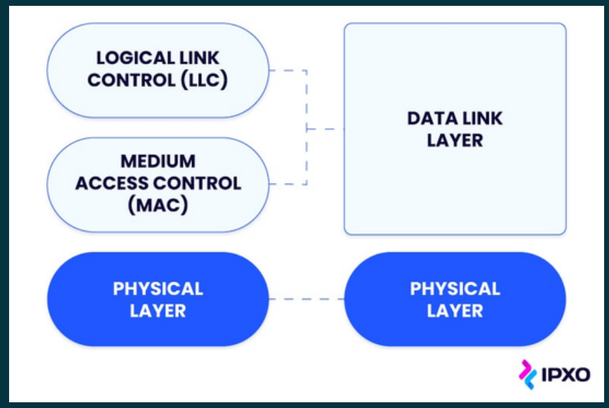
MEDIUM ACCESS SUB LAYER: MEDIUM ACCESS SUB LAYER – CHANNEL ALLOCATIONS

OVERVIEW

The Medium Access Control (MAC) sublayer is the layer 2 of the OSI (Open Systems Interconnection) model, which sits between the physical layer and the network layer. The MAC layer is responsible for controlling the access to the shared communication medium and enabling multiple devices to share the same physical transmission channel.

Its main function are to

- manage the transmission of data packets and ensure that they are sent and received without collisions or errors
- error checking
- addressing
- flow control.



Different types of channel access methods, such as FDMA, TDMA, CDMA, and CSMA/CA, can be implemented in the MAC layer to enable multiple devices to access the same communication channel.

IMPORTANCE OF EFFICIENT CHANNEL ALLOCATION IN WIRELESS NETWORKS

Maximizing Network Capacity

Efficient channel allocation techniques enable multiple devices to share the available bandwidth, maximizing network capacity and increasing the number of devices that can be supported.

mproving Quality of Service

Channel allocation can affect the Quality of Service (QoS) experienced by end-users. For example, allocating more channels to high-priority applications, such as voice and video, can improve their performance and ensure a better user experience.

Reducing Interference

Wireless networks often operate in environments where multiple devices are competing for the same channel. Efficient channel allocation can reduce the probability of collisions and interference between devices, which can lead to packet loss and degraded network performance.

Maximizing Network Capacity

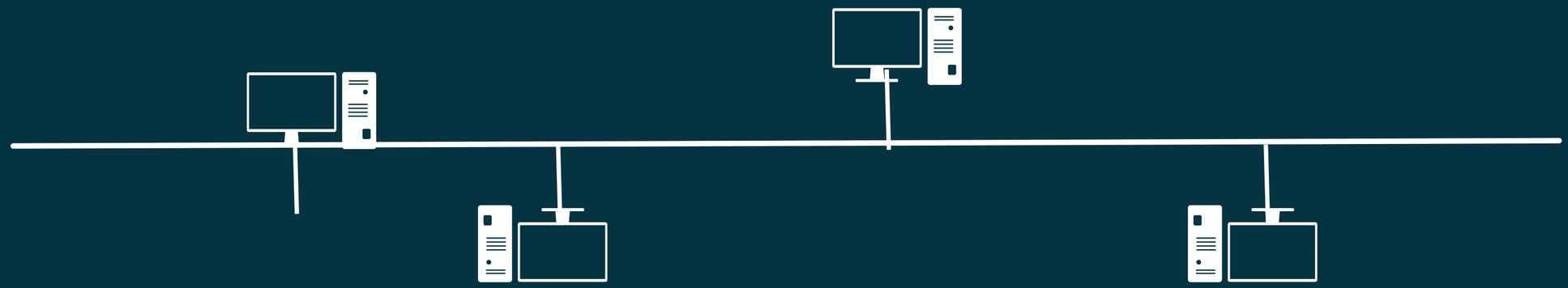
In areas with multiple wireless networks, efficient channel allocation can help avoid interference between networks and enable them to coexist without causing performance degradation.

CHANNEL ACCESS METHODS

There are several channel access methods that can be used to enable multiple devices to share the same communication medium. Here are some of the most common methods:

Frequency Division Multiple Access (FDMA)

Time Division Multiple Access (TDMA)



Code Division Multiple Access (CDMA)

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

CHANNEL ACCESS METHODS

Frequency Division Multiple Access (FDMA)

FDMA divides the available frequency band into multiple non-overlapping subcarriers, each of which is assigned to a different user. Each user is allocated a specific frequency band, and they can transmit their data simultaneously without interfering with each other.

Time Division Multiple Access (TDMA)

TDMA divides the available transmission time into discrete time slots, and each user is assigned one or more time slots to transmit their data. Multiple users can share the same frequency channel by taking turns transmitting during their assigned time slots

Code Division Multiple Access (CDMA)

CDMA uses a spread spectrum technique to allow multiple users to share the same frequency band simultaneously. Each user is assigned a unique code that spreads the signal over a wide frequency band, and the receiver uses the same code to extract the original data.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):

CSMA/CA is a random access method used in wireless networks. Each device listens to the channel before transmitting, and if the channel is busy, the device waits for a random amount of time before retrying. This method can help reduce collisions and improve network efficiency

COMPARISON OF THEIR ADVANTAGES AND DISADVANTAGES

(FDMA)

Advantages:

- Allows multiple user to transmit simultaneously without interference
- Simple to implement and suitable for low-speed applications

Disadvantages:

- Inefficient use of frequency spectrum
- Limited capacity due to the fixed allocation of frequency bands
- Susceptible to interference from other users operating in adjacent frequency bands

(TDMA)

Advantages:

- Allows multiple users to share the same channel by taking turns transmitting during assigned time slots
- Efficient use of frequency spectrum

Disadvantages:

- Requires tight synchronization between users
- Difficult to support variable-rate traffic and data-intensive applications
- Susceptible to collisions and interference if time slots are not allocated properly

(CDMA)

Advantages:

- Supports high-speed data transmissions and variable-rate traffic
- Robust against interference and jamming attack

Disadvantages:

- Complex signal processing and high power requirements
- Limited capacity due to the need for unique codes for each user
- Requires strict power control to prevent near-far problem

(CSMA/CA)

Advantages:

- Simple and easy to implement
- Efficient use of network resources by avoiding collisions
- Suitable for low-to-medium traffic applications

Disadvantages:

- Limited scalability and capacity
- Susceptible to hidden node and exposed node problems
- Increases the overhead due to the requirement for acknowledgments

WHAT ARE EACH OF THEM

FDMA

It is a channel access method that divides the available frequency band into multiple non-overlapping subcarriers, each of which is assigned to a different user. the frequency band is divided into multiple subcarriers, and each subcarrier is assigned to a different user. The bandwidth is typically narrow enough to ensure that the signal from one user does not interfere with the signal from another user. FDMA is commonly used in analog radio systems. FDMA is also used in some satellite communication systems

TDMA

It is a channel access method that divides the available time slots of a transmission channel into multiple time intervals, each of which is assigned to a different user. Each user is allocated a specific time slot, and they can transmit their data during their assigned time slot without interfering with other users.
TDMA is commonly used in digital cellular phone networks, where the available transmission channel is divided into multiple time slots, each of which is assigned to a different user

WHAT ARE EACH OF THEM

CDMA

It is a channel access method that allows multiple users to share the same frequency band simultaneously by using unique codes to differentiate between the transmitted signals. Each user is assigned a unique code used to modulate their data signal, and the receiver can use the same code to demodulate signal and extract the original data.
is commonly used in digital cellular phone networks, such as 3G and 4G networks, where multiple users share the same frequency band. Each user is assigned a unique code

CSMA/CA

It iis a channel access method used in wireless networks, where multiple users share the same communication medium. In CSMA/CA, before transmitting data, each user listens to the medium to check whether it is idle. If the medium is busy, the user waits until it becomes idle before transmitting. Once the user starts transmitting, it monitors the medium to ensure that there is no collision with other transmissions. If a collision is detected, the user stops transmitting and retries after a random backoff period.

DYNAMIC CHANNEL ALLOCATION

is a channel access method that dynamically assigns available channels to users based on their current demand. DCA allows the system to allocate available channels to users efficiently, maximizing the utilization of the communication medium. DCA is commonly used in cellular phone networks.
Advantages of DCA include efficient channel utilization, flexibility in adapting to changes in user demand, and the ability to provide high-quality service to each user.

Disadvantages of DCA include the need for additional hardware and software to monitor the traffic load and allocate channels dynamically. DCA can also introduce additional latency into the system as users are moved between channels. Additionally, DCA may not be suitable for real-time applications, such as voice and video, where a continuous stream of data needs to be transmitted.

OVERVIEW

In summary, we discussed the importance of efficient channel allocation in wireless networks and how different channel access methods can be used to allocate channels to users. We explained four primary channel access methods: FDMA, TDMA, CDMA, and CSMA/CA, and compared their advantages and disadvantages.

We also explained DCA, a dynamic channel allocation method used in cellular phone networks and some wireless LANs and ad-hoc networks. We discussed its advantages and disadvantages.

Choosing the right channel access method is crucial to ensure that the wireless network operates efficiently and effectively.

Future developments in channel allocation techniques are focused on improving the performance and efficiency of wireless networks. This includes developing new channel access methods that can handle a larger number of users, improve data rates, and reduce interference.
Some emerging technologies, such as cognitive radio, aim to improve channel allocation by dynamically sensing the available channels and selecting the best one based on the current demand.

COMPUTER NETWORKS

LAN PROTCOLS

COMPUTER NETWORK

- A computer network is a group of interconnected devices, such as computers, servers, etc, that can share resources and exchange information.
- Computer networks are essential for modern communication and collaboration across different locations and devices.
- Computer networks can be categorized based on their size and scope:
  - LAN
  - WAN
  - MAN

80%

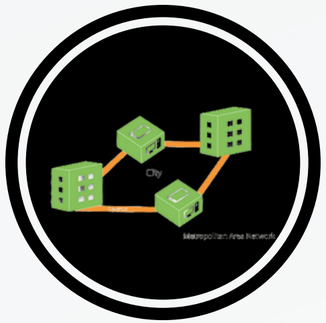
TYPES OF NETWORK

LAN

LAN is a network that connects devices within a small geographical area, commonly used for resource sharing and communication among devices within an organization.

MAN

MAN is a network that covers a larger geographical area than a LAN, typically used to connect LANs within a city or region and can be used to provide connectivity to remote offices or facilities.



WAN

WAN is a network that covers a large geographical area, typically spanning multiple cities or even countries. WANs are used to connect devices and networks that are located far apart

LOCAL AREA NETWORK (LAN)

- A Local Area Network (LAN) is a computer network that connects devices in a small geographic area, such as an office building, school, or home.

Properties of LAN:

- Geographical Scope: small geographical scope, typically limited to a single building or campus.
- Ownership: owned and managed by a single organization
- Data Transfer Rates: high data transfer rates
- Connectivity: can be connected using wired or wireless connections
- Resource Sharing: enable devices to share resources which can reduce costs and increase efficiency
- Security: secured using a variety of measures, such as firewalls, access controls, and encryption

LAN PROTOCOL

- A LAN protocol is a set of rules and standards that govern how devices communicate and exchange data within a LAN.
- LAN protocols specify how data is transmitted, received, and managed on the network, and define the format, timing, and error control mechanisms used in the communication process.
- There are several protocols that are commonly used in LANs, some are as follows:
  - Ethernet Protocol
  - Token Ring Protocol
  - WIFI Protocol
  - FDDI Protocol

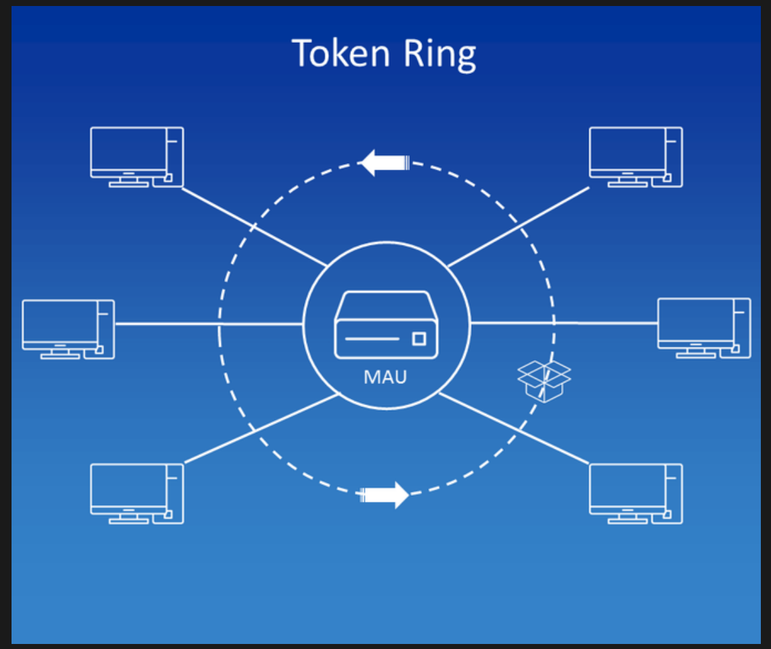
ETHERNET PROTOCOL

- Ethernet is a widely used LAN protocol that defines the standards for the physical and data link layers of communication in a LAN.
- It was developed by Xerox Corporation in the 1970s and later standardized by IEEE.

- It uses a CSMA/CD technique to manage data transmission on the network.
- It is available in different flavors and operate at various speeds by using different types of media.

- Ethernet at the physical layer uses signals, bitstreams that move on the media.
- It divides Data Link layer functions into two sublayers, Logical Link Control sublayer & the Media Access Control sublayer.

TOKEN RING PROTOCOL

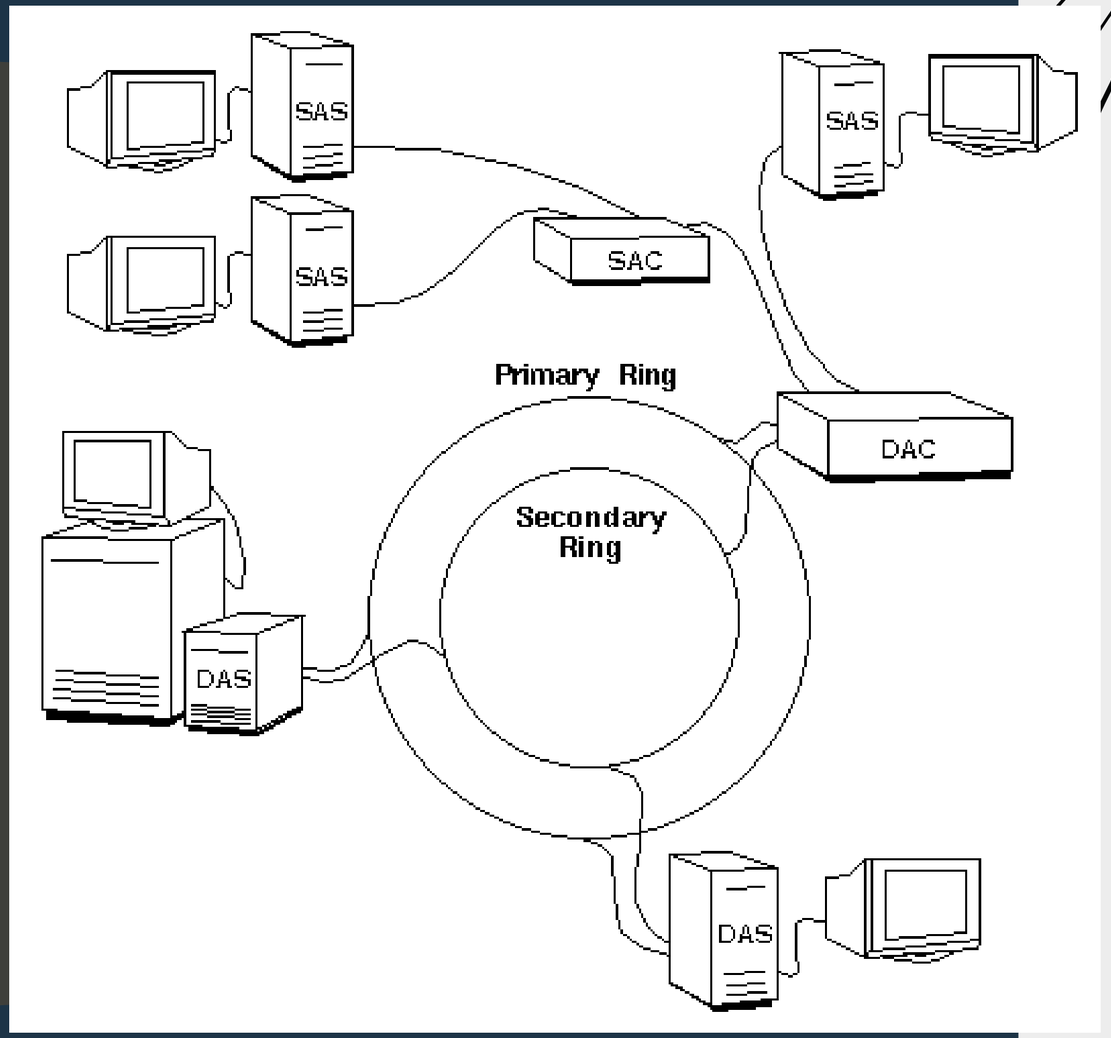


- Token Ring is a LAN protocol that was developed in the 1980s by IBM as an alternative to Ethernet.
- It defines the standards for the physical and data link layers of communication in a LAN.
- It uses a token passing mechanism to manage data transmission on the network.
- It supports data transfer rates of up to 16 Mbps and uses twisted pair copper cables to connect devices on the network.
- Token Ring was widely used in the 1980s and 1990s, but has since been largely replaced by Ethernet as the dominant LAN protocol.

