DATA LINK LAYER

Syllabus

UNIT-I (8 Lectures)

DATA COMMUNICATION : Characteristics, Components, Data flow, Network criteria, Topologies, Network model, Layered tasks, ARPANET, OSI model, TCP/IP protocol suite, Addressing (Text Book 2).

PHYSICAL LAYER: Transmission Media: Guided and unguided, Connecting devices: Hub, switch, bridge, router, Gateway. (Text Book-2).

Learning Outcomes: At the end of the unit the student will be able to

state the characteristics of network components and data flow.(L1)

discuss the network models and protocol stack.(L2)

differentiate transmission media and addressing mechanisms.(L2)

UNIT-II (12 Lectures)

DATA LINK LAYER: Design issues, Error detection and correction, Elementary data link protocols, Sliding window protocols. (Text Book-1).

RANDOM ACCESS: ALOHA, CSMA/CD, CSMA/CA, Controlled access, Channelization, Wired LAN: IEEE Standards, Standard Ethernet, Wireless LAN:IEEE802.11, ATM: architecture,layers (Text Book-2).

Learning Outcomes: At the end of the unit the student will be able to

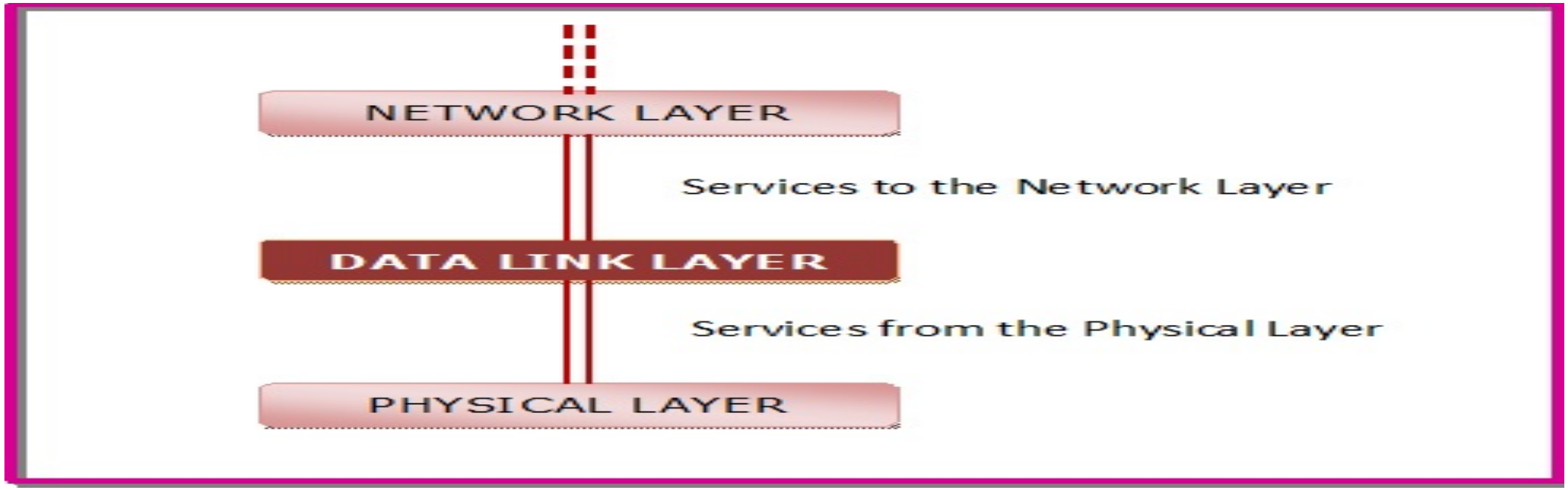
1. classify error detection and correction techniques. (L2)
2. explain random access and controlled access protocols. (L2)
3. contrast various ATM layers.(L2)

Data Link Layer Design Issues

- The data link layer in the OSI (Open System Interconnections) Model is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link. The main functions and the design issues of this layer are
- Providing services to the network layer
- Framing
- Error Control
- Flow Control

Services to the Network Layer

- In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it.
- The data link layer uses the services offered by the physical layer.The primary function of this layer is to provide a well defined service interface to network layer above it.

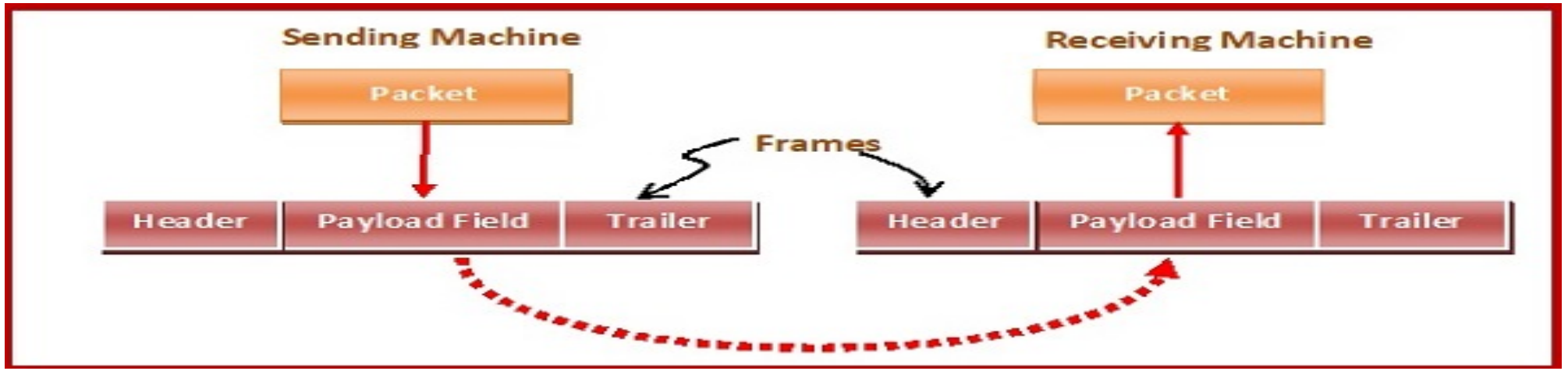


Services to the Network Layer

- The types of services provided can be of three types −
- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

Framing

- The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.
- A frame has three parts, namely −
- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



Error Control

- The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −
- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

Flow Control

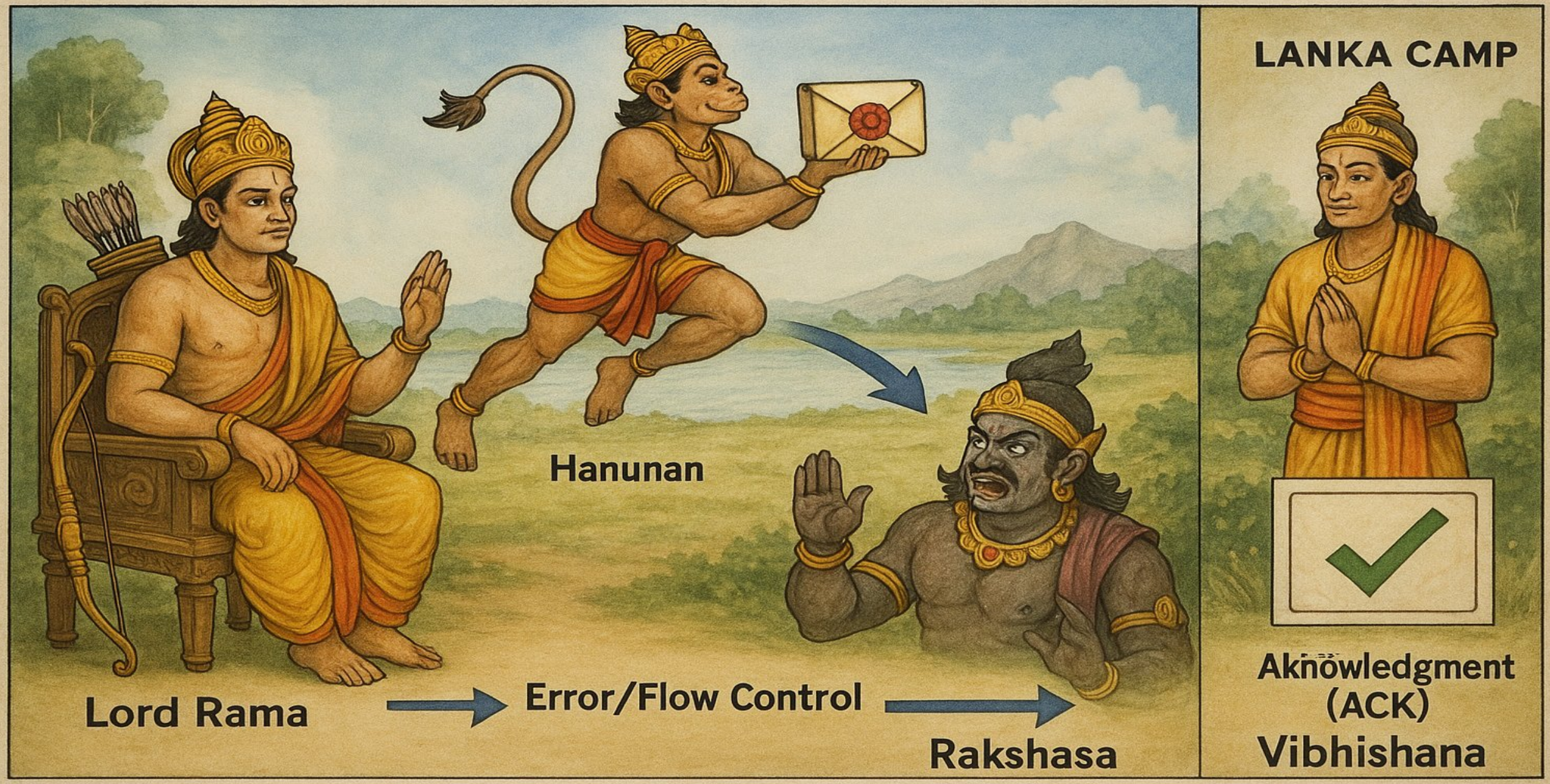
- The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −
- Feedback based flow control
- Rate based flow 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.

Data Link Layer Issue	Story Analogy
1. **Framing**	Lord Rama puts each message in a sealed envelope with a title (frame)
2. **Error Control**	Hanuman checks for torn messages. If message is corrupted, he returns
3. **Flow Control**	Hanuman waits before next flight until Vibhishana reads previous one
4. **Access Control**	Multiple messengers (pigeons/Vanaras) take turns — only one flies at a time
5. **Message Acknowledgment**	Vibhishana sends a royal scroll back: “Message Received” (ACK)

DATA LINK LAYER DESIGN ISSUES




Error detection and correction
Stop-and-Wait
Packet
ACK
Timeout
Sliding Window
1
2
4
6
ACK
ACK
ACK
ACK
ACK
Data Frame
Start bit
Data
Checksum
Stop bit

Error Detection Techniques

- These techniques **detect** the presence of errors but **do not correct** them. Once an error is detected, the receiver typically requests a retransmission.
- **1. Parity Bits**
- **Description**: Adds an extra bit to data to make the number of 1s either even (even parity) or odd (odd parity).
- **Types**:
  - Even Parity
  - Odd Parity

Error Detection Techniques

- **2. Checksum**
- **Description**: Sender adds up all data segments as binary numbers, and the result (checksum) is sent along. The receiver performs the same operation and compares the result.
- **Used in**: UDP, TCP, IP protocols.
- **Limitation**: Not very reliable for detecting all errors.
- **3. Cyclic Redundancy Check (CRC)**
- **Description**: Treats the data as a polynomial and divides it by a predetermined generator polynomial. The remainder is the CRC.
- **Receiver**: Performs the same operation and compares the CRC.
- **Advantages**: Detects burst errors effectively.
- **Used in**: Ethernet, HDLC, etc.

