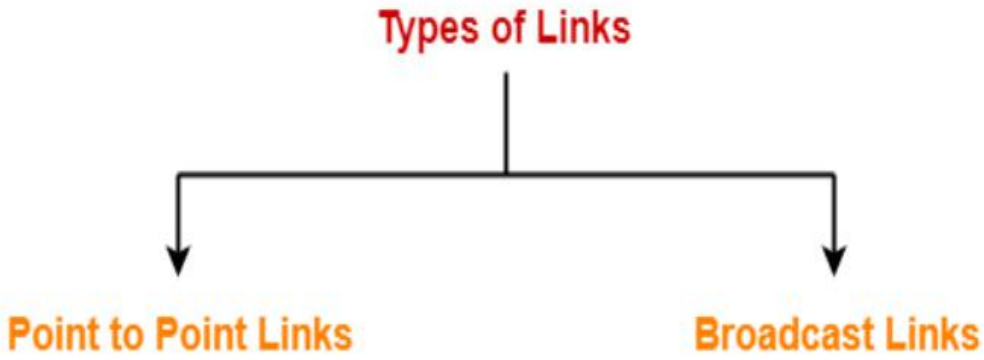
CN: WEEK 10

Access Control in Networking



Point to Point Link-

- Point to Point link is a dedicated link that exists between the two stations.
- The entire capacity of the link is used for transmission between the two connected stations only.
- Depending upon the Type Of Channel, the data flow takes place between the stations.

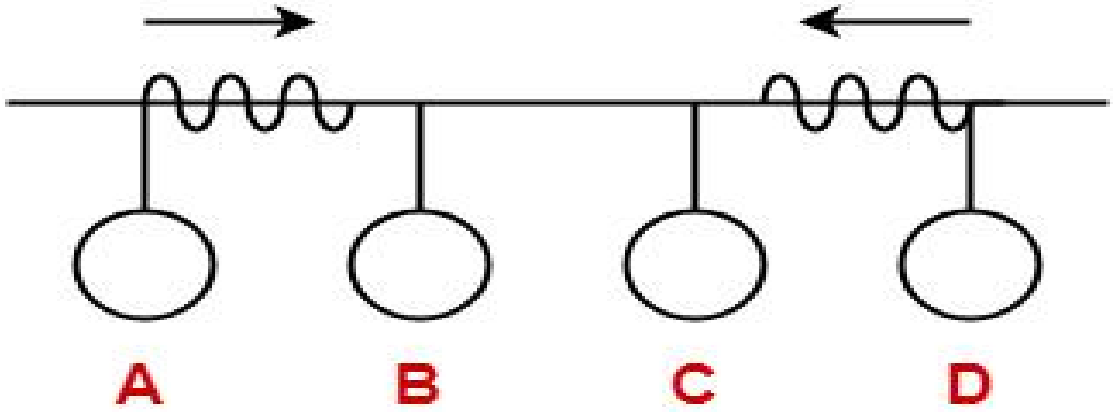
Broadcast Link-

- Broadcast link is a common link to which multiple stations are connected.
- The capacity of the link is shared among the connected stations for transmission.

- Access Control is a mechanism that controls the access of stations to the transmission link.
- Broadcast links require the access control.
- This is because the link is shared among several stations.

Consider a situation where-

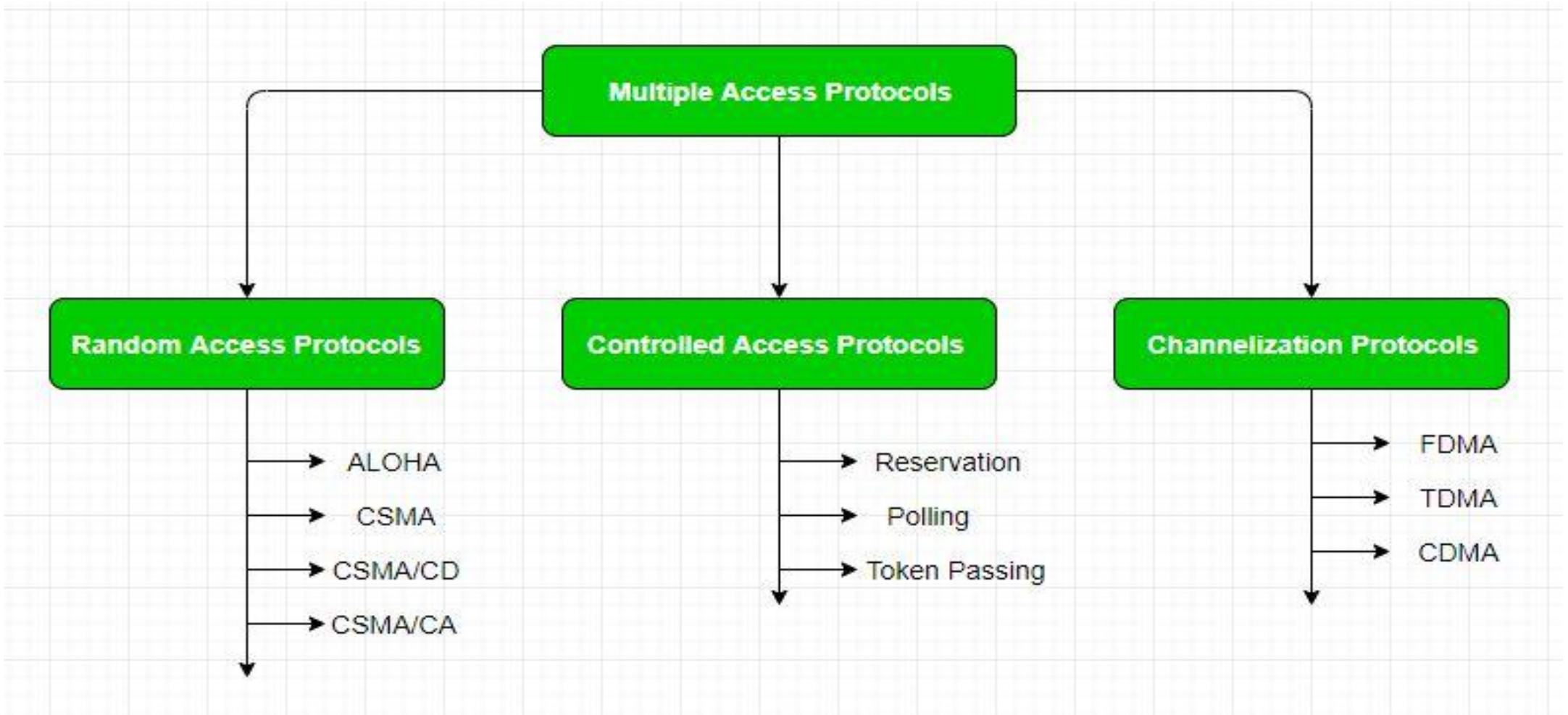
Multiple stations place their data packets on the link and starts transmitting simultaneously.
Such a situation gives rise to a collision among the data packets.
Collision of data packets causes the data to get corrupt.
To prevent the occurrence of collision or if the collision occurs, to deal with it.



Here,

- ✓ Two stations A and D starts transmitting their data packets simultaneously.
- ✓ This situation gives rise to a collision between the data packets transmitted by them.
- ✓ Thus, to prevent the collision or to deal with it, access control is needed.

- ***Access control methods are the methods used for providing access control.***
- ***They prevent the collision or deal with it and ensures smooth flow of traffic on the network.***
- ***They are implemented at the data link layer of the OSI reference model.***

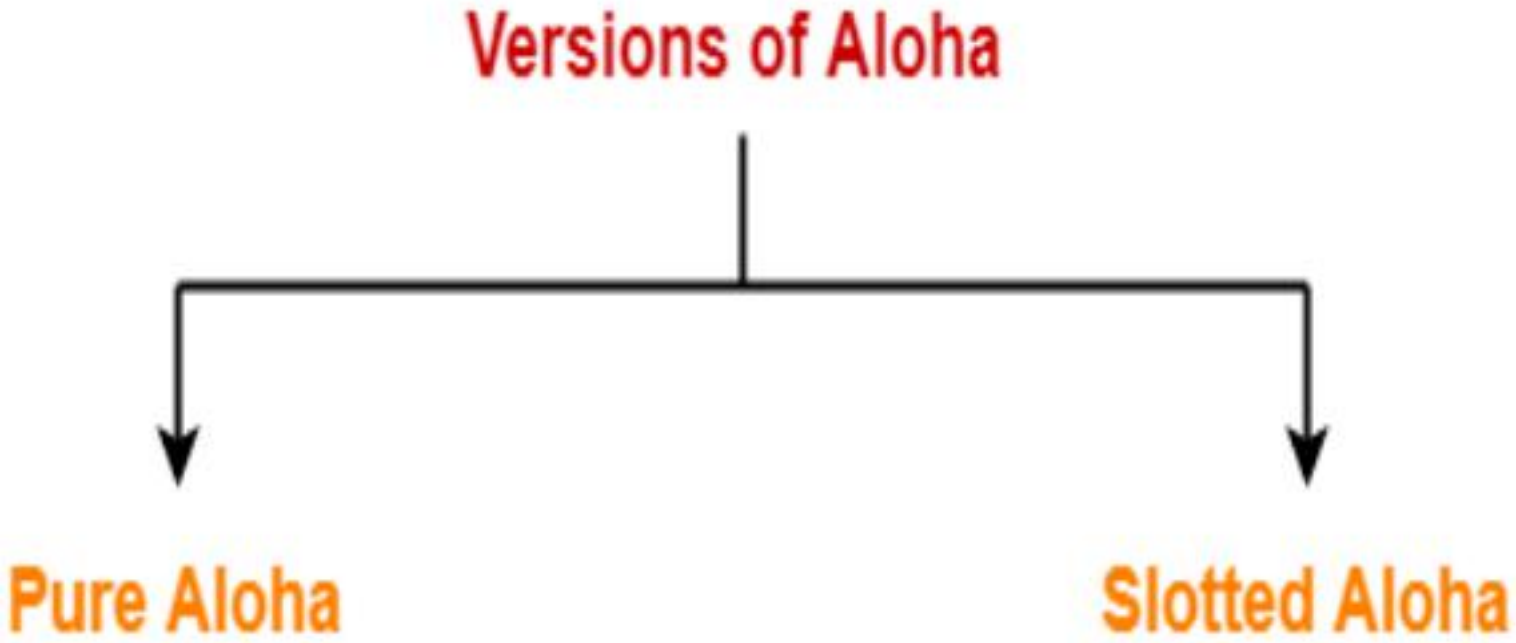


In Random Access Protocol, all stations have same superiority that is no station has more priority than another station.

