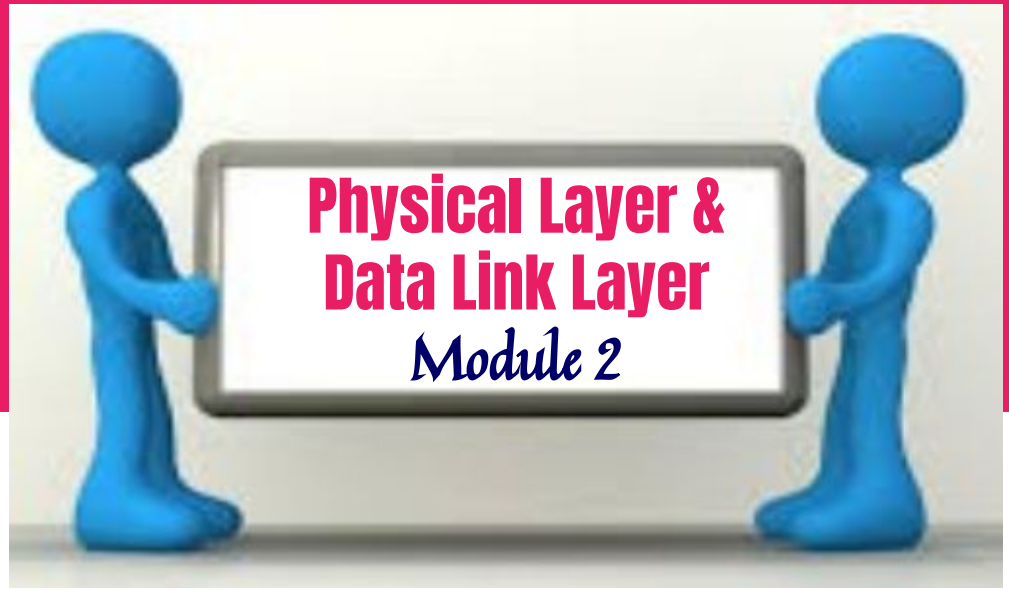

Physical Layer &
Data Link Layer
Module 2

Data Link Layer

Data Link Layer Functions

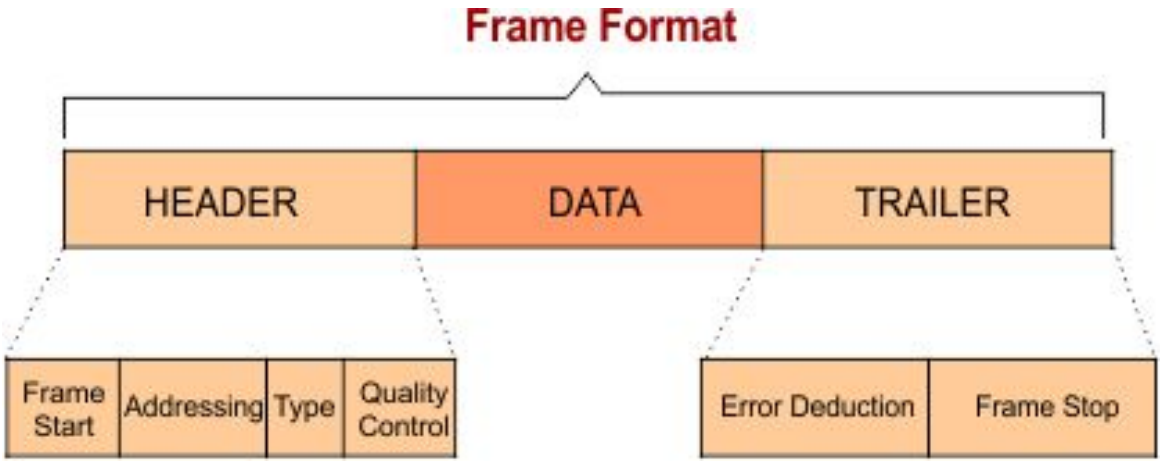
- Hop to hop delivery
  - Data Link Layer can be delivery of packets from the host's network interface card(NIC) to the router's interface or it can be delivery of packets from one router's interface to another router's interface or it can be delivery of packets from one router's interface to host's network interface card(NIC). It does not directly deliver the packets from source to destination instead delivers them from one hop(node) to another.
  - If we are in the same network, then hop to hop communication takes place by layer-2 devices such as switches, bridges, etc

- Flow control
  - It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver
  - Methods of Flow Control are Stop-and-wait , and Sliding window.
- Error control
  - Error Control is a combination of both error detection and error correction of frames that are rames that have been corrupted or lost during transmission.
  - It ensures that the data received at the receiver end is the same as the one sent by the sender.

- Data link layer follows a technique to detect transit errors and take necessary actions, which is retransmission of frames whenever error is detected or frame is lost. The process is called Automatic Repeat Request (ARQ).
  - Error Control Techniques
    - Stop and Wait ARQ
    - Go-Back-N ARQ
    - Selective Repeat ARQ
  - Error Detection Techniques: Parity Check, Checksum and Cyclic Redundancy Check (CRC).

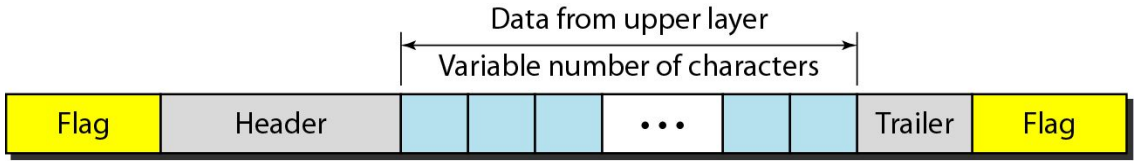
- Media access control
    - CSMA/ CD, Aloha, Slotted Aloha, Token Ring
- Physical Addressing
- Framing

Data link layer PDU



Framing

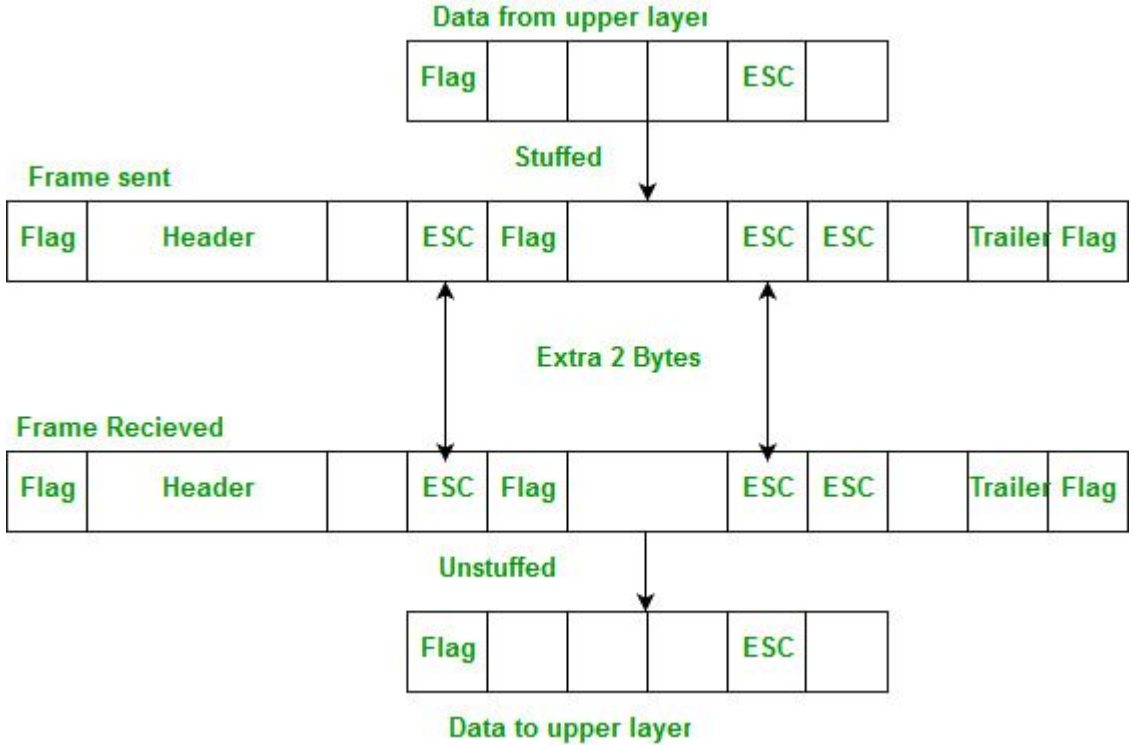
- The data link layer needs to pack bits into frames, so that each frame is **distinguishable** from another.
- Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the **delimiter**.



Framing

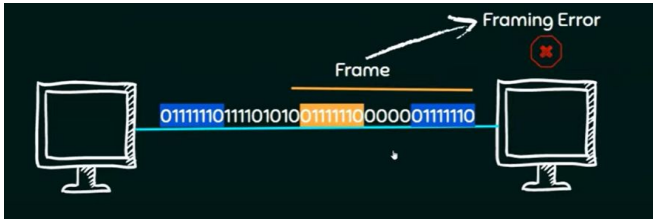
- Character Stuffing Approach
- Bit Stuffing Approach
- Insertion of Time Gaps
- Character Count

- Character Stuffing Approach

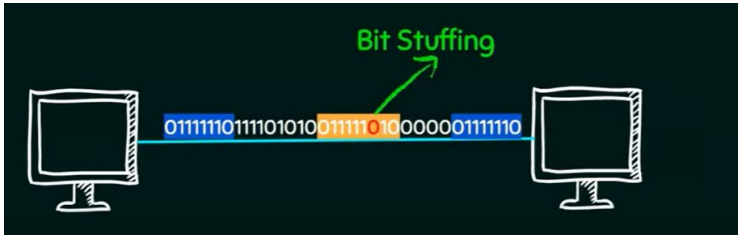


- Bit Stuffing Approach
  - In HDLC, flag of 01111110 is appended

Problem



Solution is bit stuffing



Error Control

- Error control can be done in two ways
  - Error detection − Error detection involves checking whether any error has occurred or not. The number of error bits and the type of error does not matter.
  - Error correction − Error correction involves ascertaining the exact number of bits that has been corrupted and the location of the corrupted bits.
- For both error detection and error correction, the sender needs to send some additional bits along with the data bits.
- The receiver performs necessary checks based upon the additional redundant bits. If it finds that the data is free from errors, it removes the redundant bits before passing the message to the upper layers.