WIFI PROTOCOL

- Wi-Fi (Wireless Fidelity), is a wireless networking protocol that allows devices to connect to a LAN without the need for cables.
- It is based on the IEEE 802.11 family of standards, which define the specifications for wireless LANs.
- It uses radio waves to transmit data between devices on the network.
- Devices that support Wi-Fi have a Wi-Fi adapter, which converts data into radio waves and transmits it to other devices on the network.
- The most common Wi-Fi standards used today are 802.11n, 802.11ac, and 802.11ax.

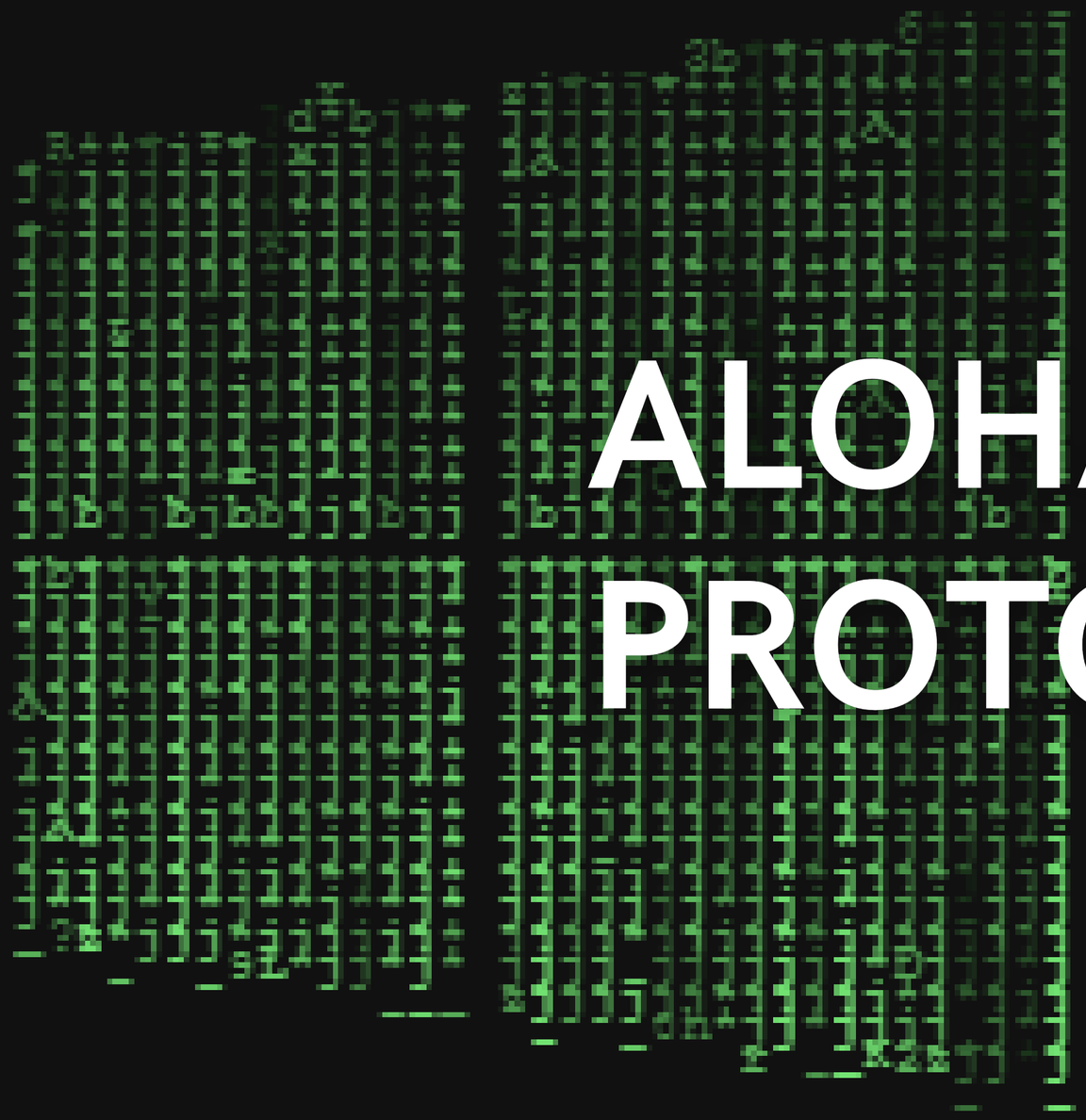
fddi protocol



- FDDI (Fiber Distributed Data Interface), is a high-speed LAN protocol that uses optical fiber cables to connect devices on the network.
- It was developed in the 1980s by ANSI as an alternative to Ethernet.
- It supports hig data transfer rates.
- It uses a dual ring topology, with two fiber optic rings that provide redundancy and fault tolerance.
- FDDI also uses a token passing mechanism, similar to Token Ring, to manage data transmission on the network.
- FDDI is designed for high-speed, high-bandwidth applications and high-performance computing environments.
- It is less common than Ethernet and other LAN protocols

REFERENCES

- https://www.techwalla.com/articles/wanlan-protocols
- https://www.eecs.yorku.ca/course_archive/2015-16/F/3213/CSE3213_15_LANProtocols_F2015_posted.pdf
- https://www.filibeto.org/sun/lib/networking/internetworking_technology_overview/Introduction_to_LAN_Protocols.pdf
- https://netcert.tripod.com/ccna/internetworking/lanprotocols.html
- https://www.techtarget.com/searchnetworking/definition/protocol



ALOHA PROTOCOLS

INTRODUCTION

ALOHA Protocols are a family of protocols used in communication networks for sharing a common communication channel among multiple users.

- They were first developed at the University of Hawaii in the early 1970s for the purpose of sharing a single radio channel among multiple computer terminals on the Hawaiian Islands.
- ALOHA Protocols are based on the principle of **random access**, where each user transmits data packets independently without any coordination with other users. The receiver checks for the presence of collisions and sends an acknowledgment to the sender in case of successful transmission.
- The ALOHA Protocols have been widely used in wireless and satellite communication networks, and their basic principles have been incorporated into many modern communication protocols.
- The two main types of ALOHA Protocols are Pure ALOHA and Slotted ALOHA, each with its advantages and disadvantages.

HISTORY OF ALOHA PROTOCOLS

1. ALOHA Protocols were first developed at the University of Hawaii in the early 1970s by a team of researchers led by Norman Abramson. The team was working on a project called the ALOHAnet, which was aimed at developing a communication network that could connect various computer terminals located across the Hawaiian Islands. At the time, there were no existing technologies that could be used for this purpose, so Abramson and his team had to come up with a new solution.
2. The ALOHAnet used a single radio channel to transmit data packets between the computer terminals. However, since multiple terminals could potentially transmit at the same time, there was a risk of collisions and interference, which could result in data loss and decreased efficiency. To solve this problem, Abramson and his team developed the ALOHA Protocol, which was based on the principle of random access.
3. The basic idea behind the ALOHA Protocol was that each computer terminal would transmit its data packets independently, without waiting for permission from a central control node. If there was a collision, the computer terminal would wait for a random amount of time before attempting to transmit again. The receiver would check for the presence of collisions and send an acknowledgment to the sender in case of successful transmission.

TYPES OF ALOHA PROTOCOLS

There are two main types of ALOHA Protocols: **Pure ALOHA** and **Slotted ALOHA**. These protocols differ in the way they allocate time slots for data transmission.

Pure ALOHA Protocol:

- In the Pure ALOHA Protocol, each station transmits its data packet at any time without any coordination with other stations.
- If a collision occurs, each station waits for a random amount of time before re-transmitting the packet.
- The Pure ALOHA Protocol optimizes for transmission efficiency, but it is prone to collisions and low throughput.
- Pure ALOHA is not widely used in modern networks due to its inefficiency.

Slotted ALOHA Protocol:

- In the Slotted ALOHA Protocol, the time is divided into discrete slots, and each station is assigned a specific slot for transmission.
- Stations transmit data packets only at the beginning of a slot, and a collision can occur only if two or more stations transmit in the same slot.
- If a collision occurs, the stations wait for the next slot to transmit their packets.
- The Slotted ALOHA Protocol improves efficiency and reduces collisions, but it requires more coordination and is less flexible than the Pure ALOHA Protocol.
- Slotted ALOHA is widely used in modern networks due to its efficiency and reliability.

Multiple Access ALOHA Protocol:

- The Multiple Access ALOHA Protocol is an extension of the basic ALOHA Protocols that improves efficiency and reduces collisions.
- It uses time-division multiplexing to allocate time slots to multiple stations, allowing them to transmit data packets simultaneously.
- The Multiple Access ALOHA Protocol is commonly used in satellite communication systems and wireless networks.

In summary, ALOHA Protocols have evolved over time to include various types, with Slotted ALOHA being the most widely used. Multiple Access ALOHA has also been developed to improve efficiency and reduce collisions in modern communication systems.

COMPARISON B/W PURE AND SLOTTED

Criteria	Pure ALOHA	Slotted ALOHA
Timing	Unsynchronized transmission	Synchronized transmission with fixed time slots
Efficiency	Low efficiency due to high probability of collisions	High efficiency due to reduced probability of collisions
Throughput	Low throughput due to more re-transmissions	High throughput due to fewer re-transmissions
Complexity	Simple, no coordination required	Complex, requires synchronization and allocation of time slots
Flexibility	More flexible, suitable for low traffic scenarios	Less flexible, suitable for high traffic scenarios

APPLICATION OF ALOHA PROTOCOLS

ALOHA Protocols have been widely used in various wireless communication systems for many years. Here are some common applications of ALOHA Protocols:

1. Satellite Communication:ALOHA Protocols are used in satellite communication systems to coordinate transmissions between earth stations and satellites.
2. RFID Technology:ALOHA Protocols are used in Radio Frequency Identification (RFID) technology to allow multiple RFID tags to communicate with a reader without collision.
3. Ethernet:ALOHA Protocols have been used in the Ethernet protocol to provide a mechanism for multiple computers to share a network segment.
4. Wireless Sensor Networks:ALOHA Protocols have been used in wireless sensor networks for various applications such as environmental monitoring and smart homes.
5. Cellular Networks:ALOHA Protocols have been used in cellular networks for managing voice and data transmissions between mobile devices and base stations.

The ALOHA Protocol's ability to handle multiple access in a distributed environment has made it a popular choice for many wireless communication systems.

LIMITATIONS OF ALOHA PROTOCOLS

The Aloha protocol is a simple communication protocol that allows multiple users to share a single communication channel. While the Aloha protocol has some advantages, it also has some limitations, including:

1. Low Efficiency: The Aloha protocol is not very efficient in terms of channel utilization. This is because it allows users to transmit at any time, which can result in collisions and wasted channel resources.
2. High Collision Probability: Since users can transmit at any time, there is a high probability of collisions, particularly in high traffic scenarios. This can result in a lot of retransmissions, leading to increased latency and decreased throughput.
3. No Priority Mechanism: The Aloha protocol does not have a priority mechanism, which means that all users have equal access to the channel. This can be problematic in situations where some users require higher priority access to the channel.
4. Limited Range: The Aloha protocol was designed for short-range communications, and its performance degrades as the distance between users increases. This makes it unsuitable for long-range applications.
5. Vulnerability to Interference: The Aloha protocol is vulnerable to interference from other wireless devices operating on the same frequency band. This can lead to a decrease in performance and increased error rates.

CONCLUSION

ALOHA protocols are a simple and efficient way to handle multiple users or nodes in a shared communication channel. The pure ALOHA protocol is less efficient than the slotted ALOHA protocol due to the higher probability of collisions. However, both protocols are highly scalable and suitable for a wide range of applications.

PATTERNS IN THE ENVIRONMENT

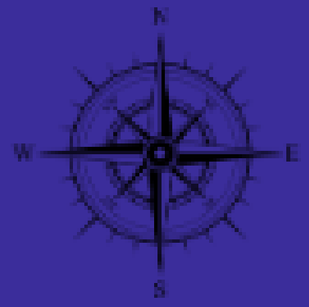
COMPUTER NETWORKS

OVERVIEW OF IEEE STANDARDS - FDDI

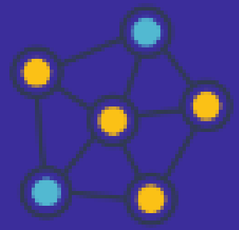
Overview of IEEE standards - FDDI

In this presentation

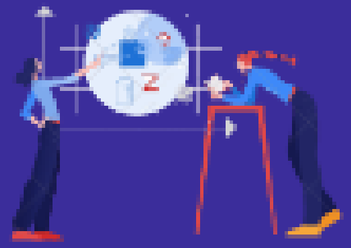
CONTENTS



About IEEE & IEEE standards



FDDI and its working



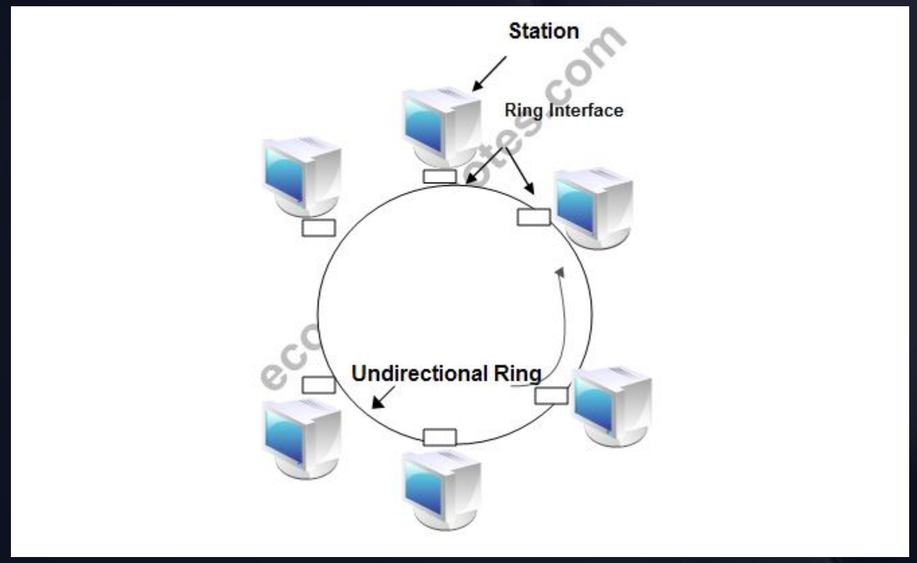
Applications of FDDI

About IEEE & IEEE standards

- IEEE stands for Institute of Electrical and Electronics Engineers. The main AIM of IEEE is to foster technological innovation and excellence for the benefit of humanity.
- The IEEE standards in computer networks ensure communication between various devices; it also helps to make sure that the network service, i.e., the Internet and its related technologies, must follow a set of guidelines and practices so that all the networking devices can communicate and work smoothly.
- The IEEE 802 is a collection of networking standards that deals with the data link layer and physical layer technologies like ethernet and wireless communications.

IEEE 802.5

Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring. A token is a special bit pattern (3 bytes long). There is only one token in the network.



Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token in order to transmit data, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. Since only one station can possess the token and transmit data at any given time, there are no collisions.

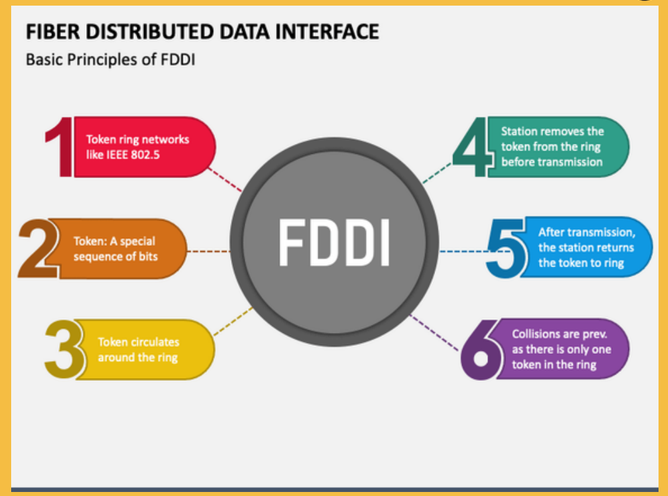
ABOUT FDDI (FIBER DISTRIBUTED DATA INTERFACE)

FDDI (Fiber Distributed Data Interface) is a network standard that uses fiber optic connections in a local area network (LAN) that can extend in range up to 200 kilometers (124 miles).