Error Detection Techniques

- **4. Hamming Distance (for detection)**
- Measures the number of differing bits between two binary strings.
- If Hamming distance ≥ 2, at least 1-bit error can be detected.

Error Correction Techniques

- These techniques **detect and correct** errors without needing retransmission.
- **1. Hamming Code**
- **Detects and corrects** single-bit errors.
- **Working**: Redundant bits are added at specific positions in the data.
- **Capability**: Can correct 1-bit errors and detect 2-bit errors.

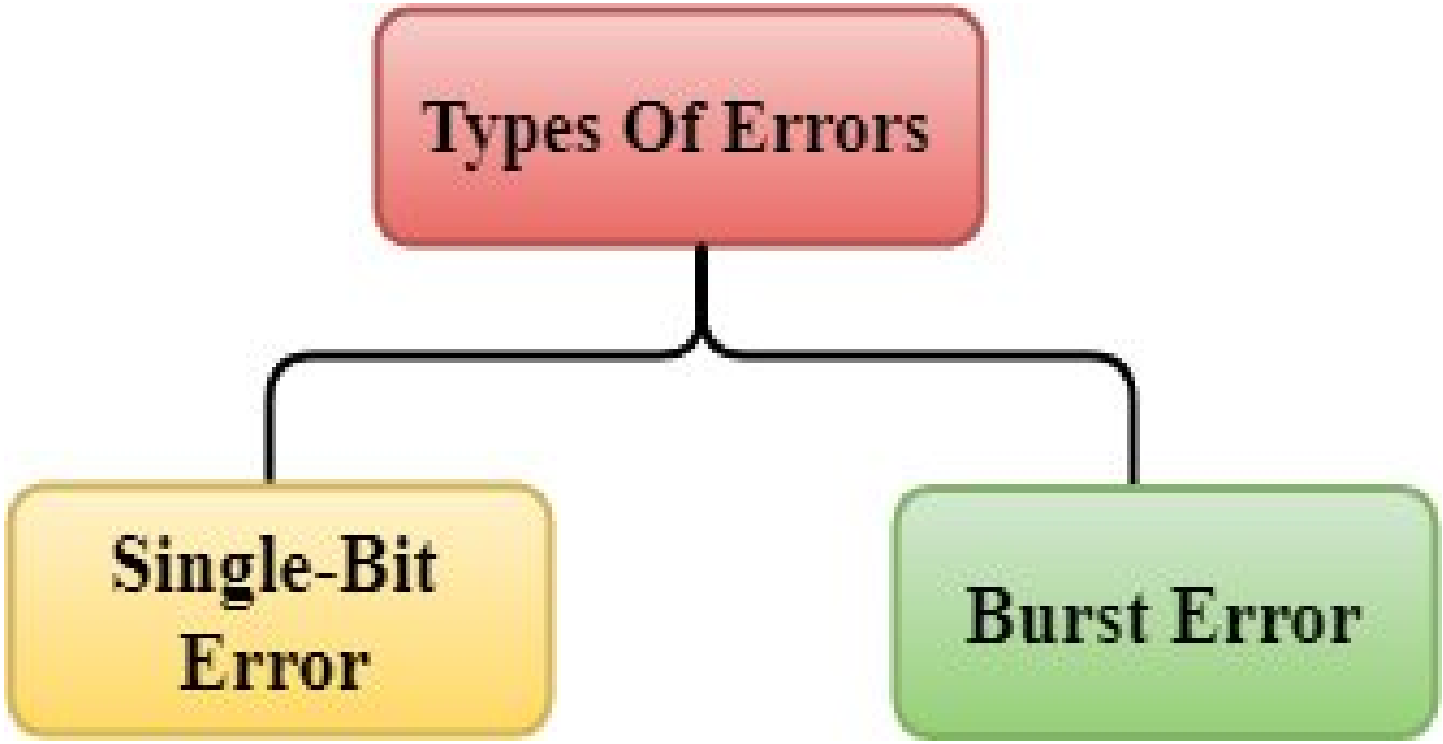
Error Correction Techniques

- **2. Forward Error Correction (FEC)**
- **Used in**: Real-time systems like audio/video streaming, satellite communication.
- **Description**: Sender encodes data with redundant information so the receiver can detect and correct errors independently.
- **Examples**:
  - Hamming Code
  - Reed-Solomon Code
  - Convolutional Code
- **3. Automatic Repeat reQuest (ARQ)**
- **Not exactly correction**, but a protocol-level technique.
- **Types**:
  - Stop-and-Wait ARQ
  - Go-Back-N ARQ
  - Selective Repeat ARQ
- **Working**: If an error is detected, the receiver requests the sender to retransmit the data.

Technique	Type	Correction	Common Usage	Detects Burst Errors?
Parity Bit	Detection	No	Simple hardware systems	No
Checksum	Detection	No	TCP, UDP, IP	Weakly
CRC	Detection	No	Ethernet, HDLC	Yes
Hamming Code	Correction	Yes	Memory systems	Limited
Reed-Solomon	Correction	Yes	CDs, DVDs, Satellite Comm	Yes
ARQ Protocols	Protocol-level	Retransmit	TCP, Wireless Networks	Yes