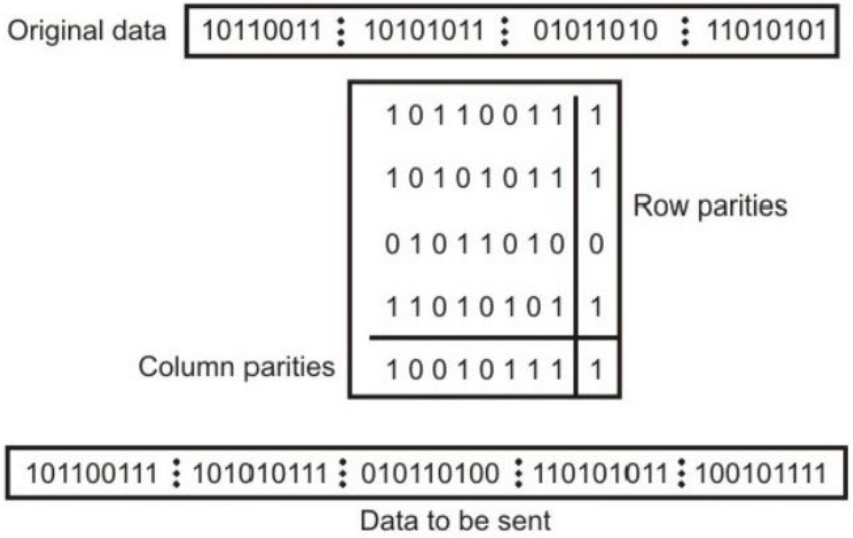
Error Detection Techniques

- **Parity Check**
  - The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity.
  - In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
  - In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

One bit Parity

Original Data	Even Parity	Odd Parity
0 0 0 0 0 0 0 0	0	1
0 1 0 1 1 0 1 1	1	0
0 1 0 1 0 1 0 1	0	1
1 1 1 1 1 1 1 1	0	1
1 0 0 0 0 0 0 0	1	0
0 1 0 0 1 0 0 1	1	0

2D Parity



Parity Bit Check

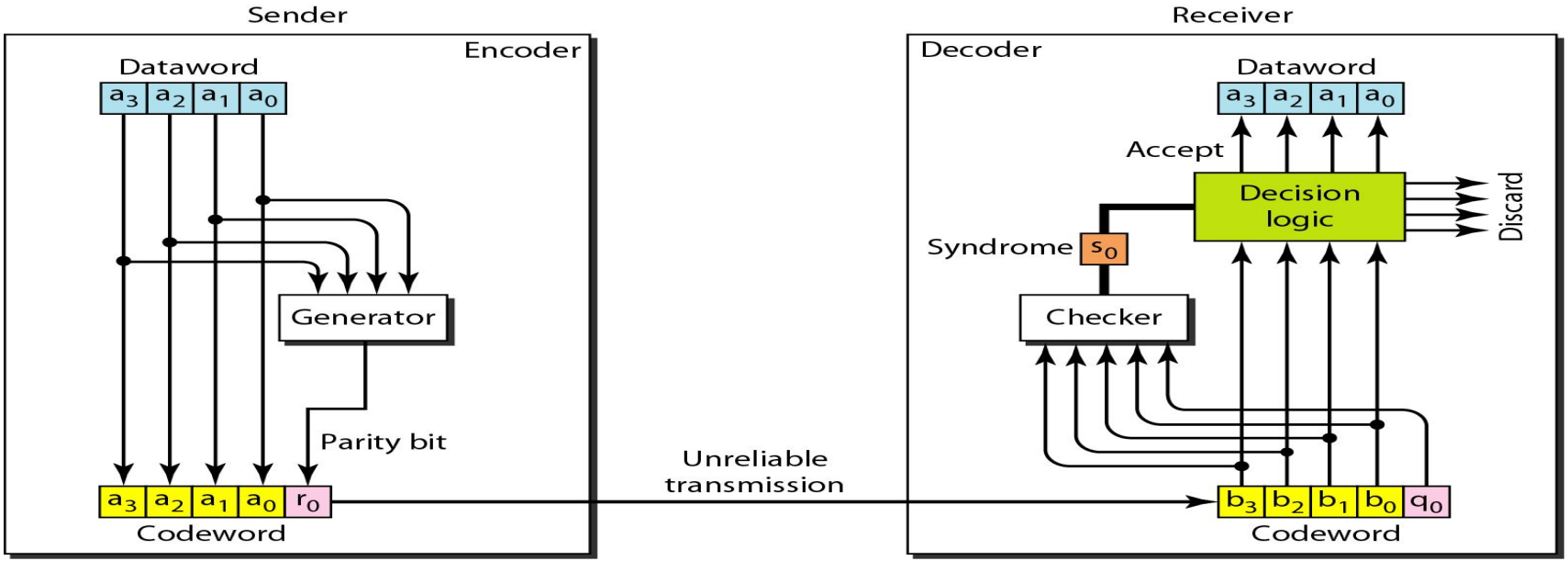
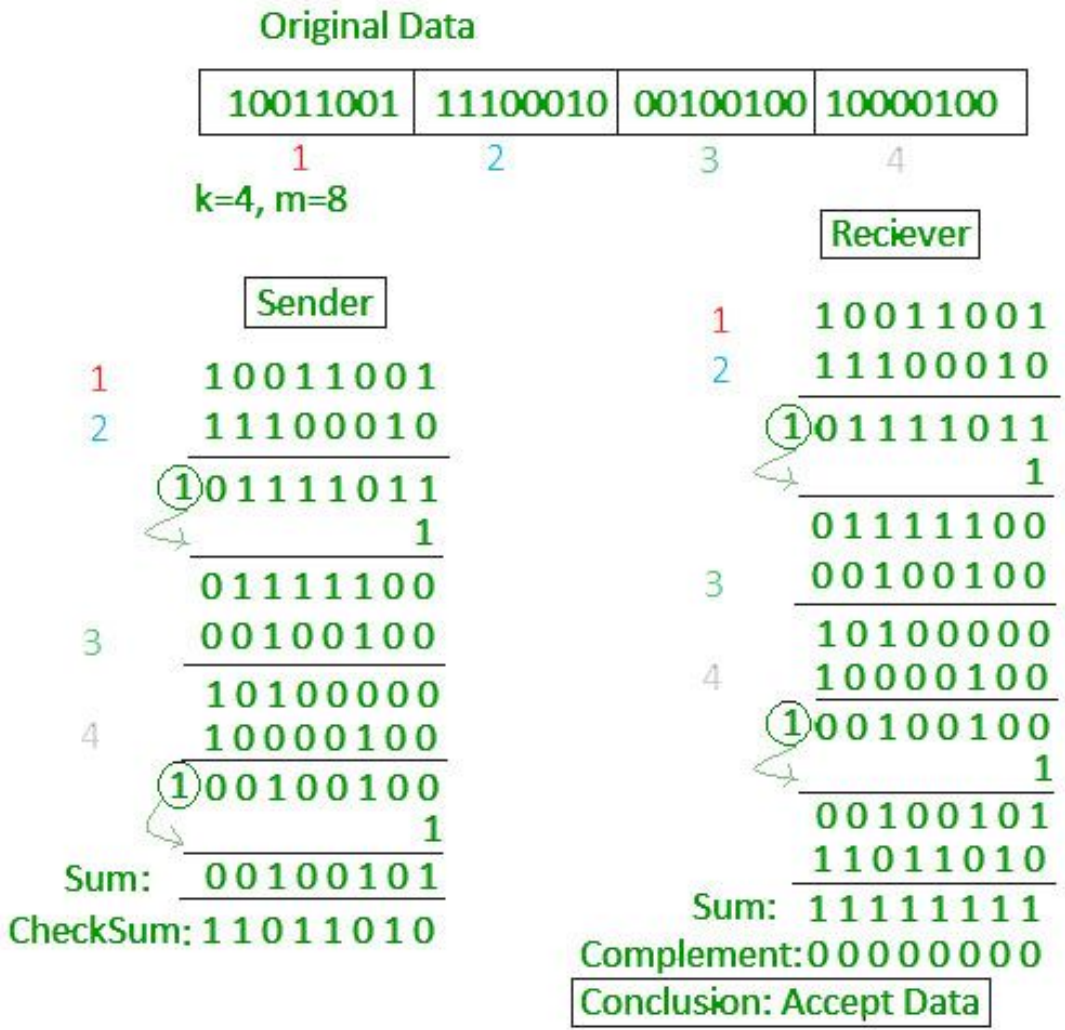


Fig: Encoder and decoder for simple parity-check code

- **Checksum**
  - In checksum error detection scheme, the data is divided into k segments each of m bits.
  - In the sender's end the segments are added using 1's complement arithmetic to get the sum.
  - The sum is complemented to get the checksum.
  - The checksum segment is sent along with the data segments..
  - At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum.
  - The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded.


Original Data
10011001
11100010
00100100
10000100
1
2
3
4
k=4, m=8
Sender
1 10011001
2 11100010
1 01111011
1
01111100
3 00100100
10100000
4 10000100
1 00100100
1
Sum: 00100101
CheckSum: 11011010
Reciever
1 10011001
2 11100010
1 01111011
1
01111100
3 00100100
10100000
4 10000100
1 00100100
1
00100101
11011010
Sum: 11111111
Complement: 00000000
Conclusion: Accept Data

- **Cyclic Redundancy Check (CRC)**
  - Cyclic Redundancy Check (CRC) involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system.
  - The divisor is generated using polynomials.
  - At the **sender** performs binary division of the data segment by the divisor. It then appends the remainder called CRC bits to the end of the data segment. This makes the resulting data unit exactly divisible by the divisor.
  - The **receiver** divides the incoming data unit by the divisor. If there is no remainder, the data unit is assumed to be correct and is accepted. Otherwise, it is understood that the data is corrupted and is therefore rejected.

Construct CRC message, let the divisor is 1101 and the data is 1011011.

At Sender

CRC, 001 is added

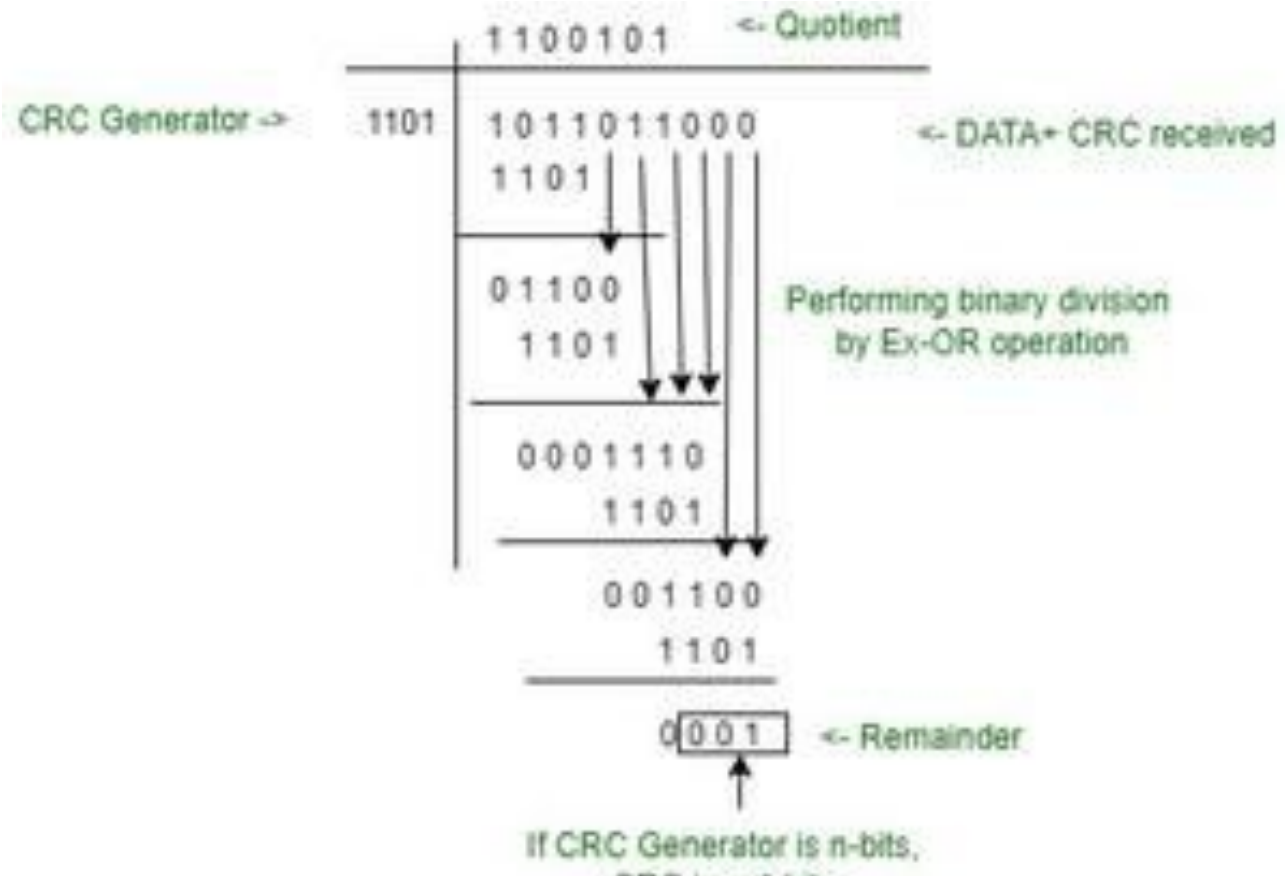
to the message

1011011.

