DATALINK LAYER

Data Link Layer

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.

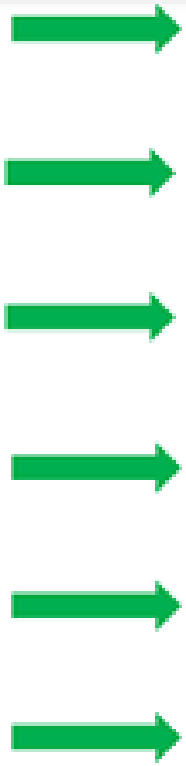
- The communication channel that **connects the adjacent nodes is known as links**, and in order to move the datagram from **source to the destination**, the datagram must be moved across an individual link.

- The main responsibility of the **Data Link Layer is to transfer the datagram across an individual link.**

- The Data link layer protocol defines the format of the packet exchanged **across the nodes** as well as the actions such as **Error detection, retransmission, flow control, and random access.**

- The Data Link Layer protocols are **Ethernet, token ring, FDDI and PPP**.

Services of Data link Layer

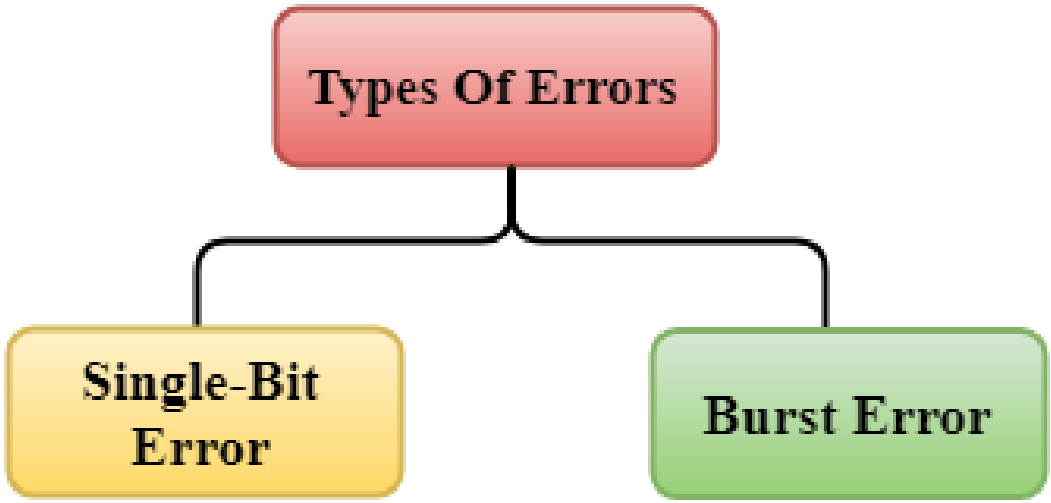


- Framing & Link access
- Reliable Delivery
- Flow Control
- Error Detection
- Error Correction
- Half-Duplex & full-Duplex

Error Detection

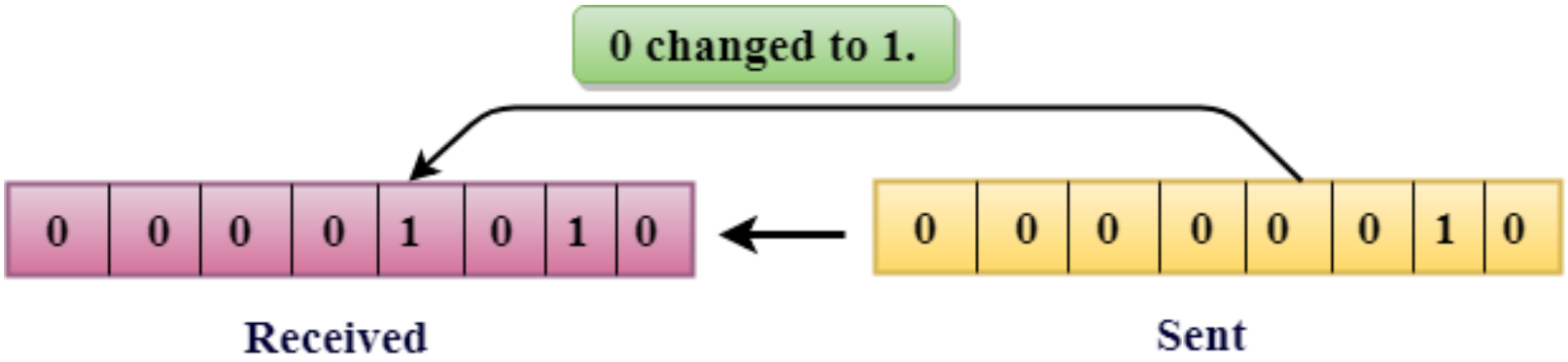
When data is transmitted from one device to another device, **the system does not guarantee whether the data received by the device is identical to the data transmitted by another device.**

An Error is a situation when the message received at the receiver end is not identical to the message transmitted.



➢**Single-Bit Error** does not appear more likely in Serial Data Transmission

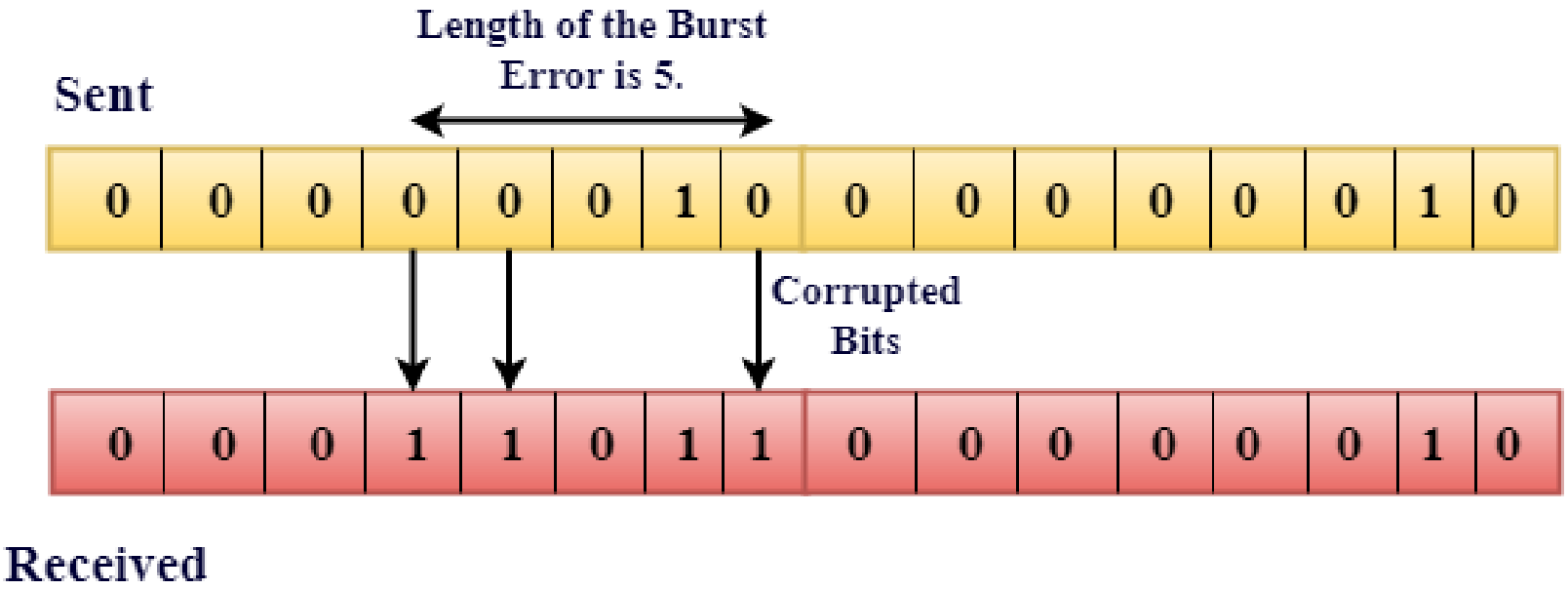
➢**Single-Bit Error** mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.



Burst Error:

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

➢The **Burst Error** is determined from the first corrupted bit to the last corrupted bit.



Error Detecting Techniques:

- The most popular Error Detecting Techniques are:
- **Single parity check**
- **Two-dimensional parity check**
- **Checksum**
- **Cyclic redundancy check**

Single Parity Check

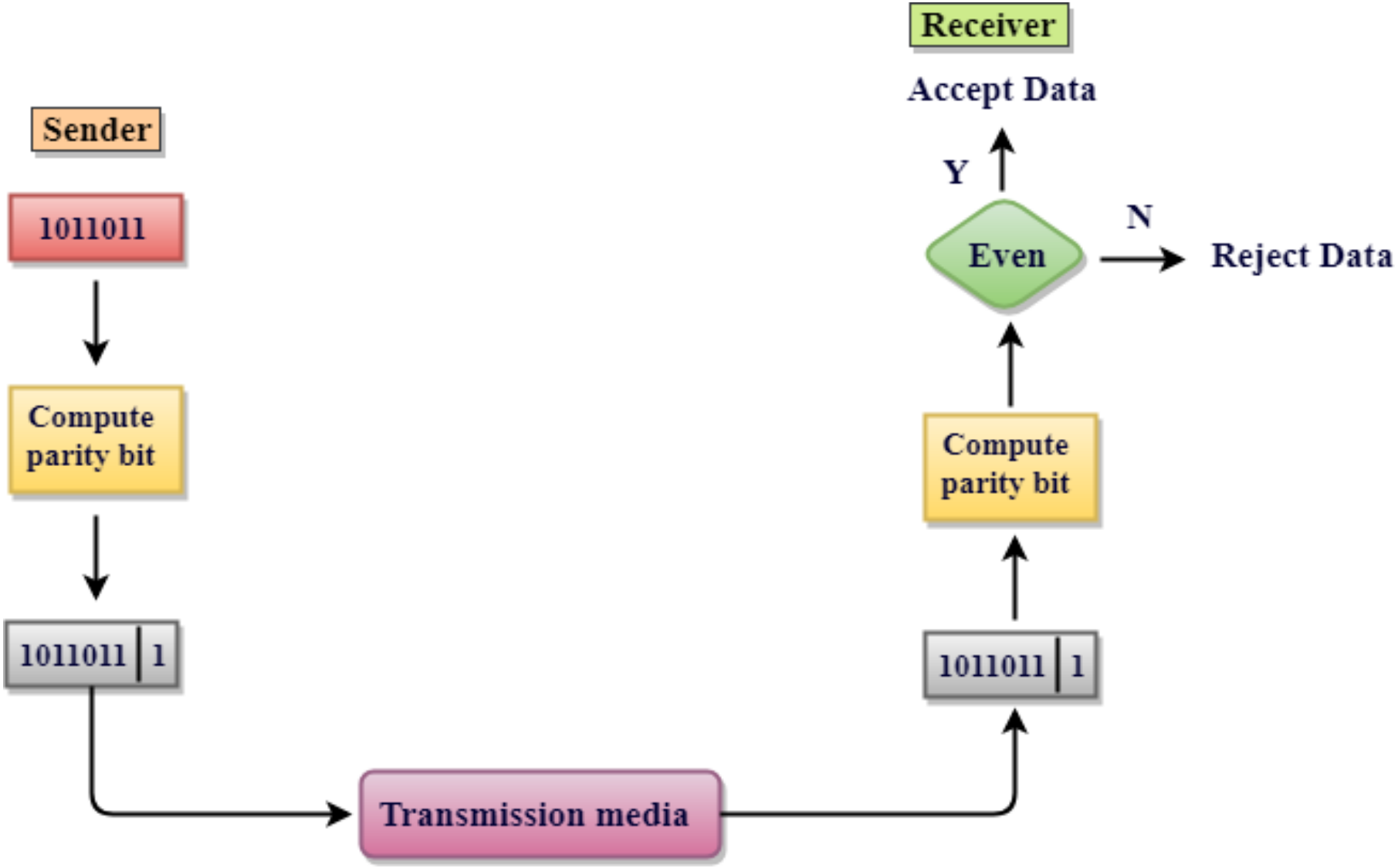
- Single Parity checking is the simple mechanism and inexpensive to detect the errors.

