# Computer Network And Network Design(CNND)
# ITC402


**Subject Incharge**

Ms. Jesleena Gonsalves

Assistant Professor

Room No. 326

email: jesleenagonsalves@sfit.ac.in


**Whatsapp Group Invite Link -**

# Module 2

# Physical Layer & Data Link Layer

# Outline

**Physical layer**

- Guided Media and Unguided Media
- Wireless Transmission: Electromagnetic Spectrum.
- Switching: Circuit-Switched Networks, Packet Switching, Structure Of A Switch

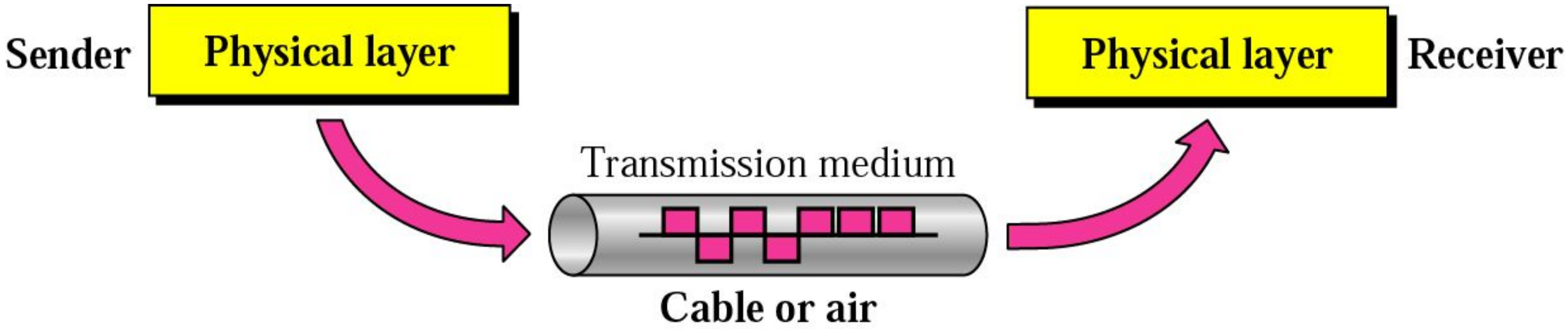
**Data Link Layer**

- DLL Design Issues (Services, Framing, Error Control, Flow Control)
- Error Detection and Correction(Hamming Code , Parity, CRC, Checksum)
- Elementary Data Link protocols : Stop and Wait, Sliding Window(Go Back N, Selective Repeat), Piggybacking, HDLC
- Medium Access Protocols: Random Access, Controlled Access, Channelization.
- Ethernet Protocol: Standard Ethernet, Fast Ethernet (100 Mbps), Gigabit Ethernet, 10-Gigabit Ethernet.

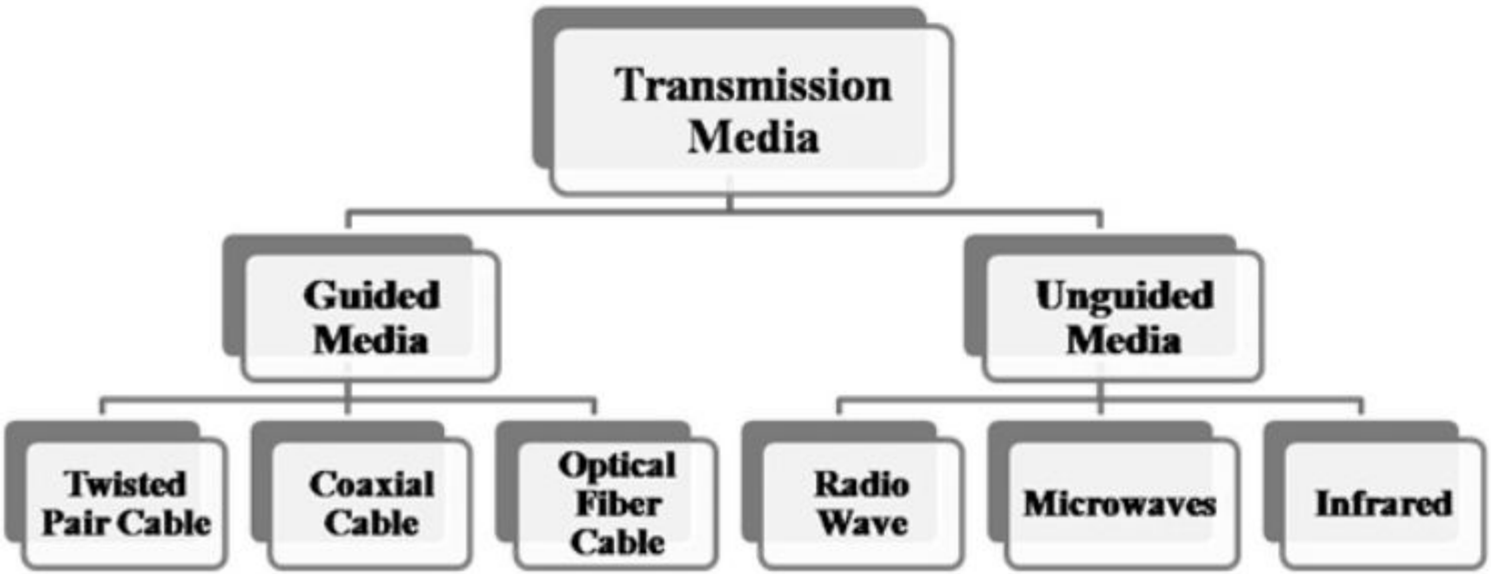
# Physical Layer

# TRANSMISSION MEDIA

- Transmission medium can be defined as anything that can carry information from a source to a destination.



# TRANSMISSION MEDIA

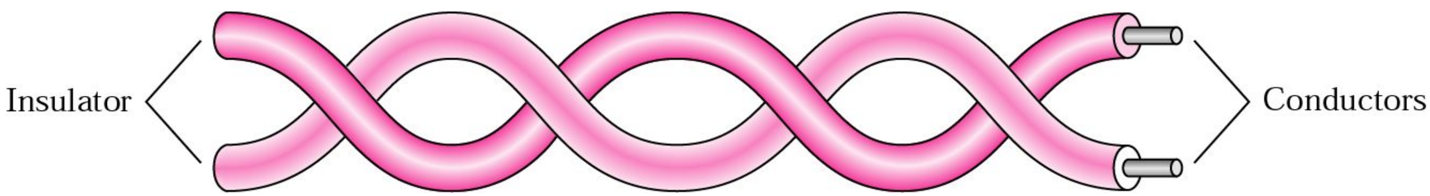


# GUIDED MEDIA

A signal traveling along guided media is directed and contained by the physical limits of the medium.

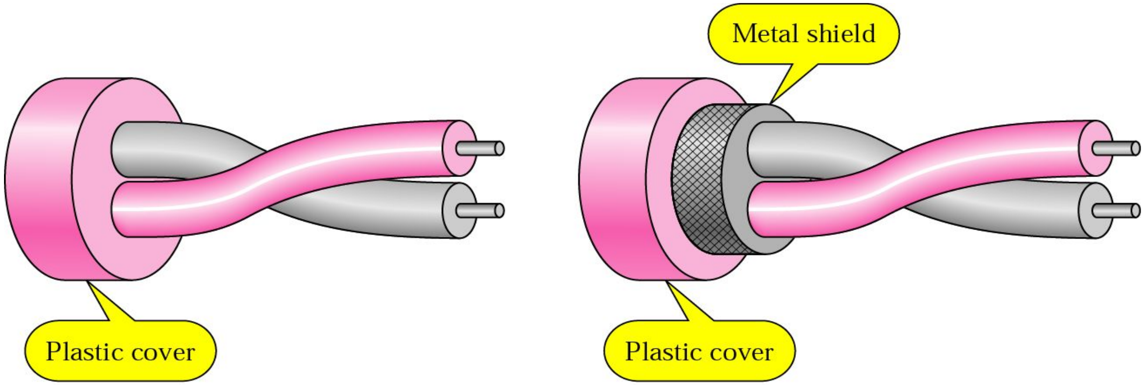
**Twisted-pair cable**

- A twisted pair consists of two insulated copper wires in a regular spiral pattern.
- One of the wires is used to carry signals to the receiver and the other is used only as a ground reference.



# GUIDED MEDIA

## Unshielded versus Shielded Twisted-pair cable




a. UTP b. STP

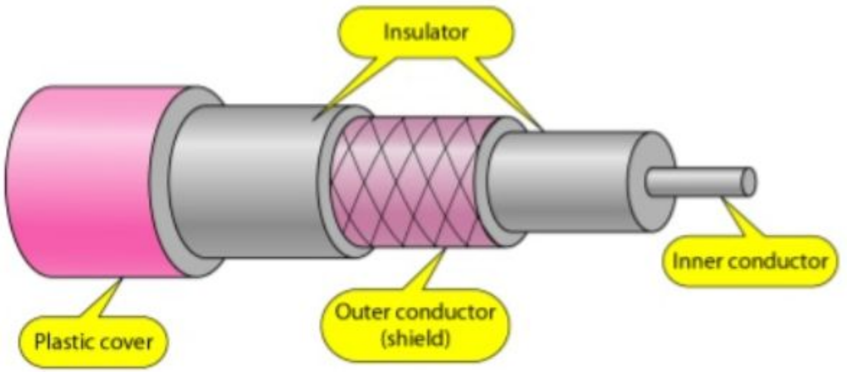
## Applications

- Twisted-pair cables are used in telephone lines to provide voice and data channels.
- 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.
- Local-area networks, such as lOBase-T and lOOBase-T, also use twisted-pair cables.

# GUIDED MEDIA

## Co-axial cable

- It carries signals of higher frequency ranges than those in twisted pair cable.




## Coaxial Cable Standards

- Coaxial cables are categorized by their radio government (RG) ratings.

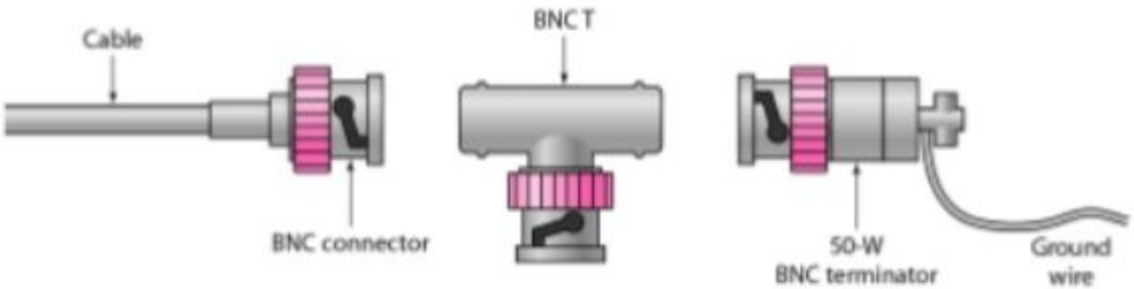
**Table 7.2** ***Categories of coaxial cables***

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

# GUIDED MEDIA

**Coaxial Cable Connectors**

- To connect coaxial cable to devices , coaxial connectors are needed such as Bayonet Neill- Concelman (BNC)




**Applications**

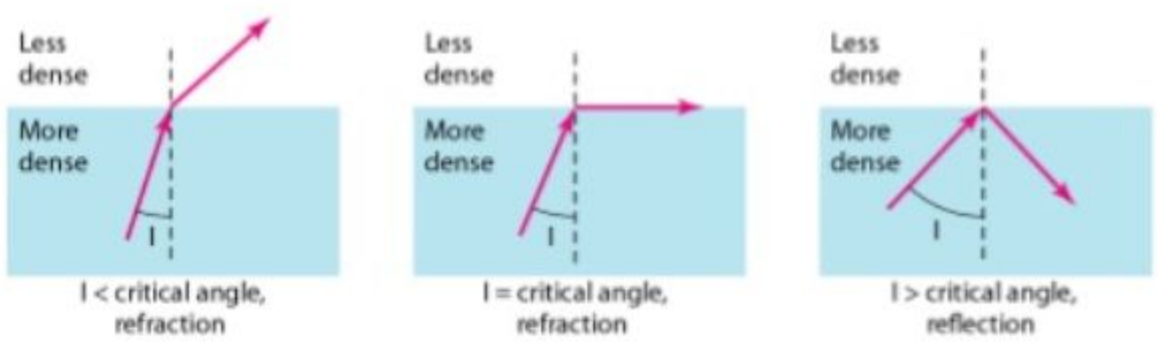
- Coaxial cable was widely used in analog telephone networks . Later it was used in digital telephone networks.
- Cable TV networks also use coaxial cables
- Used in traditional Ethernet LANs .

# GUIDED MEDIA

**Fiber-Optic Cable:**

- It is made of glass or plastic and transmits signals in the form of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light travelling through one substance suddenly enters another substance , the ray changes direction

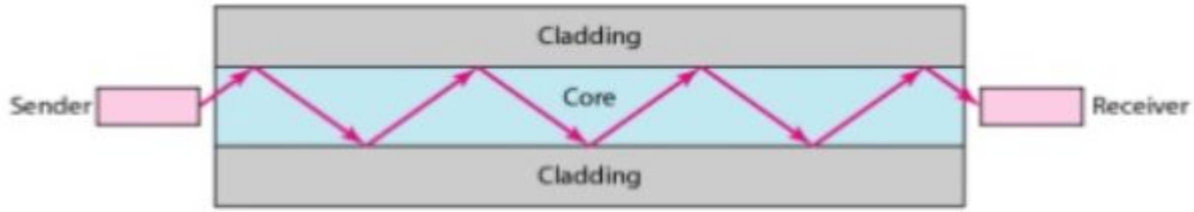
Figure 7.10 *Bending of light ray*



# GUIDED MEDIA

- Optical fiber use reflection to guide light through a channel .
- 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 7.11** ***Optical fiber***

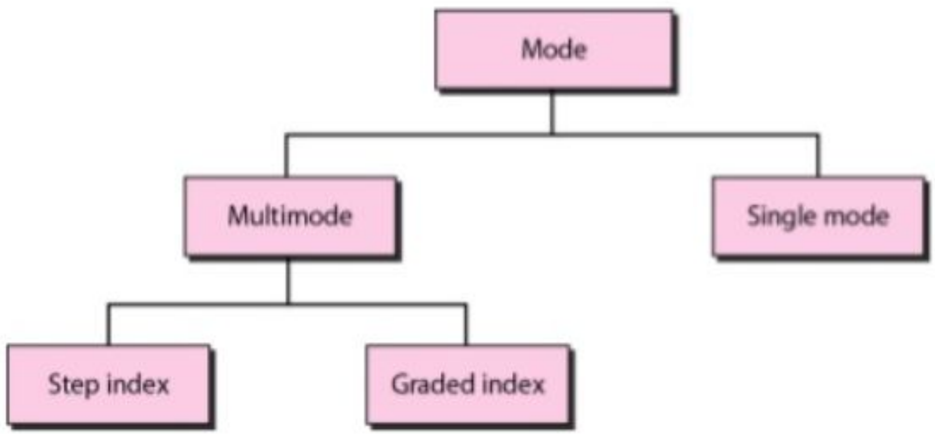


# GUIDED MEDIA

## Propagation Modes

- Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics.

Figure 7.12 *Propagation modes*



# GUIDED MEDIA

## Fiber Sizes

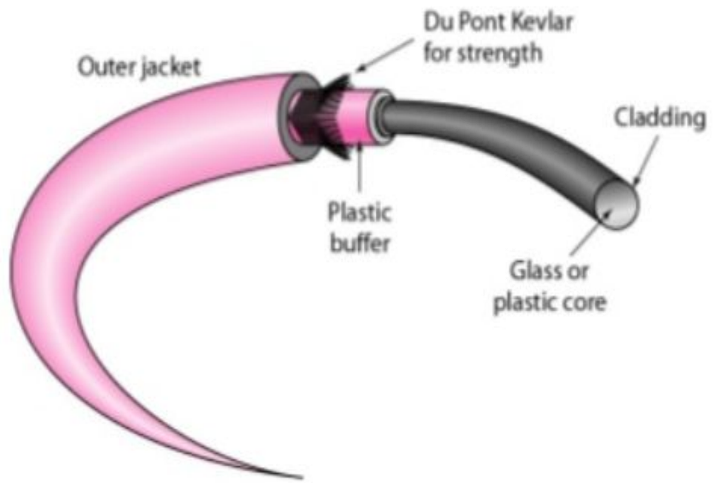
- Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers.

Table 7.3 *Fiber types*

| *Type* | *Core (μm)* | *Cladding (μm)* | *Mode* |
|---|---|---|---|
| 501125 | 50.0 | 125 | Multimode, graded index |
| 62.51125 | 62.5 | 125 | Multimode, graded index |
| 100/125 | 100.0 | 125 | Multimode, graded index |
| 7/125 | 7.0 | 125 | Single mode |

# GUIDED MEDIA

**Figure 7.14** ***Fiber construction***




**Applications**

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective.
- 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.

# GUIDED MEDIA

**Advantages of Optical Fiber:**

- Higher Bandwidth
- Less Signal Attenuation
- Immunity to Electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

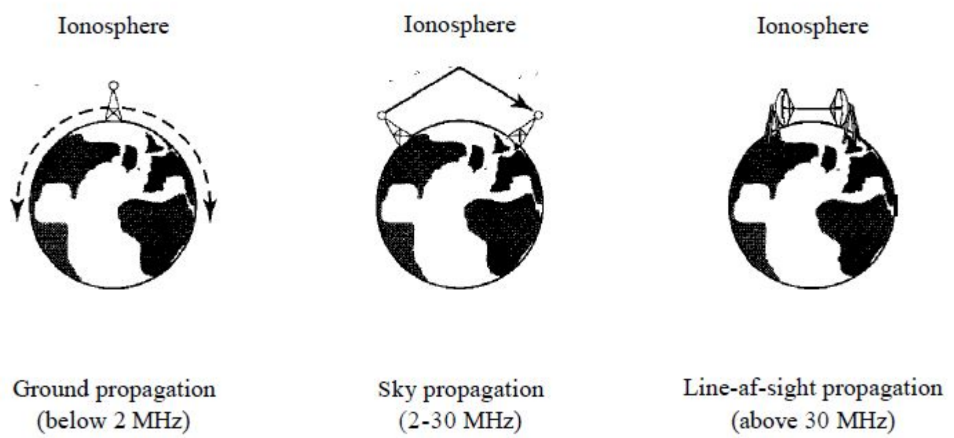
**Disadvantages of Optical Fiber:**

- Installation and Maintenance
- Unidirectional light propagation
- Cost

# UNGUIDED MEDIA

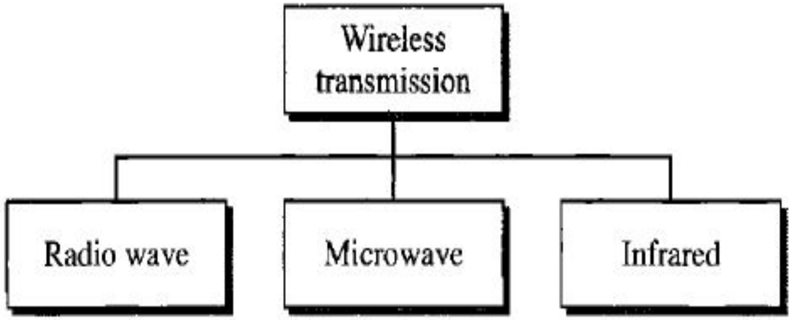
- Unguided medium transport electromagnetic waves without using a physical conductor.
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
- Unguided signals can travel from the source to the destination in several ways: Ground propagation, sky propagation and line of sight propagation.

**Figure 7.18** *Propagation methods*



# UNGUIDED MEDIA

Figure 7.19 *Wireless transmission waves*



# UNGUIDED MEDIA

**Radio Waves:**

- Electromagnetic waves ranging in frequencies between 3kHz and 1 GHz are called radio waves.
- When an antenna transmits radio waves, they are propagated in all directions.
- Radio waves, particularly those waves that propagate in the sky mode, can travel long distances.
- Radio waves of low and medium frequencies , can penetrate walls.
- Radio waves are used for multicast communications, such as radio and television, and paging systems

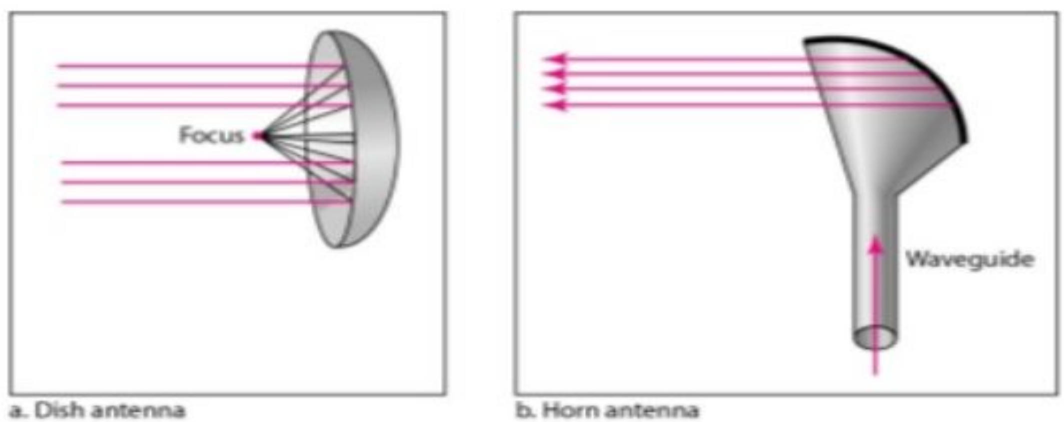
**Figure 7.20** *Omnidirectional antenna*

# UNGUIDED MEDIA

**Microwaves:**

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional.
- Microwave propagation is line of sight.
- Very high frequency microwave cannot penetrate walls.
- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

**Figure 7.21** *Unidirectional antennas*



# UNGUIDED MEDIA

**Infrared:**

- Infrared waves with frequencies from 300 GHz to 400 GHz, can be used for short range communication.
- Infrared waves, having high frequencies cannot penetrate walls.
- Infrared signals can be used for short range communication in a closed area using line of sight propagation.

# UNGUIDED MEDIA

## The Electromagnetic Spectrum

- When electrons move, they create electromagnetic waves that can propagate through space (even in a vacuum).
- The number of oscillations per second of a wave is called its frequency, f, and is measured in Hz.
- The distance between two consecutive maxima (or minima) is called the wavelength, which is universally designated by the Greek letter λ (lambda).
- When an antenna of the appropriate size is attached to an electrical circuit, the electromagnetic waves can be broadcast efficiently and received by a receiver some distance away. All wireless communication is based on this principle.
- In a vacuum, all electromagnetic waves travel at the same speed, no matter what their frequency. This speed, usually called the speed of light, c, is approximately 3 × 108 m/sec.
- The speed of light is the ultimate speed limit. No object or signal can ever move faster than it.
- The fundamental relation between f, λ, and c (in a vacuum) is

$$\lambda f = c$$

- The amount of information that a signal such as an electromagnetic wave can carry depends on the received power and is proportional to its bandwidth.

# UNGUIDED MEDIA

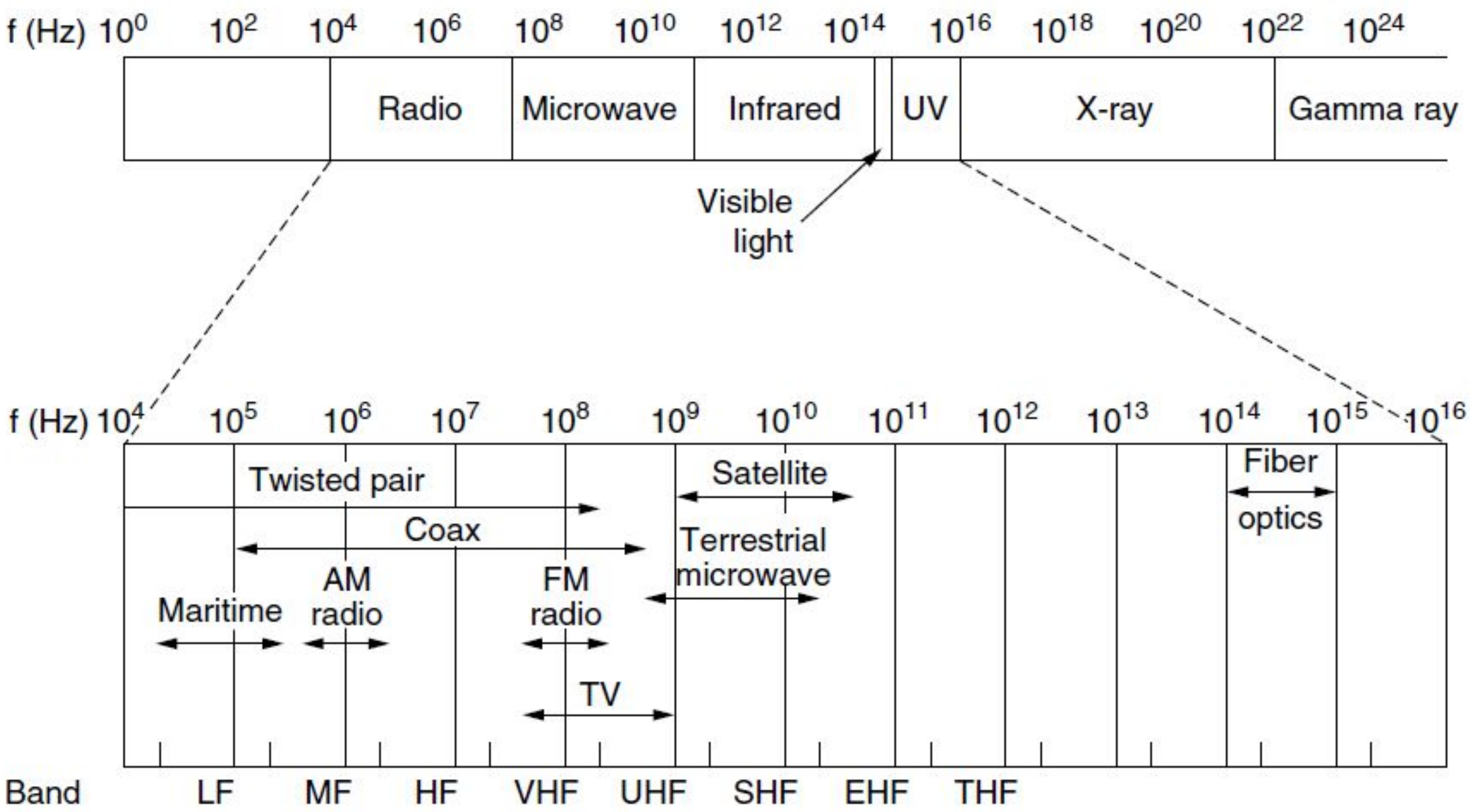



**Figure 2-10.** The electromagnetic spectrum and its uses for communication.

# SWITCHING

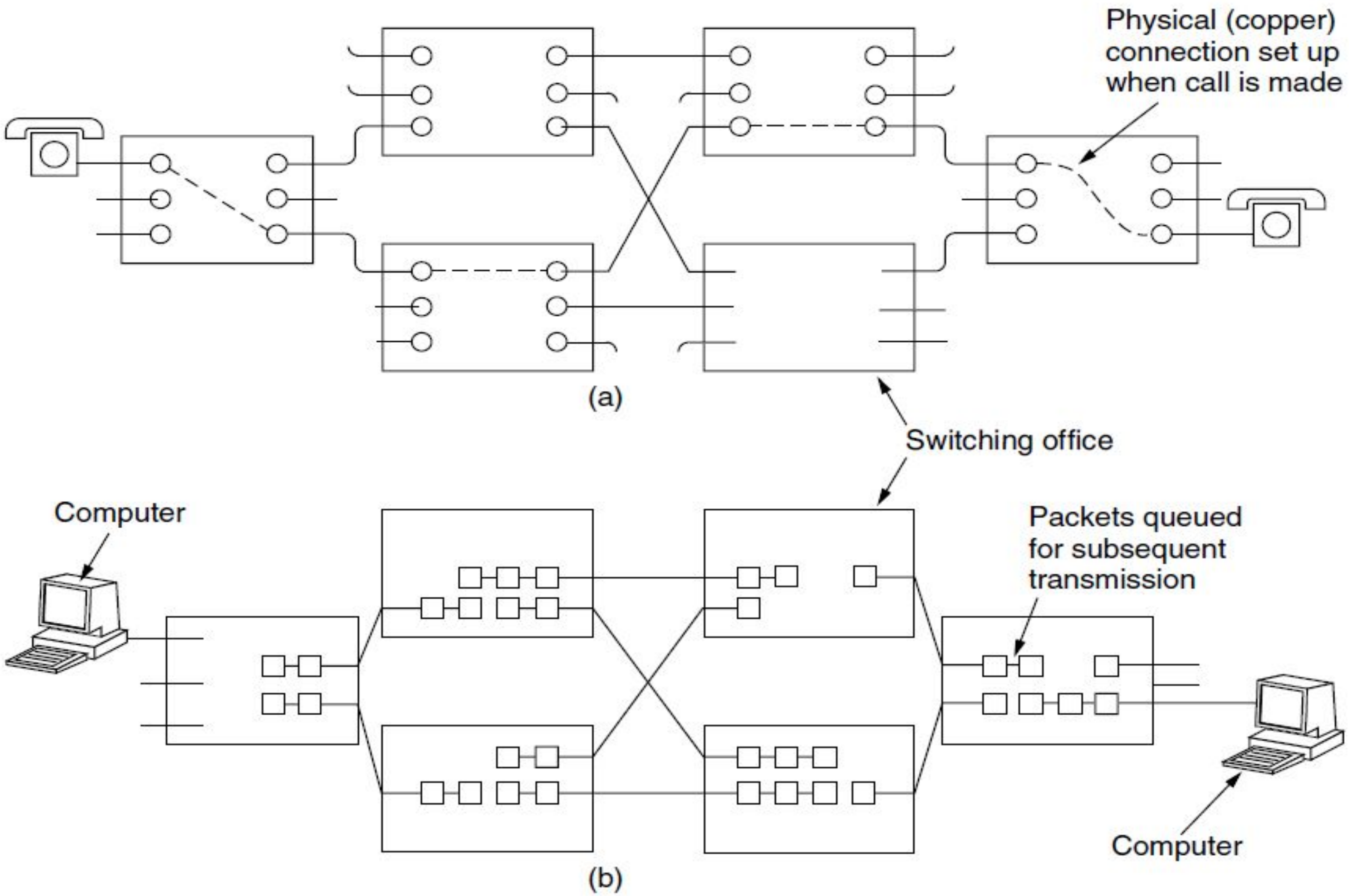



**Figure 2-42.** (a) Circuit switching. (b) Packet switching.

# SWITCHING

**Circuit Switching:**

- 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..
- Data transferred between the two stations are not packetized .
- There is no addressing involved during data transfer.