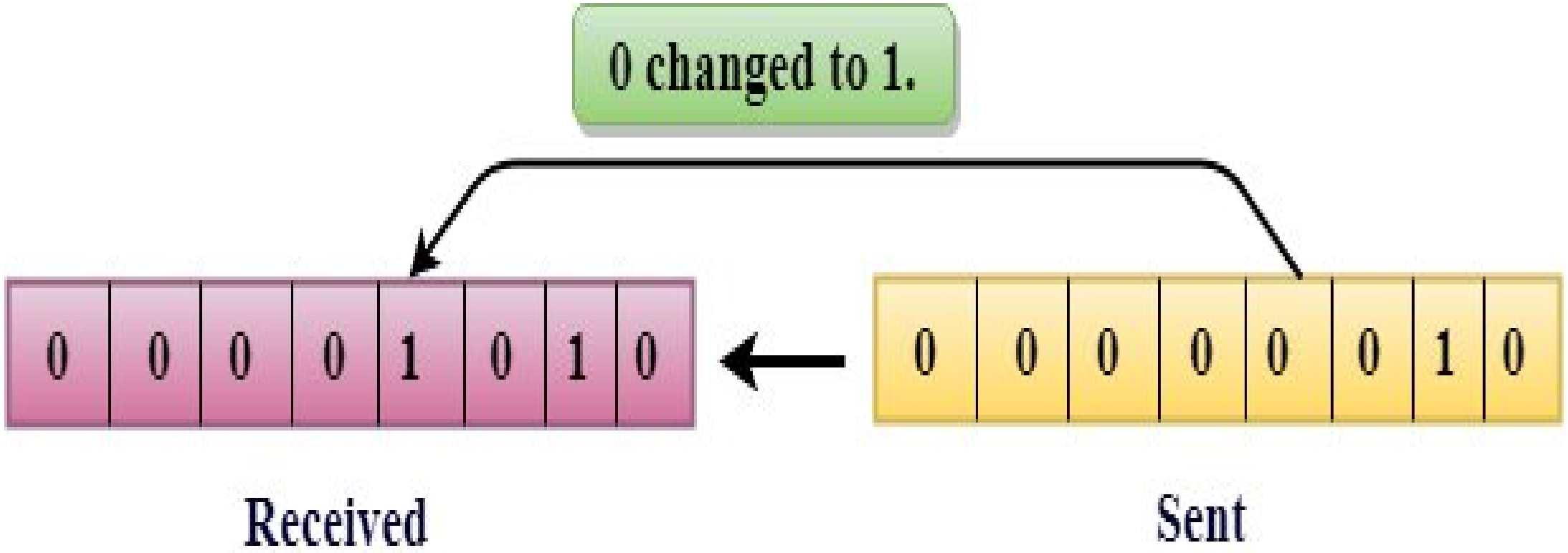
Types Of Errors

- Errors can be classified into two categories:
- Single-Bit Error
- Burst Error



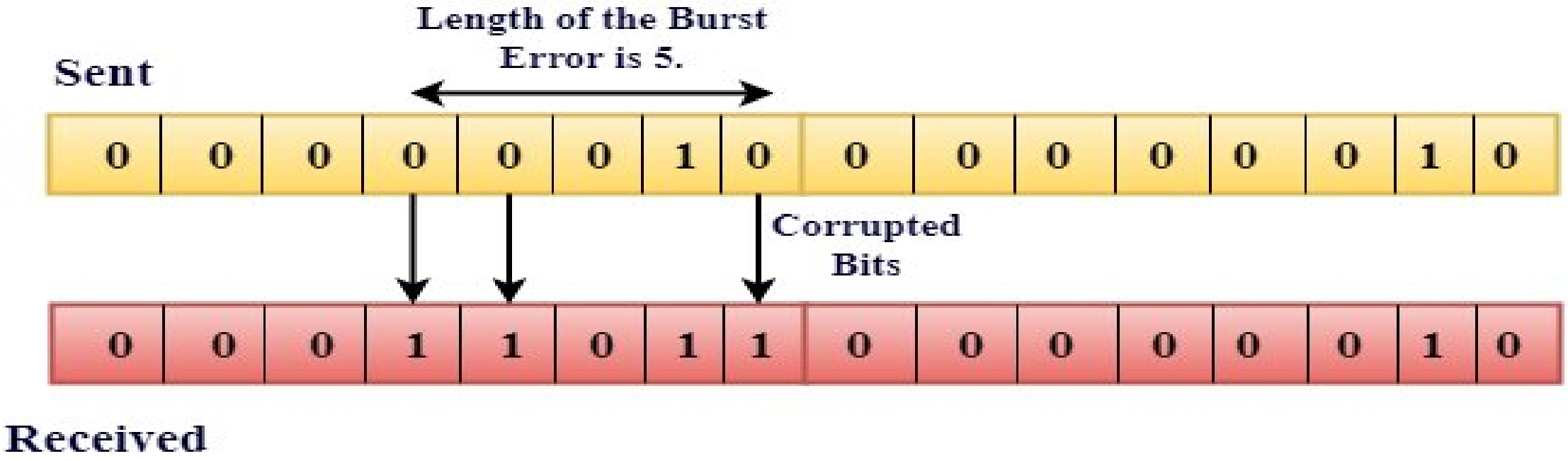
Single-Bit Error

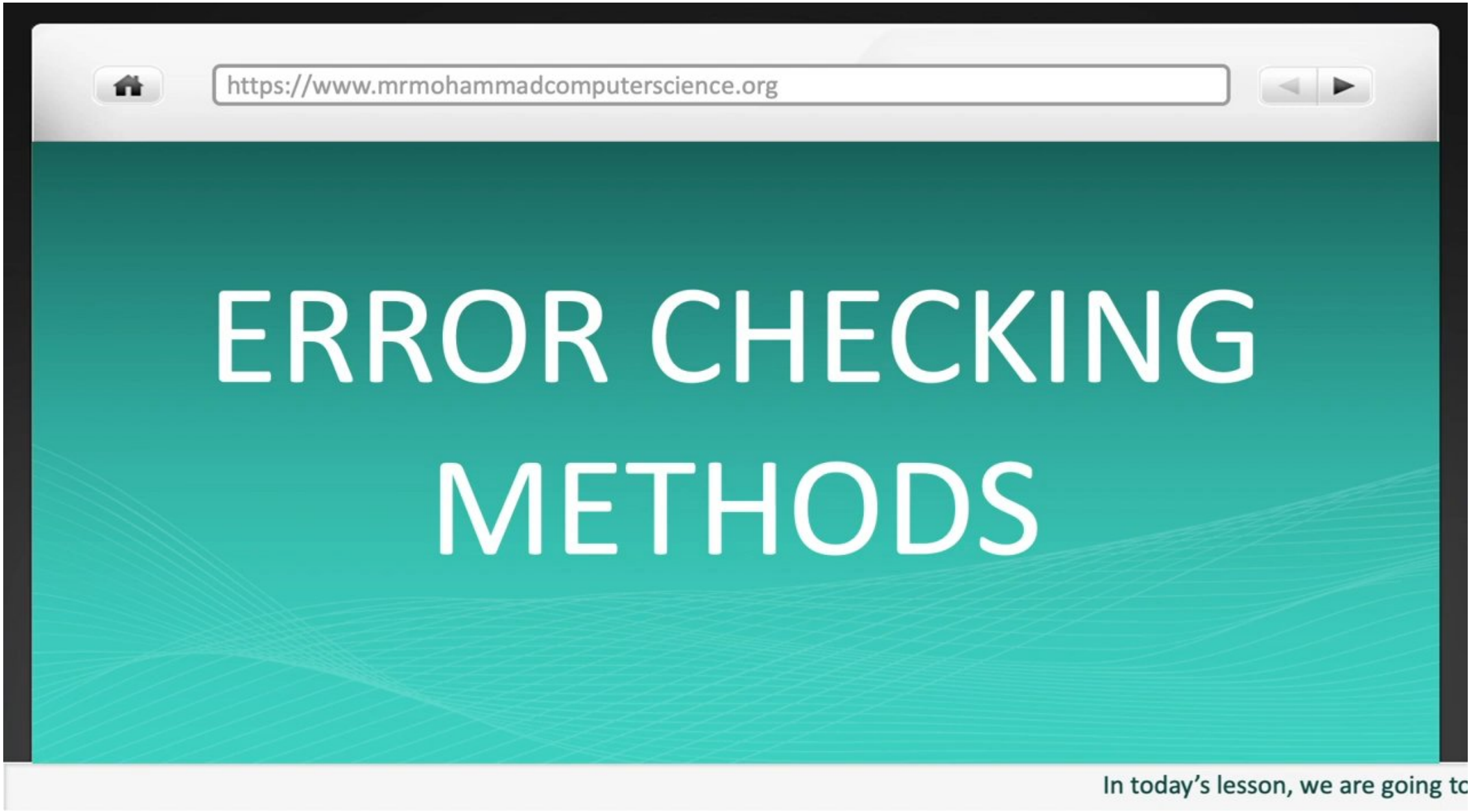
- The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



Burst Error:

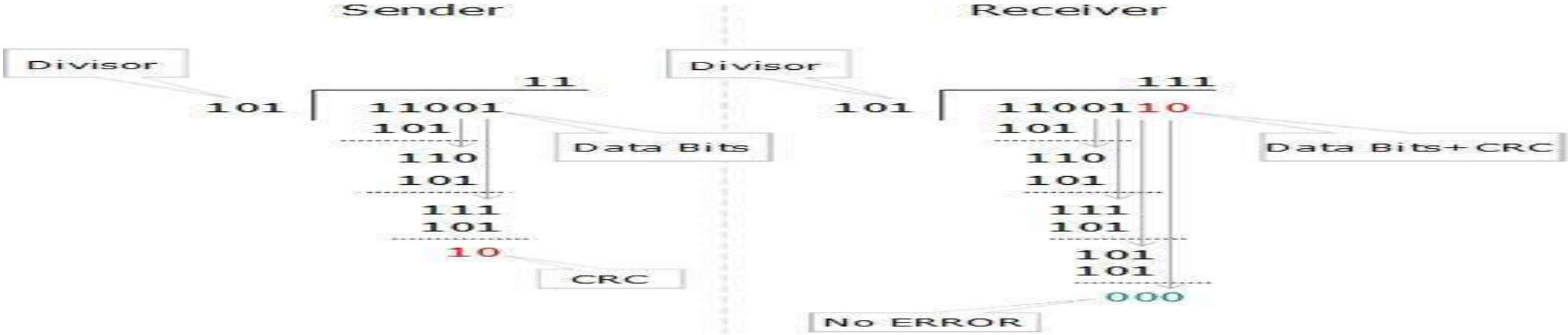
- The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.
- The Burst Error is determined from the first corrupted bit to the last corrupted bit.




https://www.mrmohammadcomputerscience.org
ERROR CHECKING METHODS
In today's lesson, we are going to

Cyclic Redundancy Check (CRC)

- CRC is a different approach to detect if the received frame contains valid data.
- This technique involves binary division of the data bits being sent. The divisor is generated using polynomials.
- The sender performs a division operation on the bits being sent and calculates the remainder.
- Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords

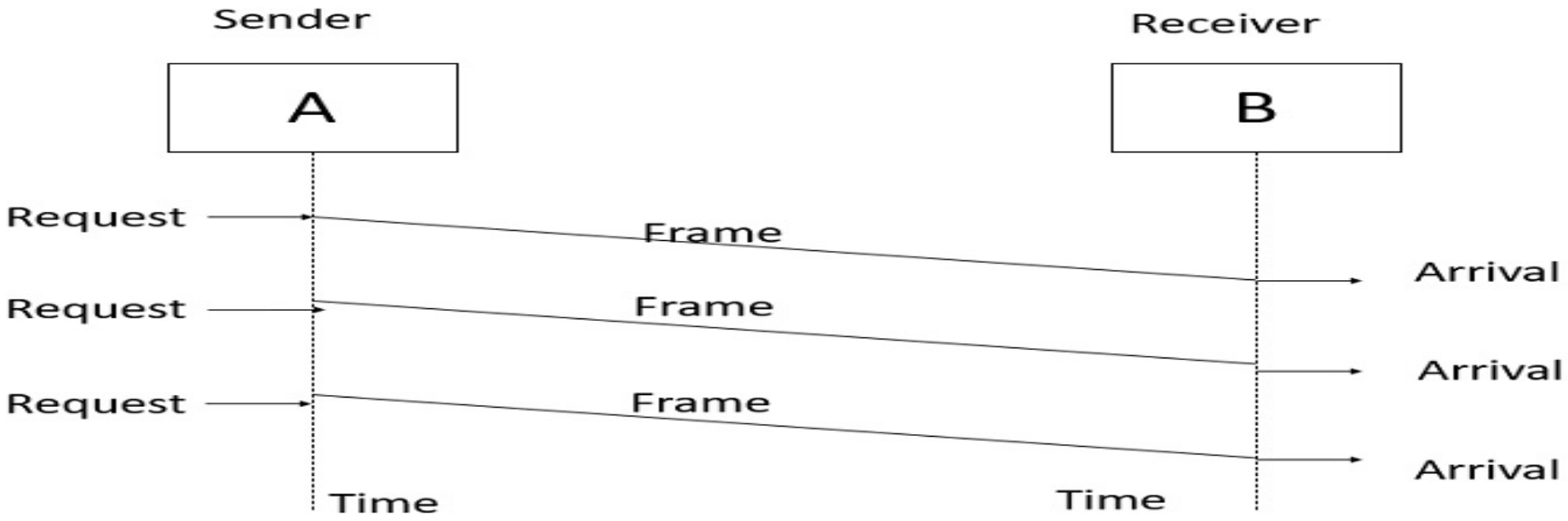


Elementary Data Link Protocols

- Elementary Data Link protocols are classified into three categories, as given below −
- Protocol 1 − Unrestricted simplex protocol
- Protocol 2 − Simplex stop and wait protocol
- Protocol 3 − Simplex protocol for noisy channels.

Unrestricted Simplex Protocol

- Data transmitting is carried out in one direction only. The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored. In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.
- The Unrestricted Simplex Protocol is diagrammatically represented as follows −

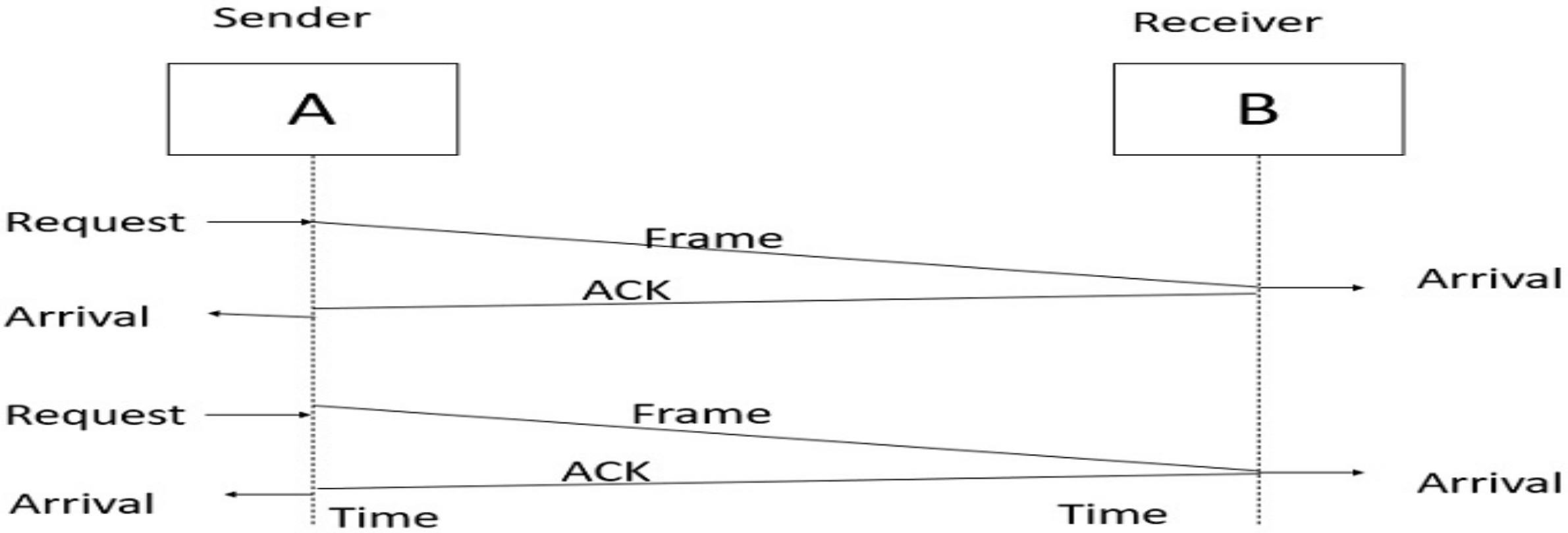


Simplex Stop and Wait protocol

- The main problem here is how to prevent the sender from flooding the receiver. The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows −
- **Step1** − The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.
- **Step 2** − Permission to send the next frame is granted.
- **Step 3** − The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.
- This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.

