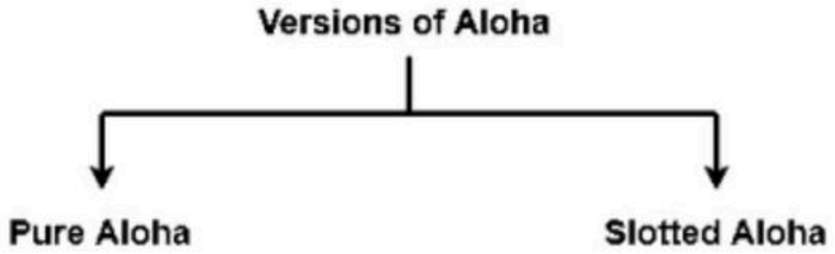
Error Control: CRC & Checksum - Part I

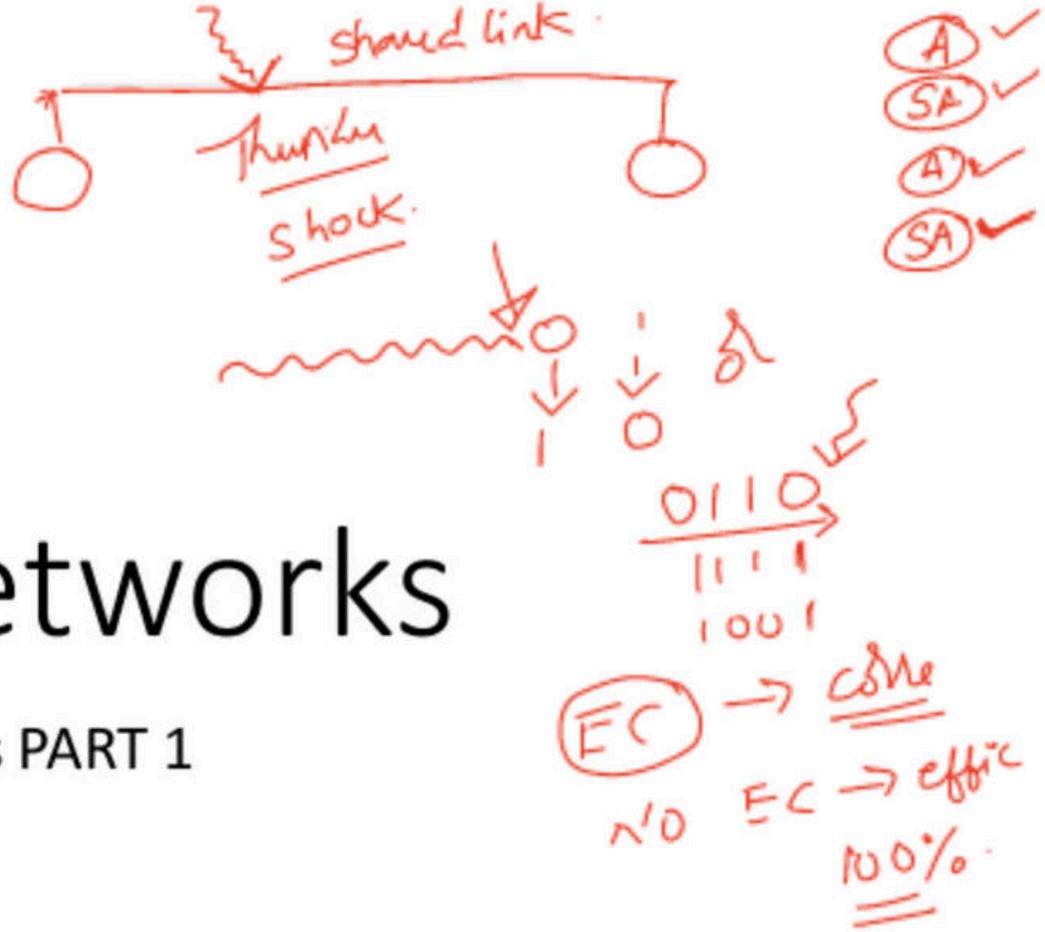
Complete Course on Computer Networks - Part II

Ravindrababu Ravula • Lesson 2 • Feb 21, 2021

Aloha-

There are two different versions of Aloha-





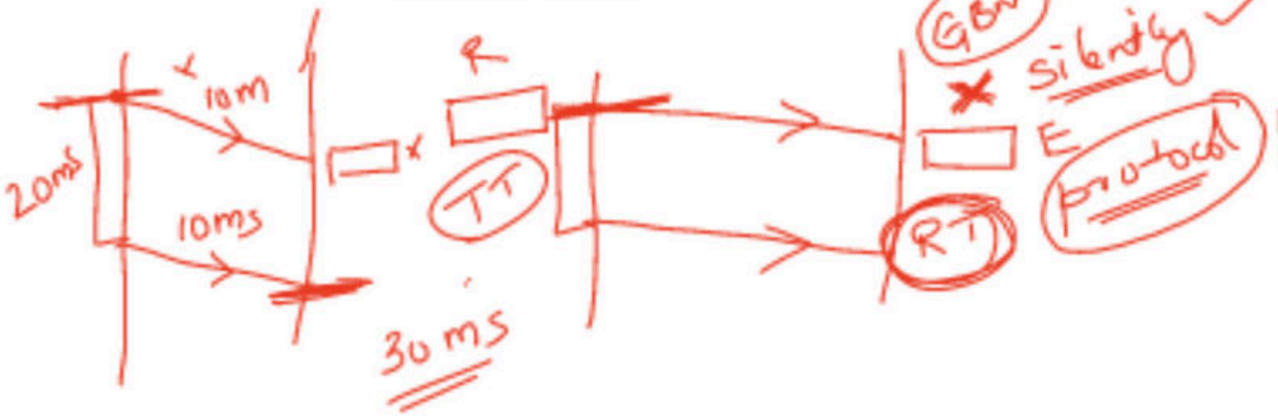
Computer Networks

Error Control Methods PART 1

Error Handling Methods

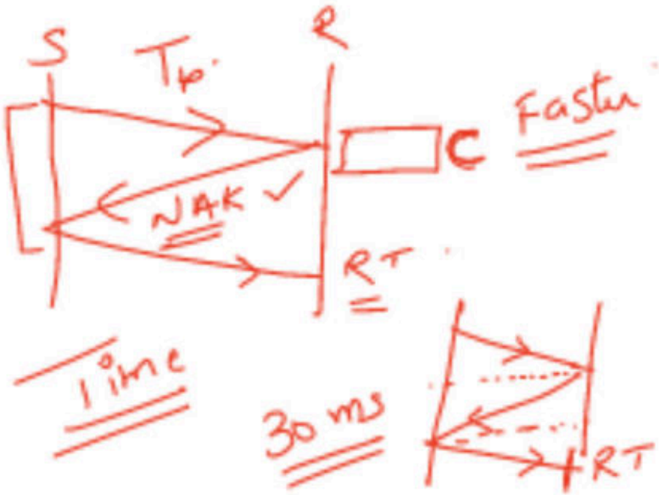
Error Detection

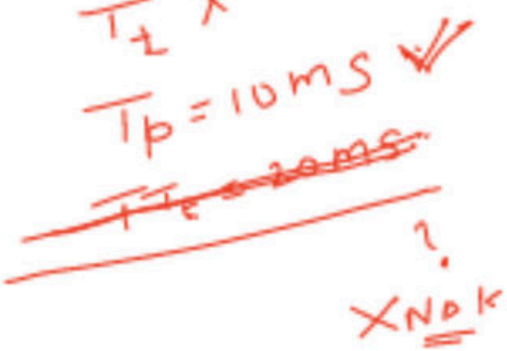
Error detection is a technique that is used to check if any error occurred in the data during the transmission.

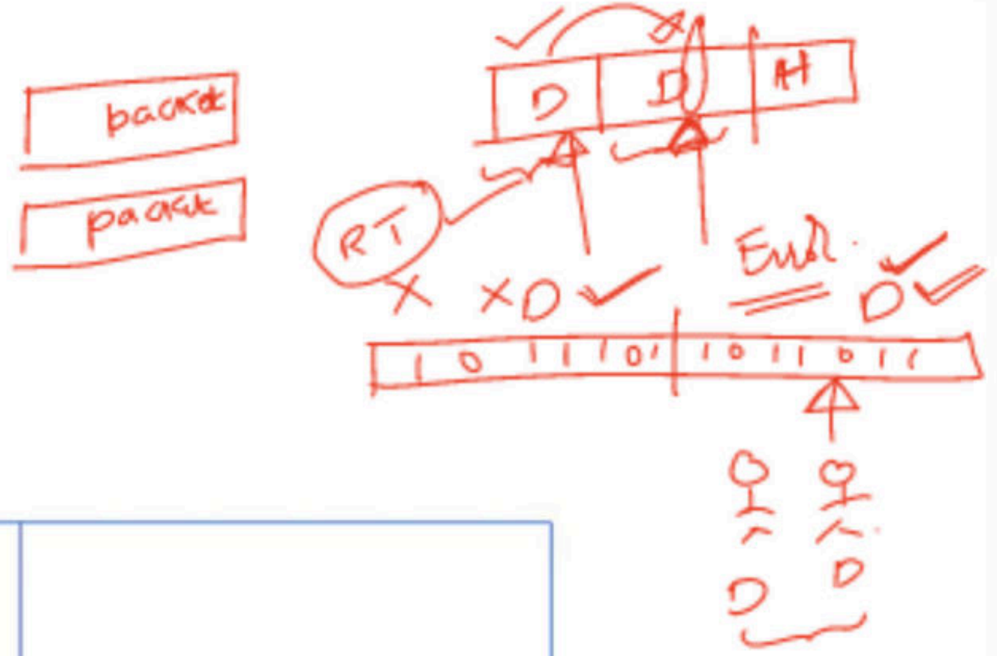


Error Correction

Error Correction is a technique that is used to correct error occurred in the data by its own during the transmission.







Error Detection

- Data + Data
- Single Parity Check
- CRC
- Checksum

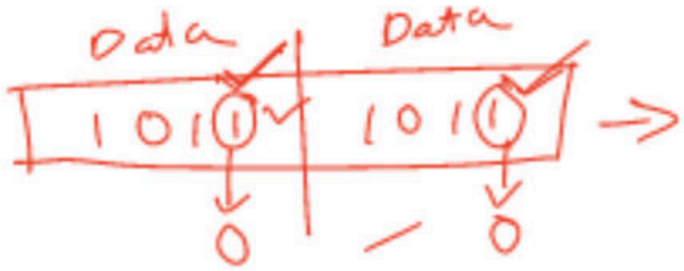
efficient.