- The actual communication in a circuit-switched network requires three phases:

1. Connection setup
2. Data transfer
3. Connection teardown.

# SWITCHING

**Packet Switching**

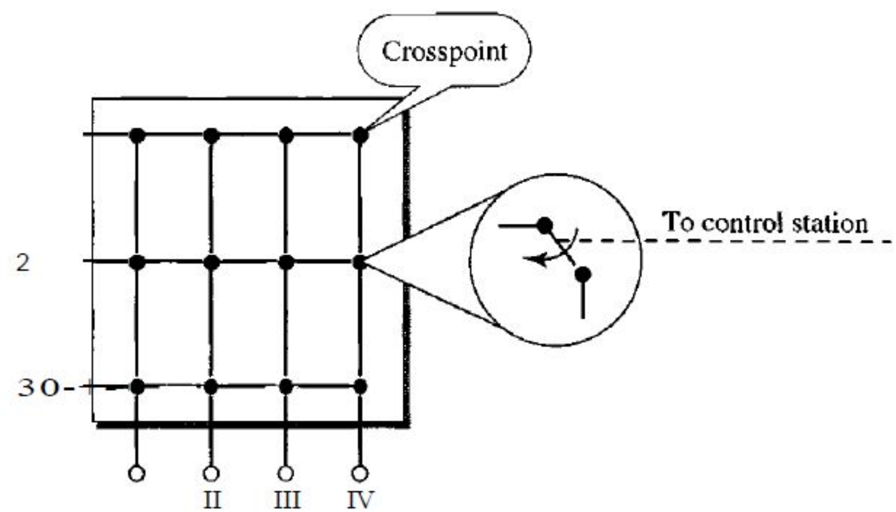
- In packet switching, there is no resource allocation for a packet. Resources are allocated on demand.
- Because no bandwidth is reserved with packet switching, packets may have to wait to be forwarded ,this introduces **queuing delay.**

# STRUCTURE OF A CIRCUIT SWITCH

Circuit switching today can use either of two technologies:

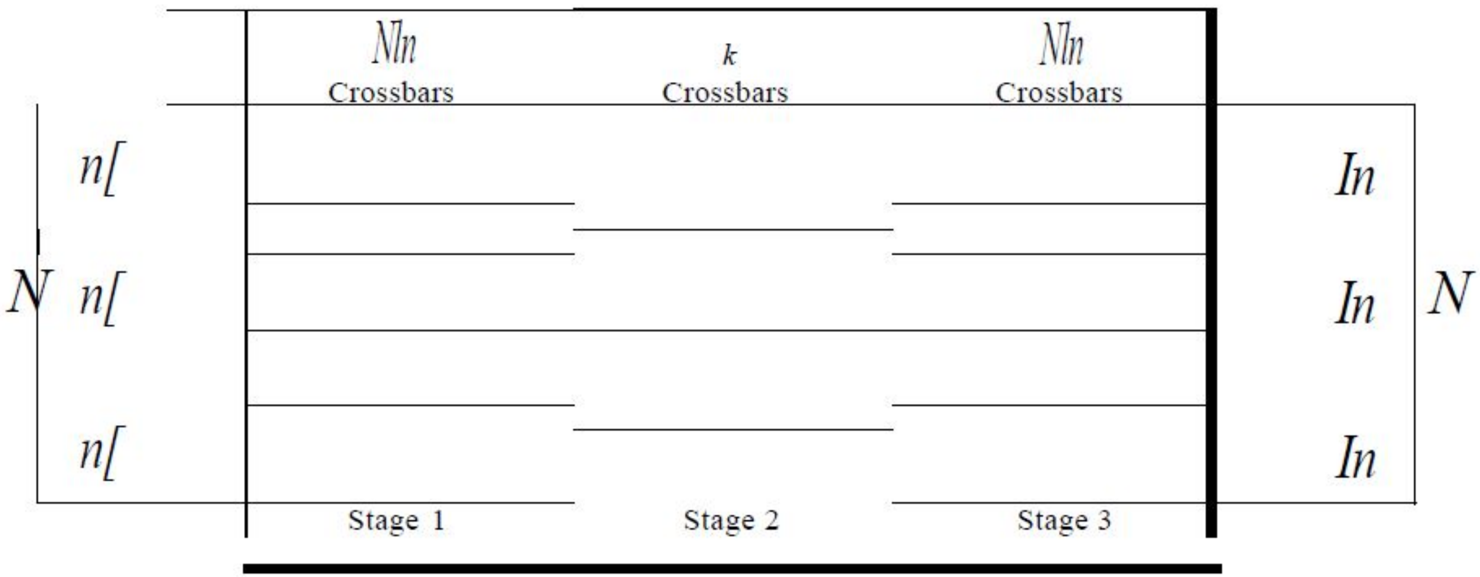
1. The space-division switch
   a. Crossbar Switch
   b. Multistage switch
2. The time-division switch.

Figure 8.17 *Crossbar switch with three inputs and four outputs*



# STRUCTURE OF A CIRCUIT SWITCH

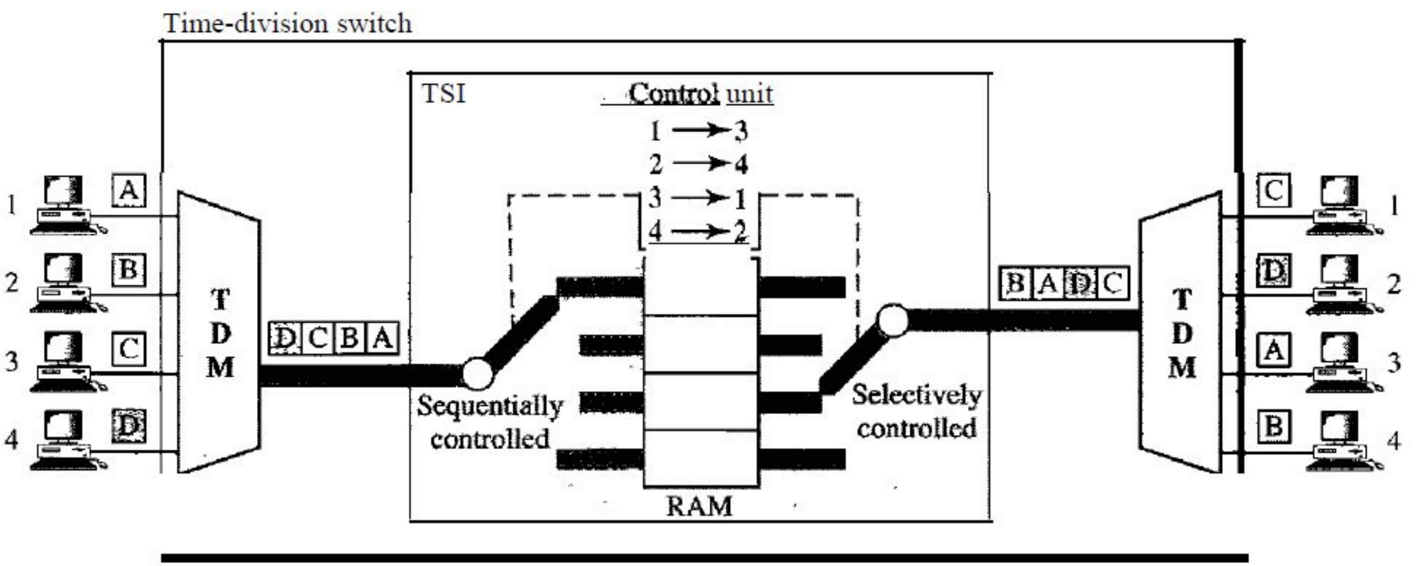
Figure 8.18 *Multistage switch*



# STRUCTURE OF A CIRCUIT SWITCH

**The Time division switch**

Figure 8.19 *Time-slot interchange*

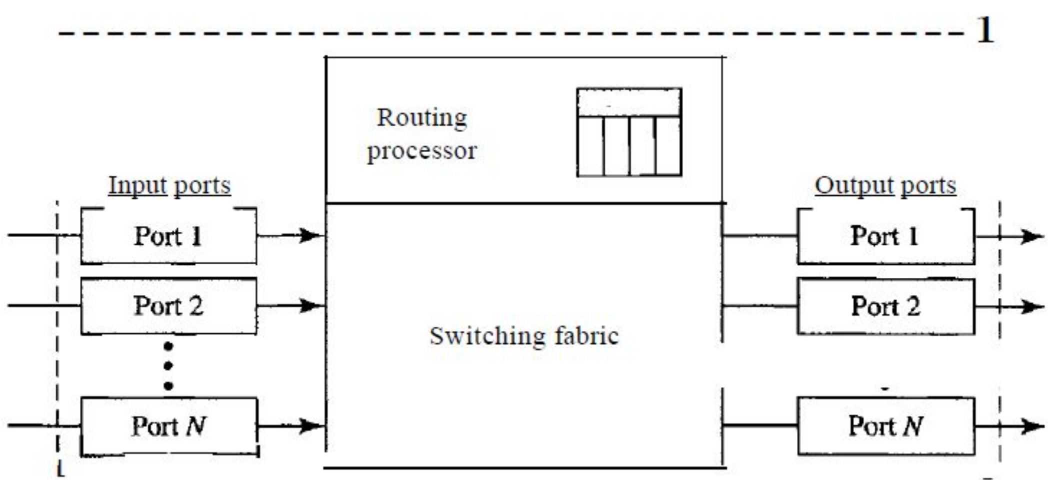


# STRUCTURE OF A PACKET SWITCH

A packet switch has four components:

1. Input ports
2. Output ports
3. The routing processor
4. Switching fabric

Figure 8.21 *Packet switch components*



# Data Link Layer

# DATA LINK LAYER

- The data link layer uses the services of the physical layer to send and receive bits over communication channels. It has a number of functions, including:

1. Providing a well-defined service interface to the network layer.
2. Dealing with transmission errors.
3. Regulating the flow of data so that slow receivers are not swamped by fast senders.

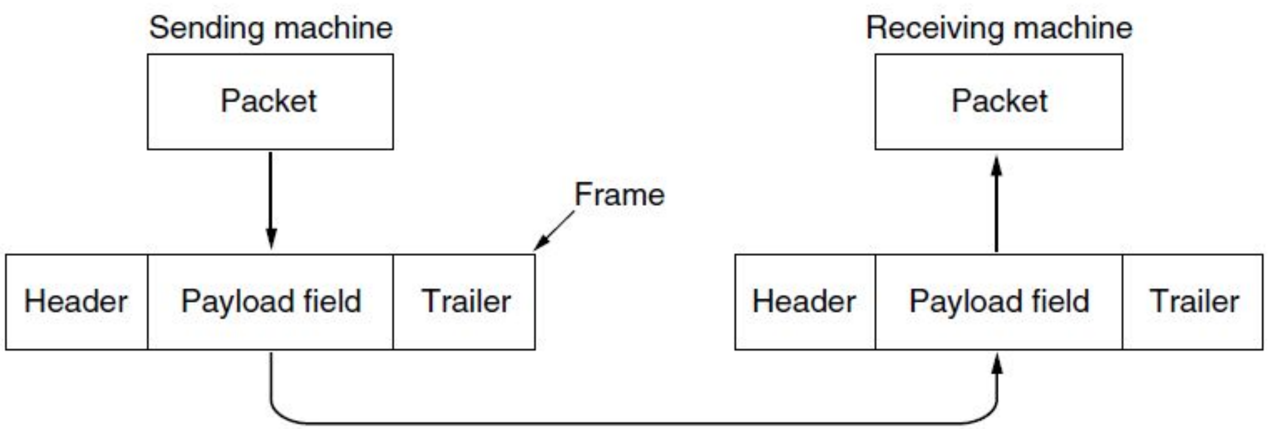



**Figure 3-1.** Relationship between packets and frames.

# DLL DESIGN ISSUES

1. Services provided to the network layer
2. Framing
3. Error Control
4. Flow control

# SERVICES PROVIDED TO THE NETWORK LAYER

- The function of the data link layer is to provide services to the network layer.
- The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine.
- The data link layer can be designed to offer various services. Three reasonable possibilities that we will consider in turn are:

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection-oriented service.

# FRAMING

- The data link layer needs to pack bits into frames, to distinguish one frame from another.
- Frames can be fixed or variable size.

**Fixed Size framing:**

- No need of frame delimiter
- The size defines the frame boundary
- E.g. – ATM Wide Area Network

**Variable Size Framing**

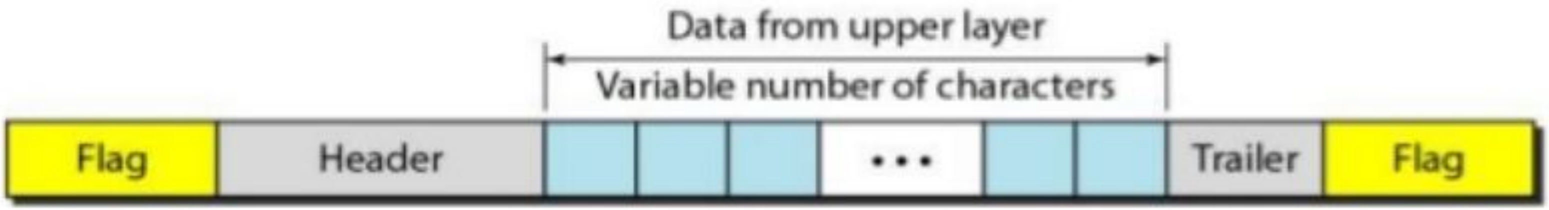
- Need to define start and end of the frame
- Two approaches are used

1. Character - Oriented Protocols
2. Bit – Oriented Protocols

# FRAMING

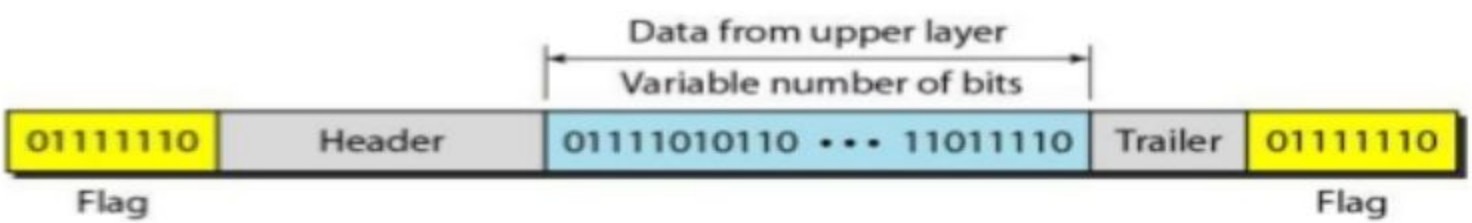
**Character – oriented protocol**

- Data as well as header, control information, trailer are all 8 bit characters.
- Use 8-bit flag at beginning and at end for frame separation.



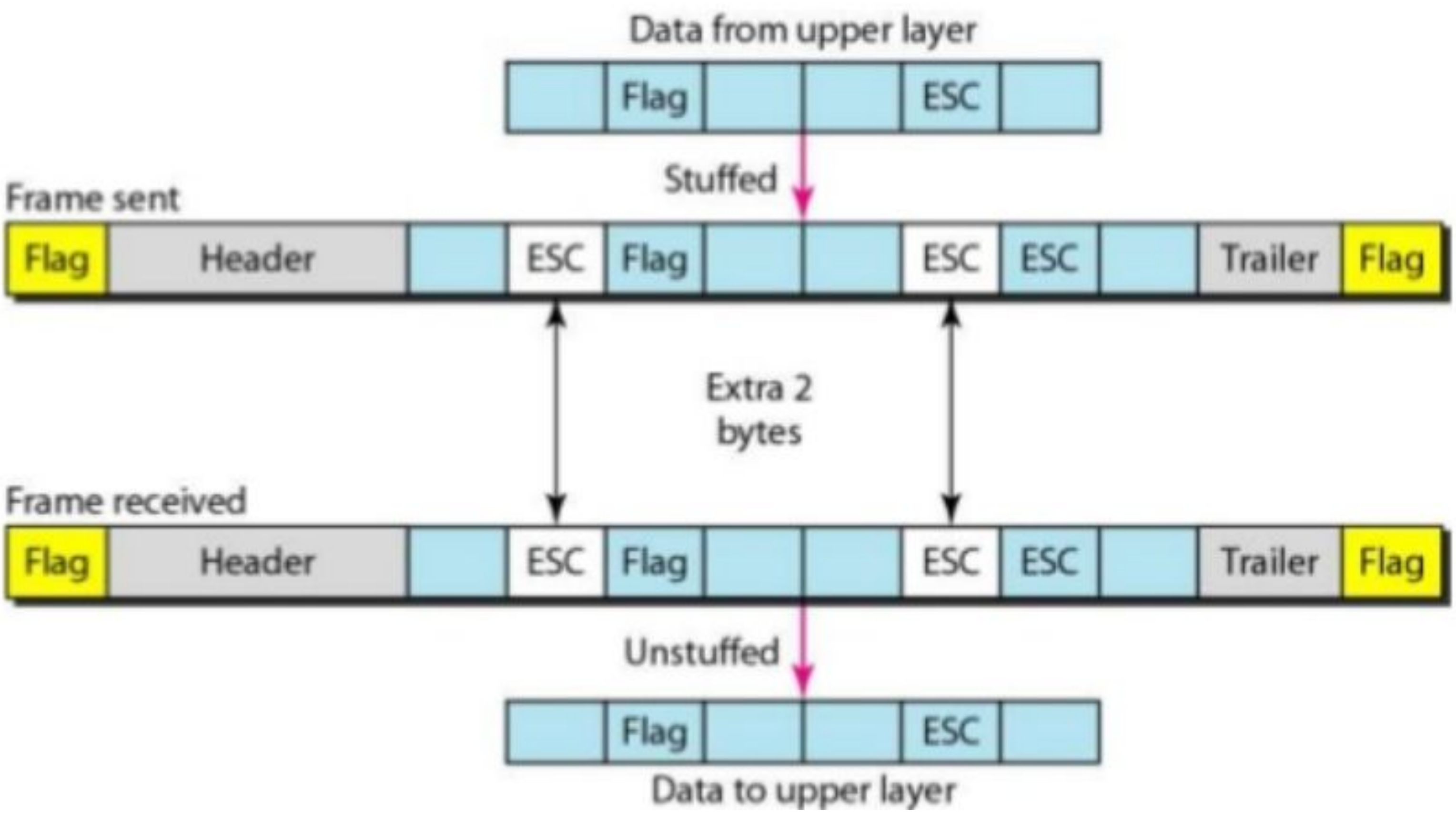

**Bit – oriented protocol**

- The data section of a frame is a sequence of bits.
- Delimiters are required for frame separation.
- Most protocols use a special 8 bit pattern flag '01111110' as delimiter



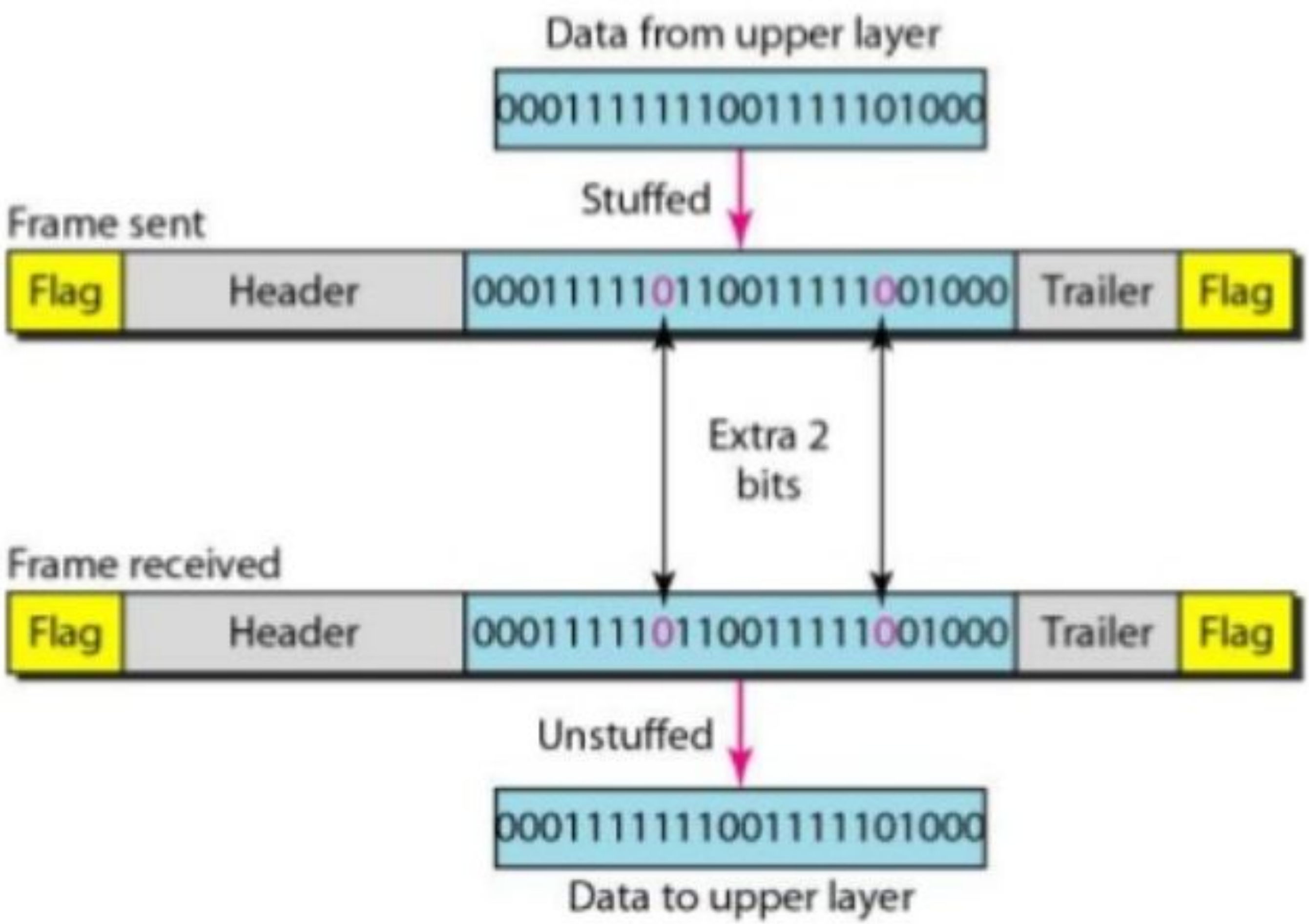
# FRAMING

Byte Stuffing and Unstuffing



# FRAMING

Bit Stuffing and Unstuffing



# ERROR CONTROL

- The whole issue of managing the timers and sequence numbers so as to ensure that each frame is ultimately passed to the network layer at the destination exactly once, no more and no less, is an important part of the duties of the data link layer.

# FLOW CONTROL

- Two approaches are commonly used:

1. Feedback-based flow control
2. Rate-based flow control

# Error Detection and Correction

# TYPES OF ERRORS

**Figure 10.1** *Single-bit error*

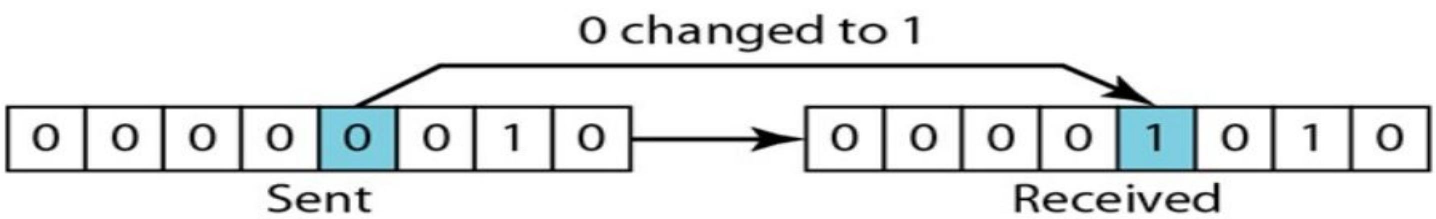
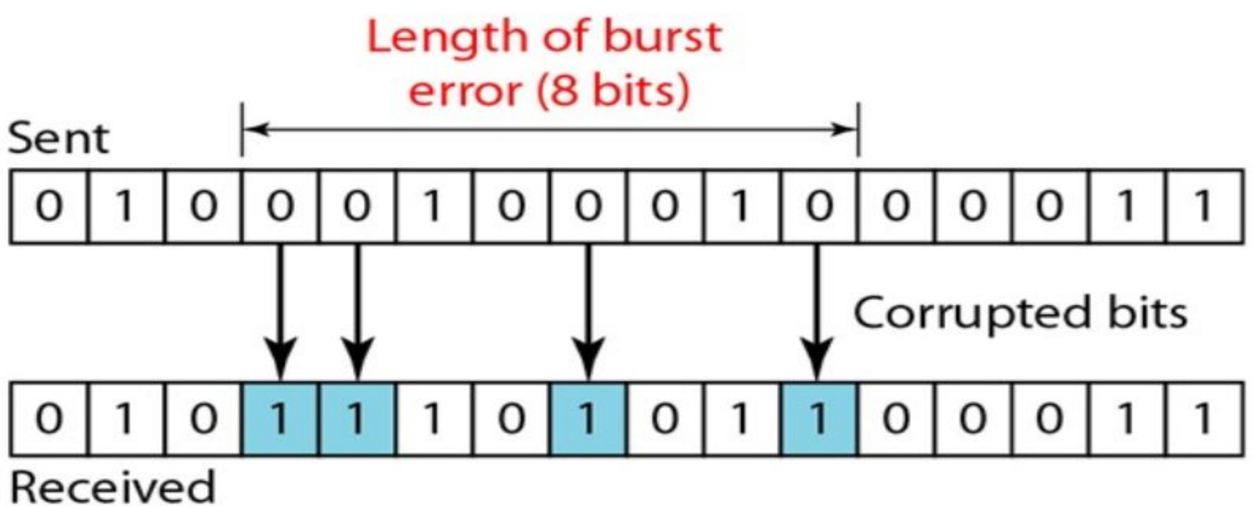



**Figure 10.2** *Burst error of length 8*



# CODING

- Redundancy is achieved through various coding schemes.
- The ratio of redundant bits to data bits and the robustness of the process are important factors in any coding scheme.

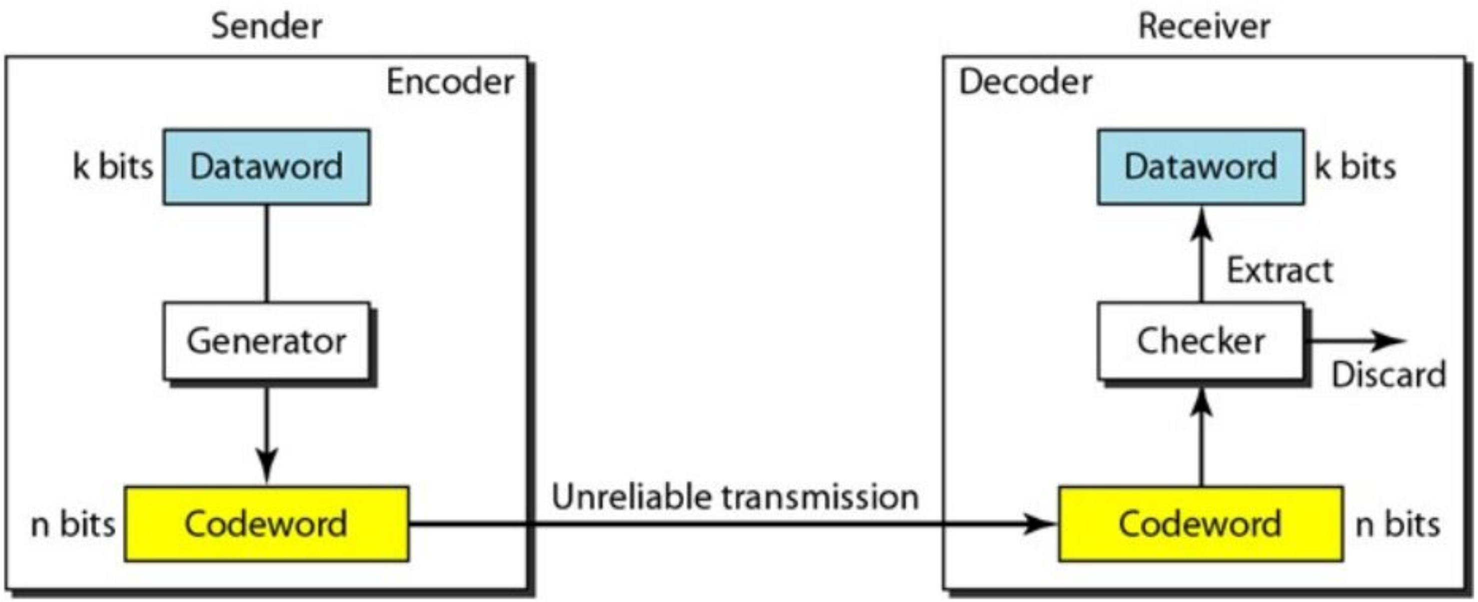
Coding schemes are divided into two categories:

1. Block Coding
2. Convolution Coding

# ERROR DETECTION

Error can be detected using block coding if the following two conditions are met:

1. The receiver has a list of valid codewords
2. The valid codeword has changed into invalid one.



# ERROR DETECTION

Example:

Let us assume : k=2, n=3

1. The receiver receives 011
2. The receiver receives 111
3. The receiver receives 000

| *Datawords* | *Codewords* |
|---|---|
| 00 | 000 |
| 01 | 011 |
| 10 | 101 |
| 11 | 110 |

# ERROR DETECTION

**Types of Error Detection Schemes:**

1. Parity check code
2. Checksum
3. Cyclic Redundancy Check

# ERROR DETECTION

**Hamming Distance:**

- The Hamming distance between two words is the number of differences between the corresponding bits.

  d(00000,01101) =3
- Hamming distance between the received codeword and the sent codeword is the number of bits that are corrupted during transmission.
- The minimum Hamming distance is the smallest Hamming distance between all possible pairs of codewords.
- If a system can detect s errors , the minimum distance between the valid codes must be s+1

**Linear Block Codes:**

- A linear block code is a code in which the exclusive OR of two valid codewords create another valid codeword.