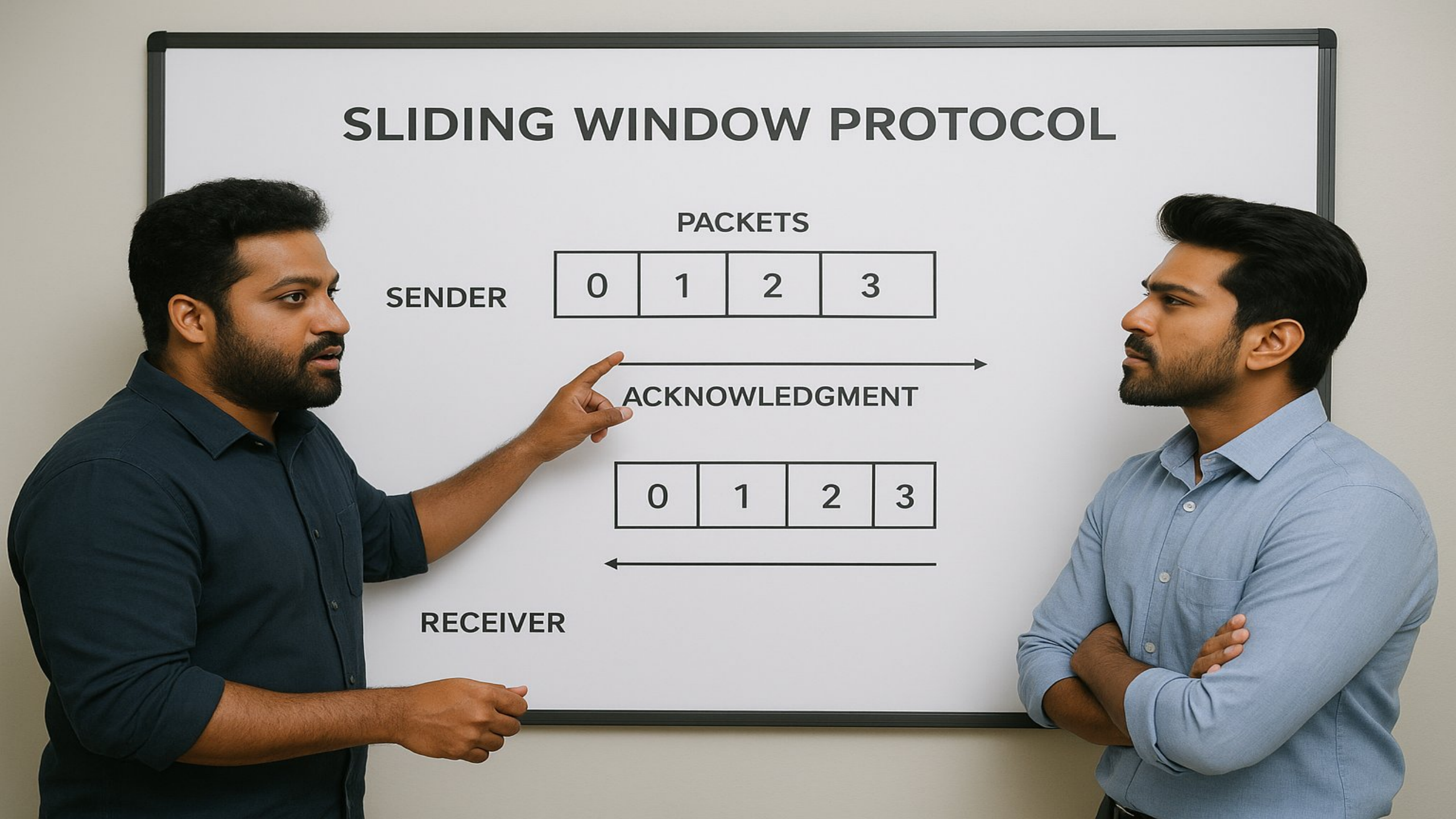
Simplex Stop and Wait protocol

- The Simplex Stop and Wait Protocol is diagrammatically represented as follows −



Simplex Protocol for Noisy Channel

- Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected. Every frame has a unique sequence number.
- After a frame has been transmitted, the timer is started for a finite time.
- Before the timer expires, if the acknowledgement is not received , the frame gets retransmitted, when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.


SLIDING WINDOW PROTOCOL
PACKETS
SENDER
0
1
2
3
ACKNOWLEDGMENT
0
1
2
3
RECEIVER

What is Sliding Window Protocol?

- Sliding Window Protocol is a flow control protocol used in reliable transmission.

- - Allows multiple frames to be sent before needing an acknowledgement.
- - Maintains a 'window' of unacknowledged packets.
- - Ensures efficient and ordered delivery.

What is a Sliding Window?

- A 'window' is the number of packets a sender can transmit without receiving an ACK.

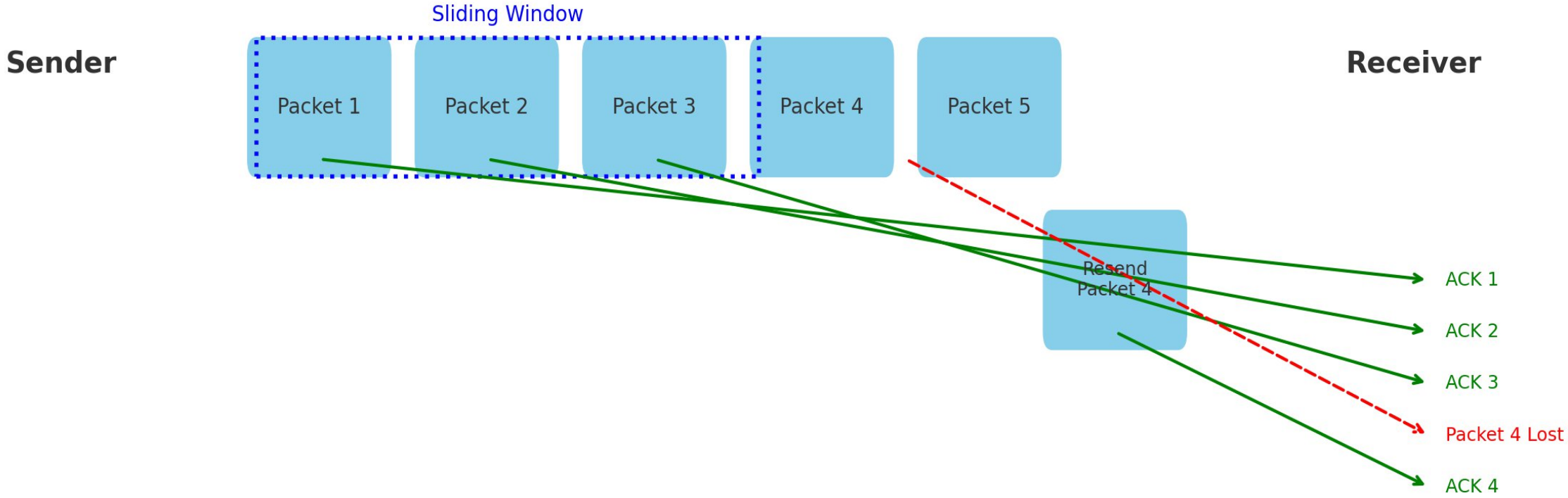
- Example:
- - Window Size = 3
- - Send packets 1, 2, 3 → Wait for ACKs
- - As ACKs arrive, the window slides forward

How It Works

- 1. Sender sends up to 'window size' packets
- 2. Receiver sends ACKs upon receiving packets
- 3. Sender slides window and sends more packets
- 4. If packet is lost, sender waits for timeout and resends

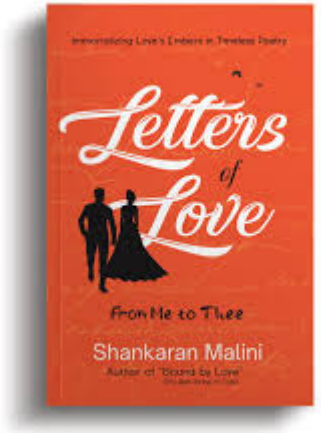
Types of Sliding Window Protocols

- - Stop-and-Wait: Window size = 1, waits for ACK after each packet
- - Go-Back-N: Resend from the lost packet onward
- - Selective Repeat: Only resend the specific lost packet


Sliding Window
Sender
Receiver
Packet 1
Packet 2
Packet 3
Packet 4
Packet 5
Resend
Packet 4
ACK 1
ACK 2
ACK 3
Packet 4 Lost
ACK 4

Letters of Love – A Sliding Window Story

A Sliding Window Story



Meet the Characters

- In this analogy, Venella (Sai Pallavi) is the Sender and Thandel (NagaChaitanya) is the Receiver.

- The 'letters' represent data packets sent from Vasitha to Thandel.

Scene Setup (The Network Analogy)

- **Sender (Vennela)** = Sender side of the protocol
- **Receiver (Thandel)** = Receiver side of the protocol
- **Letters** = Data packets
- **Birds** = Transmission medium (like the network channel)
- **Acknowledgements (ACKs)** = Return messages from Thandel confirming letter received
- **Window** = The number of letters Vennela can send before waiting for Thandel’s response

Sliding window

- **Act 1: Love in Motion – Sending Data**
- Vennela writes **5 letters at once** (assume window size = 5). She ties them to 5 birds and sends them to Thandel.
- Packets: L1, L2, L3, L4, L5 (Sent)
- Window: Slides ahead only after ACKs

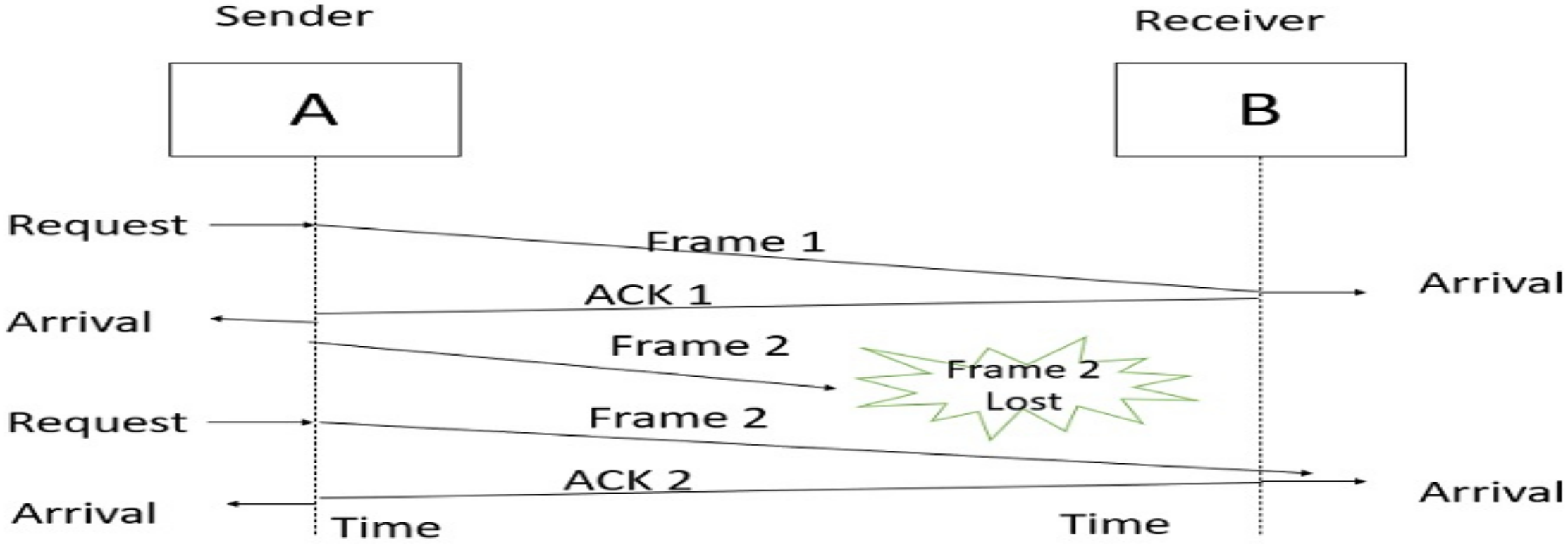
Act 2: Storm at Sea – Packet Loss

- Thandel, busy fishing in the rough sea, receives only 3 letters: **L1, L2, L4** (L3 was lost in the storm 🕊️🌊)
- He sends **ACKs** for L1, L2, and L4.