The FDDI protocol is based on IEEE standard 802.5,that is the token ring protocol

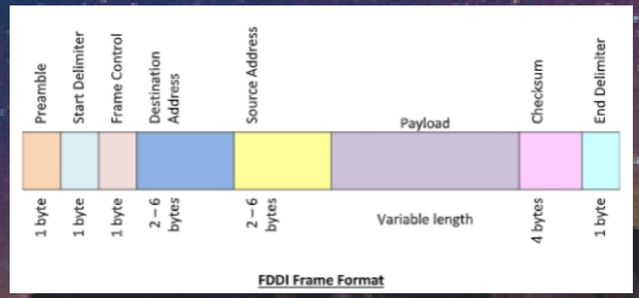
FDDI network contains two token rings: a primary ring and a secondary ring that is used as a redundant backup. The primary ring offers up to 100 megabits per second (Mbps) capacity, while the secondary ring can also be used to carry data, increasing capacity to 200 Mbps.

The single ring can extend the maximum distance of 200 km (124 miles); a dual ring can extend 100 km (62 miles). Users can connect thousands of devices to a single FDDI network.



Design & Working Of FDDI

- The FDDI network is organized into a ring topology. The fiber optic cables form a closed loop that connects all devices on the network. Data travels around the ring in one direction.
- Only the device holding the token is allowed to transmit data onto the network.
- Frame structure: Data transmitted on the FDDI network is organized into frames. Each frame contains a header(contains
- information about the frame's source and destination), data payload, and trailer(contains error checking data)



FDDI Frame Format

- To improve reliability, FDDI uses a dual-ring architecture. This means that there are two parallel rings, called the primary and secondary rings. Data travels around the primary ring in one direction, while the secondary ring is used as a backup in case the primary ring fails.

- The token circulates around the primary ring, and each device on the network checks the token as it passes by. If a device has data to transmit, it waits for the token to arrive and then seizes the token to begin transmitting.

- Token passing on the secondary ring: If the primary ring fails, the network switches to the secondary ring. A special packet, called a beacon, is transmitted on the secondary ring to indicate that the primary ring is down. The devices on the secondary ring then begin circulating the token, allowing data transmission to continue.

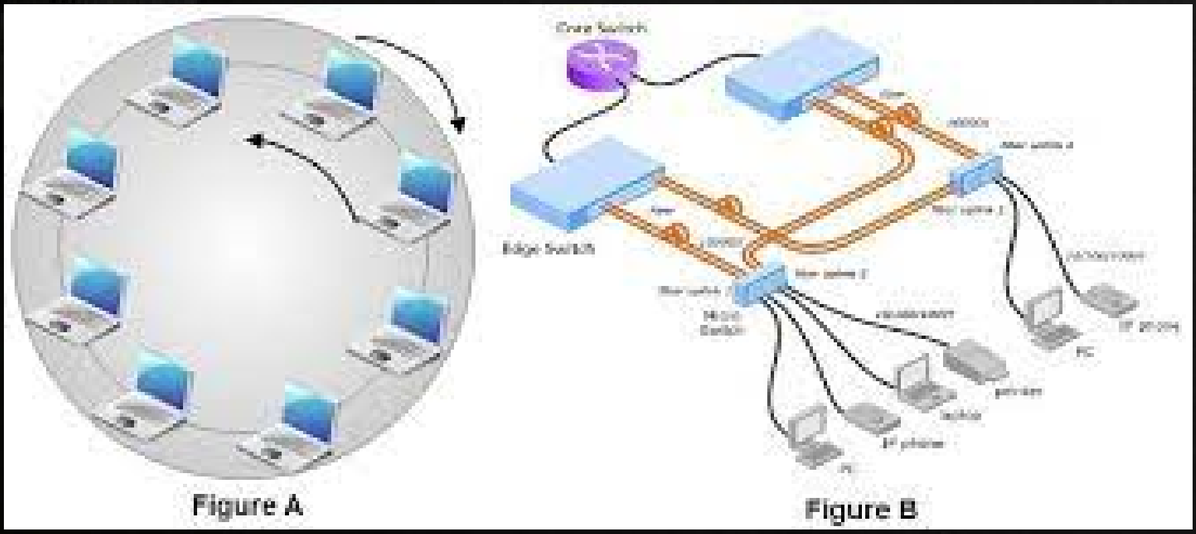


Figure A

Figure B

Figure A shows the FDDI working in token ring format whereas firgure B shows its setup in a real time network

FDDI APPLICATIONS

1. High-speed data transfer: FDDI is ideal for organizations that need to transfer large amounts of data quickly and reliably. It can be used in a variety of industries, including finance, healthcare, and manufacturing.

2. Video conferencing: FDDI's high speed and low latency make it ideal for video conferencing applications, where real-time communication is critical.

3. Industrial control systems: FDDI's reliability makes it well-suited for use in industrial control systems, where data transmission errors can have serious consequences.

4. Government networks: FDDI was originally designed for use in government networks, and it is still used in some government agencies today.

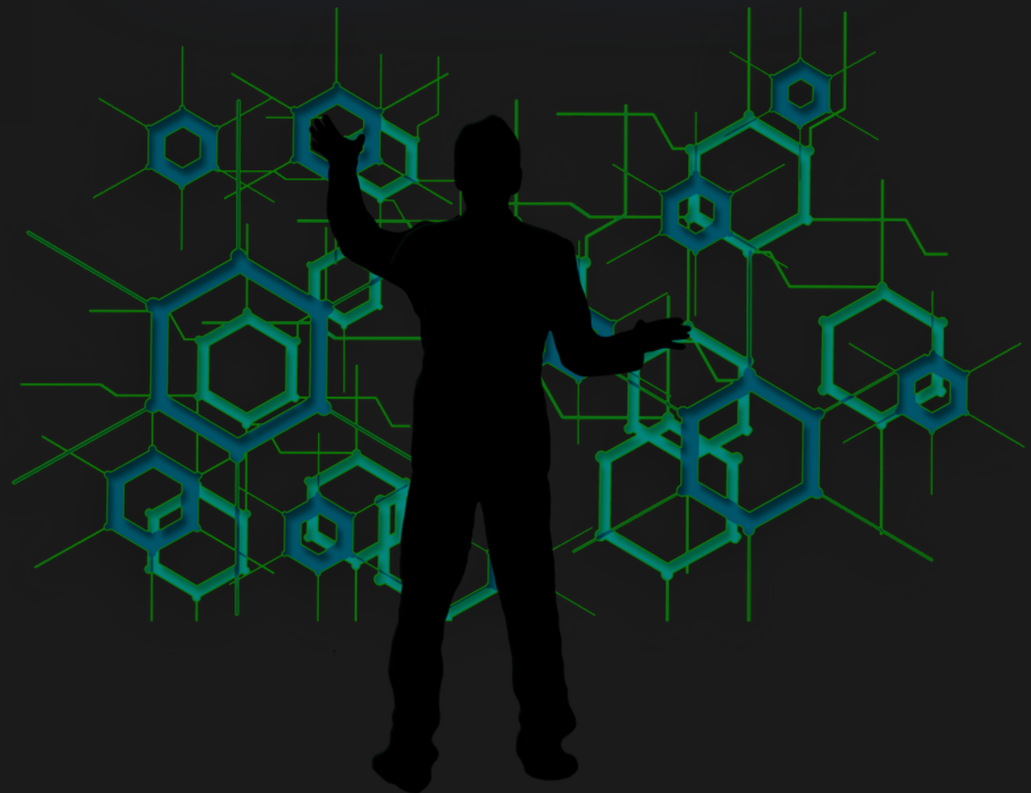
CONCLUSION

Thus , in this presentation on OVERVIEW OF IEEE STANDARDS : FDDI, we discussed about IEEE standards and the IEEE standard that is used in FDDI,IEEE 802.5.We then went on to explain FDDI,its working and its real life applications.

REFERENCES

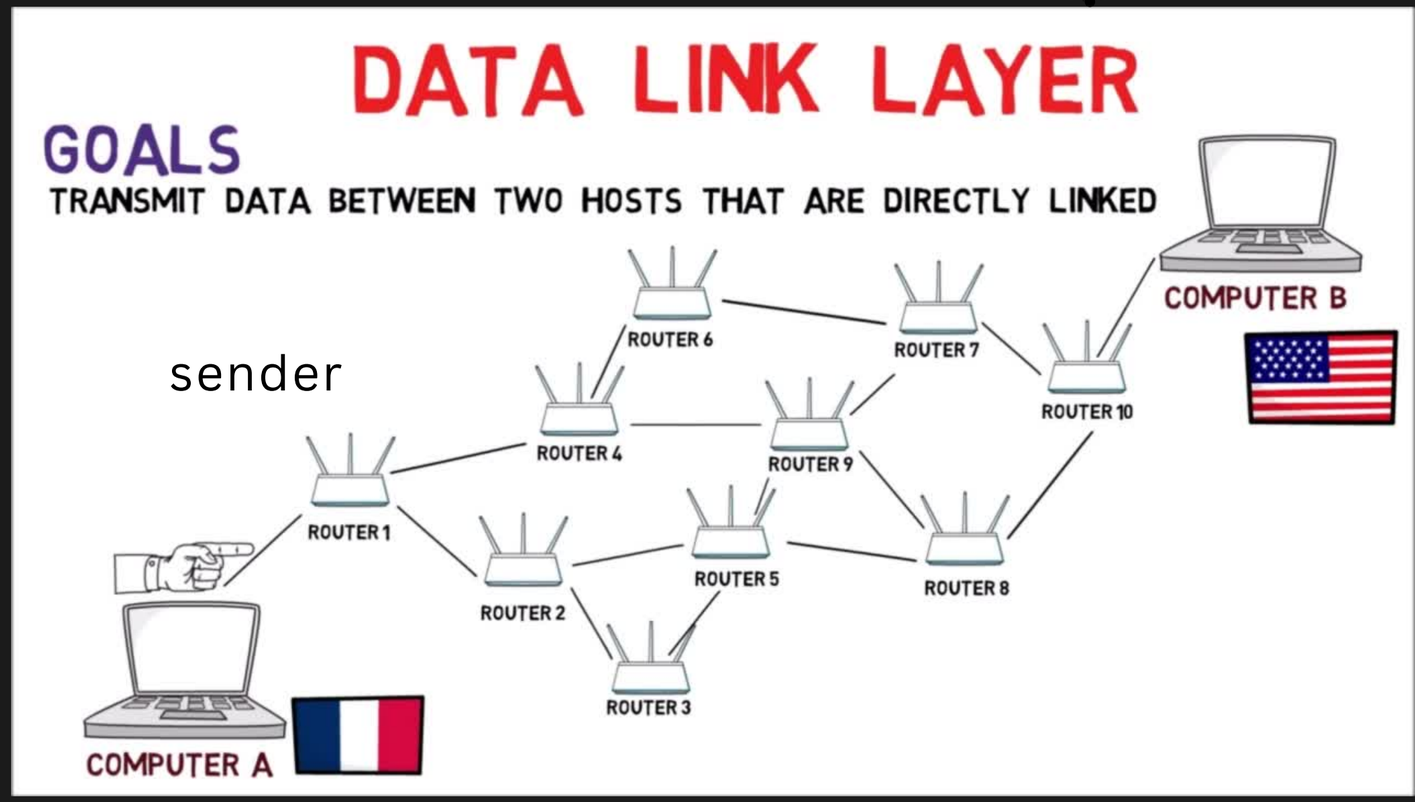
- GeeksForGeeks
- Tutorials Point
- Research Gate
- Wikipedia

DATA LINK LAYER



INTRODUCTION

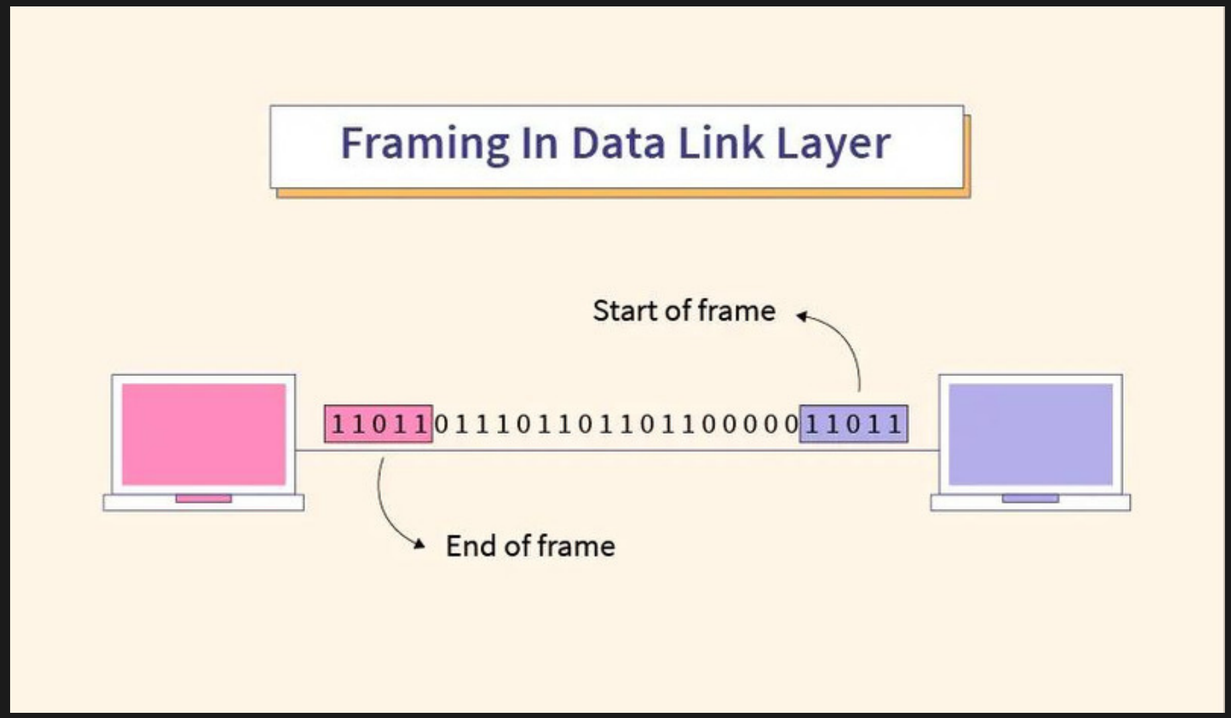
- Data Link Layer is the second layer in the OSI model.
- It provides reliable transmission of data over a physical link between two devices.
- Data Link Layer is responsible for framing, error detection and correction, flow control, and access control.