# ERROR DETECTION

## Parity Check Code

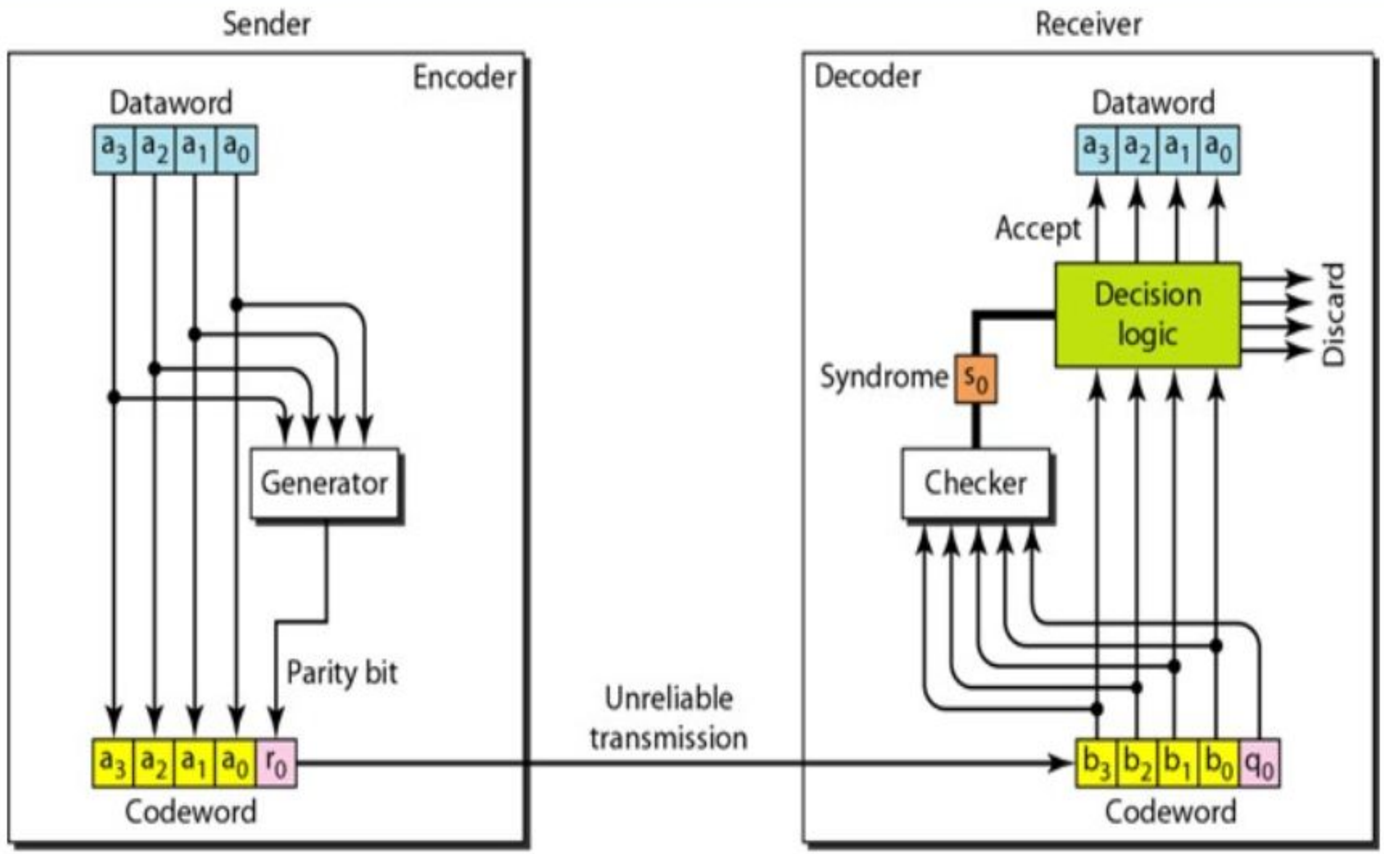
- Parity check code is the most familiar error detecting code. It is a linear block code.
- In this code the K-bit dataword is changed to n-bit codeword where n=k+1.
- The extra bit ,called the parity bit is selected to make the total number of 1s in the codeword even. The minimum Hamming distance for this category is 2.
- A simple parity-check code can detect an odd number of errors.

**Table 10.3** *Simple parity-check code C(5, 4)*

| Datawords | Codewords | Datawords | Codewords |
|---|---|---|---|
| 0000 | 00000 | 1000 | 10001 |
| 0001 | 00011 | 1001 | 10010 |
| 0010 | 00101 | 1010 | 10100 |
| 0011 | 00110 | 1011 | 10111 |
| 0100 | 01001 | 1100 | 11000 |
| 0101 | 01010 | 1101 | 11011 |
| 0110 | 01100 | 1110 | 11101 |
| 0111 | 01111 | 1111 | 11110 |

# ERROR DETECTION

Figure 10.10 *Encoder and decoder for simple parity-check code*



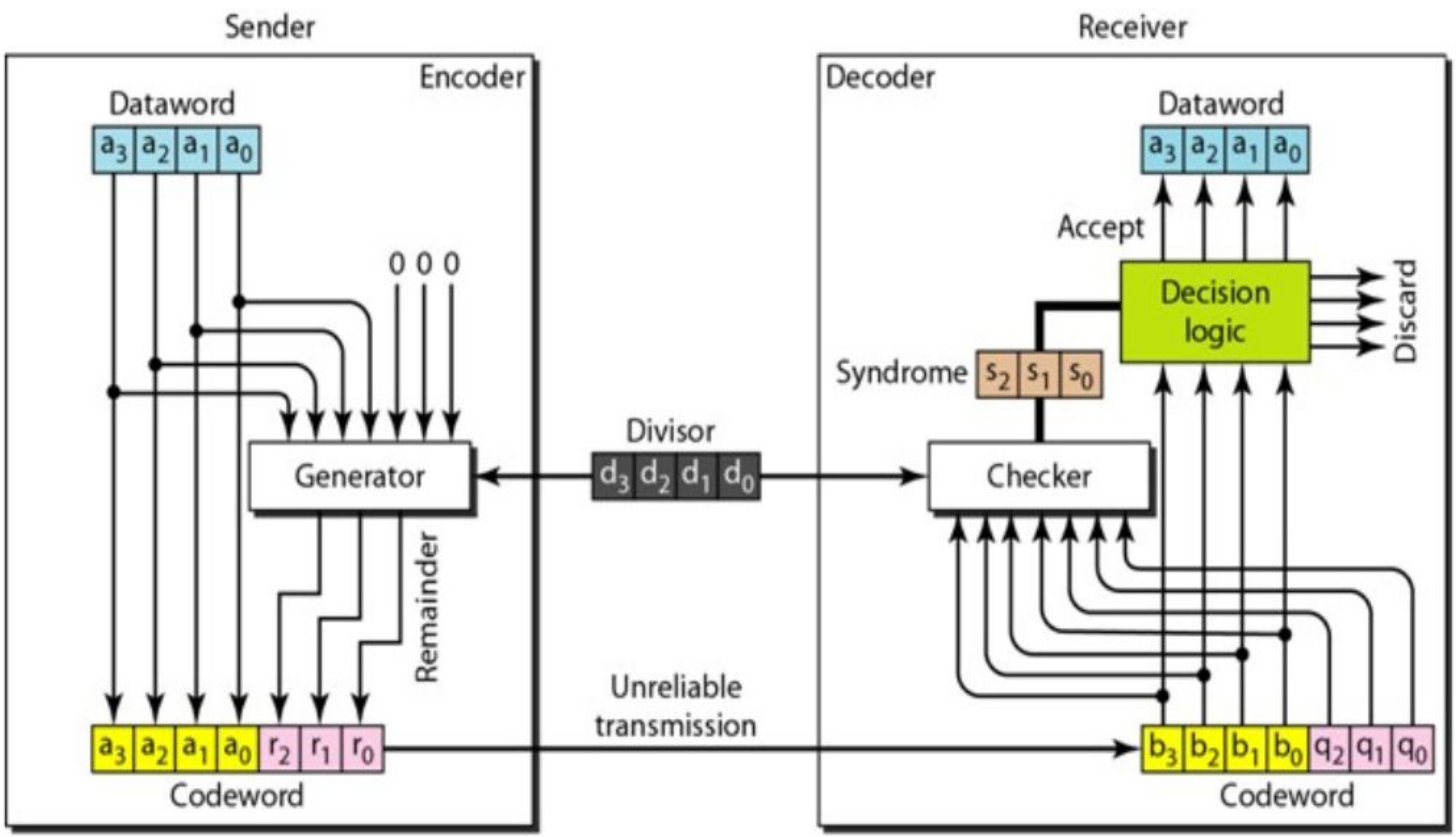
# ERROR DETECTION

**Cyclic Codes**

- Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.
- For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword.

# ERROR DETECTION

## Cyclic Redundancy Check

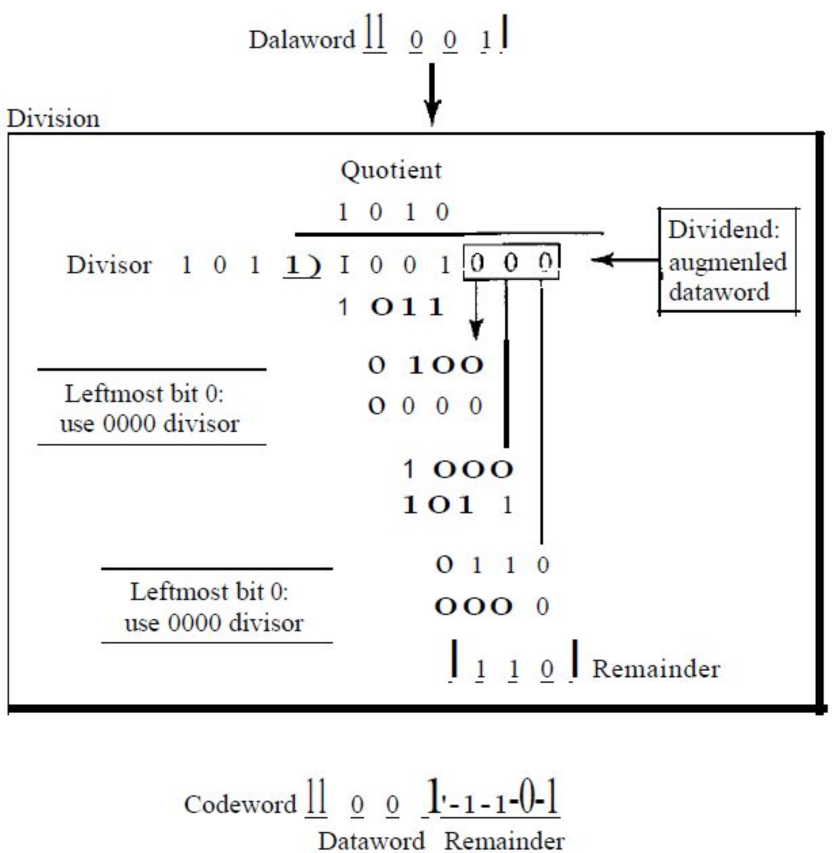


# ERROR DETECTION

Lets see an example for CRC

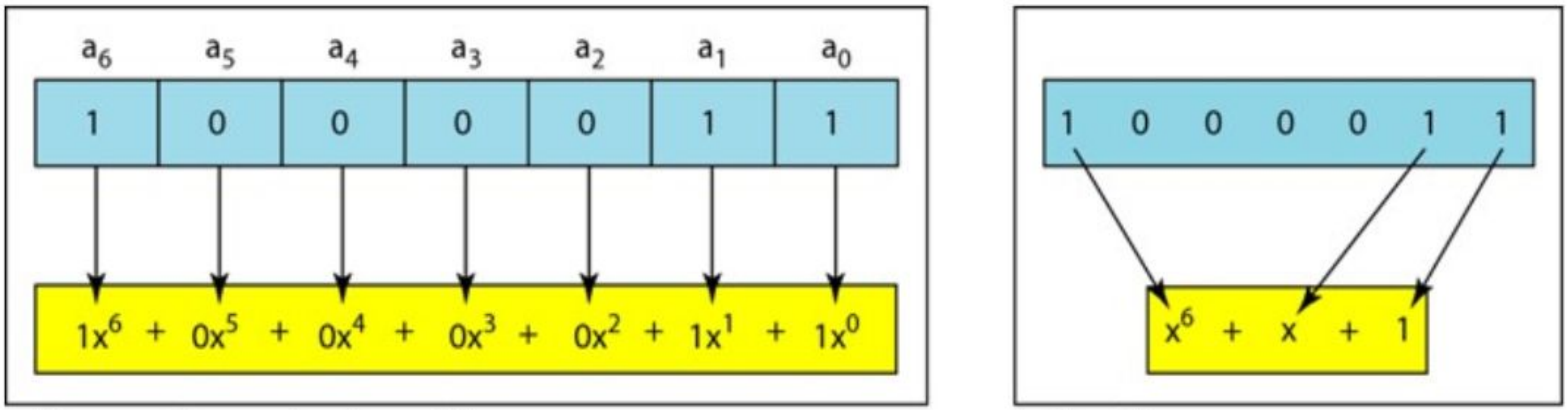
n=7, Generator word ( Divisor) = 1011, dataword=1001

Figure 10.15 *Division in CRC encoder*



# ERROR DETECTION

## Polynomials




a. Binary pattern and polynomial

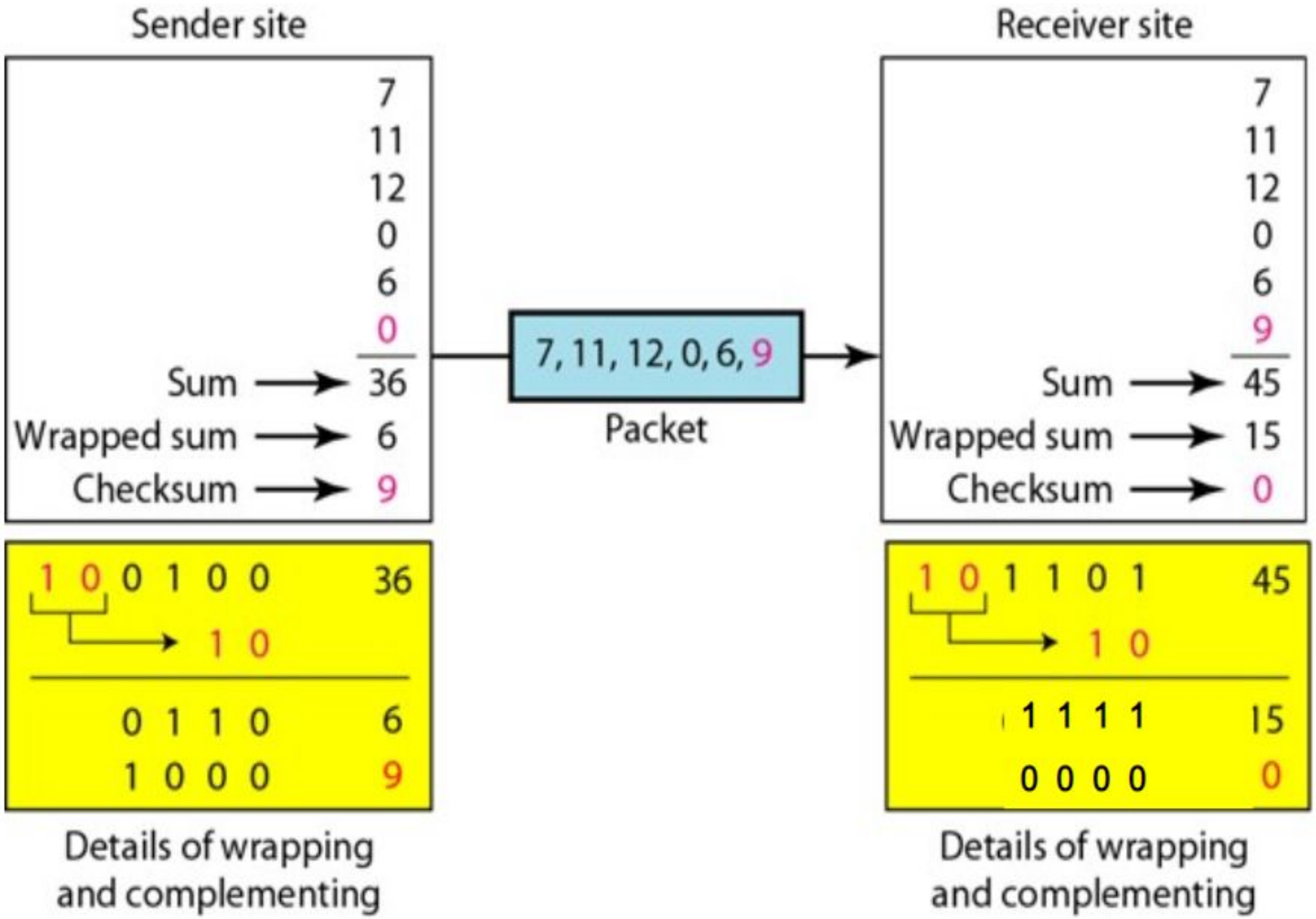
b. Short form

# ERROR DETECTION

## Checksum

- Checksum is a error detecting technique that can be applied to a message of any length.
- At the source, the message is first divided into m-bits. The generator than creates an extra m bit called the checksum, which is sent with the message.
- At the receiver the checker creates a new checksum from the combination of the message and sent checksum.
- If the new checksum is all 0s the message is accepted, otherwise it is discarded

# ERROR DETECTION



# ERROR CORRECTION

There are four different error-correcting codes:

1. Hamming codes.
2. Binary convolutional codes.
3. Reed-Solomon codes.
4. Low-Density Parity Check codes.

# ERROR CORRECTION

**Hamming code:**

- The Hamming codes were initially designed with $d_{min} = 3$ .
- $d_{min}$ decides the error detection and correction capability
- Number of error detected = $d_{min}$ -1
- Number of error corrected = ($d_{min}$ -1)/2
- E.g. for (7,4) Hamming code with $d_{min}$ =3
- Equations are:

$$r_0 = a_2 + a_1 + a_0$$
$$r_1 = a_3 + a_2 + a_1$$
$$r_2 = a_1 + a_0 + a_3$$

'+' is mod-2 addition performed with XOR

# ERROR CORRECTION

- Set of equations for detection:

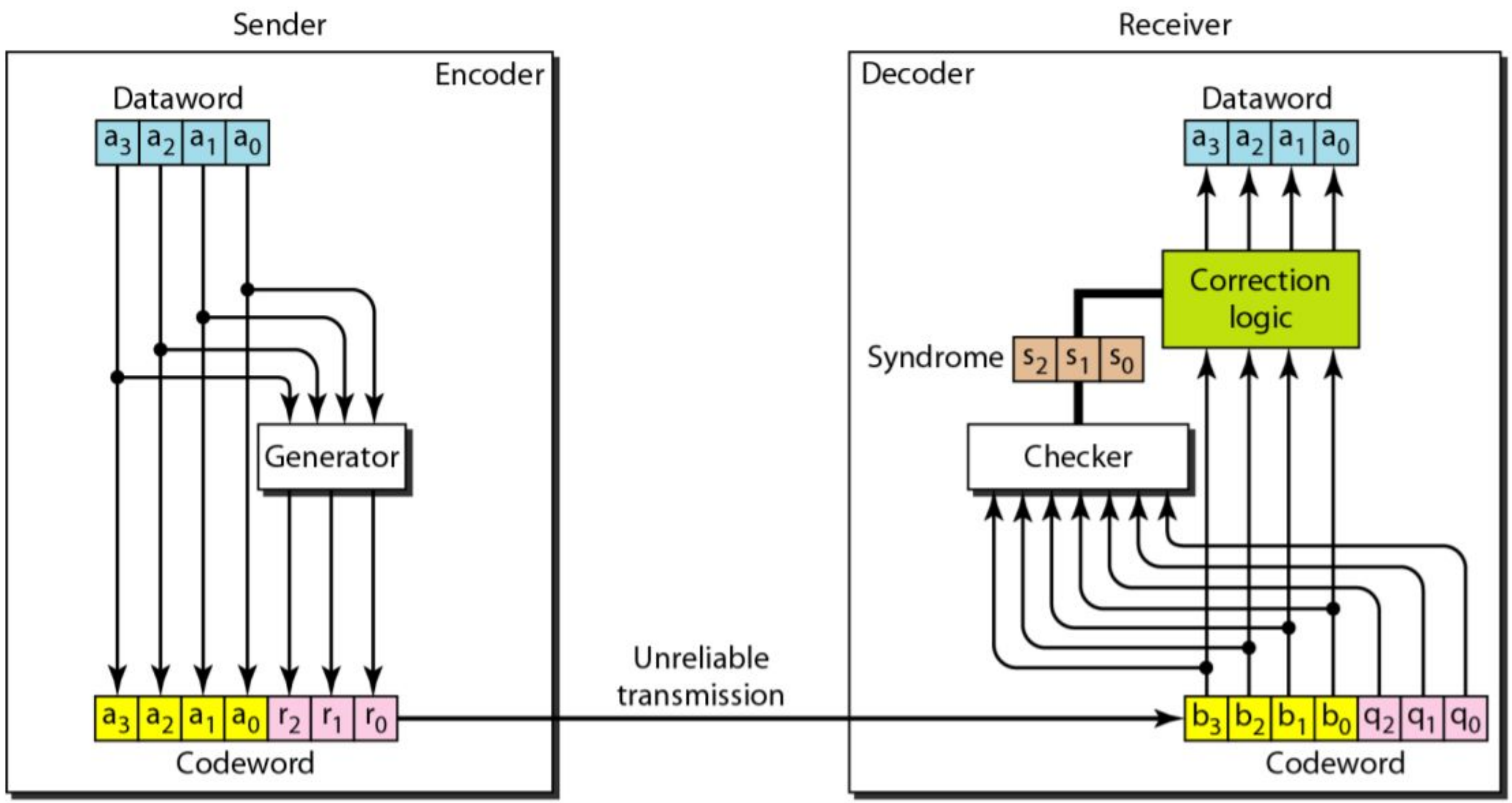
$$s_0 = b_2 + b_1 + b_0 + q_0$$
$$s_1 = b_3 + b_2 + b_1 + q_1$$
$$s_2 = b_1 + b_0 + b_3 + q_2$$

- Logical decision made by the correction logic analyzer

| *Syndrome* | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| *Error* | None | $q_0$ | $q_1$ | $b_2$ | $q_2$ | $b_0$ | $b_3$ | $b_1$ |

# ERROR CORRECTION

***The structure of the encoder and decoder for a Hamming code***



# ERROR CORRECTION

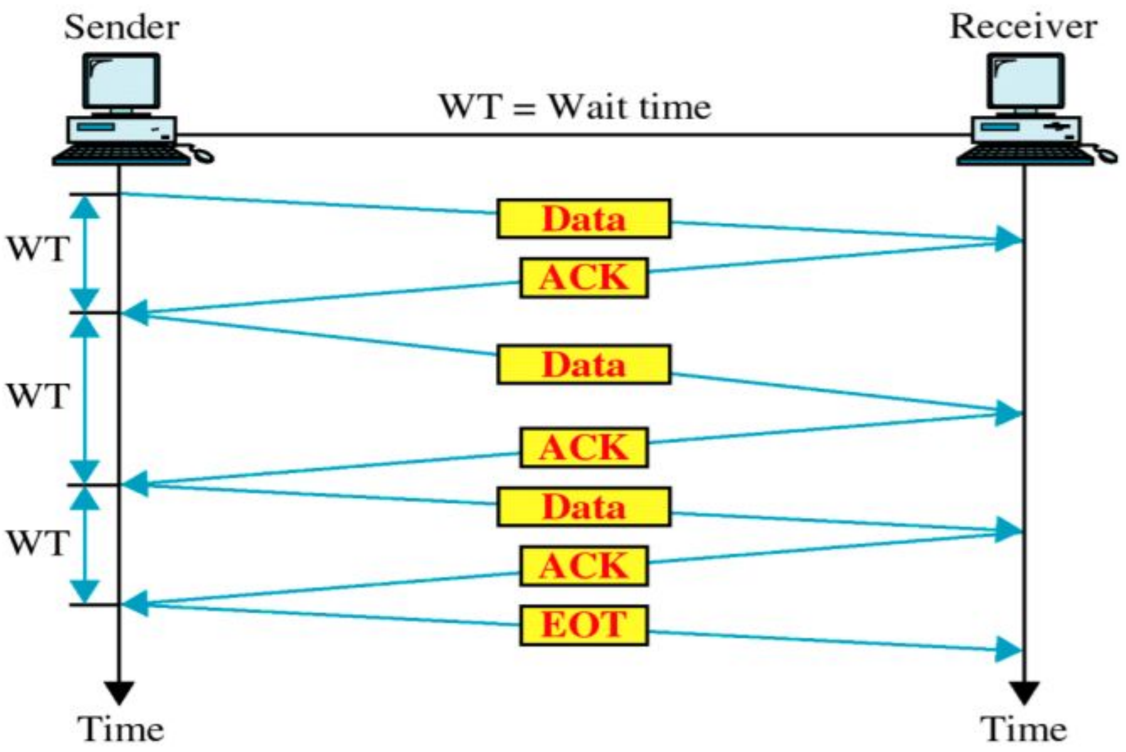
Example:

1. For Hamming code C(7,4) with $d_{min}$ =3, Find the codeword for data 0100. Find transmitted codeword. If the received codeword is 0100011, find syndrome, detect and correct the error, and find final dataword.
2. Dataword=0111. received codeword= 0011001
3. Dataword=1101. received codeword= 0001000

# Elementary Data Link Layer Protocols

# STOP AND WAIT

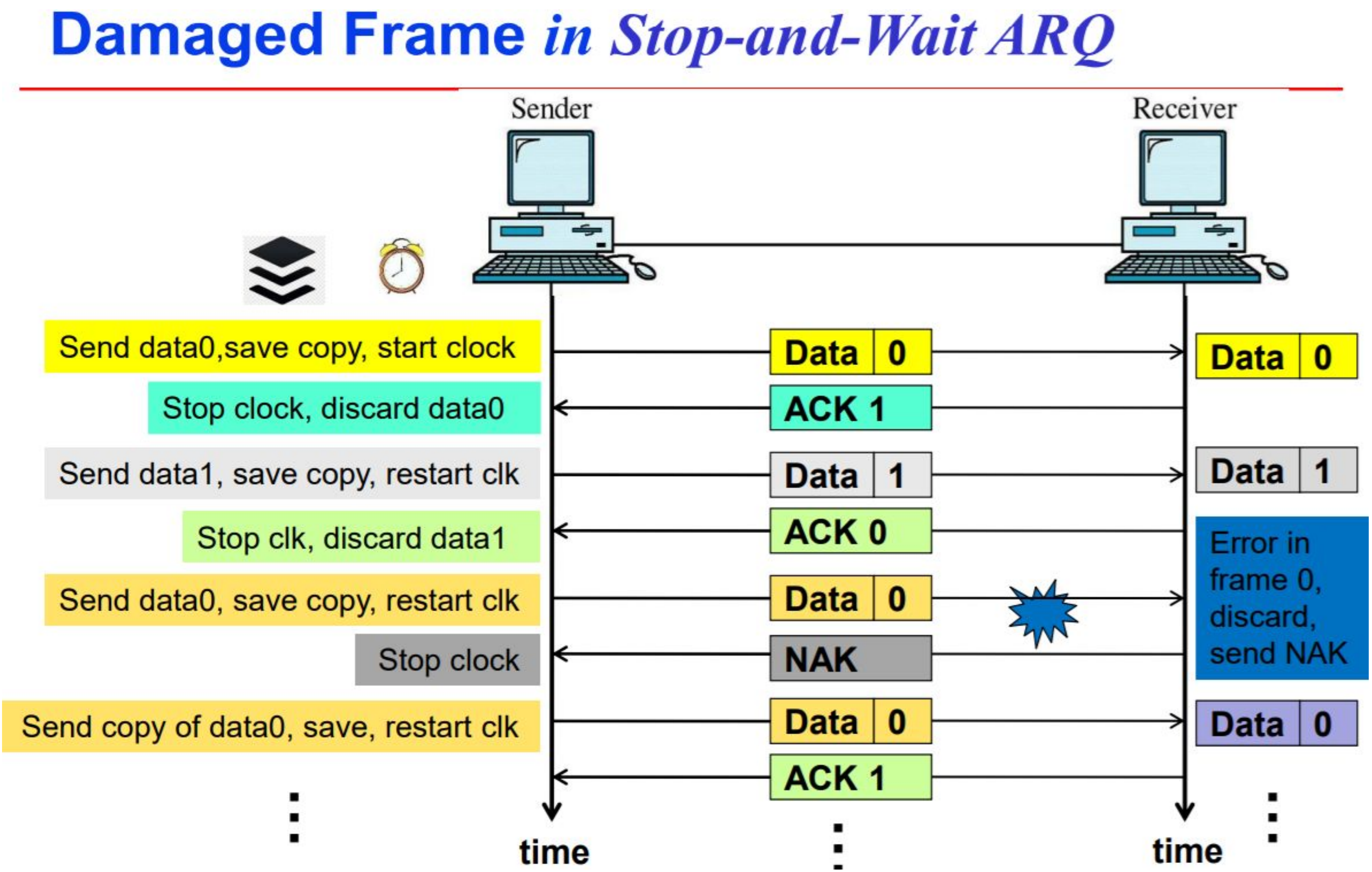
- The sender waits for an ACK after every frame it sends.
- Only after receiving ACK, the next frame is send.
- Advantage: simplicity
- Disadvantage: slow, inefficient



# STOP AND WAIT ARQ

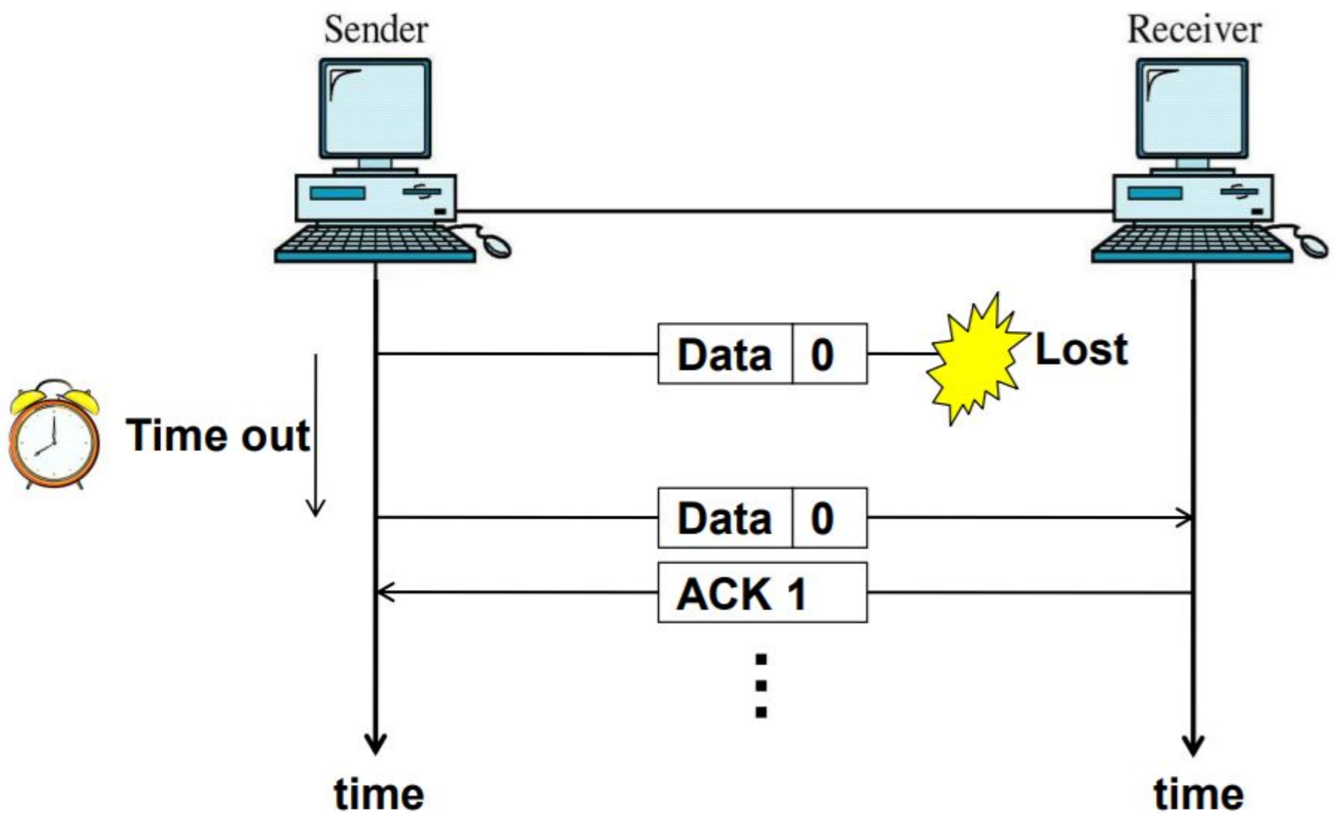
- When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded.
- Lost frames are more difficult to handle than corrupted ones.
- In Stop-and-Wait ARQ sequence numbers are used to number the frames .
- The sender keeps a copy of the sent frame. At the same time, it starts a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted.
- Since an ACK frame can also be corrupted and lost, it too needs redundancy bits and a sequence number. The ACK frame for this protocol has a sequence number field.

