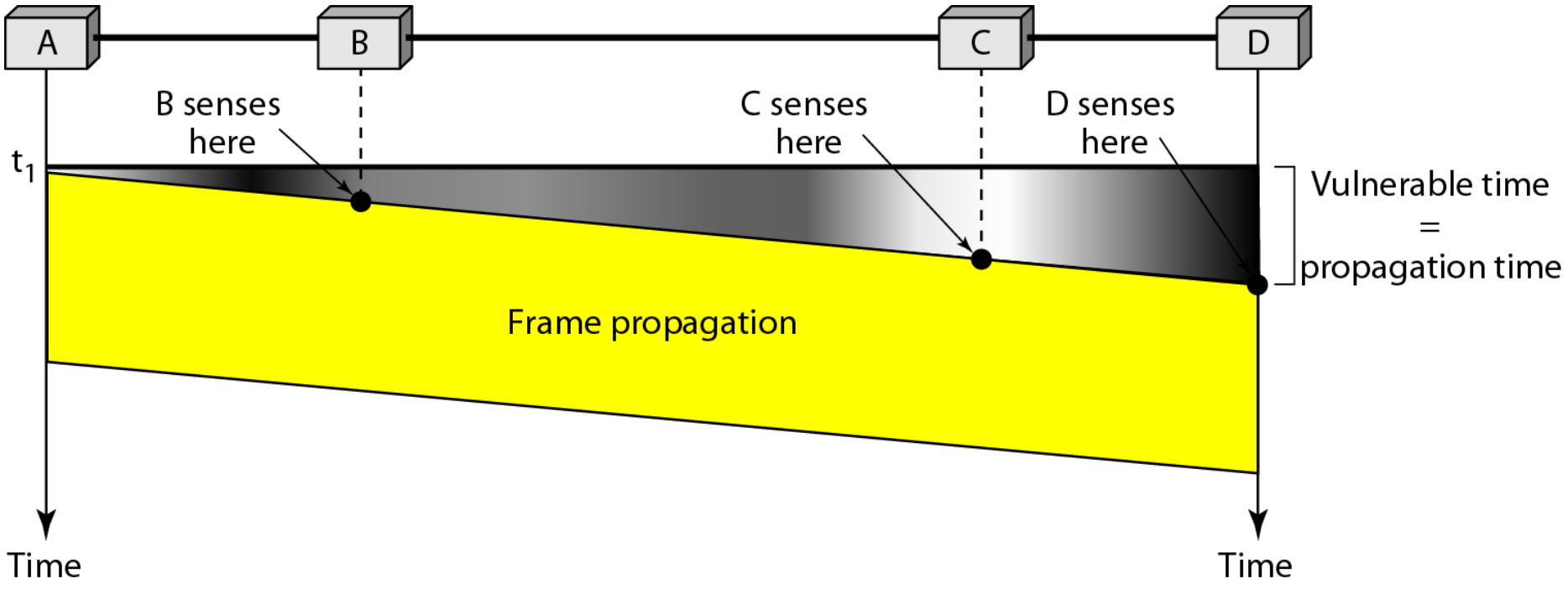


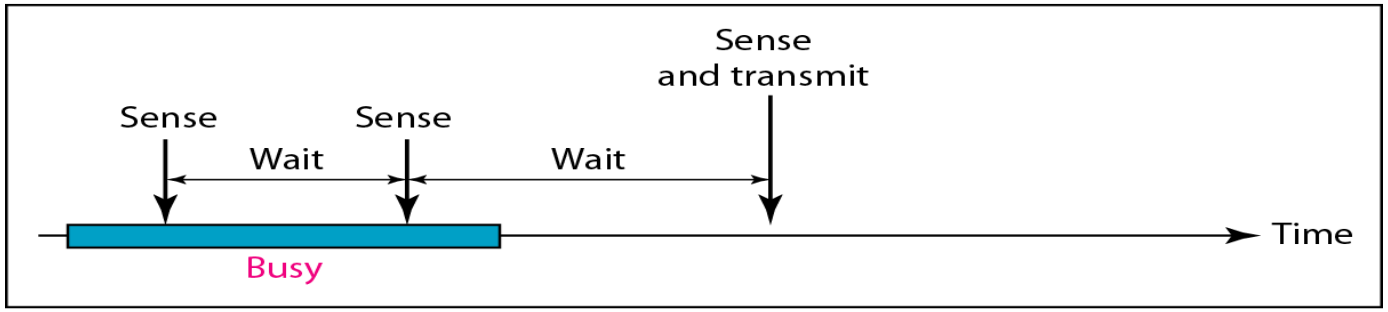
Figure Behavior of three persistence methods

What should a station do if the channel is busy?

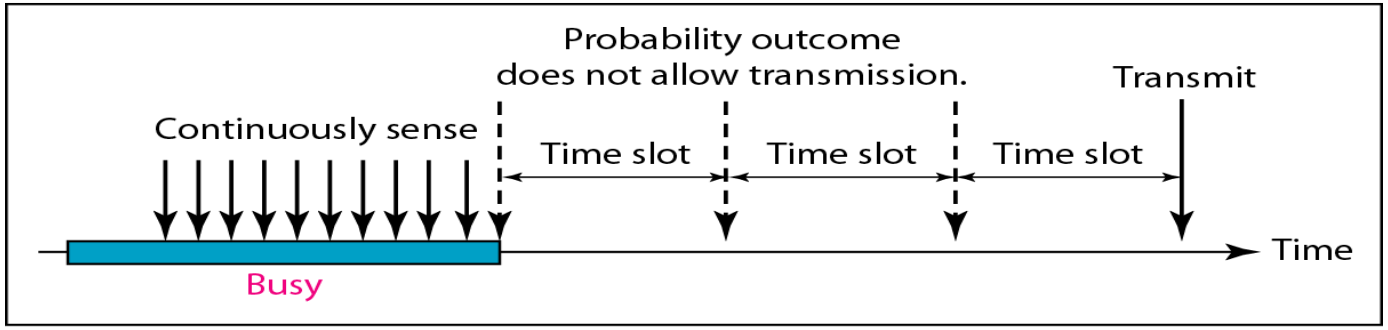
What should a station do if the channel is idle?

Three methods have been devised to answer these questions

a. 1-persistent



b. Nonpersistent



c. p-persistent

I-Persistent

In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).

This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

Nonpersistent

In the nonpersistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.

The nonpersistent approach reduces the chance of collision.