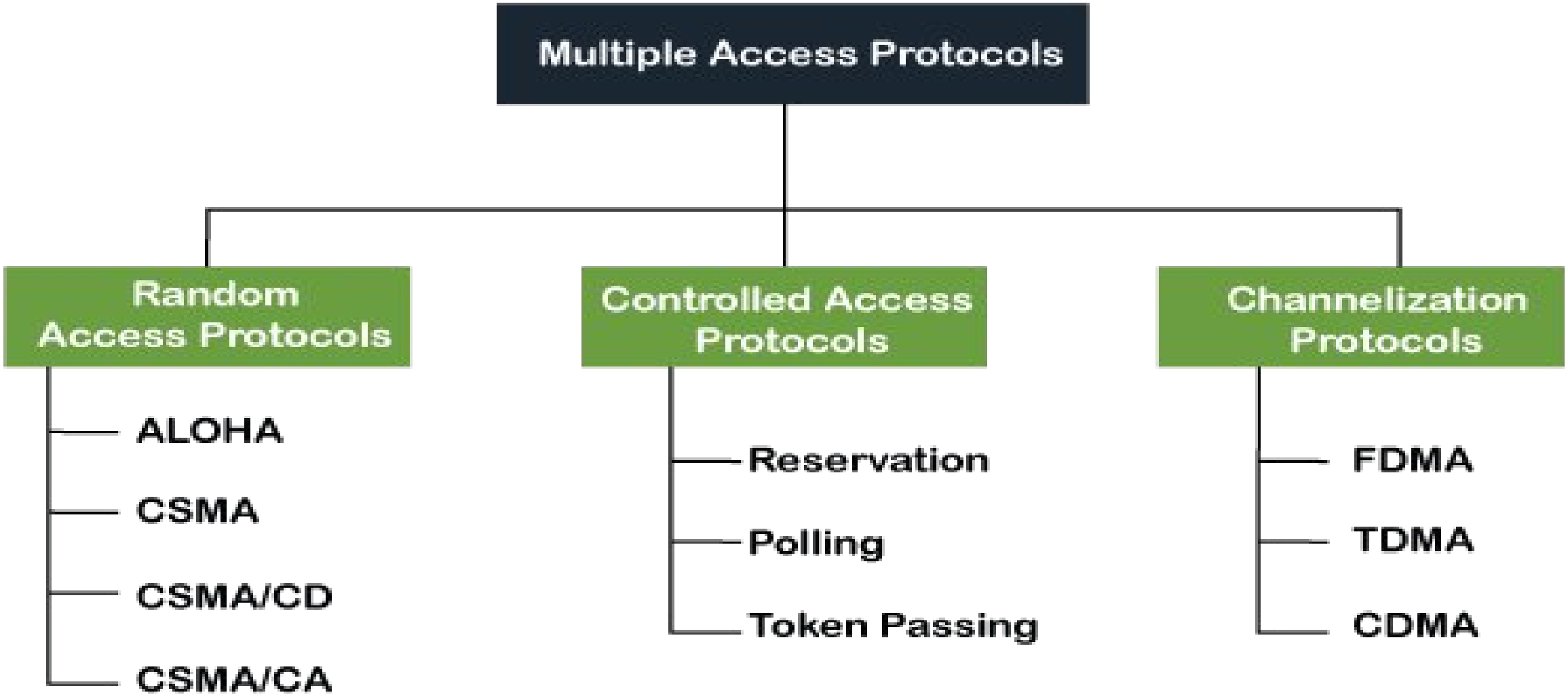

Sliding Window with Letters
Vasitha sends 3 letters ✉✉✉
Thandel receives 2 letters ✉✉
Vasitha retransmits missing lett
Thandel gets all 3 letters ✉✉✉

Simplex Protocol for Noisy Channel

- The Simplex Protocol for Noisy Channel is diagrammatically represented as follows −



RANDOM ACCESS ALOHA, CSMA/CD



Multiple Access Protocol

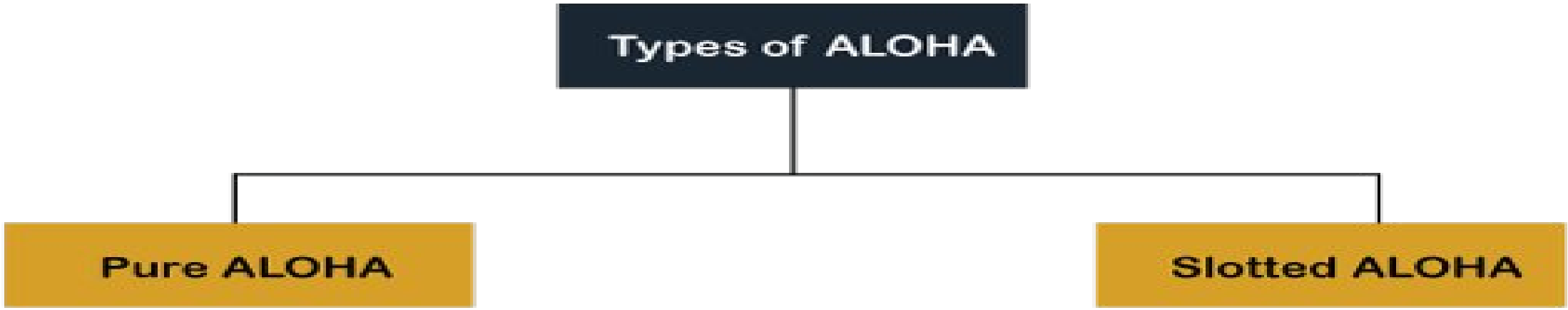
- When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel.
- Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits 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.

ALOHA Random Access Protocol

- It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

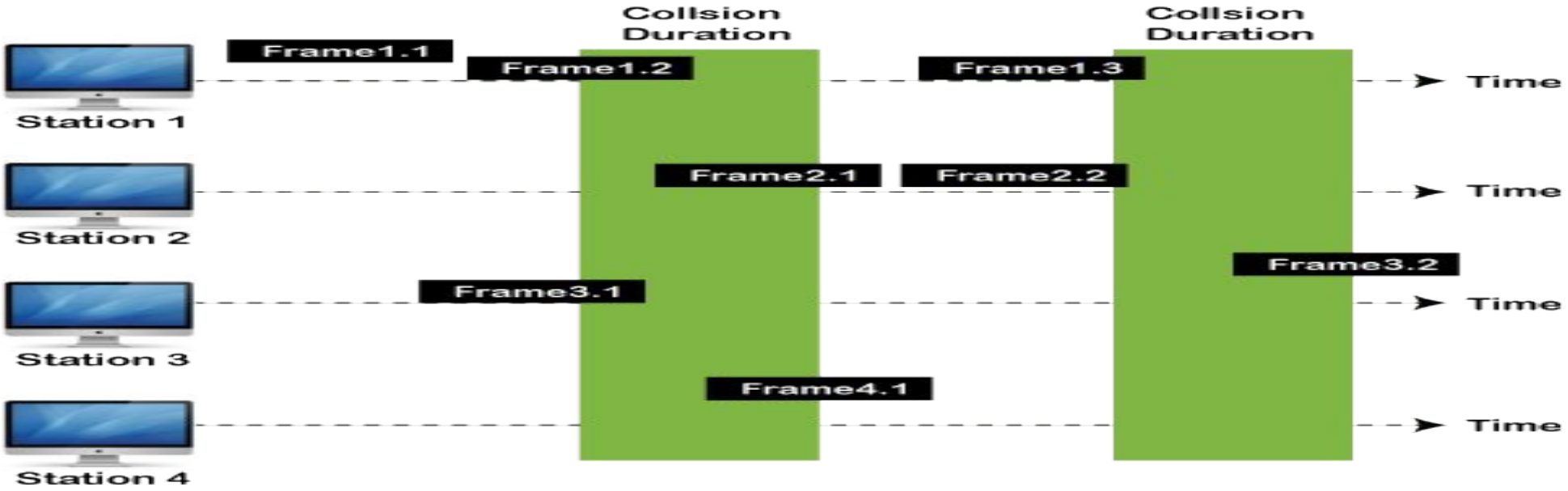
Aloha Rules

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



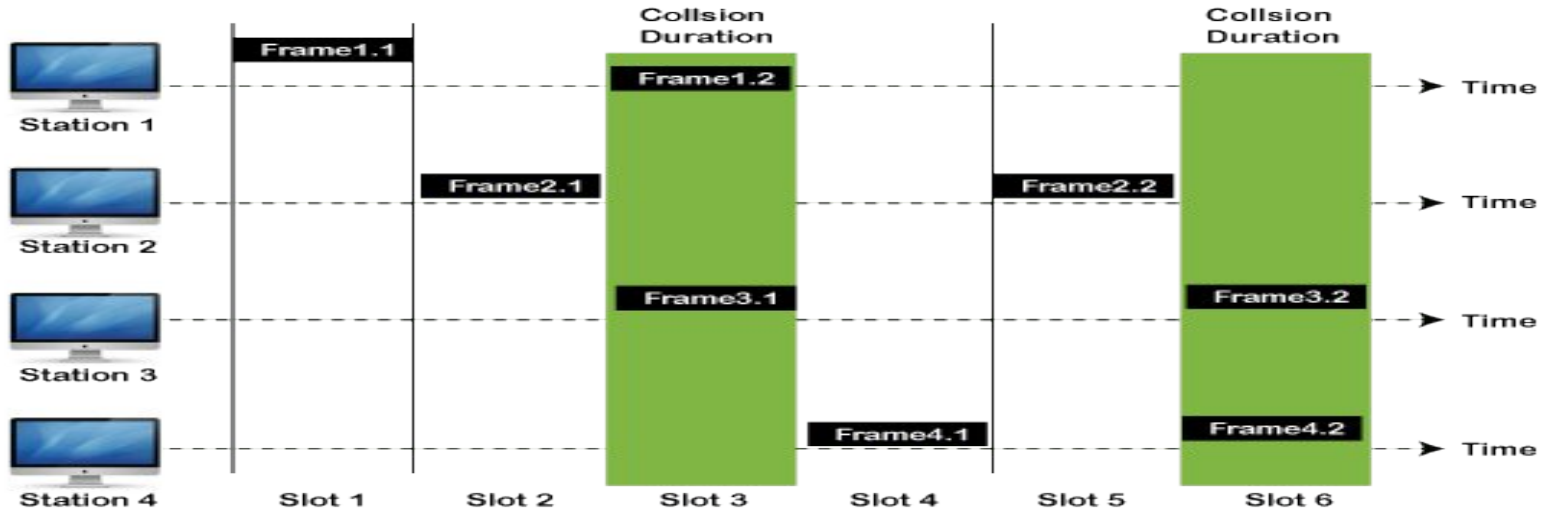
PURE ALOHA

- Whenever data is available for sending over a channel at stations, we use Pure Aloha.
- In pure Aloha, when 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.