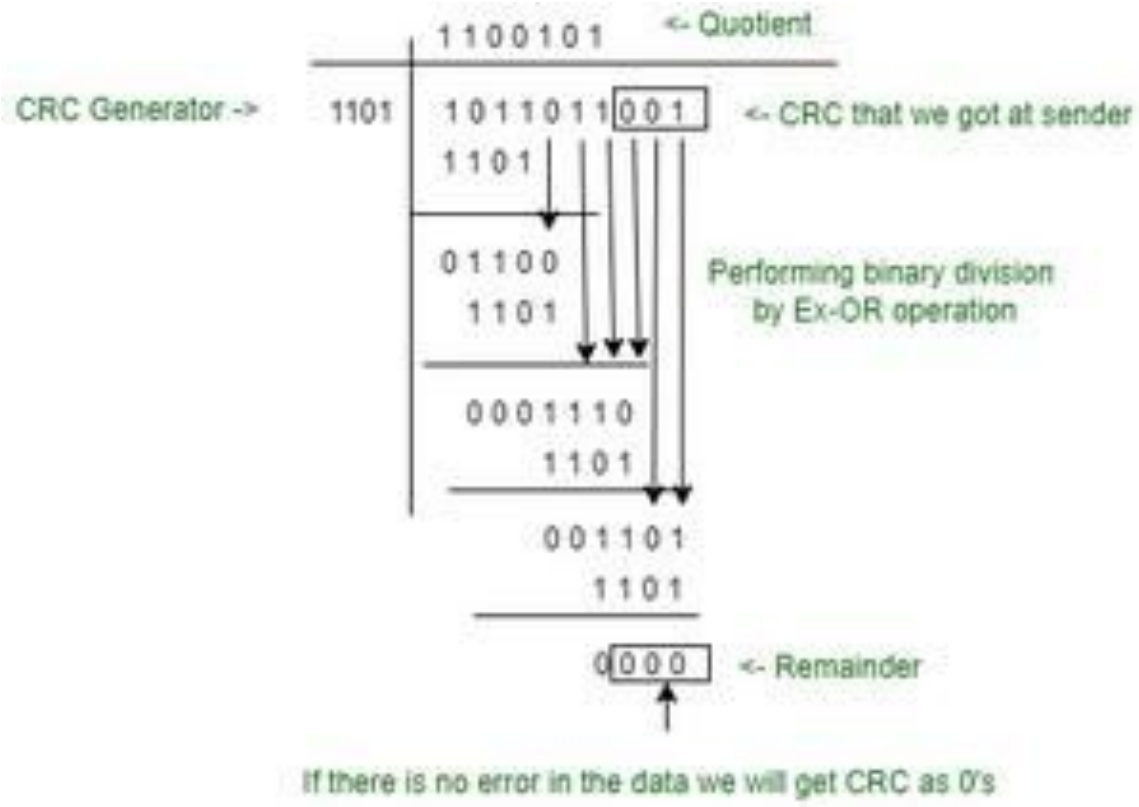
The transmitted

message is

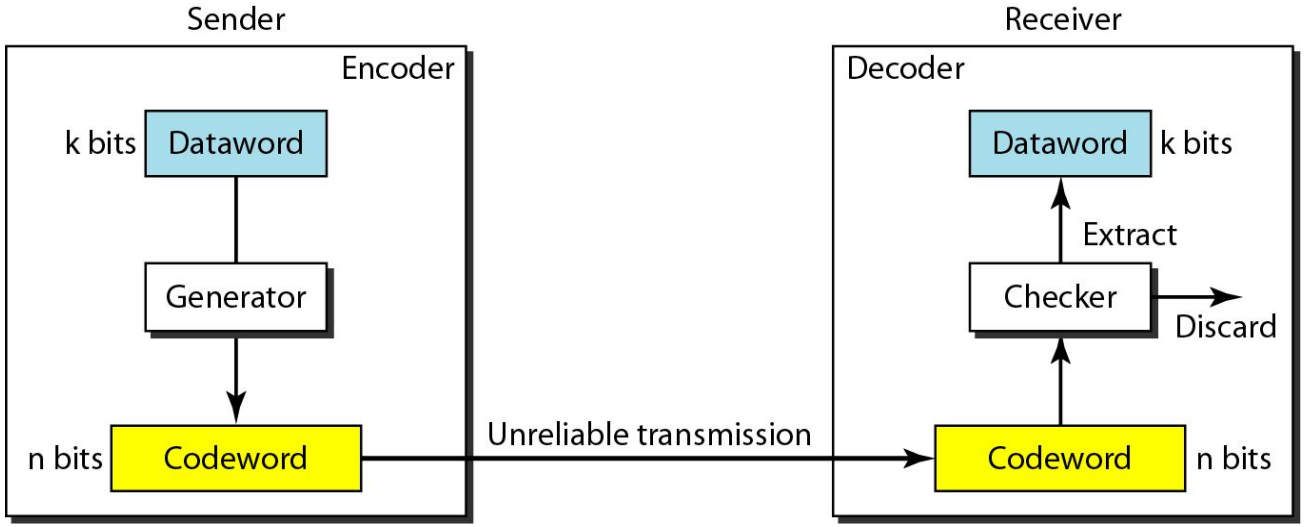
1011011001



At Receiver


1100101
<- Quotient
CRC Generator ->
1101
1011011001
<- CRC that we got at sender
1101
01100
1101
Performing binary division
by Ex-OR operation
0001110
1101
001101
1101
0000
<- Remainder
If there is no error in the data we will get CRC as 0's

CRC


Sender
Encoder
k bits
Dataword
Generator
n bits
Codeword
Unreliable transmission
Receiver
Decoder
Dataword
k bits
Extract
Checker
Discard
Codeword
n bits

CRC codewords
Error Detection

Dataword	*Codeword*	*Dataword*	*Codeword*
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

Fig: A CRC code with c(7,4)

CRC Encoder & Decoder

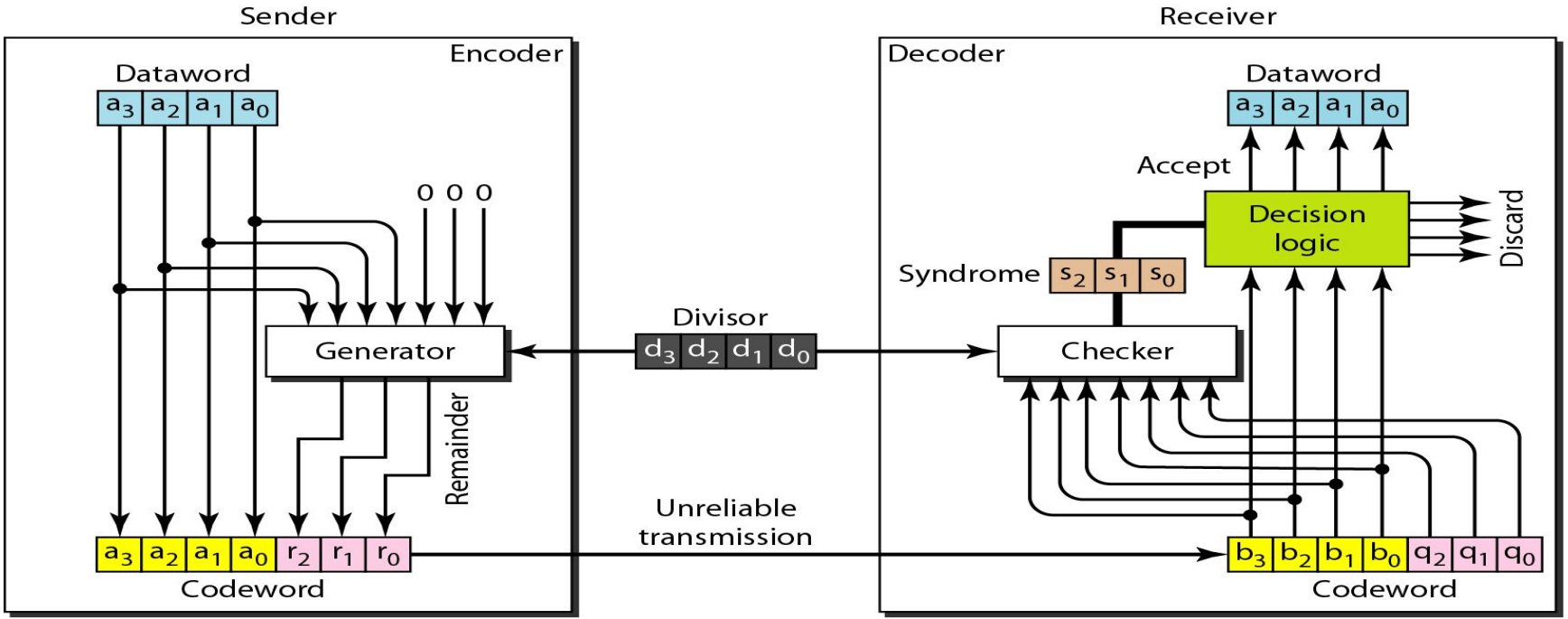


Fig : CRC Encoder & Decoder

TRy it yourself

1. Generate CRC code for dataword 110010101. The Divisor is 10101.

   Q) Check whether received codeword 1100100101011 has error or not.

   (The divisor is 10101).

2. Assume that g(x) is CRC-4, which equals X4 + X + 1, and the source data M is 10110011.

— — —

- **Hamming Code**
  - used for the set of error-correction codes
  - Process
    - Calculation of total numbers of redundant bits.
    - Checking the position of the redundant bits.
    - Lastly, calculating the values of these redundant bits.
  - Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.
  - n– number of data bits

    p – number of redundant bits which are added to it so that np can indicate at least (n + p + 1) different states.

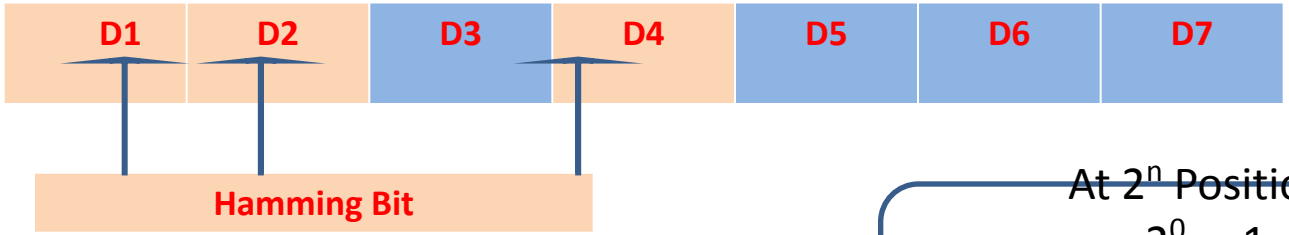
    2p >= (n + p + 1).

  - to correct a single-bit error.

- Here, all the redundant bit, p1, is must calculated as the parity. It should cover all the bit positions whose binary representation should include a 1 in the 1st position excluding the position of p1.
- P1 is the parity bit for every data bits in positions whose binary representation includes a 1 in the less important position not including 1 Like (3, 5, 7, 9, ...)
- P2 is the parity bit for every data bits in positions whose binary representation include 1 in the position 2 from right, not including 2 Like (3, 6, 7, 10, 11,...)
- P3 is the parity bit for every bit in positions whose binary representation includes a 1 in the position 3 from right not include 4 Like (5-7, 12-15,...)

Hamming Code (4,7)

Error Detection & Correction



D1 : 1, 3, 5, 7
D2 : 2, 3, 6, 7
D4 : 4, 5, 6, 7

At 2^n Position:
$2^0 = 1$
$2^1 = 2$
$2^2 = 4$

Example : Dataword = 1011

$\Rightarrow 2^r \geq p + k + 1$

→ So for $k = 4$ message bits.

$\Rightarrow 2^p \geq p + 4 + 1$

$\Rightarrow 2^p \geq p + 5$

For $p = 1$: $2^1 \geq 6$ — ✗

For $p = 2$: $2^2 \geq 7$ — ✗

For $p = 3$: $2^3 = 8$ — ✓

$\Rightarrow p = 3$ for $k = 4$ bits.

$\Rightarrow n = 3 + 4 = 7$ bits.