this method reduces the efficiency of the network

p-Persistent

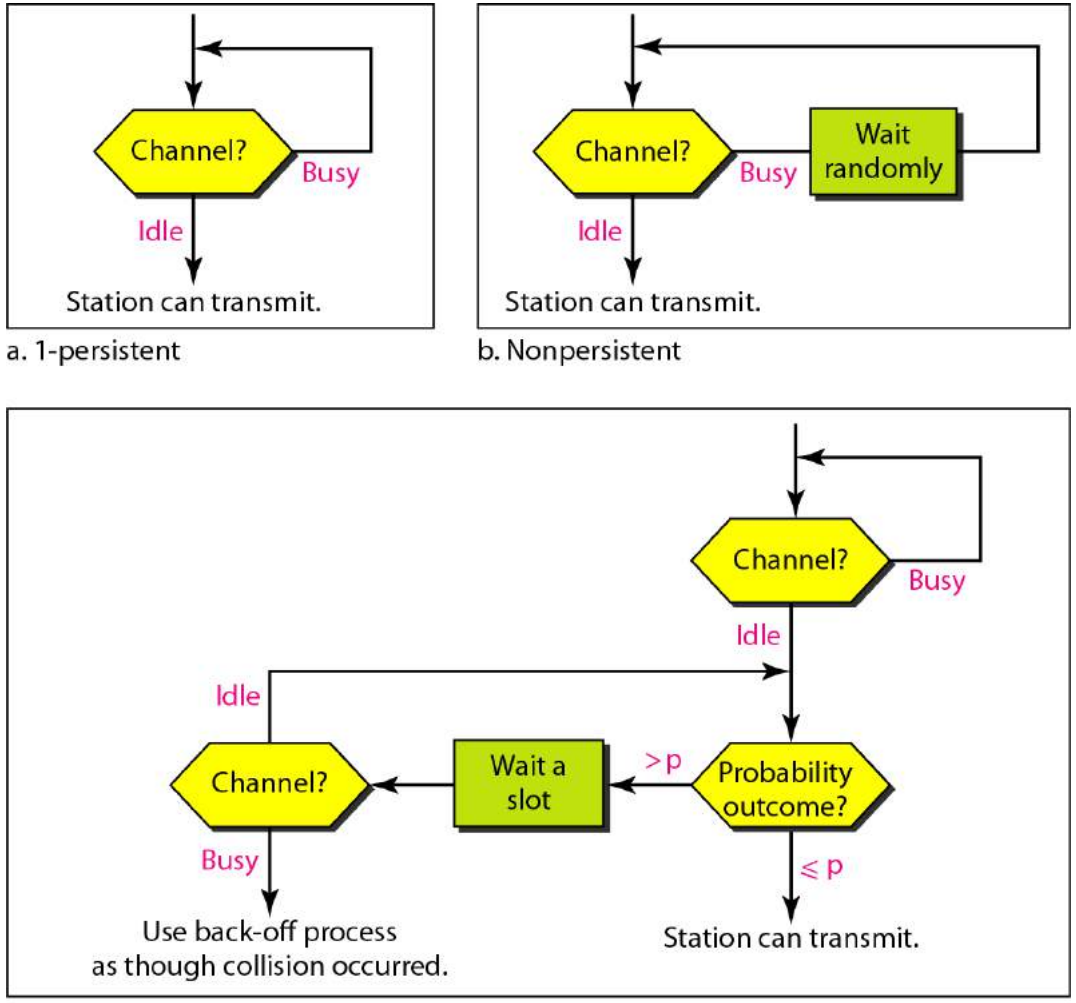
The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.

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. With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.
   a. If the line is idle, it goes to step 1.
   b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

Figure Flow diagram for three persistence methods



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

Detecting the Collision-

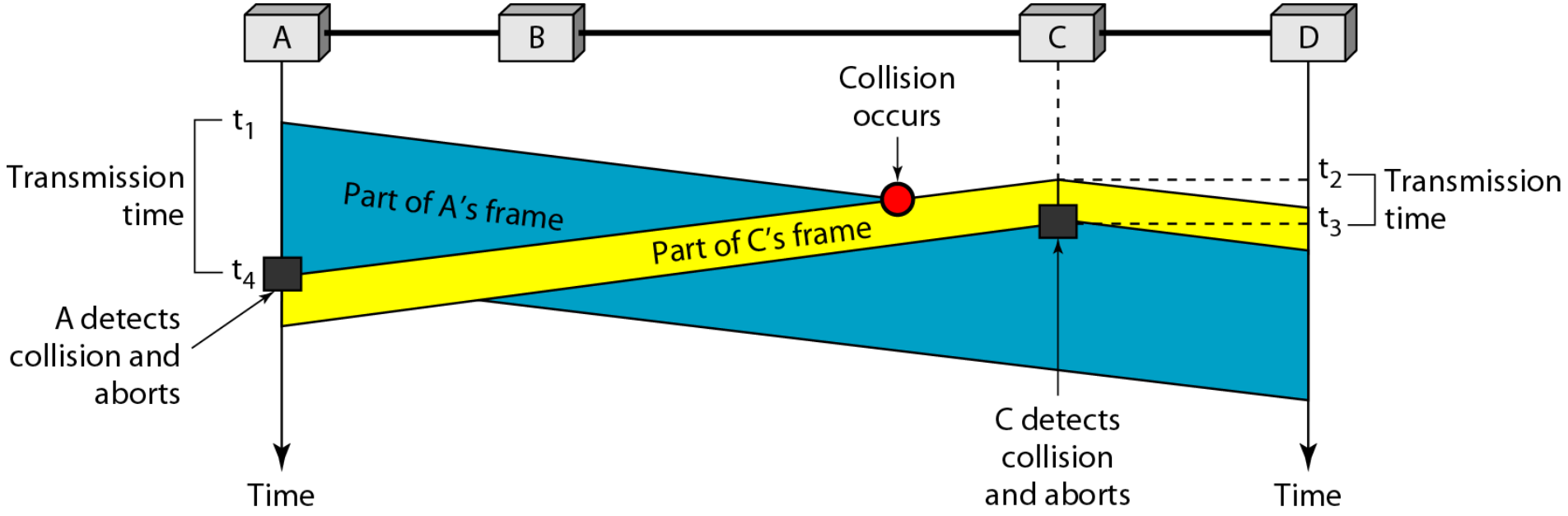
In CSMA / CD,

- It is the responsibility of the transmitting station to detect the collision.
- For detecting the collision, CSMA / CD implements the following condition.
- This condition is followed by each station-
- Transmission delay >= 2 x Propagation delay

According to this condition,

- Each station must transmit the data packet of size whose transmission delay is at least twice its propagation delay.
- If the size of data packet is smaller, then collision detection would not be possible.

Figure Collision and abortion in CSMA/CD



Example

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time is 25.6 μs, what is the minimum size of the frame?

Example

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time is 25.6 μs, what is the minimum size of the frame?

Solution

The frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet.

Problem

A network with CSMA/CD protocol in the MAC layer is running at 1 Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 2 x 10^8 m/sec. The minimum frame size for this network should be

Two cases are possible

Case-01:

If no collided signal comes back during the transmission,

- It indicates that no collision has occurred.
- The data packet is transmitted successfully.

Case-02:

If the collided signal comes back during the transmission,

- It indicates that the collision has occurred.
- The data packet is not transmitted successfully.
- Releasing Jamming signal

Releasing Jam Signal

- Jam signal is a 48 bit signal.
- It is released by the transmitting stations as soon as they detect a collision.
- It alerts the other stations not to transmit their data immediately after the collision.
- Otherwise, there is a possibility of collision again with the same data packet.

Waiting For Back Off Time

- After the collision, the transmitting station waits for some random amount of time called as **back off time**.
- After back off time, it tries transmitting the data packet again.
- If again the collision occurs, then station again waits for some random back off time and then tries again.
- The station keeps trying until the back off time reaches its limit.
- After the limit is reached, station aborts the transmission.