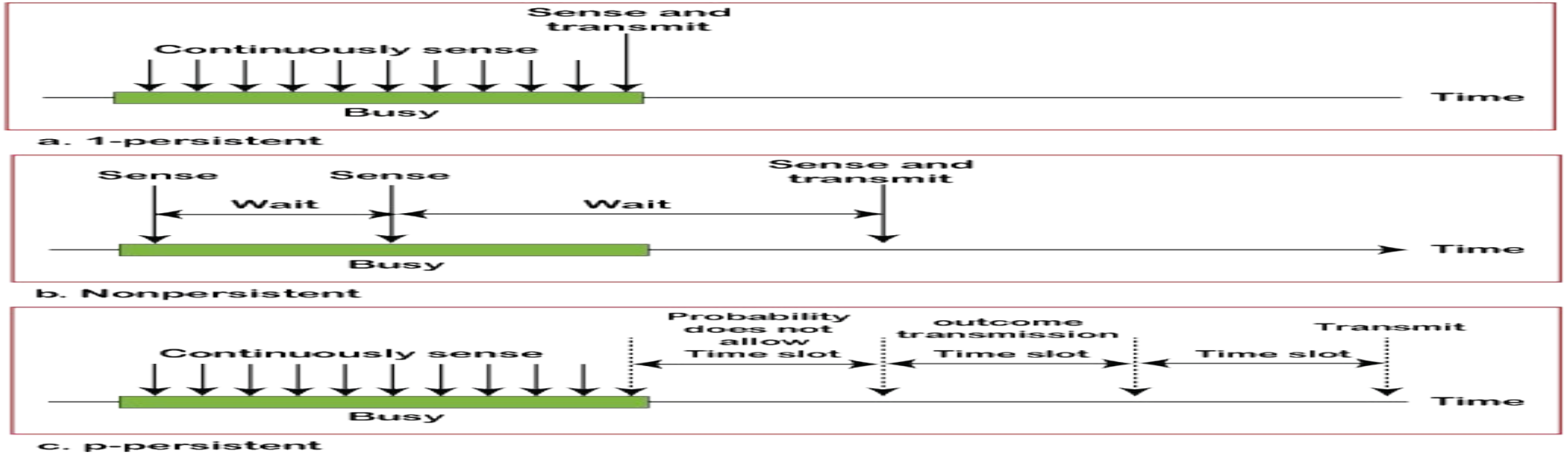
Frames in Slotted ALOHA

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:** In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.
- **Non-Persistent:** It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

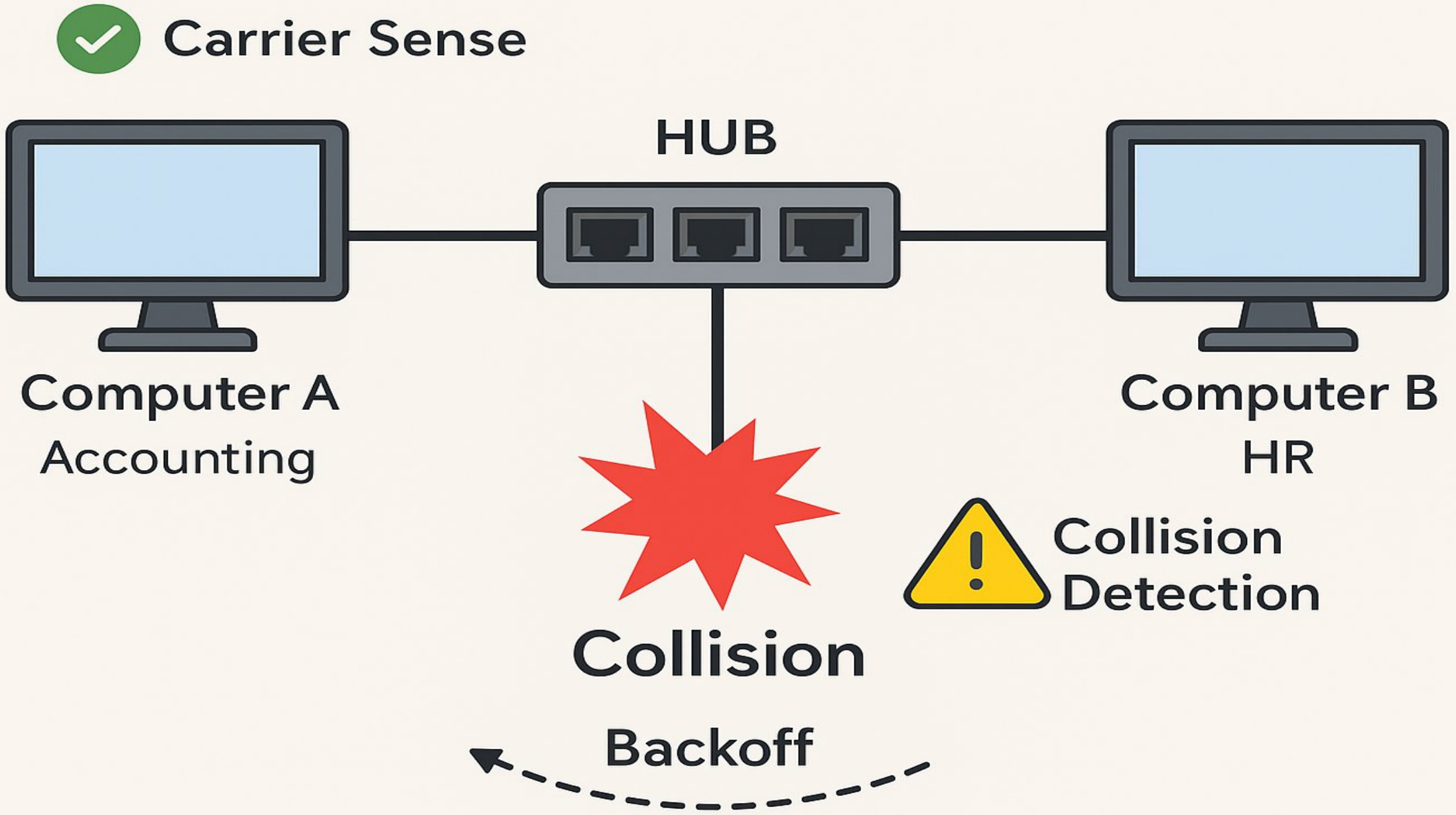
CSMA Access Modes

- **P-Persistent:** It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.
- **O- Persistent:** It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



CSMA/ CD

- It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames.
- The CSMA/CD protocol works with a medium access control layer. Therefore, 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.

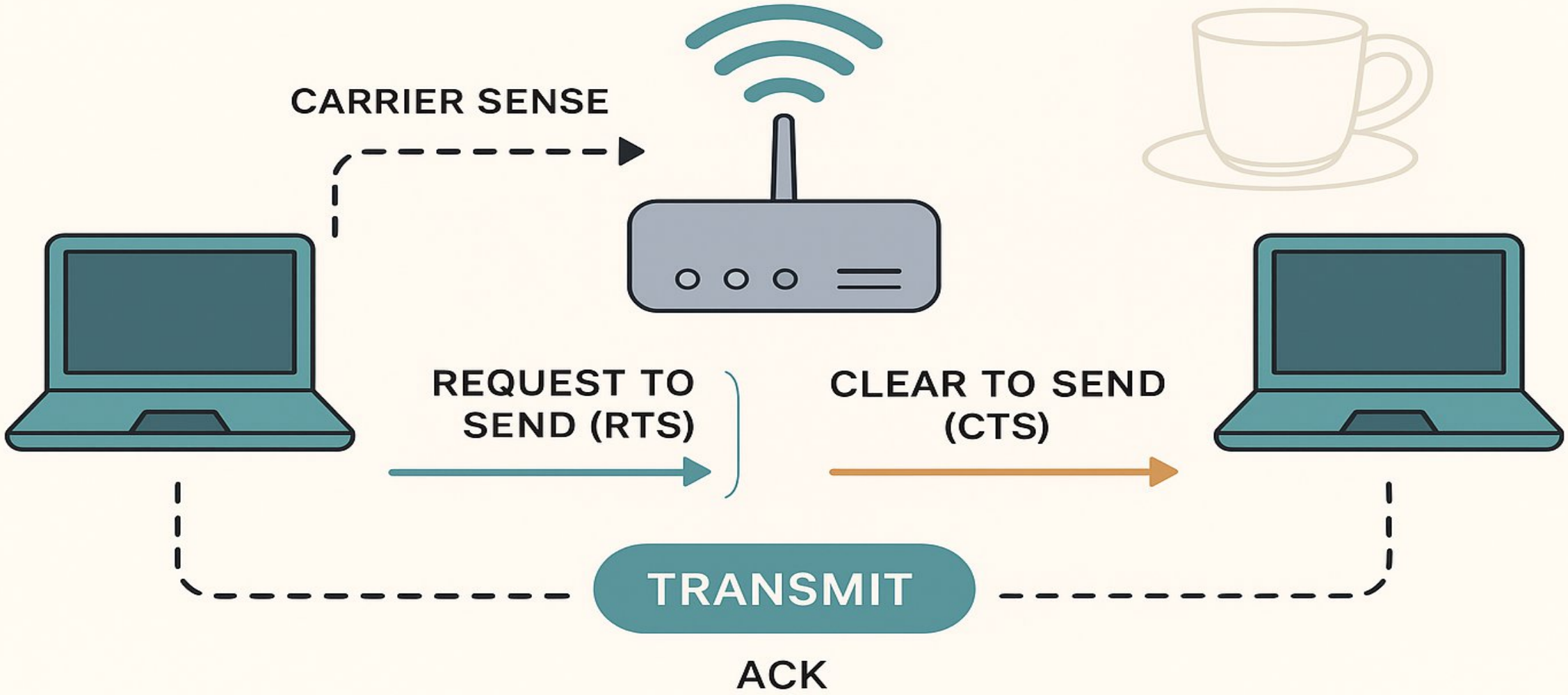

Carrier Sense
HUB
Computer A
Accounting
Computer B
HR
Collision
Detection
Collision
Backoff

CSMA/ CA

- It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer.
- When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal

CSMA/CA

CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE



CSMA:

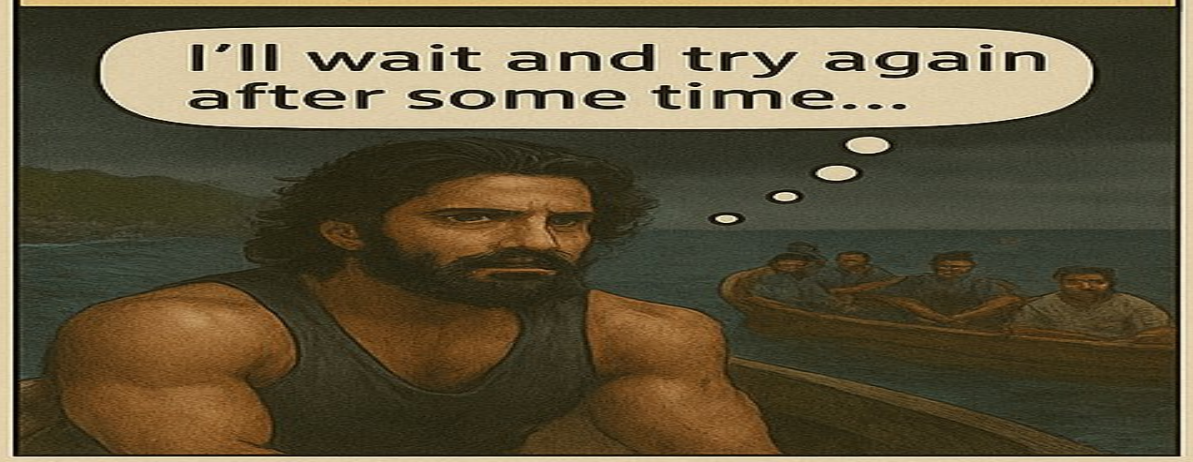
Analogy with the film ‘Tandel’

Nodes waiting to send data

Carrier Sensing

Collision

Backoff

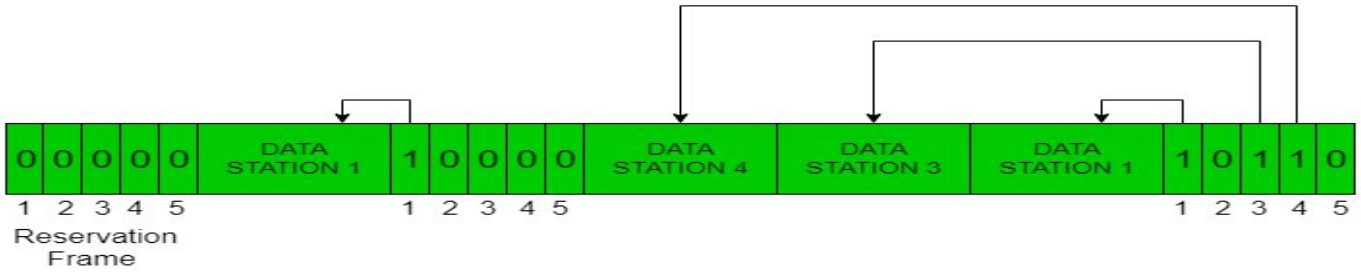


Collision when two nodes send at once

Controlled Access Protocol

- It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations.
- It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**

Reservation

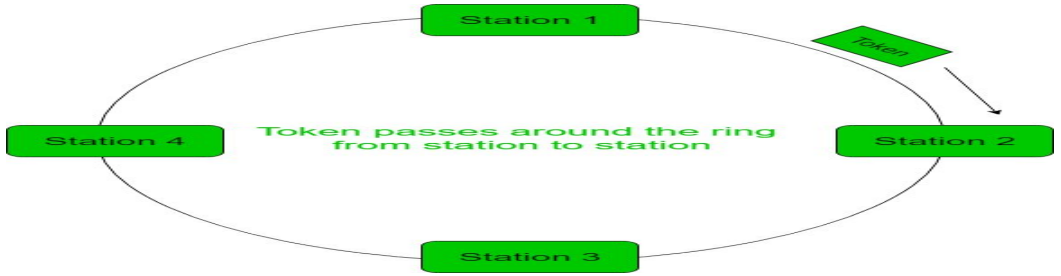


- In the reservation method, a station needs to make a reservation before sending data.
- The time line has two kinds of periods:
  - Reservation interval of fixed time length
  - Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.

Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message but the addressed one responds to it and sends data, if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.

Token Passing



- In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station
  uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.

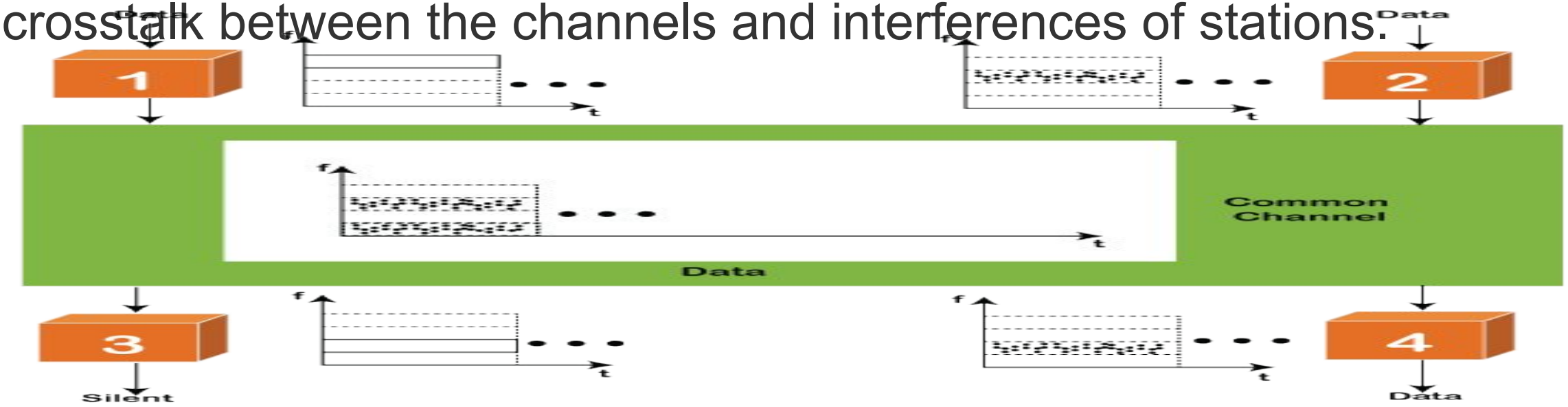

RESERVATION
POLLING
Do you have something to say?
TOKEN PASSING

Channelization

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

FDMA

- It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel.
- Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA

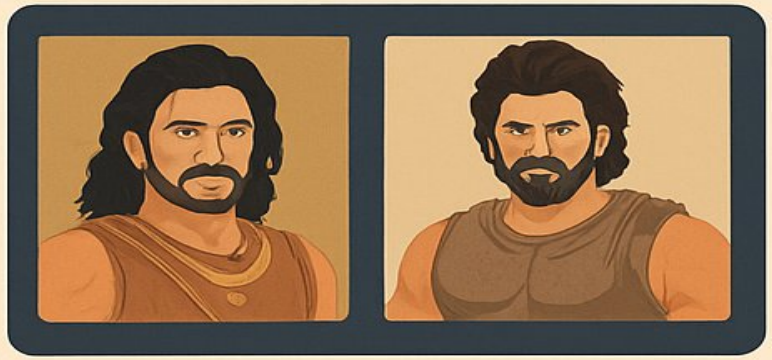
- Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames.
- The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA

- The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times.
- It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence.
- Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

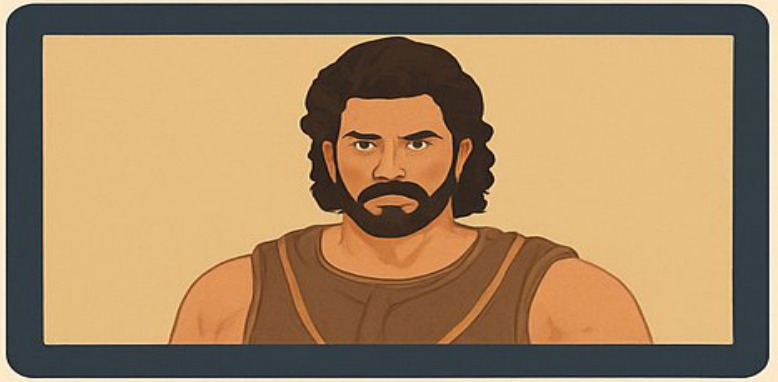
Channelization

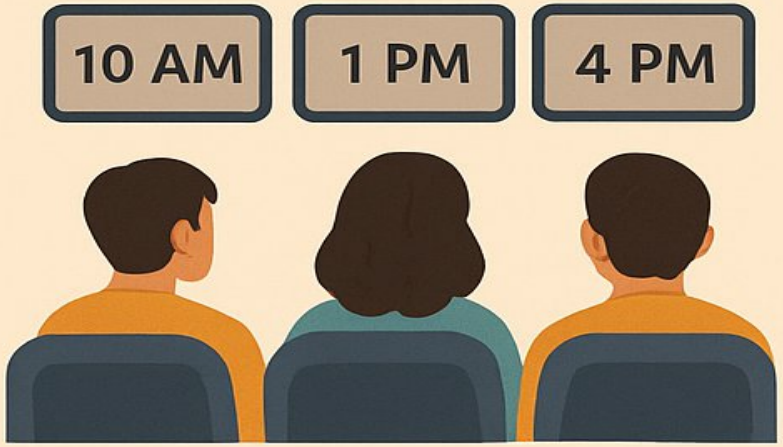
FDMA



Frequency Division
Multiple Access

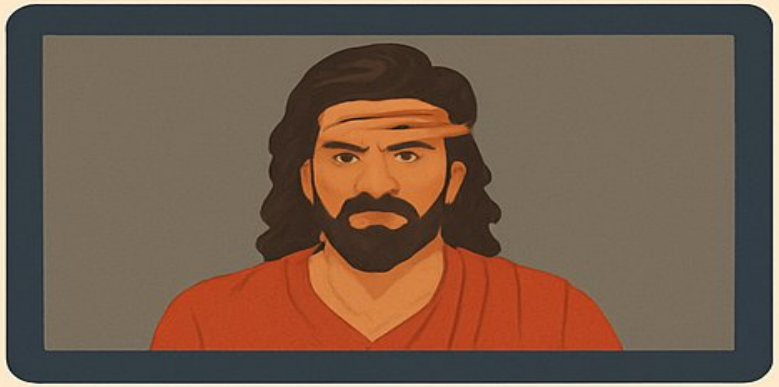
TDMA



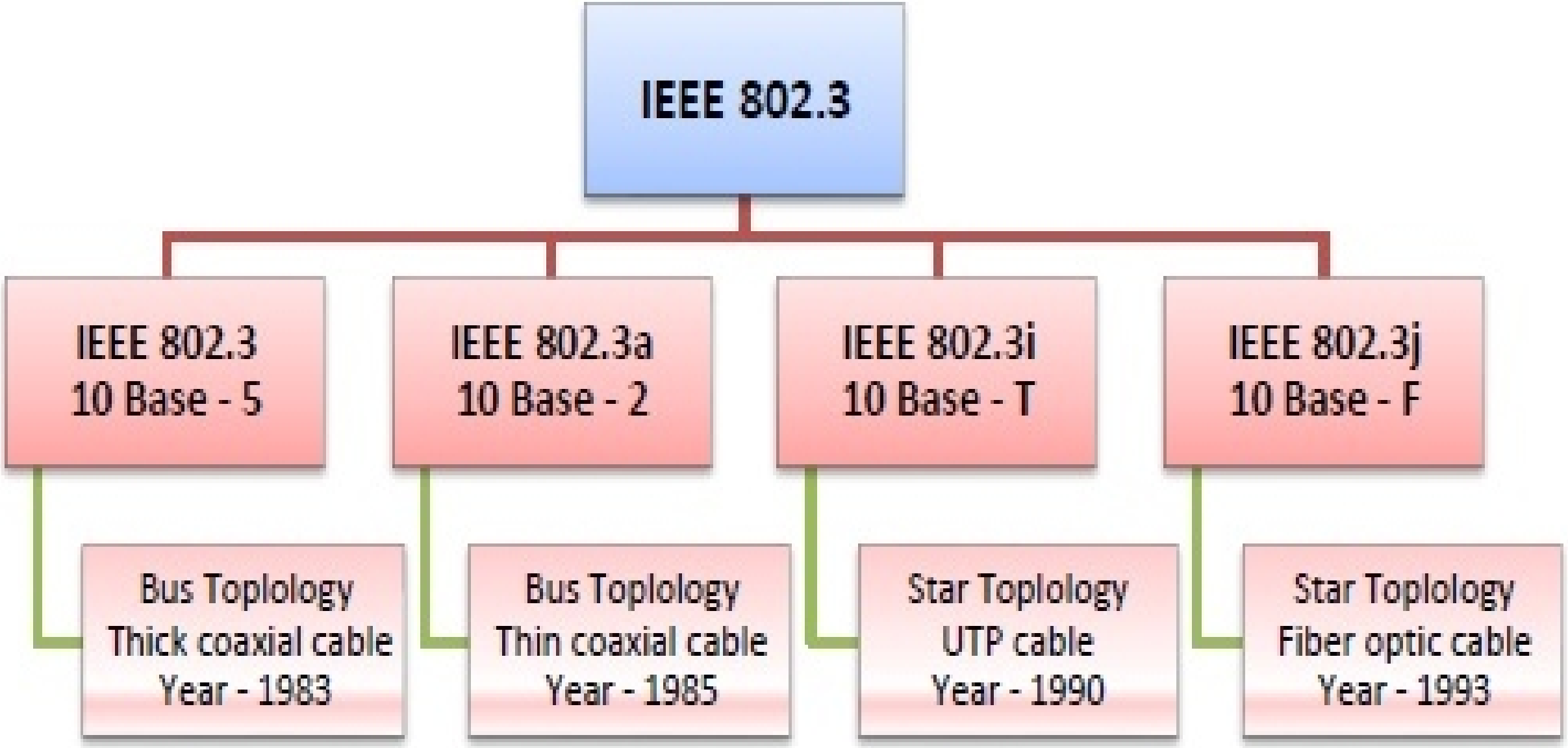


Time Division
Multiple Access

CDMA



Code Division
Multiple Access


IEEE 802.3
IEEE 802.3
10 Base - 5
IEEE 802.3a
10 Base - 2
IEEE 802.3i
10 Base - T
IEEE 802.3j
10 Base - F
Bus Toplology
Thick coaxial cable
Year - 1983
Bus Toplology
Thin coaxial cable
Year - 1985
Star Toplology
UTP cable
Year - 1990
Star Toplology
Fiber optic cable
Year - 1993

IEEE 802.3 and Ethernet

- Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.
- Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used. Most varieties of classic Ethernet have become obsolete in present communication scenario.

IEEE 802.3 Popular Versions

- There are a number of versions of IEEE 802.3 protocol. The most popular ones are -
- **IEEE 802.3**: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.

IEEE 802.3 Popular Versions

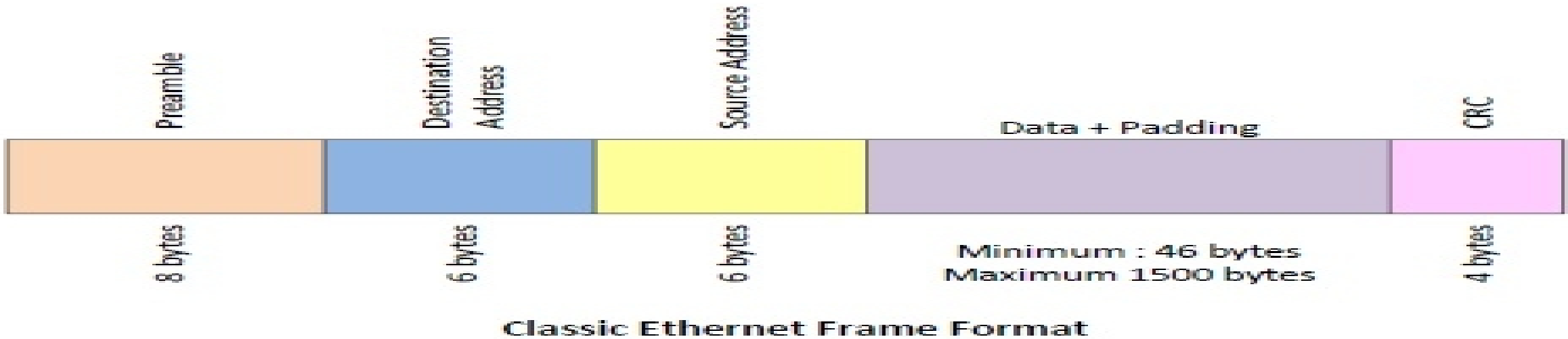
- IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- IEEE 802.3i: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.
- IEEE 802.3i: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.

Frame Format of Classic Ethernet and IEEE 802.3

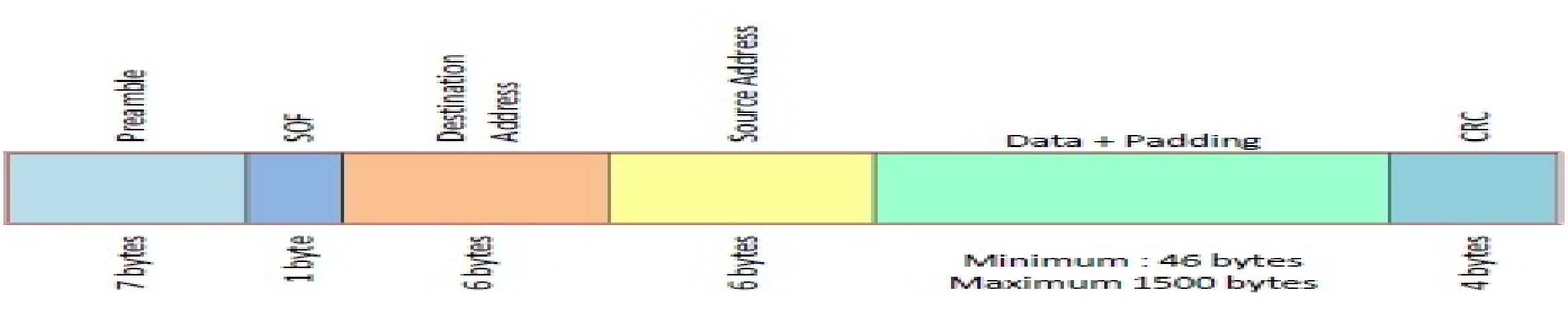
- The main fields of a frame of classic Ethernet are -
  - **Preamble**: It is the starting field that provides alert and timing pulse for transmission. In case of classic Ethernet it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
  - **Start of Frame Delimiter**: It is a 1 byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
  - **Destination Address**: It is a 6 byte field containing physical address of destination stations.
  - **Source Address**: It is a 6 byte field containing the physical address of the sending station.

Frame Format of Classic Ethernet and IEEE 802.3

- **Length**: It a 7 bytes field that stores the number of bytes in the data field.
- **Data**: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding**: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC stands for **cyclic redundancy check**. It contains the **error detection** information.



Classic Ethernet Frame Format



IEEE 802.3 Frame Format

Wireless LAN and IEEE 802.11

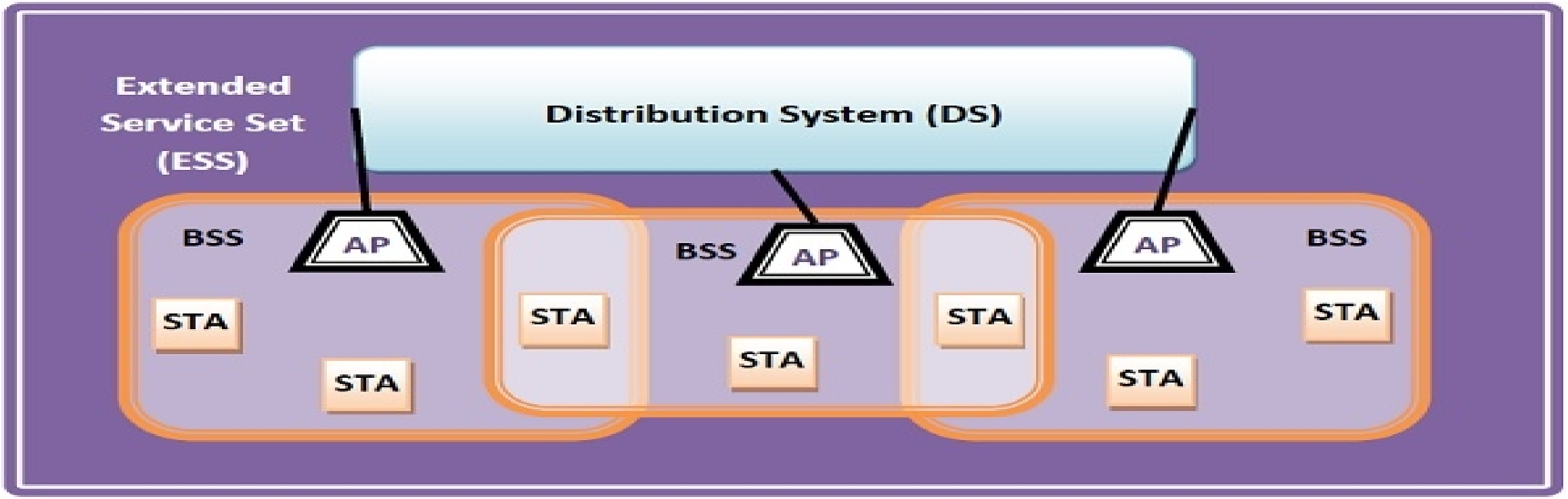
- Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (**Local Area Network**). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

Components of Wireless LANs

- **Stations (STA)** : Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types ?
  - Wireless Access Point (WAP or AP)
  - Client
- **Basic Service Set (BSS)** A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories
- Infrastructure BSS
- Independent BSS

Components of Wireless LANs

- Extended Service Set (ESS) It is a set of all connected BSS.
- Distribution System (DS) It connects access points in ESS.

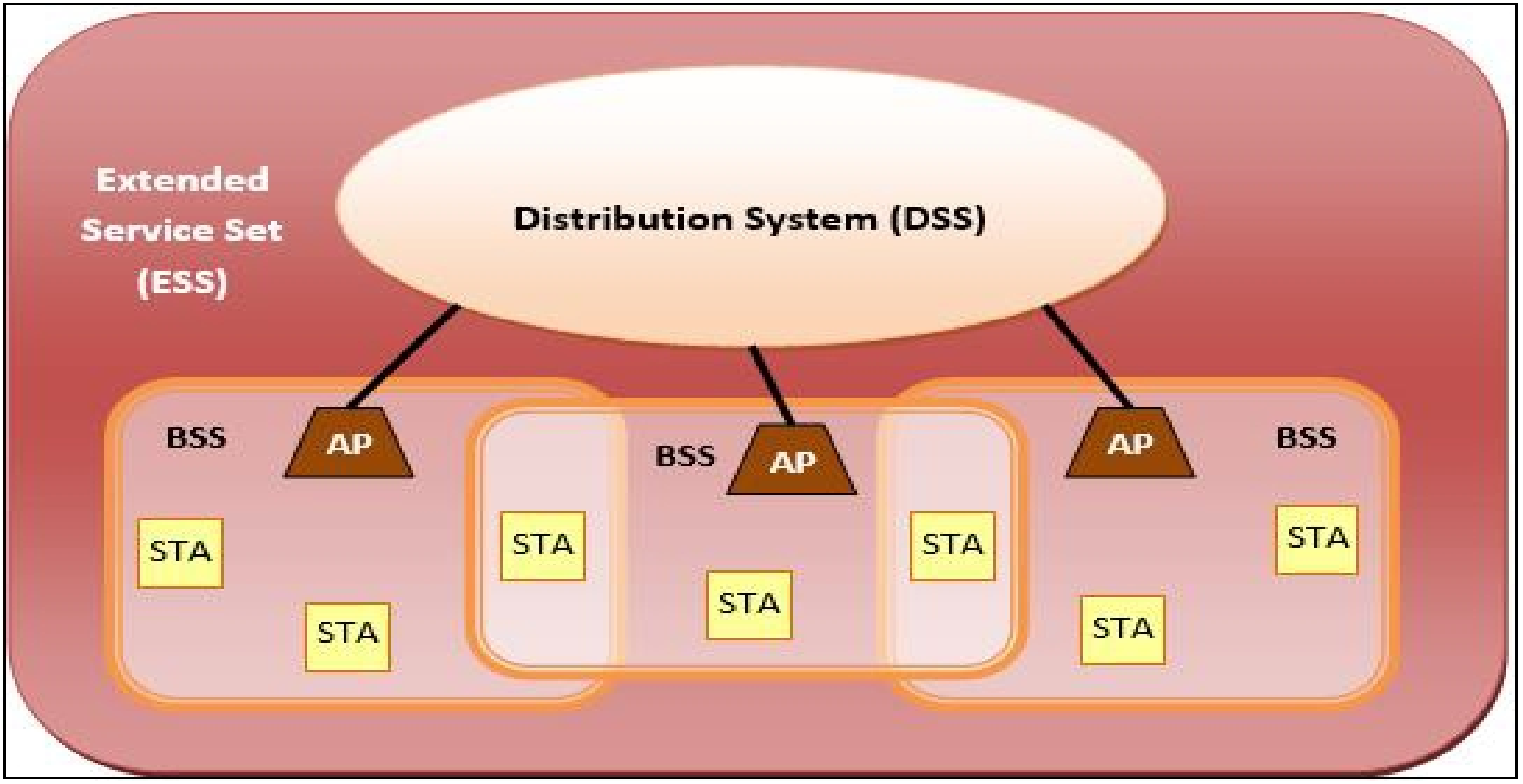


IEEE 802.11 Architecture

- The components of an IEEE 802.11 architecture are as follows
- 1) Stations (STA) – Stations comprise all devices and equipments that are connected to the wireless LAN.
- A station can be of two types:
- Wireless Access Pointz (WAP) – WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- Client. – Clients are workstations, computers, laptops, printers, smartphones, etc.

IEEE 802.11 Architecture

- Each station has a wireless network interface controller.
- **2) Basic Service Set (BSS) –**A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:
- **Infrastructure BSS –** Here, the devices communicate with other devices through access points.
- **Independent BSS –** Here, the devices communicate in peer-to-peer basis in an ad hoc manner.
- **3) Extended Service Set (ESS) –** It is a set of all connected BSS.
- **4) Distribution System (DS) –** It connects access points in ESS.


Extended
Service Set
(ESS)
Distribution System (DSS)
BSS
AP
BSS
AP
AP
BSS
STA
STA
STA
STA
STA
STA
STA