Functions of Data Link Layer

Framing

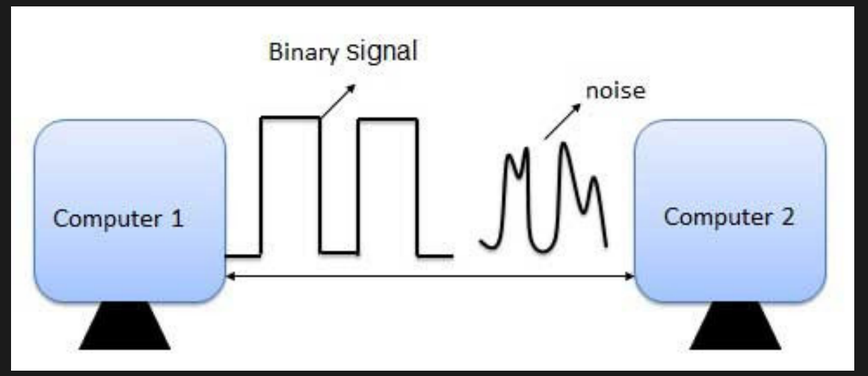
- Divides the data into frames.
- Each frame includes a header and a trailer.
- Header contains information such as source and destination addresses
- Trailer contains error detection information



Flow Control

Regulates the flow of data between two devices

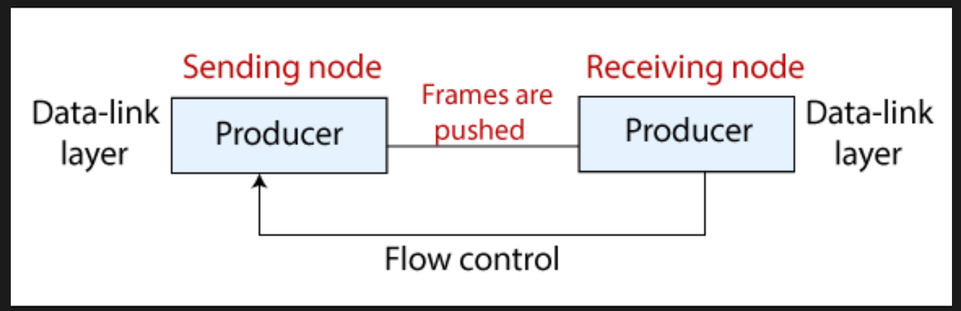
Ensures that the receiving device can handle the amount of data being sent



Access Control

Determines which device has access to the transmission medium

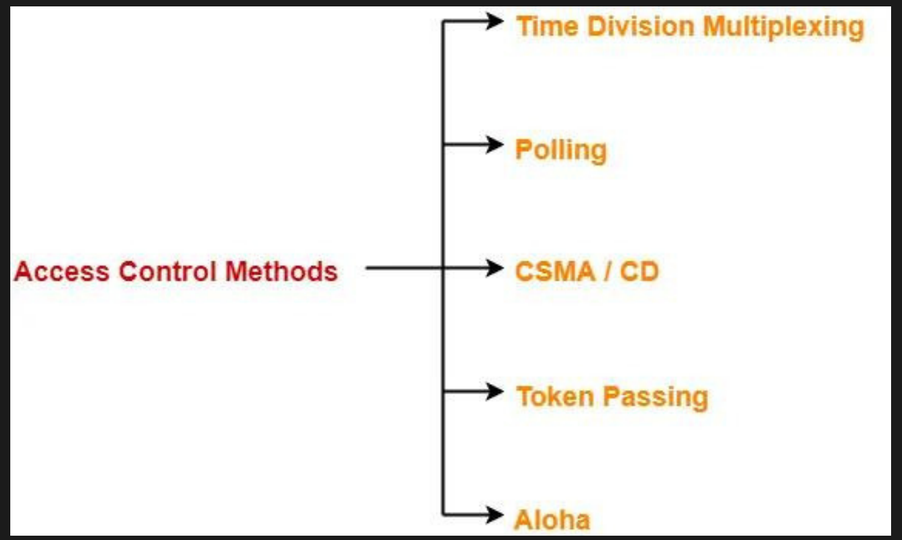
Prevents collisions between multiple devices trying to transmit at the same time



Error Detection and Correction

Detects errors during transmission using techniques such as CRC

Corrects errors using techniques such as retransmission



Flow Control in Data link layer

Protocols

Noiseless Channels

- Simplest
- Stop ans Wait

Noisyl Channels

- Stop & wait ARQ
- Go-Back-N-ARQ
- Selective repeat ARQ

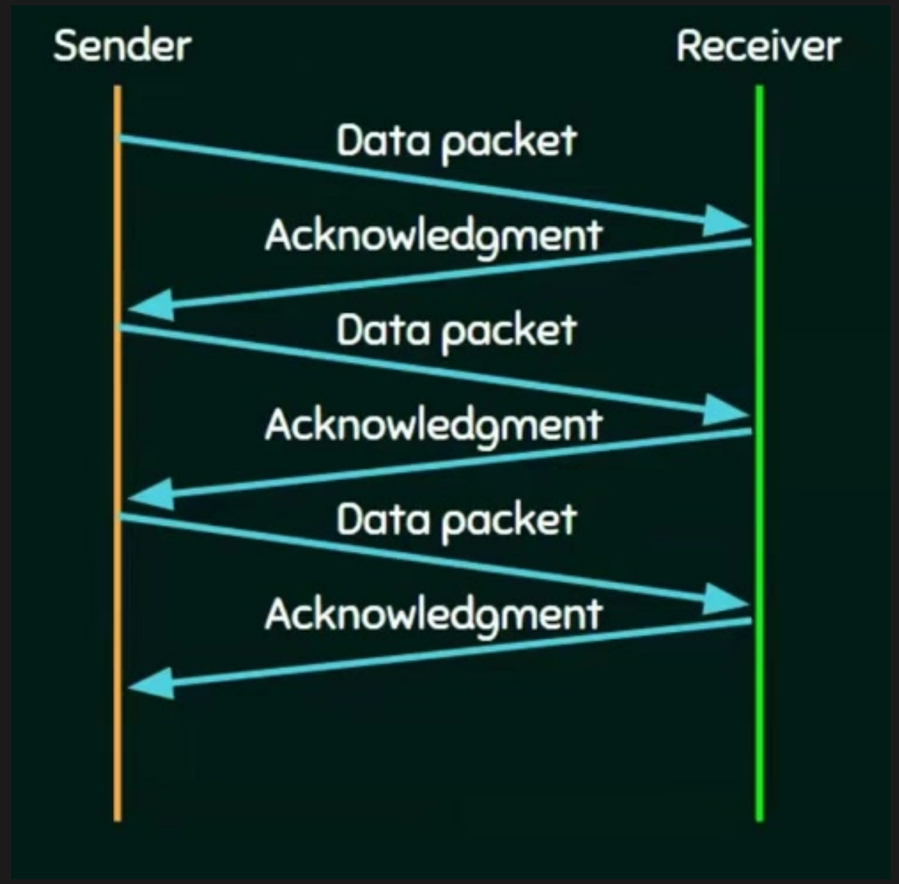
Stop and Wait

Sender:

- Send one data packet at a time.
- Send the next packet only after receiving acknowledgement for the previous.

Receiver:

- Send acknowledgement after receiving and consuming a data packet.
- After consuming packet acknowledgement need to be sent (Flow Control).



Stop and Wait ARQ

Sender:

Sender sends a data frame or packet with sequence number 0.

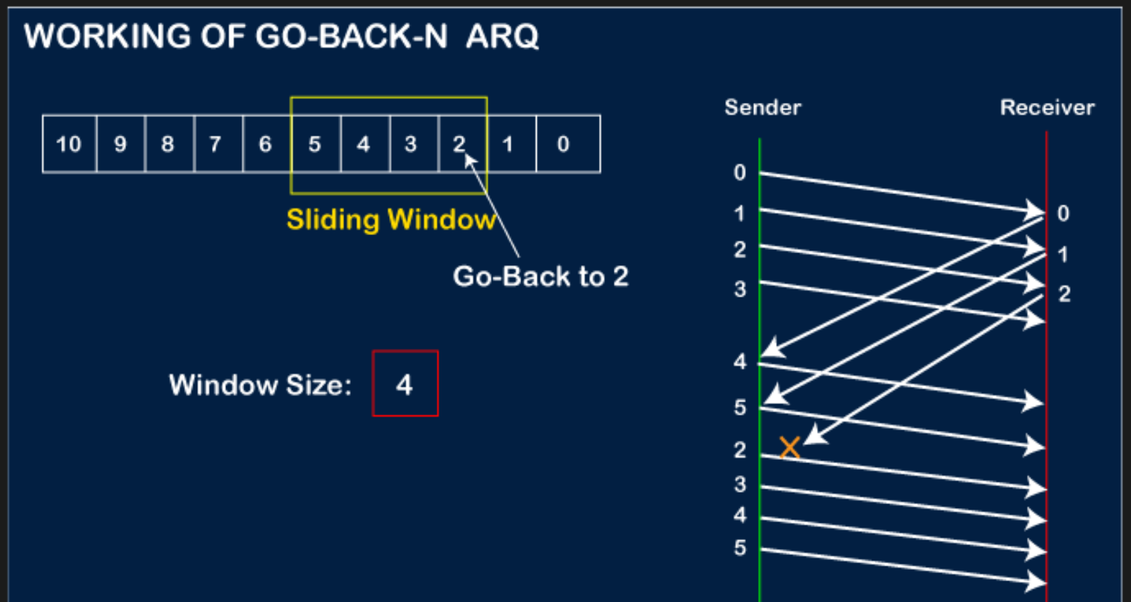
Receiver:

After receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet).

Go-back-N ARQ

- Go Back N ARQ is a sliding window protocol which is used for flow control purposes. Multiple frames present in a single window are sent together from sender to receiver.

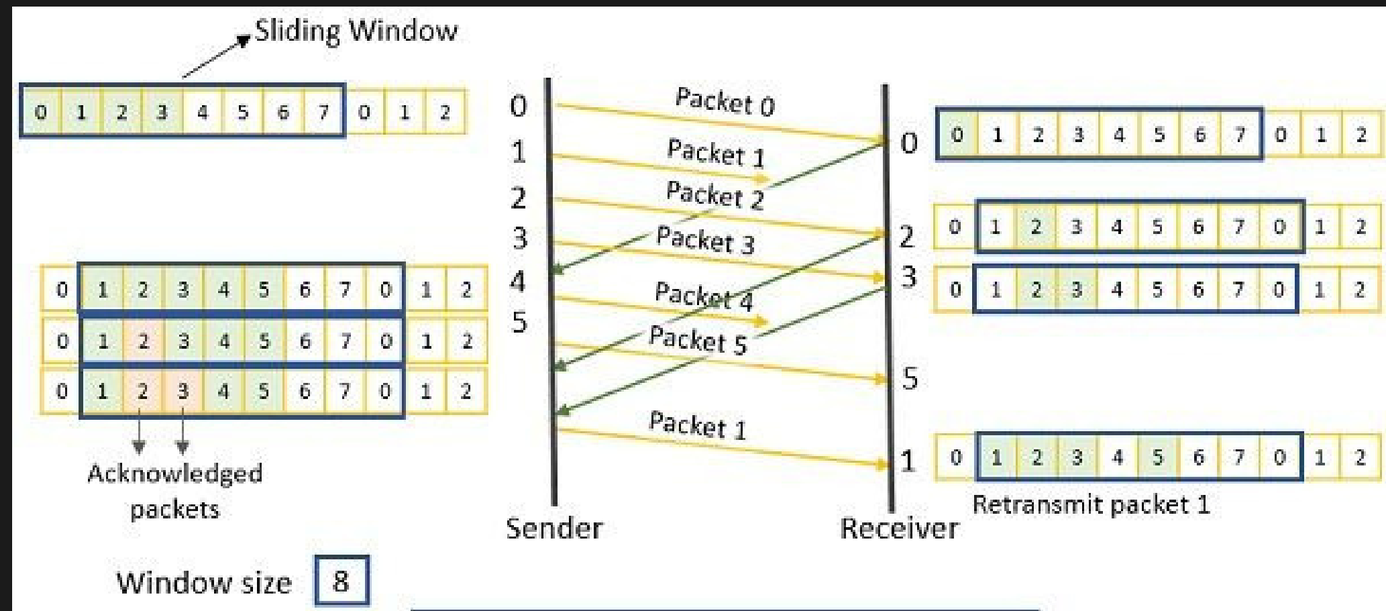
- Pipelining is allowed in the Go Back N ARQ protocol. Pipelining means sending a frame before receiving the acknowledgment for the previously sent frame.



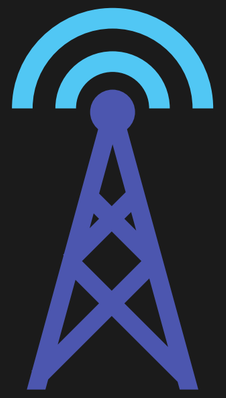
Selective Repeat ARQ

In the selective repeat, the sender sends several frames specified by a window size even without the need to wait for individual acknowledgement from the receiver as in Go-Back-N ARQ. In selective repeat protocol, the retransmitted frame is received out of sequence.

In Selective Repeat ARQ only the lost or error frames are retransmitted, whereas correct frames are received and buffered.



DATA LINK LAYER PROTOCOLS



Asynchronous Protocols

Transmits data in a byte-by-byte fashion
Uses start and stop bits to indicate the beginning and end of each byte

Synchronous Protocols

Transmits data in a continuous stream
Uses clock signals to synchronize the sending and receiving devices.

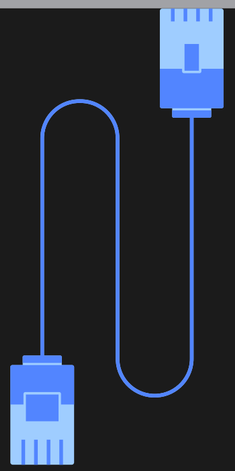
Error-Correcting Protocols

Detect and correct errors during transmission
Example: ARQ (Automatic Repeat Request).

DATA LINK LAYER STANDARDS

Ethernet

it uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
CSMA/CD helps in detecting and avoiding collisions between devices.

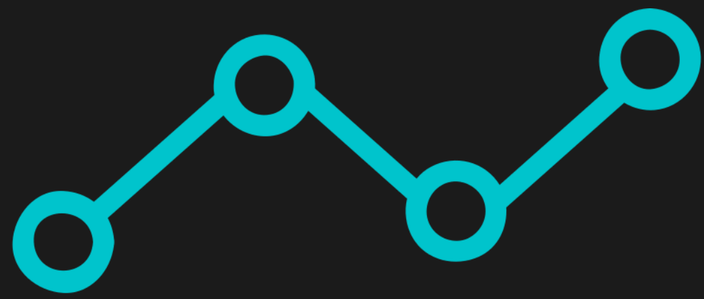


Wifi

It uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
CSMA/CA helps in avoiding collisions between devices by deferring transmission.

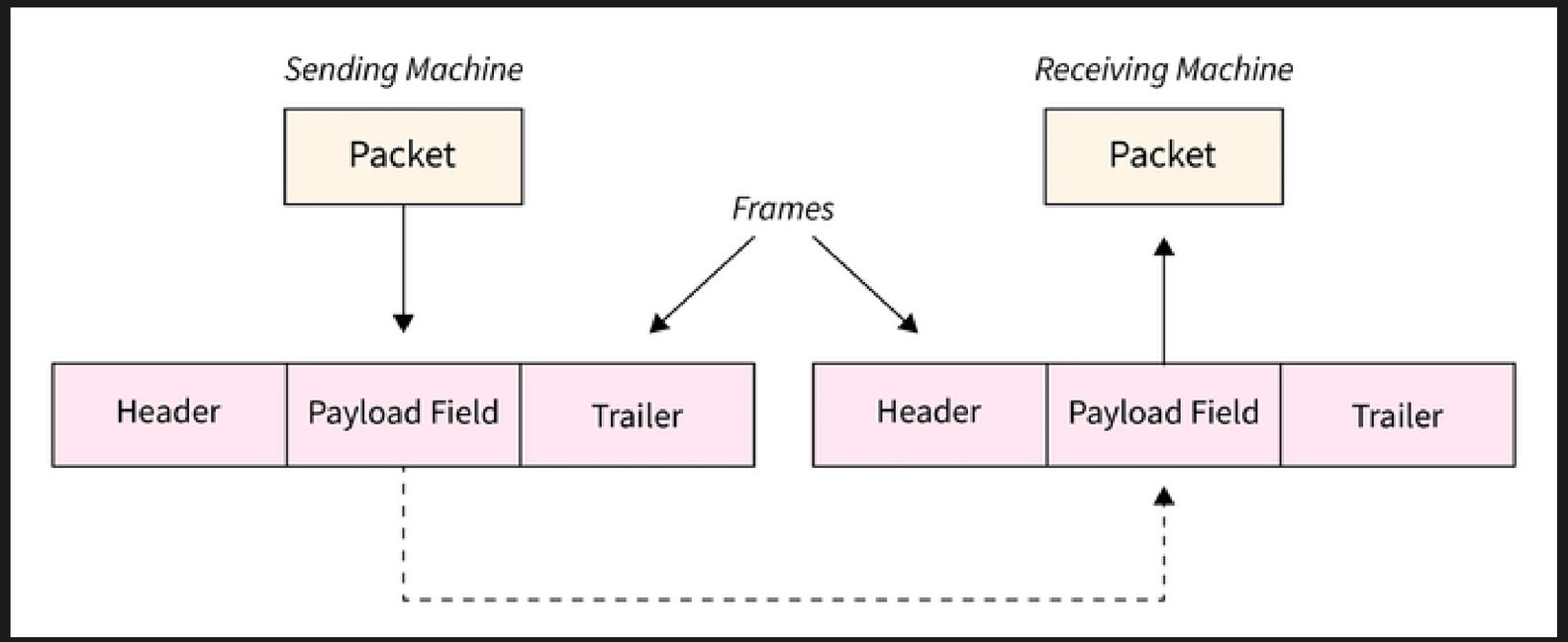
PPP

PPP is used to establish a direct connection between two devices
It provides authentication and encryption
PPP is widely used for dial-up connections and Virtual Private Networks (VPNs).



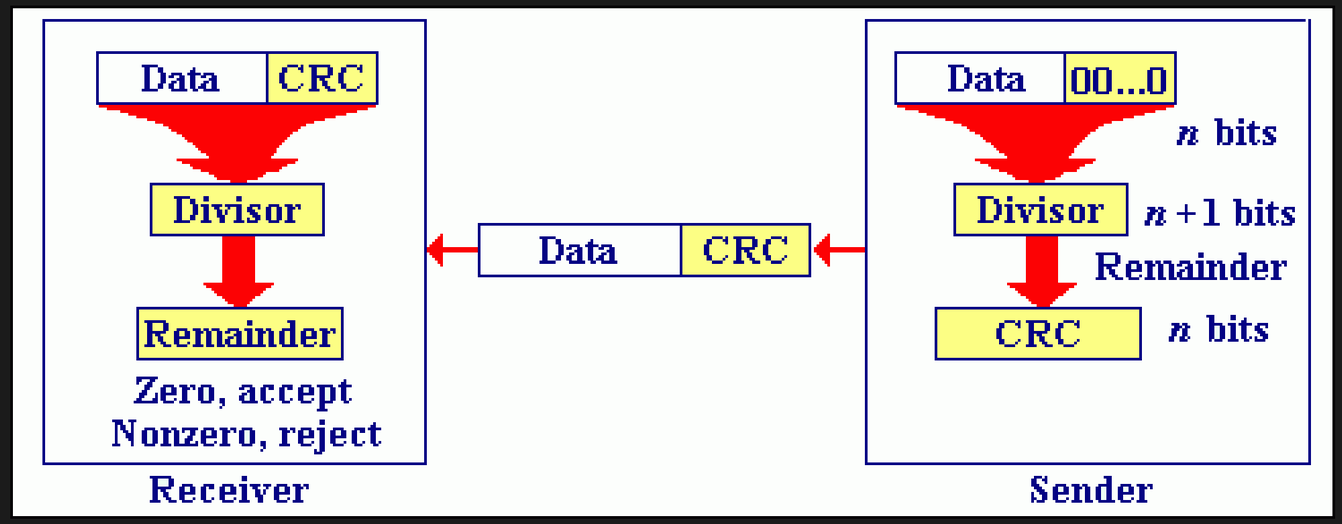
FRAMING

- Framing is the process of dividing data into frames.
- Each frame contains a header and a trailer.
- Header contains information such as source and destination addresses.
- Trailer contains error detection information.



ERROR DETECTION & CORRECTION

- Error detection is the process of detecting errors during transmission.
- Techniques such as CRC are used for error detection.

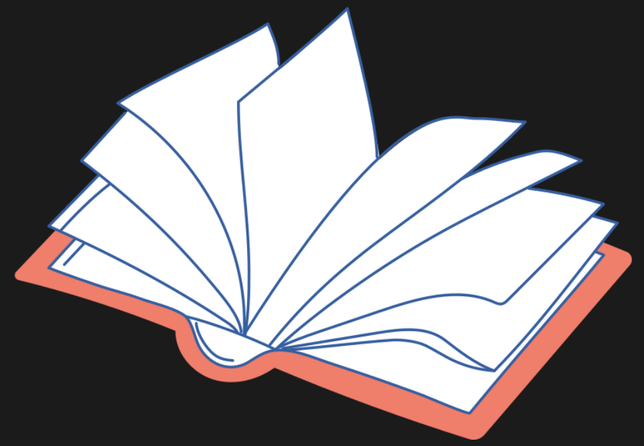


- Error correction is the process of correcting errors during transmission.
- Techniques such as retransmission are used for error correction.

CONCLUSION

- The Data Link Layer plays a critical role in ensuring reliable transmission of data over a physical link.
- It provides framing, error detection and correction, flow control, and access control.
- Various protocols such as Ethernet, Wi-Fi, and PPP are used in different types of networks.
- A well-designed Data Link Layer can significantly improve the performance and reliability of a network.

REFERENCES



- https://www.geeksforgeeks.org/data-link-layer/
- https://www.youtube.com/watchv=WfIhQ3o2xow&ab_channel=NesoAcademy
- https://www.geeksforgeeks.org/framing-in-data-link-layer
- https://www.youtube.com/watch?v=oQzueBVyAM4&list=PLBlnK6fEyqRgMCUAG0XRw78UA8qnv6jEx&index=16&ab_channel=NesoAcademy

Thank you
so much!

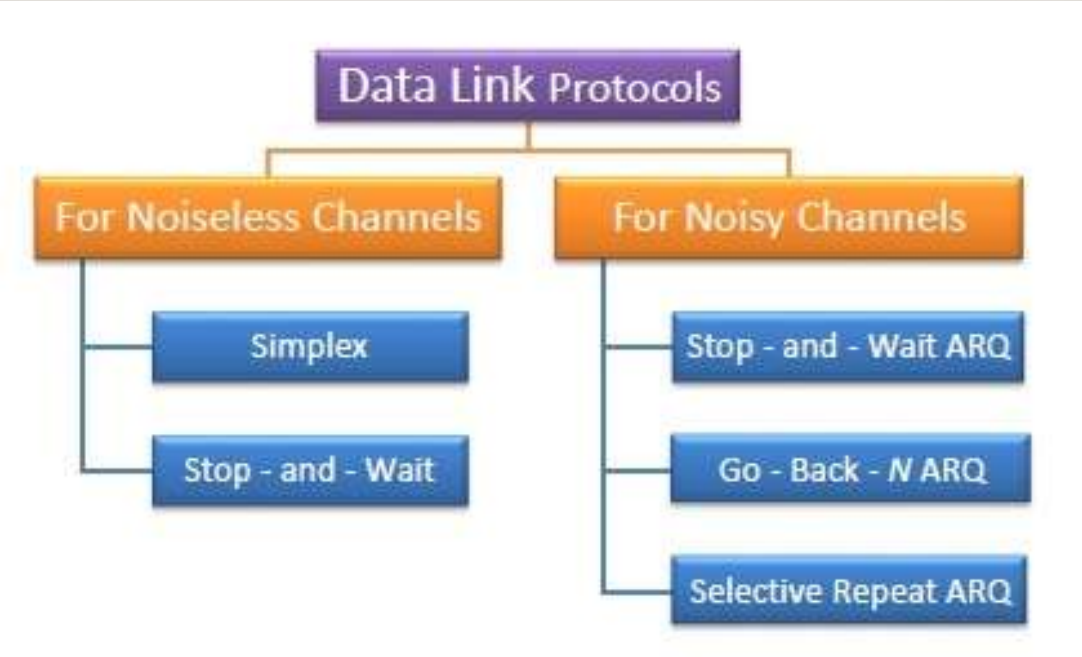
ELEMENTARY DATA LINK PROTOCOLS

INTRODUCTION

Framing, error control, and flow control are three essential tasks that the data link layer must be able to complete. Bit streams from the physical layer are split into data frames that range in size from a few hundred to a few thousand bytes during the framing process. Transmission faults and the retransmission of damaged and missing frames are dealt with via error control techniques. Flow control controls delivery speed so that a fast sender doesn't overpower a slow receiver.

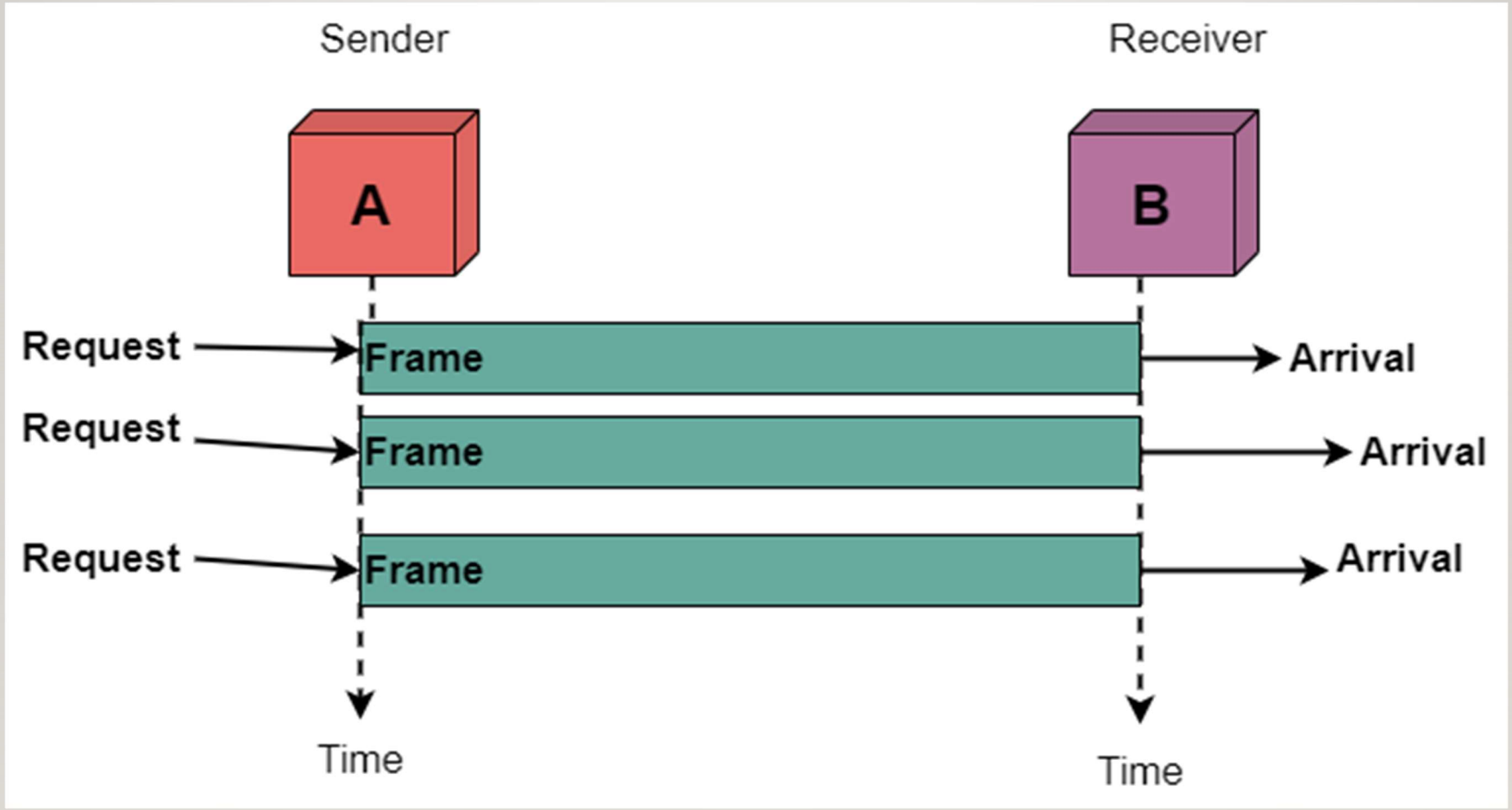
TYPES OF DATA LINK PROTOCOLS

Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



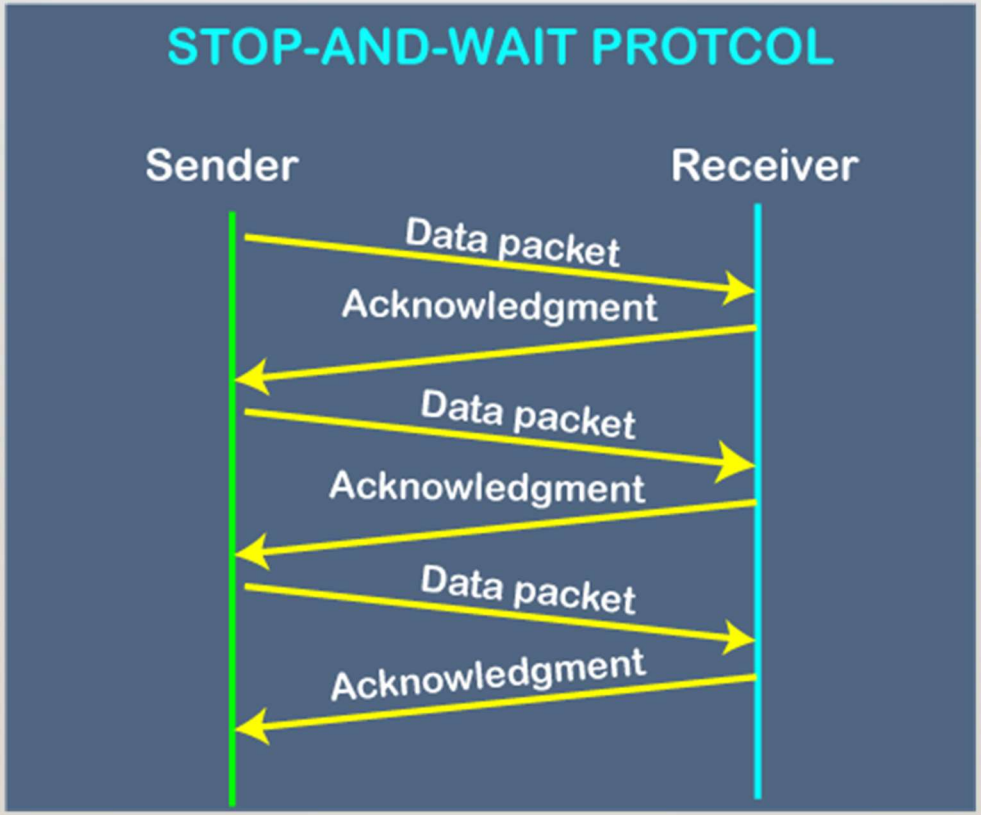
SIMPLEX PROTOCOL

A hypothetical protocol called Simplex is created for unidirectional data transmission across an ideal channel, or a channel where transmission is always successful. It has separate transmitter and receiver processes. As soon as data is accessible in its buffer, the transmitter simply sends all available data onto the channel. It is anticipated that the receiver will immediately process all incoming data. Since it doesn't deal with flow control or error control, it is purely hypothetical.


Sender
Receiver
A
B
Request
Frame
Arrival
Request
Frame
Arrival
Request
Frame
Arrival
Time
Time

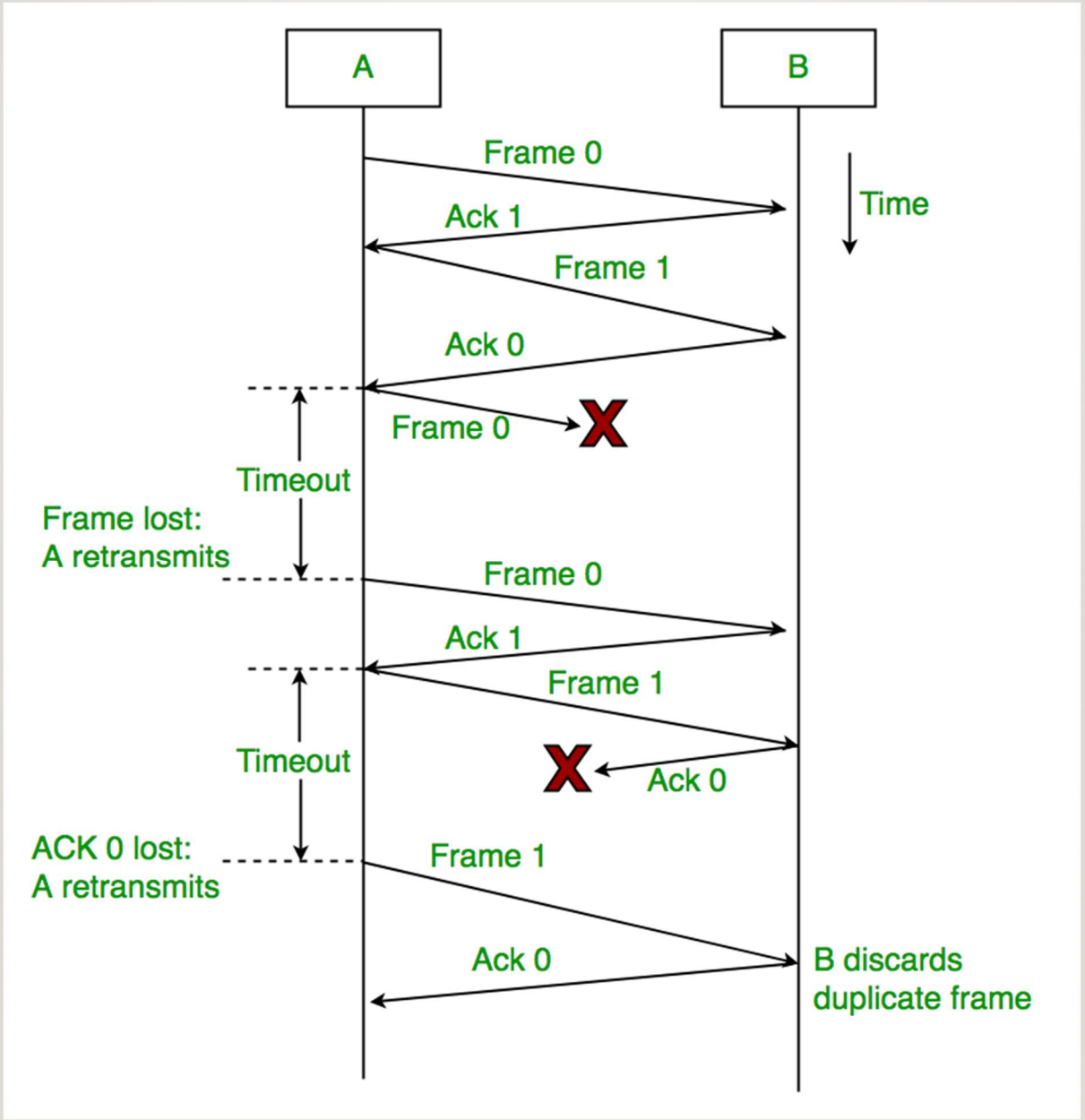
STOP – AND – WAIT PROTOCOL

The Stop-and-Wait protocol is also applicable to noiseless channels. It offers one-way data communication without any mistake correction tools. To prevent a quick transmitter from drowning a sluggish receiver, it does, however, offer flow control. The receiver's processing speed and buffer size are both finite. Only after receiving notification from the receiver that it is ready for additional data processing can the sender send a frame.


STOP-AND-WAIT PROTCOL
Sender
Receiver
Data packet
Acknowledgment
Data packet
Acknowledgment
Data packet
Acknowledgment

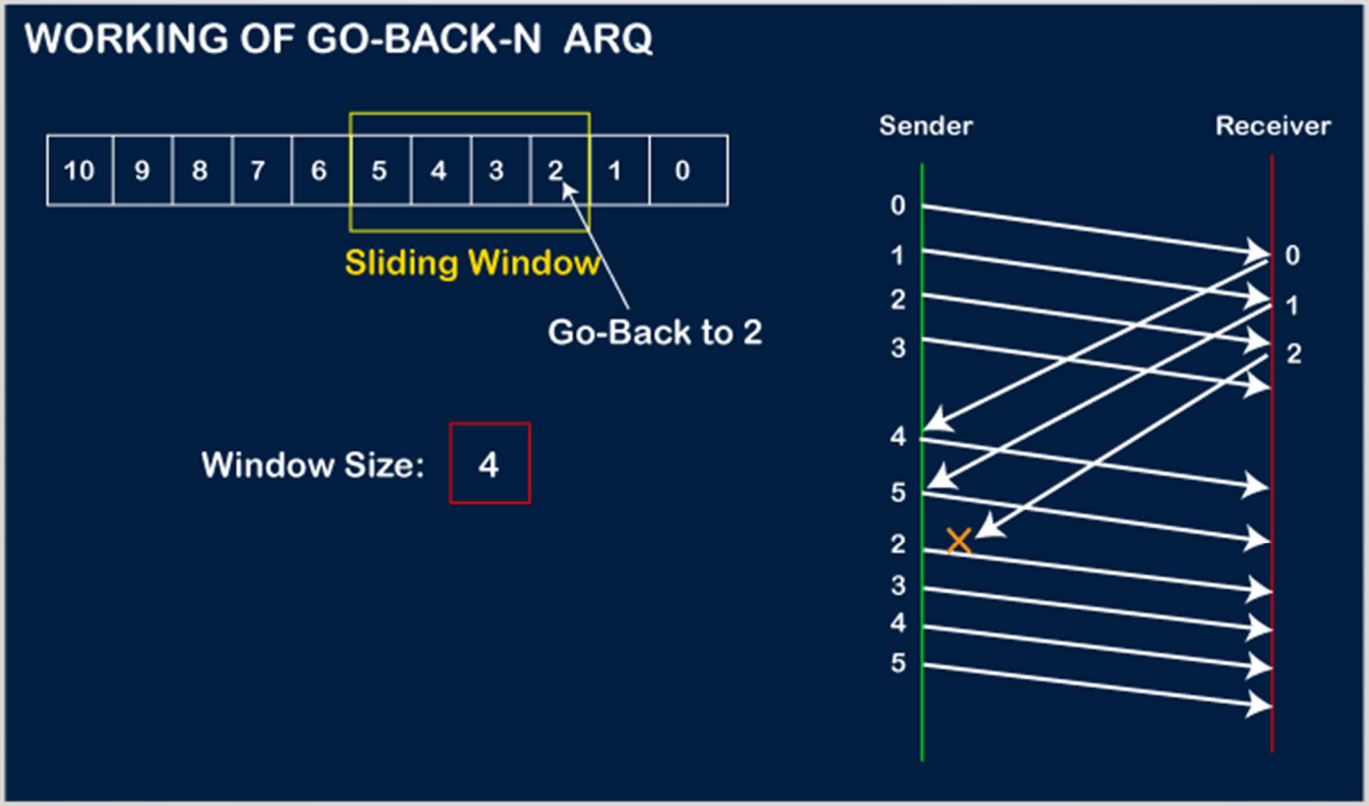
STOP – AND – WAIT ARQ

Stop –and- wait Automatic Repeat Request (Stop-and-Wait ARQ), a variant of the aforementioned protocol with additional error-control techniques, is suitable for noisy channels. A copy of the sent frame is kept by the sender. It then waits for the receiver to respond positively for a set amount of time. The frame is sent again if the timer runs out if there is no positive acknowledgment. The following frame is sent if a positive acknowledgment is received.


A
B
Frame 0
Time
Ack 1
Frame 1
Ack 0
Frame 0
X
Timeout
Frame lost:
A retransmits
Frame 0
Ack 1
Frame 1
Timeout
X
Ack 0
ACK 0 lost:
A retransmits
Frame 1
Ack 0
B discards
duplicate frame

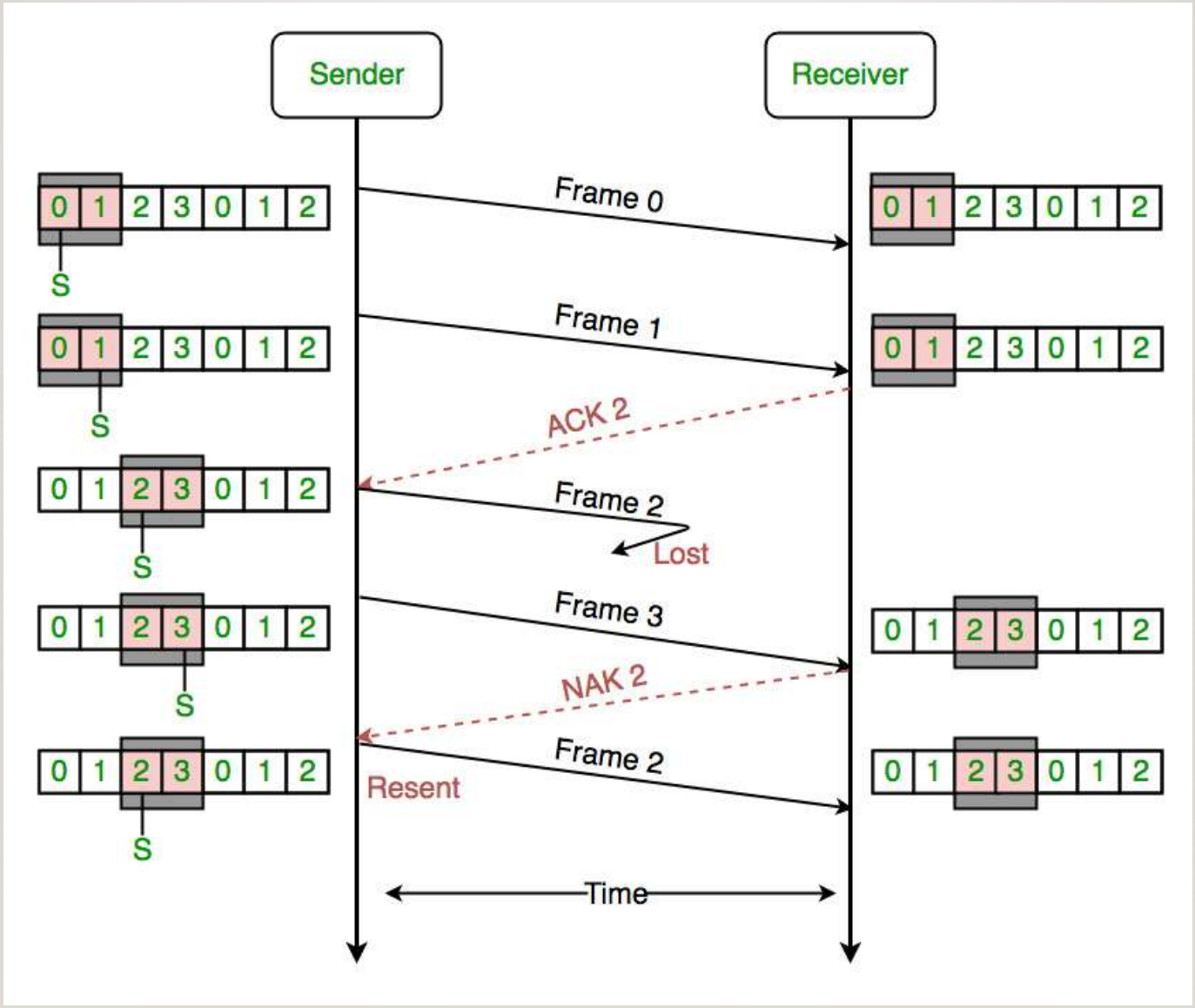
GO – BACK – N ARQ

Before getting the acknowledgement for the first frame, Go-Back-N ARQ allows for the sending of numerous frames. The phrase "sliding window protocol" refers to the idea behind it. A limited amount of frames are sent, each of which is consecutively numbered. All frames after the one that was not acknowledged are retransmitted if the acknowledgement is not received in the allotted time.


WORKING OF GO-BACK-N ARQ
10
9
8
7
6
5
4
3
2
1
0
Sliding Window
Go-Back to 2
Window Size:
4
Sender
Receiver
0
1
2
3
4
5
2
3
4
5
0
1
2

SELECTIVE REPEAT ARQ

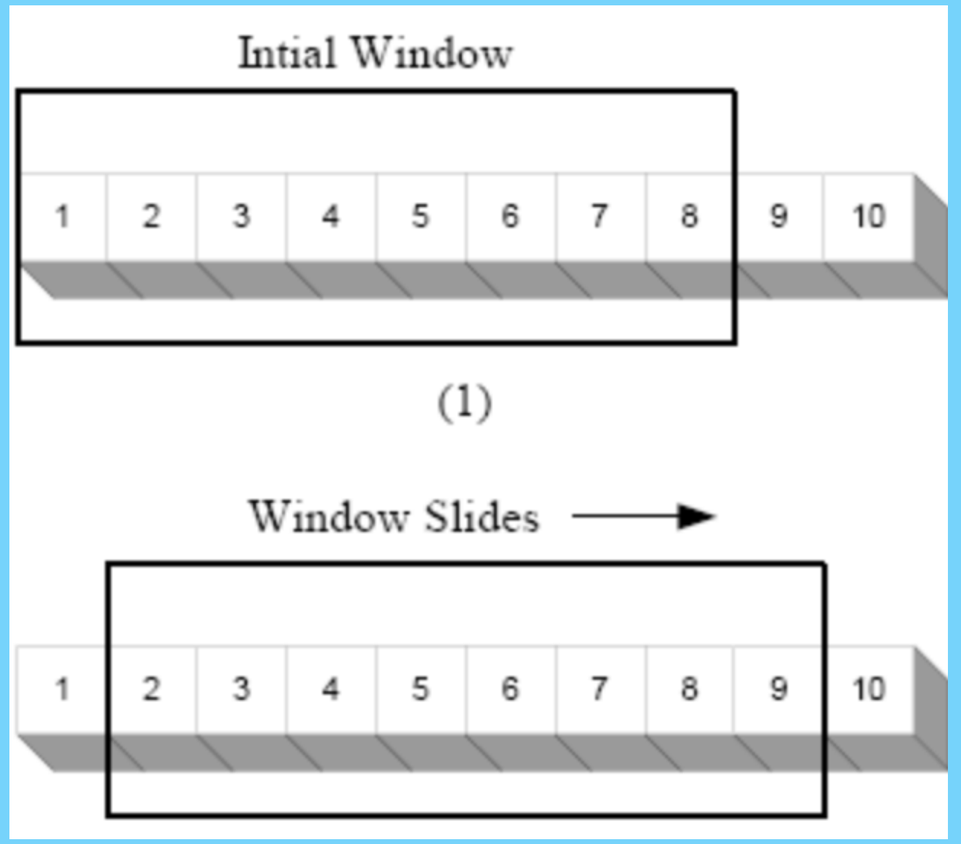
Additionally, this protocol enables transmitting additional frames before getting an acknowledgement for the initial frame. The good frames are received and buffered, whereas only the incorrect or lost frames are retransmitted in this case.


Sender
Receiver
0 1 2 3 0 1 2
S
Frame 0
Frame 1
ACK 2
Frame 2
Lost
Frame 3
NAK 2
Frame 2
Resent
Time

SLIDING WINDOW PROTOCOL

SLIDING WINDOW

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.
In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.



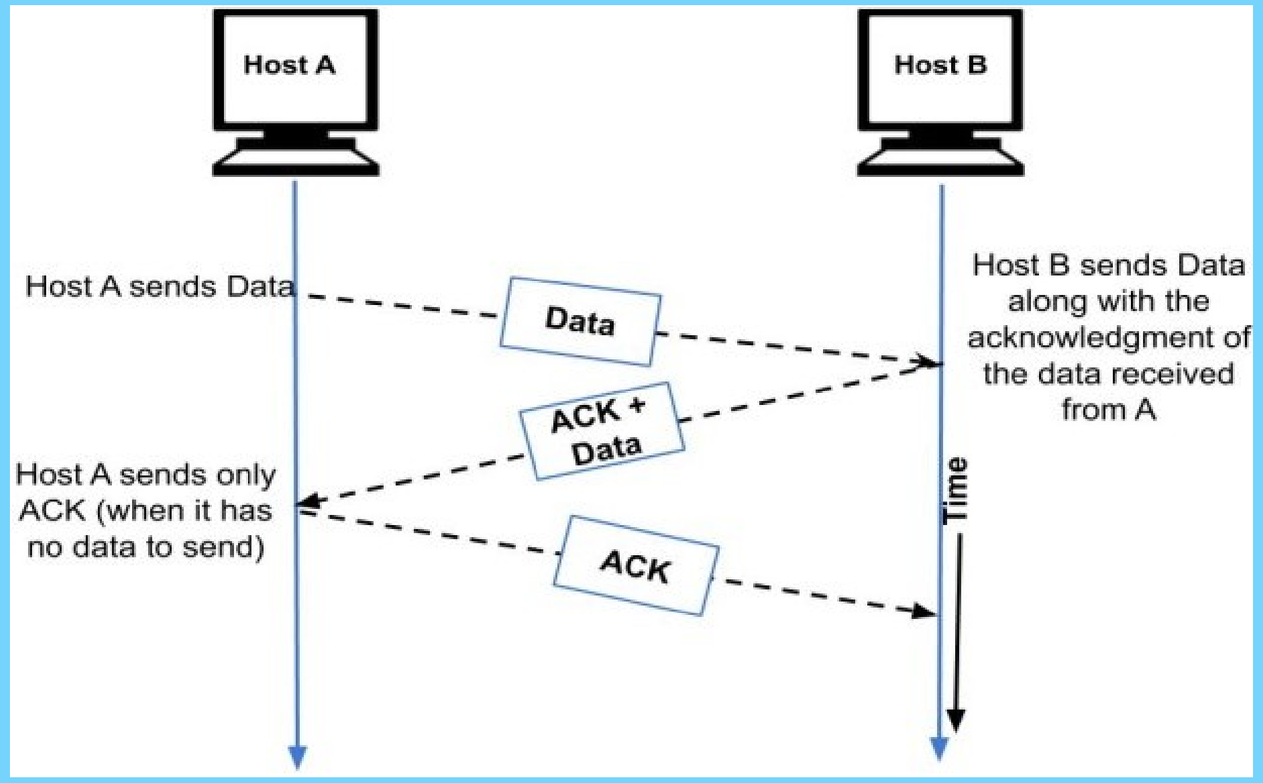
KEY CONCEPTS

Both sender and receiver maintain a finite size buffer to hold outgoing and incoming packets from the other side.

Every packet sent by the sender,must be acknowledged by the receiver. The sender maintains a timer for every packet sent, and any packet unacknowledged in a certain time, is resent.

Piggybacking

- When a data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it to the next packet.
- The acknowledgement is attached to the outgoing data frame.
- The technique of temporarily delaying outgoing acknowledgements so they can be hooked onto the next outgoing data frame is piggybacking



Sender Side

- To keep track of the frames, sender station sends sequentially numbered frames.
- Since the sequence number to be used occupies a field in the frame, it should be limited size.
- If the header of the frame allows k bits, the sequence numbers rangeb from 0 to 2^k-1
- Sender maintains a list of sequence numbers that it is allowed to send.

RECEIVER SIDE

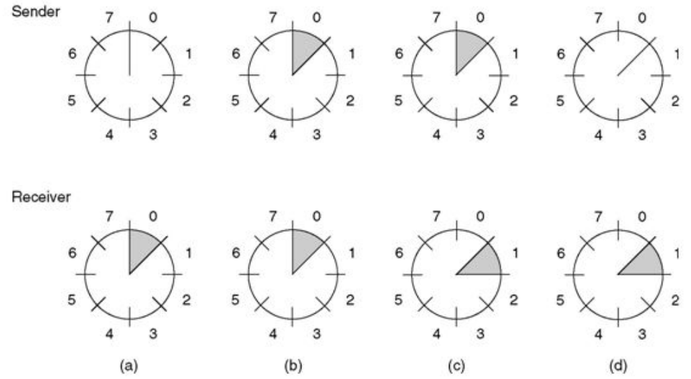
- Receiver always maintains window size as 1.
- The receiver acknowledges a frame buy sending an ACK frame that includes the sequence number of the next frame expected.
- This scheme can be used to acknowledge multiple frames.
- The receiver needs a buffer of size 1.

One bit Sliding Window

- Here K=1 at the senders side.
- Then the size of the senders window is,
  2^k-1
  K=1, 2-1=1
- This is same as the stop and wait protocol.

A One-Bit Sliding Window Protocol

A sliding window protocol with a maximum window size of 1 is called a one-bit sliding window protocol. Such a protocol uses stop-and-wait since the sender transmits a frame and waits for its acknowledgement before sending the next one.

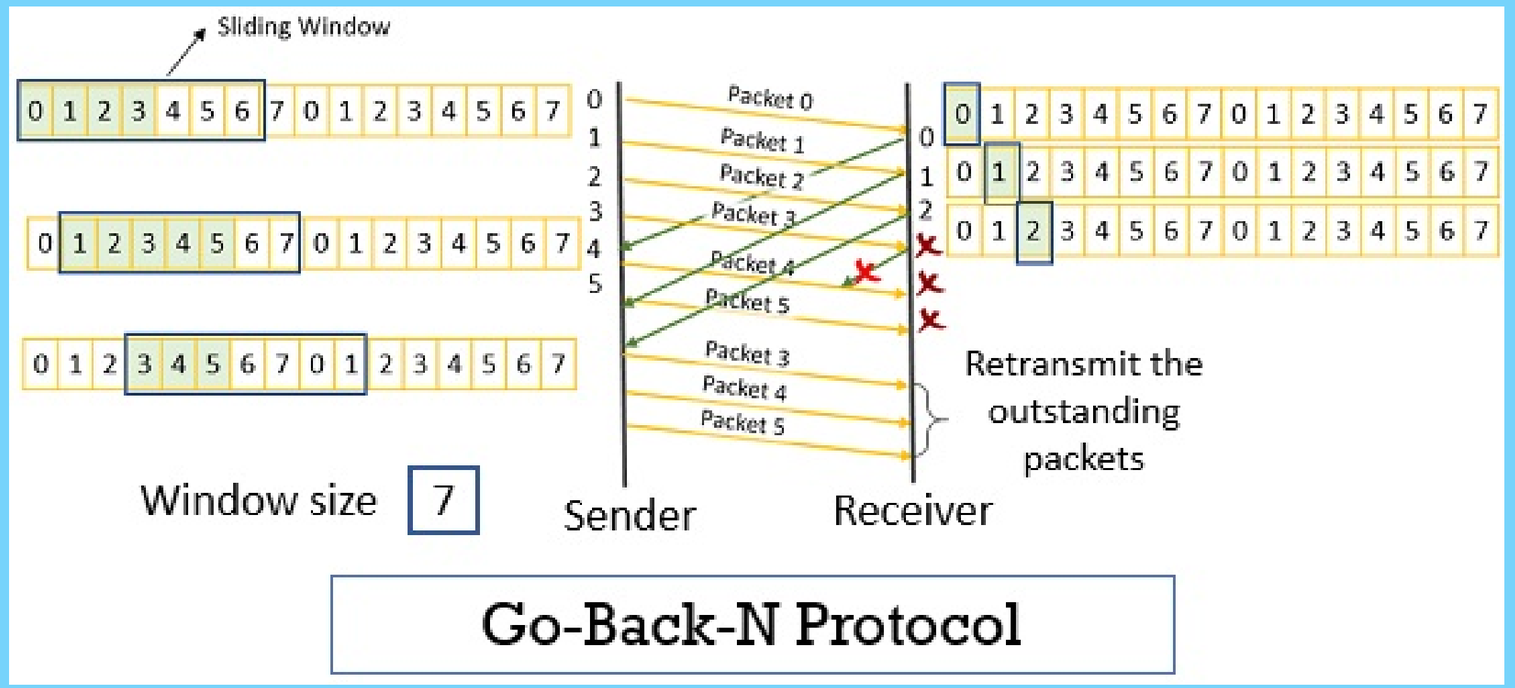


A sliding window of size 1, with a 3-bit sequence number.
(a) Initially.
(b) After the first frame has been sent.
(c) After the first frame has been received.
(d) After the first acknowledgement has been received.

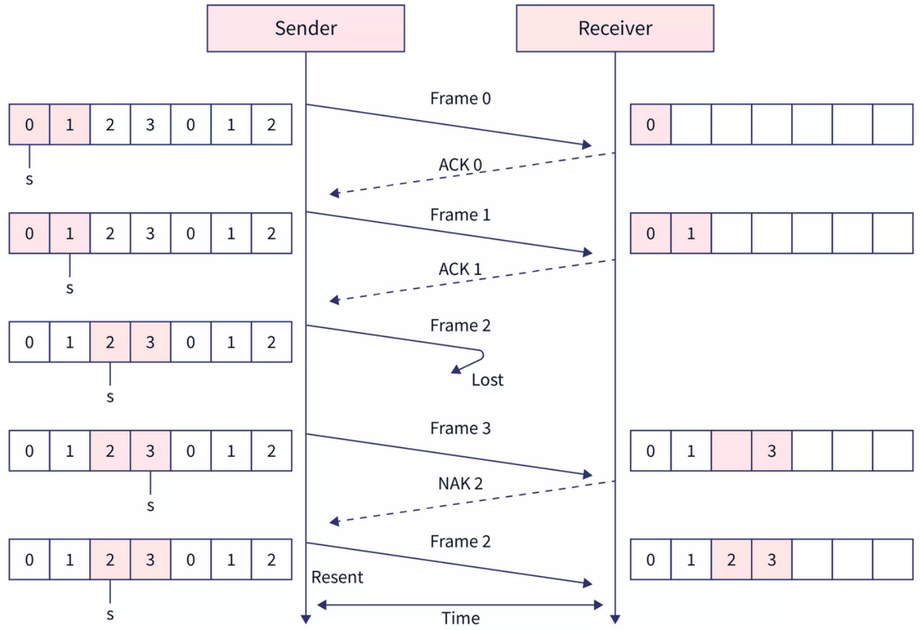
GO-BACK-N PROTOCOL

In Go-Back-N ARQ, The number of frames that can be sent at a time totally depends on the size of the sender's window. So, we can say that 'N' is the number of frames that can be sent at a time before receiving the acknowledgment from the receiver.

Go back N work with concept , If the acknowledgment of a frame is not received within an agreed-upon time period, then all the frames available in the current window will be retransmitted.

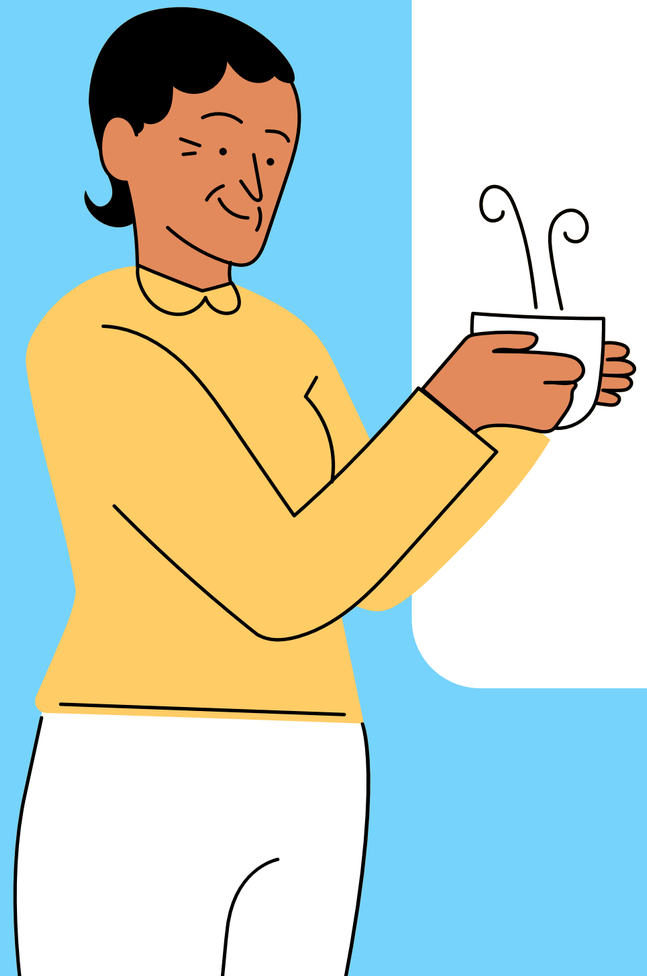


SELECTIVE REPEAT PROTOCOL



The selective repeat ARQ is one of the Sliding Window Protocol strategies that is used where reliable in-order delivery of the data packets is required. The selective repeat ARQ is used for noisy channels or links and it manages the flow and error control between the sender and the receiver. In the selective repeat ARQ, we only resend the data frames that are damaged or lost. If any frame is lost or damaged then the receiver sends a negative acknowledgment (NACK) to the sender and if the frame is correctly received, it sends back an acknowledgment (ACK). As we only resend the selected damaged frames so we name this technique the Selective Repeat ARQ technique. The ACK and the NACK have the sequence number of the frame that helps the sender to identify the lost frame.

THANK YOU!



Have a great day ahead.

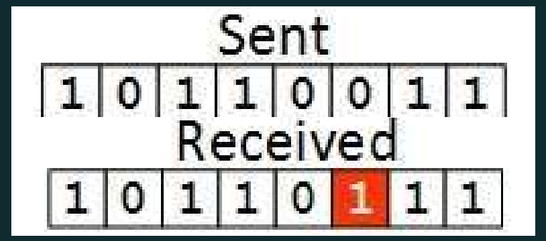
Error Handling
in Data Transmission

Error in Data Transmission

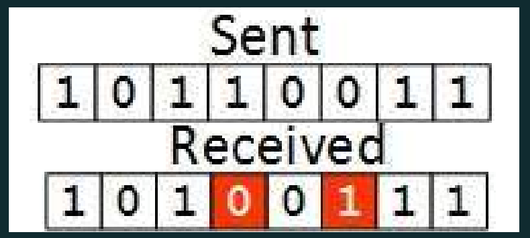
An Error is a condition when the receiver's information does not match with the sender's information.

- Reasons for data corruption include noise, cross-talk etc. Data-link layer uses error control mechanism to ensure that frames are transmitted accurately.

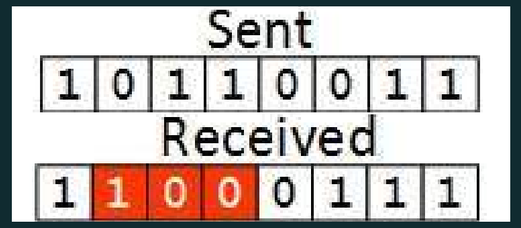
Single Bit Error: Only one bit, anywhere though, is corrupt.



Multiple Bit Error: Frame with more than one bits in corrupted state.



Burst Error: Frame contains more than 1 consecutive bits corrupted.

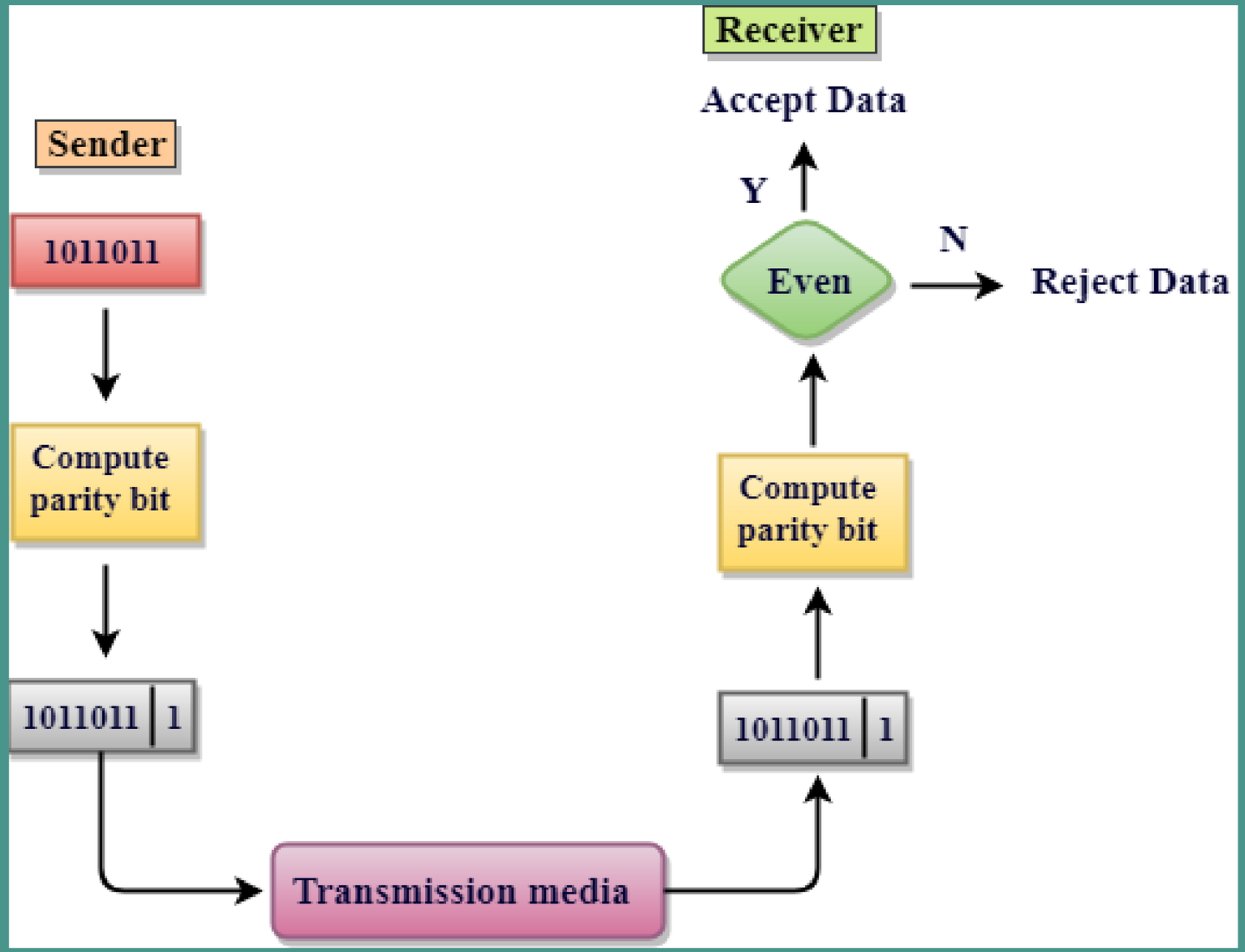


Error Detection

- To avoid corruption of data by noise, Error Detecting Codes are used.
- In these codes, additional bits are added to the message to detect if any error has occurred.