Figure Flow diagram for the CSMA/CD

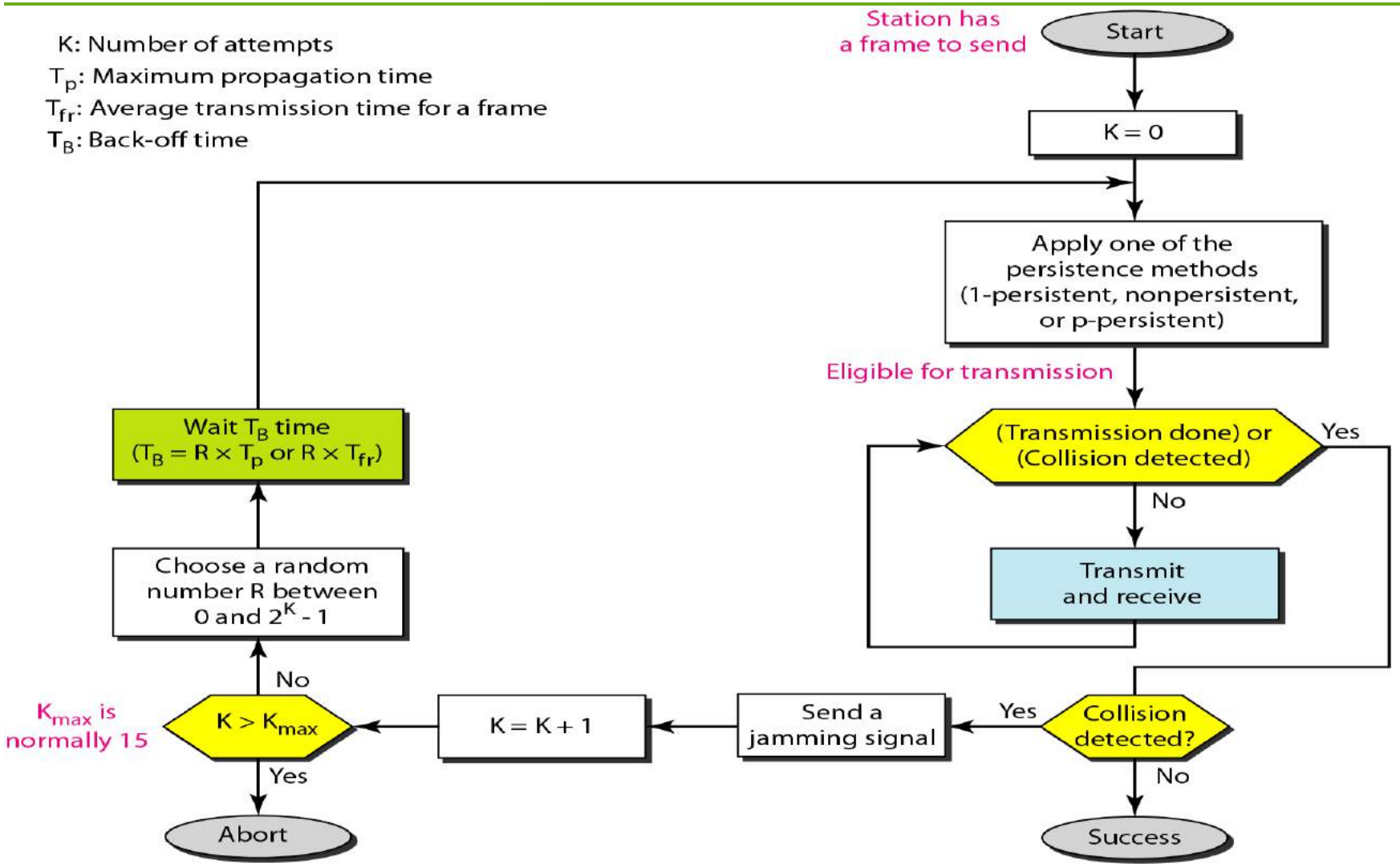
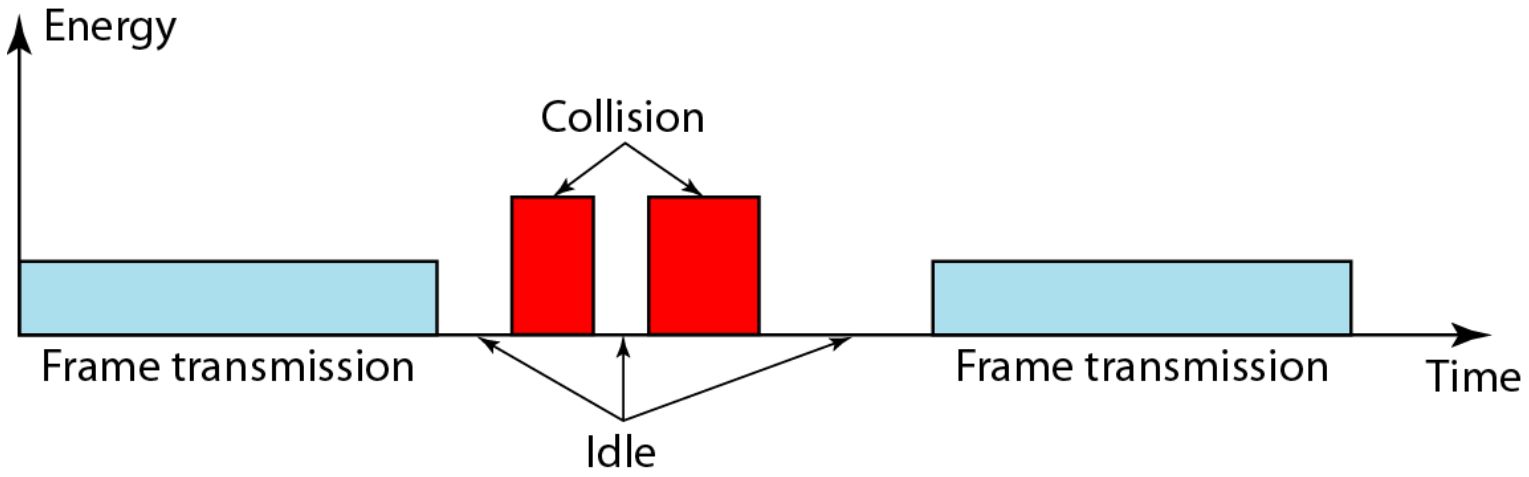


Figure Energy level during transmission, idleness, or collision

At the zero level, the channel is idle.

At the normal level, a station has successfully captured the channel and is sending its frame.

At the abnormal level, there is a collision and the level of the energy is twice the normal level.



Carrier sense multiple access with collision avoidance (CSMA/CA)

In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision.

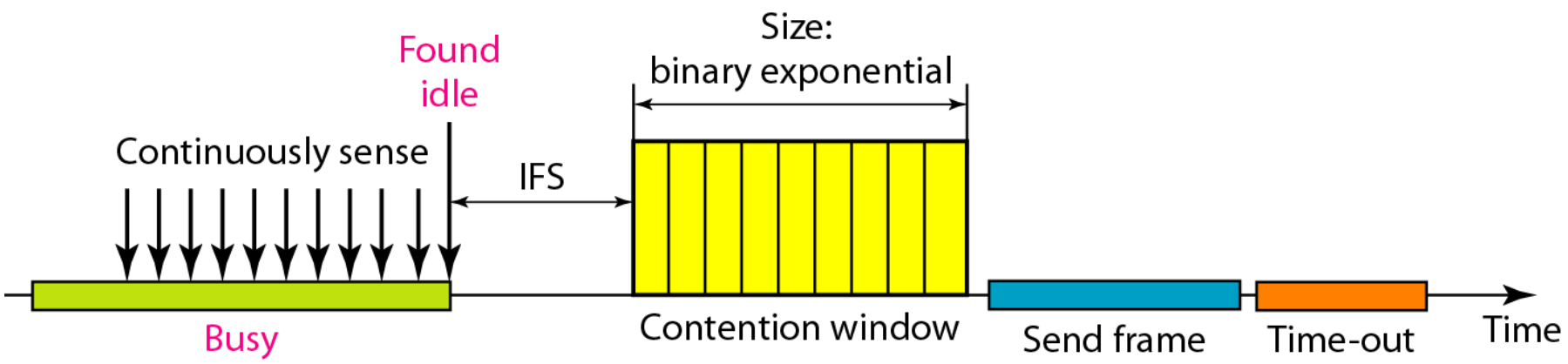
In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can’t be used by the station to sense collision.

Therefore **CSMA/CA has been specially designed for wireless networks**.

Figure Timing in CSMA/CA

Collisions are avoided through the use of CSMA/CA's three strategies:

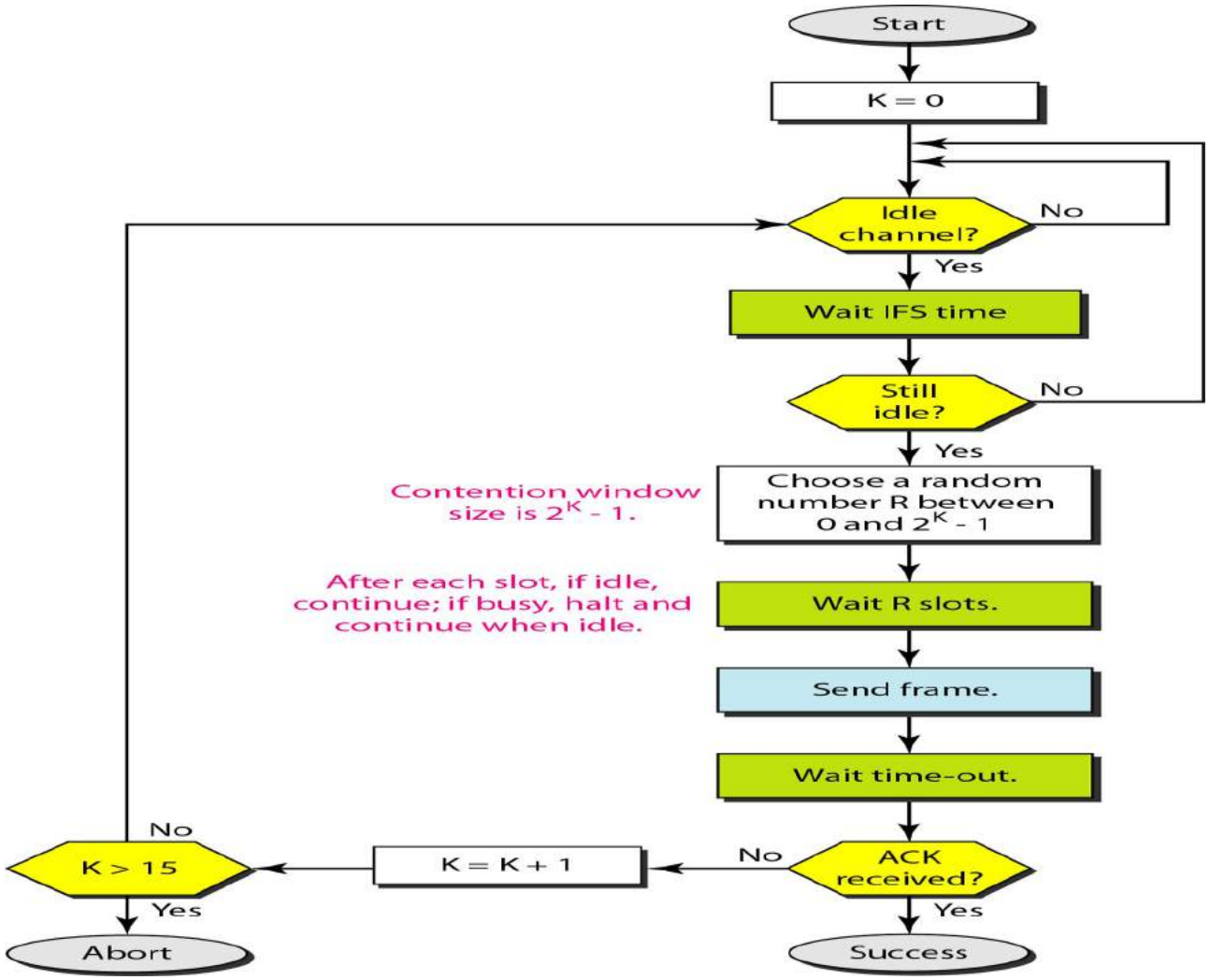
1. the interframe space
2. the contention window
3. acknowledgments



Note

In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

Figure Flow diagram for CSMA/CA



Network Layer: Logical Addressing

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

Note

An IPv4 address is 32 bits long.

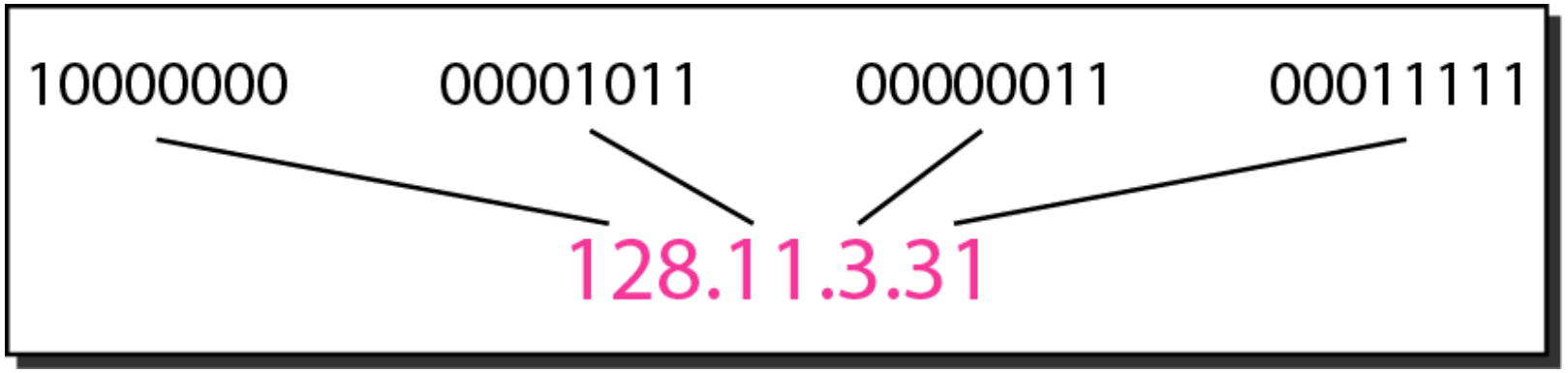
Note

The IPv4 addresses are unique
and universal.

Note

The address space of IPv4 is
2^{32} or 4,294,967,296.

Figure *Dotted-decimal notation and binary notation for an IPv4 address*



Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

a. There must be no leading zero (045).

b. There can be no more than four numbers.

c. Each number needs to be less than or equal to 255.

d. A mixture of binary notation and dotted-decimal notation is not allowed.

Note

In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

Figure *Finding the classes in binary and dotted-decimal notation*

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

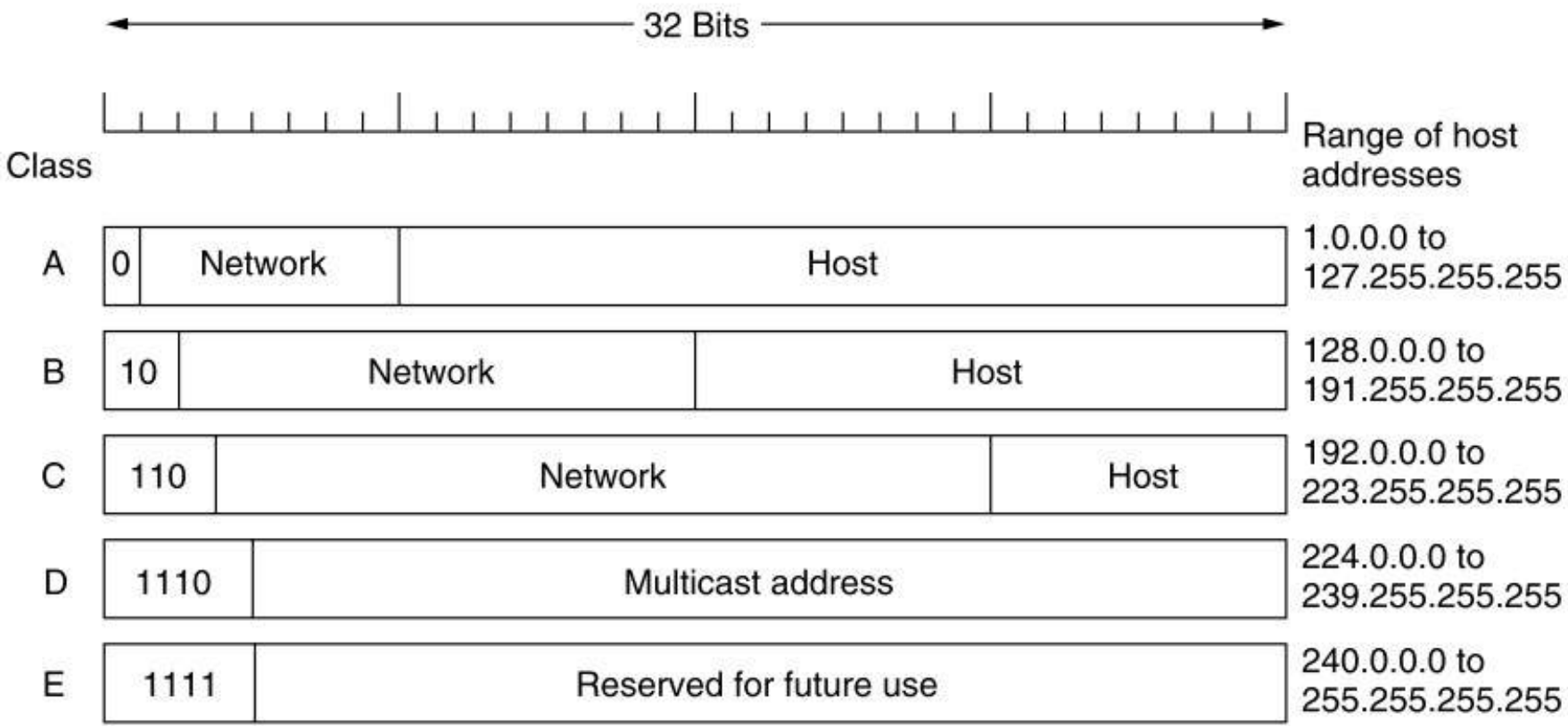
	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

1. **Network ID** represents the IP Address of the network and is used to identify the network.