- In this technique, **a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even**. Therefore, the total number of transmitted bits would be 9 bits.

- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.

- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.

- This technique generates the total number of 1s even, so it is known as even-parity checking.


Receiver
Accept Data
Sender
Y
1011011
N
Even
Reject Data
Compute parity bit
Compute parity bit
1011011 | 1
1011011 | 1
Transmission media

Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.

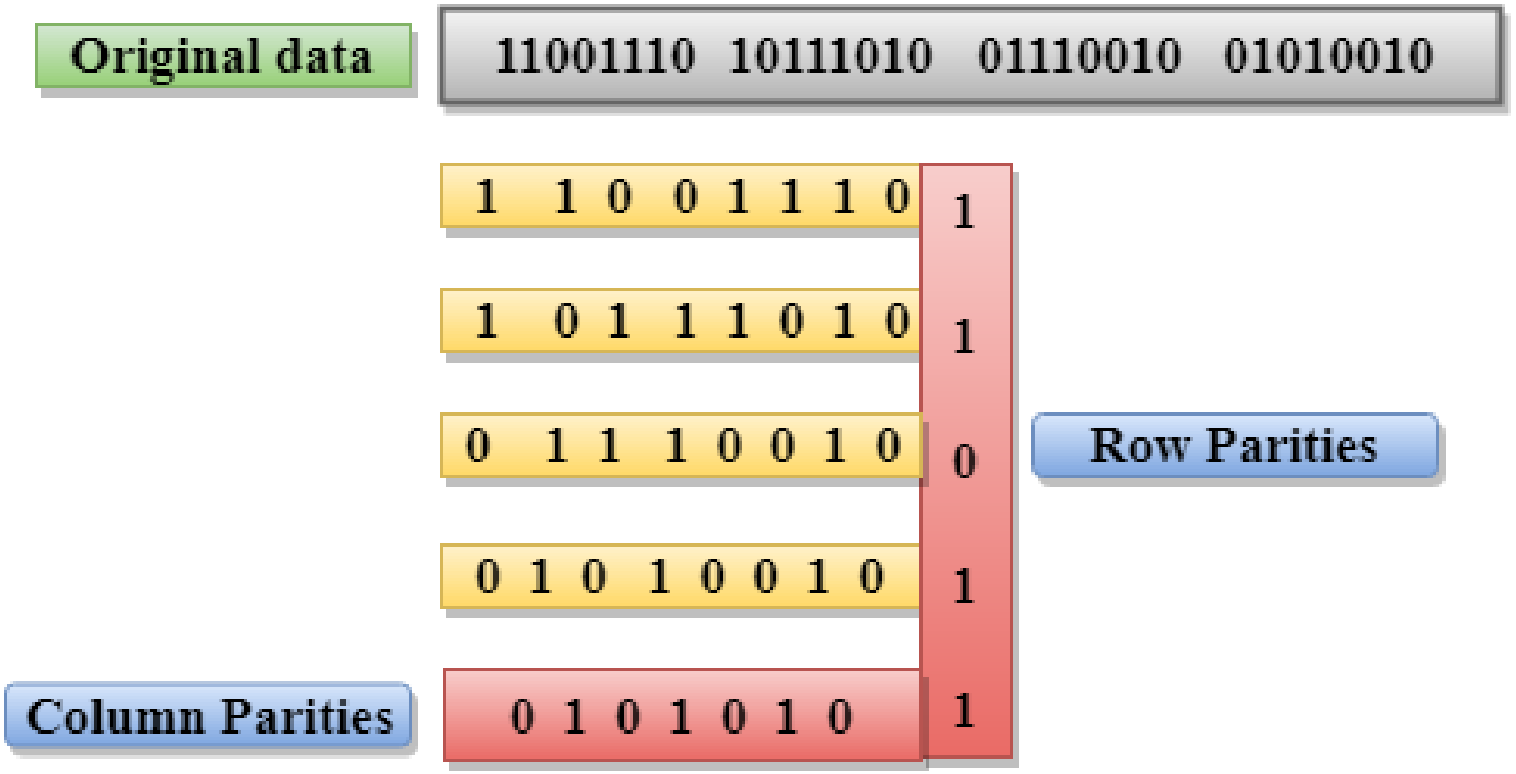
Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.

- Parity check bits are computed for each row, which is equivalent to the single-parity check.

- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.

- At the receiving end, the parity bits are compared with the parity bits computed from the received data.


Original data
11001110 10111010 01110010 01010010
1 1 0 0 1 1 1 0
1 0 1 1 1 0 1 0
0 1 1 1 0 0 1 0
0 1 0 1 0 0 1 0
0 1 0 1 0 1 0
1
1
0
1
1
Row Parities
Column Parities

Original Data

10011001	11100010	00100100	10000100

Row parities

10011001	0
11100010	0
00100100	0
10000100	0
11011011	0

Column parities

100110010	111000100	001001000	100001000	110110110

Data to be sent

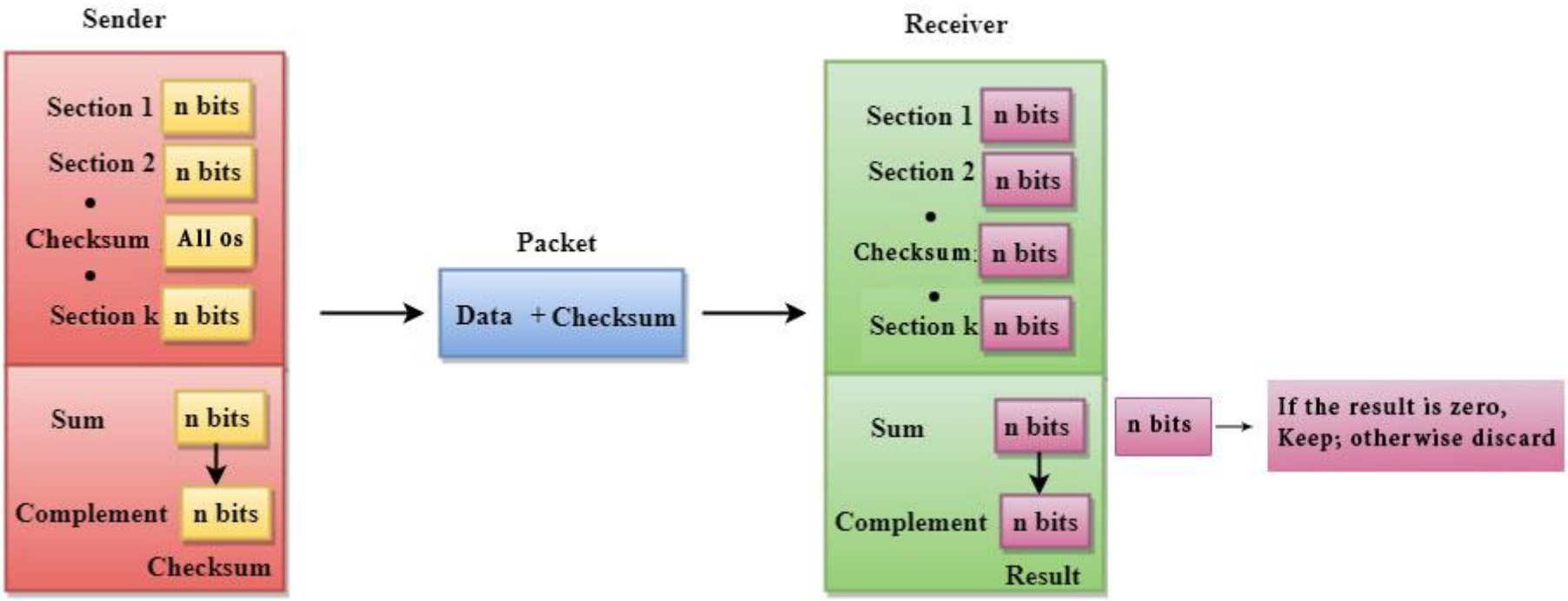
Checksum

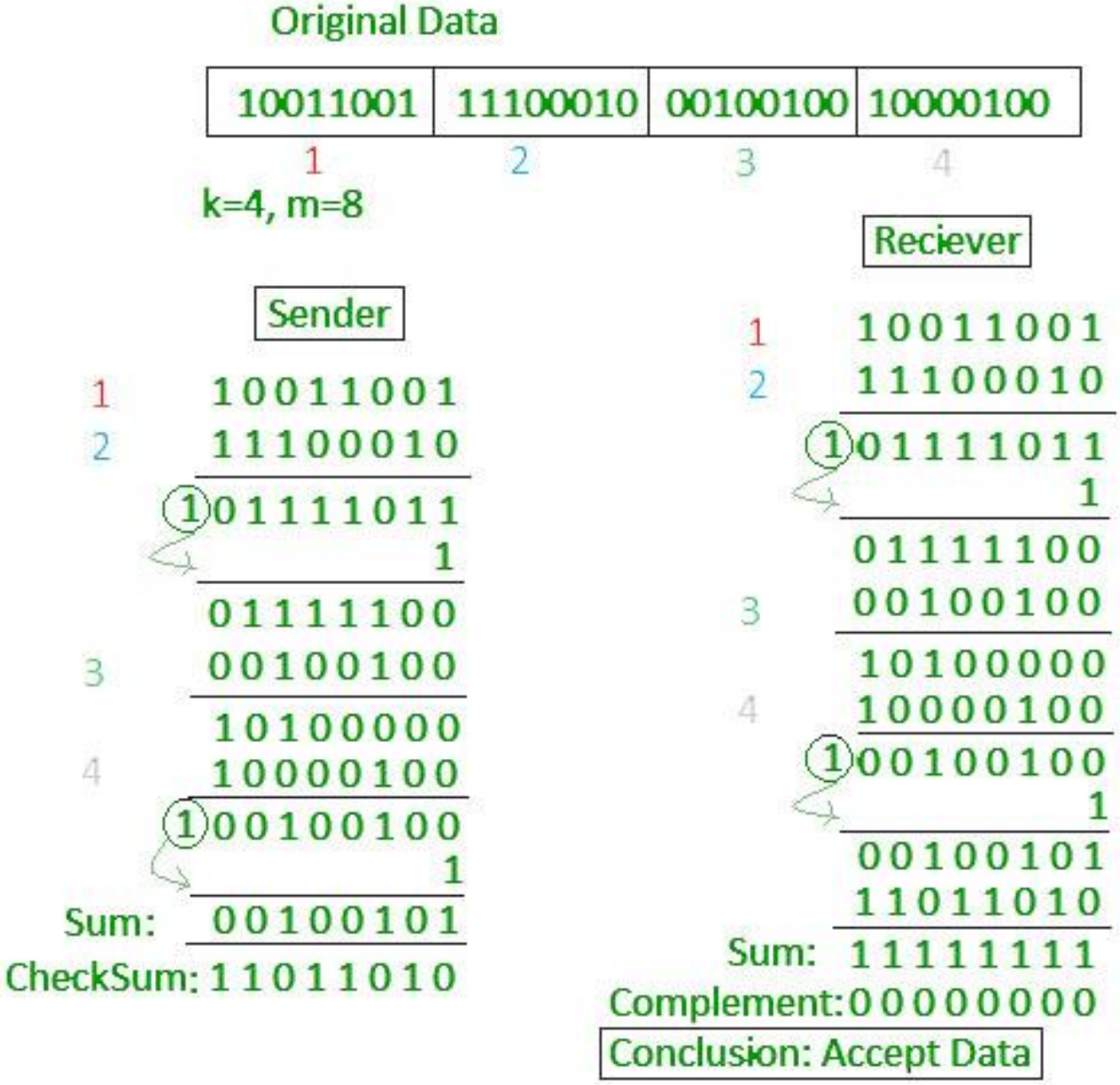
- A Checksum is an error detection technique based on the concept of redundancy.