2Y

BW Link

R GW

Burdan



100% guar

Loss

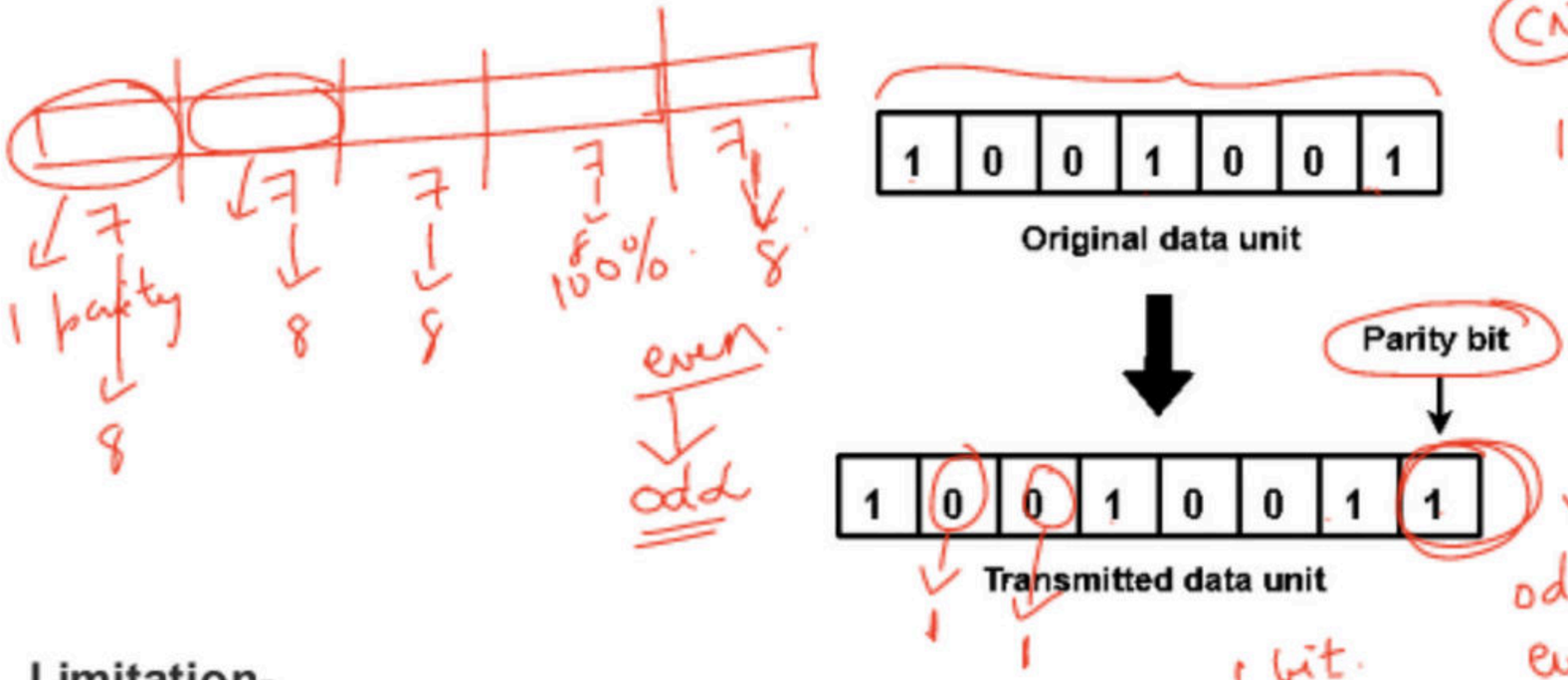
b^2

$\frac{1}{10^6} \times \frac{1}{10^6}$

Single Parity Check-

In this technique,

- One extra bit called as **parity bit** is sent along with the original data bits.
- Parity bit helps to check if any error occurred in the data during the transmission.



Limitation-

- This technique can not detect an even number of bit errors (two, four, six and so on).
- If even number of bits flip during transmission, then receiver can not catch the error.

Cyclic Redundancy Check-

- Cyclic Redundancy Check (CRC) is an error detection method.
- It is based on binary division.

Cyclic Generator-

Data to be sent : 1 0 1 1 0 1 1

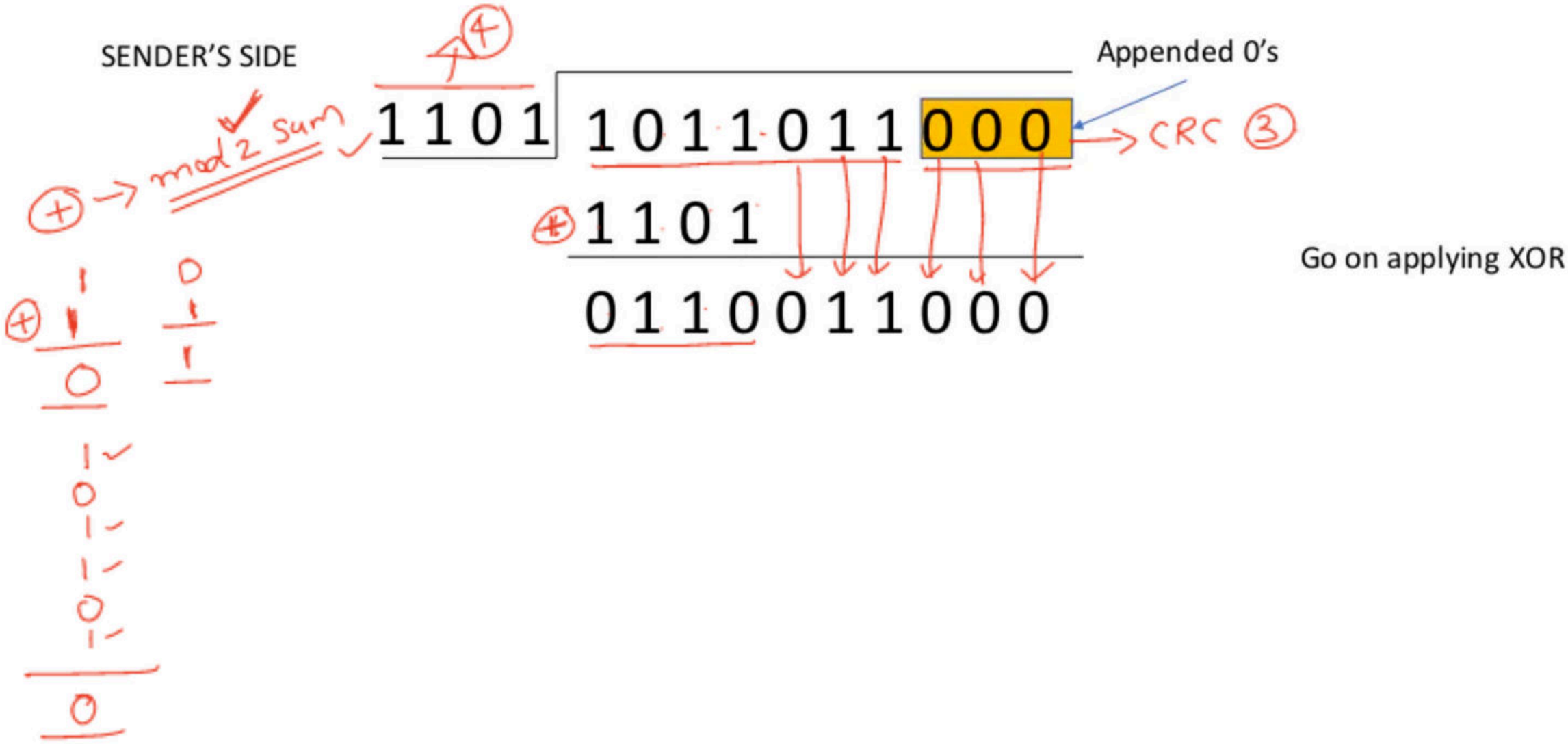
CRC generator: 1 1 0 1

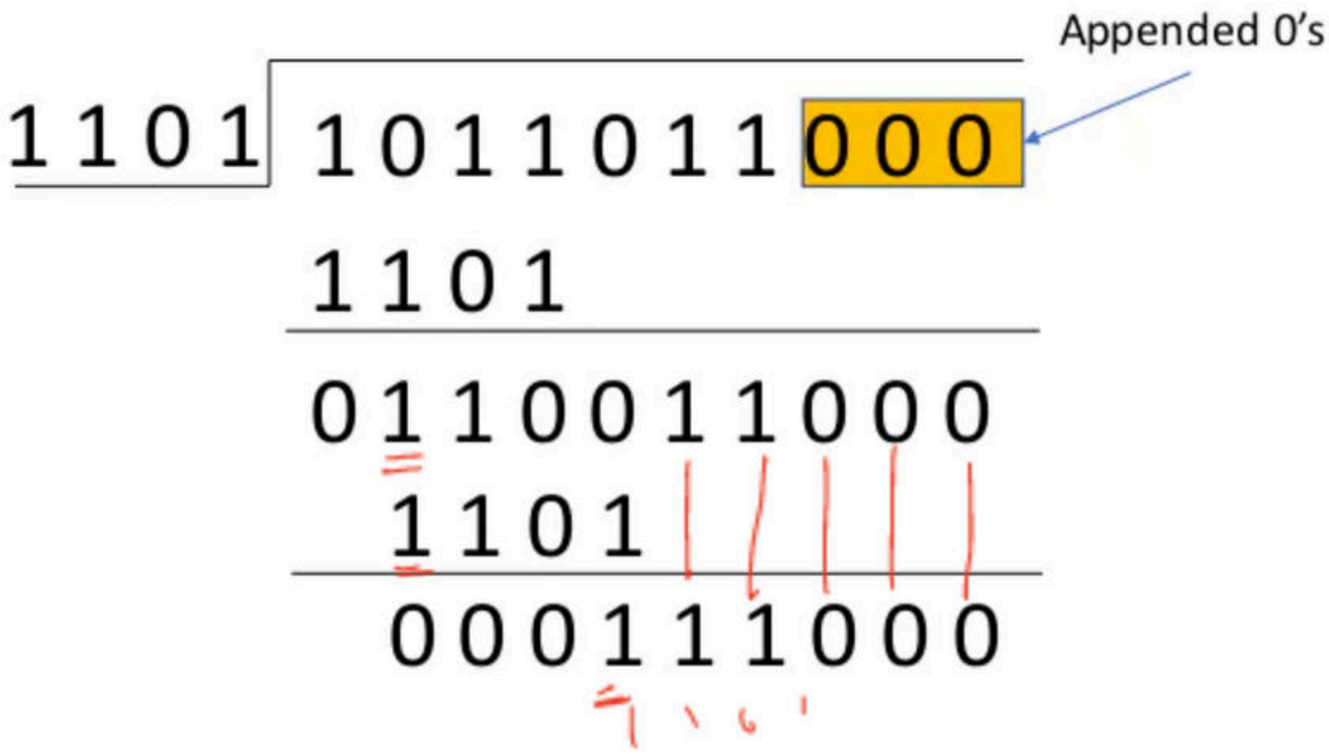
CRC generator is 4 bits

There for sender appends 3 bits of 0's to the data

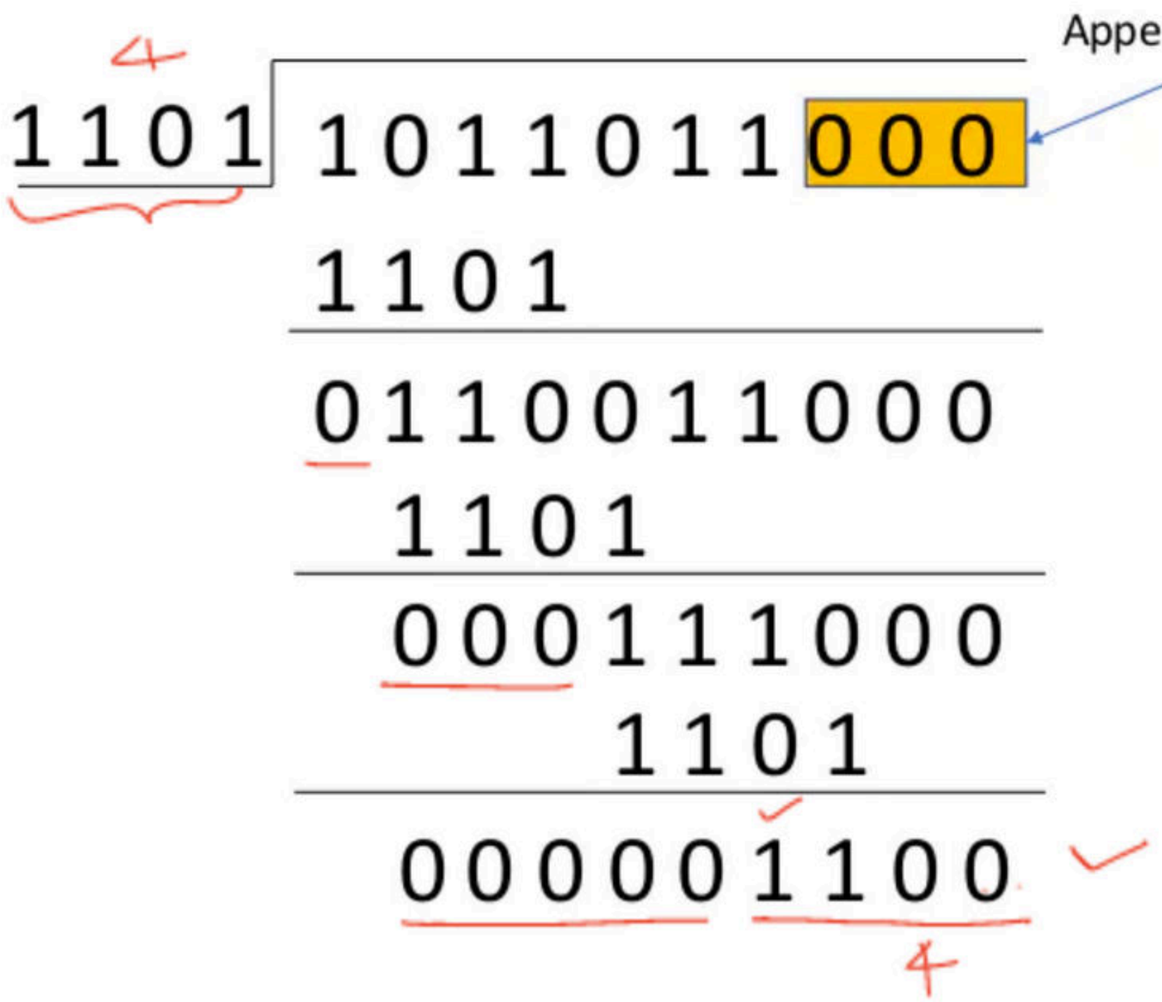
Note: if CRCG= n bits then bits to be appended in data is (n-1) 0's

SENDER'S SIDE





Go on applying XOR

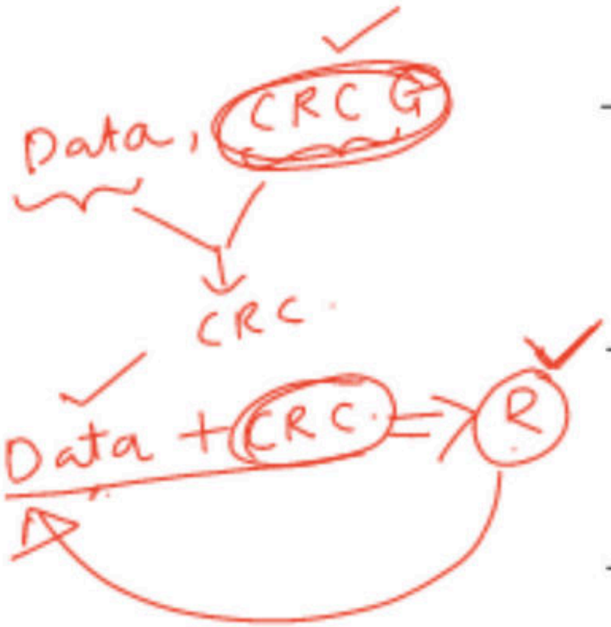

Appended 0's
1 1 0 1 1 0 1 1 0 1 1 0 0 0
1 1 0 1
0 1 1 0 0 1 1 0 0 0
1 1 0 1
0 0 0 1 1 1 0 0 0
1 1 0 1
0 0 0 0 0 1 1 0 0
Go on applying XOR

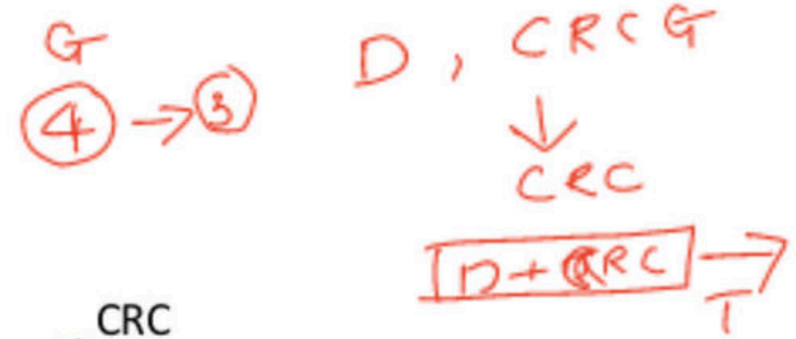
Appended 0's

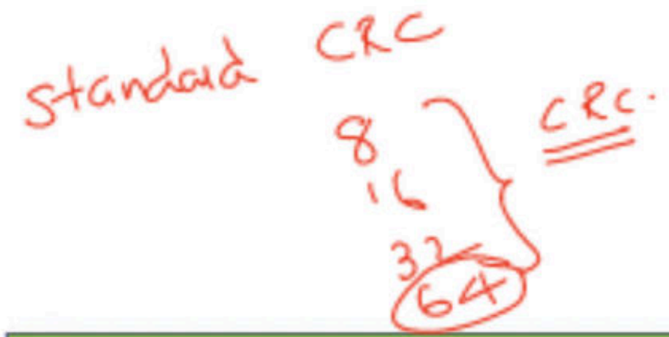
```
1101 | 10110110000
       1101
       ----
       01100110000
         1101
         ----
         00011100 0
           1101
           ----
           00000 1100
             1101
             ----
             0000000 001
```

CRC

Go on applying XOR

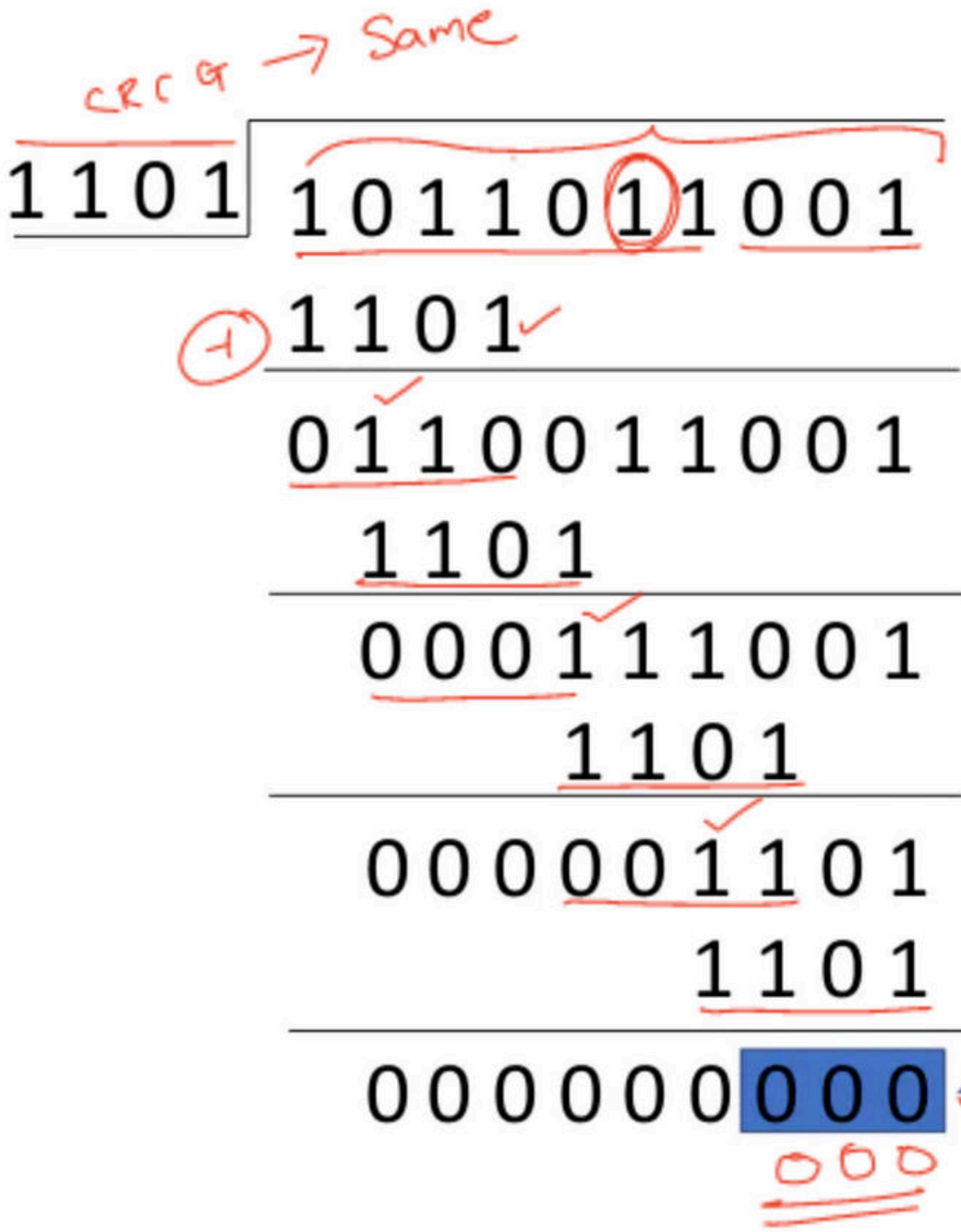






DATA SENT : 10110110001

RECEIVER'S SIDE



Go on applying XOR

CRC IS 0, DATA RECEIVED IS RIGHT!

000 → CRC 0's ∴ D ✓

CRC gen. ← 1101

1100111001 → Data

CRC.

CRC → function

$x^3 + x + 1$

⇓

$1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$

1011

Rec. ✓ 000

CRC ⇒ 0's ✓

Computer Networks

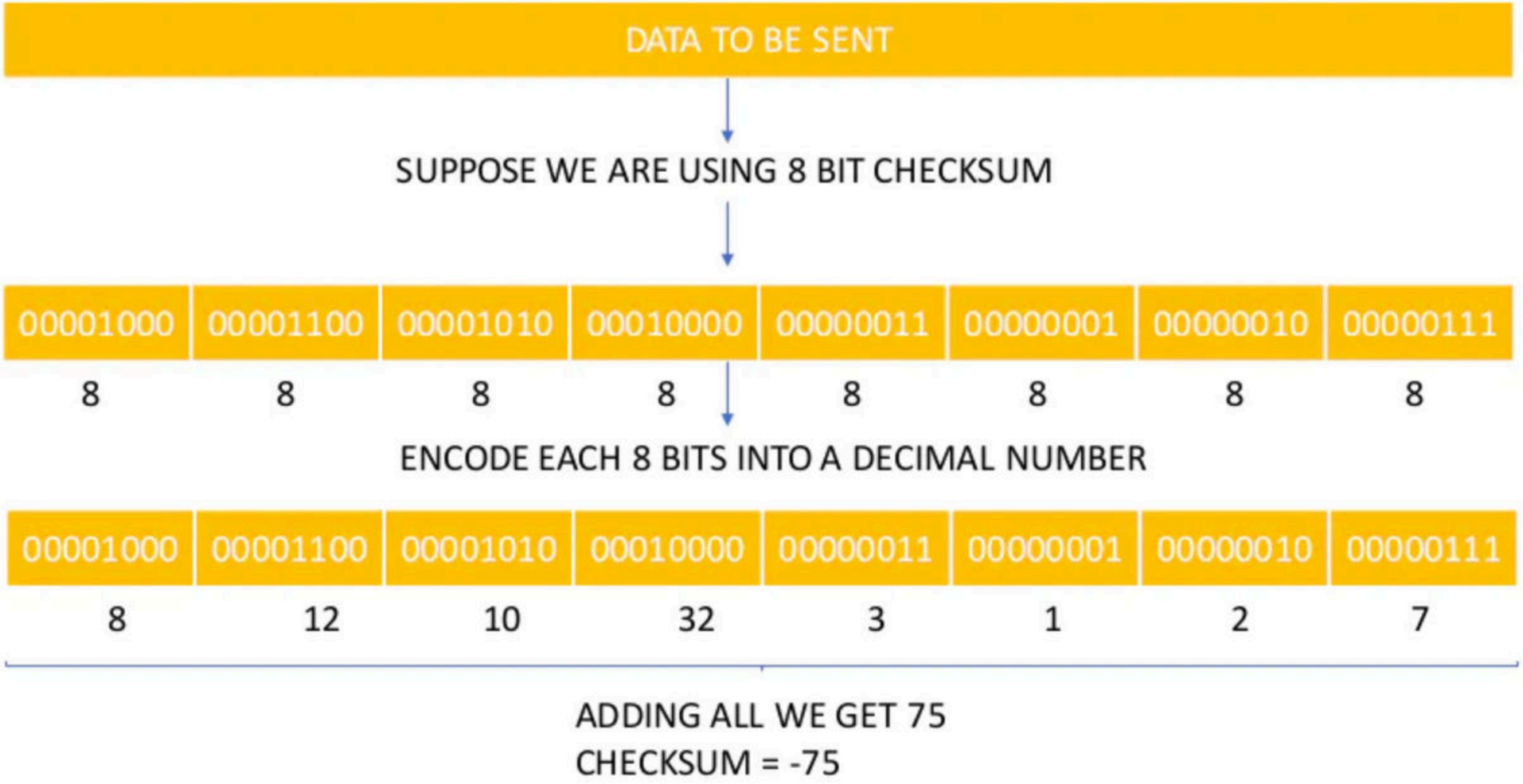
Error Control Methods PART 2

CHECKSUM

CHECK SUM

To verify

Addition

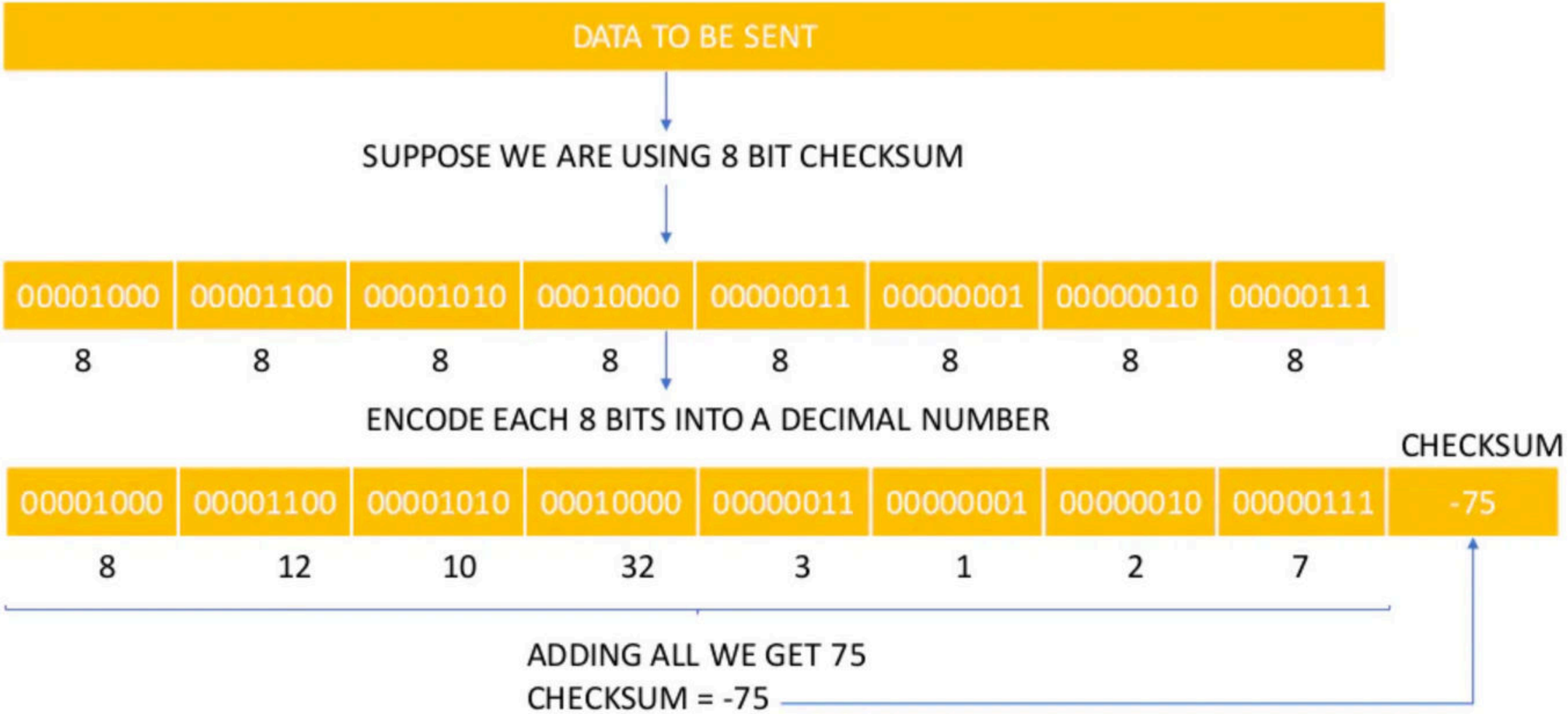


CHECKSUM

CHECK SUM

To verify

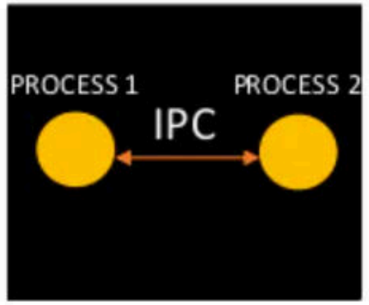
Addition



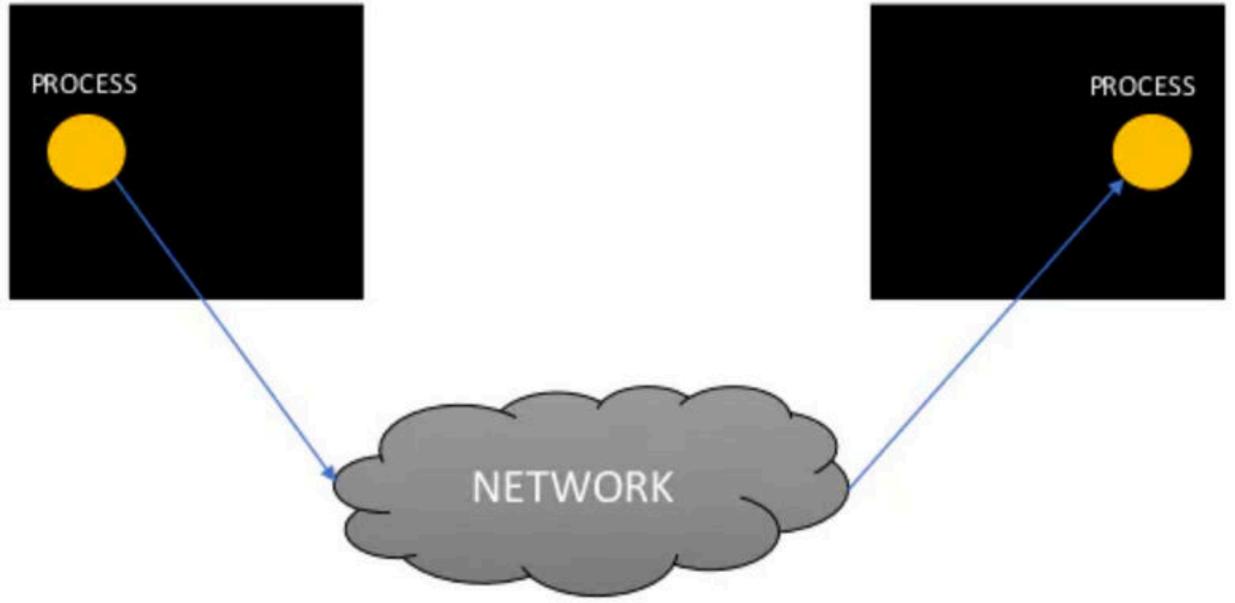
Computer Networks

ISO – OSI LAYERS

Communication between processes of same host



Communication between processes of different hosts



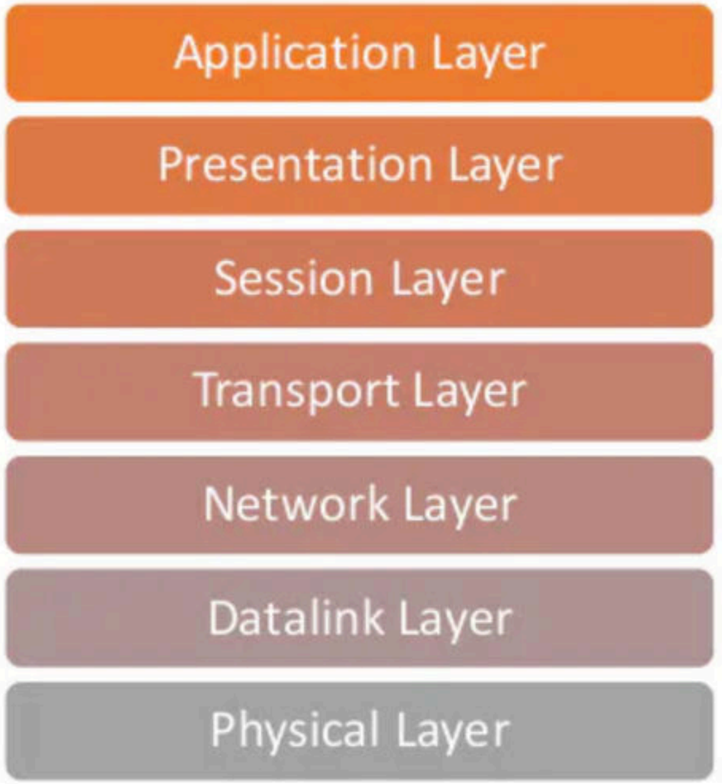
There are certain models that provide functionalities like OSI, TCP/IP,ATM,IEEE

ISO – OSI MODEL

ISO stands for International organization of Standardization.

OSI is Open System Interconnection and the model is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.
They are:



ADVANTAGES OF LAYERING

- DIVIDE AND CONQUER
- ENCAPSULATION
- ABSTRACTION
- TESTING

To Remember the Layers

Application Layer	ALLIGATOR
Presentation Layer	PET
Session Layer	STEVE'S
Transport Layer	TOUCH
Network Layer	NOT
Datalink Layer	DO
Physical Layer	PLEASE

Computer Networks

Physical Layer

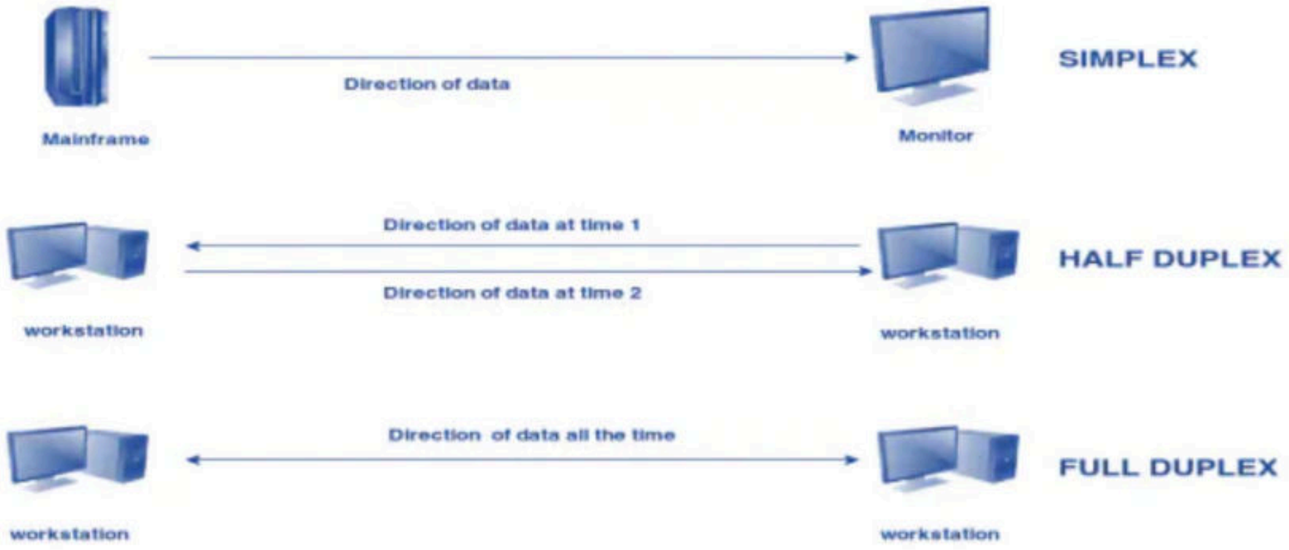
Functions of Physical Layer

1.) Physical Layer is electrical, mechanical, procedural and functional characteristics of physical links

It depends upon the type of links we are using to communicate.

If it is a copper wire then messages will be converted into electrical signals.
If link is an optical fibre then messages will be converted to light signals.
In case of Wireless communication, messages are sent into form of Electro Magnetic Waves.

2.) Physical Layer also includes the Transmission Mode – Simplex / Duplex



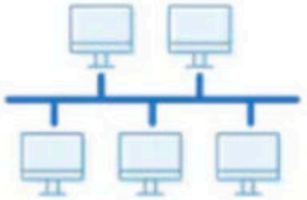
3.) Physical Layer also deals with Topologies

Point to Point topology is the simplest topology which connects two nodes directly together with a common link.

1 Point to point

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other

2 Bus



Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.

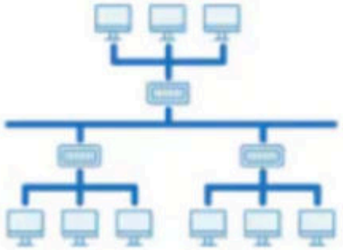
3 Ring

4 Star

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss.

Each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected.

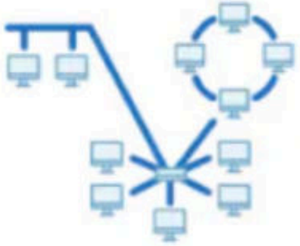
5 Tree



6 Mesh

A mesh topology is a network setup where each computer and network device is interconnected with one another.

7 Hybrid

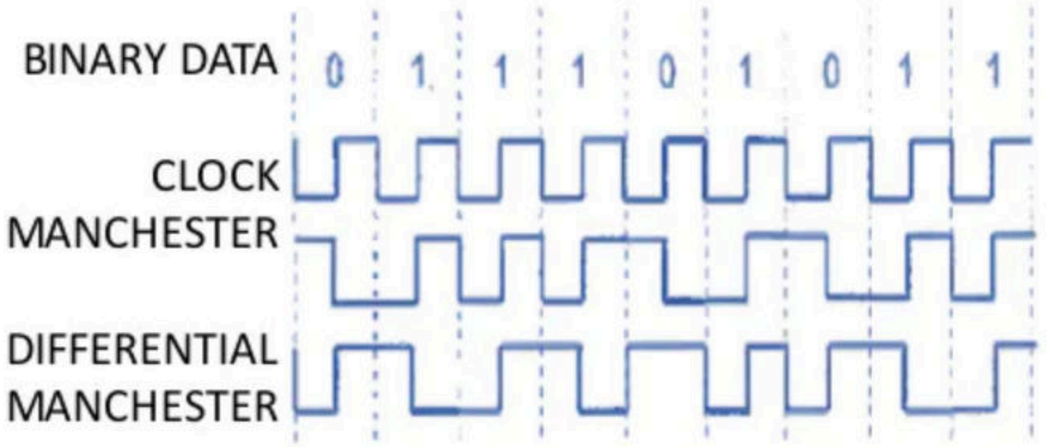


Hybrid topology is an integration of two or more different topologie s to form a resultant topology

4.) Encoding -

Encoding is a method of converting a stream of data bits into a predefined code. 1- To provide a predictable pattern that can be recognized by both the sender and the received. 2- To distinguish data bits from control bits and provide better media error detection. 3- To provide codes for control purposes such as identifying the beginning and end of a frame.

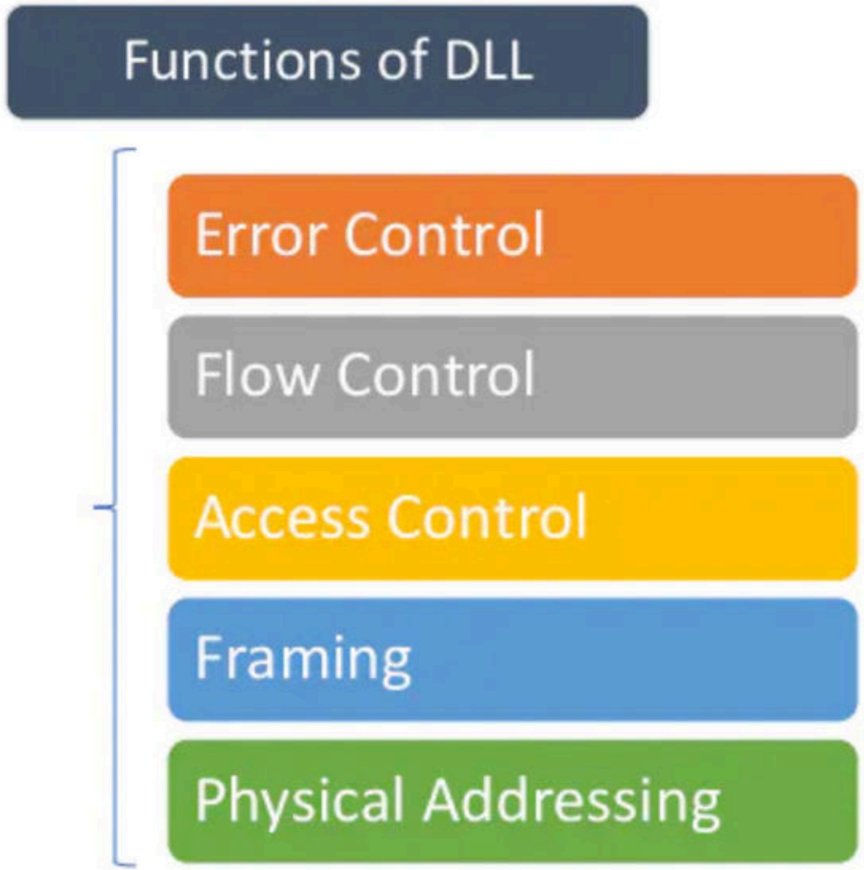
Signaling, the Physical layer must generate the electrical, optical, or wireless signals that represent the "1" and "0" on the media.



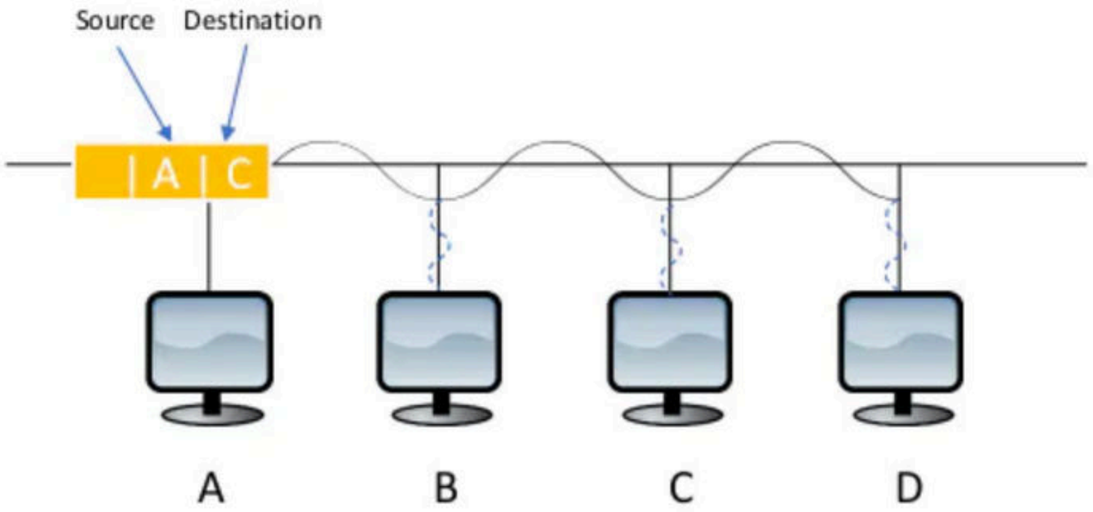
Baud rate = 2*bit rate

Computer Networks

Data Link Layer


Functions of DLL
Error Control
Flow Control
Access Control
Framing
Physical Addressing

FRAMING

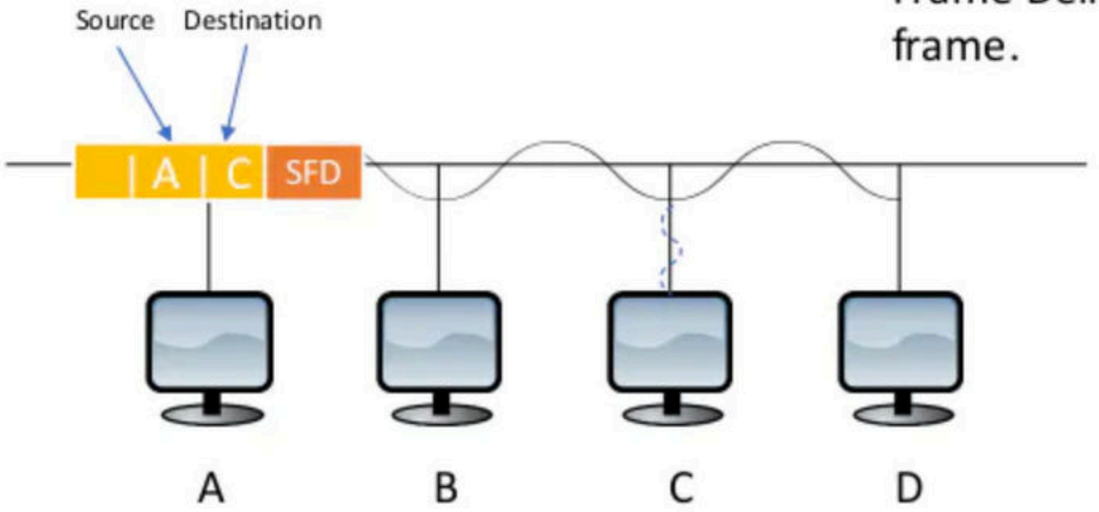


Suppose A wants to send a message to C.
It will send a frame which includes A and C as Source and Destination respectively.
The message would received by every node connected to the link but accepted by the one in the destination address of the message.
The question is,
When should any node look for a message?
Also, all the must only check the beginning of the Frame and see whether that frame is for them or no,
How will they know the beginning of the frame?

FRAMING

Start Frame Delimiter

It is a 1 byte field which is always set to 10101011. The last two bits "11" indicate the end of Start Frame Delimiter and marks the beginning of the frame.

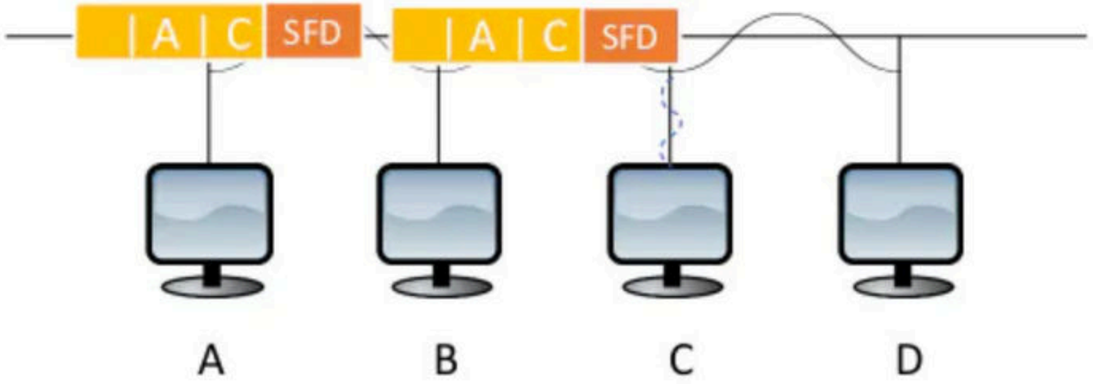


- The above two fields are added by the physical layer and represents the physical layer header.
- Sometimes, Start Frame Delimiter (SFD) is considered to be a part of Preamble.
- That is why, at many places, Preamble field length is described as 8 bytes.

SFD will be added at the beginning of the frame, So that the hosts will come to know that a data packet has arrived and they have to check the destination address that is after the SFD

FRAMING

Suppose after sending this frame,
A or some other station sends one more frame then C should know the end of the First frame i.e when it has to stop reading.



FRAMING

FIXED LENGTH

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.

VARIABLE LENGTH

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

Two ways to define frame delimiters in variable sized framing are :

•**Length Field** − Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).

•**End Delimiter** − Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situation −

- **Character-Stuffing** − A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.
- **Bit – Stuffing** − A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

GATE 2004 IT

In a data link protocol, the frame delimiter flag is given by 0111. Assuming that bit stuffing is employed, the transmitter sends the data sequence 01110110 as

A. 01101011

B. 011010110

C. 011101100

D. 0110101100

In the data link layer, bits stuffing is employed then bit stuffing is done using the flag delimiter. If there is a flag of n bits then we will compare the data sequence with the flag and for every n-1 bits matched found, a bit 0 is stuffed in the data sequence.

Thus using the above logic,

Delimiter flag: 0111

Data sequence: 01110110

So, for a flag of 4 bits we will compare data sequence with a pattern of 3 bits, i.e., 011.

0 1 1 0 1 0 1 1 0 0

In the above pattern the underlined bits are found matched. Hence, 0 in italics is stuffed. Thus resulting in the data sequence as 0110101100

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-

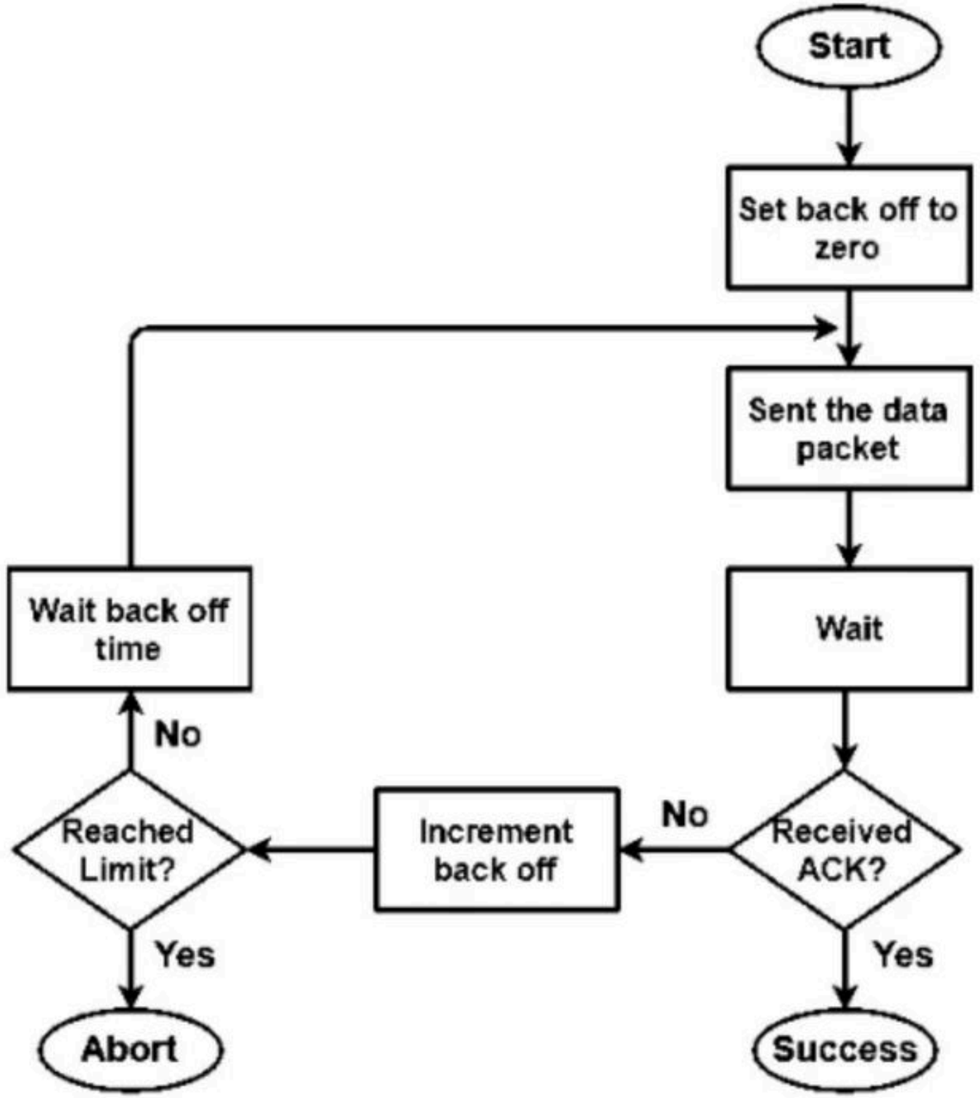
Case-01:

•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.



Flowchart for Pure Aloha

Efficiency-

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

where G = Number of stations willing to transmit data

Maximum Efficiency-

For maximum efficiency,

- We put $d\eta / dG = 0$
- Maximum value of η occurs at $G = 1/2$
- Substituting $G = 1/2$ in the above expression, we get-

Maximum efficiency of Pure Aloha

$= 1/2 \times e^{-2 \times 1/2}$

$= 1 / 2e$

$= 0.184$

$= 18.4\%$

Thus, Maximum Efficiency of Pure Aloha (η) = 18.4%

2. 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.

Efficiency-

$$\text{Efficiency of Slotted Aloha } (\eta) = G \times e^{-G}$$

where G = Number of stations willing to transmit data at the beginning of the same time slot

Maximum Efficiency-

For maximum efficiency,

- We put $d\eta / dG = 0$
- Maximum value of η occurs at $G = 1$
- Substituting $G = 1$ in the above expression, we get-

Maximum efficiency of Slotted Aloha

$= 1 \times e^{-1}$

$= 1 / e$

$= 0.368$

$= 36.8\%$

Thus,

Maximum Efficiency of Slotted Aloha (η) = 36.8%

Pure Aloha	Slotted Aloha
Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
Vulnerable time in which collision may occur $= 2 \times T_t$	Vulnerable time in which collision may occur $= T_t$
Probability of successful transmission of data packet $= G \times e^{-2G}$	Probability of successful transmission of data packet $= G \times e^{-G}$
Maximum efficiency = 18.4% (Occurs at G = 1/2)	Maximum efficiency = 36.8% (Occurs at G = 1)
The main advantage of pure aloha is its simplicity in implementation.	The main advantage of slotted aloha is that it reduces the number of collisions to half and doubles the efficiency of pure aloha.

Computer Networks

Practice questions on Access Control Methods and GATE PYQ

Problem 1: GATE2015(CS)

Consider a CSMA/CD network that transmits data at a rate of 100 Mbps (10^8 bits per second) over a 1 km (kilometer) cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, what is the signal speed (km/sec) in the cable?

(A) 8000
(B) 10000
(C) 16000
(D) 20000

Solution:

Data should be transmitted at the rate of 100 Mbps.

Transmission Time >= 2*Propagation Time
= 1250*8 / (100 * 10^6)
= 2*length/signal speed
= signal speed = (2 * 10^3 * 100 * 10^6) / (1250 * 8)
= 2 * 10 * (10^3) km/sec = 20000

D is correct.

Problem 2: GATE2016(CS)

Consider a LAN with four nodes S1, S2, S3 and S4. Time is divided into fixed-size slots, and a node can begin its transmission only at the beginning of a slot. A collision is said to have occurred if more than one node transmit in the same slot. The probabilities of generation of a frame in a time slot by S1, S2, S3 and S4 are 0.1, 0.2, 0.3 and 0.4, respectively. The probability of sending a frame in the first slot without any collision by any of these four stations is _____.

(A) 0.462
(B) 0.711
(C) 0.5
(D) 0.652

Solution:

The probability of sending a frame in the first slot
without any collision by any of these four stations is sum of following 4 probabilities
Probability that S1 sends a frame and no one else does
+ Probability thatS2 sends a frame and no one else does
+ Probability thatS3 sends a frame and no one else does
+ Probability thatS4 sends a frame and no one else does
= 0.1 * (1 - 0.2) * (1 - 0.3) *(1 - 0.4)
+ (1 -0.1) * 0.2 * (1 - 0.3) *(1 - 0.4)
+ (1 -0.1) * (1 - 0.2) * 0.3 *(1 - 0.4)
+ (1 -0.1) * (1 - 0.2) * (1 - 0.3) * 0.4
= 0.4404

Problem-3:

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

Solution-

Given-

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

Calculating Propagation Delay-

Propagation delay (T_p)

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

Calculating Minimum Frame Size-

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

Computer Networks

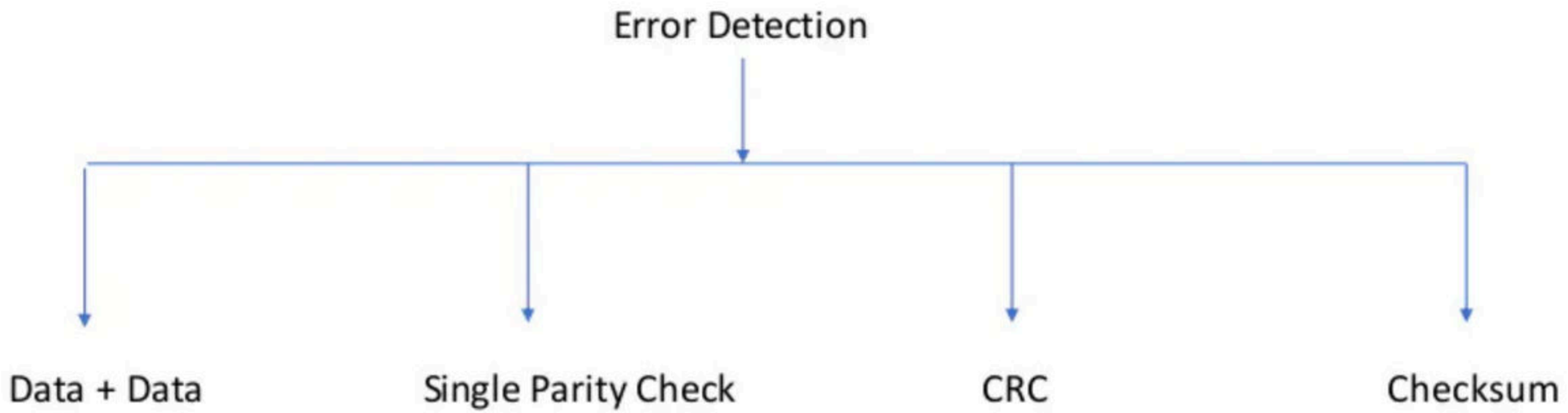
Error Control Methods PART 1

Error Detection

Error detection is a technique that is used to check if any error occurred in the data during the transmission.

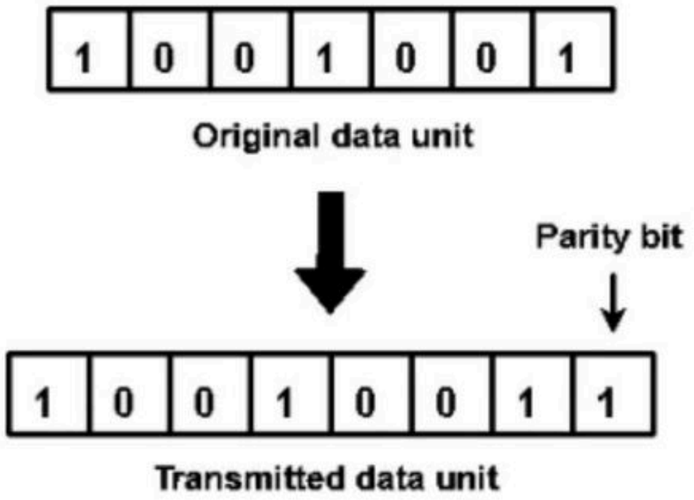
Error Correction

Error Correction is a technique that is used to correct error occurred in the data by its own during the transmission.


Error Detection
Data + Data
Single Parity Check
CRC
Checksum

Single Parity Check-

In this technique,
•One extra bit called as **parity bit** is sent along with the original data bits.
•Parity bit helps to check if any error occurred in the data during the transmission.



Limitation-

•This technique can not detect an even number of bit errors (two, four, six and so on).
•If even number of bits flip during transmission, then receiver can not catch the error.

Cyclic Redundancy Check-

- Cyclic Redundancy Check (CRC) is an error detection method.
- It is based on binary division.

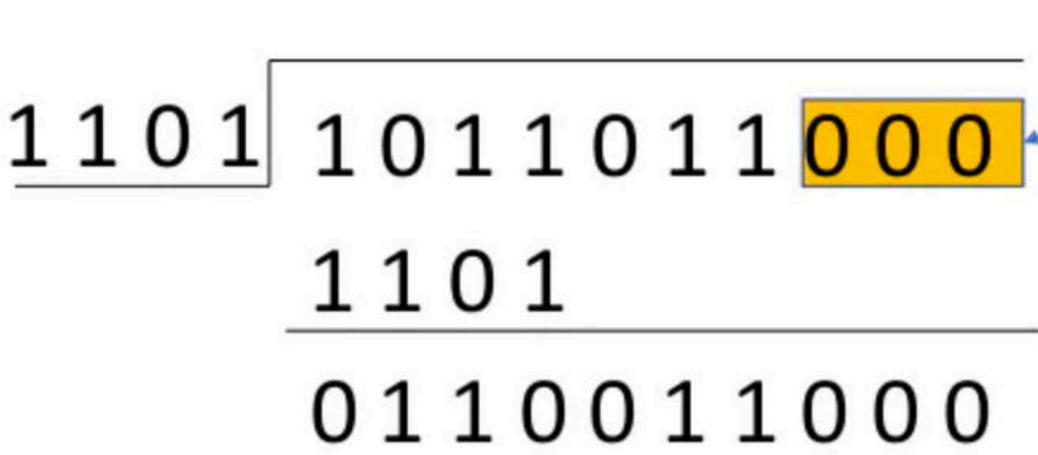
Cyclic Generator-

Data to be sent : 1 0 1 1 0 1 1
CRC generator: 1 1 0 1

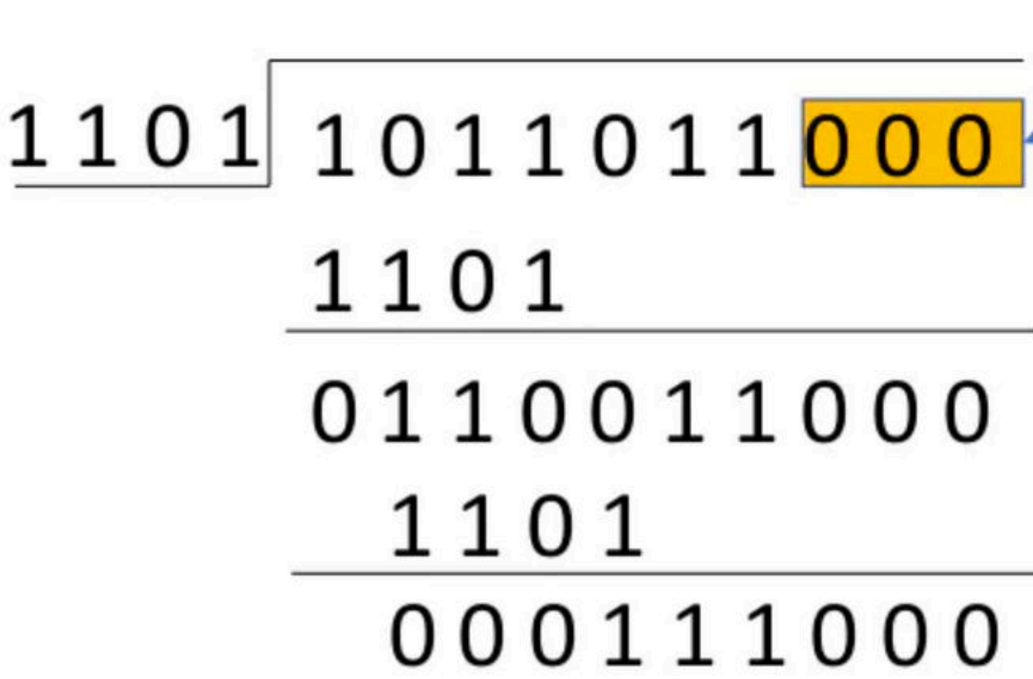
CRC generator is 4 bits
There for sender appends 3 bits of 0's to the data