2. **Host ID** represents the IP Address of the host and is used to identify the host within the network.

Format of an IP Address


32 Bits
Class
Range of host addresses
A
0
Network
Host
1.0.0.0 to 127.255.255.255
B
10
Network
Host
128.0.0.0 to 191.255.255.255
C
110
Network
Host
192.0.0.0 to 223.255.255.255
D
1110
Multicast address
224.0.0.0 to 239.255.255.255
E
1111
Reserved for future use
240.0.0.0 to 255.255.255.255

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Find the class of each address.

a. 00000001 00001011 00001011 11101111
b. 11000001 10000011 00011011 11111111
c. 14.23.120.8
d. 252.5.15.111

Solution

a. *The first bit is 0. This is a class A address.*
b. *The first 2 bits are 1; the third bit is 0. This is a class C address.*
c. *The first byte is 14; the class is A.*
d. *The first byte is 252; the class is E.*

Table *Number of blocks and block size in classful IPv4 addressing*

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Class of IP Address	Total Number of IP Addresses	1st Octet Decimal Range	Number of Networks available	Hosts per network	Default Subnet Mask
Class A	2^{31}	1 – 126	$2^{7} – 2$	$2^{24} – 2$	255.0.0.0
Class B	2^{30}	128 – 191	2^{14}	$2^{16} – 2$	255.255.0.0
Class C	2^{29}	192 – 223	2^{21}	$2^{8} – 2$	255.255.255.0
Class D	2^{28}	224 – 239	Not defined	Not defined	Not defined
Class E	2^{28}	240 – 254	Not defined	Not defined	Not defined

In class A, total number of IP Addresses available for networks are 2 less.

- This is to account for the two reserved network IP Addresses 0.xxx.xxx.xxx and 127.xxx.xxx.xxx.
- IP Address 0.0.0.0 is reserved for broadcasting requirements.
- IP Address 127.0.0.1 is reserved for loopback address used for software testing.

In all the classes, total number of hosts that can be configured are 2 less.

- This is to account for the two reserved IP addresses in which all the bits for host ID are either zero or one.
- When all Host ID bits are 0, it represents the Network ID for the network(NID).
- When all Host ID bits are 1, it represents the Broadcast Address(DBA).

Note

In classful addressing, a large part of the available addresses were wasted.

IPv6 - Address

IPv6 Address format, we shall look into Hexadecimal Number System. Hexadecimal is a positional number system that uses radix (base) of 16. To represent the values in readable format, this system uses 0-9 symbols to represent values from zero to nine and A-F to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.

Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.

For example, given below is a 128 bit IPv6 address represented in binary format and

```
0010000000000001 0000000000000000 0011001000111000 1101111111100001
0000000001100011 0000000000000000 0000000000000000 1111111011111011
```

Each block is then co

```
2001:0000:3238:DFE1:0063:0000:0000:FEFB
```

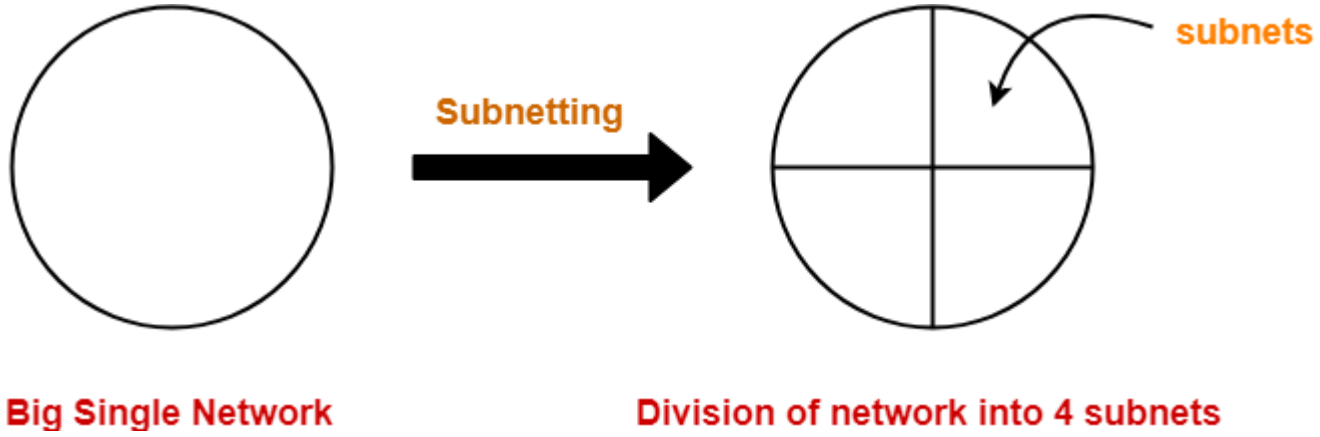
y ‘:’ symbol:

IPv6 looks different than IPv4 but there are some similarities. For example we have unicast addresses and we still have a “public” and “private” range. We use different names for these but the idea is the same.

Subnetting in Networking

Subnetting

- The process of dividing a single network into multiple sub networks is called as **subnetting**.
- The sub networks so created are called as **subnets**.



Advantages

The two main advantages of subnetting a network are-

- It improves the security.
- The maintenance and administration of subnets is easy.

Disadvantages of Subnetting-

- We have to face a loss of IP Addresses.
- This is because two IP Addresses are wasted for each subnet.
- One IP address is wasted for its network address.
- Other IP Address is wasted for its direct broadcasting address.
- Subnetting leads to complicated communication process.

Subnet ID

- Each subnet has its unique network address known as its **Subnet ID**.
- The subnet ID is created by borrowing some bits from the Host ID part of the IP Address.
- The number of bits borrowed depends on the number of subnets created.

How to Calculate Subnet Mask?

For any given IP Address, the subnet mask is calculated-

- By setting all the bits reserved for network ID part and subnet ID part to 1.
- By setting all the bits reserved for host ID part to 0.

- Subnet Mask is used to determine to which subnet the given ip address belongs to.

Default mask for different classes of IP Address are-

- Default subnet mask for Class A = 255.0.0.0
- Default subnet mask for Class B = 255.255.0.0
- Default subnet mask for Class C = 255.255.255.0

Problems

In a class B, network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet? Number of subnet?

Suppose a network with IP Address 192.16.0.0. is divided into 2 subnets, find number of hosts per subnet.

Also for the first subnet, find-

1. Subnet Address
2. First Host ID
3. Last Host ID
4. Broadcast Address

Problems

If the subnet mask 255.255.255.128 belongs to class C, find-

1. Number of subnets
2. Number of hosts in each subnet

Problems

Consider the following routing table at an IP router

Network No.	Net Mask	Next Hop
128.96.170.0	255.255.254.0	Interface 0
128.96.168.0	255.255.254.0	Interface 1
128.96.166.0	255.255.254.0	R2
128.96.164.0	255.255.254.0	R3
0.0.0.0	Default	R4

For each IP address find out the next hop interface using the entries from the routing table above.

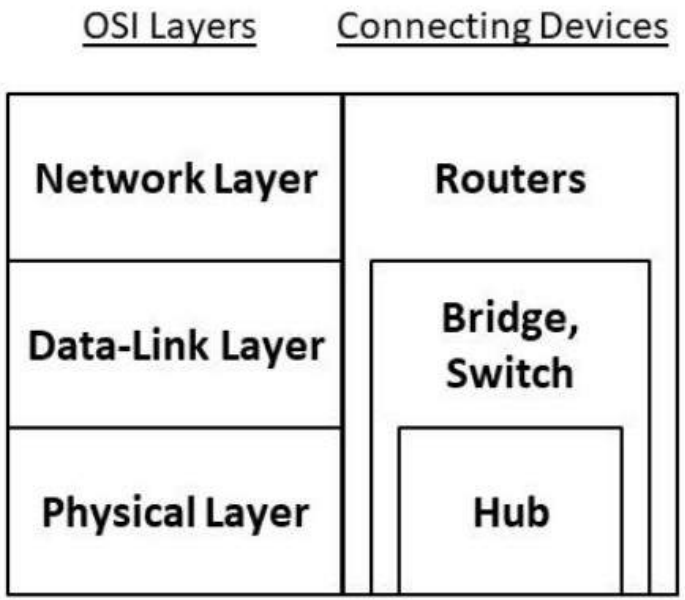
128.96.171.92 128.96.167.151

128.96.163.121 128.96.165.121

Networking Devices

Networking Devices

- Repeater
- Hub
- Bridge
- Switch
- Router



Repeater

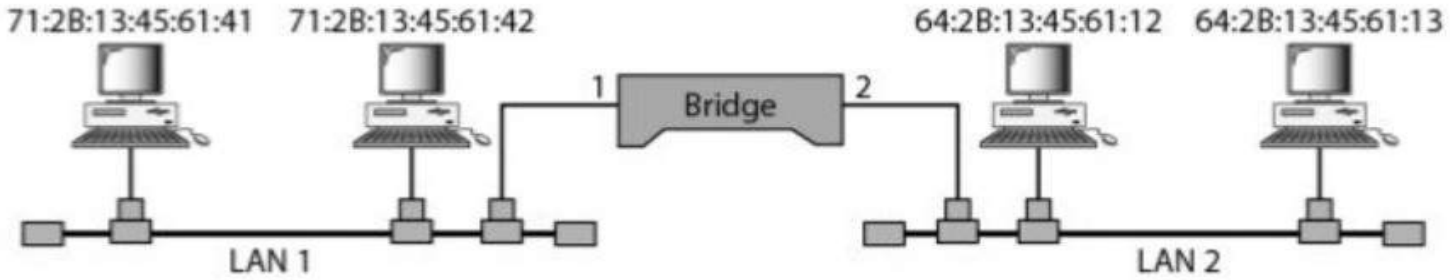
- A repeater operates at the physical layer.
- Repeater regenerate the signal over the same network before the signal becomes too weak or corrupted.
- so as to extend the length to which the signal can be transmitted over the same network.
- It is a 2 port device.

Hub

- It is also known as a **Multiport Repeater Device.**
- **A Hub is a layer-1 device and operates only in the physical network of the OSI Model.**
- It can connect devices of the same network only.
- A Hub is not an intelligent device.
- It does not maintain any address table for connected devices.
- a hub broadcasts the incoming data packets in the network
- It is less secure, as it broadcasts the data packet

Bridge

- A bridge is a layer-2 network connecting device, i.e., it works on the physical and data-link layer of the OSI model.
- A bridge connects the devices which are present in the same network. It is mainly used to segment a network to allow a large network size.
- It has two types of port - incoming and outgoing.
- A Bridge has filtering capacity.
- Improves security by limiting the scope of data frames.



Switch

- A switch acts as a multiport bridge in the network.
- **A switch is a layer-2 network connecting device, i.e., it works on the physical and data-link layer of the OSI model.**
- A switch maintains a Switch table which has the MAC addresses of all the devices connected to it.
- A Switch is an intelligent device with filtering capabilities

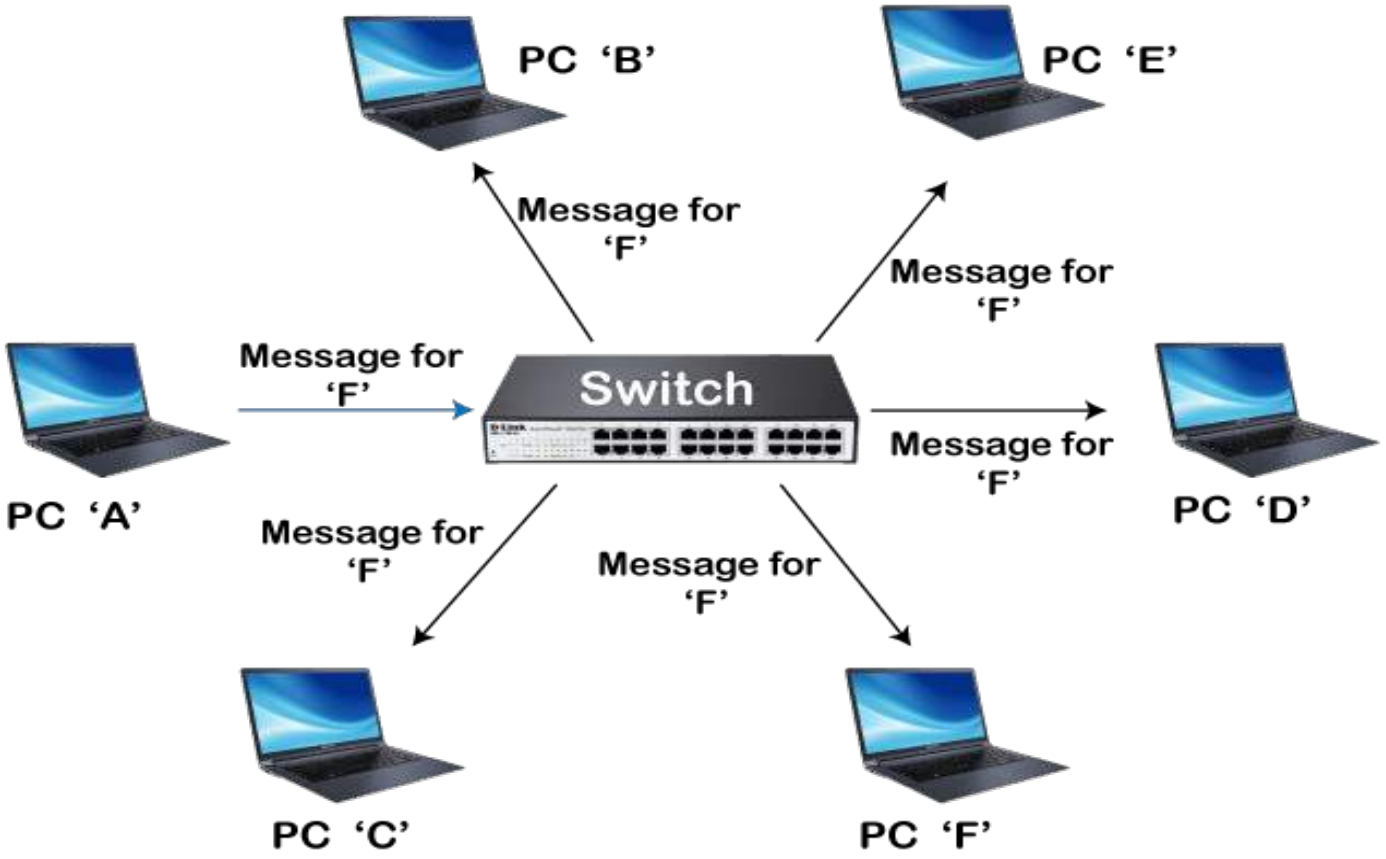
Switch

- A switch is a multicast networking device that works under the Datalink layer of the OSI model and connects a bunch of computers or devices in a network.

- a switch acts as the central interconnecting device that connects all the devices of a network in order to ensure proper resource sharing.

- Basically, in a network, all the end devices like a computer printer, servers, etc. are connected through the switch

Switch


PC 'B'
PC 'E'
Message for 'F'
Message for 'F'
Message for 'F'
Switch
Message for 'F'
PC 'A'
PC 'D'
Message for 'F'
Message for 'F'
PC 'C'
PC 'F'

Router

A Router is a networking device that operates under the network layer of the OSI model and is used to connect two or more networks.

A router is a device that is used to interconnect various switches of different networks to form even a wider network.

A Router is a layer-3 network connecting device, i.e., it works on the physical, data-link and network layer of the OSI model.

A router maintains a routing table using the routing algorithms

Switch & Router

Switch works on the data link layer of the OSI model.

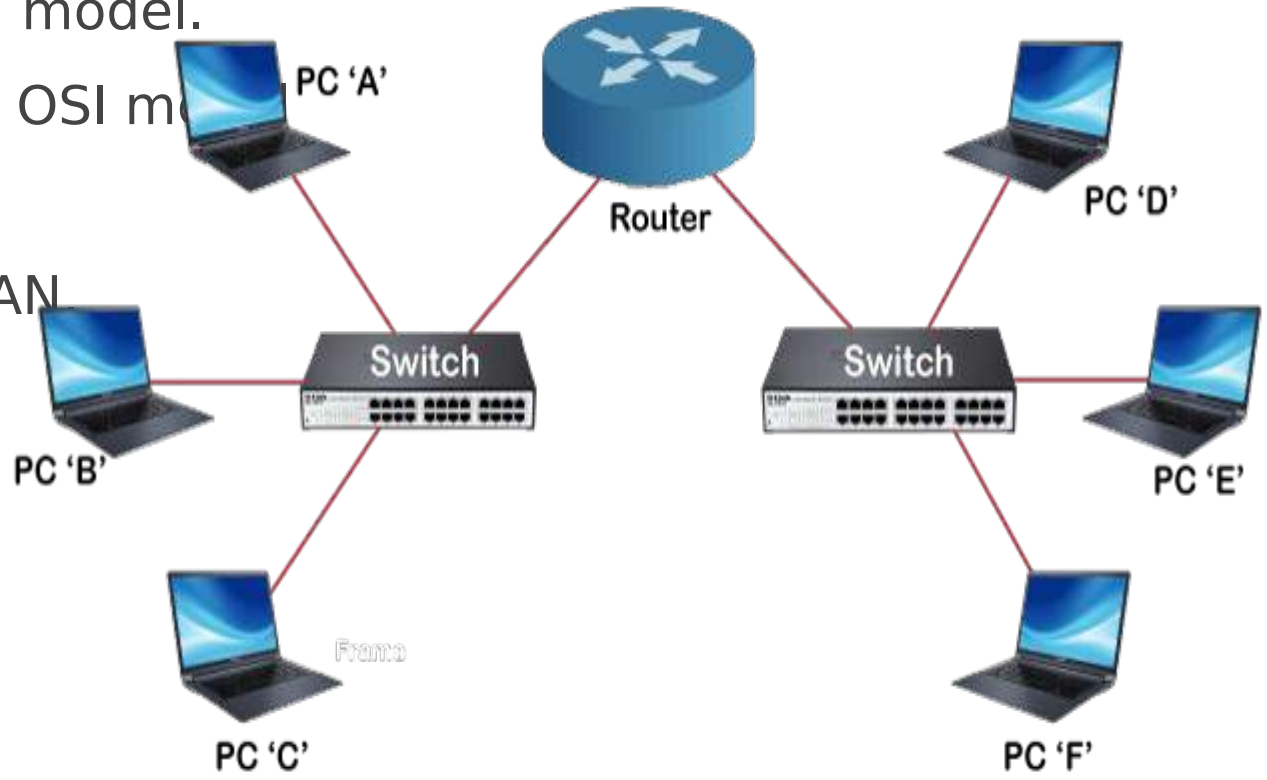
The Router works on the network layer of the OSI m

Switch can join multiple devices within one LAN

A Router can link both LAN as well as WAN.

Switch works based on the MAC address,

Router works based on IP address.



Connection of networks through Router

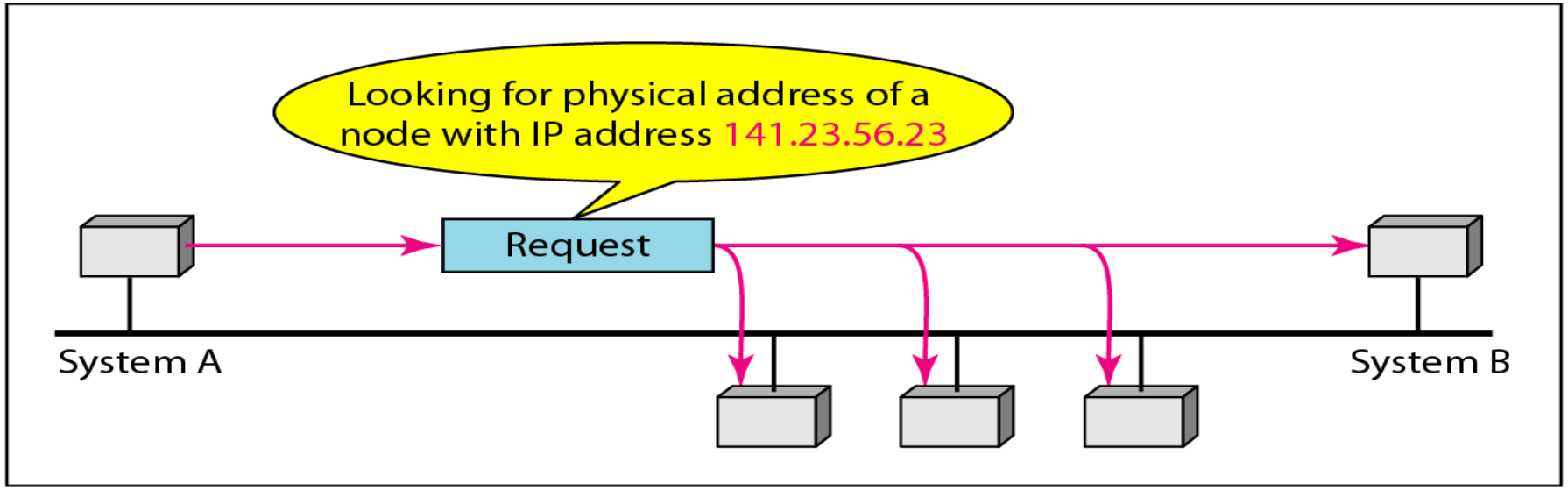
PROTOCOL

ARP AND RARP

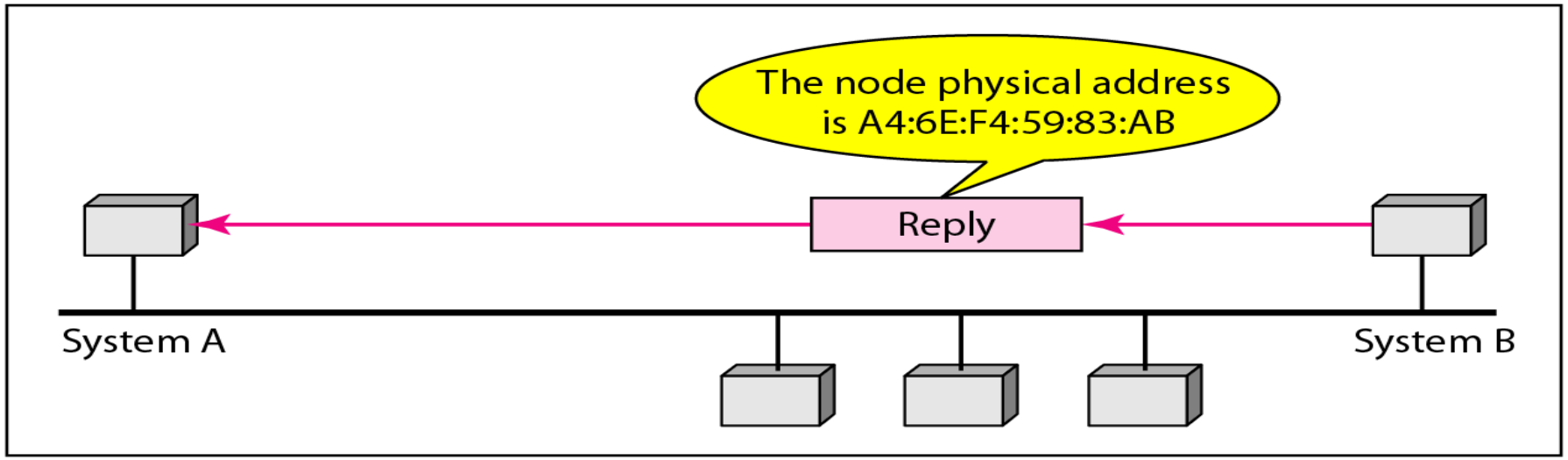
The basic difference between ARP and RARP is that