→ This is (7, 4) code.

7	6	5	4	3	2	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1

$P_1 = 2^0 = 1$

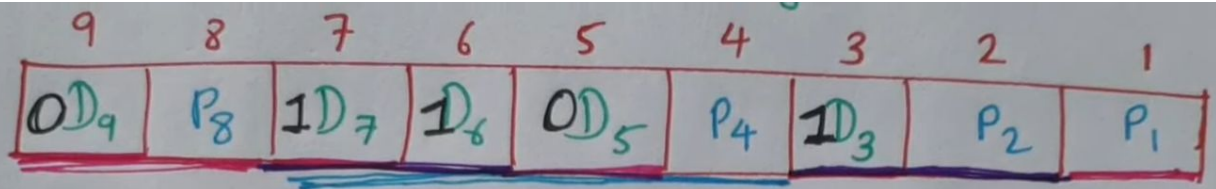
$P_2 = 2^1 = 2$

$P_4 = 2^2 = 4$

→ $P_1 \rightarrow D_3\ D_5\ D_7$ (XOR)

→ $P_2 \rightarrow D_3\ D_6\ D_7$ (XOR)

→ $P_4 \rightarrow D_5\ D_6\ D_7$ (XOR).



→ Position of Parity bits.

$P_1 = 2^0 = 1$

$P_2 = 2^1 = 2$

$P_4 = 2^2 = 4$

$P_8 = 2^3 = 8$

→ Value of Parity bits.

$P_1 \rightarrow D_3\ D_5\ D_7\ D_9$

$P_2 \rightarrow D_3\ D_6\ D_7$

$P_4 \rightarrow D_5\ D_6\ D_7$

$P_8 \rightarrow D_9$

→ $P_1 = 1 \oplus 0 \oplus 1 \oplus 0 = 0$

→ $P_2 = 1 \oplus 1 \oplus 1 = 1$

→ $P_4 = 0 \oplus 1 \oplus 1 = 0$

→ $P_8 = D_9 = 0$

Code

0011100110

TRy it yourself

If the 7 bit hamming code word received by receiver is 1011011 , assuming the even parity, state whether the received code word is correct or wrong? If wrong locate the bit having error?

Channelization

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

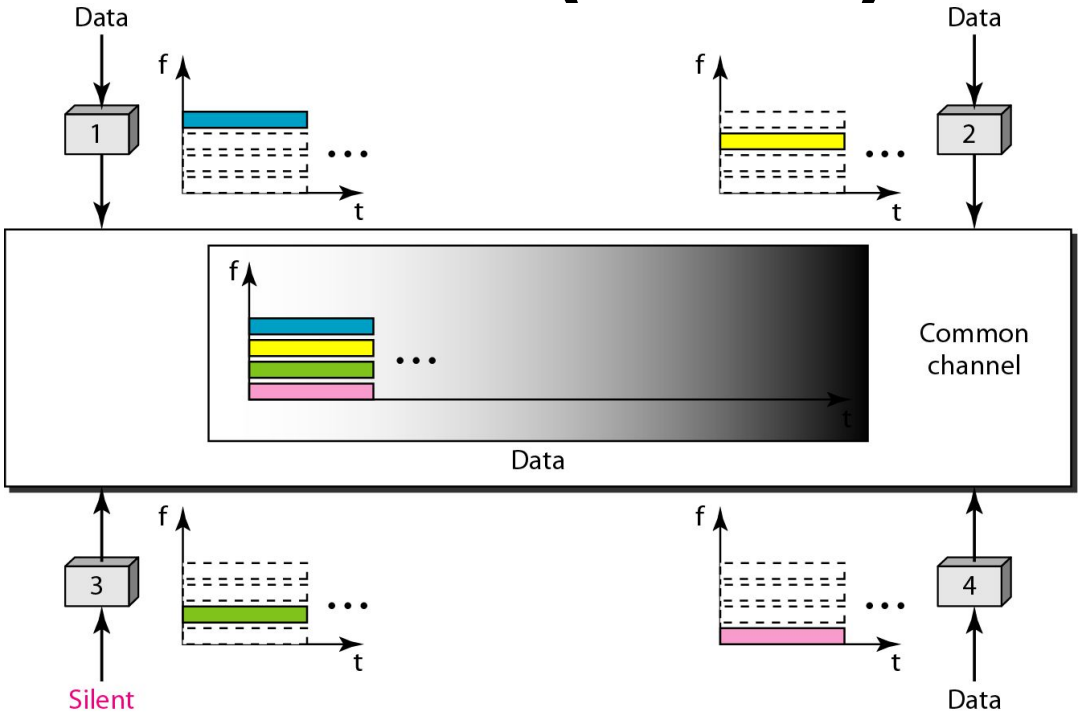
- Static Channel Allocation
- Dynamic Channel Allocation

Static Channel Access

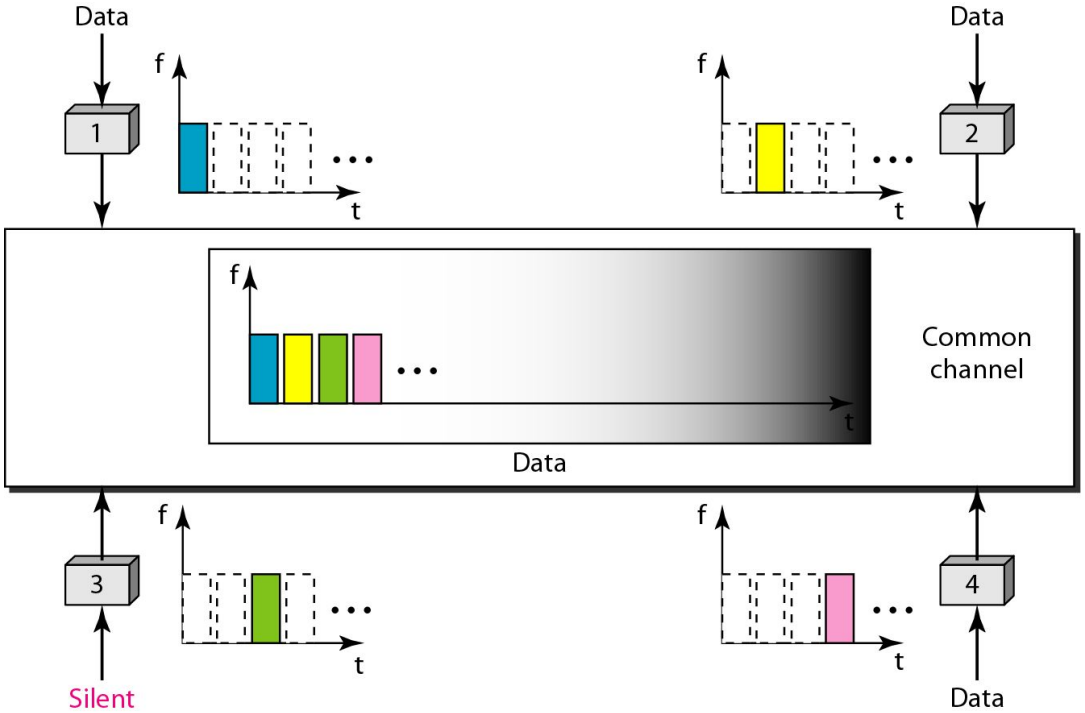
Three Common Method:

- Frequency-Division Multiple Access
- Time-Division Multiple Access
- Code-Division Multiple Access.

Frequency-division multiple access (FDMA)



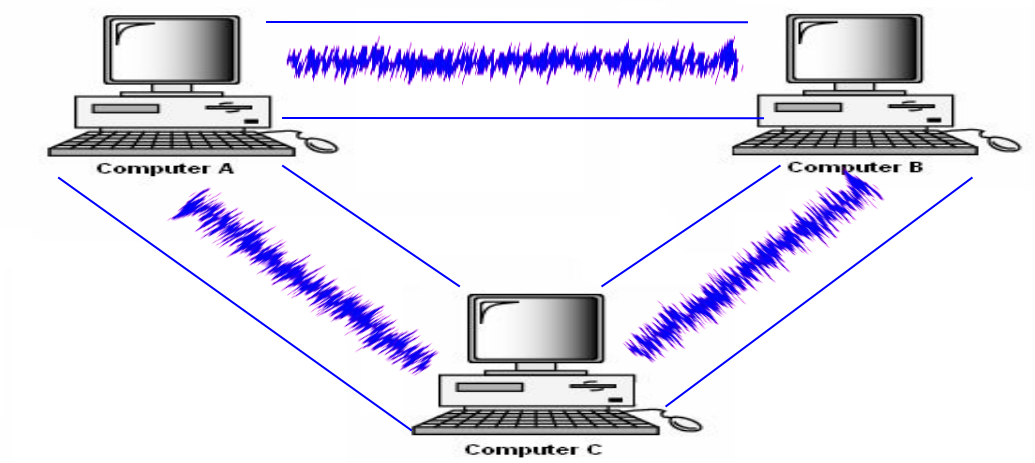
Time-division multiple access (TDMA)



Transmission technology can be categorized into two categories :

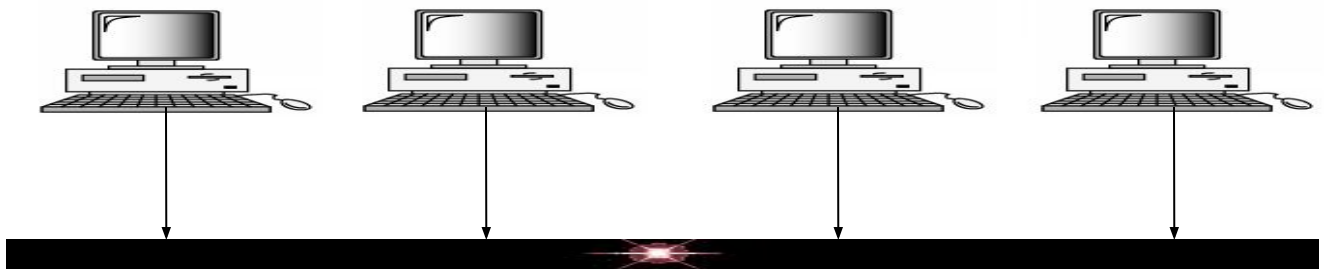
- *Point-to point networks*
- *Broadcast networks*

Point-to-point networks



Broadcast networks

Broadcast networks have a single communication channel that is shared by all the machines on the network. A packet sent by one computer is received by all the other computers on the network. The packets that are sent contain the address of the receiving computer; each computer checks this field to see if it matches its own address. If it does not then it is usually ignored; if it does then it is read. Broadcast channels are sometimes known as multi-access channel.



Shared channel

Need of protocols in Broadcast channel

Issues in multi-access channel :

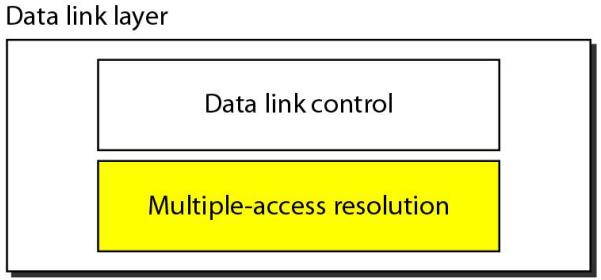
- *WHO is going to use the channel ?*
- *For HOW much time the channel is used ?*

Due to shared channel and unregulated traffic over the network collisions and data loss occur. Some protocol must be followed for regulated and safe transmission over the network.

MEDIUM ACCESS SUBLAYER

MAC (Medium access control sub layer) is a sub layer of Data link layer. MAC is the bottom part of the Data link layer. The protocols used to determine who goes next on a multi-access channel belongs to this layer. Some of the algorithms for allocating multi-access channel are as follows:

- *Aloha protocol*
- *Carrier Sense Multiple Access Protocols(CSMA)*
- *Collision-free protocols :*
- *Limited contention protocol*
- *Digital Cellular radio*



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.