# STOP AND WAIT ARQ



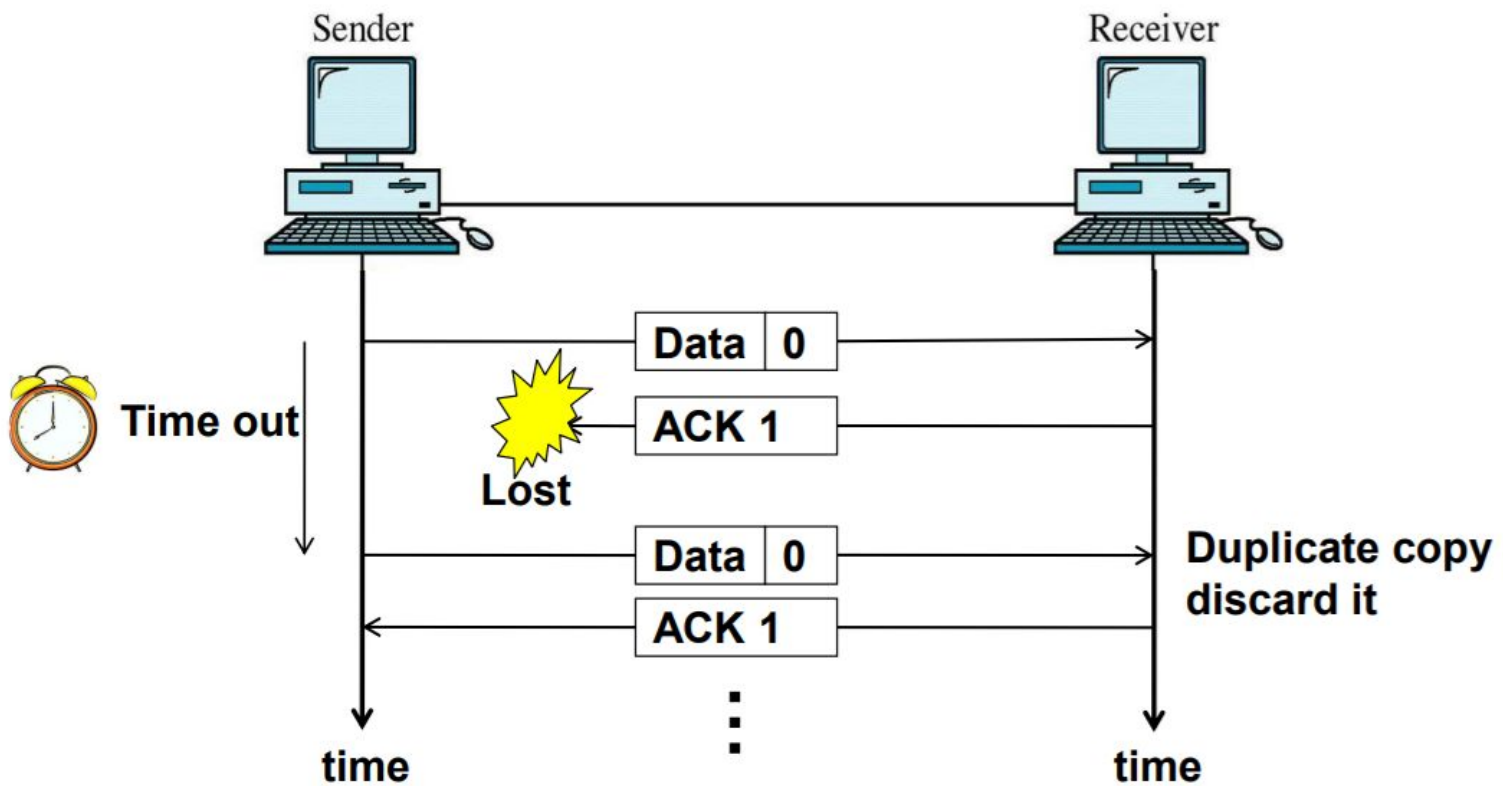
# STOP AND WAIT ARQ

## Lost data frame *in Stop-and-Wait ARQ*



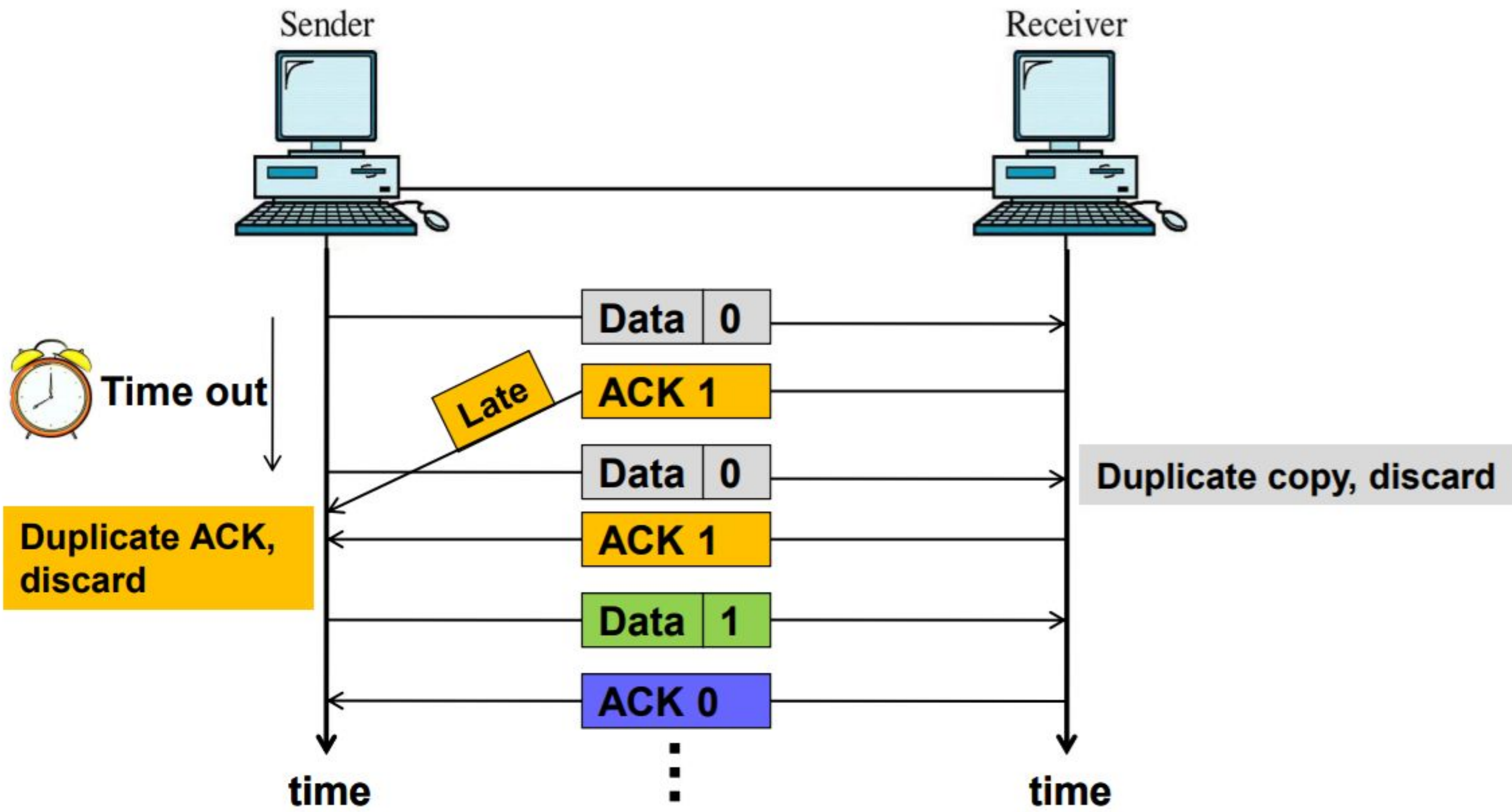
# STOP AND WAIT ARQ

## Lost ACK frame *in Stop-and-Wait ARQ*



# STOP AND WAIT ARQ

## Late ACK frame *in Stop-and-Wait ARQ*

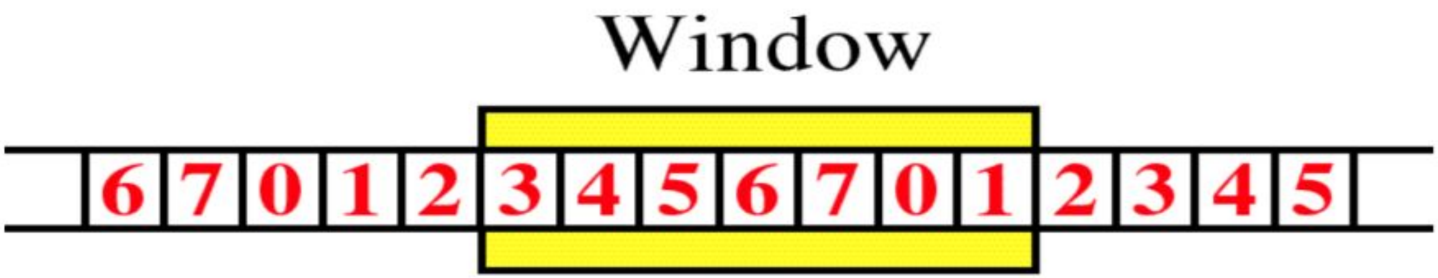


# SLIDING WINDOW

- Sender can transmit several frames before needing an ACK.
- Thus link carry several frames at once, increasing the efficiency.
- Receiver acknowledges multiple frames using single ACK

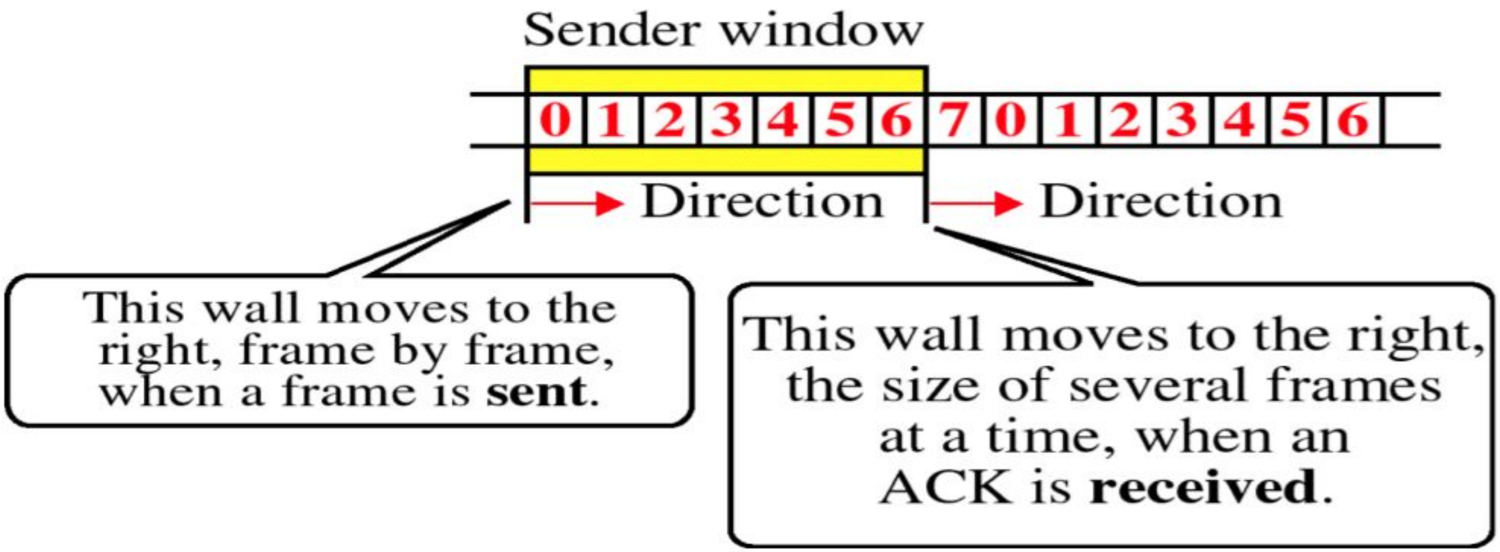
**Sliding Window:**

- This virtual window hold frames at either end.
- Frames are numbered modulo-n. E.g.- for n=8 frames numbers are 0,1,2,3,4,5,6,7,0,1,2,3,-----
- Size of the window is (n-1).
- ACK’s number always indicate the next frame receiver expects to receive.



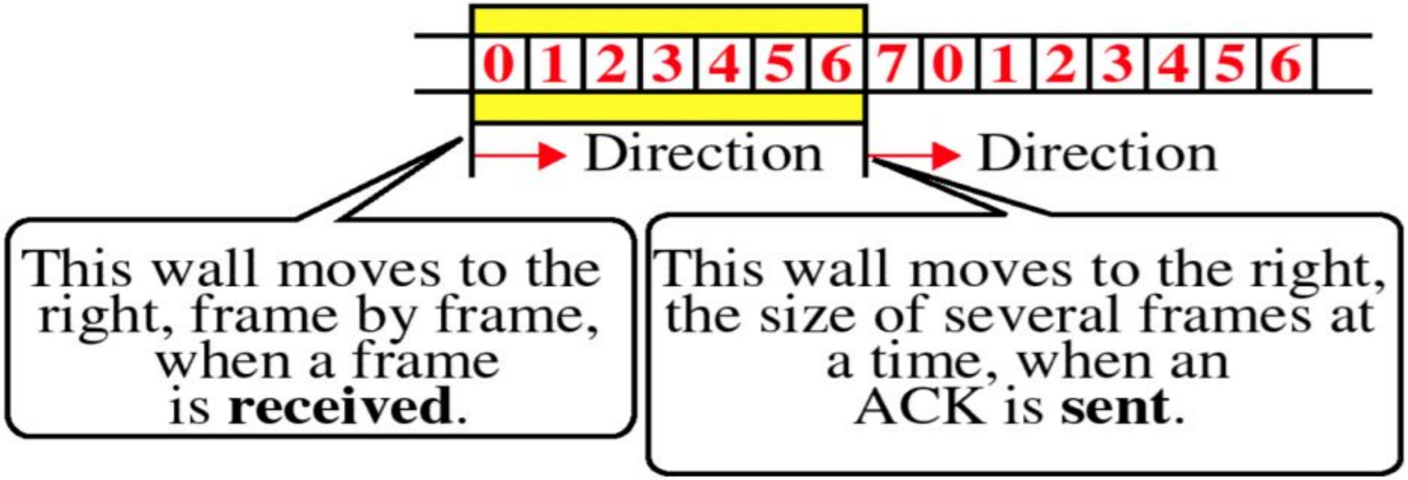
# SENDER SLIDING WINDOW

- At the beginning of a transmission, this window contains n-1 frames.
- As frames are sent out, the left boundary moves inward, shrinking the size of window.
- Once an ACK arrives, the window expands to allow number of new frames equal to the number of frames acknowledged by that ACK

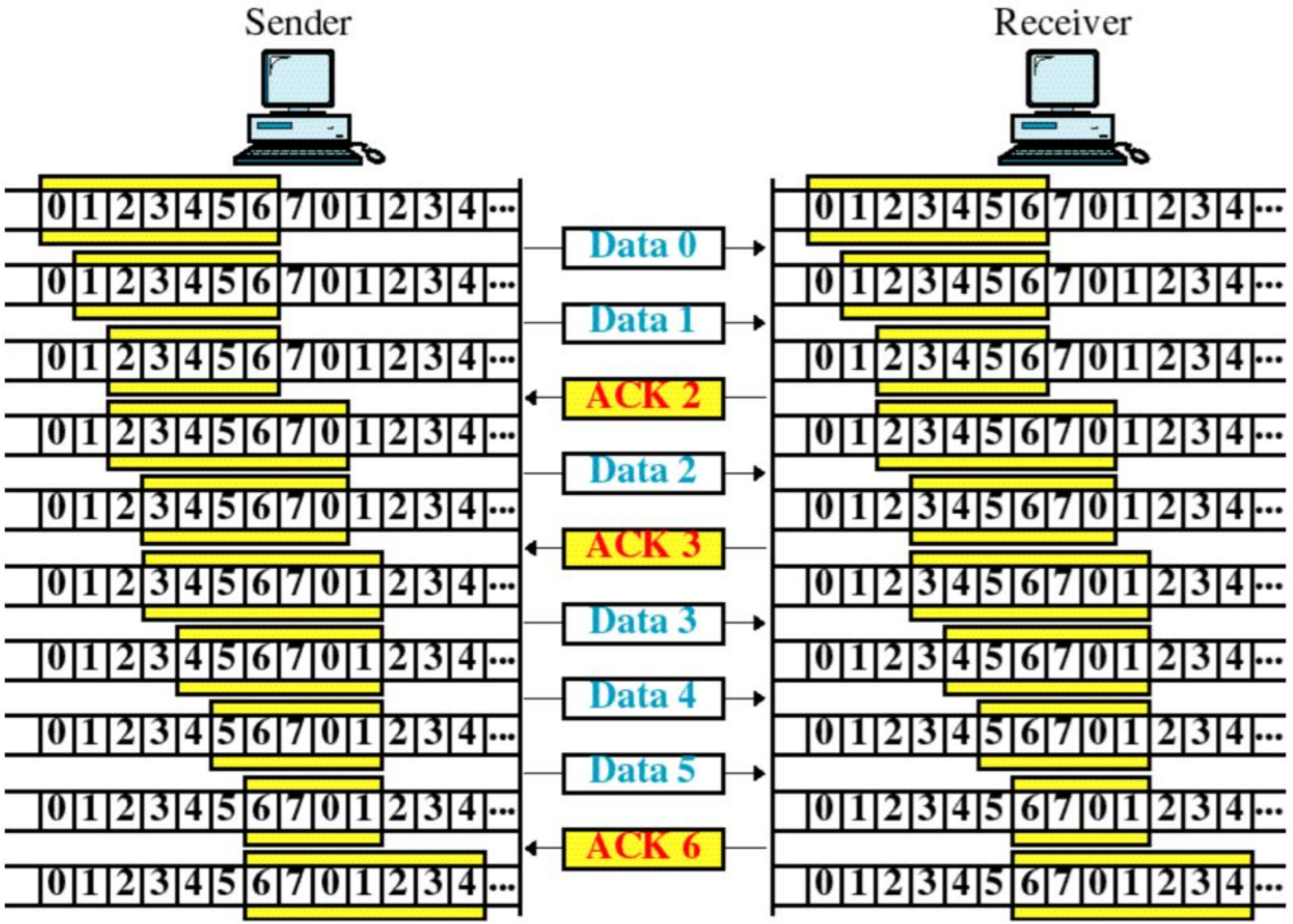


# RECEIVER SLIDING WINDOW

- At the beginning of transmission, this window contains n-1 spaces.
- As new frames come in, the size of this window shrinks.
- This window always holds number of frames that may still be received before an ACK is sent.
- When ACK is sent, the window expands to include places for number of frames equal to the number of frames acknowledged.



# SLIDING WINDOW



# SLIDING WINDOW ARQ

- For retransmission, three features are added to sliding window flow control:

1. Sending device keeps the copy of all transmitted frames until it receives an ACK for those frames

- E.g. – If frames 0 through 6 are transmitted, ACK 3 is received, sender keeps copy of 3 through 6 until their ACK.

2. NAK is incorporated & numbered. NAK carry number of a damaged frame. NAK works as both positive and negative acknowledgement

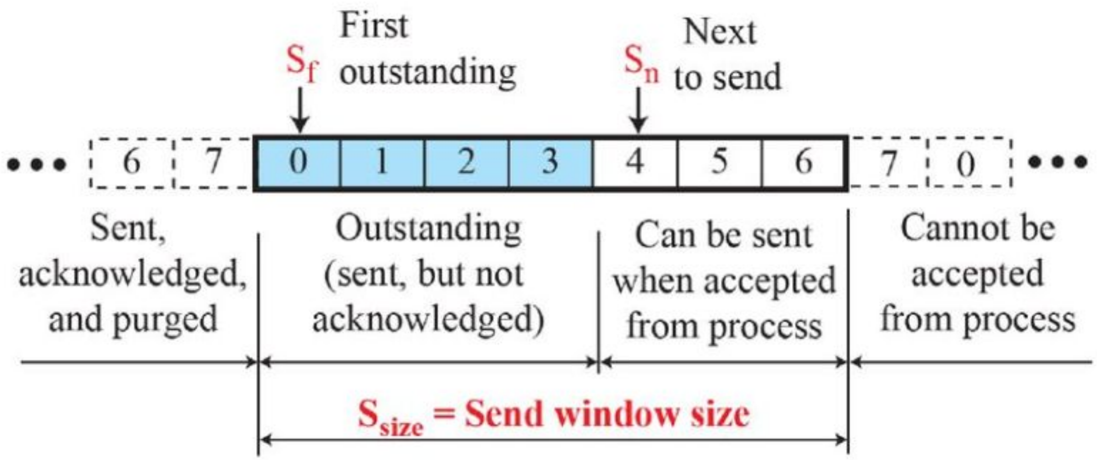
- E.g. – If NAK 4 is received, means frames 0,1,2,3 are received intact and frame 4 is damaged.

3. Sender is equipped with timer to handle lost ACK's

- Here n-1 frames may be send before ACK is received, thus if n-1 frames are waiting for ACK, the sender starts a timer and waits before sending any more. After time out sender transmits one or all frames again
- After time out sender does not know whether the lost frames are data, ACK or NAK
- By retransmission two possibilities are covered, lost data and lost NAK
- If ACK is lost, receiver can recognize it by the frame number (duplicated) and discard the data.

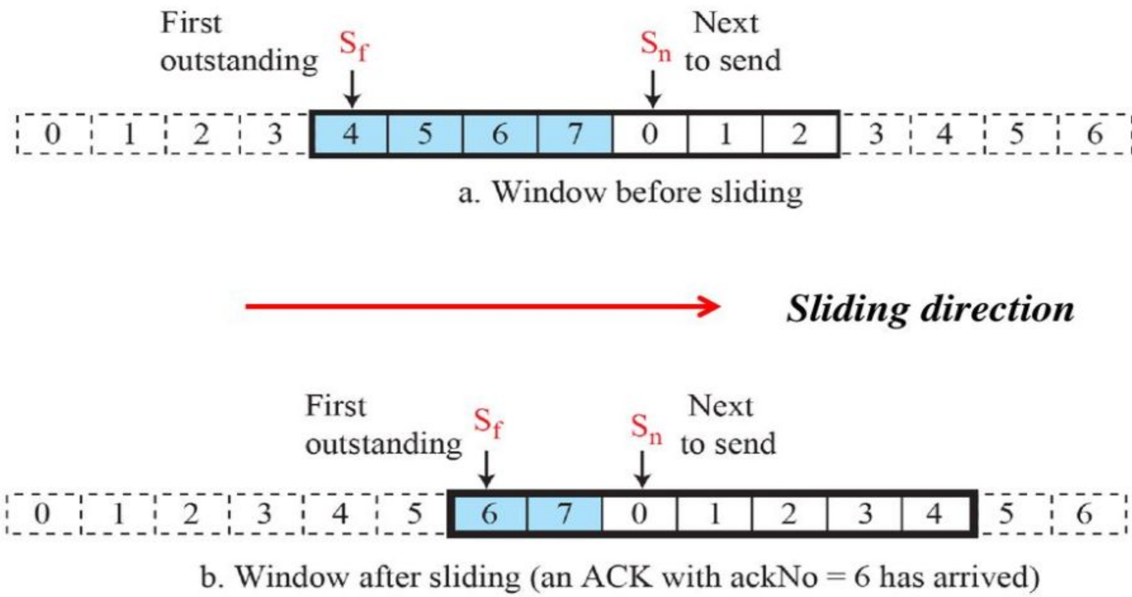
# GO-BACK N ARQ

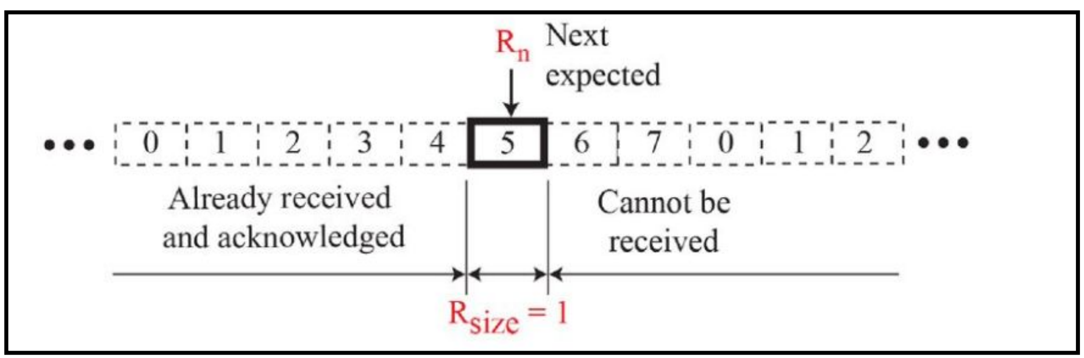
- In Go-Back-N protocol , multiple packets are in transition while the sender is waiting for an acknowledgement.
- The receiver can buffer only one packet.
- Go-Back-n Retransmission : If one frame is lost or damaged, all frames sent since the last frame acknowledged are retransmitted.



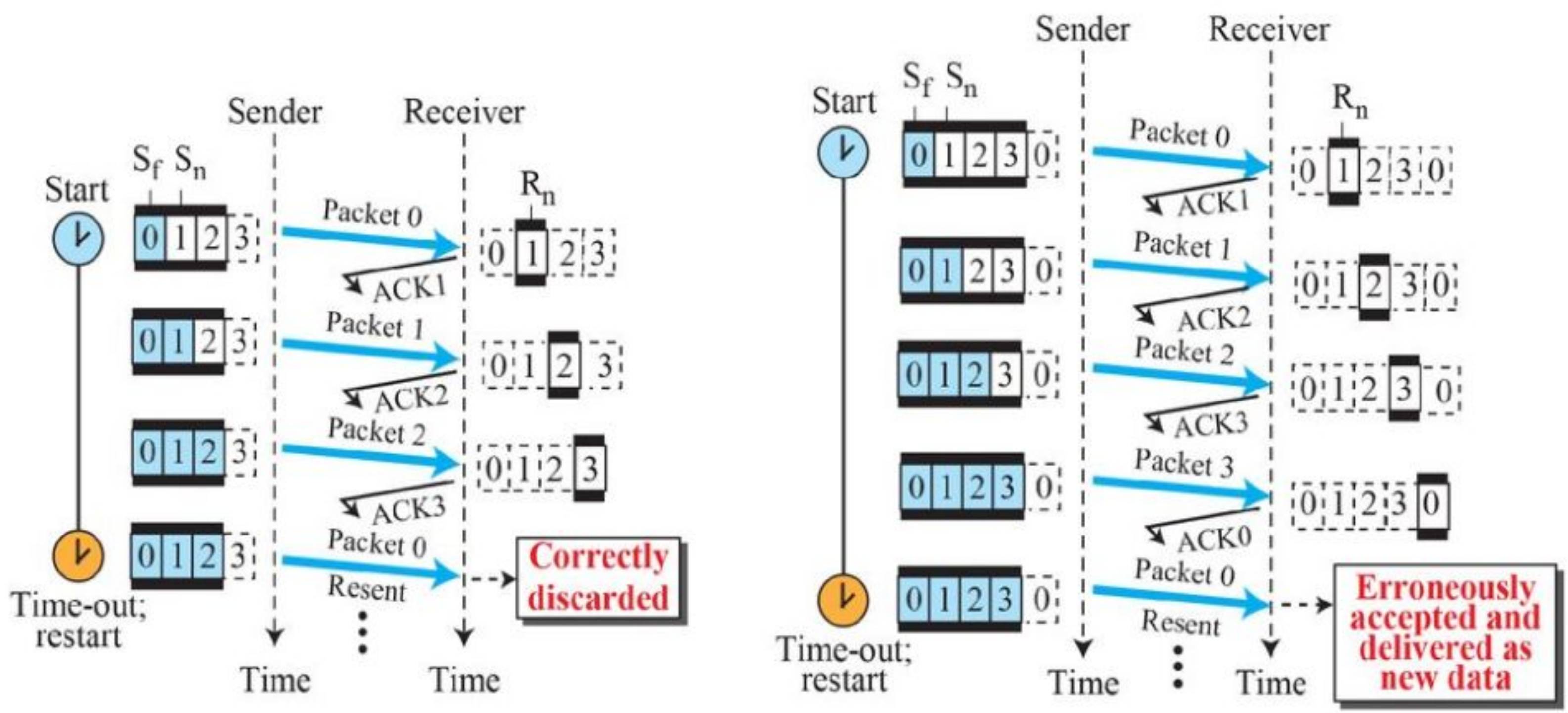
# GO-BACK N ARQ

## Sliding the send window



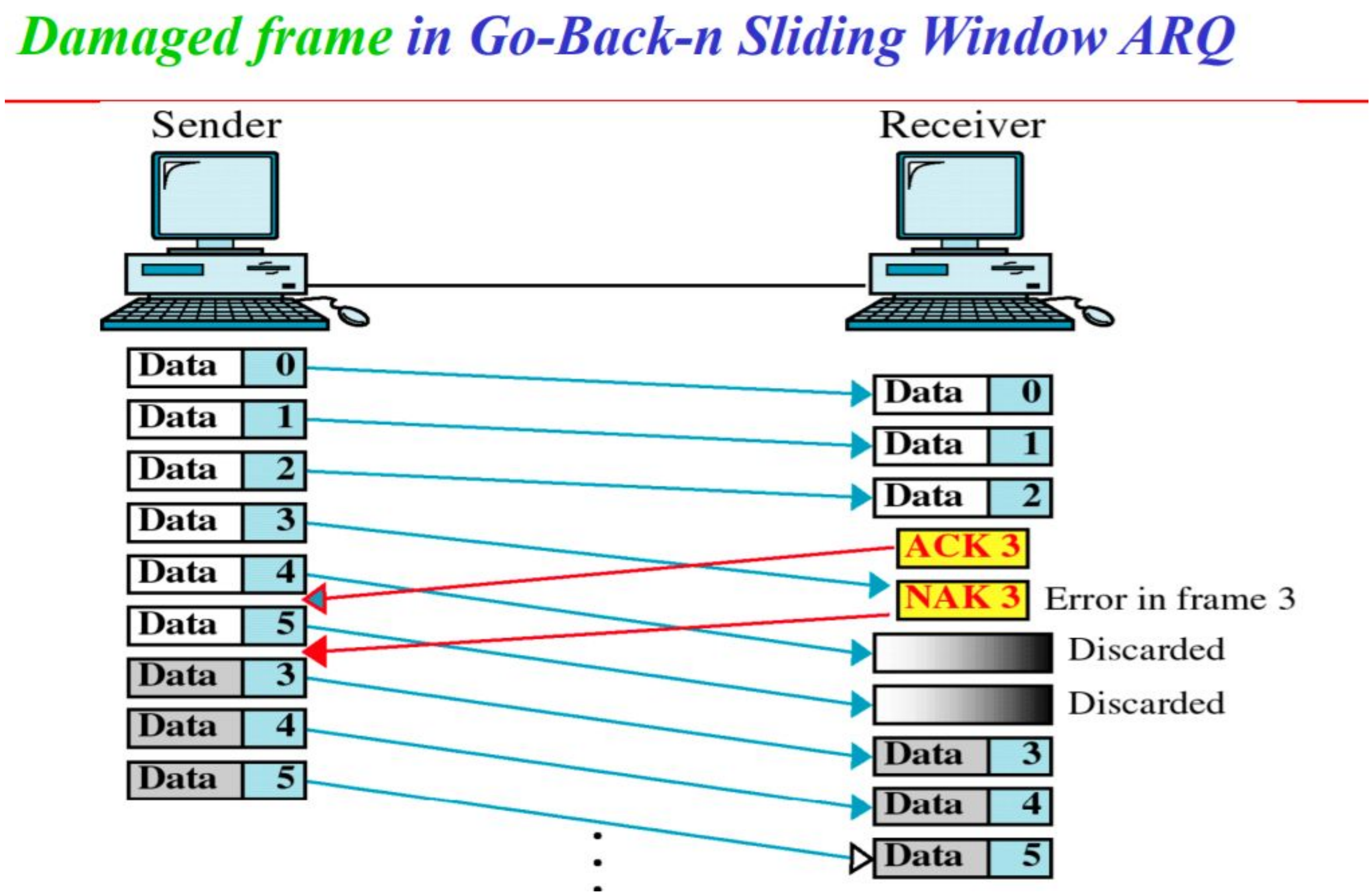
# GO-BACK N ARQ



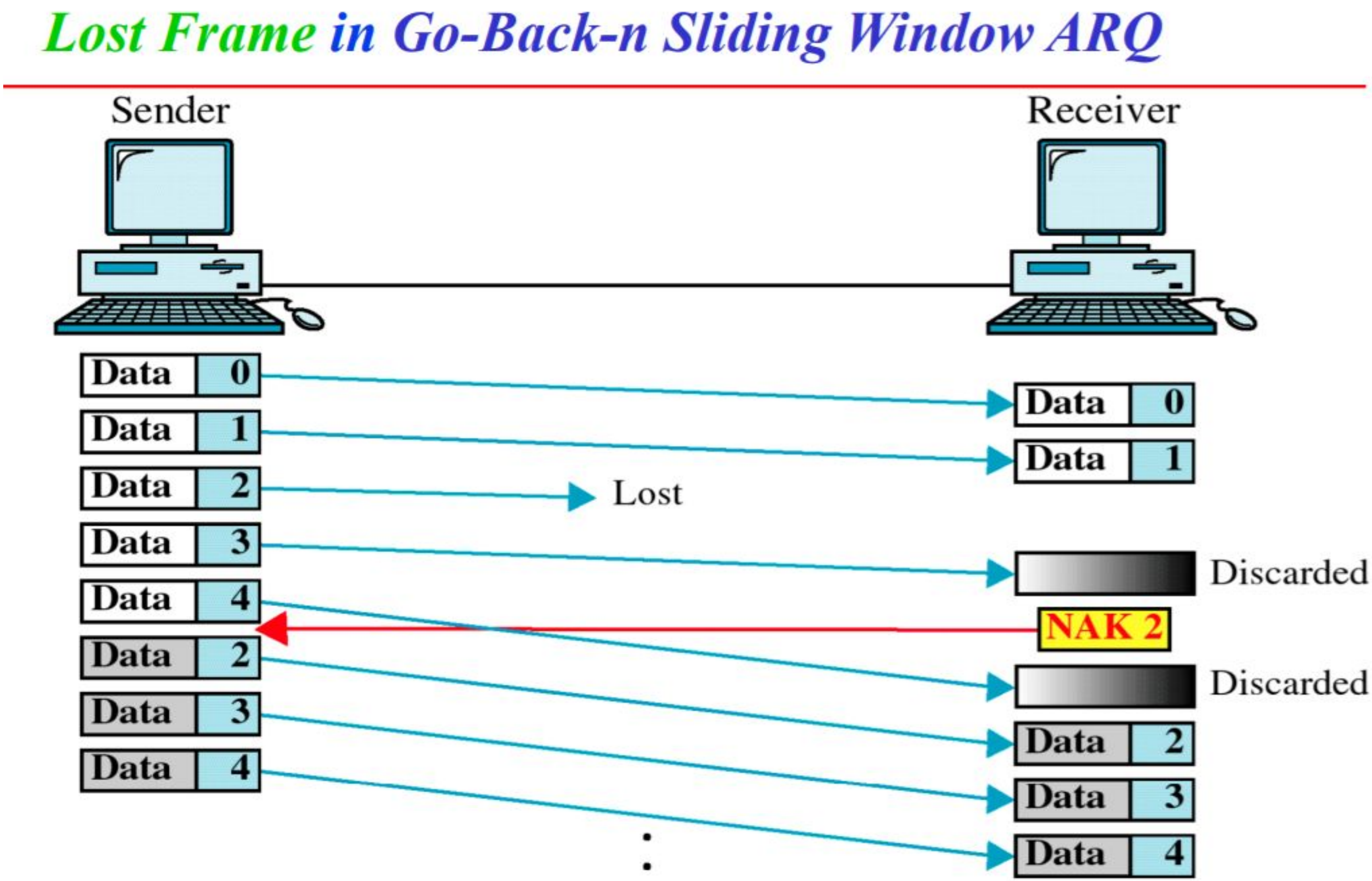

a. Send window of size < $2^m$

b. Send window of size = $2^m$

# GO-BACK N ARQ

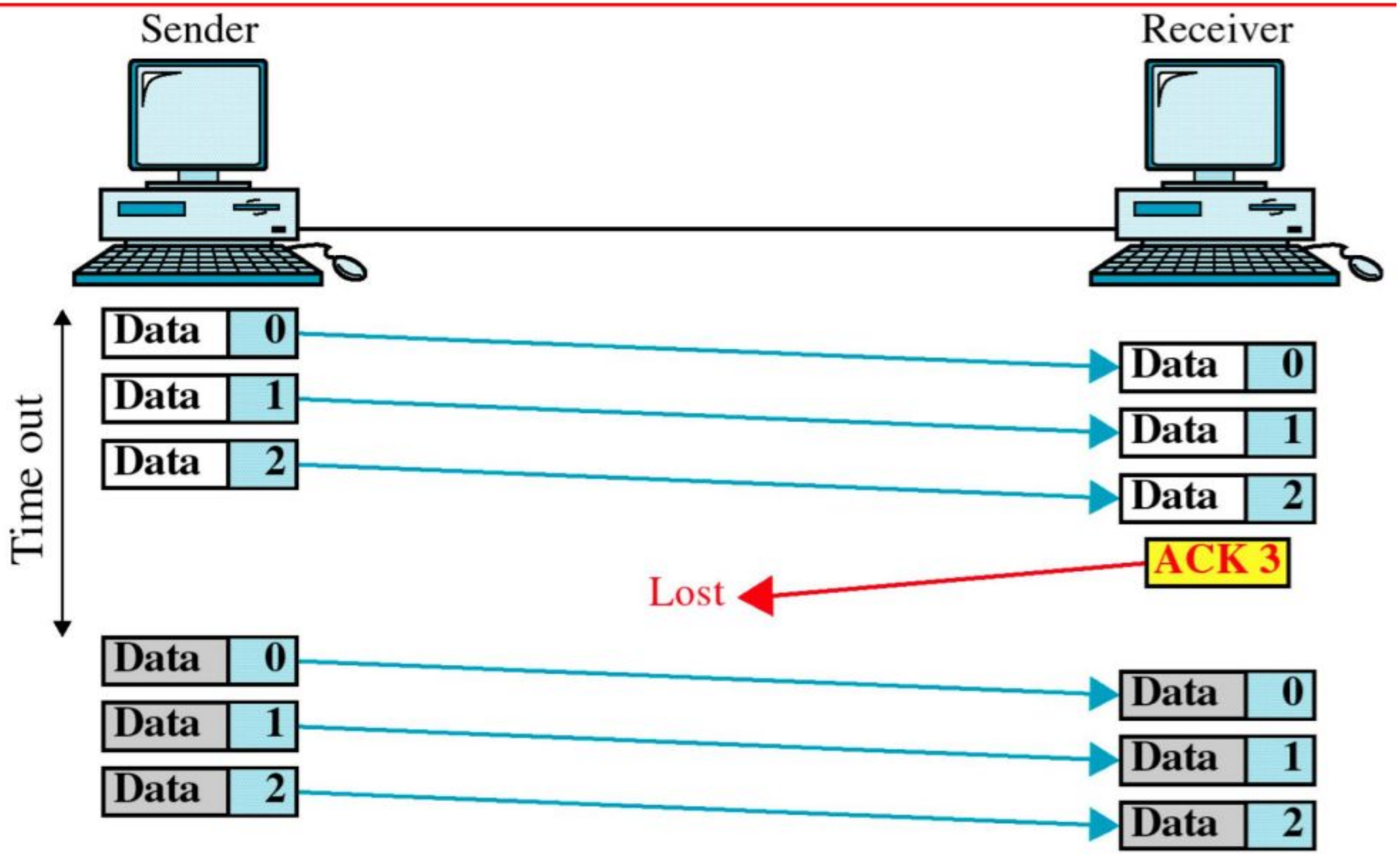

Damaged frame in Go-Back-n Sliding Window ARQ
Sender
Receiver
Data 0
Data 1
Data 2
Data 3
Data 4
Data 5
Data 3
Data 4
Data 5
Data 0
Data 1
Data 2
ACK 3
NAK 3
Error in frame 3
Discarded
Discarded
Data 3
Data 4
Data 5

# GO-BACK N ARQ


Lost Frame in Go-Back-n Sliding Window ARQ
Sender
Receiver
Data 0
Data 1
Data 2
Data 3
Data 4
Data 2
Data 3
Data 4
Lost
Discarded
NAK 2
Discarded
Data 0
Data 1
Data 2
Data 3
Data 4

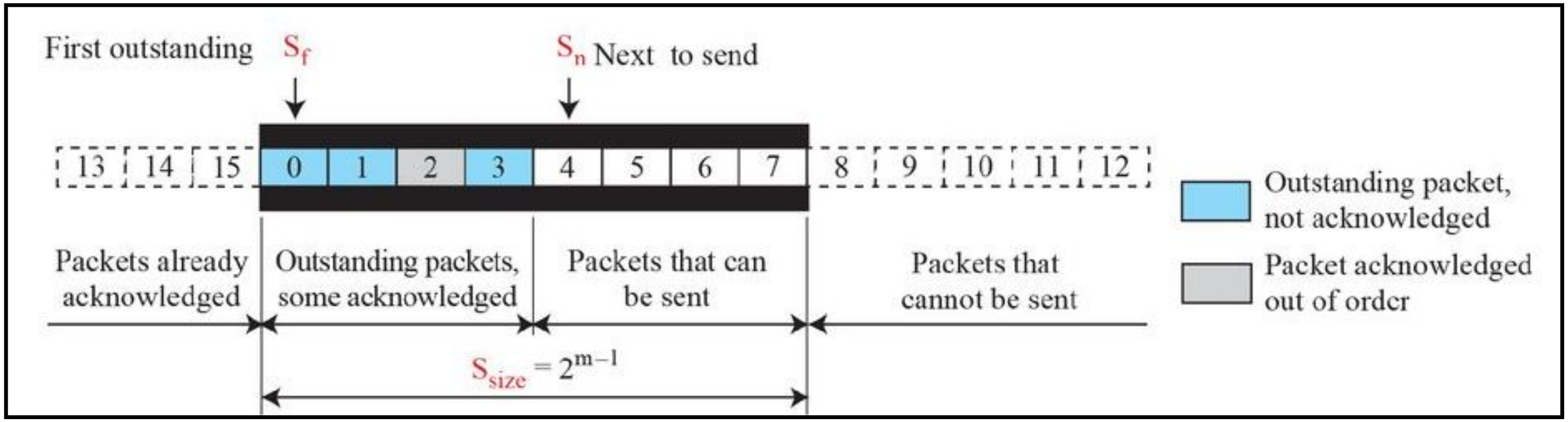
# GO-BACK N ARQ

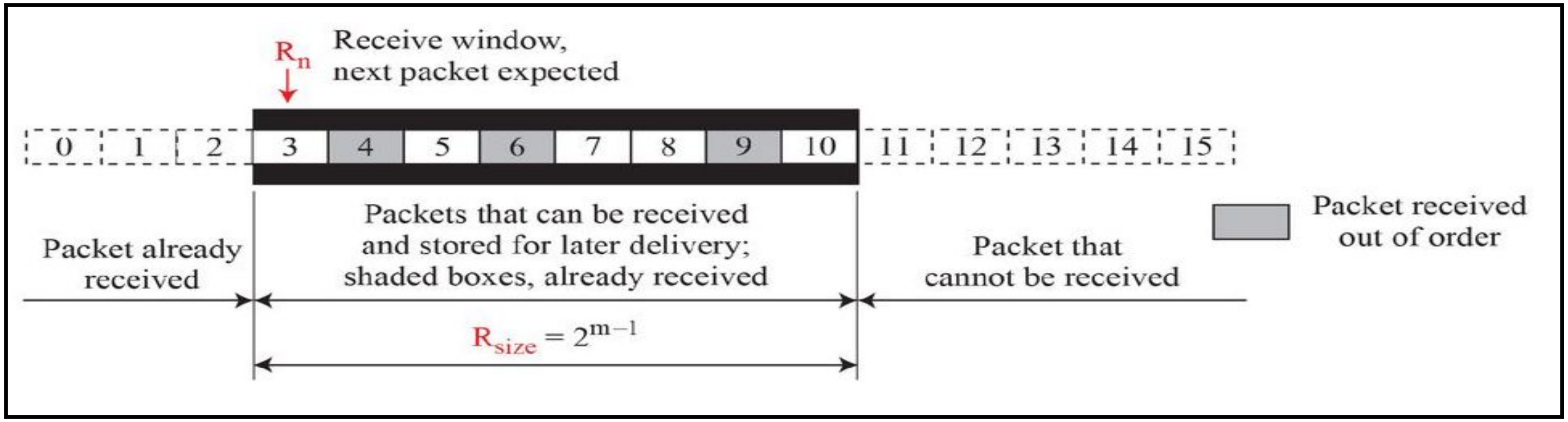
## Lost ACK in Go-Back-n Sliding Window ARQ



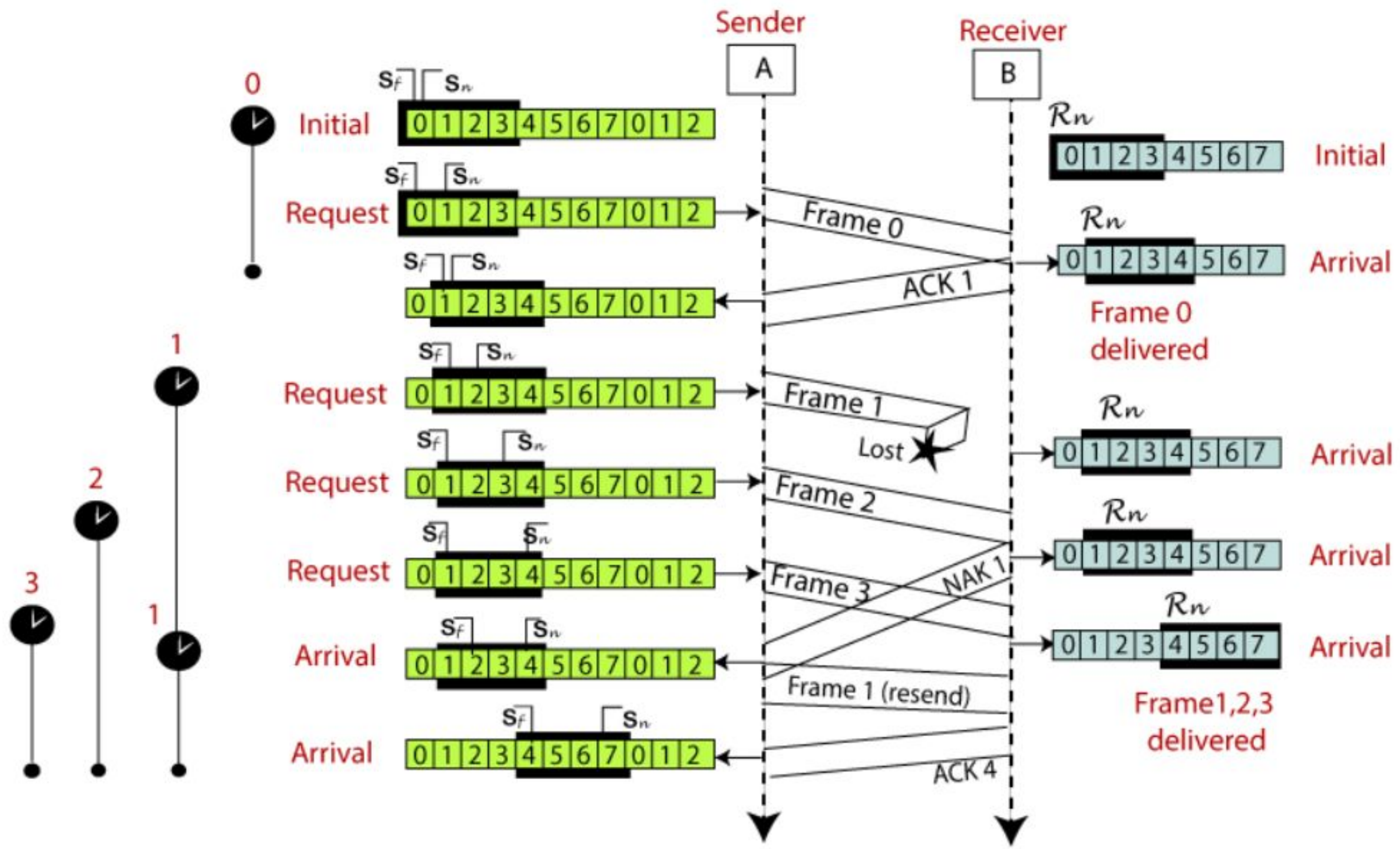
# SELECTIVE REPEAT ARQ

- Only specific damaged or lost frame is retransmitted.
- If NAK is received, the frame is resent out of sequence.



# SELECTIVE REPEAT ARQ



# PIGGYBACKING

- The flow and error control protocols are unidirectional.
- Data frames flow in only one direction and control , ACK, NAK frames flow in other direction.
- In actual communication networks, data frames and control, ACK, NAK needs to flow in both the direction.
- A technique ,“ piggybacking ” is used to improve the efficiency of protocols.

# HDLC

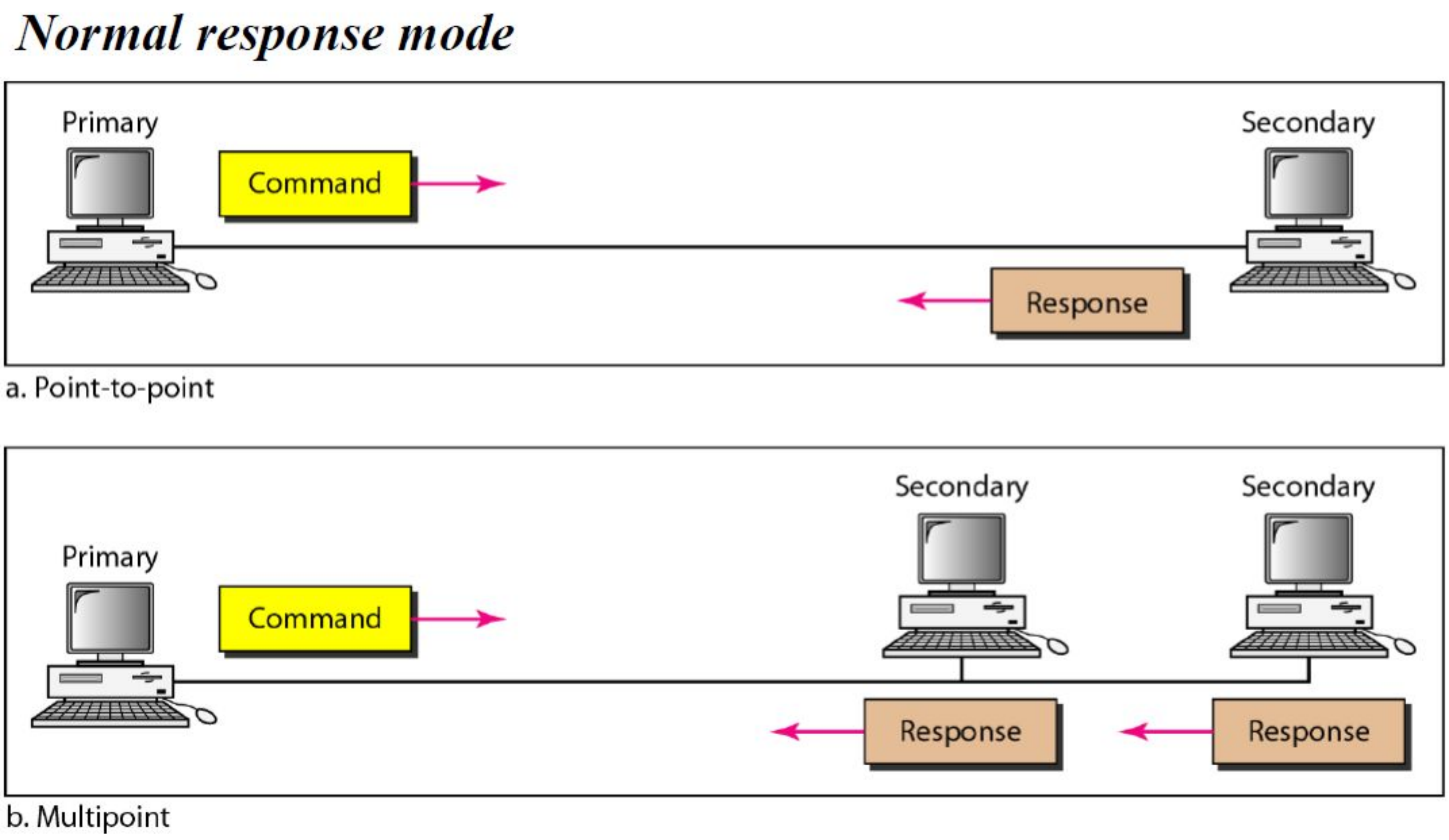
- High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.

**Configurations and Transfer Modes**

- HDLC provides two common transfer modes that can be used in different configurations:

1. Normal response mode (NRM)
2. Asynchronous balanced mode (ABM).

# HDLC


Normal response mode
Primary
Command
Secondary
Response
a. Point-to-point
Primary
Command
Secondary
Secondary
Response
Response
b. Multipoint

# HDLC

***Asynchronous balanced mode***

# HDLC

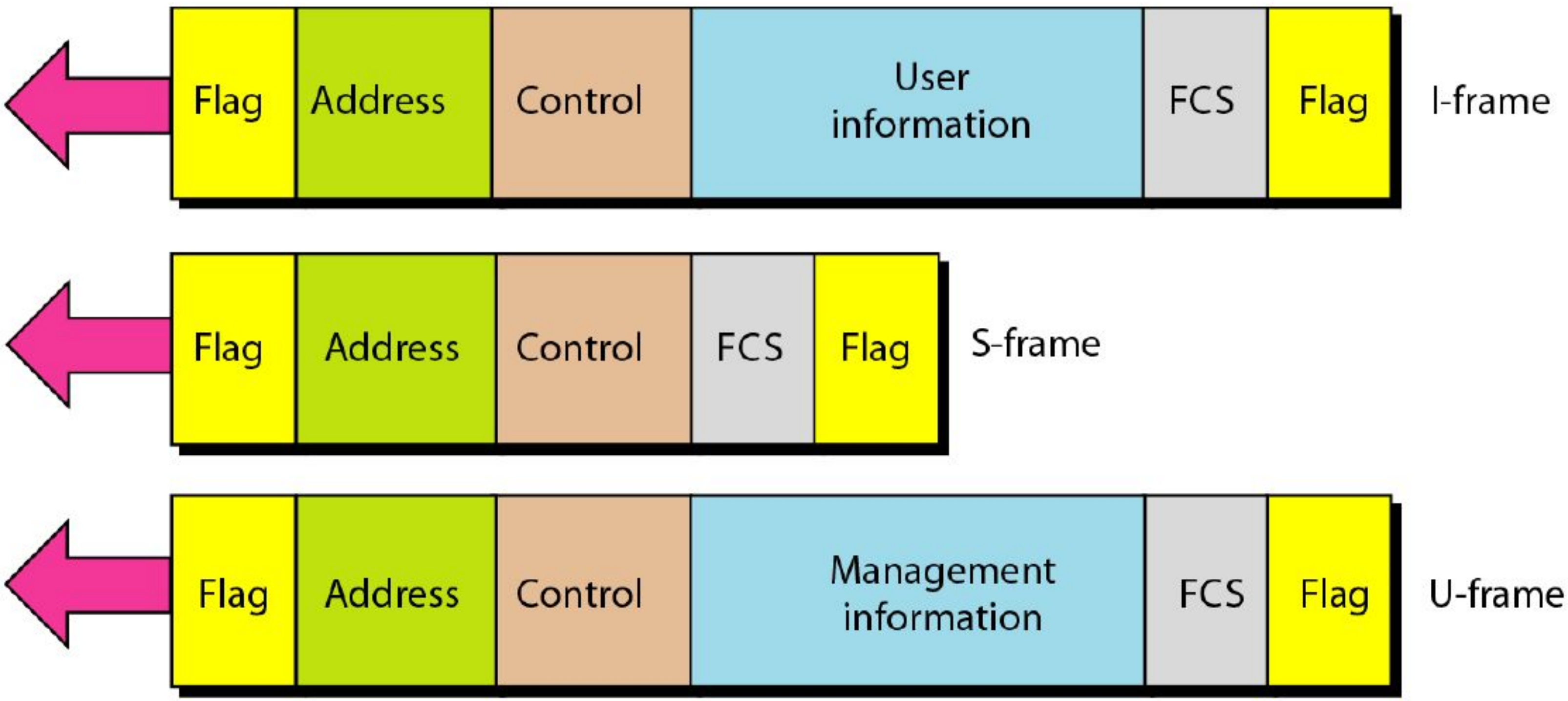
## HDLC FRAMES

- To provide the flexibility necessary to support all the options possible in the modes and configurations , HDLC defines three types of frames:

1. **Information Frames:** Used for transport of user data and control information.
2. **Supervisory Frames:** Used for transport of only control information.
3. **Unnumbered Frames:** Reserved for system management.

# HDLC

## *HDLC frames*

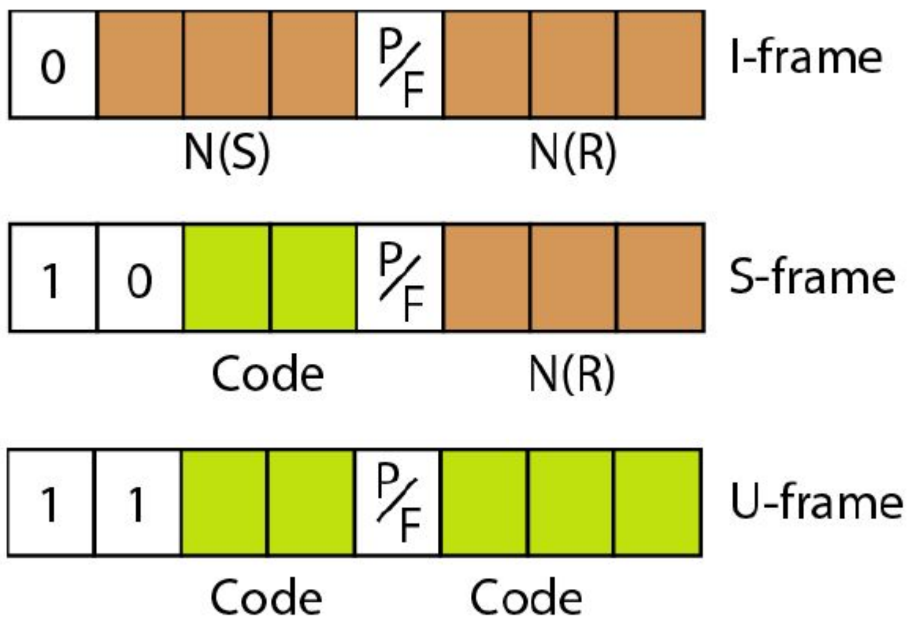


# HDLC

1. **Flag field:** The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame.
2. **Address field:** This field contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary creates the frame, it contains a from address.
3. **Control field:** The control field is a 1- or 2-byte segment of the frame used for flow and error control.
4. **Information field:** This field contains the user's data from the network layer or management information.
5. **FCS field:** The frame check sequence (FCS) is the HDLC error detection field.

# HDLC

## *Control field format for the different frame types*

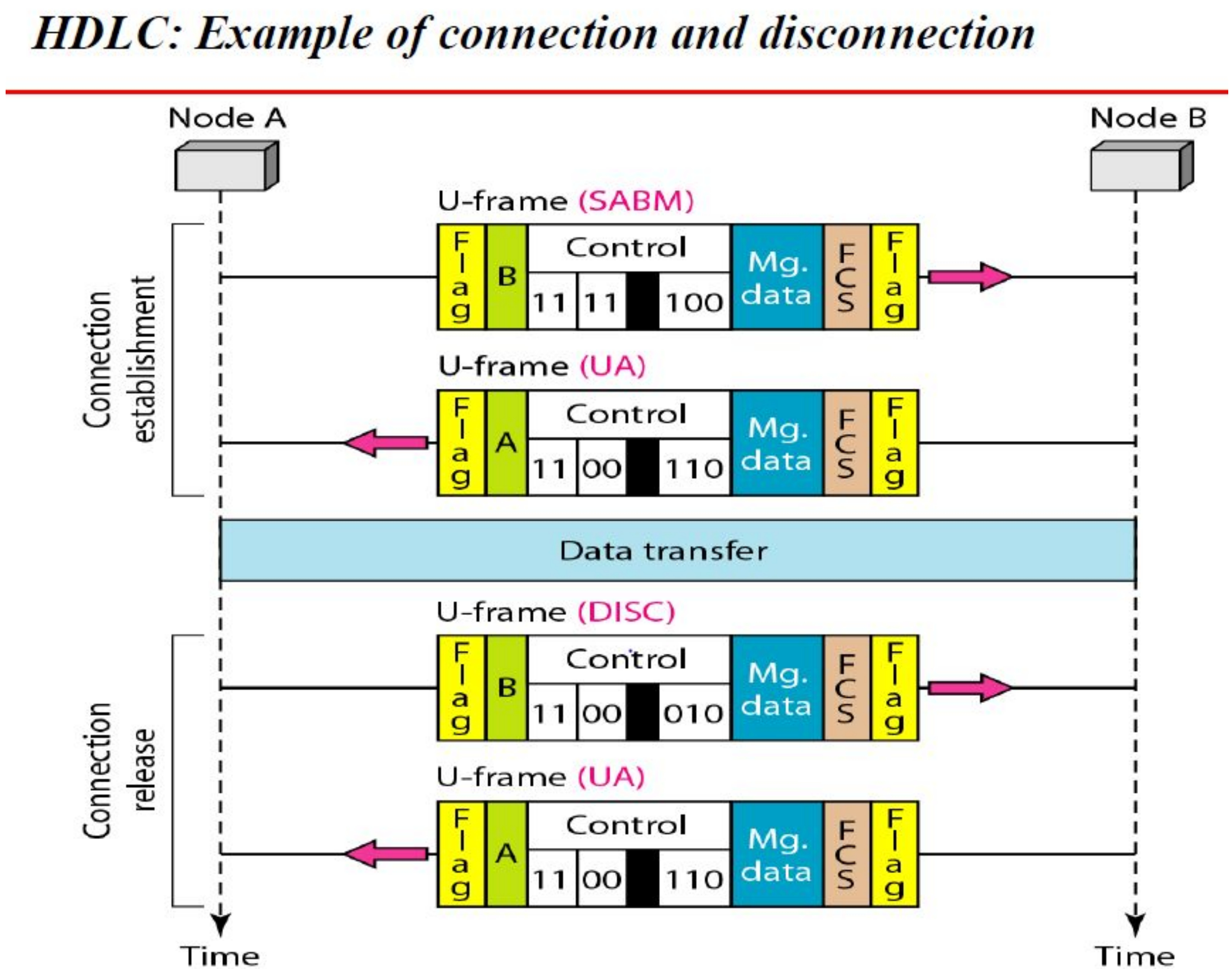


# HDLC

## *U-frame control command and response*

| *Code* | *Command* | *Response* | *Meaning* |
|---|---|---|---|
| **00 001** | SNRM | | Set normal response mode |
| **11 011** | SNRME | | Set normal response mode, extended |
| **11 100** | SABM | **DM** | Set asynchronous balanced mode or **disconnect mode** |
| **11 110** | SABME | | Set asynchronous balanced mode, extended |
| **00 000** | UI | **UI** | Unnumbered information |
| **00 110** | | **UA** | **Unnumbered acknowledgment** |
| **00 010** | DISC | **RD** | Disconnect or **request disconnect** |
| **10 000** | SIM | **RIM** | Set initialization mode or **request information mode** |
| **00 100** | UP | | Unnumbered poll |
| **11 001** | RSET | | Reset |
| **11 101** | XID | **XID** | Exchange ID |
| **10 001** | FRMR | **FRMR** | Frame reject |

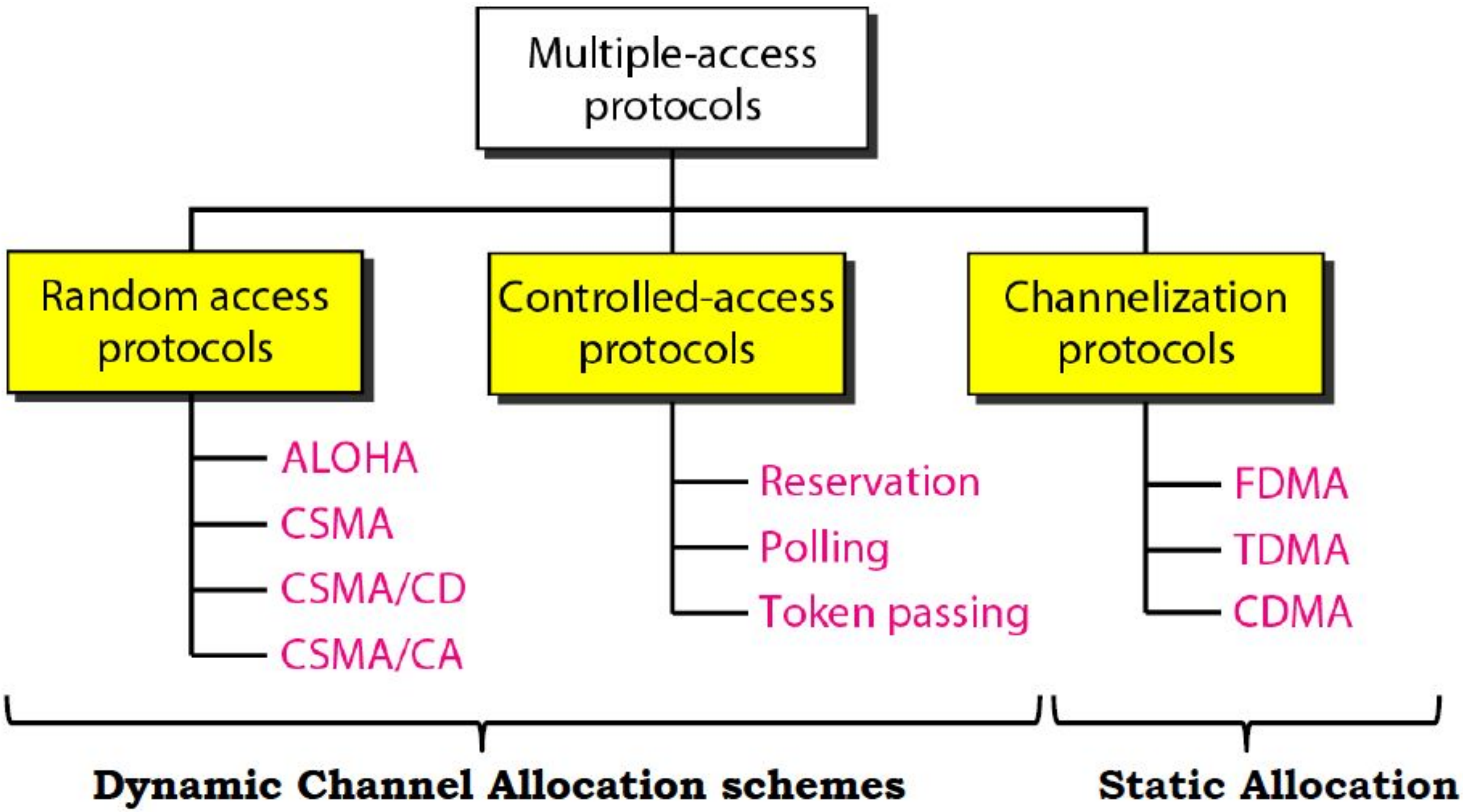
# HDLC


HDLC: Example of connection and disconnection
Node A
Node B
Connection establishment
U-frame (SABM)
Flag
B
Control
11
11
100
Mg. data
FCS
Flag
U-frame (UA)
A
11
00
110
Data transfer
Connection release
U-frame (DISC)
010
Time
Time

# MEDIUM ACCESS PROTOCOLS

- In networking usually devices share the links among the available devices
- The link between the devices is known as a ‘medium’.
- Thus it is important for any device on network, to check availability of medium before transmitting.

# MEDIUM ACCESS PROTOCOLS

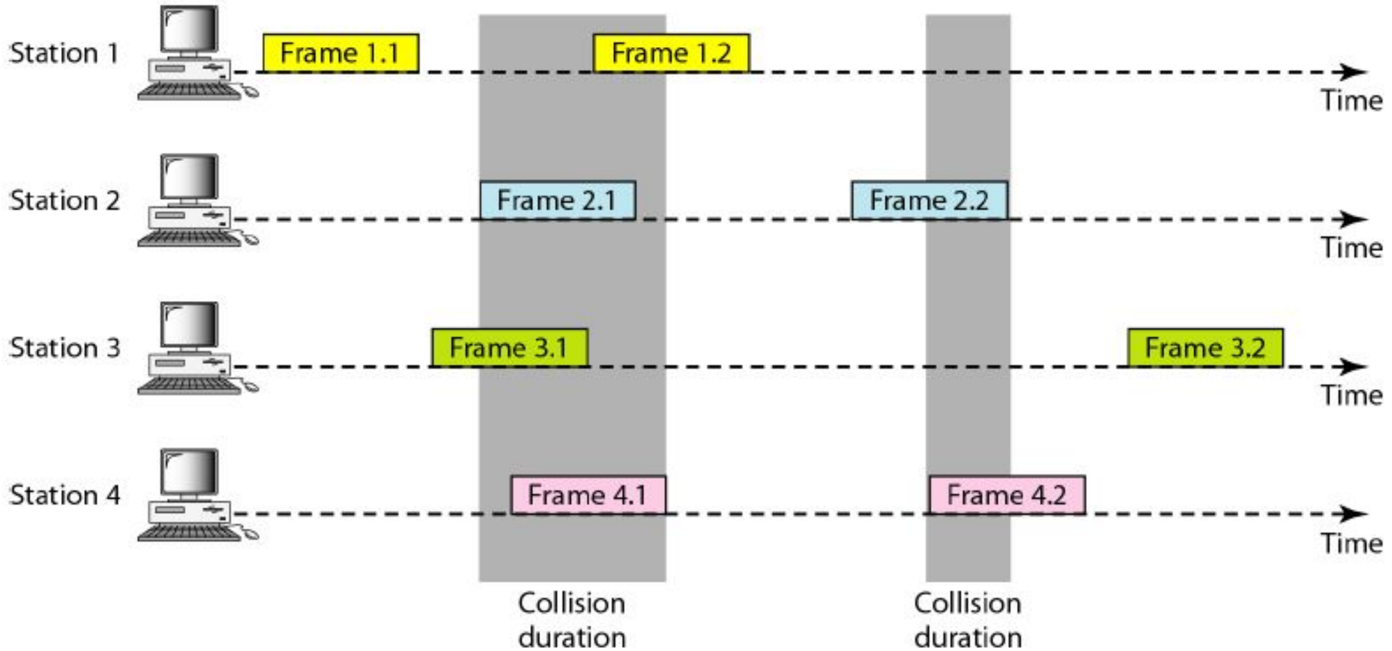


# RANDOM ACCESS PROTOCOLS

# ALOHA

**Pure ALOHA**

- The original ALOHA protocol is called pure ALOHA.
- The idea is that each station sends a frame whenever it has a frame to send.
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations.

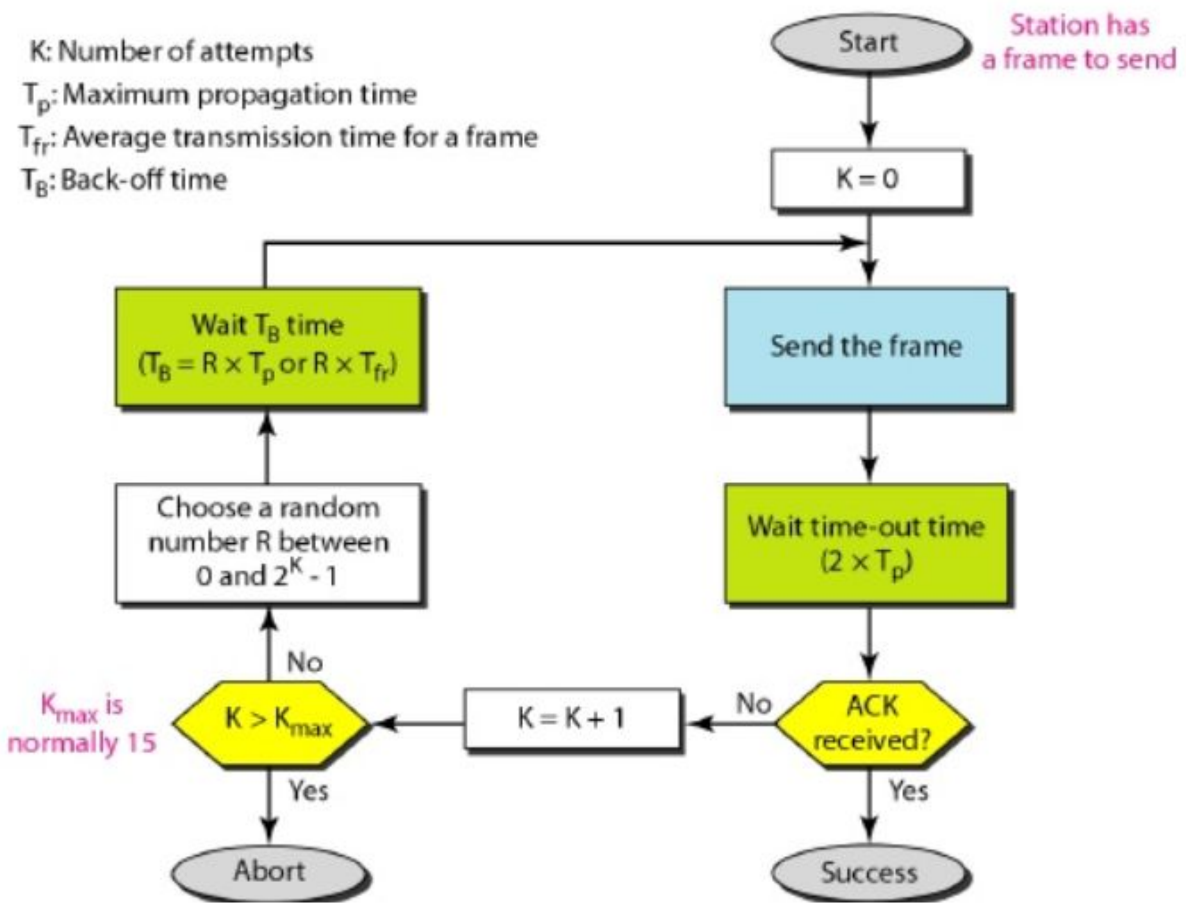


# PURE ALOHA

- When the frames collide, they are destroyed.
- Receiver sends ACK's for the lost frames.
- If sender does not receive an ACK for sent frame then he assumes loss of frame and resends the same.
- Now the chances of this stations colliding together while resending are even high.
- Pure ALOHA solves this problem by making each station wait a random amount of time before resending its frame
- This random time is called "back-off time".
- Another method to reduce congestion is, it sets limit on maximum number of retransmission attempts $K_{max}$ .
- If $K_{max}$ is reached a station must give up and try later

# ALOHA

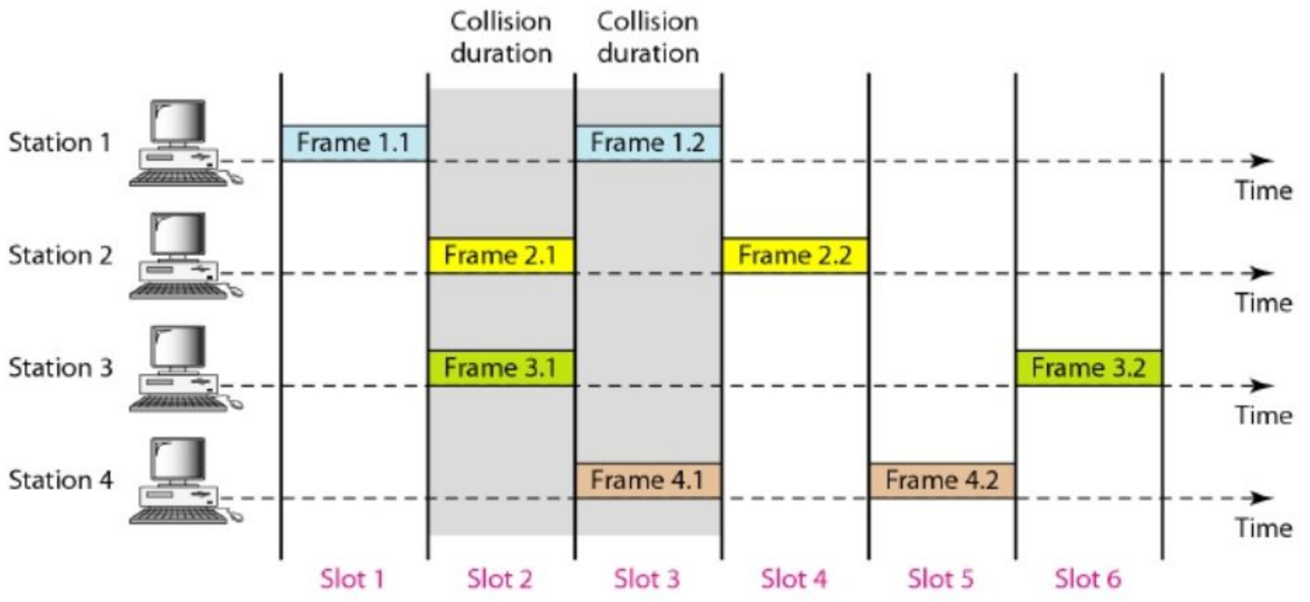
**Figure 12.4** ***Procedure for pure ALOHA protocol***



# SLOTTED ALOHA

- In Slotted ALOHA the time is divided into slots of $T_{fr}$ seconds and the stations are forced to send only at the beginning of the time slot.
- Because the stations are allowed to send only at the beginning of the time slot, collisions are reduced.
- The throughput of slotted ALOHA (37%) is double of the Pure ALOHA (18%).

**Figure 12.6** *Frames in a slotted ALOHA network*



# CSMA

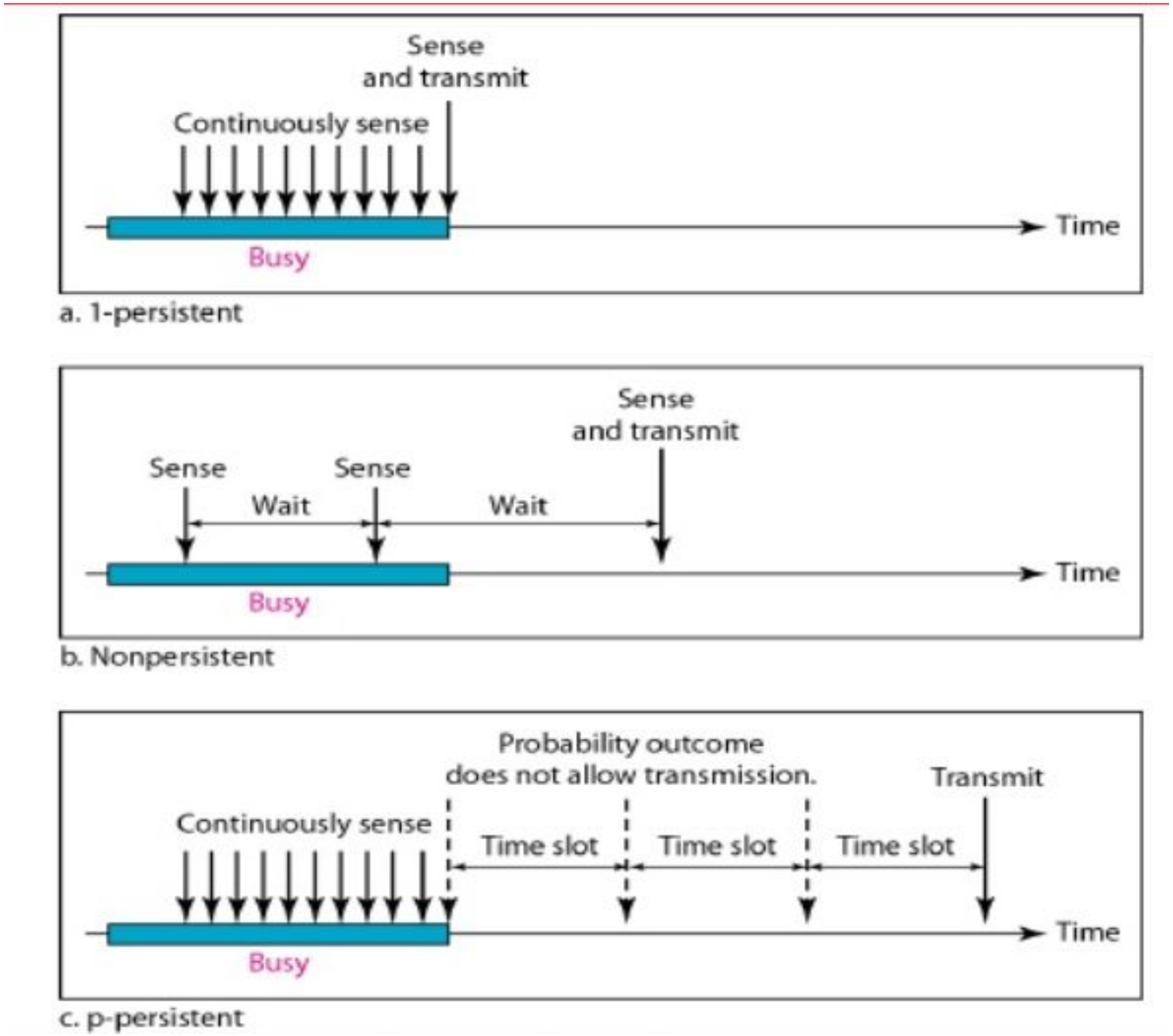
- The chance of collision is reduced if a station senses the medium before trying to use it .
- CSMA forces each station first to listen to the medium before sending data (carrier sense)
- Carrier sense methods:

1. I-Persistent CSMA
2. Non Persistent CSMA
3. P-Persistent CSMA

- The collisions still exists, if two stations transmit at the same time. The two types are:

1. With Collision Detection (CD)
2. With Collision Avoidance (CA)

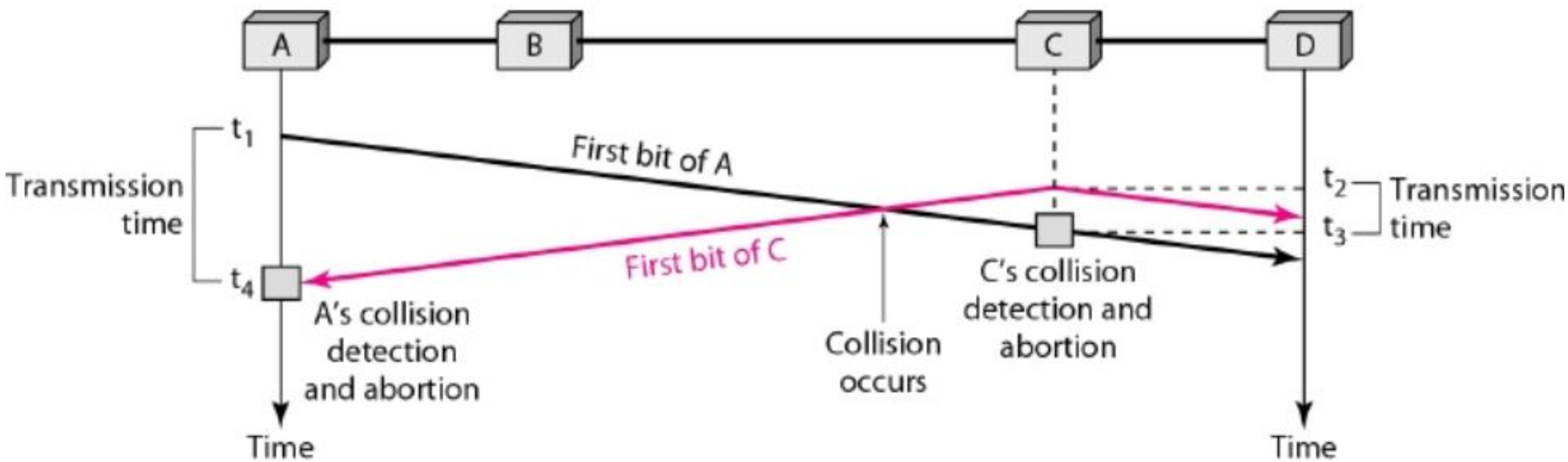
# PERSISTENT METHODS



# CSMA/CD

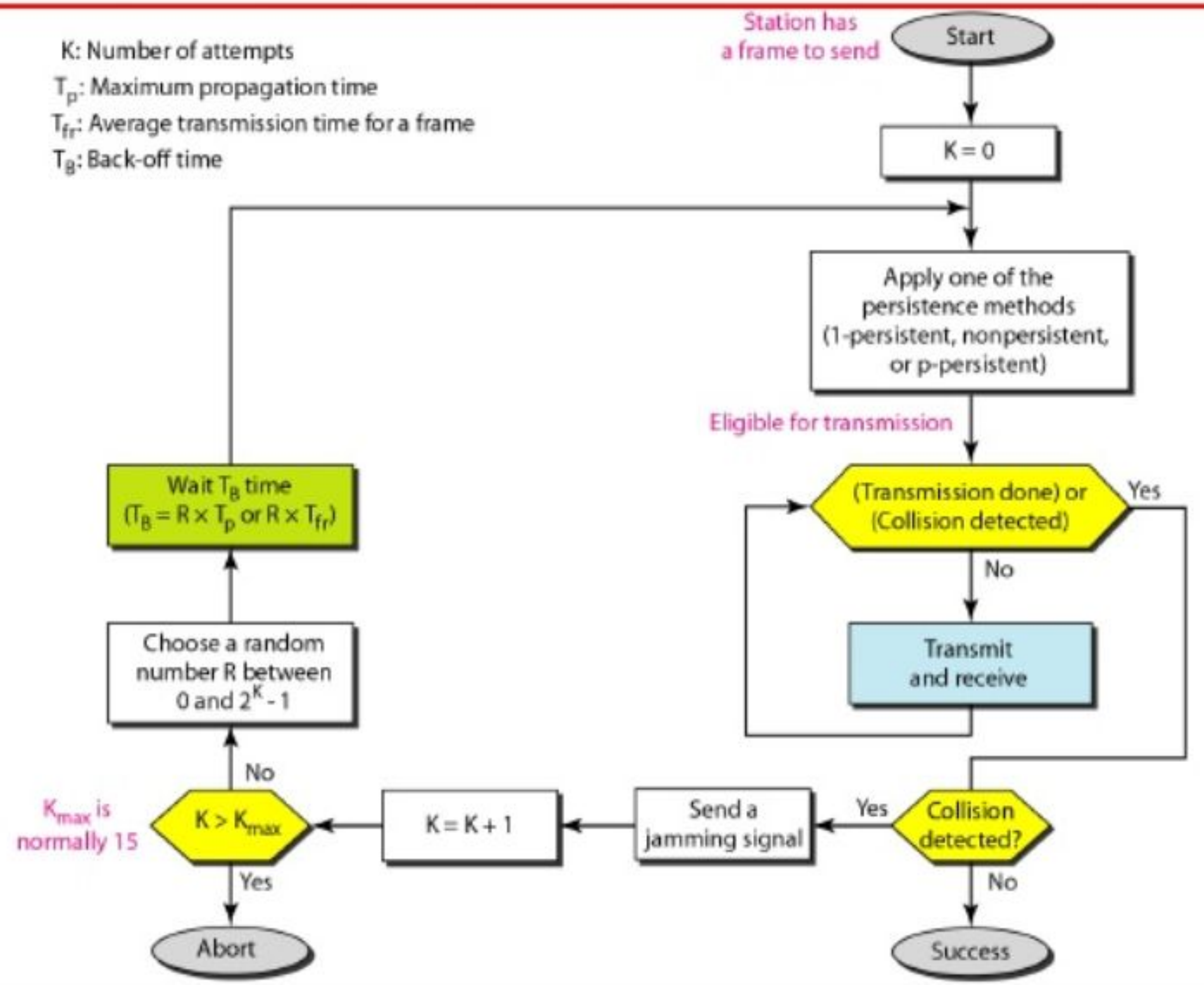
- In CSMA/CD, a station monitors the medium after it sends the frame to see if the transmission was successful.

**Figure 12.12** ***Collision of the first bit in CSMA/CD***



# CSMA/CD

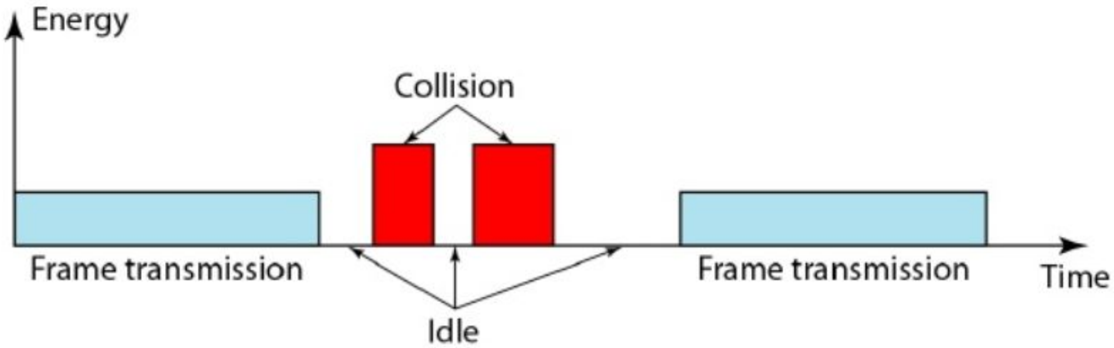
**Figure 12.14** *Flow diagram for the CSMA/CD*



# CSMA/CD

**Energy Level:**

- The level of energy in a channel has three values: Zero, normal and abnormal



# CSMA/CA

- CSMA/CA was invented for wireless networks.
- Collisions are avoided through the use of CSMA/CA's three strategies: Interframe Space, Contention window and Acknowledgement.

**Interframe Space (IFS)**

When an idle channel is found , the station does not send immediately, it waits for a period of time called the interframe space.

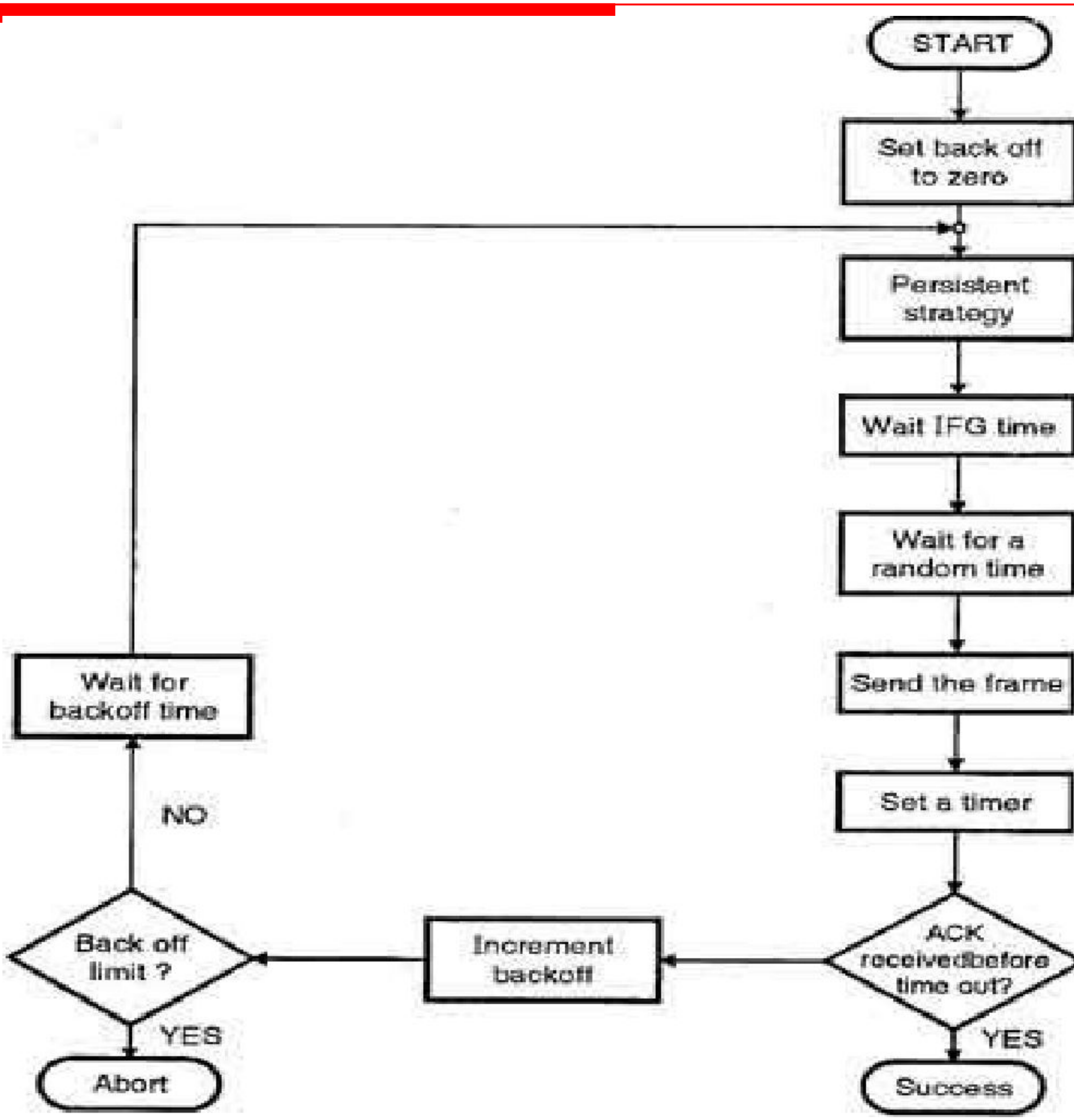
**Contention Window:**

The contention window is the amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.

**Acknowledgment:**

The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

# CSMA/CA


START
Set back off to zero
Persistent strategy
Wait IFG time
Wait for a random time
Send the frame
Set a timer
ACK received before time out?
YES
Success
Increment backoff
Back off limit ?
YES
Abort
NO
Wait for backoff time

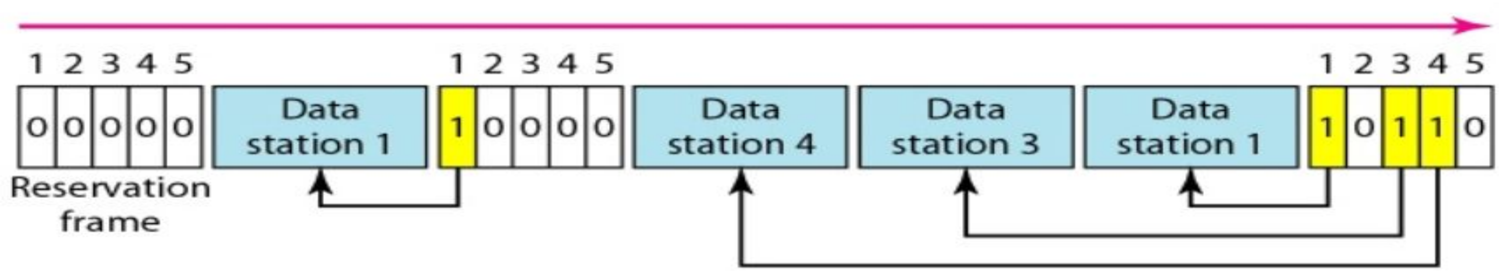
# CONTROLLED ACCESS PROTOCOLS

# CONTROLLED ACCESS

- In controlled access, the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.

## Reservation

- In this method, a station needs to make a reservation before sending data.
- Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.



# CONTROLLED ACCESS

**Polling**

- In Polling one device is designated as primary station and the other devices are secondary stations.
- The primary device controls the link. This method uses poll and select functions to prevent collisions.

**Select**

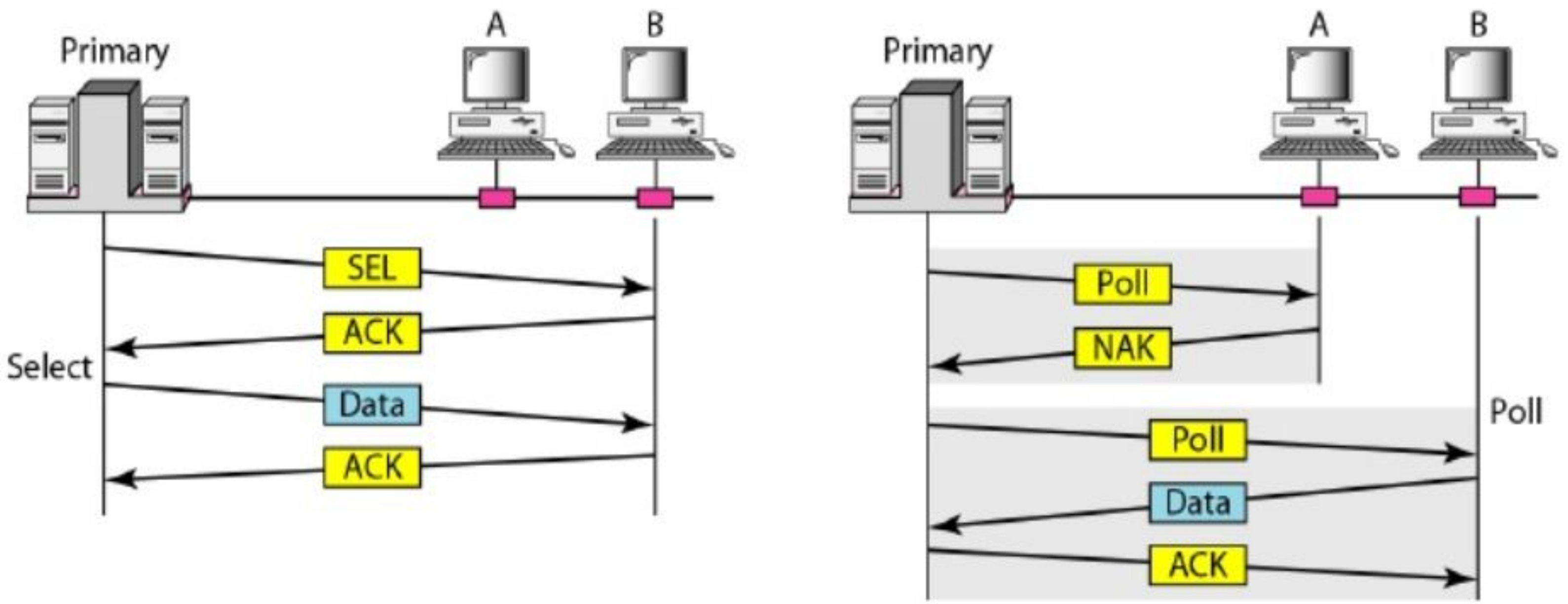
- The select function is used whenever the primary device has something to send.
- The primary station alerts the secondary station to the upcoming transmission.

**Poll**

- The poll function is used by primary station to solicit transmission from secondary devices.

# CONTROLLED ACCESS

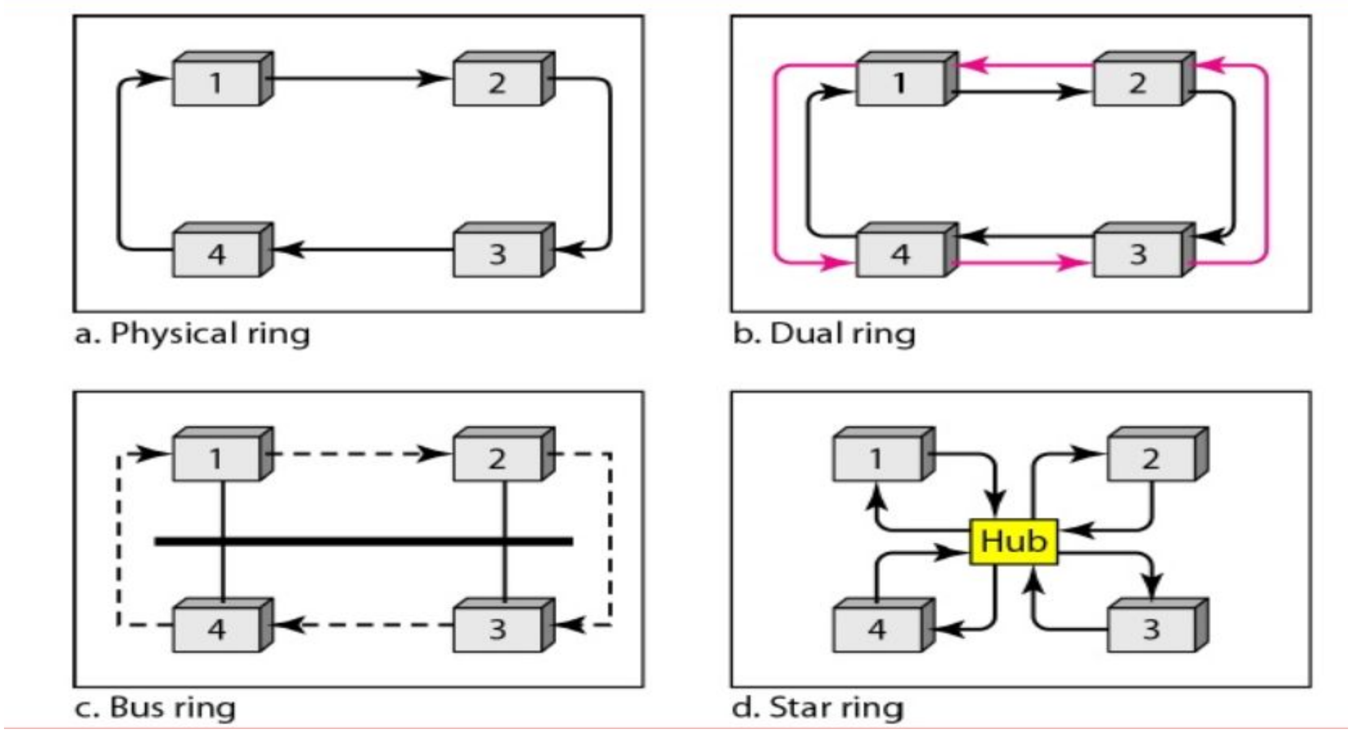
**Figure 12.19** ***Select and poll functions in polling access method***



# CONTROLLED ACCESS

## Token Passing

- In token passing method , the stations are organized in a logical ring. For each station there is a predecessor and a successor.
- The possession of the token gives the station the right to access the channel and send its data



# CHANNELIZATION PROTOCOLS

# CHANNELIZATION PROTOCOLS

- Channelization is a multiple access method in which the available bandwidth of a link is shared in time, frequency or through code among different stations.

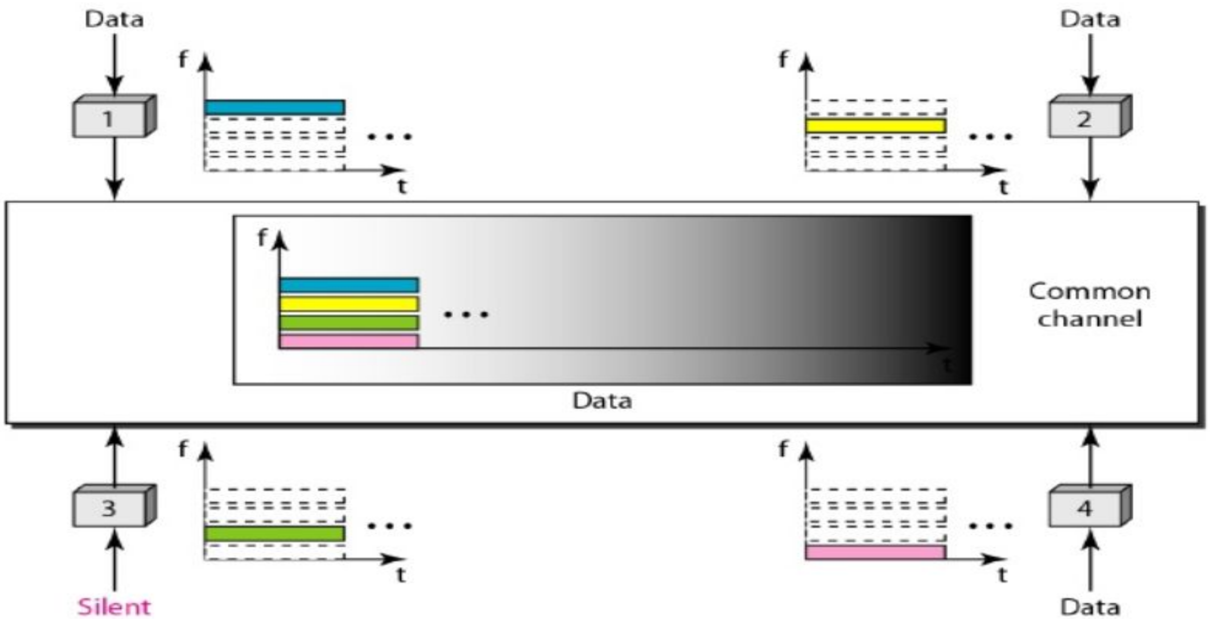
**Different Channelization protocols:**

1. Frequency Division Multiple Access (FDMA)
2. Time Division Multiple Access (TDMA)
3. Code Division Multiple Access (CDMA)

# FDMA

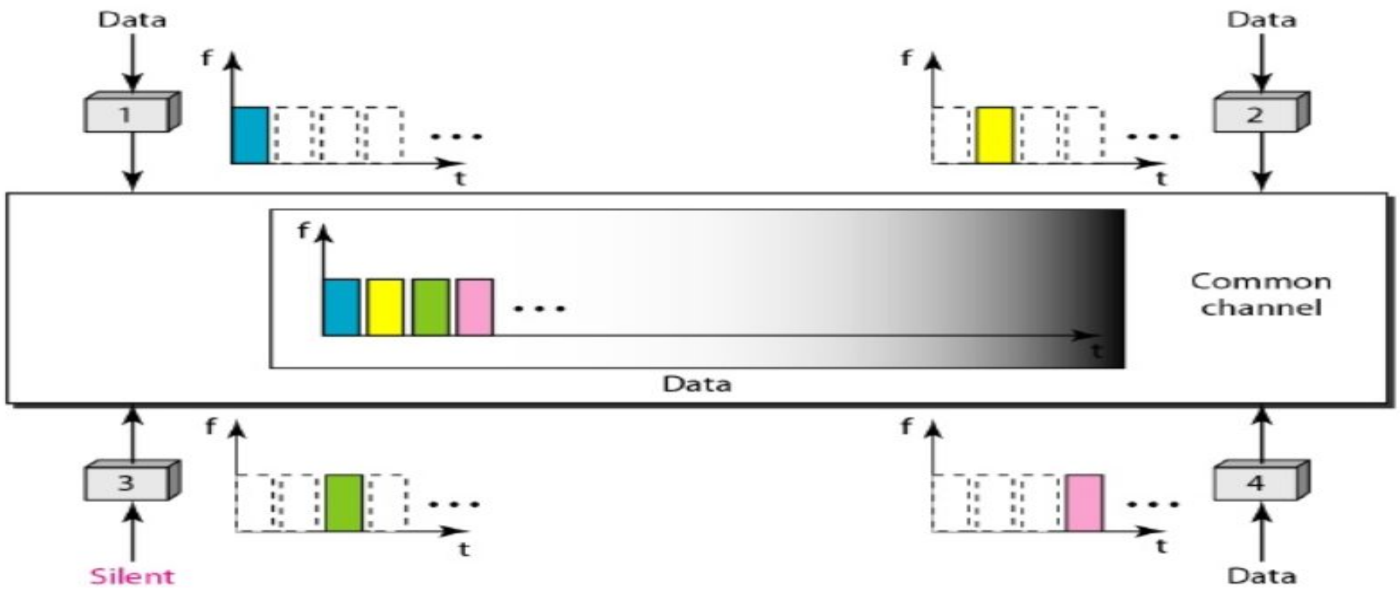
- In FDMA the available bandwidth is divided into frequency bands.
- Each station is allocated a band to send its data
- To prevent station interferences, the allocated bands are separated from one another by small guard bands

**Figure 12.21** ***Frequency-division multiple access (FDMA)***



# TDMA

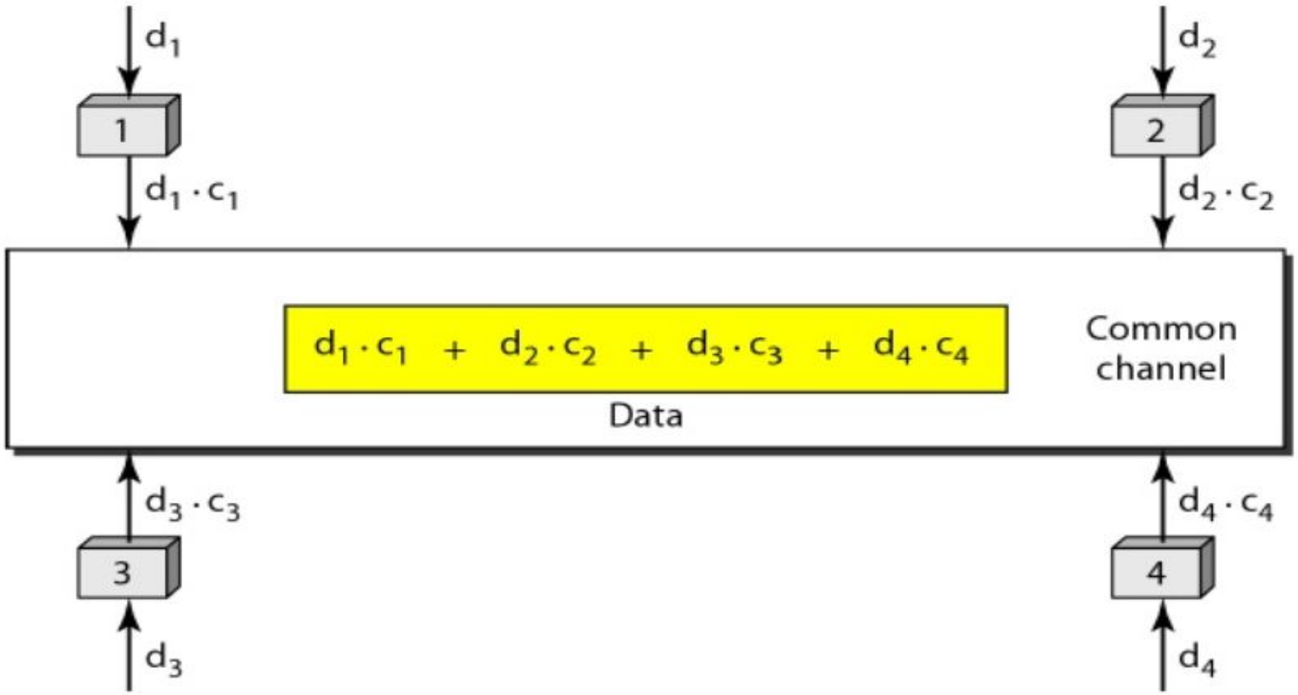
- In TDMA, the stations share the bandwidth of the channel in time.
- The main problem in TDMA is achieving synchronization between different stations.
- Synchronization is accomplished by having some synchronization bits at the beginning of each slot.



# CDMA

- In CDMA one channel carries all transmissions simultaneously.
- Codes have two properties:

1. If we multiply each code by another, we get 0
2. If we multiply each code by itself we get 4

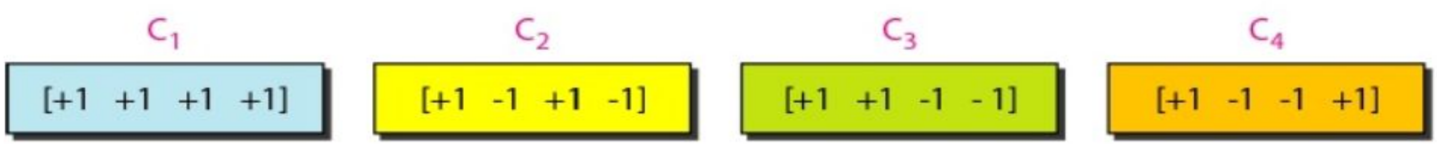


# CDMA

**Chips**

- The code assigned to each station is a sequence of numbers called chips.
- These sequences have the following properties:

1. Each sequence is made of N elements, where N is the number of stations.
2. If we multiply a sequence by a number , every element in the sequence is multiplied by that element.
3. If we multiply two equal sequences, element by element and add the results, we get N, where N is the number of elements in that sequence
4. If we multiply two different sequences, element by element and add the results, we get 0




**Data Representation:**

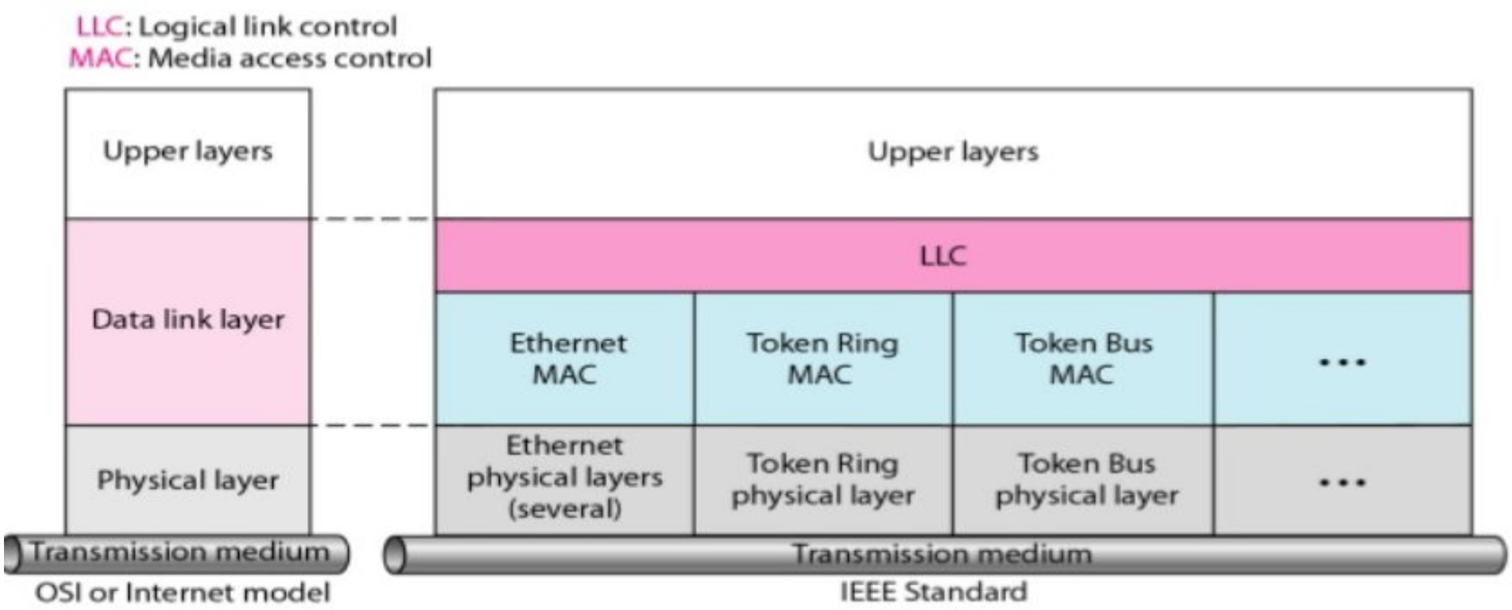
# ETHERNET PROTOCOL

# ETHERNET PROTOCOL

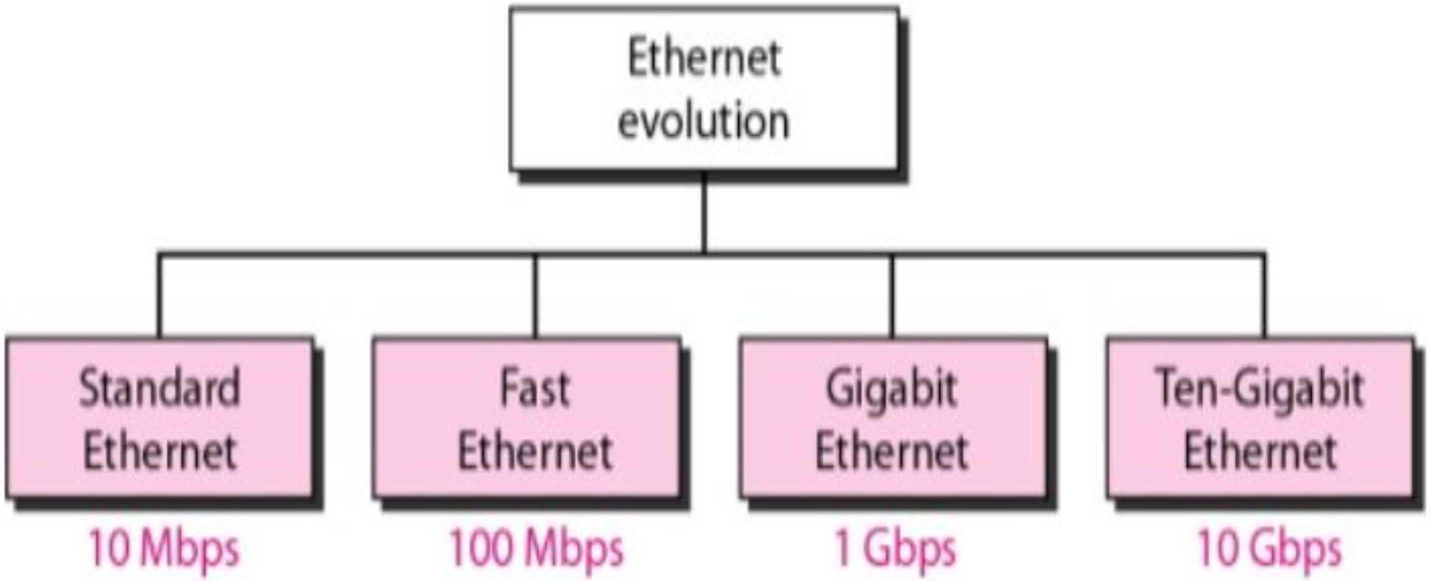
- A standard for wired LANs
- Defined by IEEE's project 802

**IEEE Project 802**

- Project 802 was started to enable intercommunication among equipment from a variety of manufacturers.
- It specifies functions of the physical layer and the data link layer of major LAN protocols.



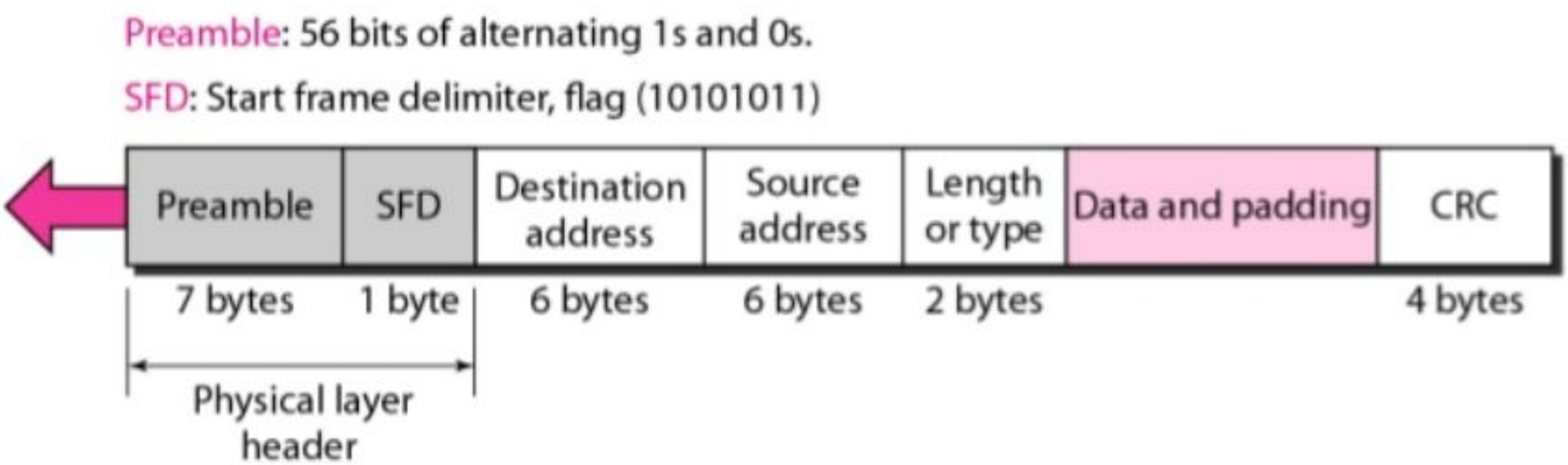
# ETHERNET EVOLUTION



# STANDARD ETHERNET

- The original Ethernet technology with the data rate of 10Mbps is referred to as Standard Ethernet.

**Frame Format:**



# STANDARD ETHERNET

**Frame Length:**

- Ethernet has imposed restrictions on both minimum and maximum length of a frame.
- An Ethernet frame needs to have a minimum length of 64 bytes. The minimum data length is 46 bytes.
- The standard defines the maximum length of a frame as 1518 bytes. The maximum data length is 1500 bytes.

# STANDARD ETHERNET

**Addressing:**

- Each station on Ethernet network has its own NIC. The NIC fits into the station and provide the station with a link layer address.
- The Ethernet address is 6 bytes, and is written in hexadecimal notation.

**4A:30:10:21:10:1A**

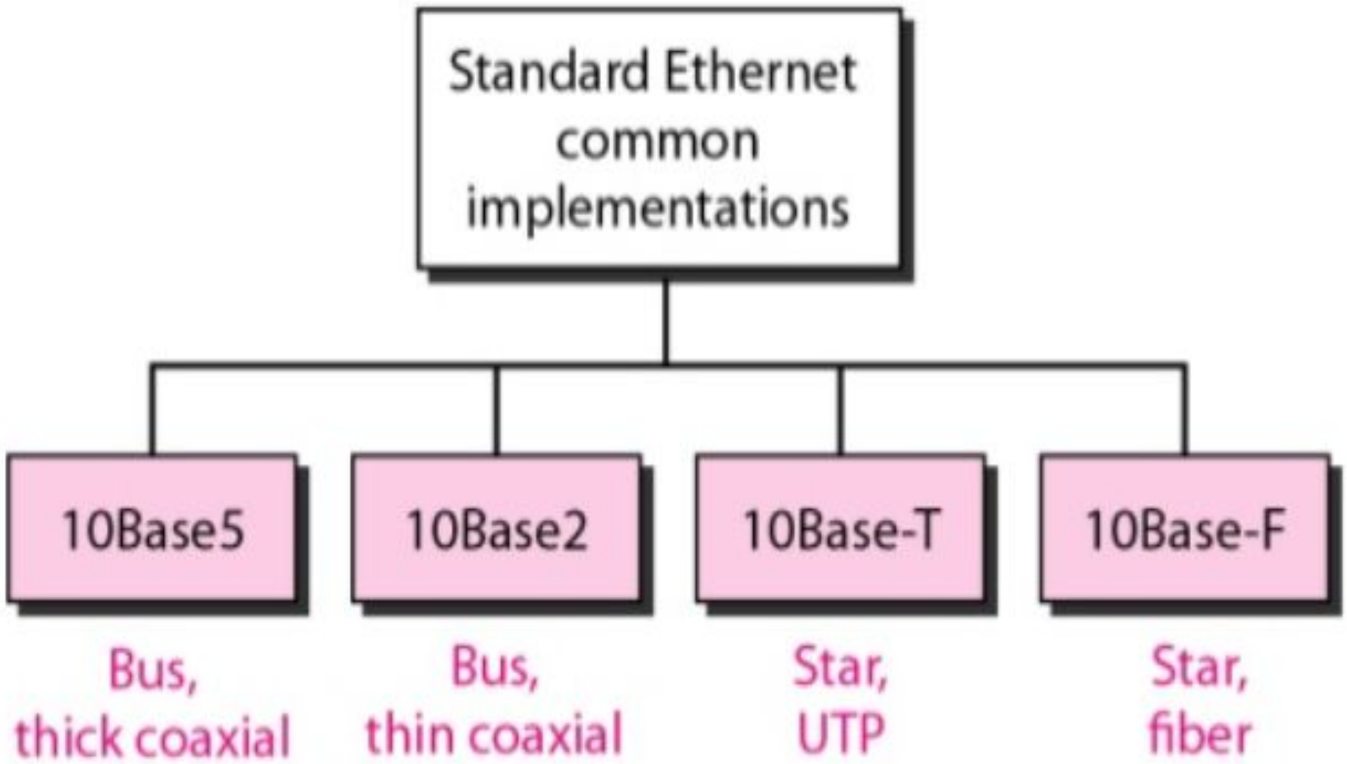
- A source address is always unicast, the destination address can be unicast, multicast or broadcast.

# STANDARD ETHERNET

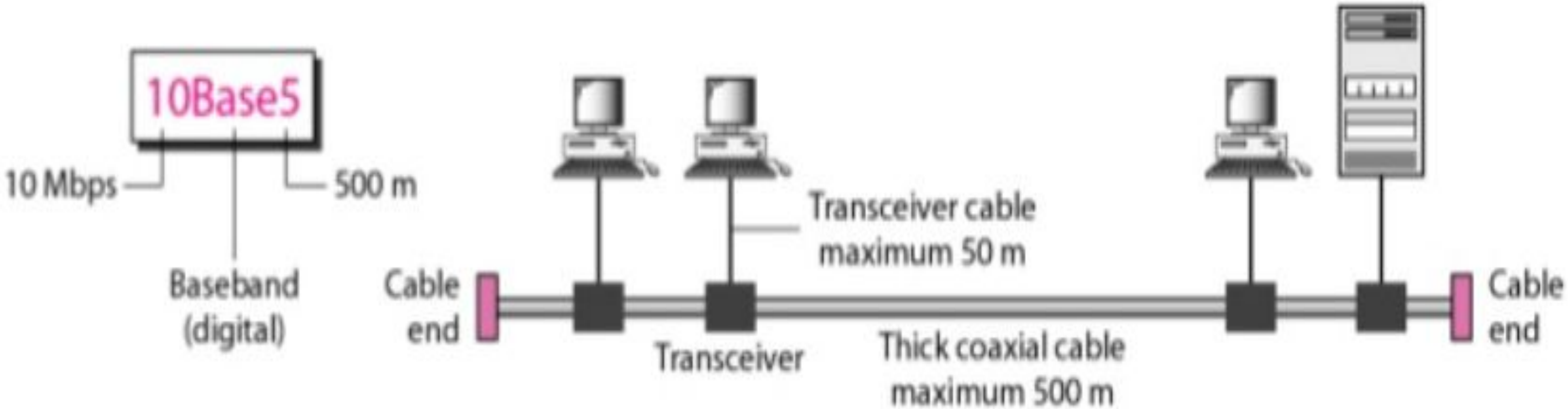
- The standard Ethernet uses CSMA/CD with I-persistent method to control access to the sharing medium.
- Efficiency of the Ethernet is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station.

$$\text{Efficiency}=1/(1+64*a)$$

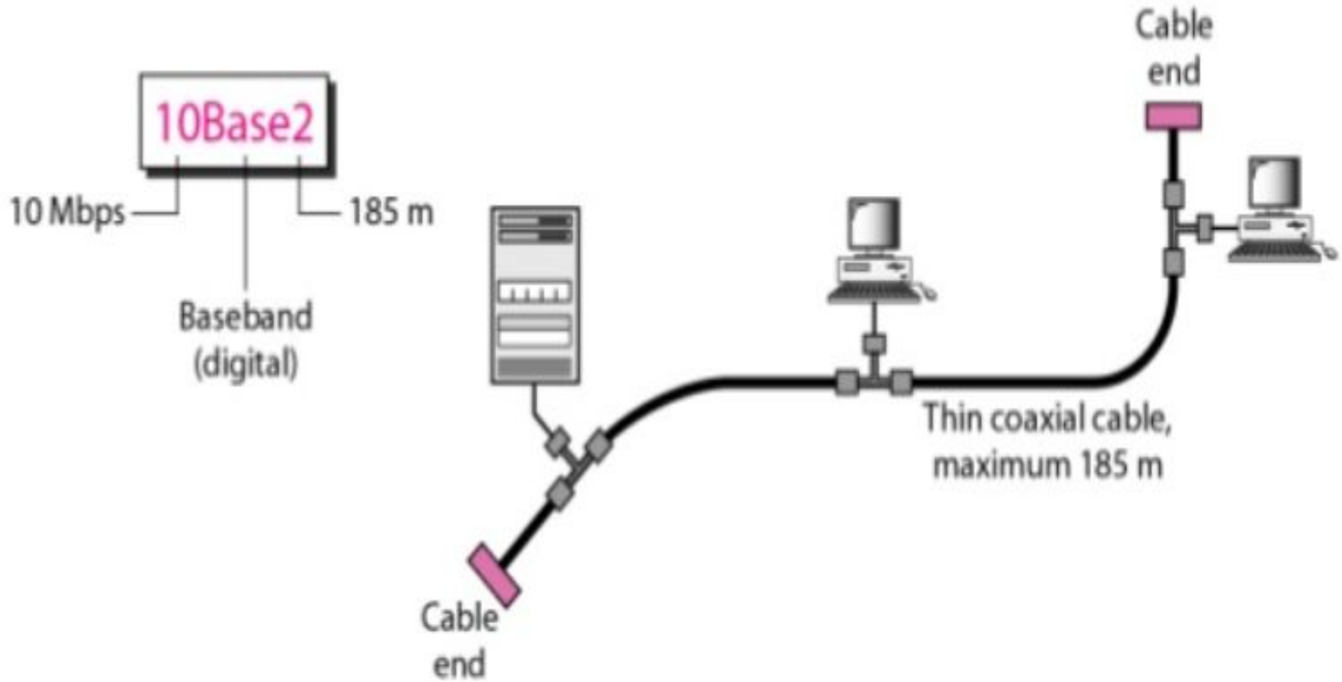
# STANDARD ETHERNET



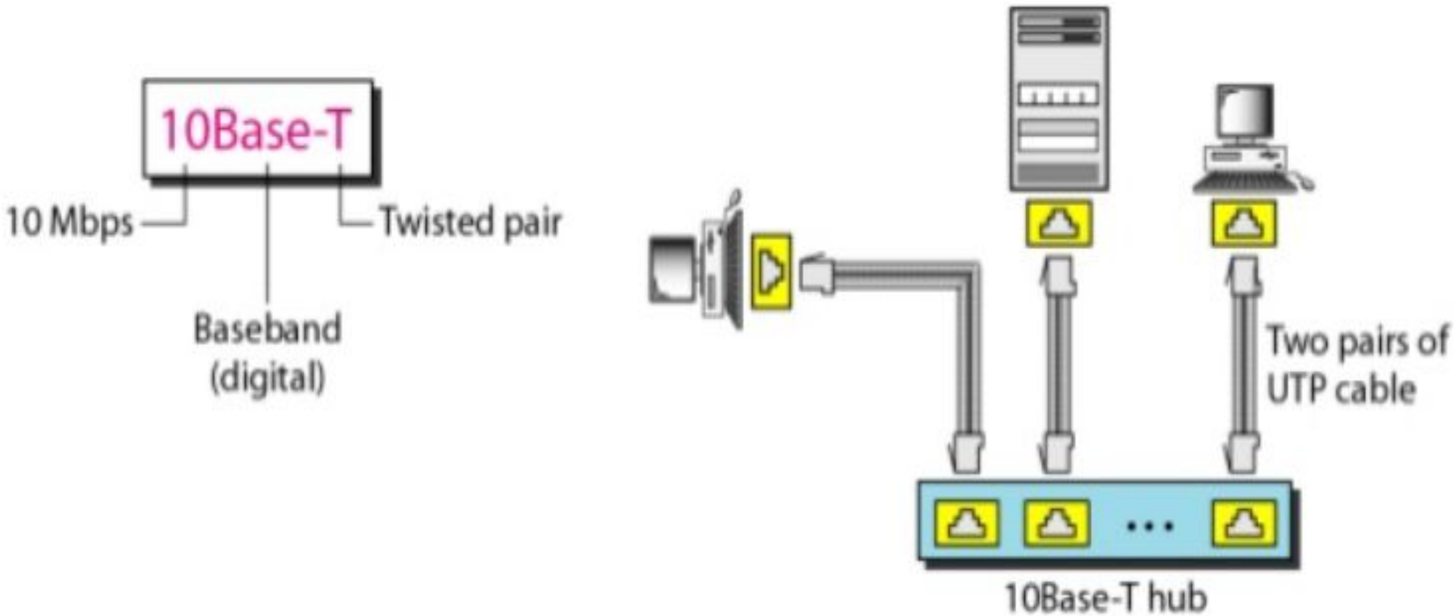
# 10Base5 IMPLEMENTATION



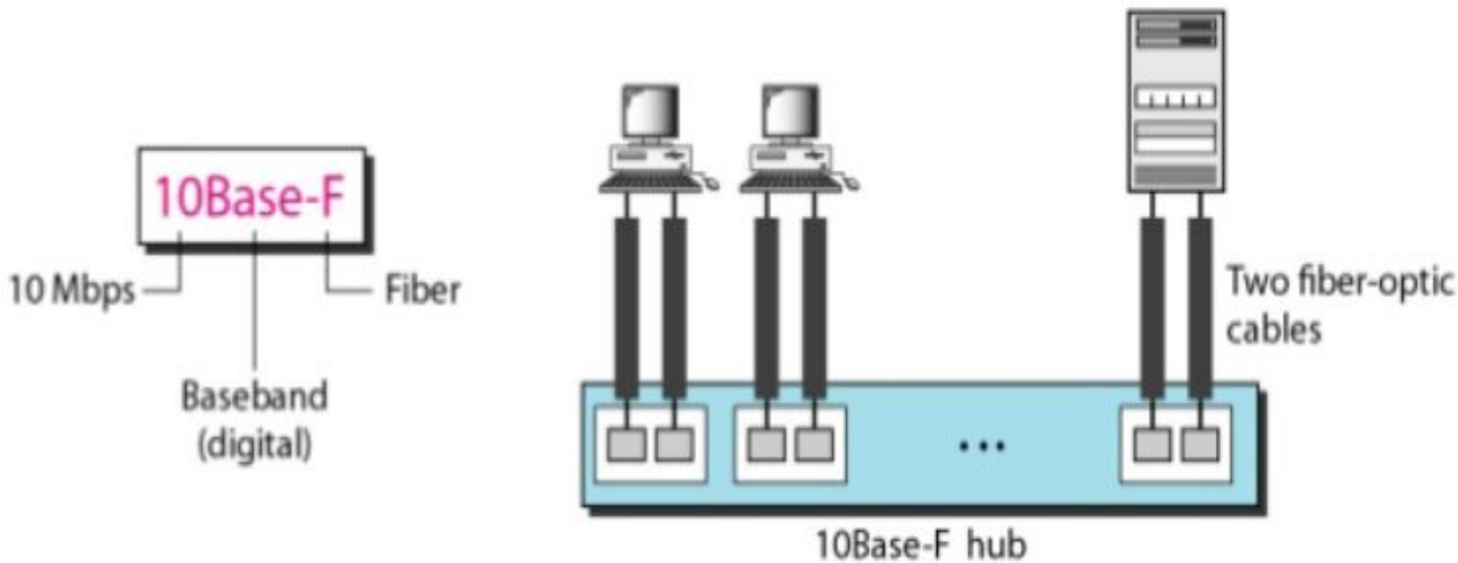
# 10Base2 IMPLEMENTATION



# 10Base-T IMPLEMENTATION



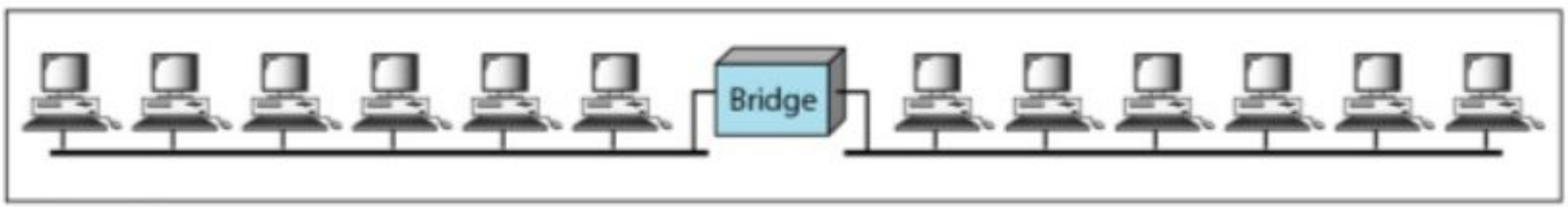
# 10Base-F IMPLEMENTATION



# BRIDGED ETHERNET

- The first step in Ethernet evolution is division of LAN by bridges.
- Bridges have two effects on an Ethernet LAN: They raise the bandwidth and they separate the collision domains.

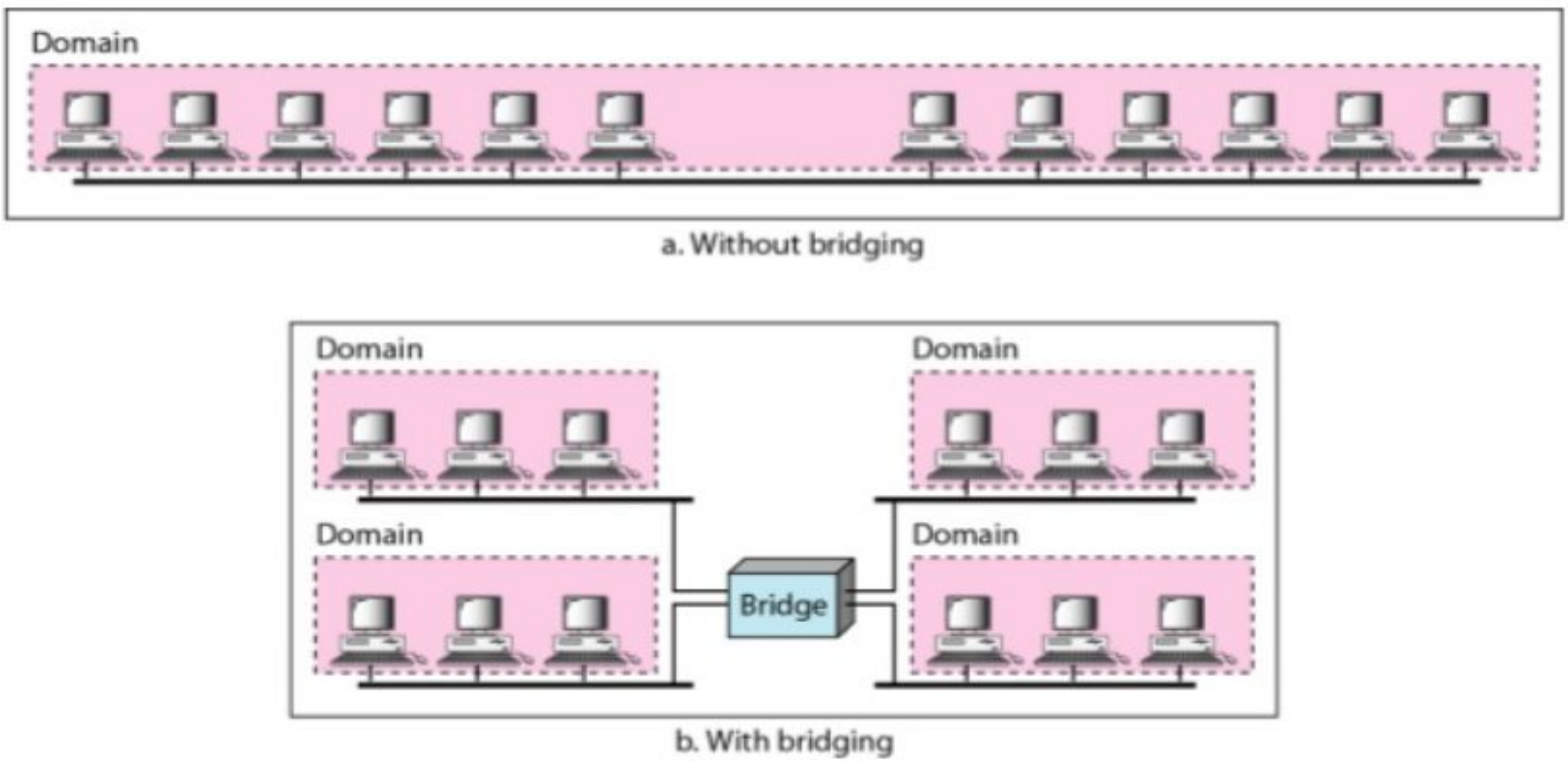
a. Without bridging



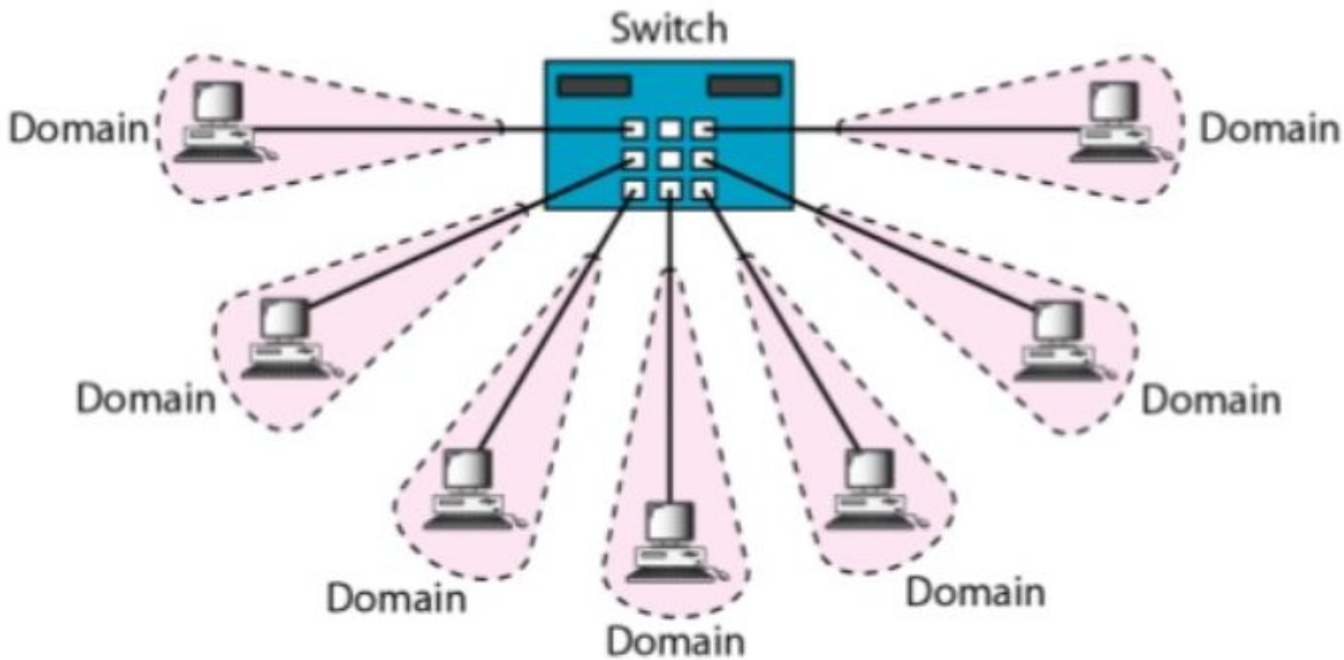

b. With bridging

# BRIDGED ETHERNET

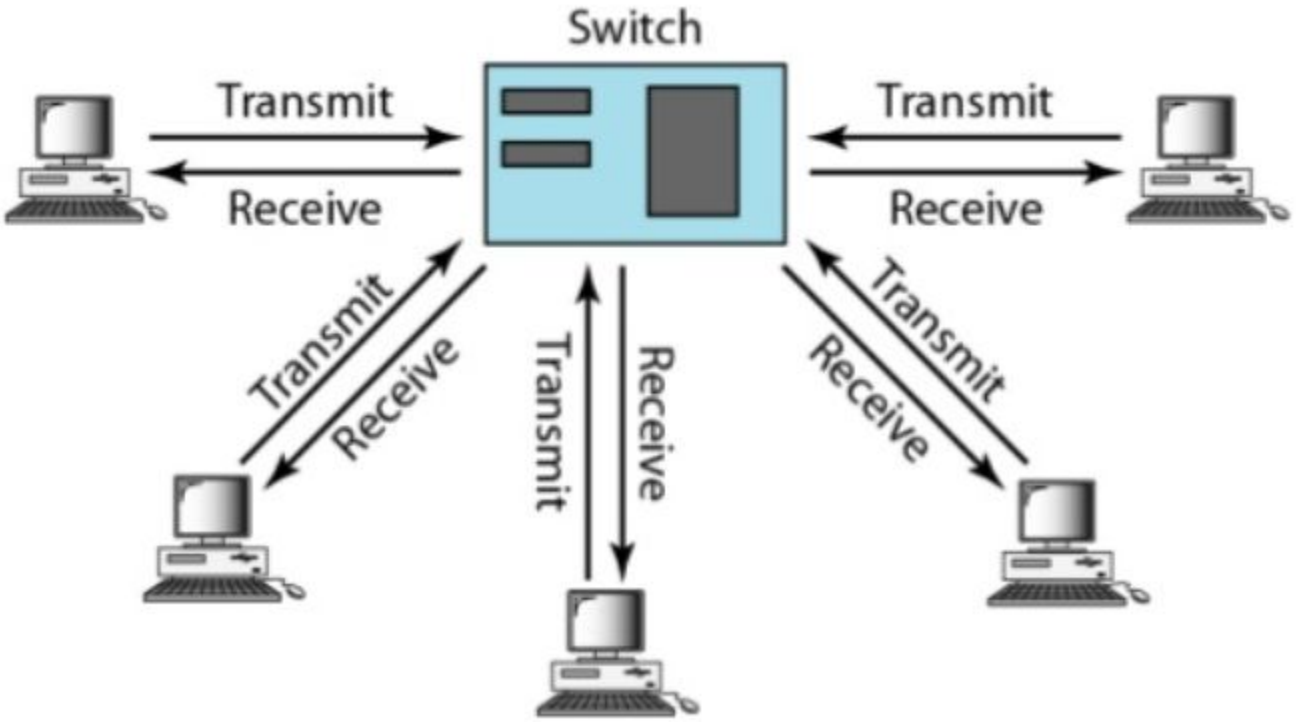
**Figure 13.16** ***Collision domains in an unbridged network and a bridged network***



# SWITCHED ETHERNET



# FULL DUPLEX ETHERNET



# FAST ETHERNET

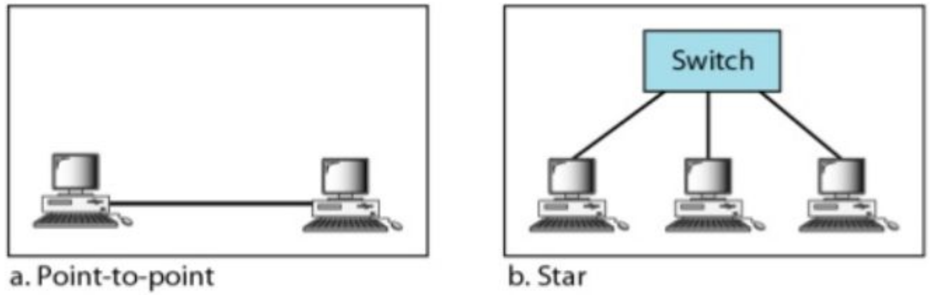
Goals of Fast Ethernet:

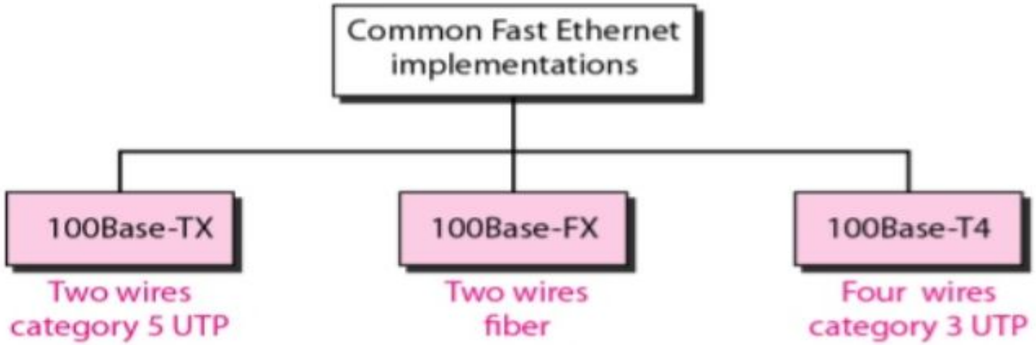
1. Upgrade the data rate to 100 Mbps
2. Make it compatible with Standard Ethernet
3. Keep the same 48-bit Address
4. Keep the same frame format

- If the frame size is still 512 bits, and it is transmitted 10 times faster, the collision needs to be detected 10 times sooner, which means that the maximum length of the network should be 10 times shorter.

# FAST ETHERNET

**Figure 13.19** ***Fast Ethernet topology***

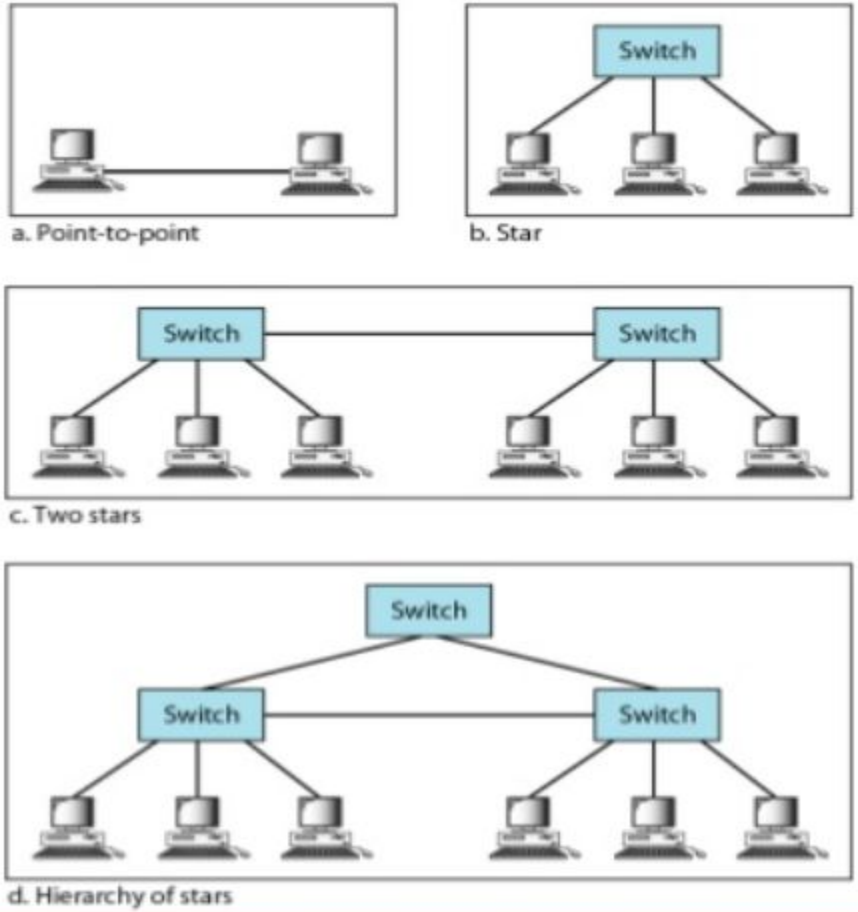


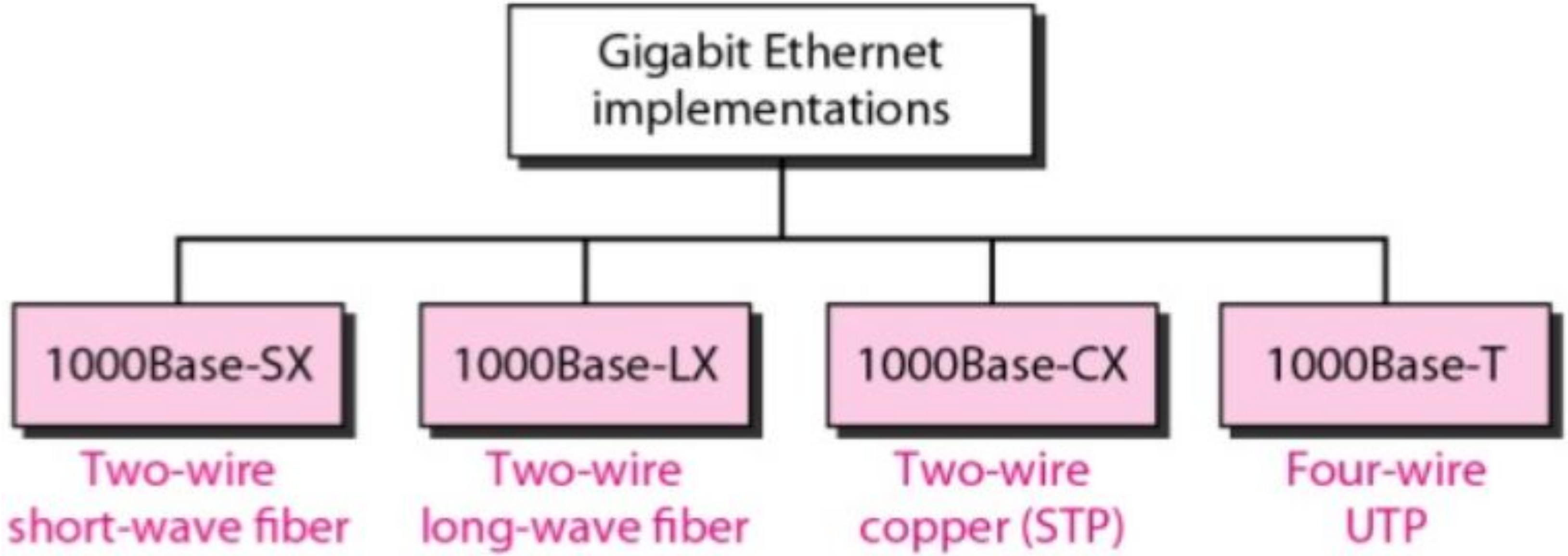
# GIGABIT ETHERNET

- In Full Duplex mode of Gigabit Ethernet, there is no collision.

**Figure 13.22** ***Topologies of Gigabit Ethernet***



# GIGABIT ETHERNET



# 10-GIGABIT ETHERNET

The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM

Table 13.4 *Summary ofTen-Gigabit Ethernet implementations*

| *Characteristics* | *lOGBase-S* | *lOGBase-L* | *lOGBase-E* |
|---|---|---|---|
| Media | Short-wave<br>S50-nrn<br>rnultimode | Long-wave<br>131O-nrn<br>single mode | Extended<br>1550-mrn<br>single mode |
| Maximum length | 300m | 1Okm | 40km |

# Thank you …