ARP when provided with the logical address of the receiver it obtains the physical address of the receiver whereas in

RARP when provided with the physical address of the host, it obtains the logical address of the host from the server.



a. ARP request is broadcast



b. ARP reply is unicast

BASIS FOR COMPARISON	ARP	RARP
Full Form	Address Resolution Protocol.	Reverse Address Resolution Protocol.
Basic	Retrieves the physical address of the receiver.	Retrieves the logical address for a computer from the server.
Mapping	ARP maps 32-bit logical (IP) address to 48-bit physical address.	RARP maps 48-bit physical address to 32-bit logical (IP) address.

ICMP

ICMP or Internet Control Message Protocol is one of the major protocols of the TCP/IP.

ICMP is a mechanism used by the host, routers, and gateways to send error messages back to the sender.

As the IP does not provide any mechanism for error reporting and control, ICMP has been designed to compensate for these deficiencies of the IP.

However, it only reports the error and doesn't correct the error.

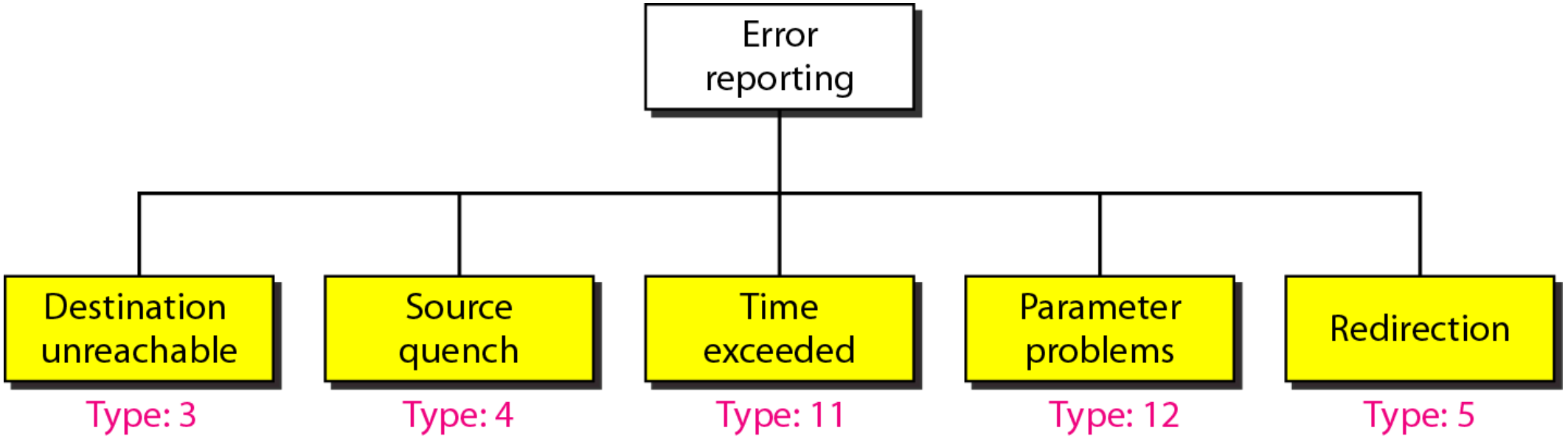
ICMP

When you are not connected to the internet and search for any website then you get an error message like destination unreachable or time limit exceeded etc.

These messages are displayed through the ICMP protocol.

The IP protocol does not have any mechanism for error reporting and sending query messages. This problem is resolved by the ICMP protocol.

Error-reporting messages



IGMP

The IP protocol can be involved in two types of communication:

unicasting and multicasting.

The Internet Group Management Protocol (IGMP) is one of the necessary protocols that is involved in multicasting.

Online streaming of videos and games generally uses the IGMP protocol for more efficient use of the resources. I

DNS

DNS

Domain Name System is a Protocol which translate from Domain Name to IP.

Where is DNS?

DNS Cache

Browser

Router

ISP

Next ISP…etc

Where is DNS Record in Browser?

Google DNS?

How the Domain Name System (DNS) Works

How DNS Work

https://www.verisign.com/en_IN/website-presence/online/how-dns-works/index.xhtml#:~:text=DNS%20syncs%20up%20domain%20names,internet%20can%20use%20IP%20addresses.&text=In%20fact%2C%20Verisign%20processes%20more,the%20internet%20fast%20and%20reliable.

https://www.iana.org/

https://root-servers.org/

https://www.iana.org/domains/root/servers

https://www.netnod.se/dns/dns-root-server-faq

The 8 steps in a DNS lookup

1. A user types ‘example.com’ into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:

1. The browser makes a HTTP request to the IP address.
2. The server at that IP returns the webpage to be rendered in the browser.

What are the root servers?

Does the root zone contain all the DNS data?

Does all Internet traffic go through the root servers?

Who are the root server operators?

Is it true that there are only 13 root servers?

A is the most important root server, isn't it?

There are 4 DNS servers involved in loading a webpage:

DNS recursor

Root Server

TLD Server

Authoritative Server

DNS Recursor

The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers.

Root Server

The root servers are the entry points to the Domain Name System (DNS), It contains the root zone, which contains information about what Top Level Domains (TLDs) exist, and the addresses of the each TLD.

TLD Server

It hosts the second level domains of a hostname (example.com, within the TLD “.com”).

Authoritative Server

It will return the IP address for the requested hostname back to the DNS Recursor

DNS Poisoning

When unauthorized domain names or IP add are inserted into it.

DNS Cache may become corrupted

Wireshark

Wireshark is a free and open-source packet analyzer.

It is used for traffic monitor and network troubleshooting and analysis.

It captures network traffic on the local network and stores that data for offline analysis

Purposes

Network administrators use it to *troubleshoot network problems*

Network security engineers use it to *examine security problems*

QA engineers use it to *verify network applications*

Developers use it to *debug protocol implementations*

People use it to *learn network protocol* internals

Feature

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solarisand many others
- Captured network data can be browsed via a GUI
- The most powerful display filters in the industry
- Coloring rules can be applied to the packet list for quick, intuitive analysis

Wireshark Filters

Filters allow you to view the capture the way you need to see it so you can troubleshoot the issues

Wireshark Capture Filters

Capture filters limit the captured packets by the filter. Meaning if the packets don’t match the filter, Wireshark won’t save them.

Ex:

host IP-*address*: this filter limits the capture to traffic to and from the IP address

Wireshark Display Filters

Wireshark Display Filters change the view of the capture during analysis. After you have stopped the packet capture, you use display filters to narrow down the packets in the Packet List so you can troubleshoot your issue.

Ex:

ip.src==*IP-address* and ip.dst==*IP-address*

Wireshark Promiscuous Mode

By default, Wireshark only captures packets going to and from the computer where it runs.

By checking the box to run Wireshark in Promiscuous Mode in the Capture Settings, you can capture most of the traffic on the LAN.

What Wireshark is not

Here are some things Wireshark does not provide:

Wireshark isn’t an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn’t send packets on the network or do other active things.

Wireshark Is A Safe Tool Used By:
Government agencies
Educational institutions
Corporations
Small businesses
Non-profits
VARONIS

More Info

https://www.wireshark.org/docs/wsug_html_chunked/index.html

https://www.wireshark.org/faq.html

Sniff Login details from Webpages

Http Protocol (GET AND POST)

Https Protocol

FTP

SSH

http.request.method==“GET“

http.request.method=="POST"

FTP

Downloads the Sample

https://wiki.wireshark.org/SampleCaptures