Random Access

- Each station follows a procedure that answers the following questions:
  - When can the station access the medium?
  - What can the station do if the medium is busy?
  - How can the station determine the success or failure of the transmission?
  - What can the station do if there is an access

RANDOM ACCESS

- ALOHA
  - Pure Aloha
  - Slotted Aloha
- CSMA
  - CSMA/CD
  - CSMA/CA

Pure ALOHA

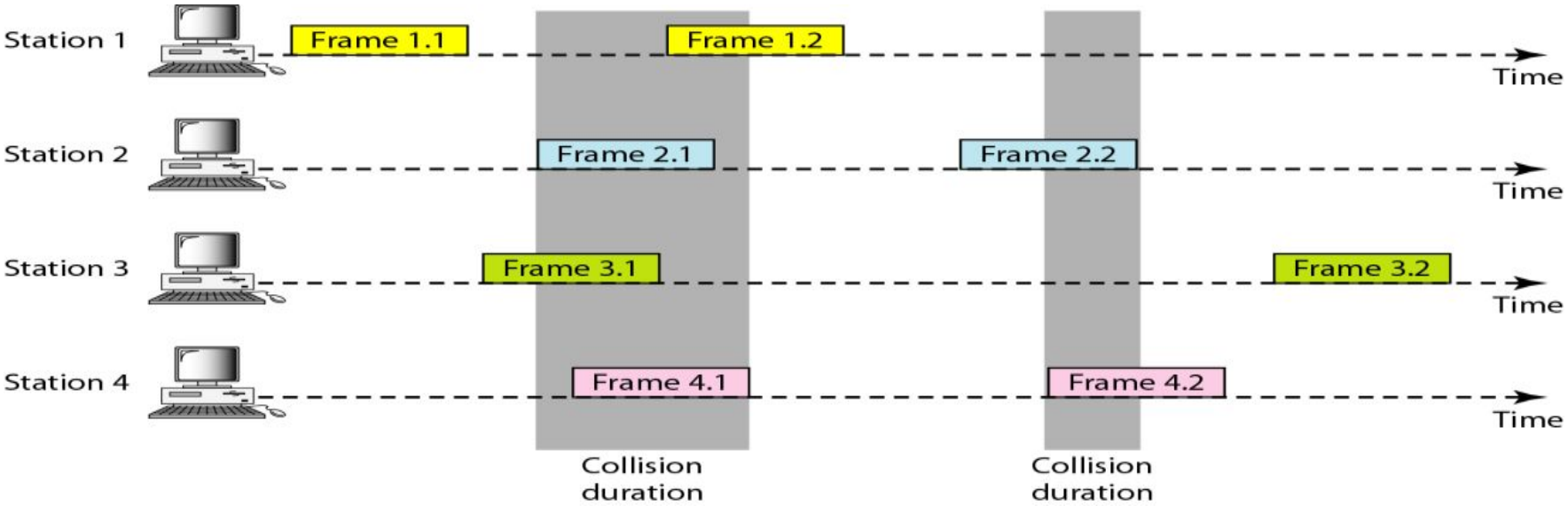
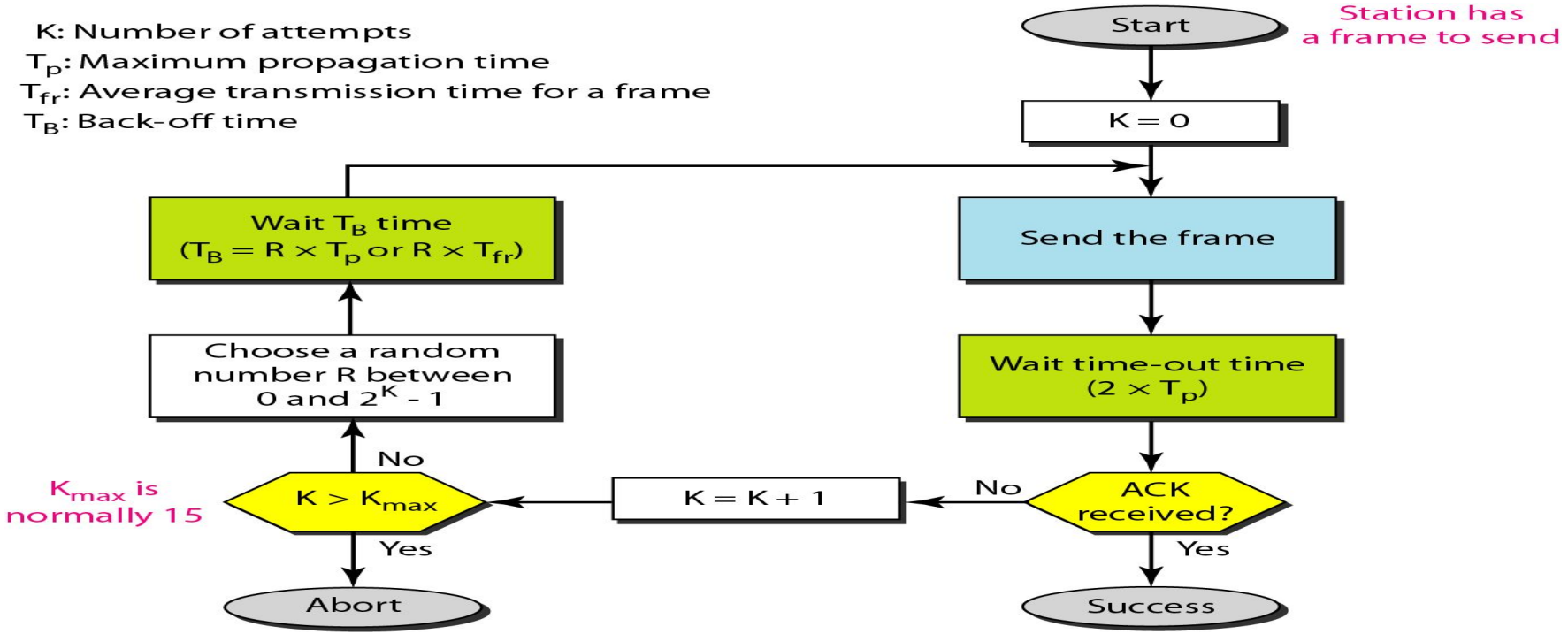


Fig: Frames in a pure ALOHA network

Procedure for pure ALOHA protocol



Throughput for pure ALOHA

The throughput for pure ALOHA is

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

The maximum throughput

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

Where G = Avg. no. of frames generated during one frame

Slotted ALOHA

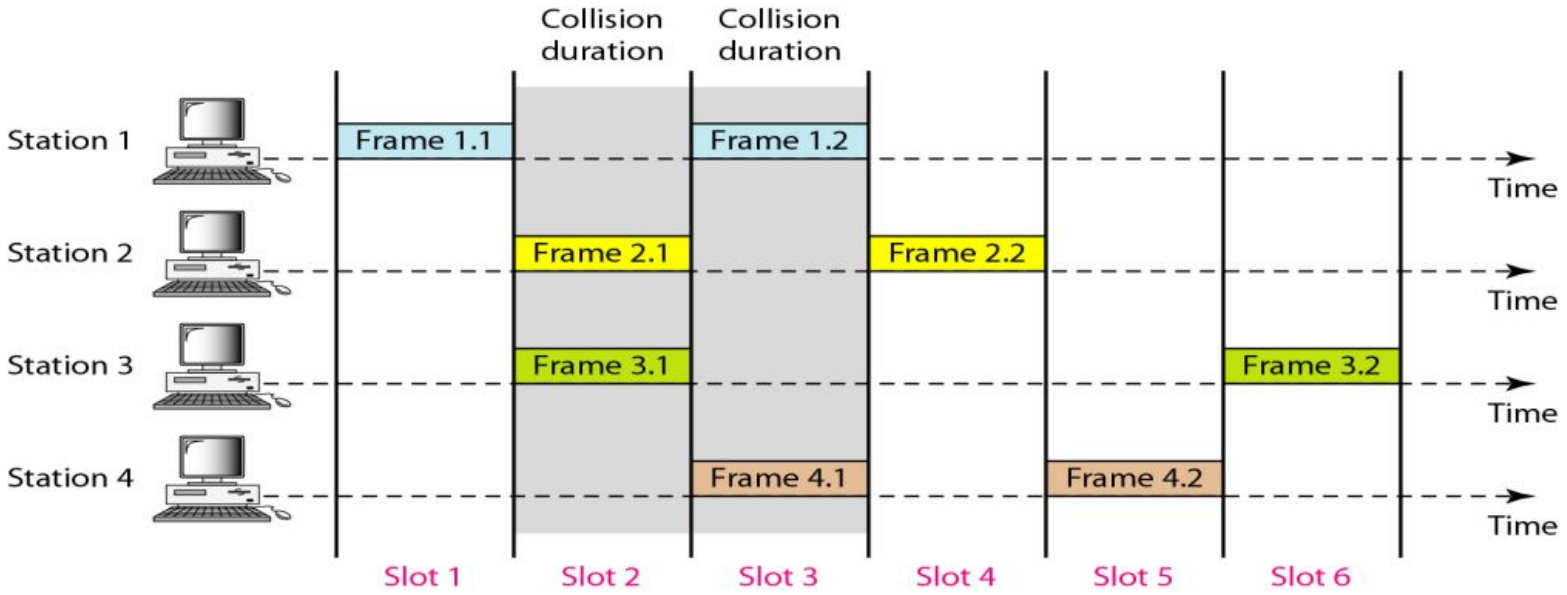


Fig: Frames in a Slotted ALOHA network

Throughput for slotted ALOHA

The throughput for slotted ALOHA is

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

The maximum throughput

$S_{max} = 0.368$ when $G = (1)$

Where G = Avg. no. of frames generated during one frame

Carrier Sense Multiple Access (CSMA)

- To minimize the chance of collision & increase the performance
- CSMA reduces the possibility of collision but it cannot eliminate it completely.
- Possibility of collision still exist because of propagation delay.