- **It is divided into two parts:**

- Checksum Generator

- A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.


Sender
Section 1
n bits
Section 2
n bits
Checksum
All 0s
Section k
n bits
Sum
n bits
Complement
n bits
Checksum
Packet
Data + Checksum
Receiver
Section 1
n bits
Section 2
n bits
Checksum
n bits
Section k
n bits
Sum
n bits
Complement
n bits
Result
n bits
If the result is zero,
Keep; otherwise discard


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)

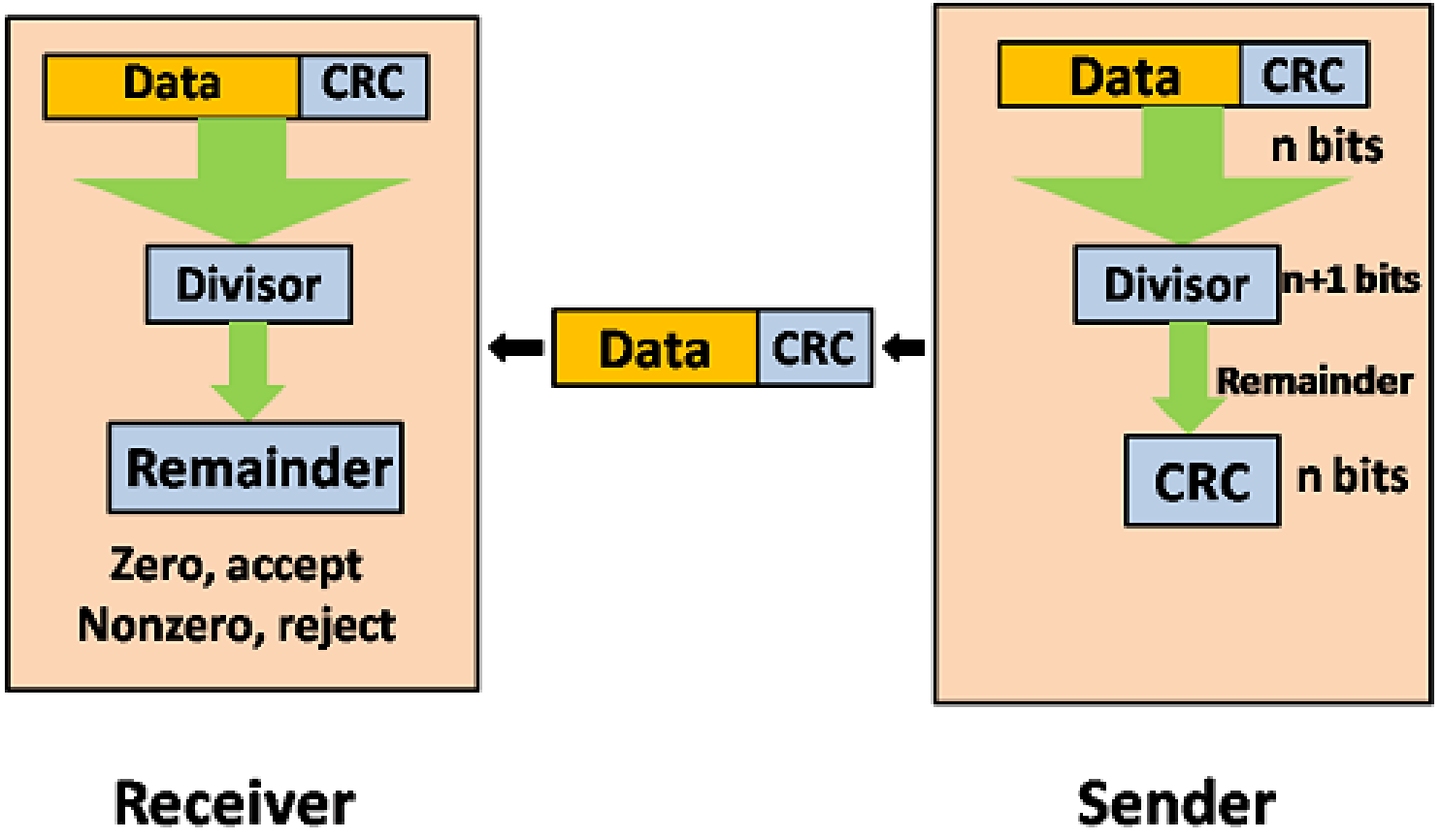
- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.

- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.

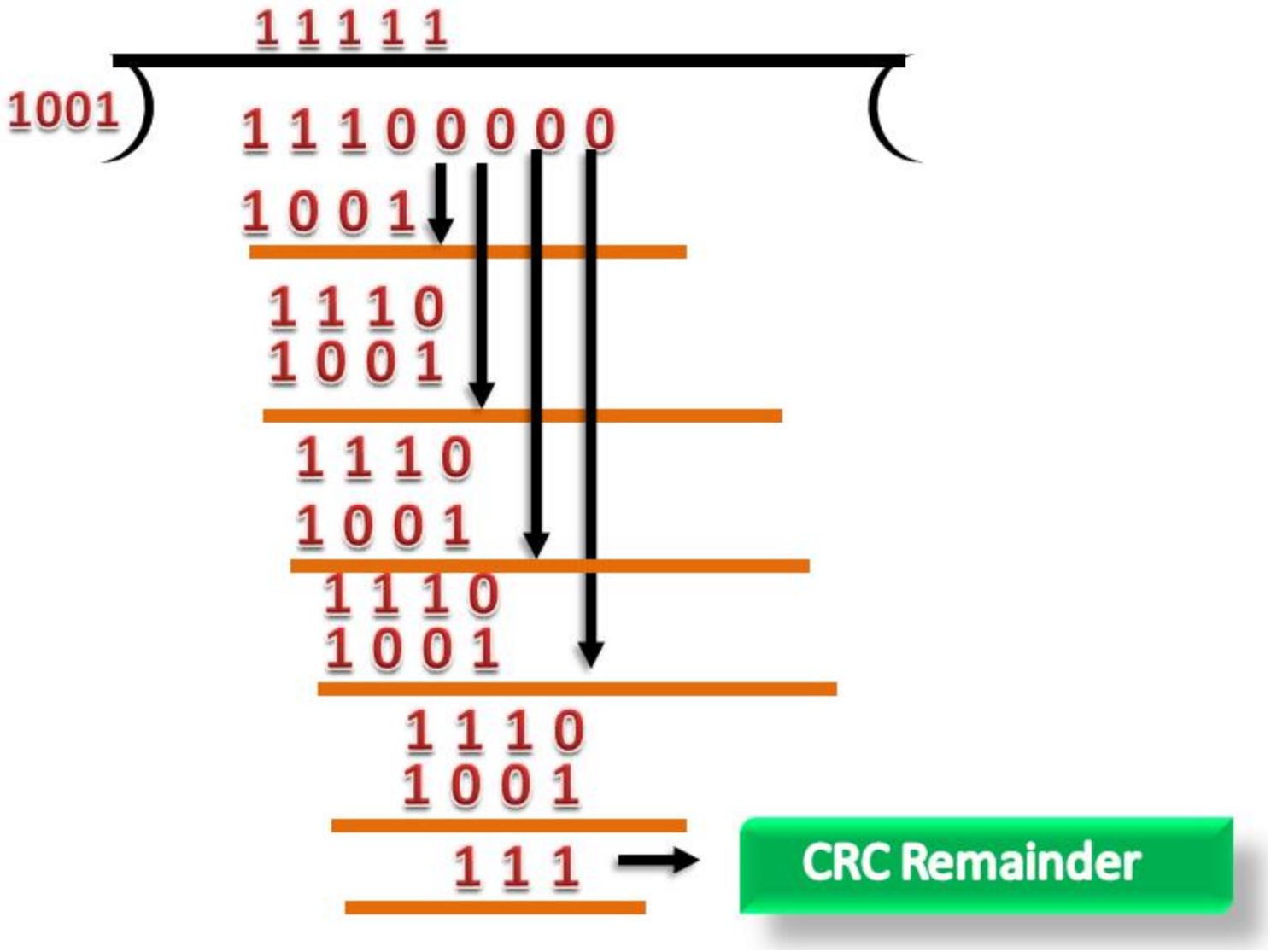
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.

- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

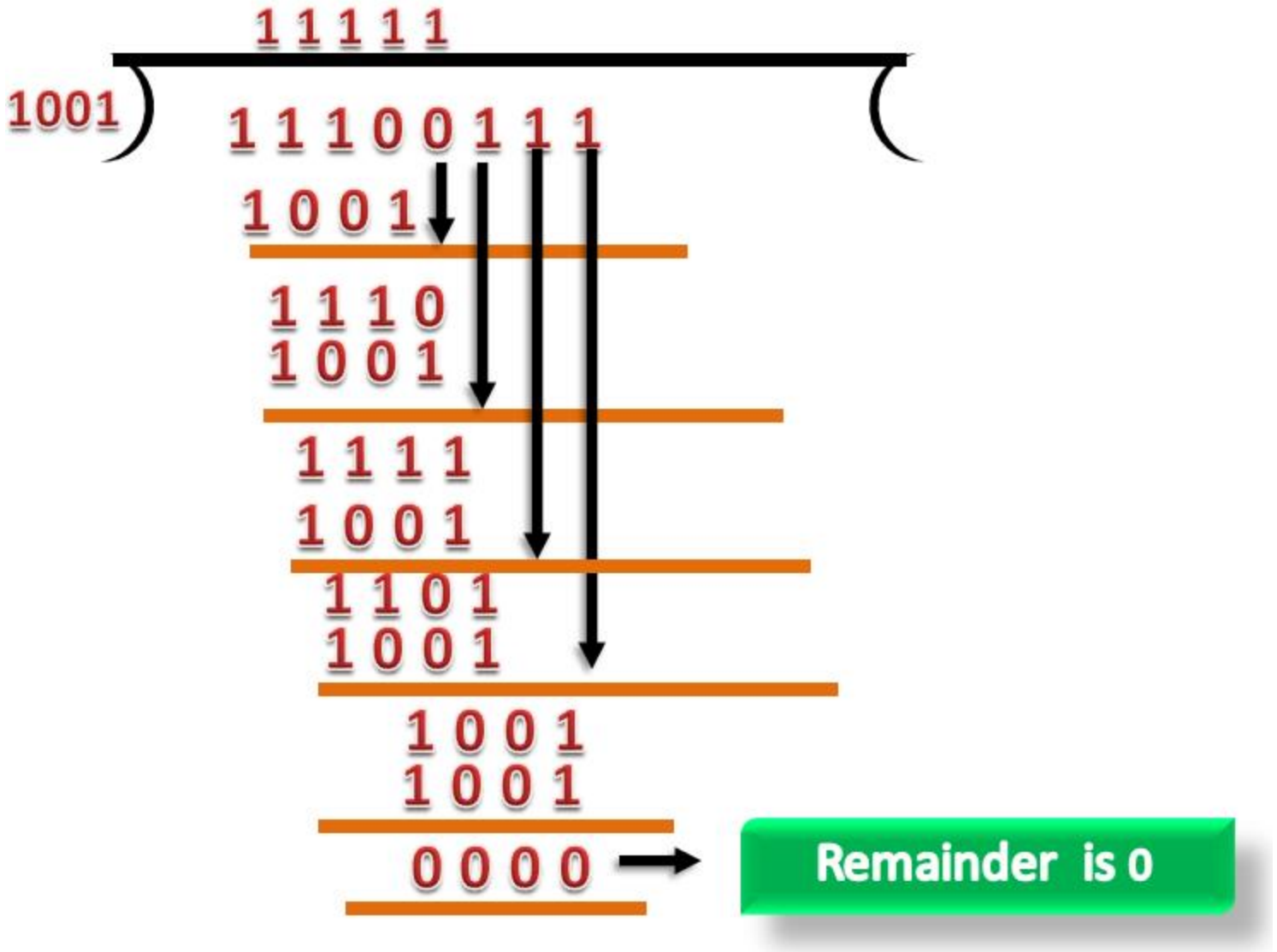
- If the resultant of this division is zero which means that it has no error, and the data is accepted.
- If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

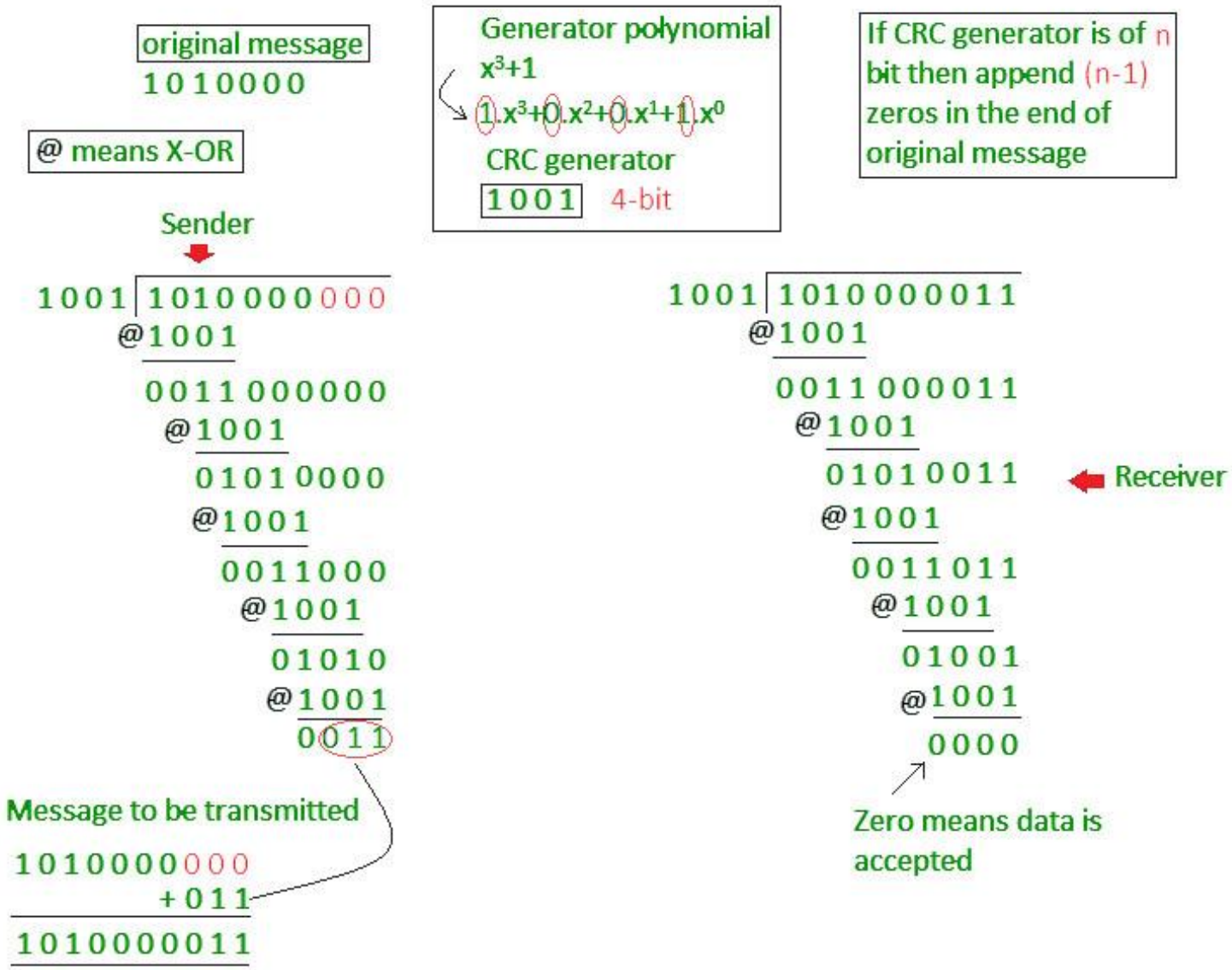

Data
CRC
Divisor
Remainder
Zero, accept
Nonzero, reject
Data
CRC
Data
CRC
n bits
Divisor
n+1 bits
Remainder
CRC
n bits
Receiver
Sender

CRC Generator



CRC Checker


1 1 1 1 1
1001
1 1 1 0 0 1 1 1
1 0 0 1
1 1 1 0
1 0 0 1
1 1 1 1
1 0 0 1
1 1 0 1
1 0 0 1
1 0 0 1
1 0 0 1
0 0 0 0
Remainder is 0


original message
1 0 1 0 0 0 0
@ means X-OR
Generator polynomial
x^3+1
$1.x^3+0.x^2+0.x^1+1.x^0$
CRC generator
1 0 0 1 4-bit
If CRC generator is of n bit then append (n-1) zeros in the end of original message
Sender
1 0 0 1 | 1 0 1 0 0 0 0 0 0 0
@1 0 0 1
0 0 1 1 0 0 0 0 0 0
@1 0 0 1
0 1 0 1 0 0 0 0
@1 0 0 1
0 0 1 1 0 0 0
@1 0 0 1
0 1 0 1 0
@1 0 0 1
0 0 1 1
Message to be transmitted
1 0 1 0 0 0 0 0 0 0
+ 0 1 1
1 0 1 0 0 0 0 0 1 1
1 0 0 1 | 1 0 1 0 0 0 0 0 1 1
@1 0 0 1
0 0 1 1 0 0 0 0 1 1
@1 0 0 1
0 1 0 1 0 0 1 1
@1 0 0 1
0 0 1 1 0 1 1
@1 0 0 1
0 1 0 0 1
@1 0 0 1
0 0 0 0
Receiver
Zero means data is accepted

Data Link Controls

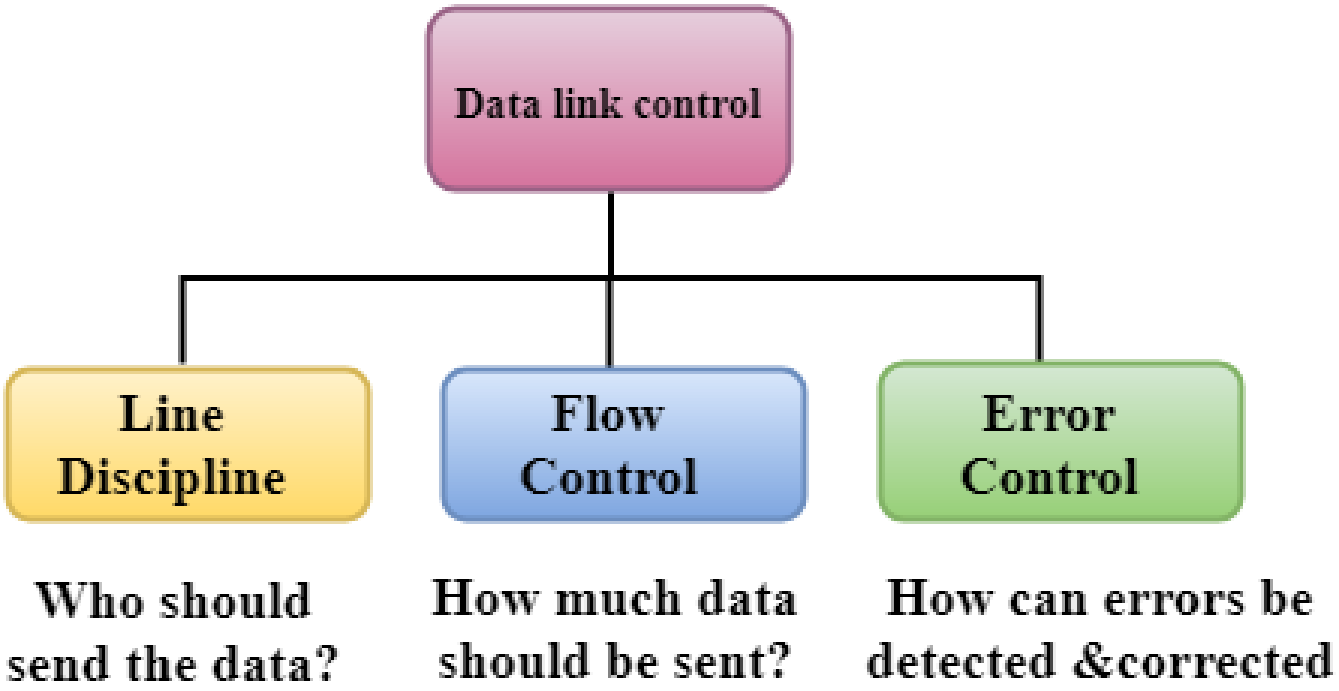
- Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium.

- For example, In the half-duplex transmission mode, one device can only transmit the data at a time.

- If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

1. Line discipline
2. Flow Control
3. Error Control


Data link control
Line Discipline
Flow Control
Error Control
Who should send the data?
How much data should be sent?
How can errors be detected &corrected

Working of ENQ/ACK

- The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

- The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.

- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.

- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

1. **Stop-and-wait**

2. **Sliding window**

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.

- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

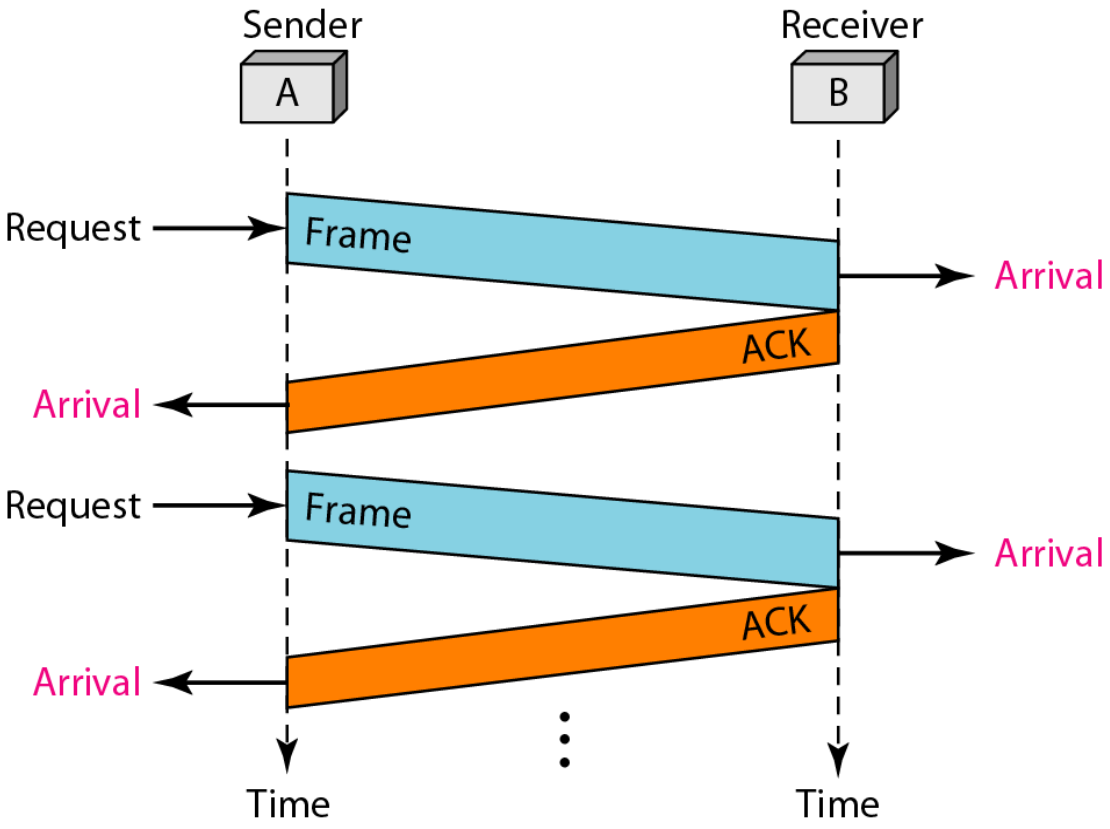
Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

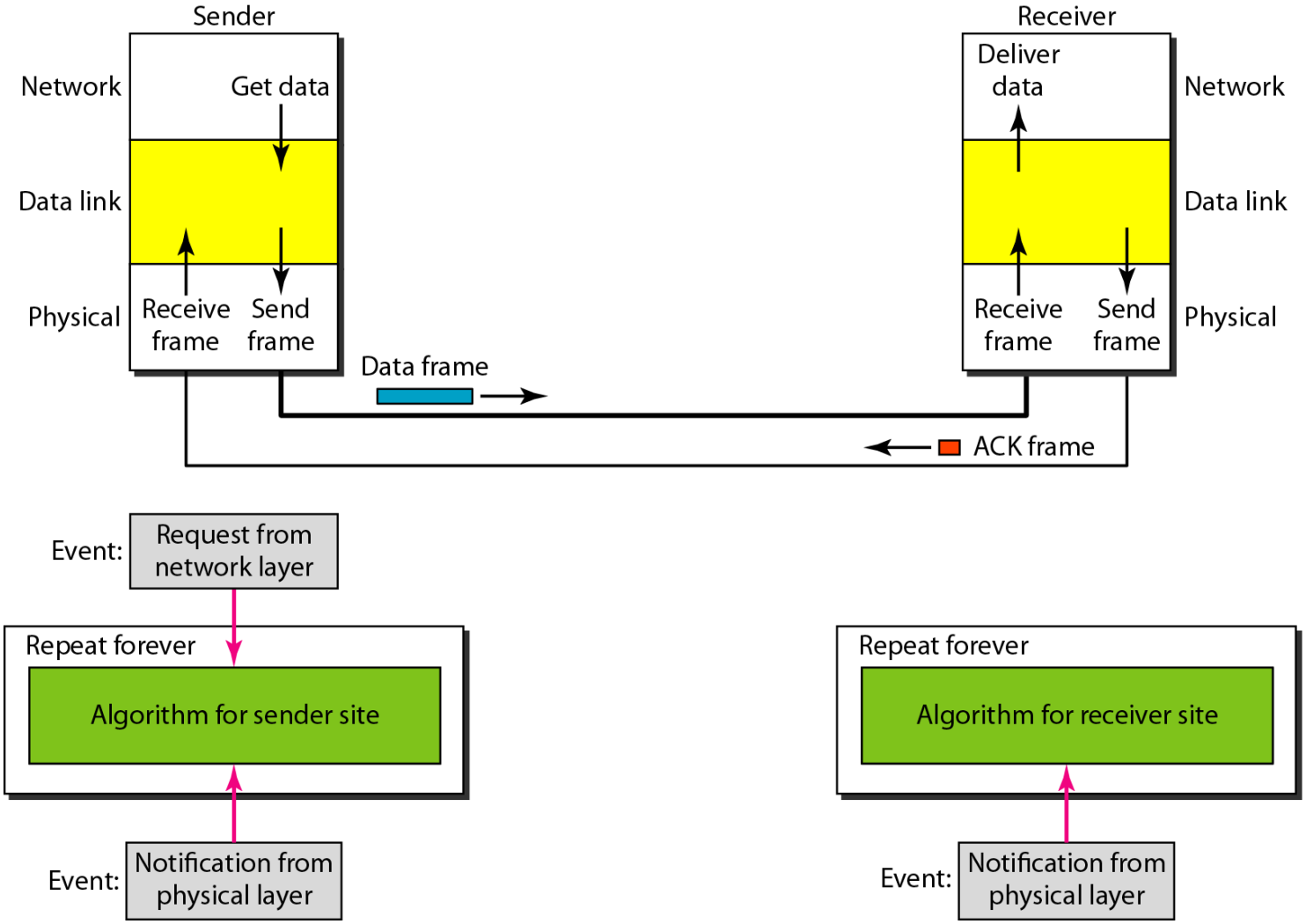
Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

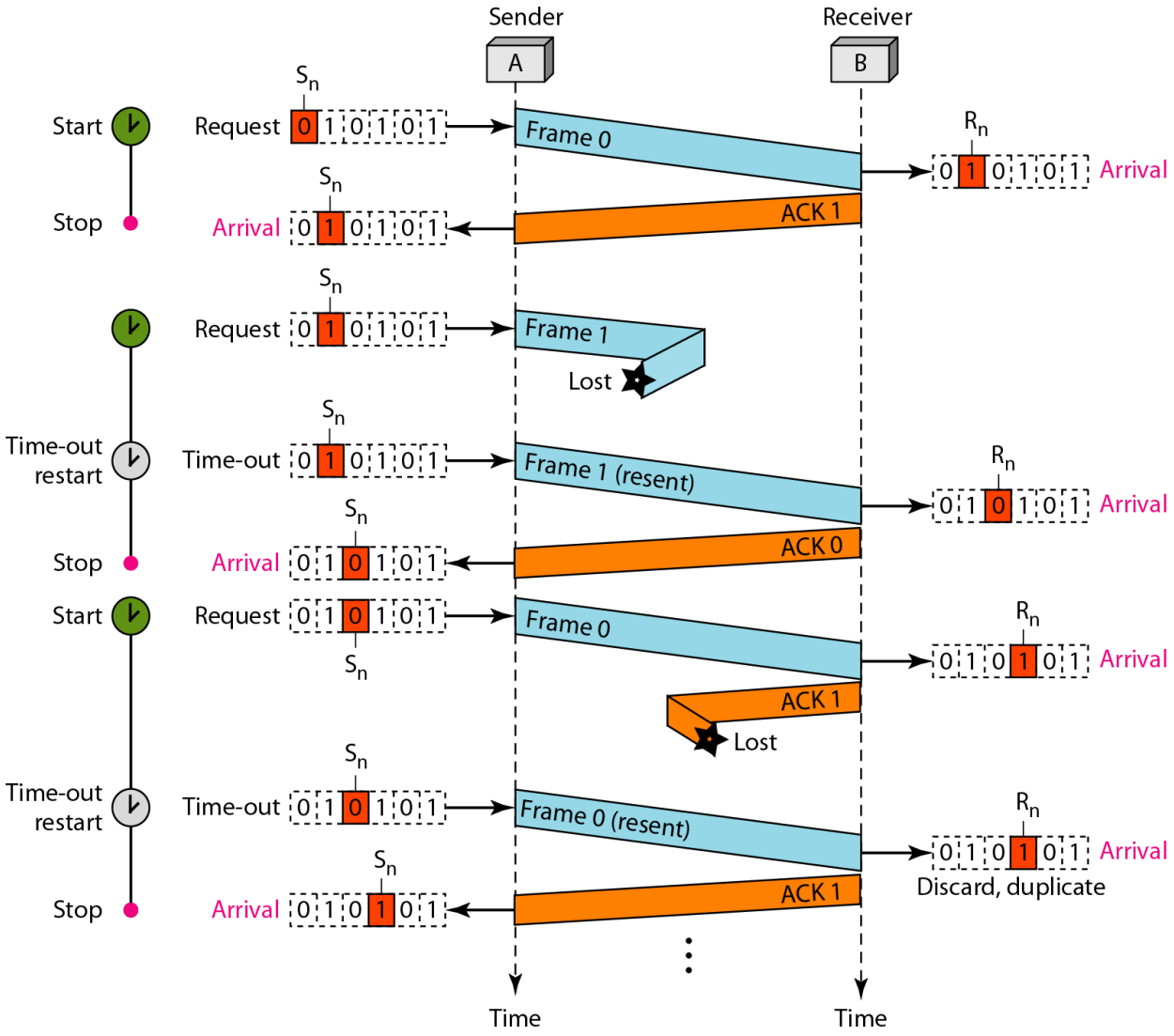
Figure 11.9 *Flow diagram for Example 11.2*