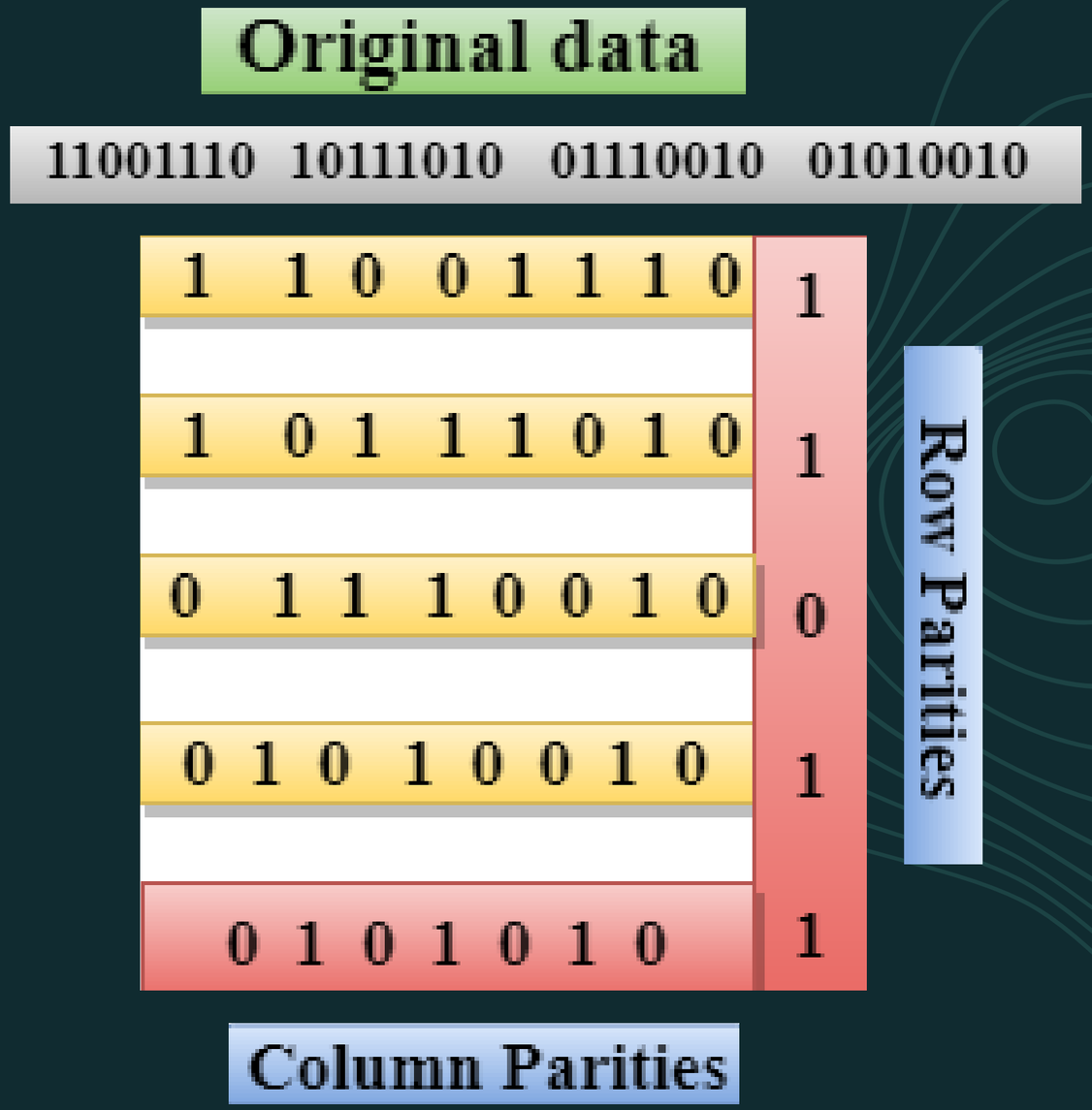
1. Single Parity Check
2. Two-Dimensional Parity Check
3. Checksum
4. Cyclic Redundancy Check

Single Bit Parity Check



- A redundant parity bit is added at the end of the data unit to make the number of 1s even.
- If the number of 1s bits is odd, then parity bit 1 is appended. Otherwise, parity bit 0 is appended .
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.

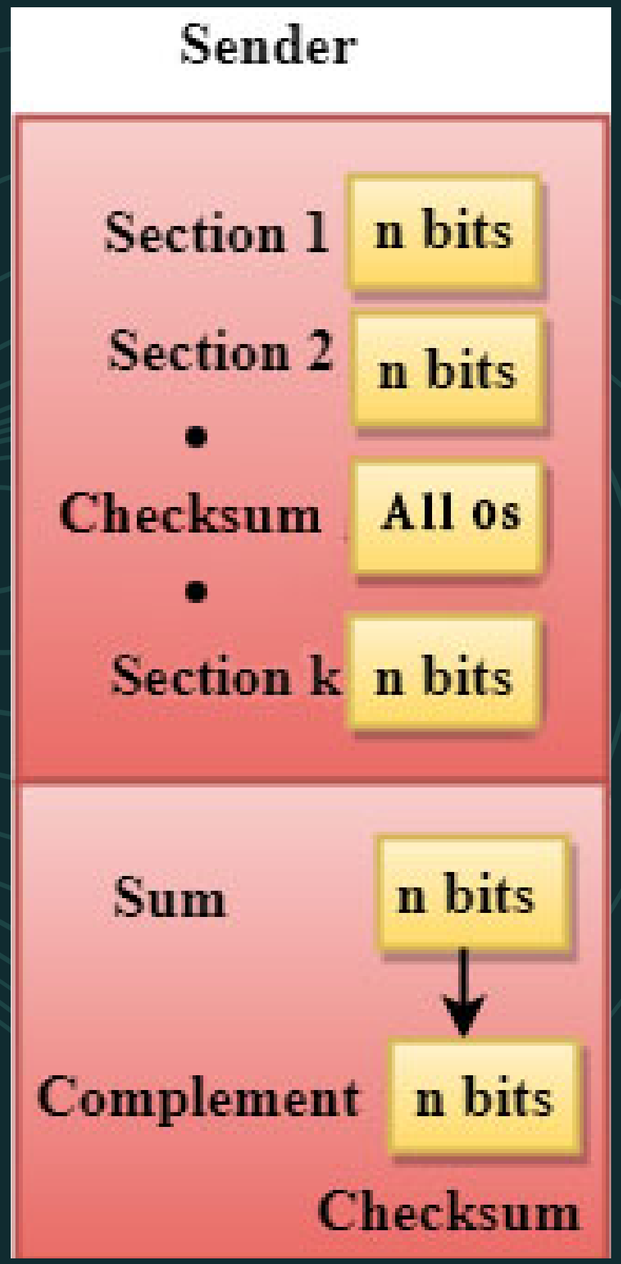
Two Dimensional Parity Check

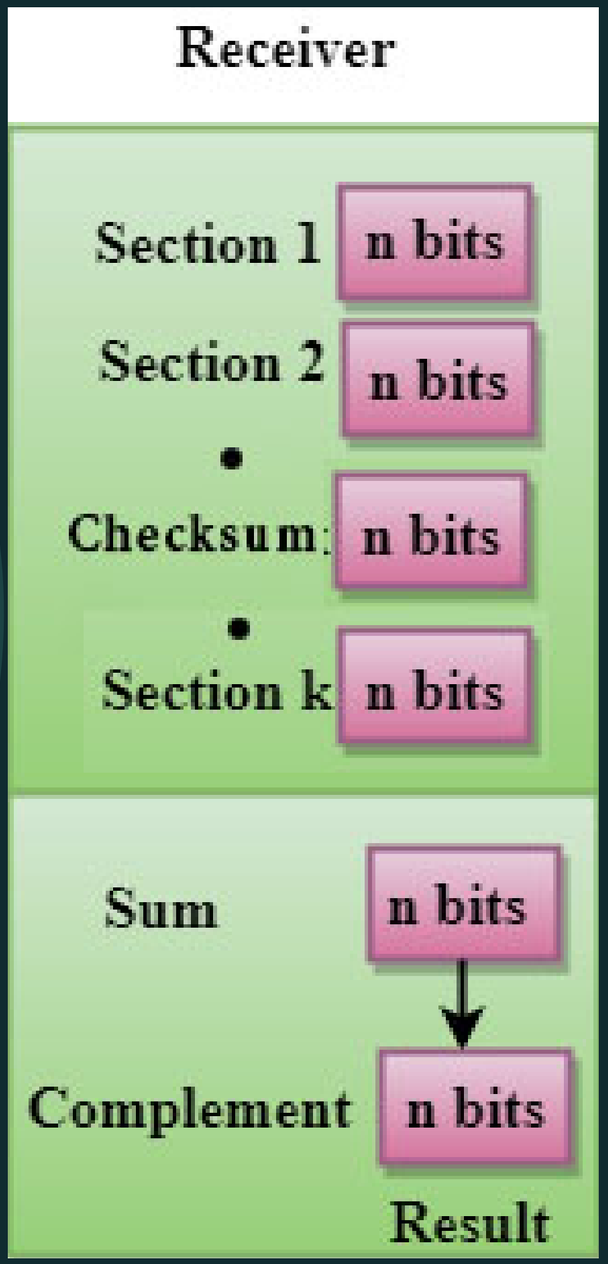


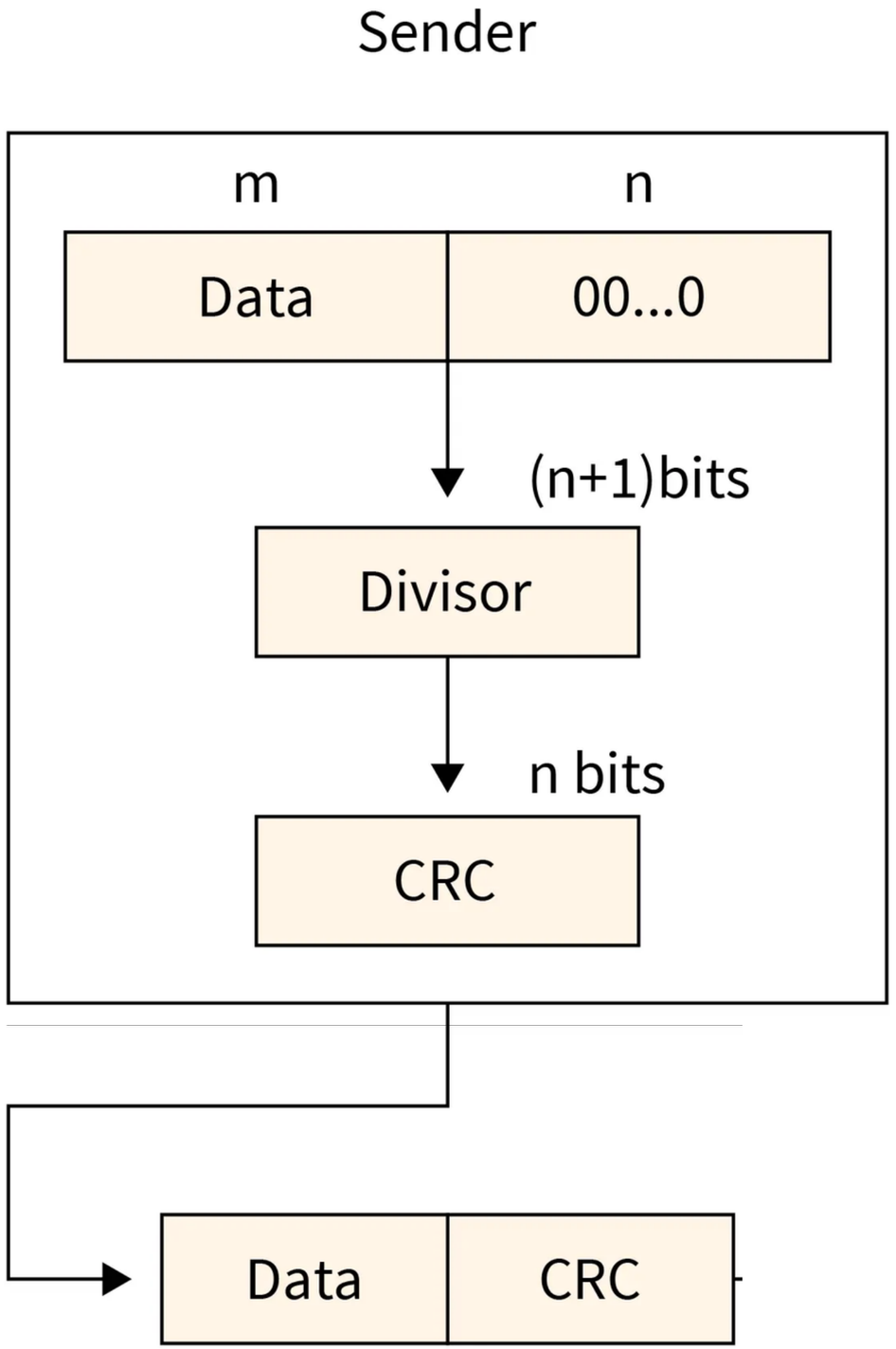
- It organizes the data in the form of a table.
- A block of bits is divided into rows and parity check bits are computed for each row and column, equivalent to the single-parity check.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.

Checksum

- Checksum is an error detection technique based on the concept of redundancy.
- The checksum is generated by sender and is checked by the receiver.
- If the sum on receiver side is 0, the data is accepted. Otherwise, it is rejected.





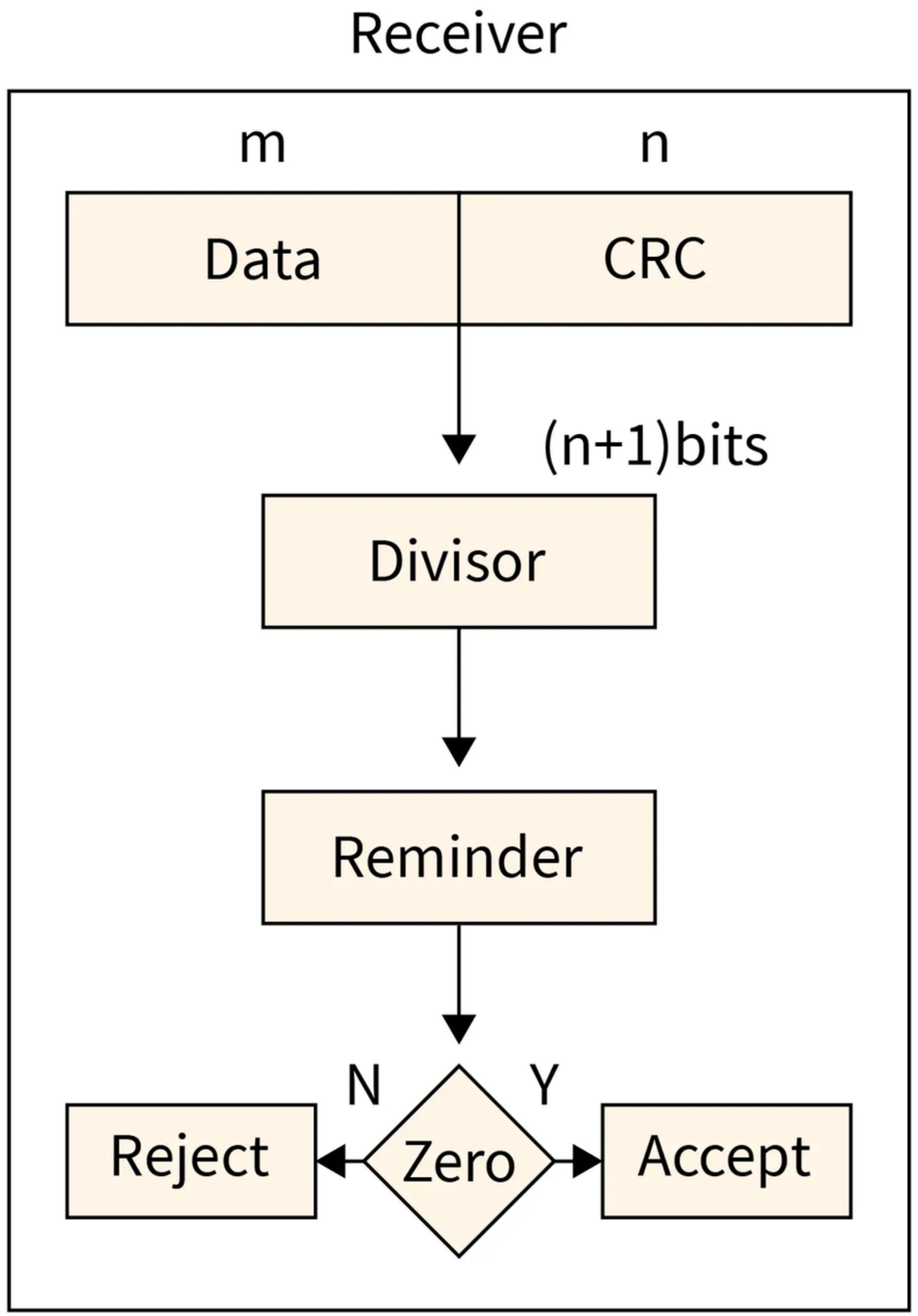


Cyclic Redundancy Check

- It uses binary division.
- A bit sequence commonly known as cyclic redundancy check is added to the end of the bits in CRC. This is done so that the resulting data unit will be divisible by the second binary number that is predetermined.

- The receiving data units on the receiver's side need to be divided by the same number.
- These data units are accepted and found to be correct only on the condition of the remainder of this division is zero.
- If the remainder shows that the data is not correct, they need to be discarded.

Disadvantage: Cyclic Redundancy Check may lead to overflow of data.



Error Correction

An error correction method is used correction of error of following its detection.

Backward Error Correction
When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

Forward Error Correction
When the receiver detects error in received data, it executes error-correcting code, helping it to auto-recover and to correct some kinds of errors.

Redundant Bits in Error Correction

A single additional bit can be used for error detection but not for error correction.
It is important to know the exact location of the error to correct that error.
For finding out the single-bit error, the error detection code checks out that the error is actually in one of the data bits.
Let d represents the number of data bits and r represents the smallest number of redundant bits such that:

$$2^r >= d+r+1$$

Hamming Code

- It is a technique for finding out the position of the error bit.
- It is based on the relationship between the redundant bits and data units.
- Its main advantage is that it can be applied to data units of any length.

Hamming Code Algorithm

- Add the information in 'd' bits to the redundant bits 'r' to make data as d+r.
- A decimal value will be assigned by the position of each (d+r) digit.
- In positions 1,2...2k, the 'r' bits will be placed.
- The parity bits are again calculated on the receiver's end. The position of an error defines the parity bit's decimal value.

Error Position	Binary Number
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Relationship b/w Error position & binary number