CSMA

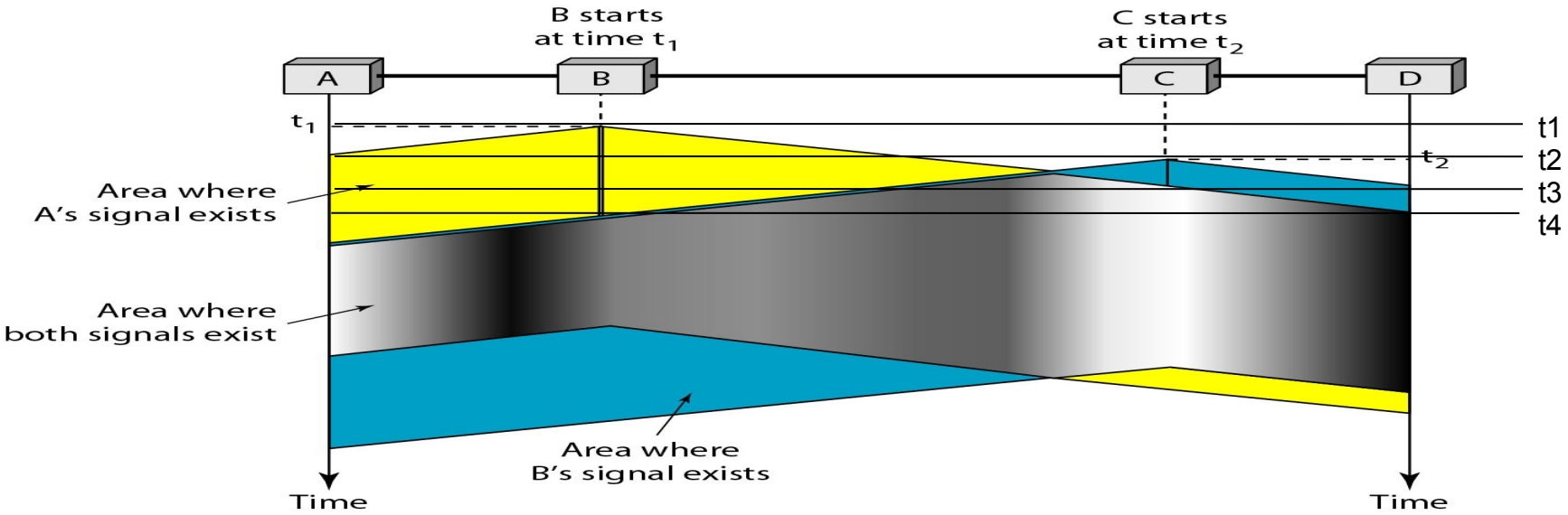
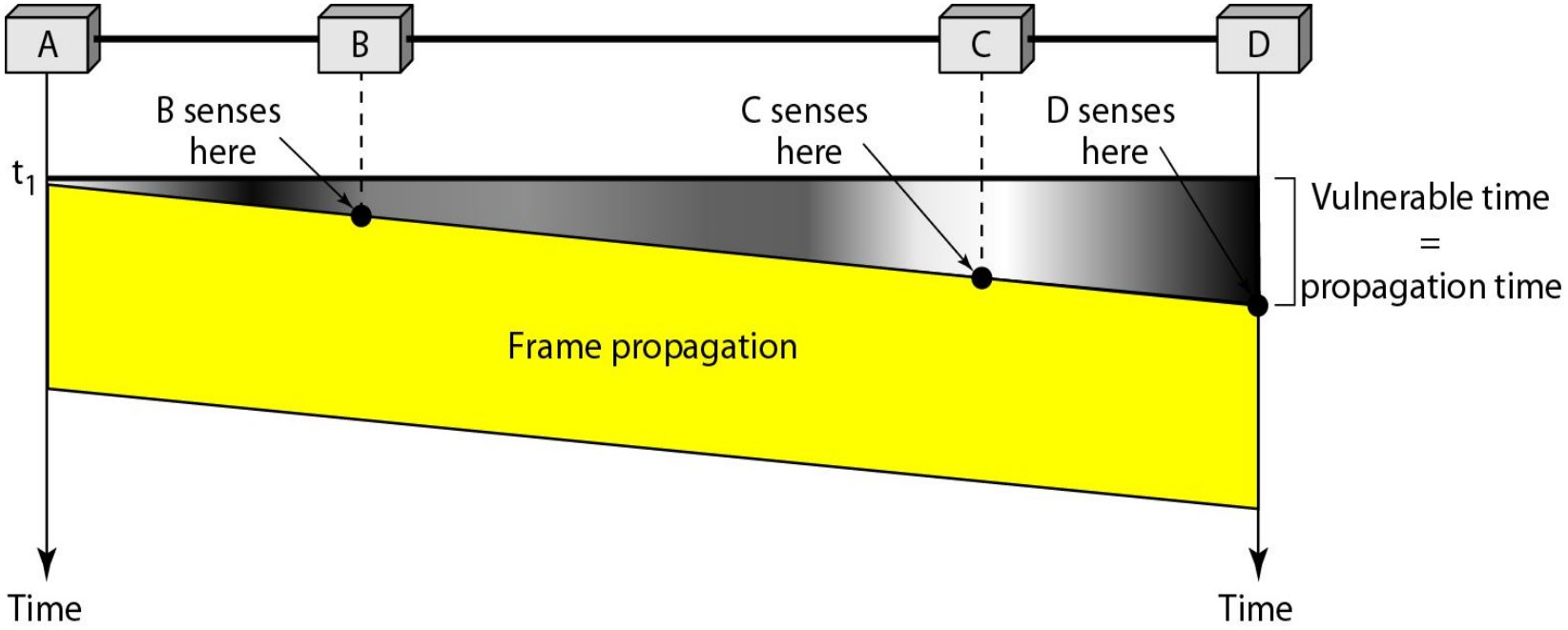


Fig. Space/time model of the collision in CSMA

Vulnerable Time



what should a station do if the channel is busy?

- There are 3 method to deal with :
  - 1-Persistent
  - Non-Persistent
  - P- Persistent

Persistence Methods

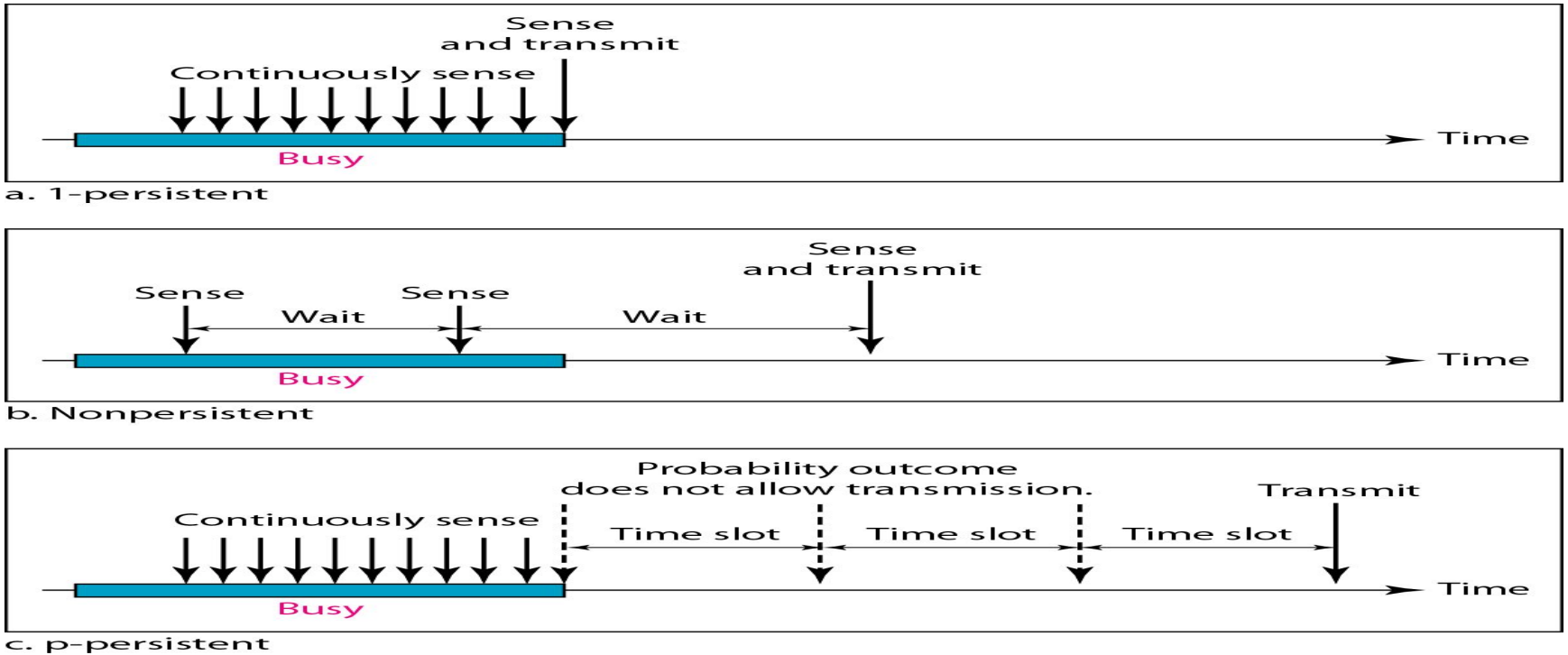


Fig. Behavior of three persistence methods

1-Persistence Method

- Simplest
- If line is idle, it send its frame immediately.
- Highest chance of collision
- Good efficiency

Non- Persistence Method

- If the line is idle, it send immediately
- If the line is busy, it waits for a random amt of time.
- Reduces the chance of collision.
- Less efficient

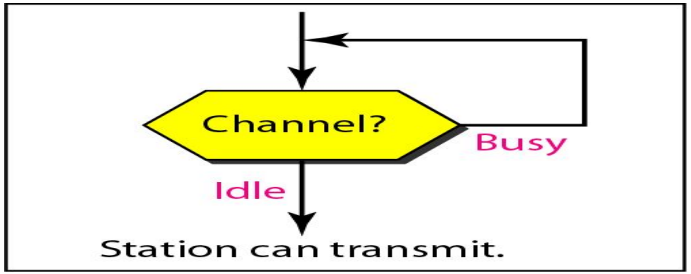
P-Persistence Method

- Channel has time slot of size >= propagation time.
- Combines the adv. of above two method.
- It reduces the chance of collision and increase efficiency.

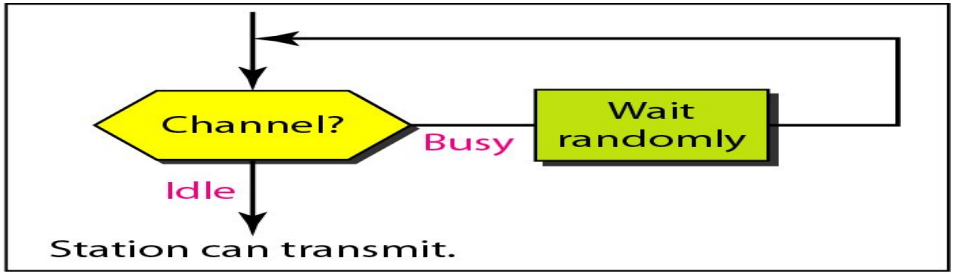
P-Persistence Method

- 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.
    - If the line is idle, it goes to step 1.

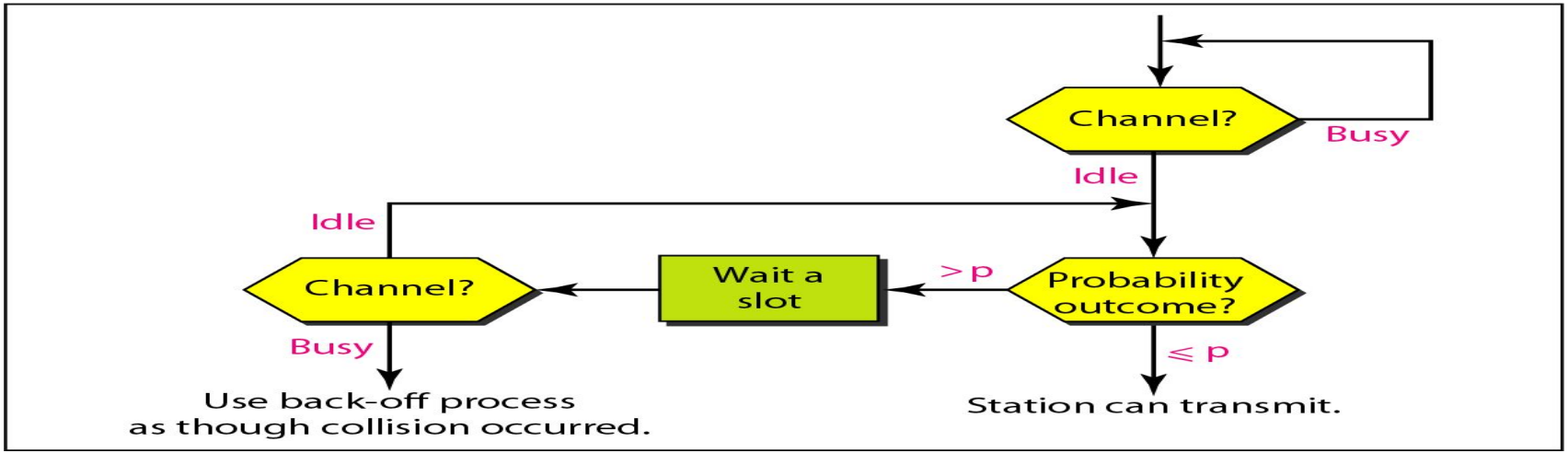
Persistence Methods



a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/CD(Collision Detection)