Design of Stop-and-Wait Protocol



Flow diagram for Example



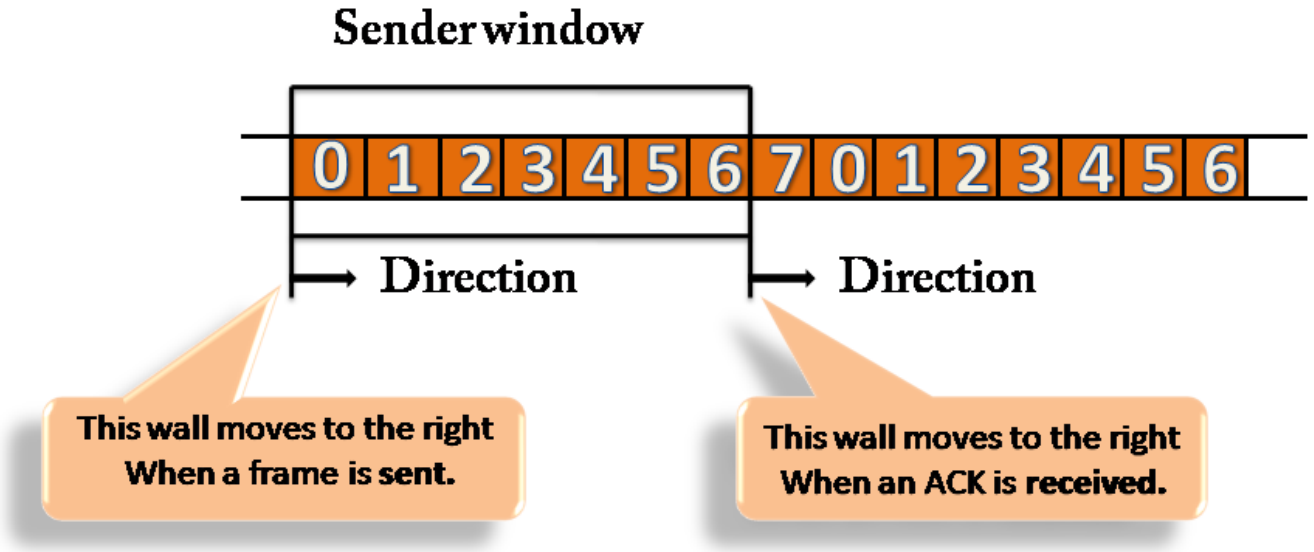
Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.

- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.

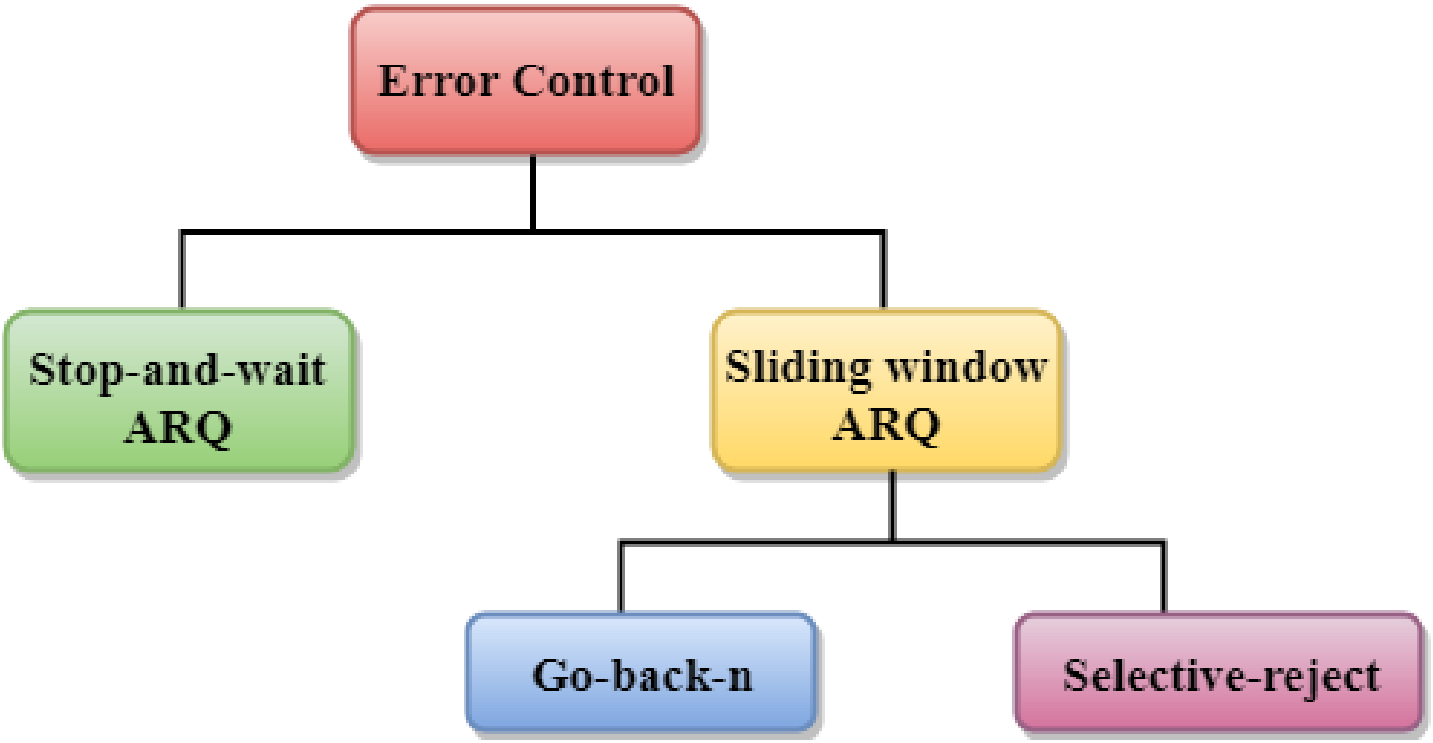
- A single ACK acknowledge multiple frames.

- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.


Sender window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right
When a frame is sent.
This wall moves to the right
When an ACK is received.

Error Control

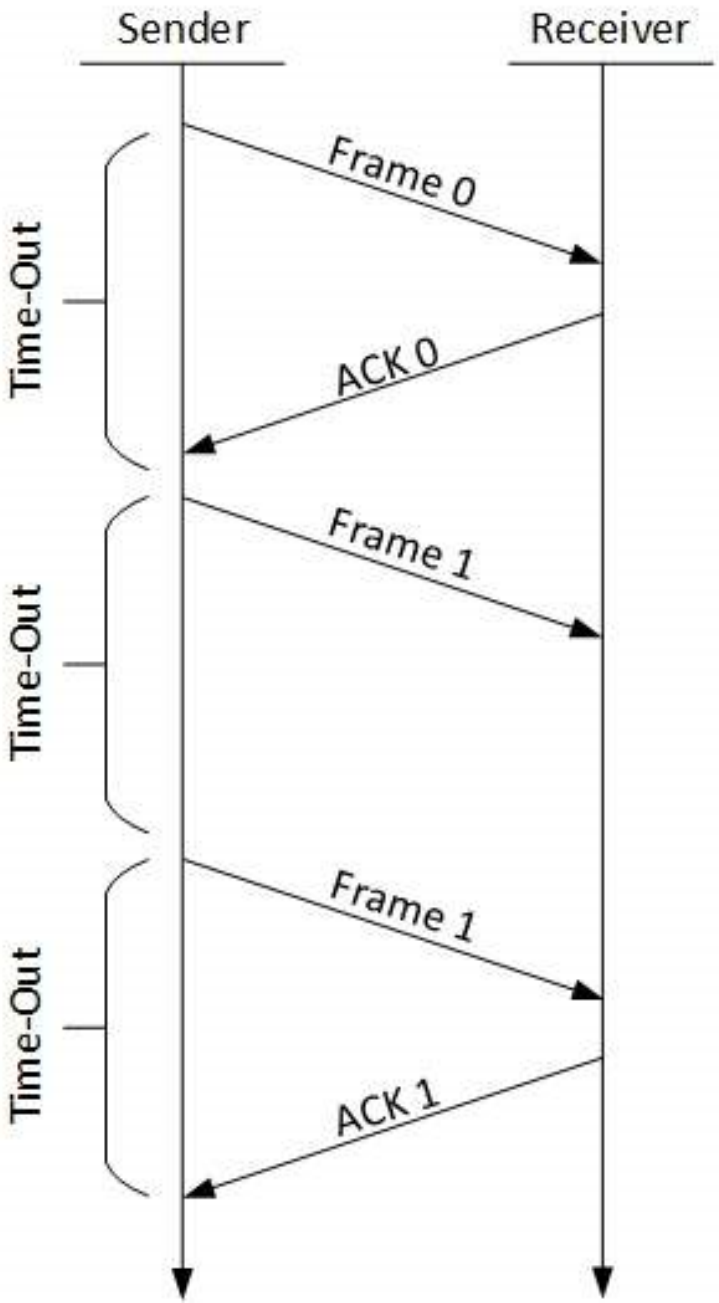
Error Control is a technique of error detection and retransmission.



Stop-and-wait ARQ

- Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

- This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.


Sender
Receiver
Frame 0
ACK 0
Frame 1
Frame 1
ACK 1
Time-Out
Time-Out
Time-Out

The following transition may occur in Stop-and-Wait ARQ:

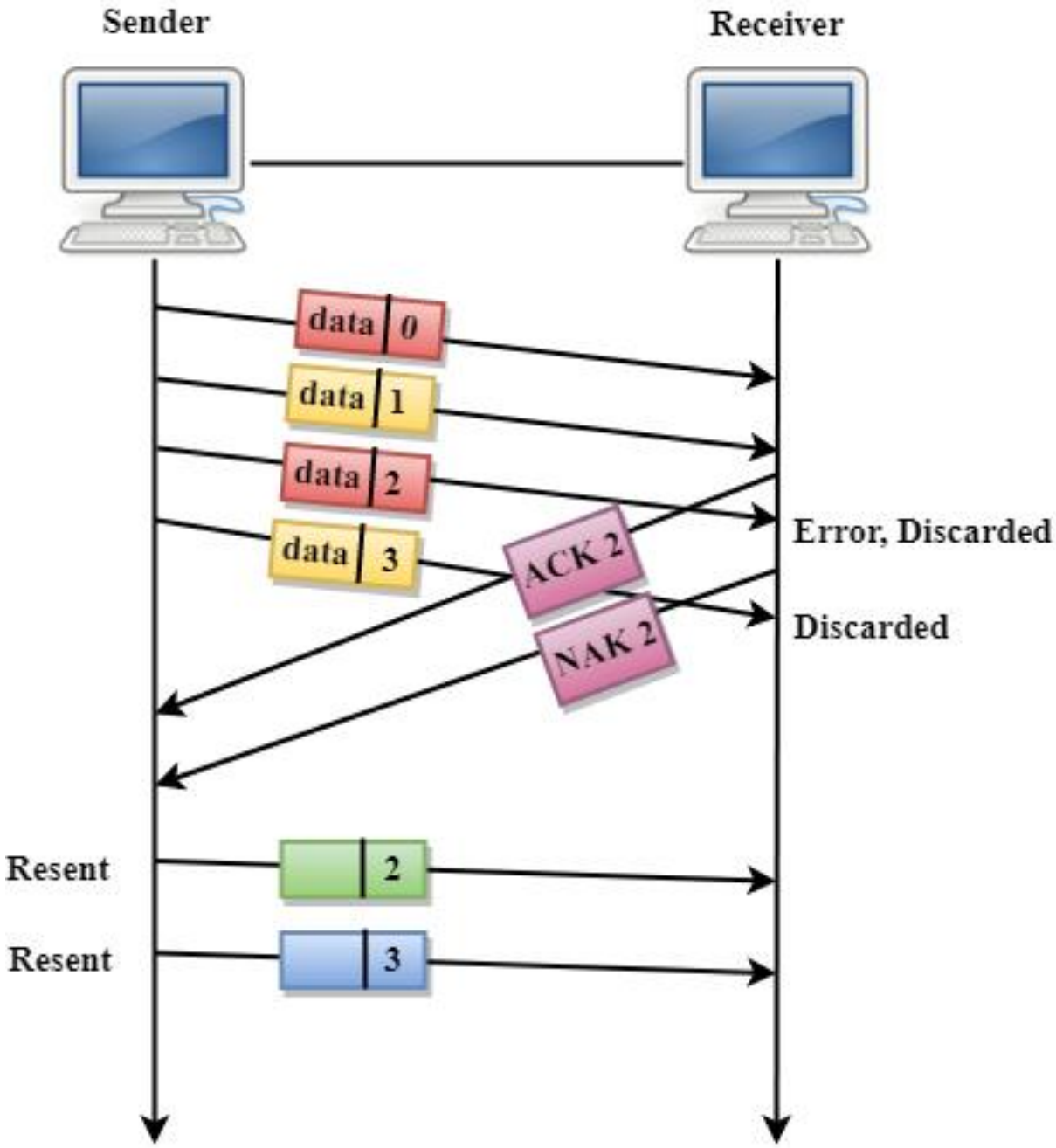
- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

Two possibilities of the retransmission:

- Damaged Frame
- Lost Frame

Go-Back-N ARQ

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.