In Controlled Access Protocol, the data is sent by that station which is approved by all other stations.

In Channelization Protocol, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

Aloha


Versions of Aloha
Pure Aloha
Slotted Aloha

Pure Aloha-

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

Then, following 2 cases are possible-

Case-01:

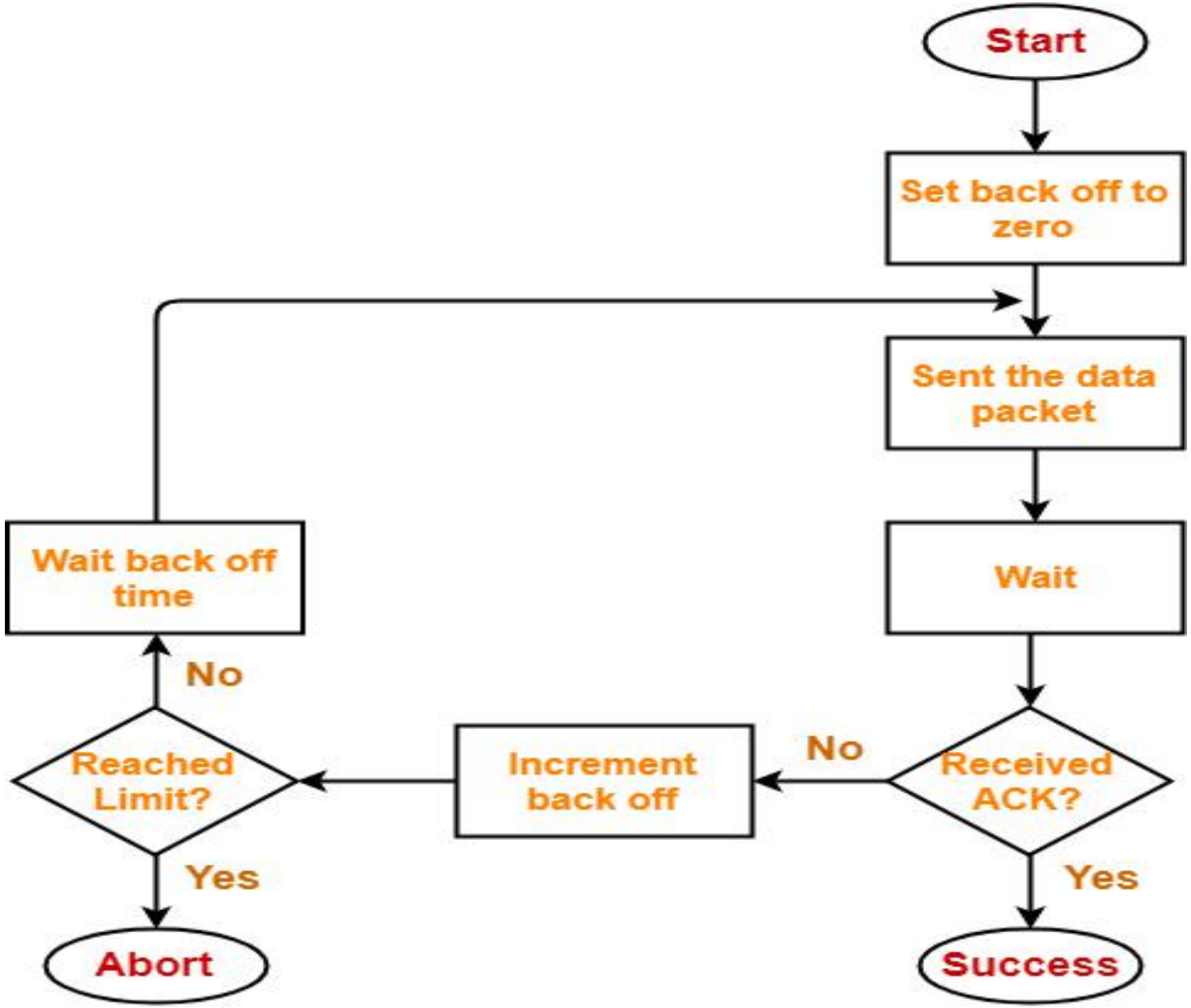
Transmitting station receives an acknowledgement from the receiving station.
In this case, transmitting station assumes that the transmission is successful.

Case-02:

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

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-

The maximum efficiency of Pure Aloha is very less due to large number of collisions.

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%

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-

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

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%

The maximum efficiency of Slotted Aloha is high due to less number of collisions.

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.

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

Throughput Of One Station-

Throughput of each station

= Number of bits sent per second

= 500 bits / 5000 ms

= 500 bits / (5000 x 10^{-3} sec)

= 100 bits/sec

Throughput Of Slotted Aloha-

Throughput of slotted aloha

= Efficiency x Bandwidth

= 0.368 x 100 Kbps

= 36.8 Kbps

Total Number Of Stations-

Throughput of slotted aloha = Total number of stations x Throughput of each station

Substituting the values, we get-

36.8 Kbps = N x 100 bits/sec

∴ N = 368

CSMA / CD

CSMA / CD stands for Carrier Sense Multiple Access / Collision Detection

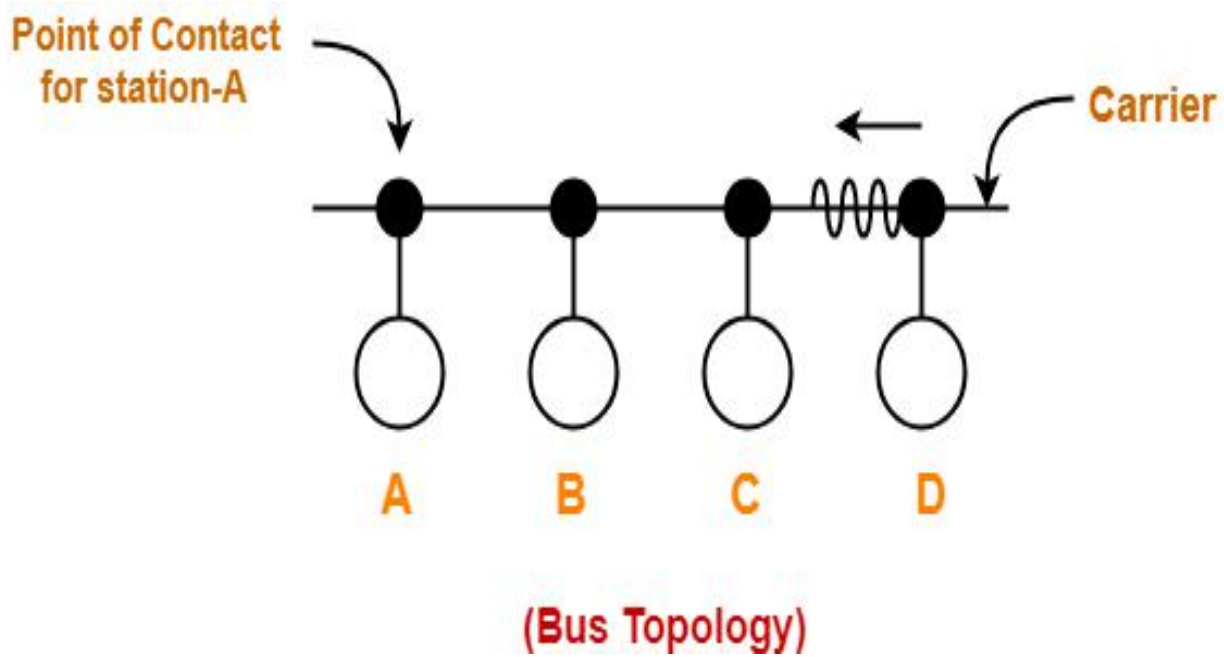
This access control method works as follows-

- ***Step-01: Sensing the Carrier***
- ***Step-02: Detecting the Collision***
- ***Step-03: Releasing Jam Signal***
- ***Step-04: Waiting For Back Off Time***

Step-01: Sensing the Carrier

- Any station willing to transmit the data senses the carrier.
- If it finds the carrier free, it starts transmitting its data packet otherwise not.
- Each station can sense the carrier only at its point of contact with the carrier.
- It is not possible for any station to sense the entire carrier.
- Thus, there is a huge possibility that a station might sense the carrier free even when it is actually not.

If station A senses the carrier at its point of contact, then it will find the carrier free. But the carrier is actually not free because station D is already transmitting its data. If station A starts transmitting its data now, then it might lead to a collision with the data transmitted by station D.



(Bus Topology)

Step-02: Detecting the Collision

In CSMA / CD,

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

According to this condition,

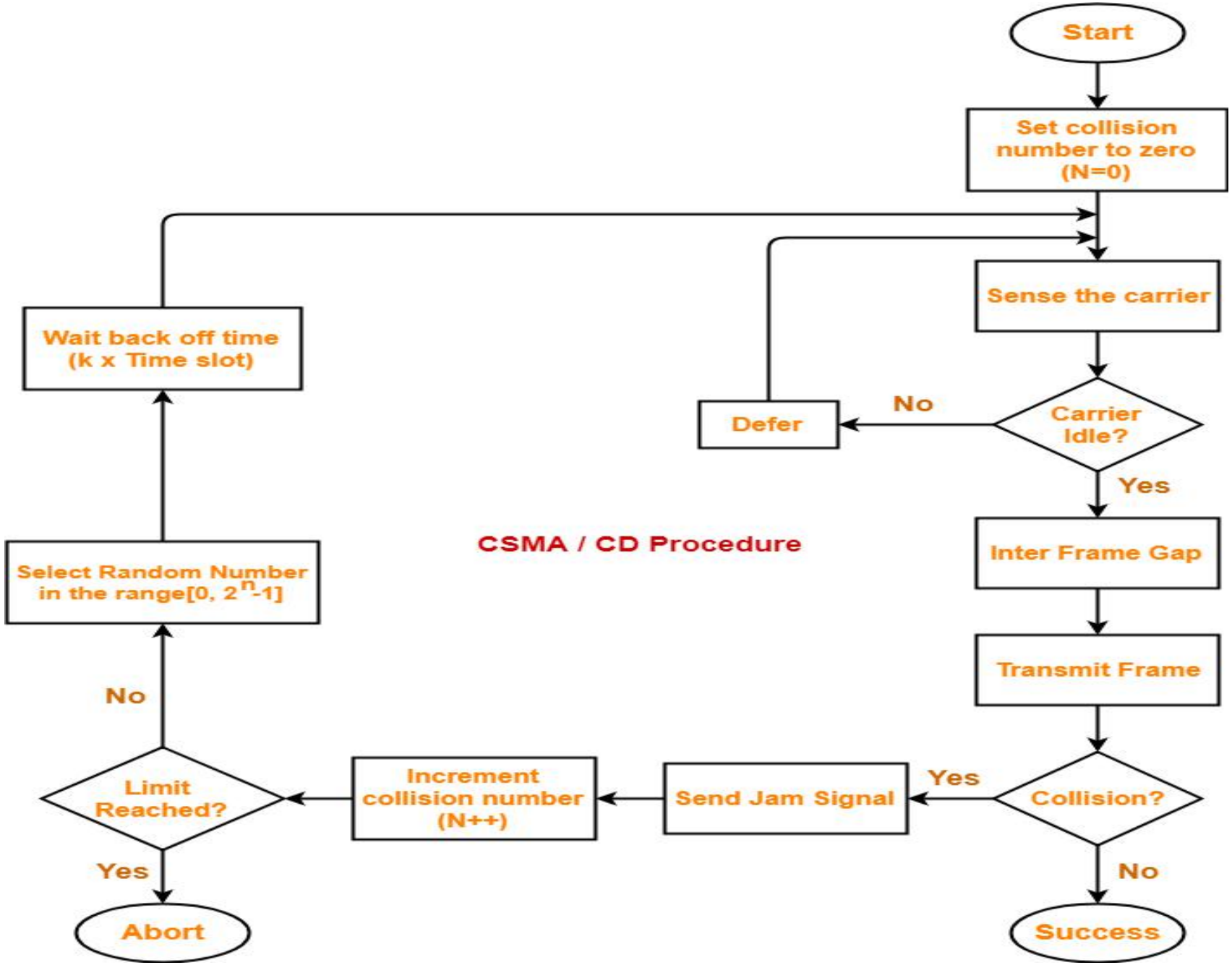
Each station must transmit the data packet of size whose transmission delay is at least twice its propagation delay. If the size of data packet is smaller, then collision detection would not be possible.

Step-03: Releasing Jam Signal

- Jam signal is a 48 bit signal.
- It is released by the transmitting stations as soon as they detect a collision.
- It alerts the other stations not to transmit their data immediately after the collision.
- Otherwise, there is a possibility of collision again with the same data packet.
- Ethernet sends the jam signal at a frequency other than the frequency of data signals.
- This ensures that jam signal does not collide with the data signals undergone collision.

Step-04: Waiting For Back Off Time

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


Start
Set collision number to zero (N=0)
Sense the carrier
Carrier Idle?
No
Defer
Yes
Inter Frame Gap
Transmit Frame
Collision?
Yes
Send Jam Signal
Increment collision number (N++)
Limit Reached?
No
Select Random Number in the range[0, 2^n-1]
Wait back off time (k x Time slot)
Yes
Abort
No
Success
CSMA / CD Procedure

Efficiency-

Efficiency (η) = Useful Time / Total Time

Before a successful transmission,

- There may occur many number of collisions.
- 2 x T_p time is wasted during each collision.

Thus,

- Useful time = Transmission delay of data packet = T_t
- Useless time = Time wasted during collisions + Propagation delay of data packet = c x 2 x T_p + T_p
- Here, c = Number of contention slots / collision slots.

$$\text{Efficiency } (\eta) = \frac{T_t}{c \times 2 \times T_p + T_t + T_p}$$

Average number of collisions before a successful transmission = e

Substituting c = e in the above relation, we get-

$$\text{Efficiency } (\eta) = \frac{T_t}{e \times 2 \times T_p + T_t + T_p}$$

OR

$$\text{Efficiency } (\eta) = \frac{T_t}{T_t + 6.44 \times T_p}$$

$$\text{Efficiency } (\eta) = \frac{1}{1 + 6.44 \times a}, \text{ where } a = T_p / T_t$$

Important Notes

Note-01:

CSMA / CD is used in wired LANs.
CSMA / CD is standardized in IEEE 802.3

Note-02:

CSMA / CD only minimizes the recovery time.
It does not take any steps to prevent the collision until it has taken place.

Important Formulas-

Condition to detect collision: Transmission delay >= 2 x Propagation delay
Minimum length of data packets in CSMA / CD = 2 x Bandwidth x Distance / Speed
Efficiency of CSMA / CD = 1 / (1 + 6.44 x a) where a = Tp / Tt

We have discussed-

- CSMA / CD allows a station to transmit data if it senses the carrier free.
- After undergoing collision, station waits for random back off time before transmitting again.
- Back Off Algorithm is used to calculate back off time.

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?

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

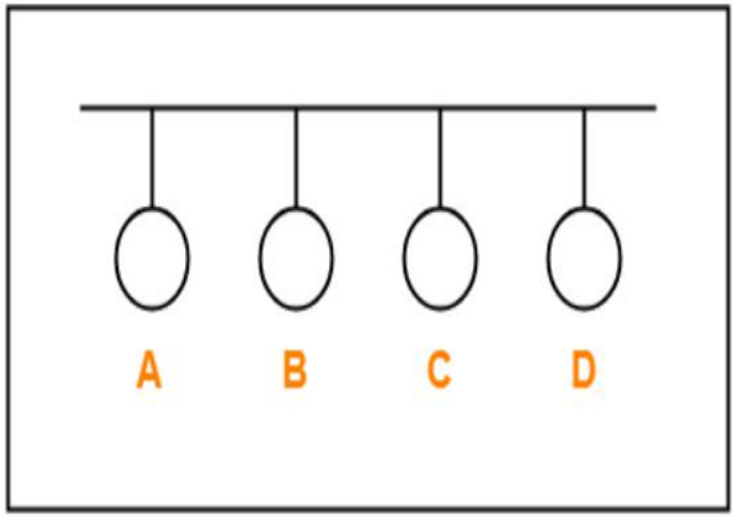
A 2 km long broadcast LAN has 107 bps bandwidth and uses CSMA / CD. The signal travels along the wire at 2×10^8 m/sec. What is the minimum packet size that can be used on this network?

50 B
100 B
200 B
None of the above

Polling

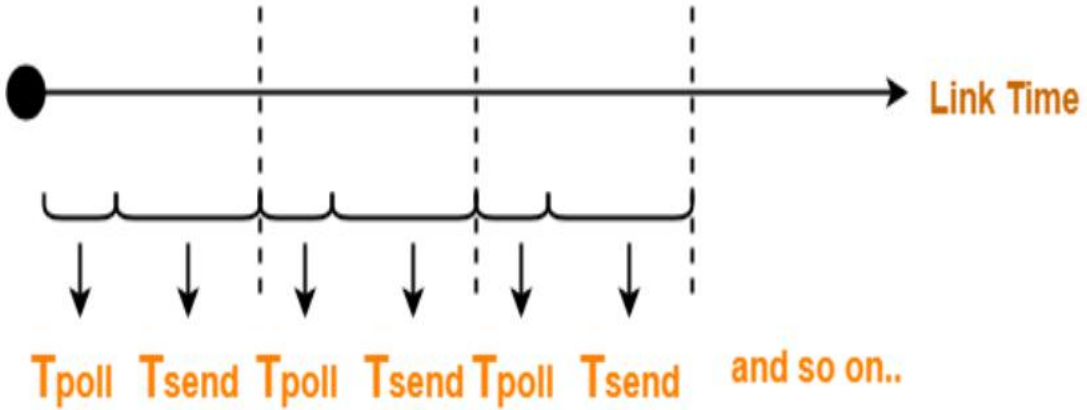
In this access control method,

- **A polling is conducted in which all the stations willing to send data participates.**
- **The polling algorithm chooses one of the stations to send the data.**
- **The chosen station sends the data to the destination.**
- **After the chosen station has sent the data, the cycle repeats.**



Here-

- T_{poll} = Time taken for polling
- T_{send} = Time taken for sending the data = Transmission delay + Propagation delay = $T_t + T_p$



Polling Access Control Method

Efficiency-

Efficiency (η) = Useful Time / Total Time

- Useful time = Transmission delay of data packet = T_t
- Useless time = Time wasted during polling + Propagation delay of data packet = $T_{poll} + T_p$

$$\text{Efficiency } (\eta) = \frac{T_t}{T_{poll} + T_t + T_p}$$

Advantages-

- Unlike in Time Division Multiplexing, no slot is ever wasted.
- It leads to maximum efficiency and bandwidth utilization.

Disadvantages-

- Time is wasted during polling.
- Link sharing is not fair since each station has the equal probability of winning in each round.
- Few stations might starve for sending the data.

Important Formulas-

- Efficiency (η) = T_t / (T_{poll} + T_t + T_p)
- Effective Bandwidth / Bandwidth Utilization / Throughput = Efficiency(η) x Bandwidth
- Maximum Available Effective Bandwidth = Total number of stations x Bandwidth requirement of 1 station

Time Division Multiplexing

In Time Division Multiplexing (TDM),

- **Time of the link is divided into fixed size intervals called as time slots or time slices.**
- **Time slots are allocated to the stations in Round Robin manner.**
- **Each station transmit its data during the time slot allocated to it.**
- **In case, station does not have any data to send, its time slot goes waste.**
- **The size of each time slot is kept such that each station gets sufficient time for the following tasks-**
  - **To put its data packet on to the transmission link**
  - **Last bit of the packet is able to get out of the transmission link**

Thus,

Size of each time slot = $T_t + T_p$

where-

- Tt = Transmission delay
- Tp = Propagation delay

Efficiency-

Efficiency (η) = Useful Time / Total Time

- Useful time = Transmission delay of data packet = T_t
- Useless time = Propagation delay of data packet = T_p

$$\text{Efficiency } (\eta) = \frac{T_t}{T_t + T_p}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{1 + a} \quad \text{where } a = \frac{T_p}{T_t}$$

Important Formulas-

- Size of each time slot in Time Division Multiplexing = $T_t + T_p$
- Efficiency (η) = 1 / (1+a) where a = T_p / T_t
- Effective Bandwidth / Bandwidth Utilization / Throughput = Efficiency(η) x Bandwidth
- Maximum Available Effective Bandwidth = Total number of stations x Bandwidth requirement of 1 station

Disadvantage-

- If any station does not have the data to send during its time slot, then its time slot goes waste.
- This reduces the efficiency.
- This time slot could have been allotted to some other station willing to send data.

If transmission delay and propagation delay of a packet in Time Division Multiplexing is 1 msec each at 4 Mbps bandwidth, then-

- ✓ **Find the efficiency.**
- ✓ **Find the effective bandwidth.**
- ✓ **How many maximum stations can be connected to the network if each station requires 2 Kbps bandwidth?**

Given-

- Transmission delay (T_t) = 1msec
- Propagation delay (T_p) = 1msec
- Bandwidth = 4 Mbps

Part-01:

For a TDM Network,

Efficiency (η) = 1 / 1+a where a = T_p / T_t

Calculating Value Of 'a'-

a = T_p / T_t
a = 1 msec / 1 msec
a = 1

Calculating Efficiency-

Efficiency (η)
= 1 / (1+a)
= 1 / (1 + 1)
= 1 / 2
= 50%

Part-02:

We know-

Effective Bandwidth = Efficiency (η) x Bandwidth

Thus,
Effective Bandwidth
= 0.5 x 4 Mbps
= 2 Mbps

Part-03:

We know-

Maximum Effective Bandwidth
= Total number of stations x Bandwidth requirement of 1 station

Let the total number of stations that can be connected be N.

Then, we have-

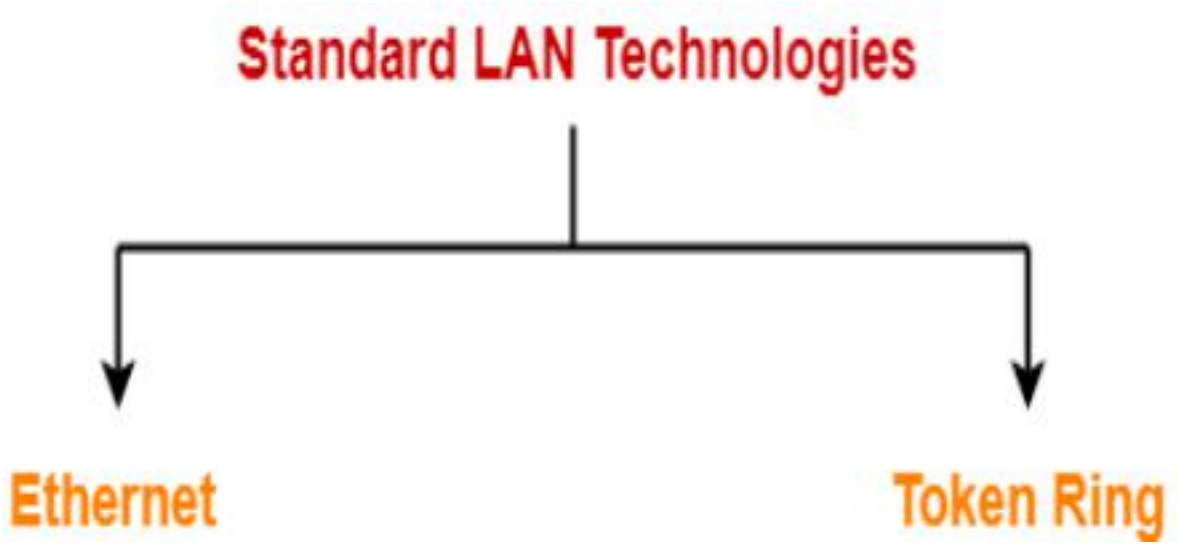
2 Mbps = N x 2 Kbps

N = 1000

Thus, maximum 1000 stations can be connected.

Ethernet

- A Local Area Network (LAN) is a network of computers.
- It is confined to a small area which may be a room, building or a group of buildings.
- A LAN may be wired, wireless or a combination of the two.



- Ethernet is one of the standard LAN technologies used for building wired LANs.
- It is defined under IEEE 802.3.

Characteristics-

- Ethernet uses bus topology.
- In bus topology, all the stations are connected to a single half duplex link.

- Ethernet uses CSMA / CD as access control method to deal with the collisions.

- Ethernet uses Manchester Encoding Technique for converting data bits into signals.

- For Normal Ethernet, operational bandwidth is 10 Mbps.
- For Fast Ethernet, operational bandwidth is 100 Mbps.
- For Gigabit Ethernet, operational bandwidth is 1 Gbps.

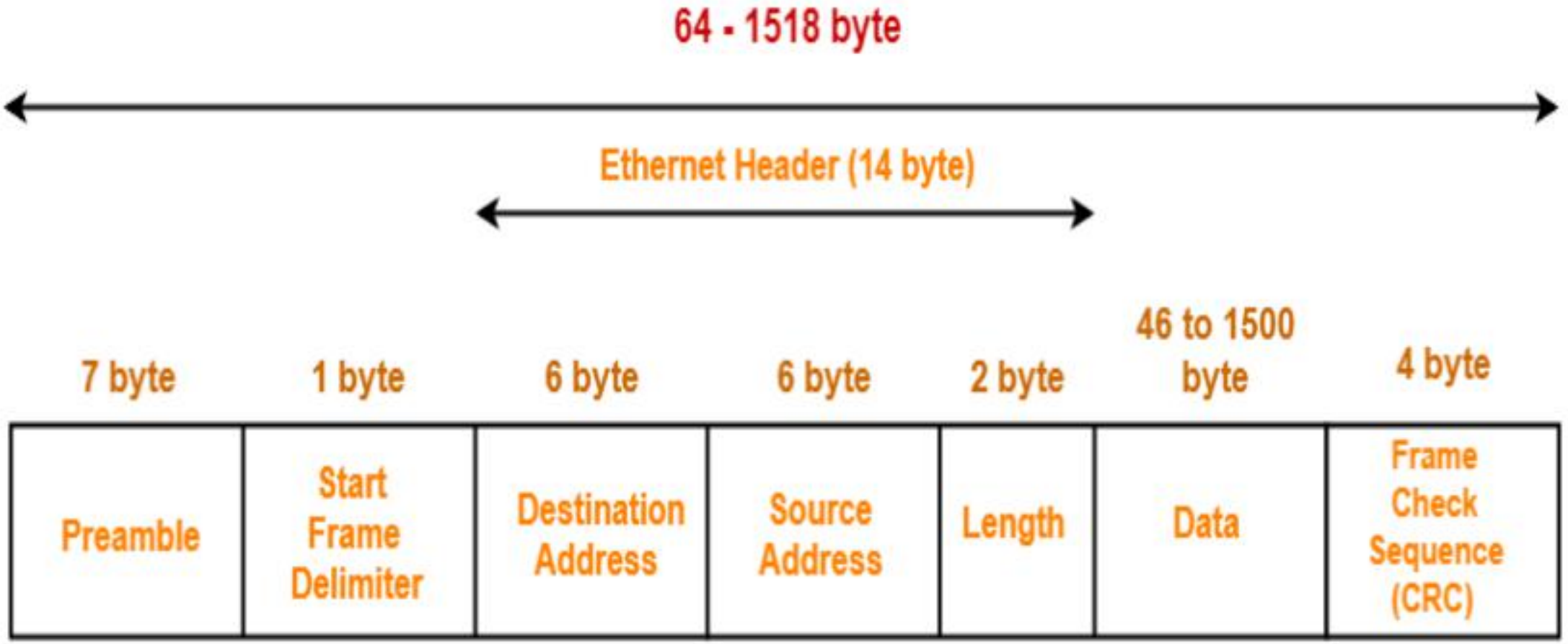
Types of Ethernet Networks

Fast Ethernet: As the term suggests, this is quite a high-speed internet, and can transmit or receive data at about 100 Mbps. This type of network is usually supported by a twisted pair or CAT5 cable. If a laptop, camera, or any other device is connected to a network, they operate at 10/100Base Ethernet and 100Base on the fiber side of the link.

Gigabit Ethernet: This type of network transfers data at an even higher speed of about 1000 Mbps or 1Gbps. Gigabit speed is an upgrade from Fast Ethernet which is slowly being phased out. In this type of network, all the four pairs in the twisted pair cable contribute to the data transfer speed. VERSITRON manufactures Gigabit Ethernet Media Converters that can handle 10/100/1000Base speeds on the Ethernet side and 1000Base Gigabit speed on the fiber side by using Fiber SFP modules.

10-Gigabit Ethernet: This is an even more advanced and high speed network type with a data transfer rate of 10 Gigabit/second. It is supported by CAT6a or CAT7 twisted pair cables, as well as fiber optic cables. By using a fiber optic cable, this network area can be extended up to around 10,000 meters.

Switch Ethernet: This type of network requires a switch or hub. Also, instead of a twisted pair cable, a normal network cable is used in this case. Network switches are used for data transfer from one device to the other, without interrupting any other devices in the network.



IEEE 802.3 Ethernet Frame Format

Preamble-

It is a 7 byte field that contains a pattern of alternating 0's and 1's.
It alerts the stations that a frame is going to start.
It also enables the sender and receiver to establish bit synchronization.

The following three fields collectively represents the Ethernet Header–

- ✓ ***Destination Address (6 bytes)***
- ✓ ***Source Address (6 bytes)***
- ✓ ***Length (2 bytes)***

Thus, Ethernet Header Size = 14 bytes.

Start Frame Delimiter (SFD)-

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.

Destination Address-

It is a 6 byte field that contains the MAC address of the destination for which the data is destined.

Source Address-

It is a 6 byte field that contains the MAC address of the source which is sending the data.

Length-

It is a 2 byte field which specifies the length (number of bytes) of the data field.
This field is required because Ethernet uses variable sized frames.

Data-

It is a variable length field which contains the actual data.
It is also called as a payload field.
The length of this field lies in the range [46 bytes , 1500 bytes].
Thus, in a Ethernet frame, minimum data has to be 46 bytes and maximum data can be 1500 bytes.

Frame Check Sequence (CRC)-

It is a 4 byte field that contains the CRC code for error detection.

- The maximum value that can be accommodated in this field = 65535.
- But it does not mean maximum data that can be sent in one frame is 65535 bytes.
- The maximum amount of data that can be sent in a Ethernet frame is 1500 bytes.
- This is to avoid the monopoly of any single station.

Advantages of Using Ethernet-

- It is not much costly to form an Ethernet network. As compared to other systems of connecting computers, it is relatively inexpensive.
- Ethernet network provides high security for data as it uses firewalls in terms of data security.
- Also, the Gigabit network allows the users to transmit data at a speed of 1-100Gbps.
- In this network, the quality of the data transfer does maintain.
- In this network, administration and maintenance are easier.
- The latest version of gigabit ethernet and wireless ethernet have the potential to transmit data at the speed of 1-100Gbps.

Disadvantages of Using Ethernet-

- The wired Ethernet network is used only for short distances.
- The mobility is limited.
- Its maintenance is difficult.
- Ethernet cables, hubs, switches, routers increase the cost of installation.

Limitations of Using Ethernet-

Point-01:

- It can not be used for real time applications.
- Real time applications require the delivery of data within some time limit.
- Ethernet is not reliable because of high probability of collisions.
- High number of collisions may cause a delay in delivering the data to its destination.

Point-02:

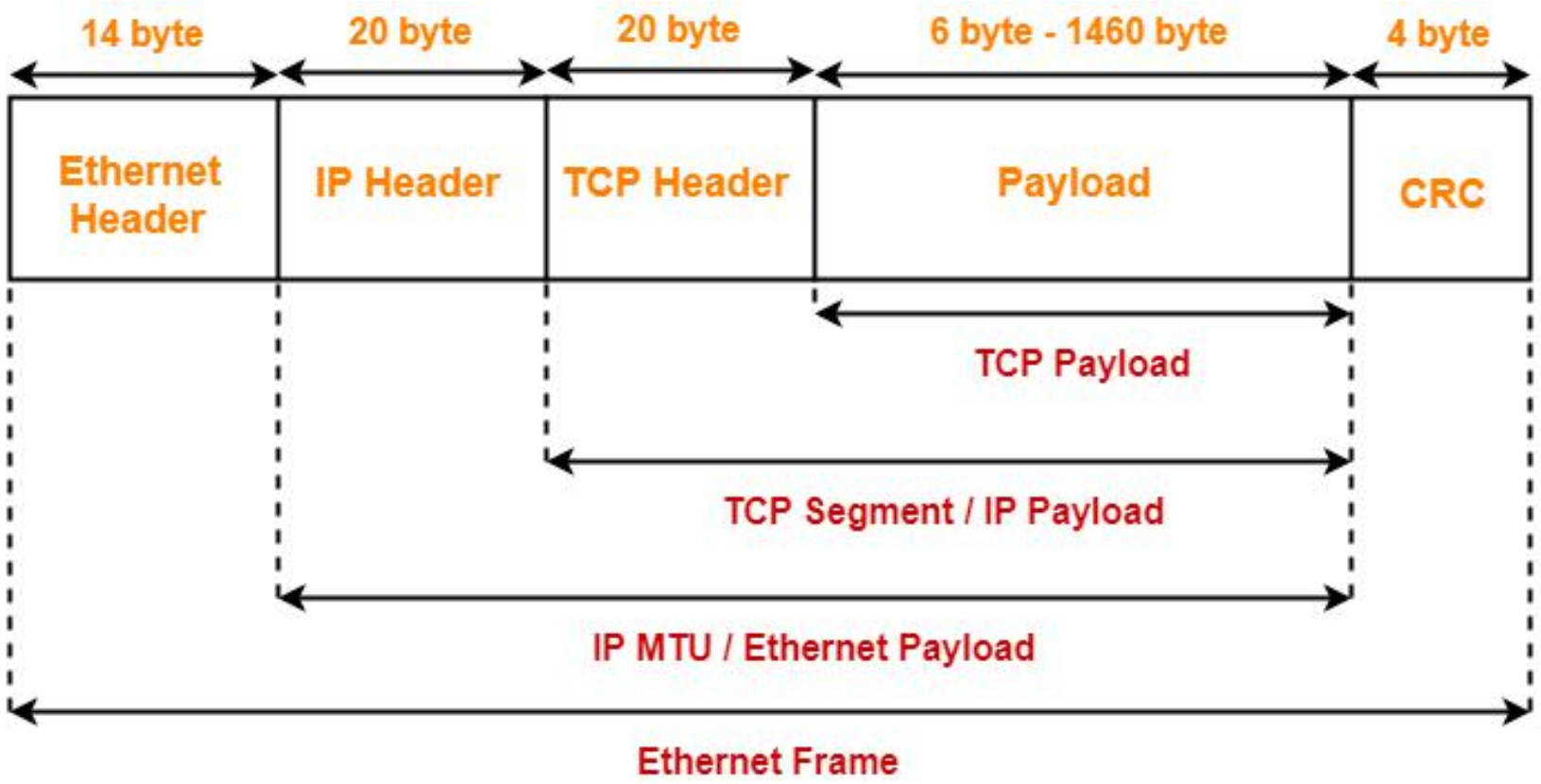
- It can not be used for interactive applications.
- Interactive applications like chatting requires the delivery of even very small amount of data.
- Ethernet requires that minimum length of the data must be 46 bytes.

Point-03:

- It can not be used for client server applications.
- Client server applications require that server must be given higher priority than clients.
- Ethernet has no facility to set priorities.

For data transmission-

- TCP segment sits inside the IP datagram payload field.
- IP datagram sits inside the Ethernet payload field.



Consider a 10 Mbps Ethernet LAN that has stations attached to a 2.5 km long coaxial cable. Given that the transmission speed is 2.3 x 108 m/sec, the packet size is 128 bytes out of which 30 bytes are overhead, find the effective transmission rate and maximum rate at which the network can send data.

Given-

- Bandwidth = 10 Mbps
- Distance = 2.5 km
- Transmission speed = 2.3×10^8 m/sec
- Total packet size = 128 bytes
- Overhead = 30 bytes

Calculating Transmission Delay-

Transmission delay (T_t)
= Packet size / Bandwidth
= 128 bytes / 10 Mbps
= (128 x 8 bits) / (10×10^6 bits per sec)
= 102.4 μsec

Calculating Propagation Delay-

Propagation delay (T_p)
= Distance / Speed
= 2.5 km / (2.3×10^8 m/sec)
= 10.8 μsec

Calculating Value of 'a'-

$a = T_p / T_t$
= 10.8 μsec / 102.4 μsec
= 0.105

Calculating Efficiency-

Efficiency(η)
= 1 / (1 + 6.44 x a)
= 1 / (1 + 6.44 x 0.105)
= 59%

Calculating Maximum Rate-

Maximum rate or Throughput
= Efficiency x Bandwidth
= 0.59 x 10 Mbps
= 5.9 Mbps

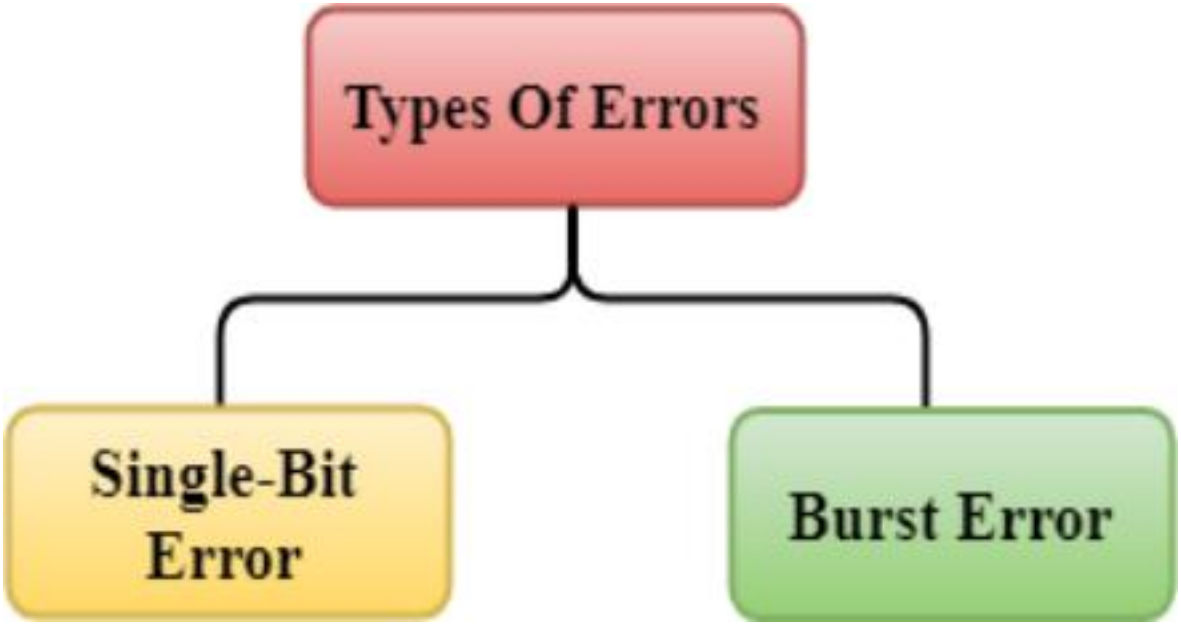
Calculating Effective Transmission Rate-

Effective transmission rate
= Throughput x (128-30 / 128)
= 5.9 Mbps x (98 / 128)
= 4.52 Mbps

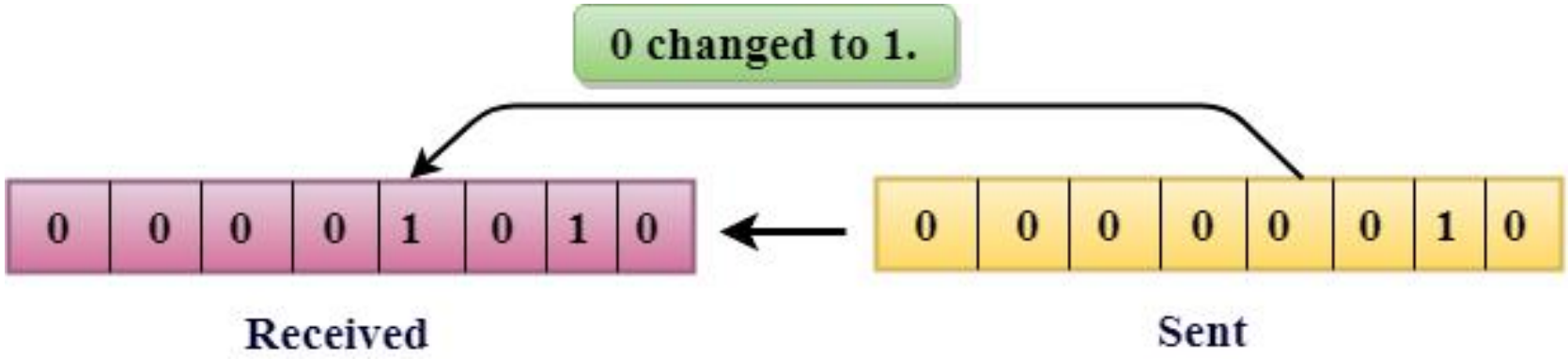
Error Control

Error Detection:

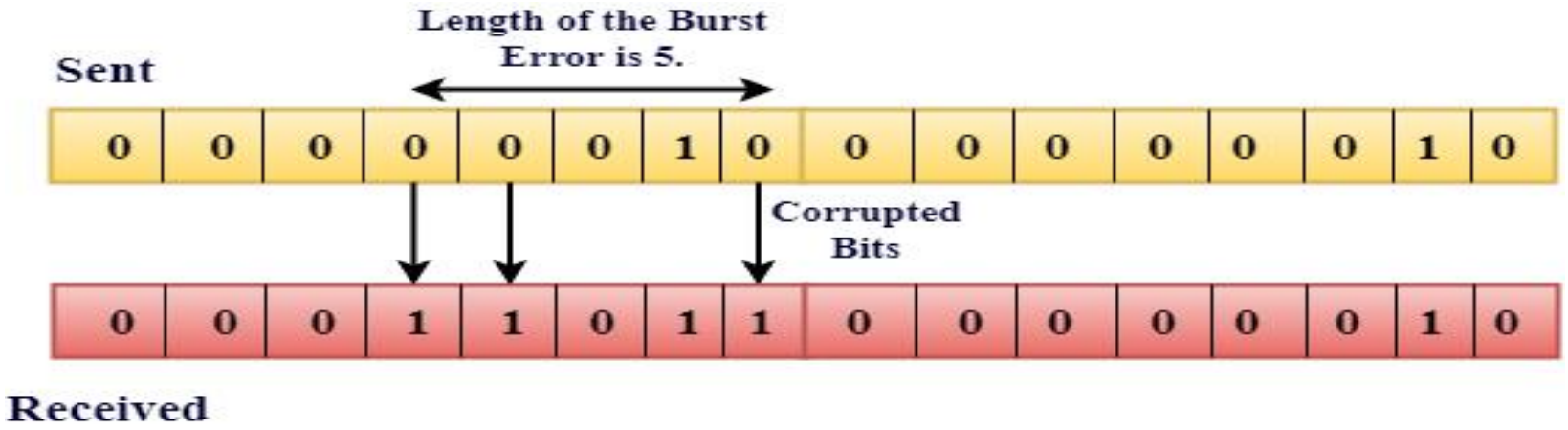
When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

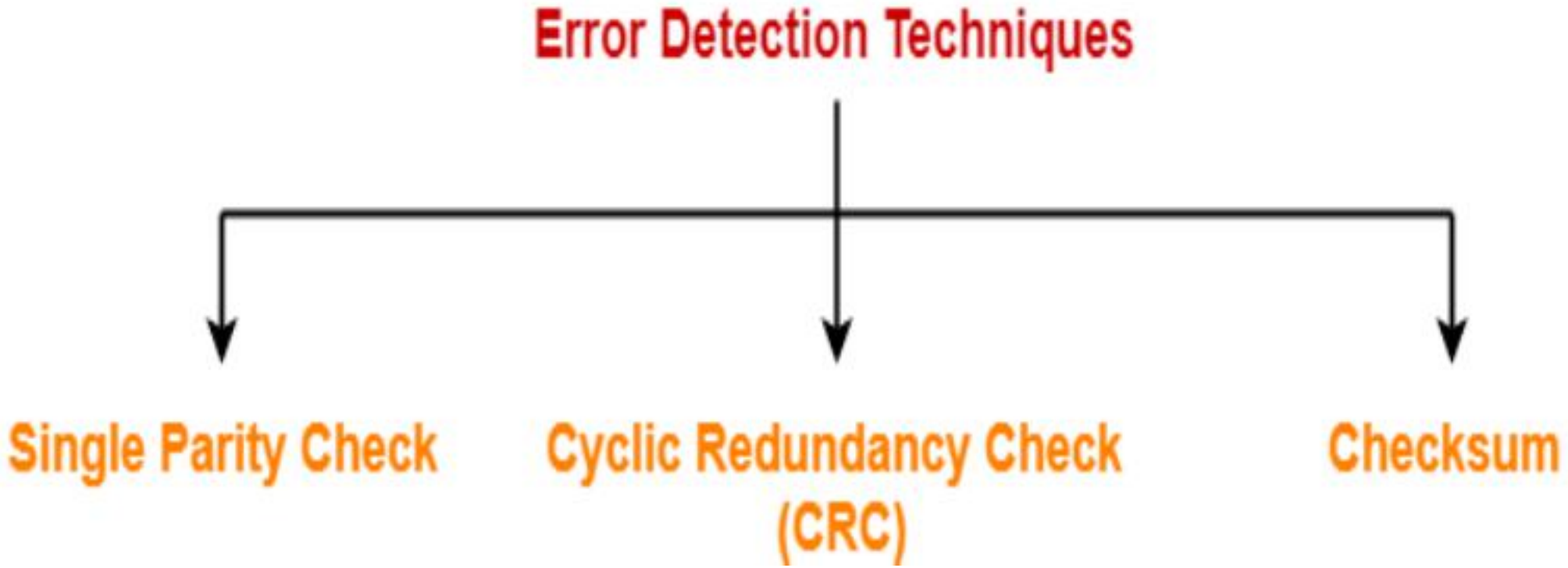


Single-Bit Error: The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



Burst Error: The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.




Error Detection Techniques
Single Parity Check
Cyclic Redundancy 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.

Step-1:

At sender side,

- Total number of 1's in the data unit to be transmitted is counted.
- The total number of 1's in the data unit is made even in case of even parity.
- The total number of 1's in the data unit is made odd in case of odd parity.
- This is done by adding an extra bit called as parity bit.

Step-2:

- The newly formed code word (Original data + parity bit) is transmitted to the receiver.

Step-3:

At receiver side,

- Receiver receives the transmitted code word.
- The total number of 1's in the received code word is counted.