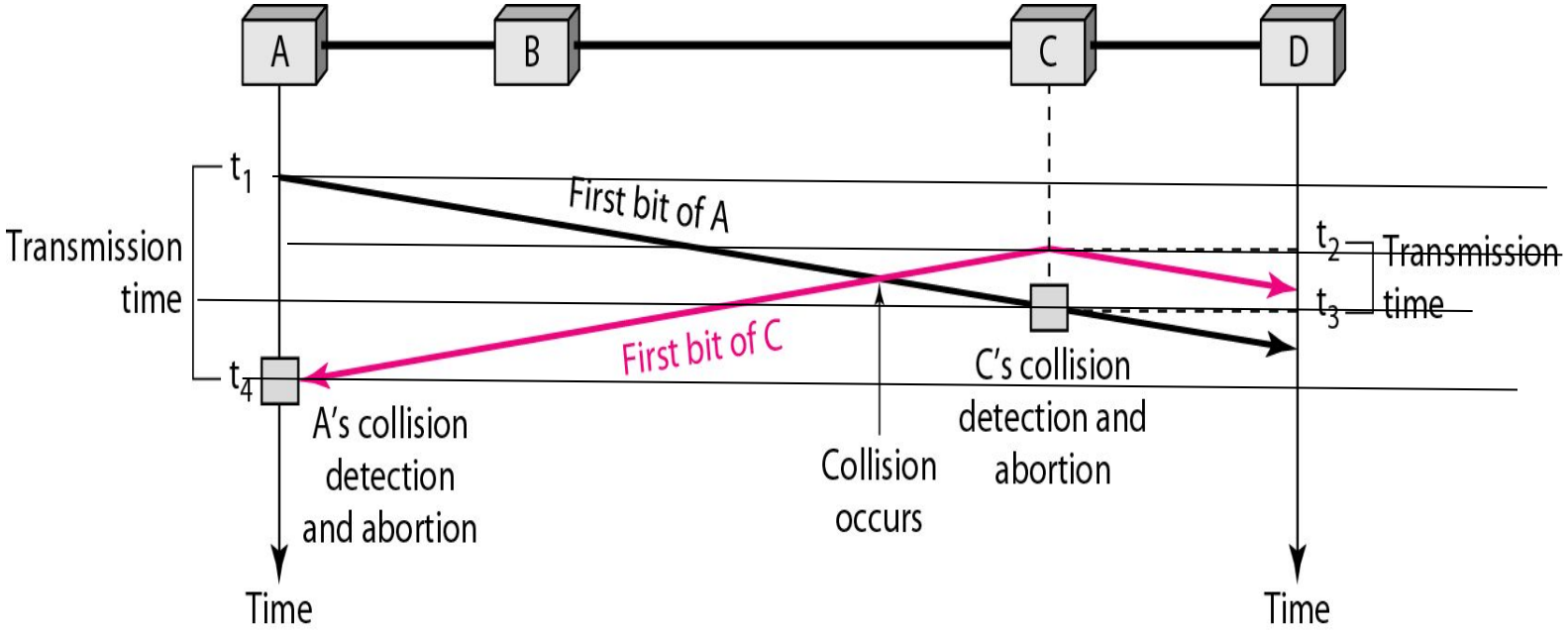


Fig. Collision of the first bit in CSMA/CD

CSMA / CD

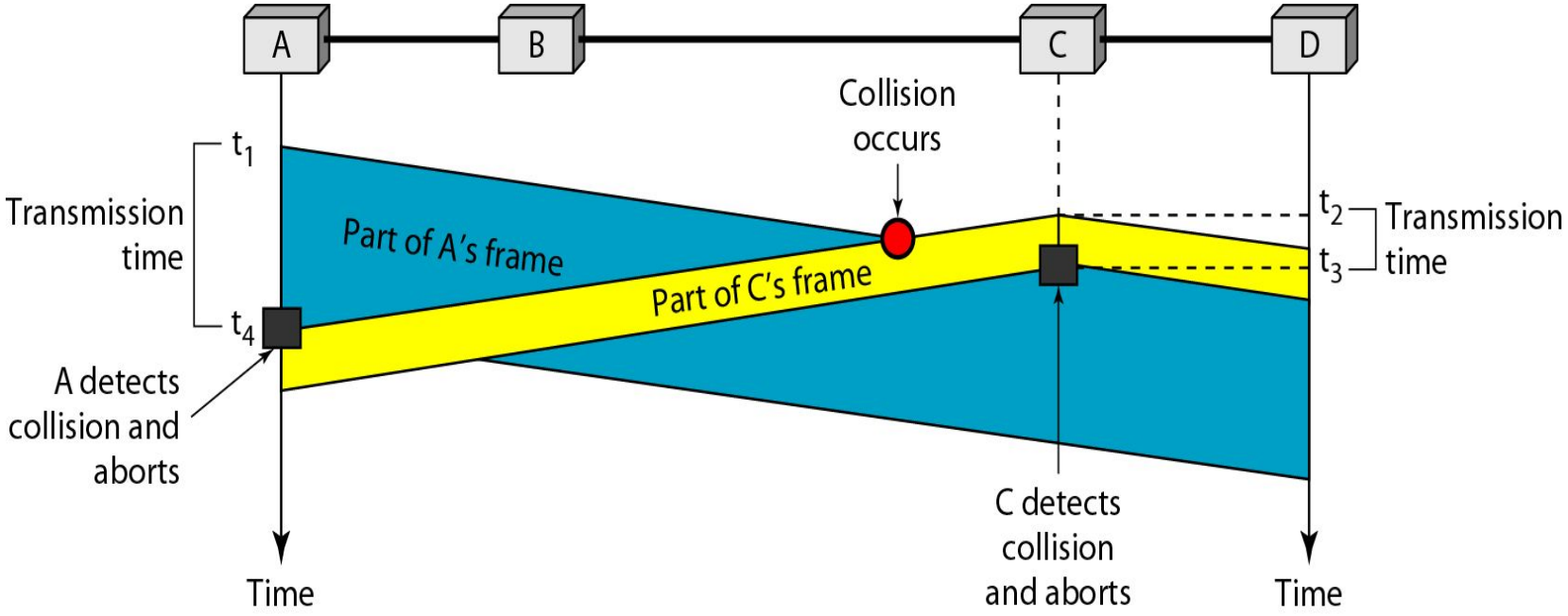


Fig. Collision and abortion in CSMA/CD

CSMA/ CA (Collision Avoidance)

- Collisions are avoided through the use of CSMAICA's three strategies:
  - Inter-frame space
  - Contention window
  - and Acknowledgments

Inter-Frame Space

- IFS time should be greater than the propagation time.

- Even if channel is idle, the station waits for IFS time.

Contention Window

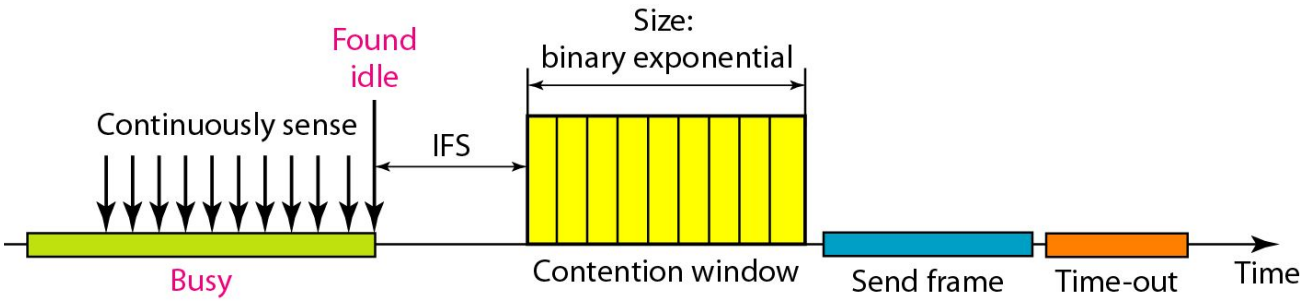
- The contention window is an amount of time divided into slots.

- A station that is ready to send chooses a random number of slots as its wait time.

Acknowledge

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

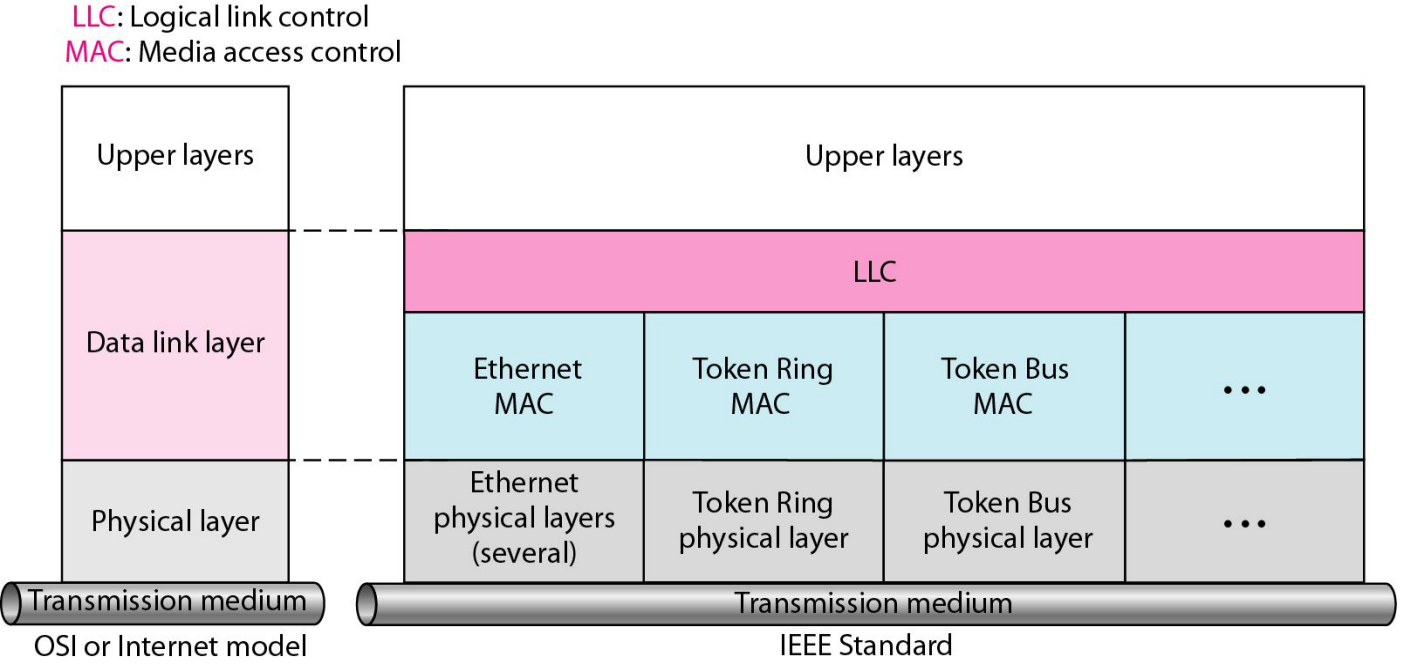
CSMA/CA


Found
idle
Size:
binary exponential
Continuously sense
IFS
Busy
Contention window
Send frame
Time-out
Time

IEEE STANDARDS

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

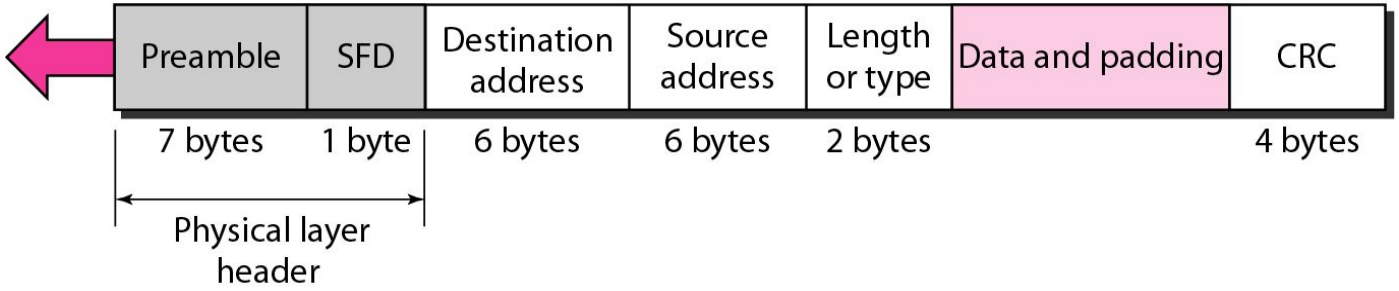
IEEE standard for LANs



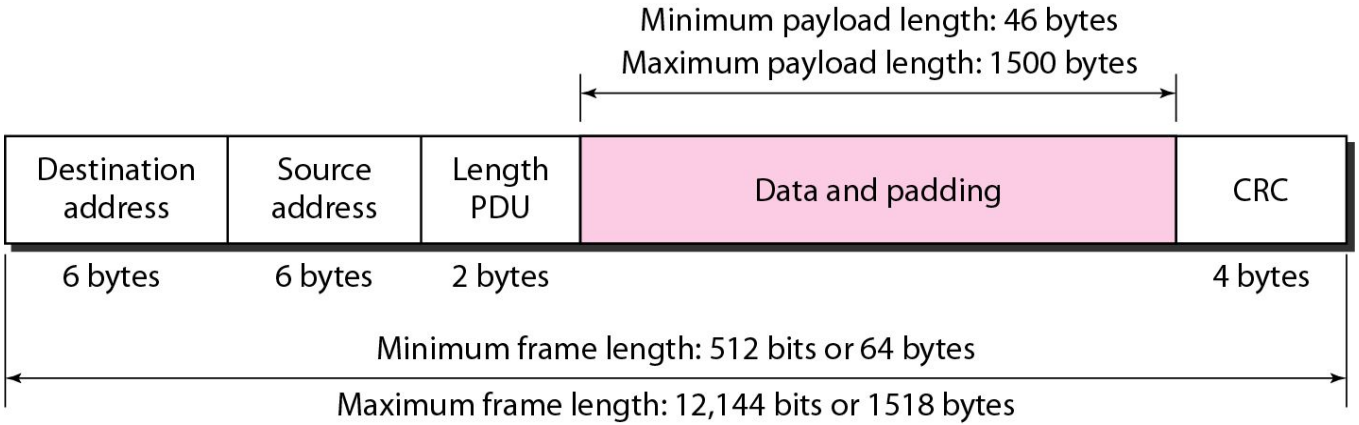
802.3 MAC frame

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Minimum and maximum lengths



Unicast and multicast addresses

The least significant bit of the first byte defines the type of address.
If the bit is 0, the address is unicast; otherwise, it is multicast.

The broadcast destination address is a special case of the multicast address in which all bits are 1s.

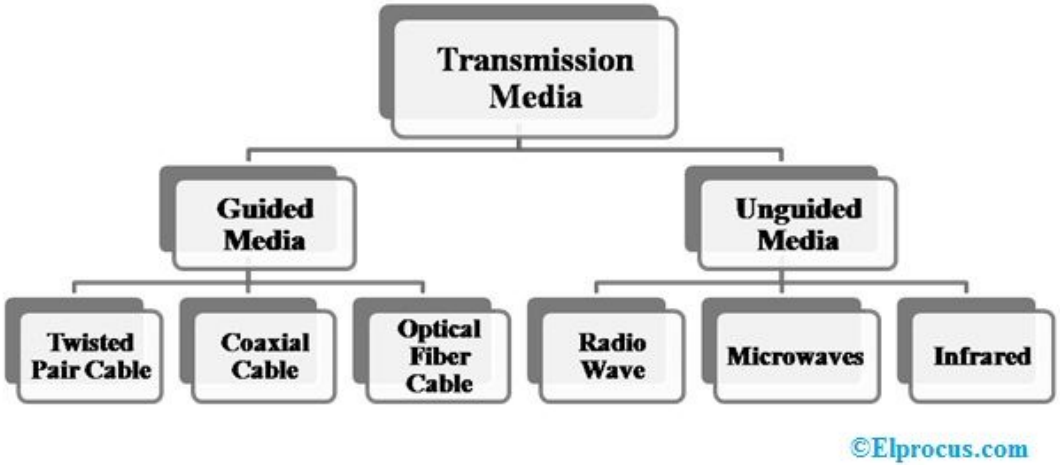
Physical layer

Transmission Media

Two types

- **Wired / Guided Media**
  - the signals can be transmitted directly through physical links
  - characteristics of wired media
  - secure, high-speed, and used in small distances

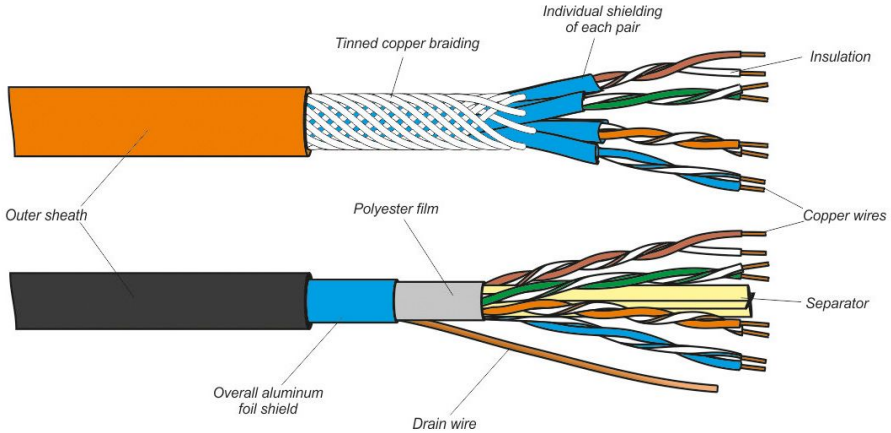
- **Wireless / Unguided Media**
  wireless media the signal characteristics are important.



Guided Media

1. Twisted Pair Cable

- It includes two separately protected conductor wires.
- pairs of cables are packaged jointly in a protective cover.
- most frequently used type of transmission media and it is available in two types. - **UTP and STP**
- **Eg: CAT 3, CAT 5**



— — —

UTP (Unshielded Twisted Pair)

- Blocked by interference.
- doesn’t depend on a physical guard
- used in telephonic applications.
- low cost, very simple to install, and high speed
- liable to exterior interference, transmits in fewer distances, and less capacity.

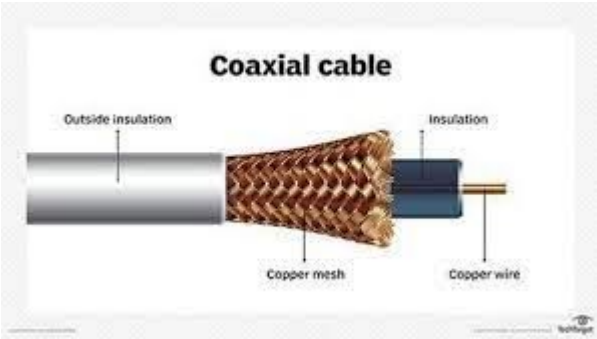
STP (Shielded Twisted Pair)

- blocks outside interference
- used in rapid data rate Ethernet, in voice & data channels of telephone lines.
- good speed, removes crosstalk.
- hard to manufacture as well as install, It is expensive and bulky also

Parameters	UTP	STP
Full Form	Unshielded Twisted Pair	Shielded Twisted Pair
Structure	cable with wires that are twisted together.	Twisted pair cable enclosed in foil / shield.
Cost	Cheaper than STP	Costlier than UTP
Weight	Lighter than STP	Heavier than UTP
Noise & interference	Prone to Noise and interference	Less prone to noise and interference
Data Speed	Supports slower speed than on STP	Support higher speed than UTP
Grounding of cable	Not required	Required
Target deployments	Locations less prone to interference like offices and homes.	Locations prone to interference like factories and airports

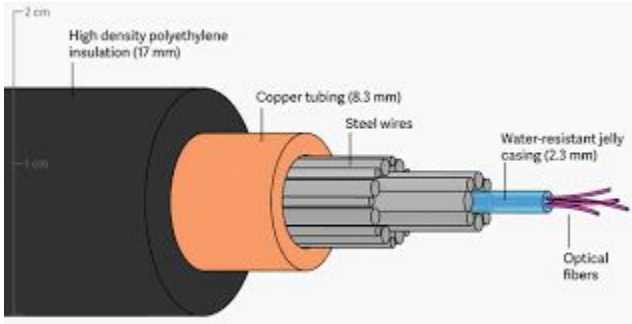
2. Coaxial Cable

- cable contains an external plastic cover and it includes two parallel conductors where each conductor includes a separate protection cover.
- used to transmit data in two modes like baseband mode as well as broadband mode, widely used in cable TVs & analog TV networks.
- high bandwidth, noise immunity is good, low cost and simple to install.
- failure of cable can disturb the whole network
- Best to be used in Bus Topology
- Eg: RG 59, RG 58



3. Optical Fibre Cable

- uses the notion of light reflected through a core that is made with plastic or glass. The core is enclosed with less thick plastic or glass and it is known as the cladding, used for large volume data transmission.
- lightweight, capacity & bandwidth will be increased, signal attenuation is less
- high cost, fragile, installation & maintenance is difficult and unidirectional.
- Best for Ring and Star Topology
- Eg: 50.11, 100/125



Comparison of Guided Media

EMI - Elect

Factor	UTP	STP	Coxial	Fiber-optic
Cost	Lowest	Moderate	Moderate	Highest
Installation	Easy	Fairly easy	Fairly easy	Difficult
Bandwidth	1-155Mbps (10Mbps)	1-155Mbps (16Mbps)	10Mbps	2Gbps (100Mbps)
Node Capacity per segment	2	2	30(10base2) 100(10base5)	2
Attenuation	High	High	Lower	Lowest
EMI	Most vulnerable	Less than UTP but still vulnerable	Less than UTP but still vulnerable	Not affected by EMI

Unguided Media

- doesn’t require any physical medium to transmit electromagnetic signals.
- less secure, the signal can be transmitted through air, and applicable for large distances. T

1. **Radiowaves**

- easy to produce as well as penetrate through buildings.
- transmitting & receiving antennas no need to align.
- frequency range of these waves ranges from 3 kHz to 1GHz.
- Used in AM & Fm radios for transmission.
- two types namely Terrestrial & Satellite

2. **Microwaves**

- sightline transmission which means the transmitting & receiving antennas need to align correctly with each other.
- distance which is covered through the signal can be directly proportional to the antenna’s height
- frequency range of microwaves ranges from 1GHz to 300GHz.
- extensively used in TV distribution & mobile phone communication

— — —

3. Infrared Waves

- extremely small distance communication as they cannot go through obstacles.
- stops intrusion between systems.
- range of frequency of these waves is 300GHz to 400THz.
- used in TV remotes, keyboards, wireless mouse, printer, etc.

Comparison of Guided and Unguided Media

BASIS FOR COMPARISON	GUIDED MEDIA	UNGUIDED MEDIA
Basic	The signal requires a physical path for transmission.	The signal is broadcasted through air or sometimes water.
Alternative name	It is called wired communication or bounded transmission media.	It is called wireless communication or unbounded transmission media.
Direction	It provides direction to signal for travelling.	It does not provide any direction.
Types	Twisted pair cable, coaxial cable and fibre optic cable.	Radio wave, microwave and infrared.

The following factors must be considered to **design the transmission media** like the following.

Bandwidth: The bandwidth mainly refers to the capacity of data-carrying in a medium otherwise a channel. So, high BW communication channels mainly support high data rates.

Radiation : The radiation refers to the signal leakage from the medium because of its unwanted electrical characteristics.

Absorption of Noise: The absorption of noise refers to the vulnerability of the media to exterior electrical noise. This noise can cause data signal distortion.

Attenuation : Attenuation refers to the energy loss when signal broadcasts externally. The loss of energy amount mainly depends on frequency. Radiation, as well as physical media characteristics, contributes to attenuation.

The transmission impairment mainly causes because of the following reasons.

Attenuation: It is the loss of energy which can be occurred due to the decrease in signal & increase in the distance.

Distortion: Distortion mainly occurs because of the change in signal shape. This kind of distortion can be observed from various signals which have different frequencies. Every frequency component has its separate propagation speed because they arrive at a different time which leads to the delay in distortion.

Noise : When data is transmitted above a transmission medium, an unwanted signal can be added to it. So the noise can be created.

Switching

Circuit Switching/ Packet Switching

(Covered in Module 1)

Structure of Switch