Sender
Receiver
data 0
data 1
data 2
data 3
Error, Discarded
ACK 2
Discarded
NAK 2
Resent
2
Resent
3

Selective-Repeat ARQ

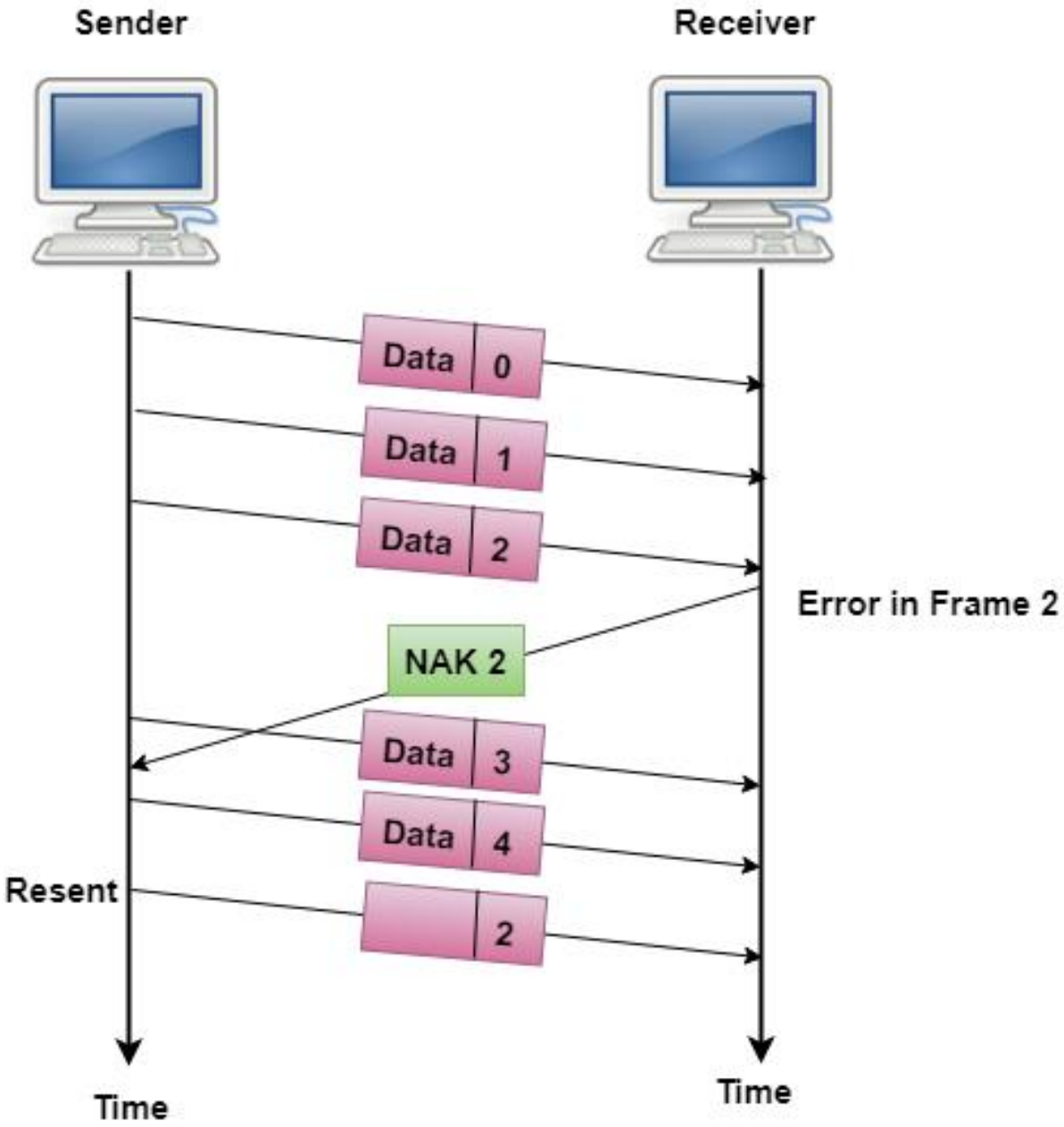
- **Selective-Repeat** ARQ technique is more efficient than Go-Back-n ARQ.

- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.

- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.

- The receiver must have an appropriate logic for reinserting the frames in a correct order.

- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.

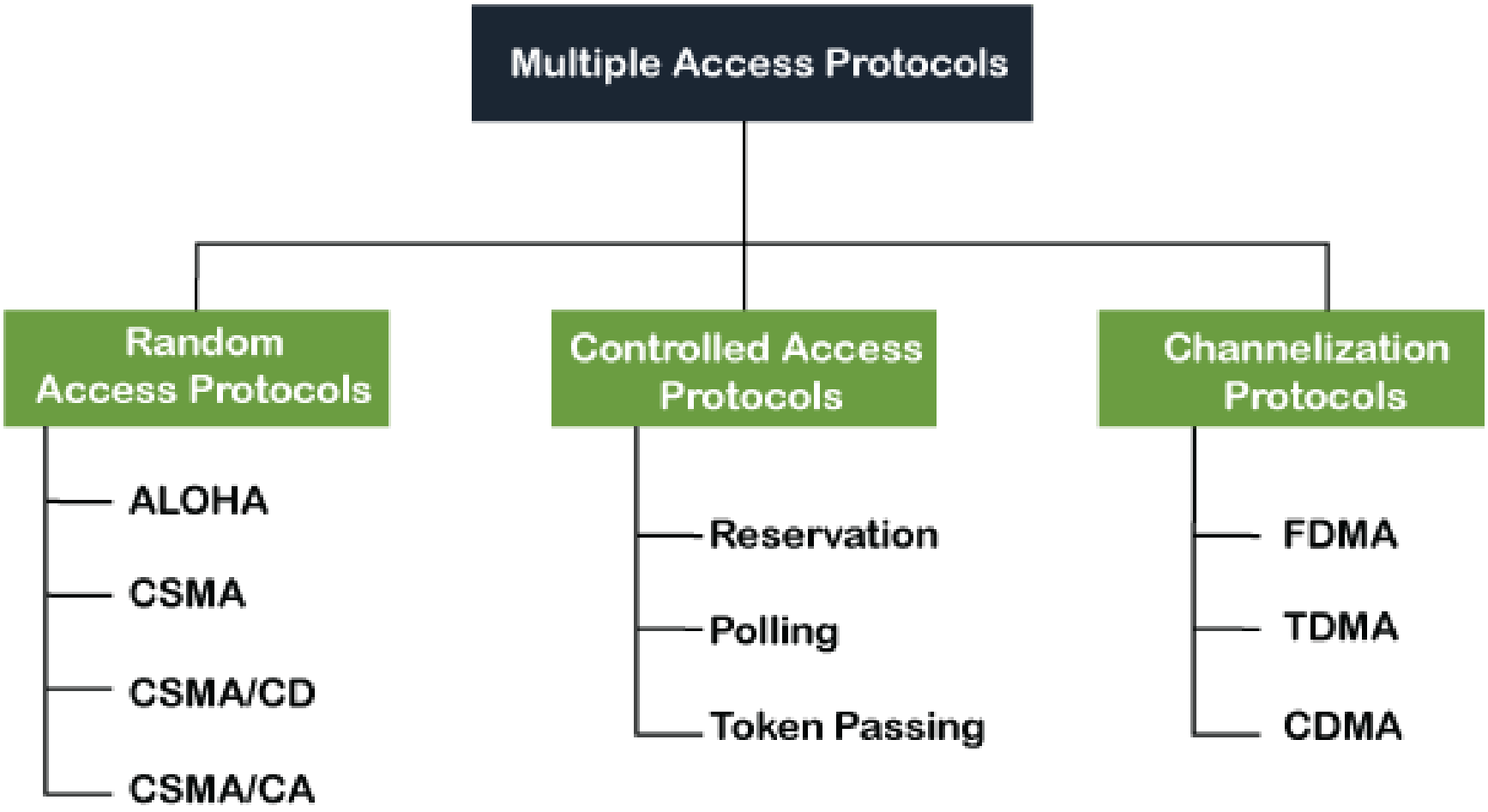

Sender
Receiver
Data 0
Data 1
Data 2
Error in Frame 2
NAK 2
Data 3
Data 4
Resent
2
Time
Time

Multiple access protocol- ALOHA, CSMA, CSMA/CA and CSMA/CD

What is a multiple access protocol?

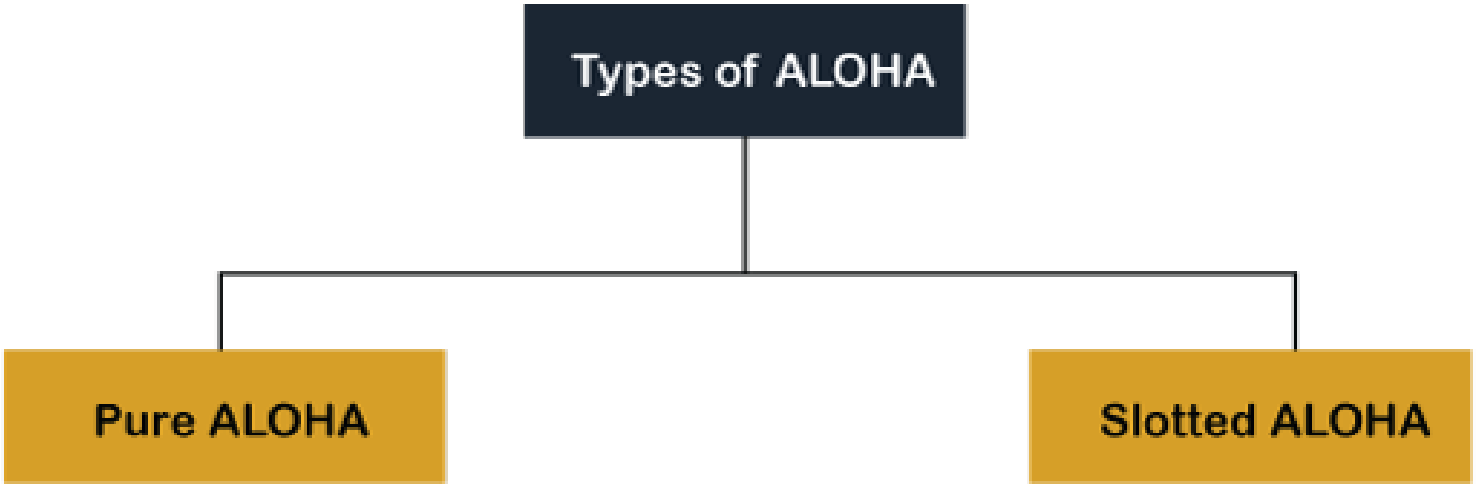
- When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices.