Note: if CRCG= n bits then bits to be appended in data is (n-1) 0's

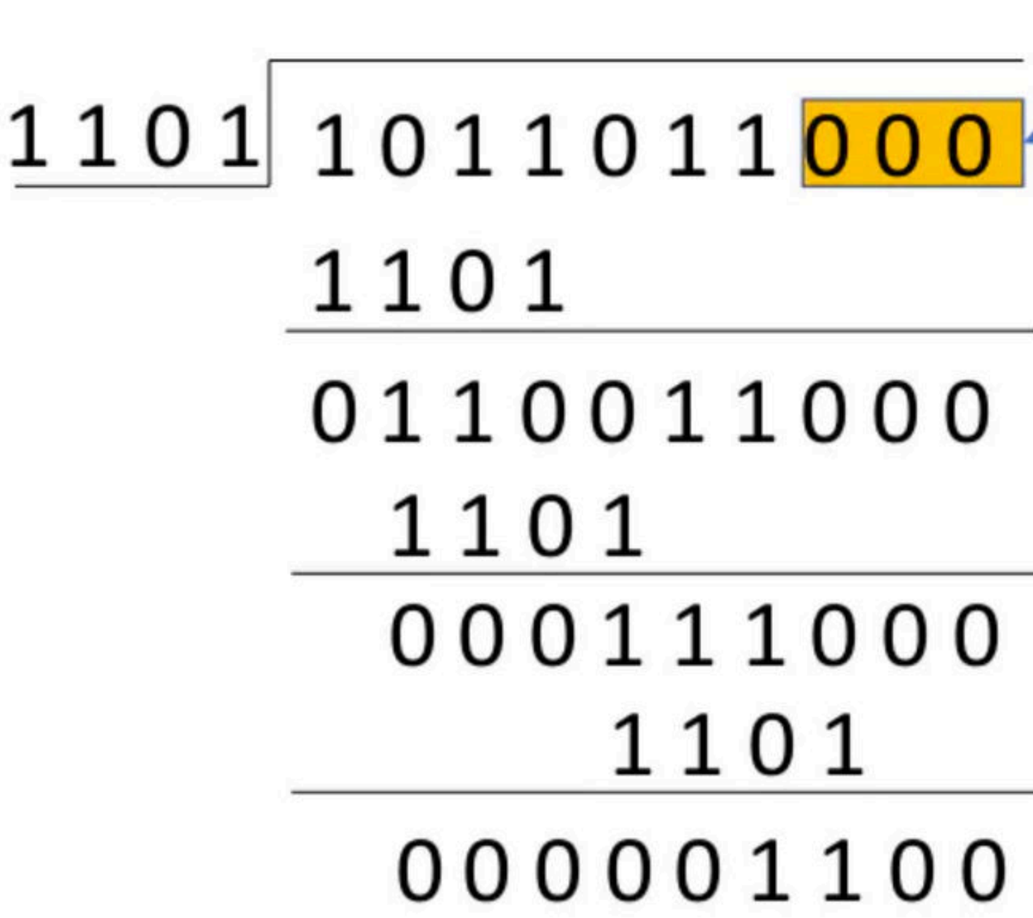
SENDER'S SIDE



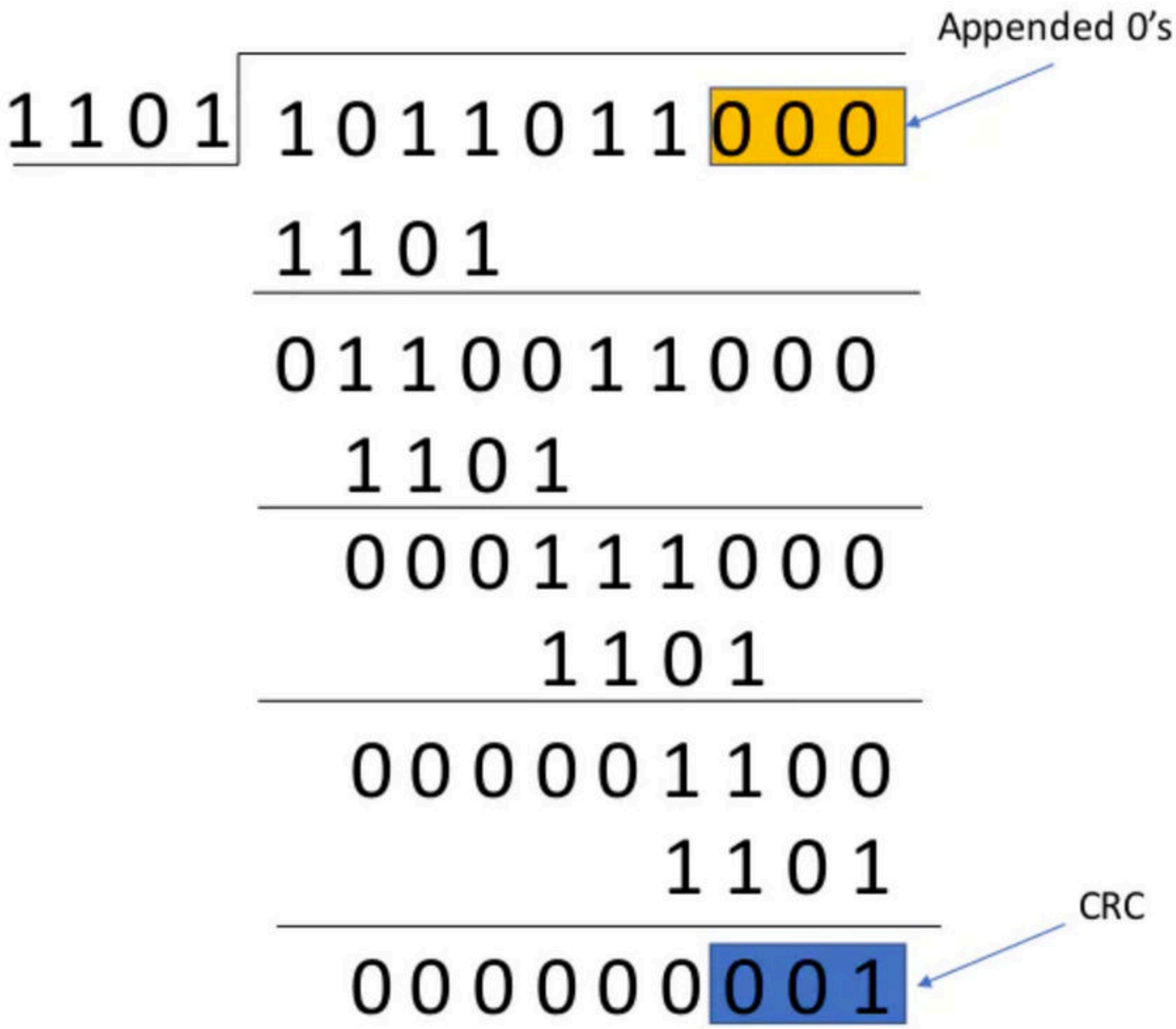
Go on applying XOR



Go on applying XOR



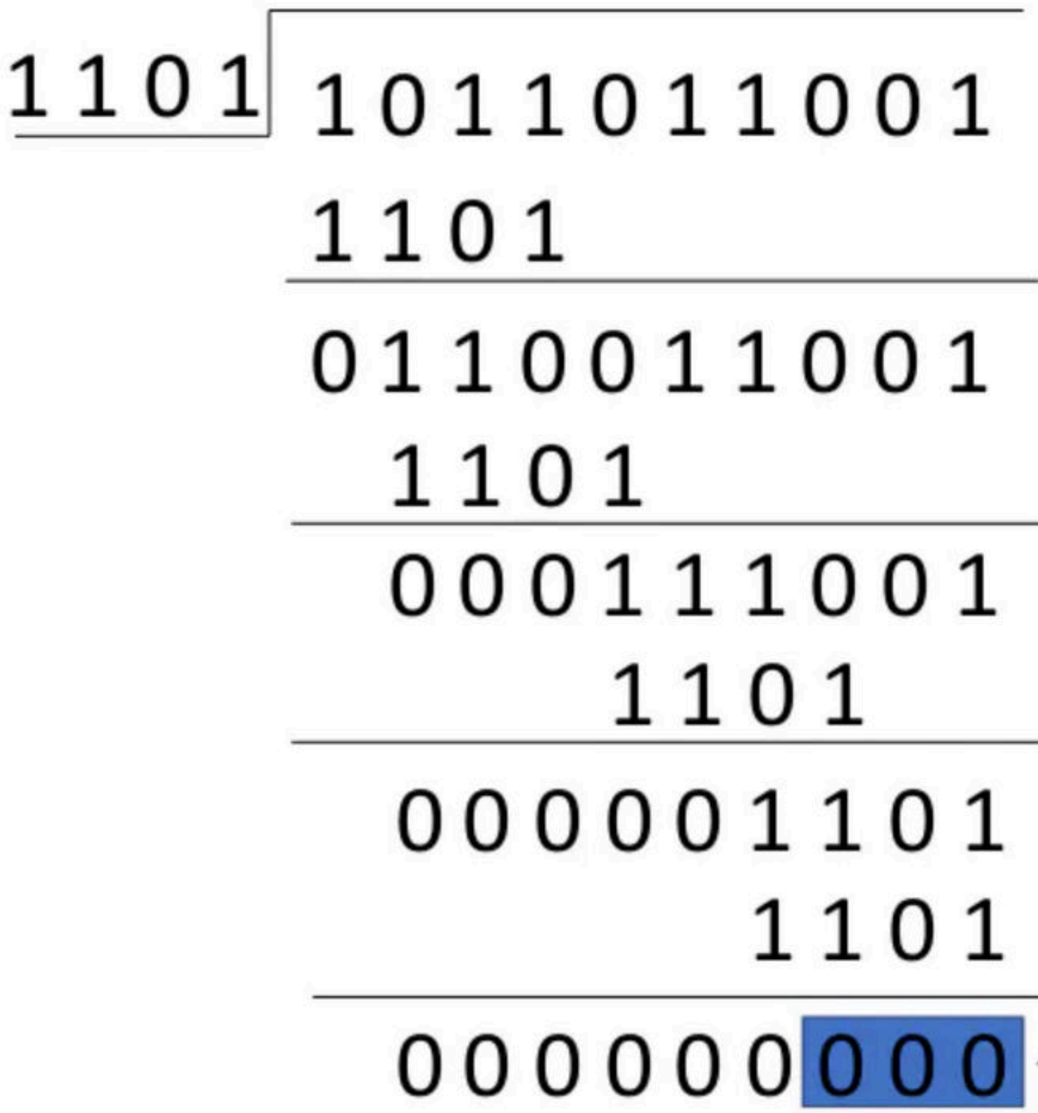
Go on applying XOR



Go on applying XOR

DATA SENT : 1 0 1 1 0 1 1 0 0 1

RECEIVER'S SIDE



Go on applying XOR

CRC IS 0, DATA RECEIVED IS RIGHT!