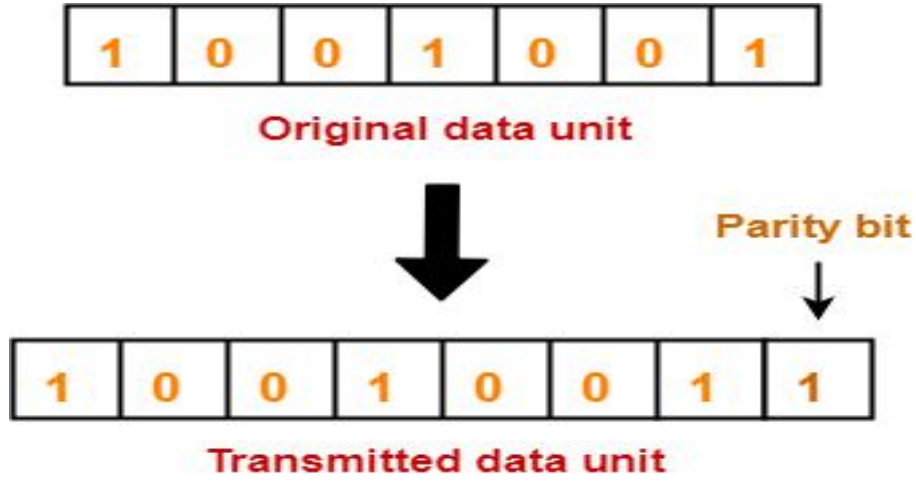
Then, following cases are possible-

- ✓ If total number of 1's is even and even parity is used, then receiver assumes that no error occurred.
- ✓ If total number of 1's is even and odd parity is used, then receiver assumes that error occurred.
- ✓ If total number of 1's is odd and odd parity is used, then receiver assumes that no error occurred.
- ✓ If total number of 1's is odd and even parity is used, then receiver assumes that error occurred.

Consider the data unit to be transmitted is 1001001 and even parity is used.

At Sender Side-

- Total number of 1's in the data unit is counted.
- Total number of 1's in the data unit = 3.
- Clearly, even parity is used and total number of 1's is odd.
- So, parity bit = 1 is added to the data unit to make total number of 1's even.
- Then, the code word 10010011 is transmitted to the receiver.



At Receiver Side-

- After receiving the code word, total number of 1's in the code word is counted.
- Consider receiver receives the correct code word = 10010011.
- Even parity is used and total number of 1's is even.
- So, receiver assumes that no error occurred in the data during the transmission.

Advantage-

- This technique is guaranteed to detect an odd number of bit errors (one, three, five and so on).
- If odd number of bits flip during transmission, then receiver can detect by counting the number of 1's.

Disadvantage-

- 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.

EXAMPLE:

- Consider the data unit to be transmitted is 10010001 and even parity is used.
- Then, code word transmitted to the receiver = 100100011
- Consider during transmission, code word modifies as 101100111. (2 bits flip)
- On receiving the modified code word, receiver finds the number of 1's is even and even parity is used.
- So, receiver assumes that no error occurred in the data during transmission though the data is corrupted.

Cyclic Redundancy Check-

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

CRC Generator:

CRC generator is an algebraic polynomial represented as a bit pattern. Bit pattern is obtained from the CRC generator using the following rule-

"The power of each term gives the position of the bit and the coefficient gives the value of the bit."

Consider the CRC generator is $x^7 + x^6 + x^4 + x^3 + x + 1$.

$$1x^7 + 1x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0$$

1	1	0	1	1	0	1	1

Thus, for the given CRC generator, the corresponding binary pattern is 11011011.

Properties Of CRC Generator-

Rule-01:

It should not be divisible by x.
This condition guarantees that all the burst errors of length equal to the length of polynomial are detected.

Rule-02:

It should be divisible by x+1.
This condition guarantees that all the burst errors affecting an odd number of bits are detected.

If the CRC generator is chosen according to the above rules, then-

- **CRC can detect all single-bit errors**
- **CRC can detect all double-bit errors provided the divisor contains at least three logic 1's.**
- **CRC can detect any odd number of errors provided the divisor is a factor of x+1.**
- **CRC can detect all burst error of length less than the degree of the polynomial.**
- **CRC can detect most of the larger burst errors with a high probability.**

Step-1: Calculation Of CRC At Sender Side-

At sender side,

- A string of n 0's is appended to the data unit to be transmitted.
- Here, n is one less than the number of bits in CRC generator.
- Binary division is performed of the resultant string with the CRC generator.
- After division, the remainder so obtained is called as CRC.
- It may be noted that CRC also consists of n bits.

Step-2: Appending CRC To Data Unit-

At sender side,

- The CRC is obtained after the binary division.
- The string of n 0's appended to the data unit earlier is replaced by the CRC remainder.

Step-3: Transmission To Receiver-

- The newly formed code word (Original data + CRC) is transmitted to the receiver.

Step-4: Checking at Receiver Side-

At receiver side,

- The transmitted code word is received.
- The received code word is divided with the same CRC generator.
- On division, the remainder so obtained is checked.

Case-01: Remainder = 0

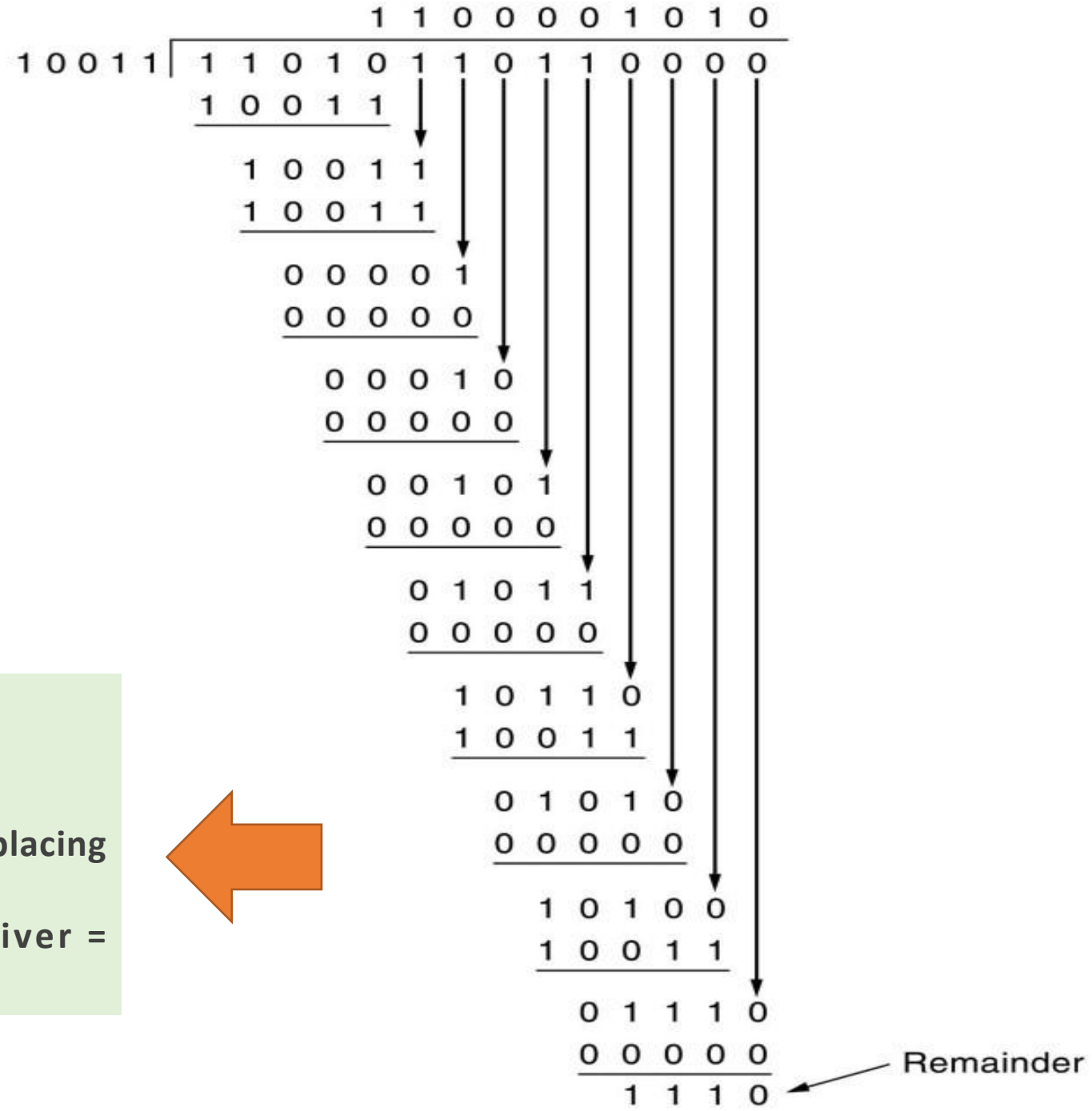
If the remainder is zero, receiver assumes that no error occurred in the data during the transmission. Receiver accepts the data.

Case-02: Remainder ≠ 0

If the remainder is non-zero, receiver assumes that some error occurred in the data during the transmission. Receiver rejects the data and asks the sender for retransmission.

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

- The generator polynomial G(x) = $x^4 + x + 1$ is encoded as 10011.
- Clearly, the generator polynomial consists of 5 bits.
- So, a string of 4 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 11010110110000.



From here, CRC = 1110.

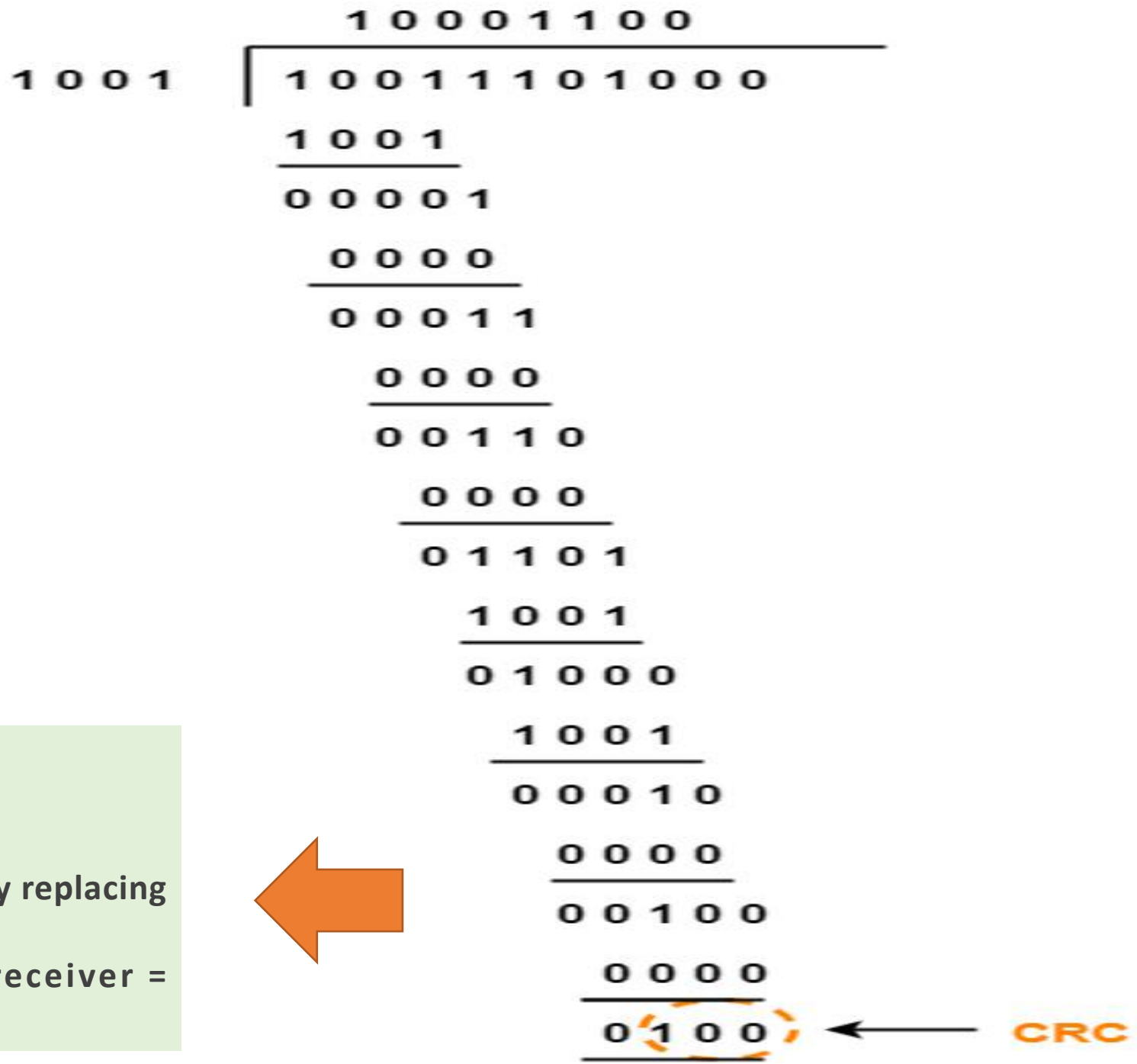
Now,
The code word to be transmitted is obtained by replacing the last 4 zeroes of 11010110110000 with the CRC.
Thus, the code word transmitted to the receiver = 11010110111110.

A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is x^3+1.

a. What is the actual bit string transmitted?

b. Suppose the third bit from the left is inverted during transmission. How will receiver detect this error?

- The generator polynomial $G(x) = x^3 + 1$ is encoded as 1001.
- Clearly, the generator polynomial consists of 4 bits.
- So, a string of 3 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 10011101000.

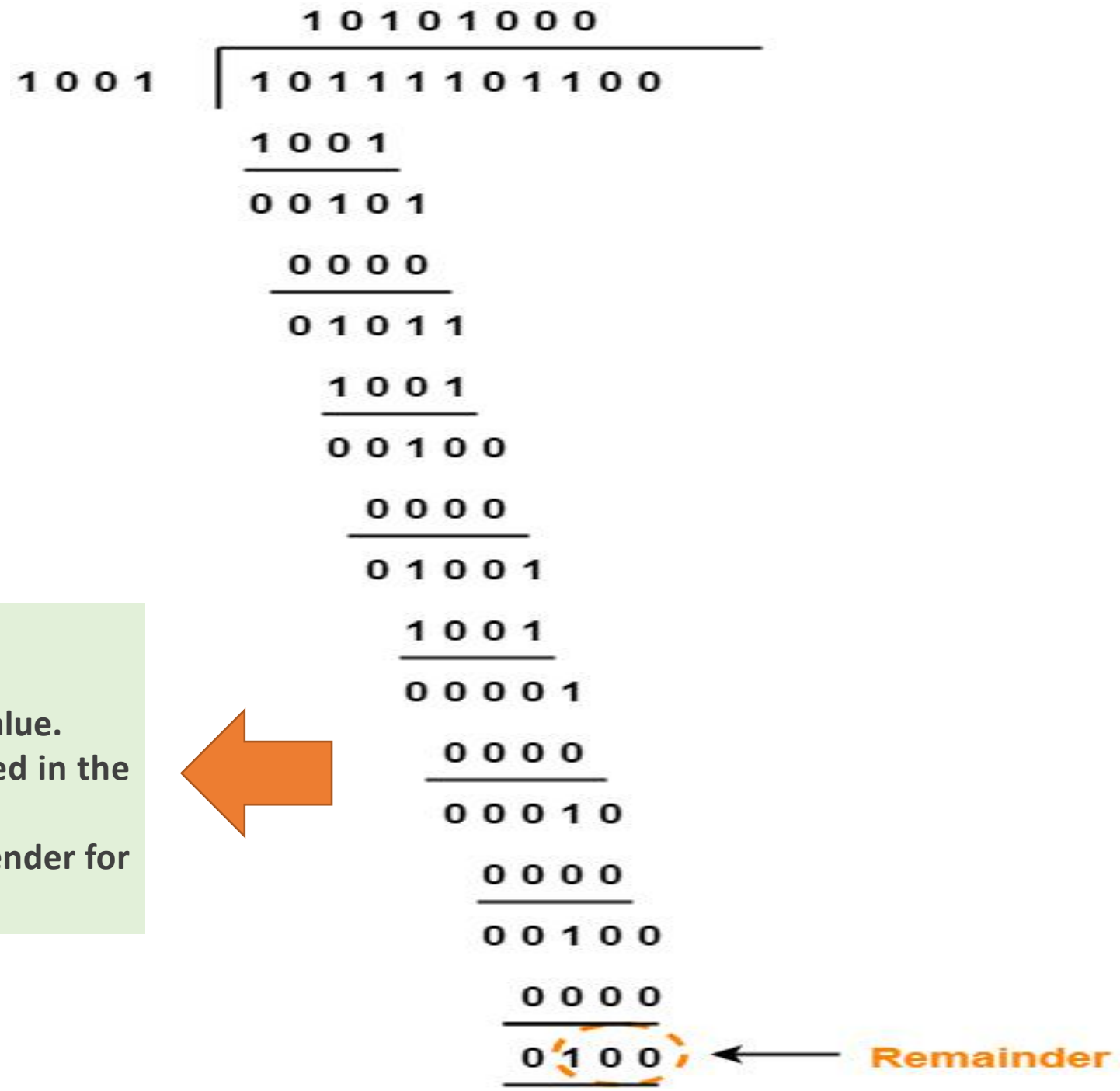


From here, CRC = 100.

Now,
The code word to be transmitted is obtained by replacing the last 3 zeroes of 10011101000 with the CRC.
Thus, the code word transmitted to the receiver = 10011101100.

According to the question,
Third bit from the left gets inverted during transmission. So, the bit stream received by the receiver = 10111101100.

Now,
Receiver receives the bit stream = 10111101100. Receiver performs the binary division with the same generator polynomial as-



From here,

The remainder obtained on division is a non-zero value.
This indicates to the receiver that an error occurred in the data during the transmission.
Therefore, receiver rejects the data and asks the sender for retransmission.

Checksum-

Step-1:

At sender side,

- If m bit checksum is used, the data unit to be transmitted is divided into segments of m bits.
- All the m bit segments are added.
- The result of the sum is then complemented using 1's complement arithmetic.
- The value so obtained is called as checksum.

Step-2:

- The data along with the checksum value is transmitted to the receiver.

Step-03:

At receiver side,

- If m bit checksum is being used, the received data unit is divided into segments of m bits.
- All the m bit segments are added along with the checksum value.
- The value so obtained is complemented and the result is checked.

Case-01: Result = 0

If the result is zero,
Receiver assumes that no error occurred in the data during the transmission. Receiver accepts the data.

Case-02: Result ≠ 0

If the result is non-zero,
Receiver assumes that error occurred in the data during the transmission.
Receiver discards the data and asks the sender for retransmission.

Consider the data unit to be transmitted is- 1001100111100010001001001000010 0. Consider 8 bit checksum is used.

Step-01:

At sender side,

The given data unit is divided into segments of 8 bits as-

10011001	11100010	00100100	10000100

Now, all the segments are added and the result is obtained as-

- 10011001 + 11100010 + 00100100 + 10000100 = 1000100011
- Since the result consists of 10 bits, so extra 2 bits are wrapped around.
- 00100011 + 10 = 00100101 (8 bits)
- Now, 1's complement is taken which is 11011010.
- Thus, checksum value = 11011010

Step-02:

- The data along with the checksum value is transmitted to the receiver.

Step-03:

At receiver side,

- The received data unit is divided into segments of 8 bits.
- All the segments along with the checksum value are added.
- Sum of all segments + Checksum value = 00100101 + 11011010 = 11111111
- Complemented value = 00000000
- Since the result is 0, receiver assumes no error occurred in the data and therefore accepts it.

END