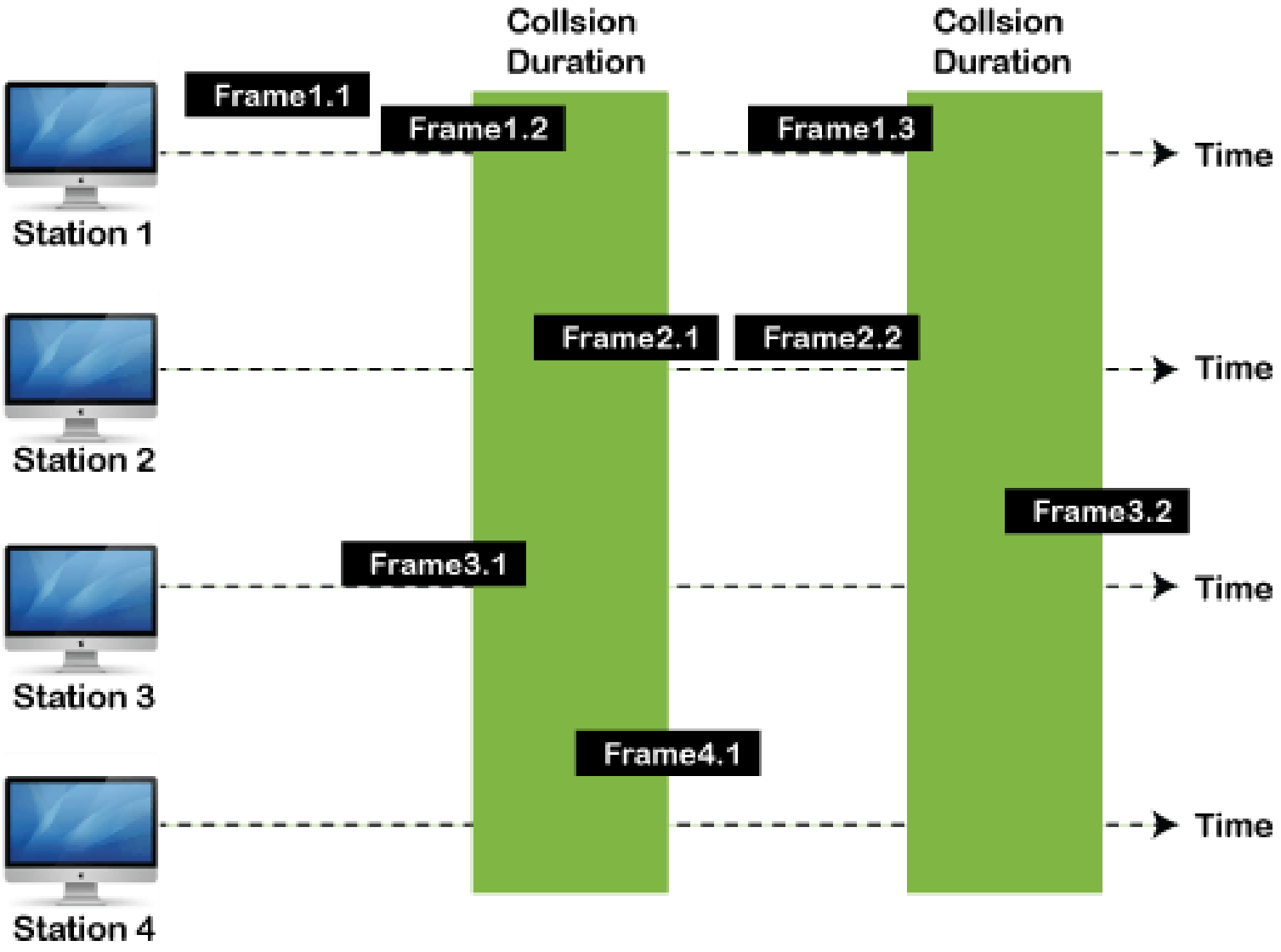
- In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the **multiple access protocol** is required to reduce the collision and avoid crosstalk between the channels.


Multiple Access Protocols
Random Access Protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Controlled Access Protocols
Reservation
Polling
Token Passing
Channelization Protocols
FDMA
TDMA
CDMA

Aloha Rules

- Any station can transmit data to a channel at any time.
- It does not require any carrier sensing.
- Collision and data frames may be lost during the transmission of data through multiple stations.
- Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
- It requires retransmission of data after some random amount of time.


Types of ALOHA
Pure ALOHA
Slotted ALOHA



Frames in Pure ALOHA

- In pure Aloha, each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost.

- When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb).

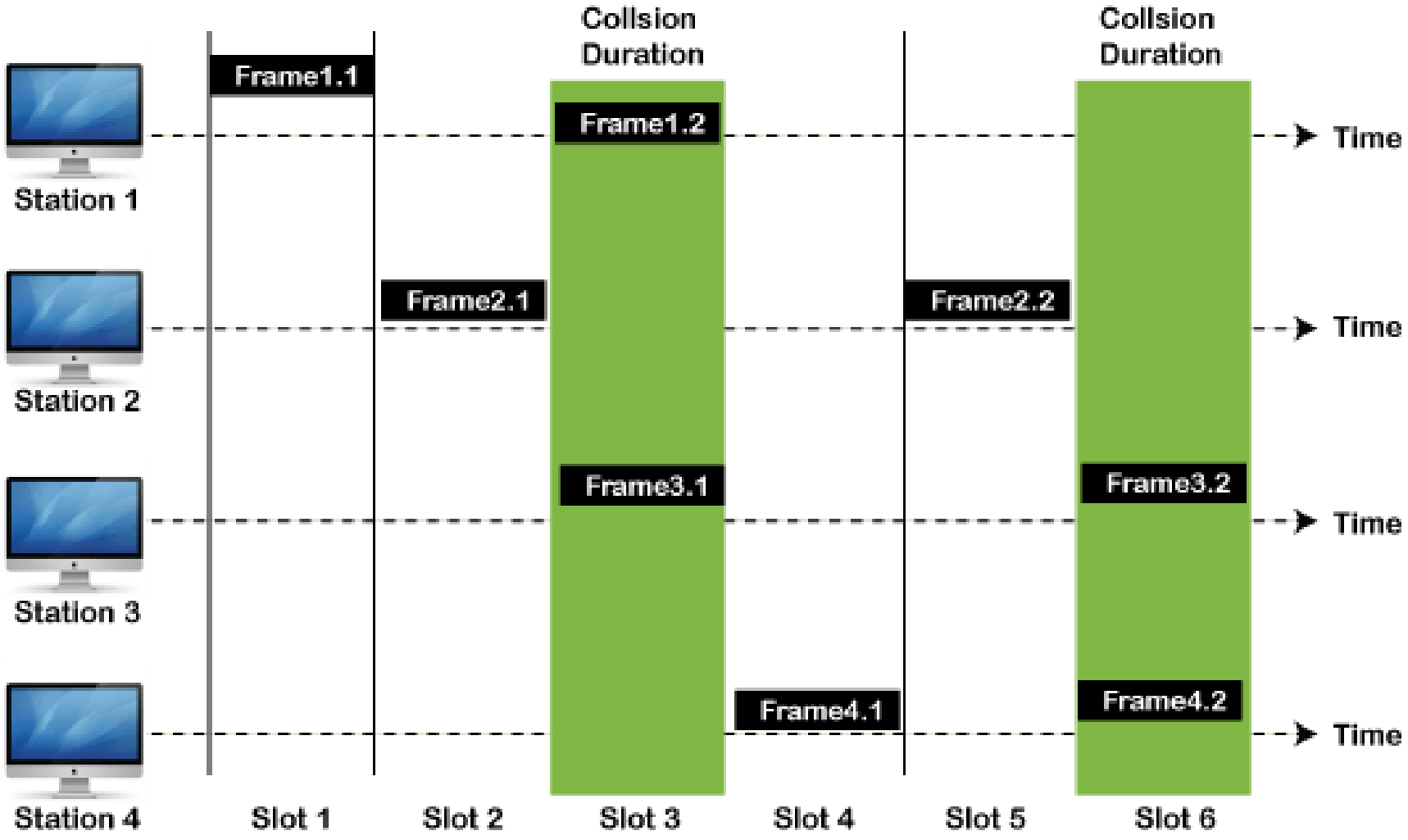
- And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

Slotted Aloha

- The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting.

- In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot.

- And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

CSMA Access Modes

1. **Persistent:**
2. **Non-Persistent:**
3. **P-Persistent:**
4. **O- Persistent:**

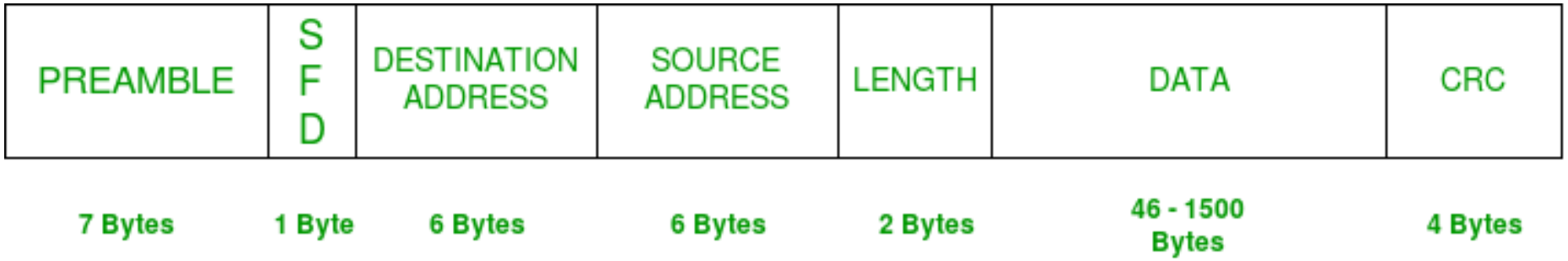
CSMA/ CD

It first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the **CSMA/CD**, the station sends a **jam/ stop** signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. In contrast to CSMA/CD (Carrier Sense Multiple Access/Collision Detection) that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.

Ethernet (IEEE 802.3) Frame Format



IEEE 802.3 ETHERNET Frame Format

PREAMBLE – Ethernet frame starts with 7-Bytes Preamble.
PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.

Start of frame delimiter (SFD) – This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame.Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places

Destination Address – This is 6-Byte field which contains the MAC address of machine for which data is destined.

Source Address – This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.

Length – Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.

Data – This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.

Cyclic Redundancy Check (CRC) – CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted