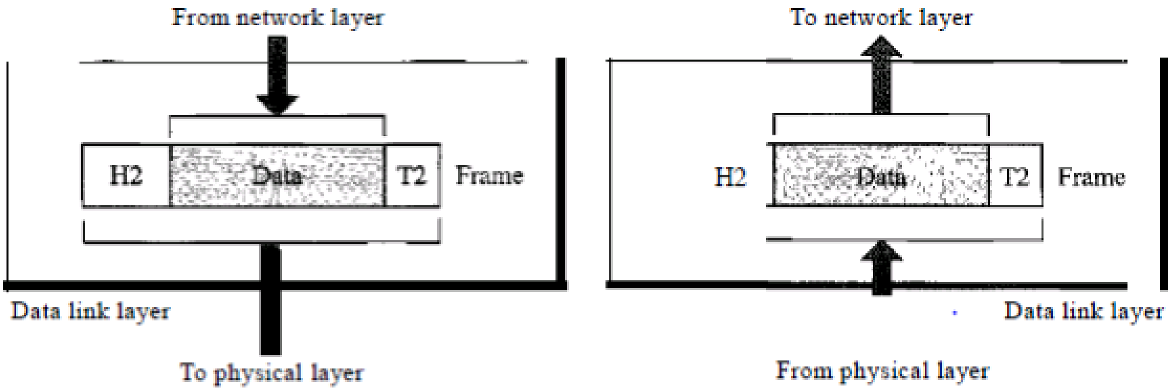
UNIT - II DATA LINK LAYER

Introduction, Framing, Flow and Error Control, Noiseless Channels, Noisy Channels, HDLC, Point to Point Protocols. Medium Access sub layer: ALOHA, CSMA/CD, LAN – Ethernet IEEE 802.3, IEEE 802.5 – IEEE 802.11

DATA LINK LAYER:

Data-link layer has the responsibility of transferring frame from one node to physically adjacent node over a link (the node-to-node) delivery of data within the same local network.

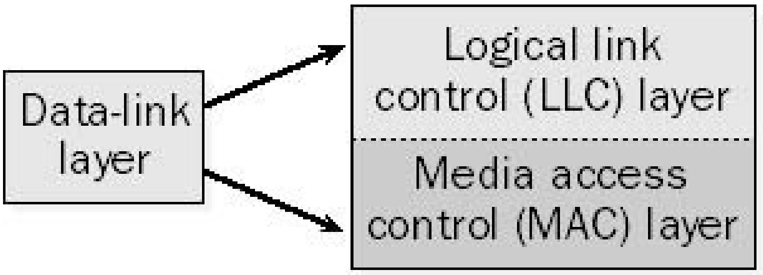


Data link Layer

The data link layer plays an important role in organizing, reframing, translating, and directing information in an efficient and sensible way. The switch is the most common device used at the data link layer. Switch transmits frames from sender to receiver. For that, the switch uses the MAC addresses of the sender and receiver. Node is also known as hop.

The data link layer is divided into two sublayers:

- **Logical Link Control (LLC):**
- **Media Access Control (MAC)**:


Data-link layer
Logical link control (LLC) layer
Media access control (MAC) layer

Logical Link Control (LLC): is an upper sublayer in the data link layer of the OSI model. It is responsible for providing a reliable connection between two devices on a network, ensuring that data is transmitted accurately and without errors. Logical Link Control deals with **flow control** from host to host.

LLC provides several functions to support this reliable connection, including:

- **Flow control**: LLC ensures that data is transmitted at a rate that both devices can handle, preventing data overflow or underflow.
- **Error detection**: LLC uses checksums and other error-detection techniques to ensure that data is transmitted accurately. If an error is detected, LLC will request that the data be retransmitted.
- **Sequencing**: LLC assigns a sequence number to each data packet transmitted, allowing the receiving device to reassemble the data in the correct order.

- **Framing**: LLC adds additional information to the data packets, such as a header and a trailer, to indicate the start and end of a transmission.

Media Access Control (MAC). The MAC sublayer governs protocol access to the physical network medium. The MAC protocol is responsible for controlling access to the physical medium, such as a network cable or wireless channel.It provides physical addressing for network components. A physical address is called **Media Access Control (MAC)** address.

Addressing: The data link layer uses physical addresses to transmit frames from sender to receiver. Generally, physical addresses are also known as MAC (Media Access Control) addresses.

- MAC is a 48-bit number printed on the network interface card of the device. MAC address is an identifier of the device.
- MAC address is divided into two parts that are Organization Unique Identifier and Unique Part. These two parts combine to form a MAC address that is unique to a device.
- Physical addresses are used for data encapsulation and media access control.
- The data link layer combines the MAC address of the sender and receiver in the frame with the IP address.
- When the sender and receiver are on the same network, instead of using IP, the MAC addresses of the sender and receiver are used to transmit the frame.
- Basically, when frames are transmitted from intermediary devices, the intermediary devices de-encapsulate the frames to understand the IP address and find the destination host.

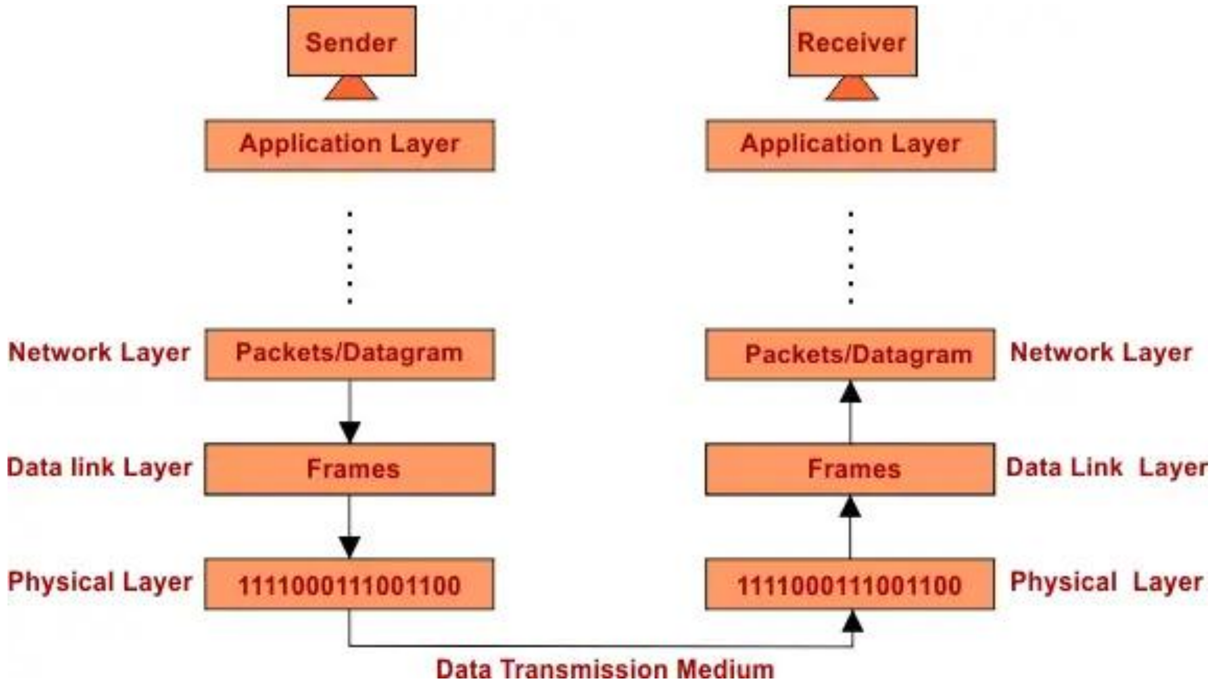
The data link layer is also responsible for reading signals from the physical layer and reassembling them into the original data link layer frame. It also performs error detection and discards bad frames. It typically does not perform error correction. It is responsible for Its major role is to ensure error-free transmission of information. DLL is also responsible for encoding, decoding, and organizing the outgoing and incoming data.

Institute of Electrical and Electronic Engineers (IEEE) 802.2, 802.3, and 802.5; ANSI's FDDI; Ethernet II; Asynchronous Transfer Mode (ATM), Frame Relay, High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), Synchronous Data Link Control (SDLC), Serial Line Internet Protocol (SLIP), and X.25 are examples of data link layer protocols and standards.

Network interface controllers or cards (NICs), bridges, and switches are the primary networking components that function at the data link layer.

On the sending device, it performs the following tasks.

- It takes data packets from the network layer and converts them into frames.
- It attaches a header and trailer to each frame.
- In the header, it puts the source and destination MAC address.
- In the trailer, it put a CRC value.
- Based on the connected media type, it converts the frame into signals and loads them on the media.



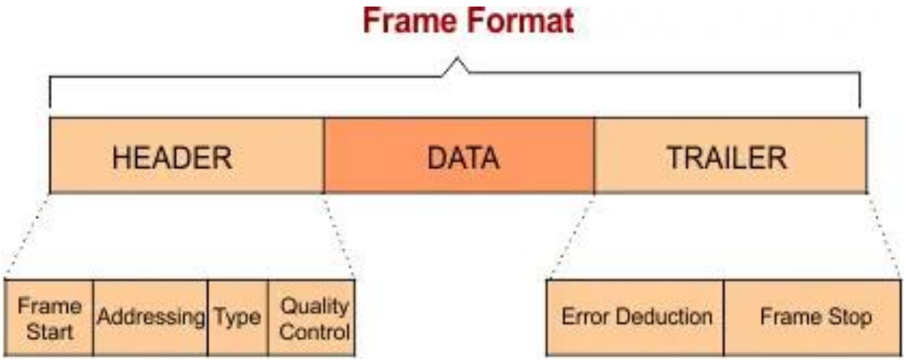
On the receiving device, it performs the following tasks.

- It picks signals from the connected media and converts them into frames.
- It uses the CRC value of each frame to confirm the frame is good.
- It deletes all bad frames.
- For all good frames, it checks their destination MAC address.
- If the destination MAC address belongs to it, it removes the header and trailer from the frame and gives it to the network layer.

Functions of the Data-Link Layer

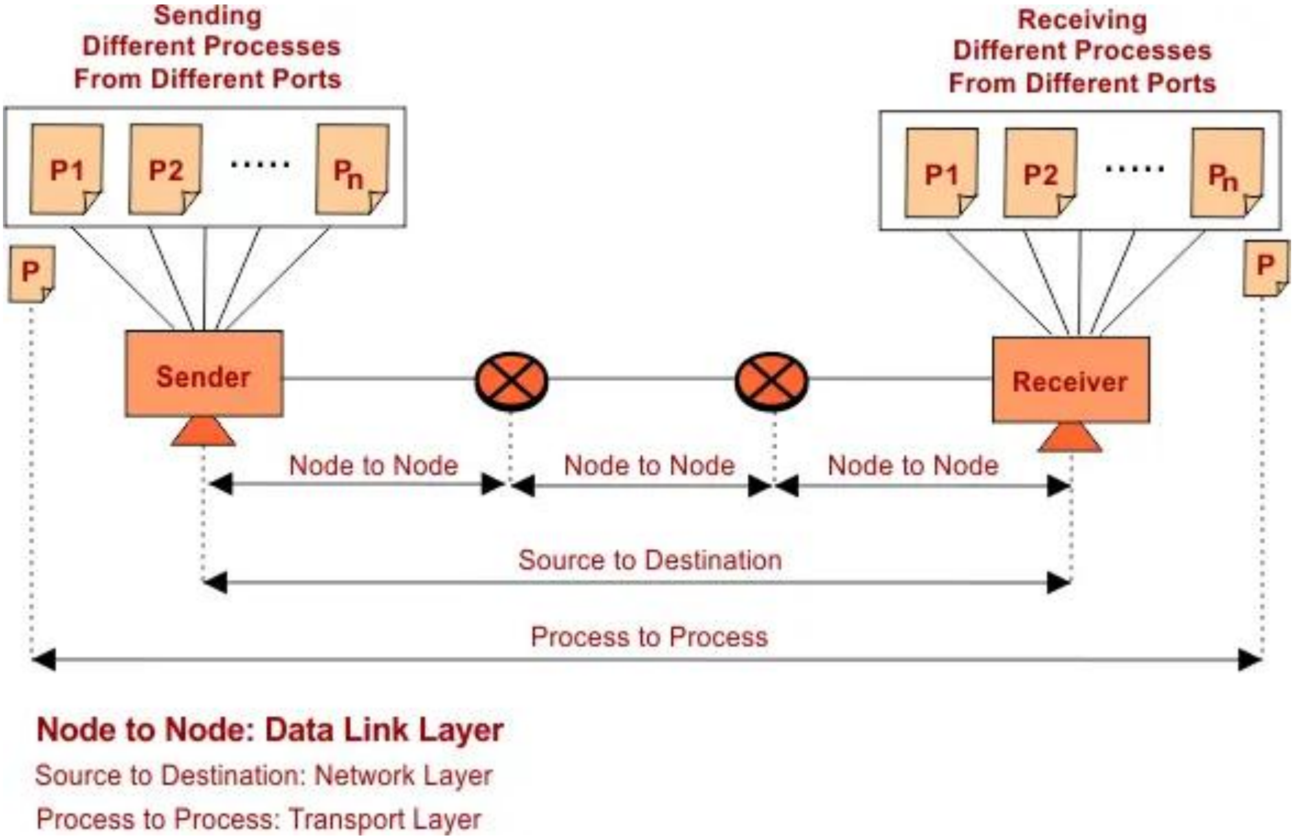
1. Framing

- The data packets received from the network layer are encapsulated in frames by the data-link layer for bit-to-bit sharing over the channel.
- It is also responsible for restructuring the framed data in the network model, and each data frame is different from the others.



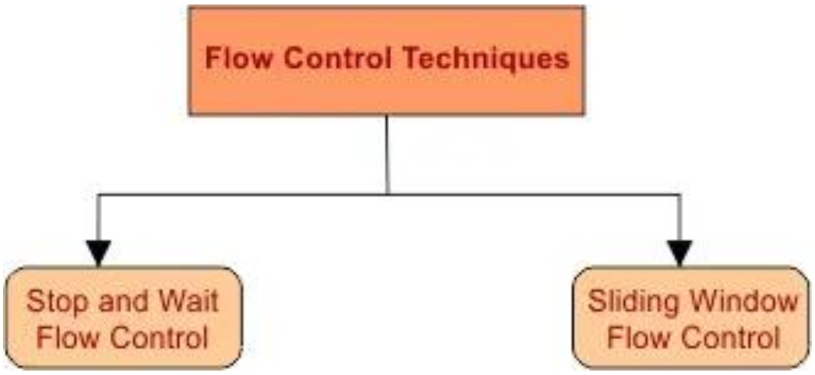
2. Node to Node Connection

To reach the data at destination it first passes through different intermediate nodes (i.e. Routers) which is done through data link layer.



3. Flow Control

The flow control enables reliable and fast communication when the sender and receiver have differences in processing capability ie Flow control restricts the fast sender when the receiver is slow. The most straightforward flow control protocol is the stop-and-wait and Sliding window protocols to control the flow of data, where the sender sends a network packet and waits for an acknowledgment.



4. Error Control

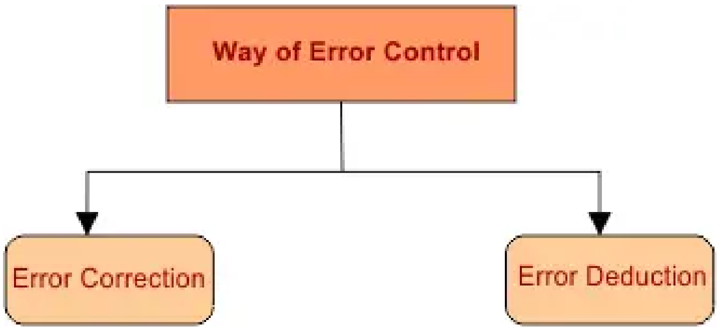
- During data transmission, due to noise or signal loss, errors might occur in the data being transmitted.

  Hardware
  Software failure (due to bugs in the code)
  Background radiation,
  Head crashes

- To minimize such data error rate, the data-link layer performs error detection and correction techniques on the transmitted data. data-link layer control these errors at each node.

Ways of Doing Error Control

There are basically two ways of doing Error control, as given below:



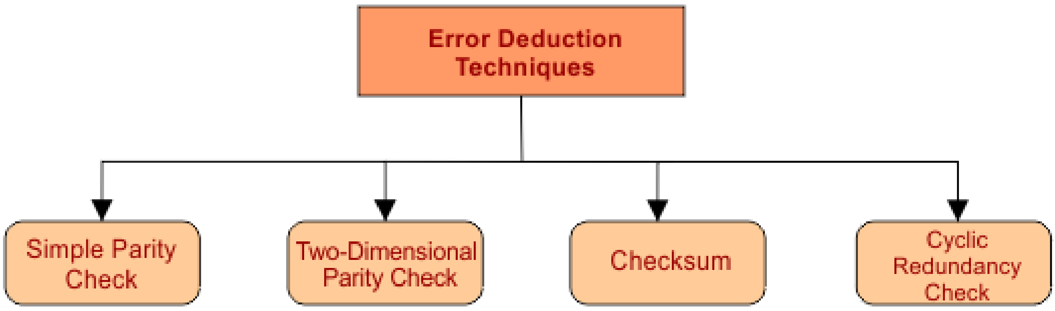
ErrorCorrection:

Error correction means fixing the errors. Our basic need is data should be error free. The error correction method is very costly and hard as well.

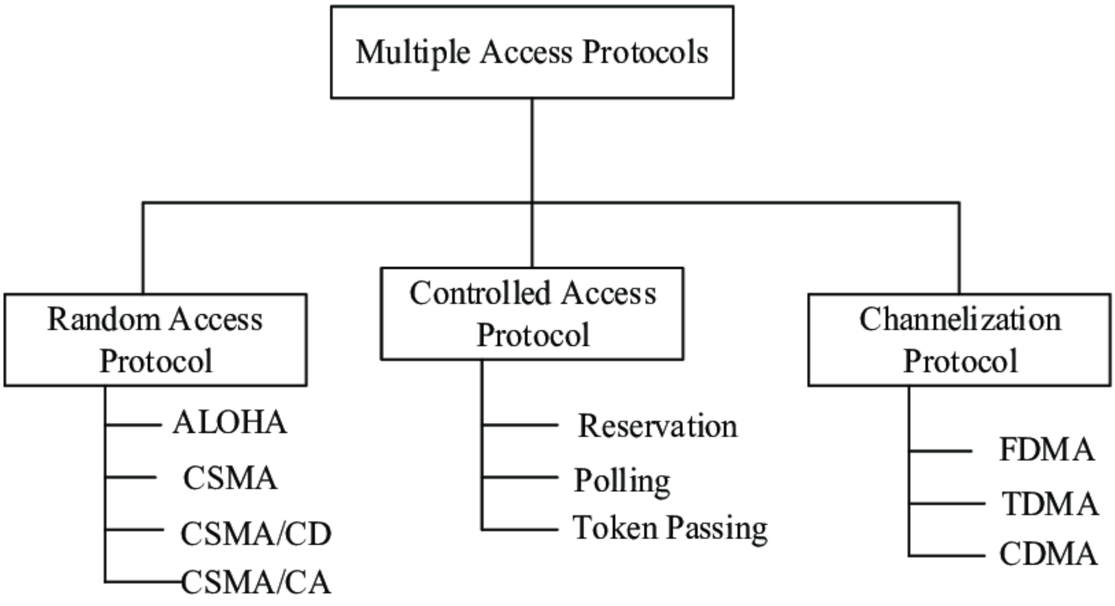
The best error correction technique at each node of the data link layer is the Hamming Code.

ErrorDetection

Error detection means identification of errors. There are different ways to identify the errors at each node in the data link layer listed under.



5. Medium / Multiple Access Control (MAC) or Access Control

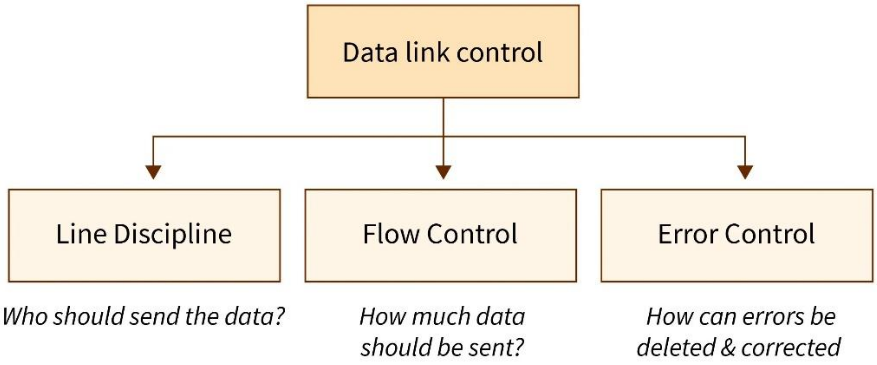


When a node on the shared link tries to transfer the data, it has a probability of collision.
For example, when multiple nodes in the bus topology try to send data at the same time, a collision may happen.
So, the Data-link layer uses the following protocols to eliminate collision
6. Physical Addressing

- The task of adding a physical address to the frame in the header format is known as addressing.
- It acts as an identification service for transmitting the frames to multiple network models over the channel.
- It provides the MAC address to each node so that it can communicate within the same network. If we want to communicate with another network, then we have to use the IP address.

Flow Control and Error Control

Data Link Layer is responsible for reliable **point-to-point data** transfer over a physical medium. To implement this data link layer provides three functions:


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

Line Discipline:

Line discipline is the functionality used to establish coordination between link systems. It decides which device sends data and when.

Flow Control:

Flow control is an essential function that coordinates the amount of data the sender can send before waiting for acknowledgment from the receiver.

Error Control:

Error control is functionality used to detect erroneous transmissions in data frames and retransmit them.

Flow Control in the Data Link Layer

Flow control is a set of procedures that restrict the amount of data a sender should send before it waits for some acknowledgment from the receiver.

- Flow Control is an essential function of the data link layer.
- It determines the amount of data that a sender can send.
- It makes the sender wait until an acknowledgment is received from the receiver’s end.
- Methods of Flow Control are Stop-and-wait, and Sliding window.

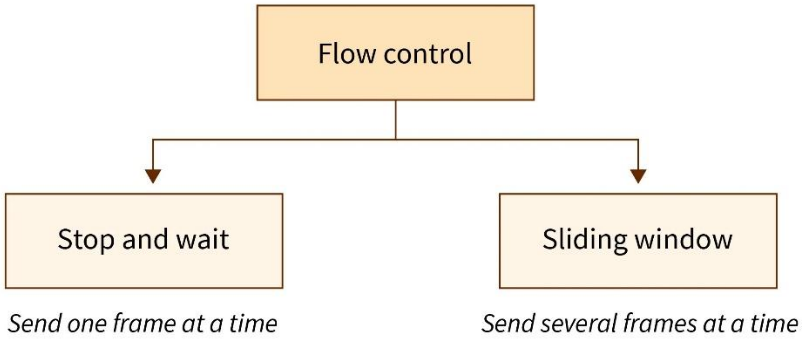
Purpose of Flow Control

The device on the receiving end has a limited amount of memory (to store incoming data) and limited speed (to process incoming data). The receiver might get overwhelmed if the rate at which the sender sends data is faster or the amount of data sent is more than its capacity.

Buffers are blocks in the memory that store data until it is processed. If the buffer is overloaded and there is more incoming data, then the receiver will start losing frames.

The flow control mechanism was devised to avoid this loss and wastage of frames. Following this mechanism, the receiver, as per its capacity, sends an acknowledgment to send fewer frames or temporarily halt the transmission until it can receive again.

Thus, flow control is the method of controlling the rate of transmission of data to a value that the receiver can handle.

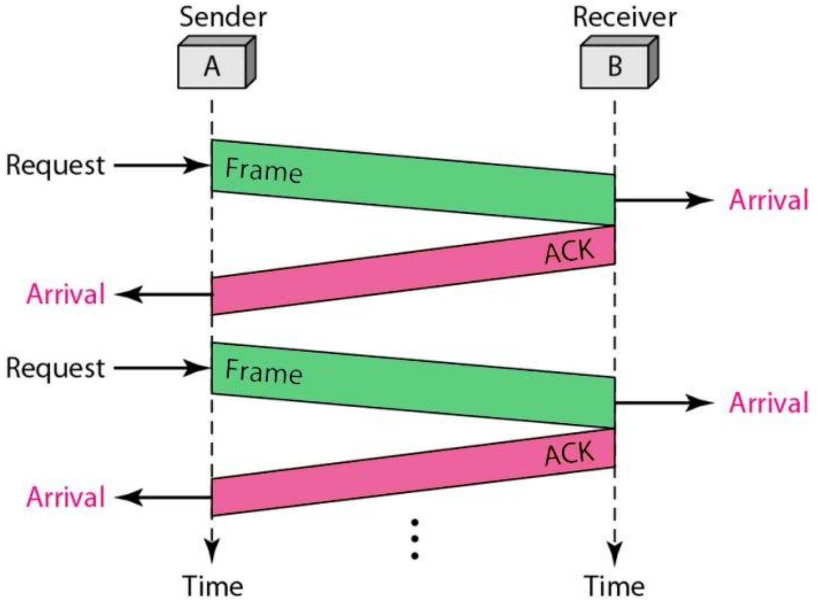


Stop-and-wait Protocol

Stop-and-wait protocol works under the assumption that the communication channel is noiseless and transmissions are error-free.

Working:

- The sender sends data to the receiver.
- The sender stops and waits for the acknowledgment.
- The receiver receives the data and processes it.
- The receiver sends an acknowledgment for the above data to the sender.
- The sender sends data to the receiver after receiving the acknowledgment of previously sent data.
- The process is unidirectional and continues until the sender sends the End of Transmission (EoT) frame.



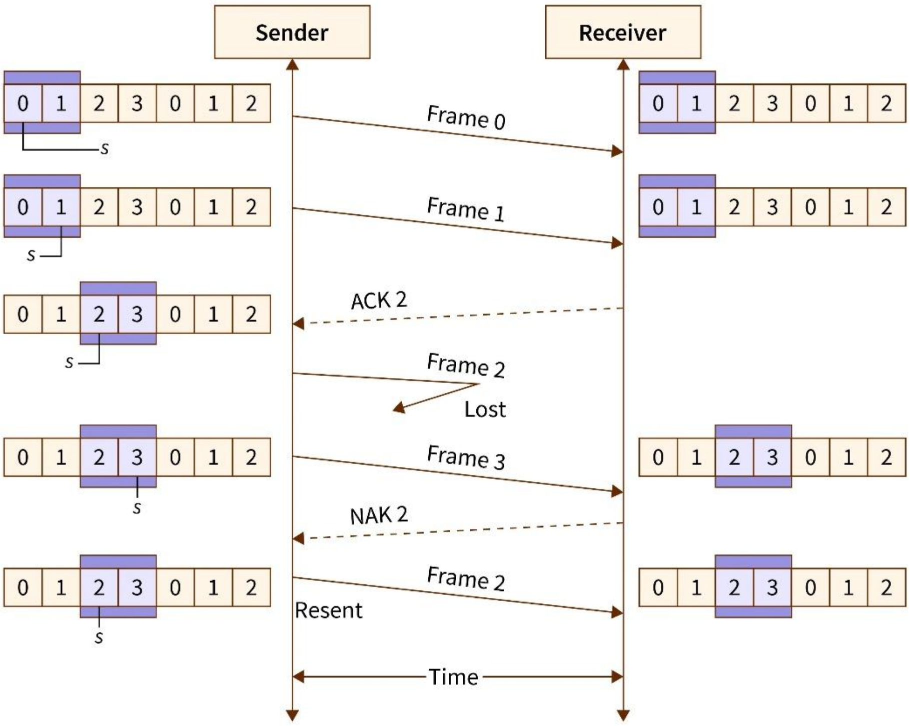
Sliding Window Protocol

The sliding window protocol is the flow control protocol for noisy channels that allows the sender to send multiple frames even before acknowledgments are received. It is called a Sliding window because the sender slides its window upon receiving the acknowledgments for the sent frames.

Working:

- The sender and receiver have a "window" of frames. A window is a space that consists of multiple bytes. The size of the window on the receiver side is always 1.
- Each frame is sequentially numbered from 0 to n – 1, where n is the window size at the sender side.
- The sender sends as many frames as would fit in a window.
- After receiving the desired number of frames, the receiver sends an acknowledgment. The acknowledgment (ACK) includes the number of the next expected frame.

Example:



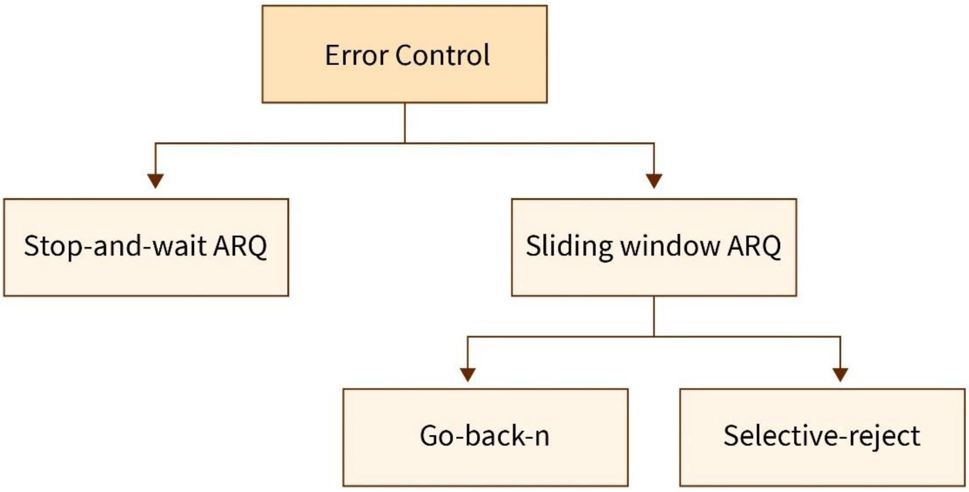
1. The sender sends the frames 0 and 1 from the first window (because the window size is 2).
2. The receiver after receiving the sent frames, sends an acknowledgment for frame 2 (as frame 2 is the next expected frame).
3. The sender then sends frames 2 and 3. Since frame 2 is lost on the way, the receiver sends back a "NAK" signal (a non-acknowledgment) to inform the sender that frame 2 has been lost. So, the sender retransmits frame 2.

Error Control in the Data Link Layer:

Error Control is a combination of both error detection and error correction. It ensures that the data received at the receiver end is the same as the one sent by the sender.

Error detection is the process by which the receiver informs the sender about any erroneous frame (damaged or lost) sent during transmission.

Error correction refers to the retransmission of those frames by the sender.



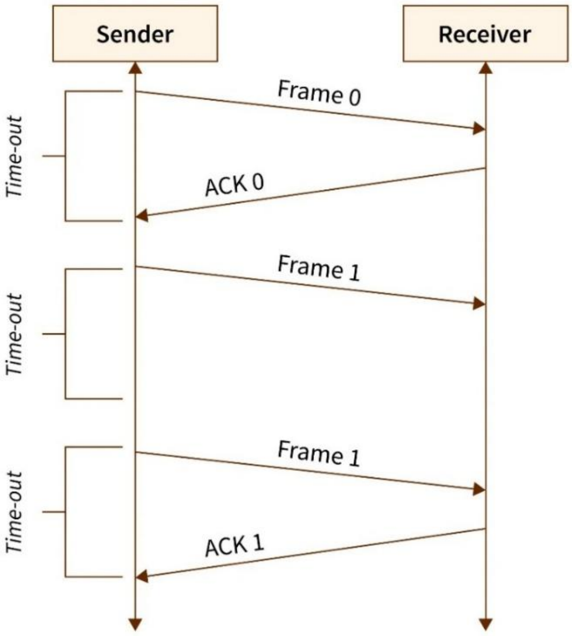
Purpose of Error Control

Error control is a vital function of the data link layer that detects errors in transmitted frames and retransmits all the erroneous frames. Error discovery and amendment deal with data frames damaged or lost in transit and the acknowledgment frames lost during transmission. The method used in noisy channels to control these errors is ARQ or Automatic Repeat Request.

Categories of Error Control

Stop-and-wait ARQ

- In the case of stop-and-wait ARQ after the frame is sent, the sender maintains a timeout counter.
- If acknowledgment of the frame comes in time, the sender transmits the next frame in the queue.
- Else, the sender retransmits the frame and starts the timeout counter.
- In case the receiver receives a negative acknowledgment, the sender retransmits the frame.



Sliding Window ARQ

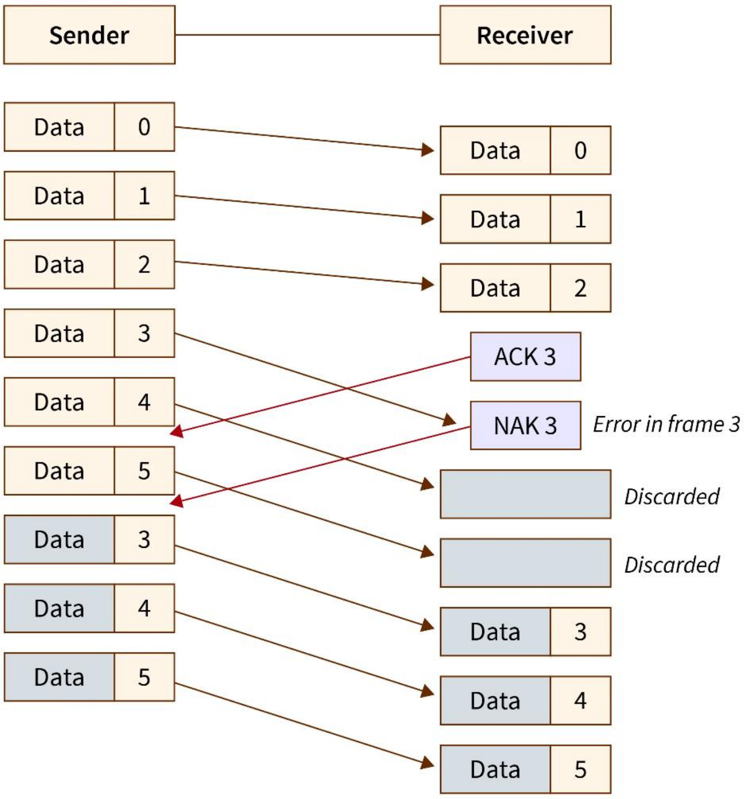
To deal with the retransmission of lost or damaged frames, a few changes are made to the sliding window mechanism used in flow control.

Go-Back-N ARQ:

In Go-Back-N ARQ, if the sent frames are suspected or damaged, all the frames are re-transmitted from the lost packet to the last packet transmitted.

Error Conrol - Go-Back-N(GBN) ARQ

Damaged Data Frame

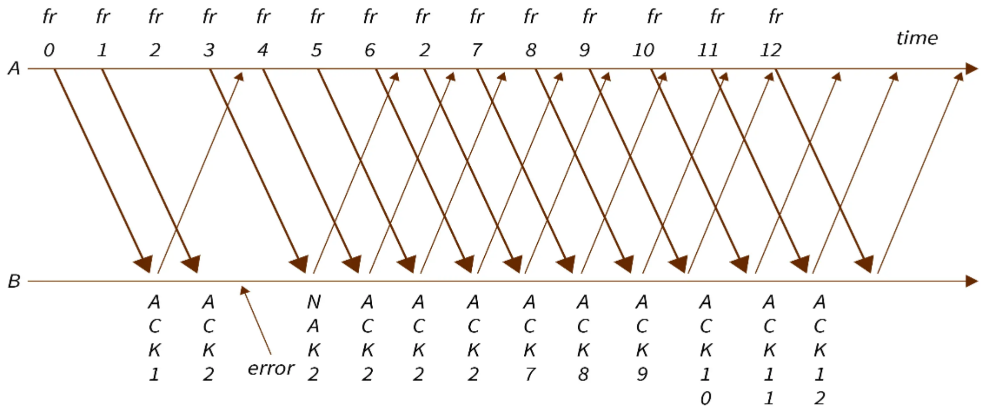


Selective Repeat ARQ:

Selective repeat ARQ/ Selective Reject ARQ is a type of Sliding Window ARQ in which only the suspected or damaged frames are re transmitted

Error Control - Selective Repeat ARQ

Error recovery in selective Repeat ARQ



Differences between Flow Control and Error Control

Flow control	**Error control**
Flow control refers to the transmission of data frames from sender to receiver.	Error control refers to the transmission of error-free and reliable data frames from sender to receiver.
Approaches for Flow Control: Feedback-based Flow Control and Rate-based Flow Control.	Approaches for error detection are Checksum, Cyclic Redundancy Check, and Parity Checking. Approaches for error correction are Hamming code, Binary Convolution codes, Reed-Solomon code, and Low-Density Parity-Check codes.
Flow control focuses on the proper flow of data and data loss prevention.	Error control focuses on the detection and correction of errors.
Examples of Flow Control techniques are: 1. Stop and Wait for Protocol, 2. Sliding Window Protocol.	**Examples of Error Control techniques are :** 1. Stop and Wait for ARQ, 2. Sliding Window ARQ.

Noisy and Noiseless Channels

Data link layer protocols are classified according to whether the transmission channel is noiseless or noisy. Noiseless is an ideal or perfect channel where no frames are lost, duplicated, or corrupted. In contrast, a noisy channel indicates that there will be a lot of disruption in the path when data is transmitted from the sender to the receiver.

Categorization of Protocol

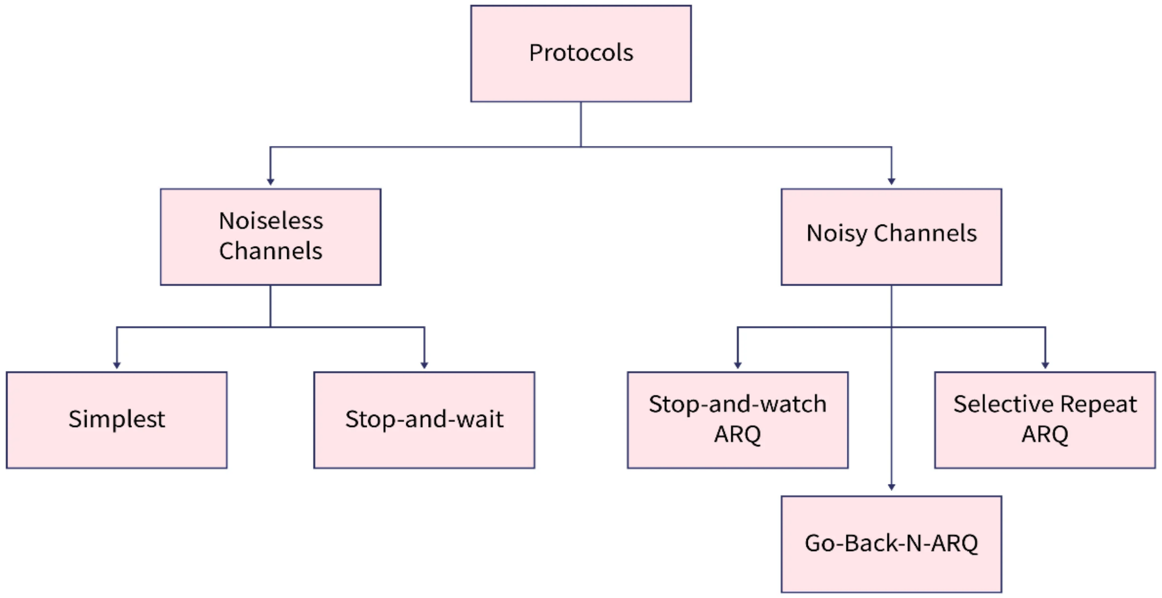
The protocols that can be used for noiseless (error-free) channels and those that can be used for noisy (error-causing) channels are studied separately.

Noiseless Channel: -

A noiseless channel is an ideal or nearly perfect channel in which no frames are lost, distorted, or duplicated. The protocol does not include error control in these types of channels.

Noisy Channel: -

A noisy channel indicates that there will be a lot of disruption in the path when data is transmitted from the sender to the receiver.

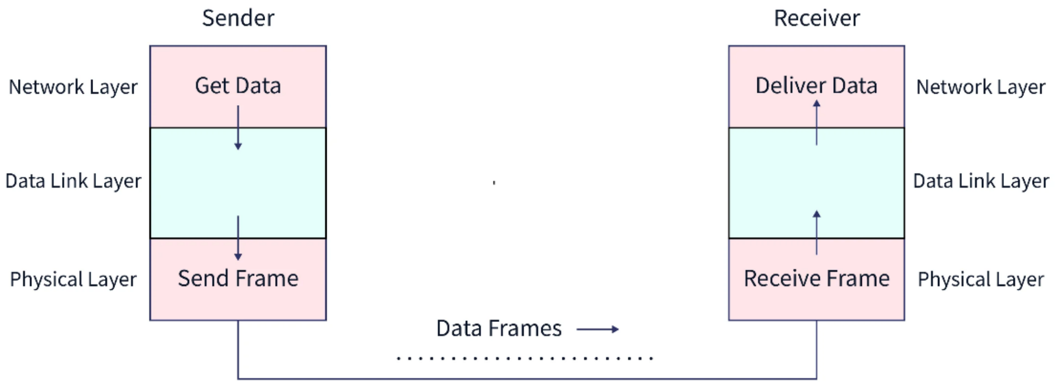


Noiseless Channel

There are two protocols in the noiseless channel, which are as follows.

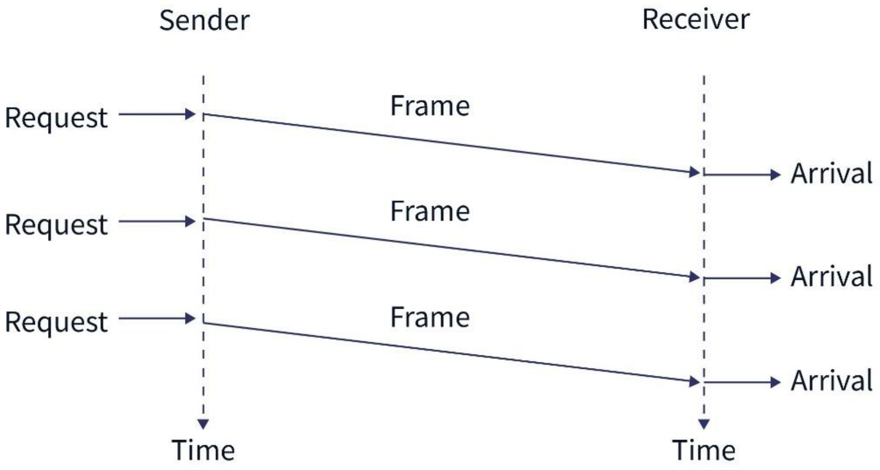
Simplest Protocol

- There is no flow control or error control mechanism in the simplest protocol. The simplest protocol is a unidirectional protocol in which the data frames travel in only one direction from the sender to the receiver. The processing time of the simplest protocol is negligible. Hence it can be neglected.
- The **transmission channel** is completely noiseless (a channel in which no frames are lost, corrupted, or duplicated).
- The **sender and the receiver** are always ready to send and receive data.
- The sender sends a sequence of data frames without thinking about the receiver.
- There is no data loss hence no ACK (Acknowledgment) or NACK (Negative acknowledgment).
- The protocol is divided into two steps: the sender and the receiver. The sender runs in the source machine's data link layer, while the receiver operates in the destination machine's data link layer. There is no usage of a sequence number or acknowledgments in this case.



Flow Diagram:

This Flow Diagram depicts a communication scenario utilizing the simplest protocol. It is pretty simple. Without regard for the receiver, the sender broadcasts a succession of frames. For example, the sender will send three frames, and the receivers will receive three frames. Remember that data frames are represented by slanted boxes, with the height of the box defining the transmission time difference between the first and last bit in the frame.



Error Detection and Correction:

Error Detection: Error detection refers to the techniques used to identify errors that might have been introduced during the transmission or storage of data. It aims to ensure the integrity of the data.

Some common error detection methods include:

Parity Checks

Checksums

Cyclic Redundancy Check (CRC)

Error Correction: Error correction involves not only detecting errors but also reconstructing the original, error-free data. It ensures that the data can be corrected even if some bits were altered during transmission or storage.

Some common error correction methods include:

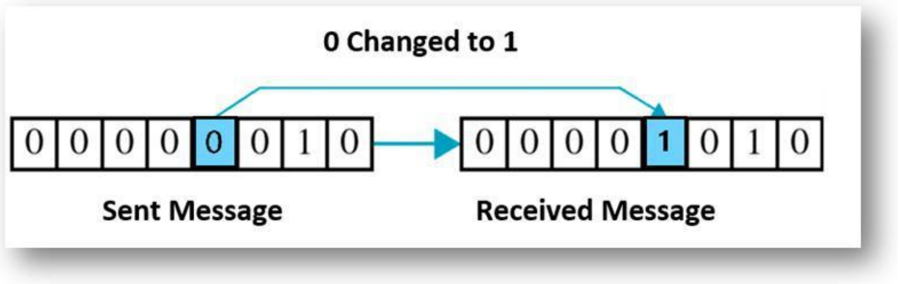
Hamming Code

Reed-Solomon Code

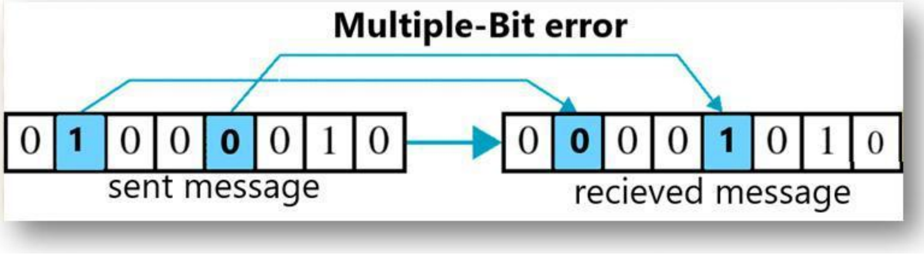
Convolutional Code

Types of Errors in Data Communication

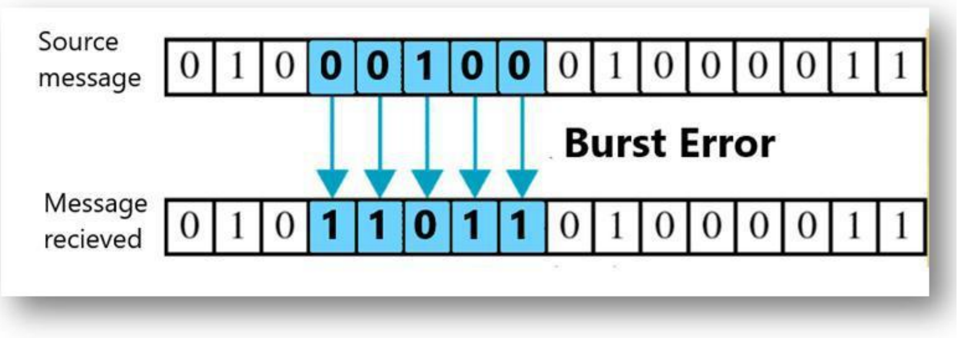
1. **Single-Bit Error**: If only one bit of transmitted data unit is changed i.e. from 1 to 0 or from 0 to 1 then it is a single bit error.



2. **Multiple-Bit Error**: This type of error occurs when more than one bit is affected. While rarer than single-bit errors, they can occur in high-noise environments.



3. **Burst Error**: This type of error occurs when a sequence of consecutive bits is flipped, resulting in several adjacent bits being incorrect.



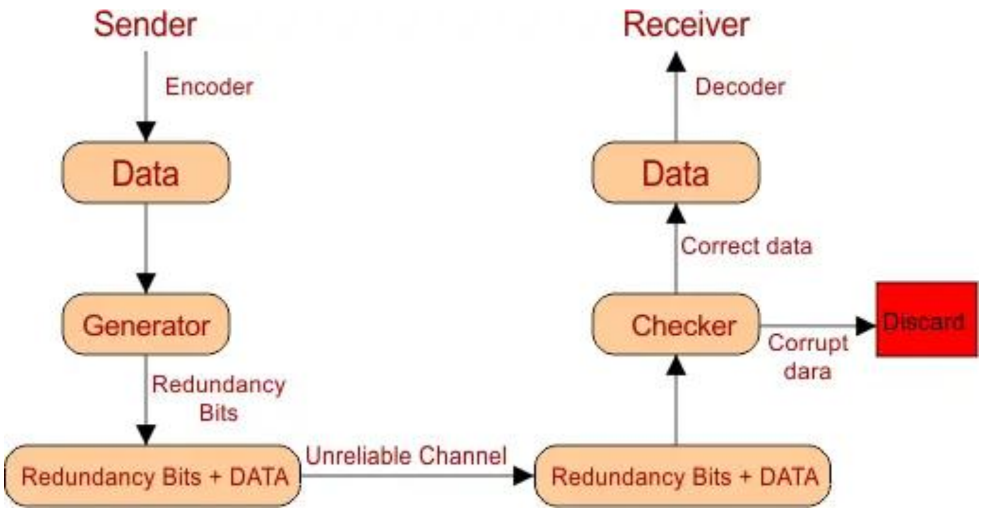
Error Detection Techniques:

Error deduction means to decide whether the received data is correct or not without having a copy of original data.

To detect or correct errors we need to send some extra bits along with original message (data). These extra bits are called redundant bits. To detect errors, we use Generator and Checker.

Generator: The generator is used at the sender end to generate redundancy bits. These redundancy bits are appended with sending data.

Checker: Checker is used at receiver end; it verifies the data and redundancy bits. If sending information is unchanged, then data is accepted; otherwise, it is rejected.



Error Detecting Techniques

The most popular Error Detecting Techniques are

- parity check
- Checksum
- Cyclic redundancy check

Parity check Vertical Redundancy Check (VRC):

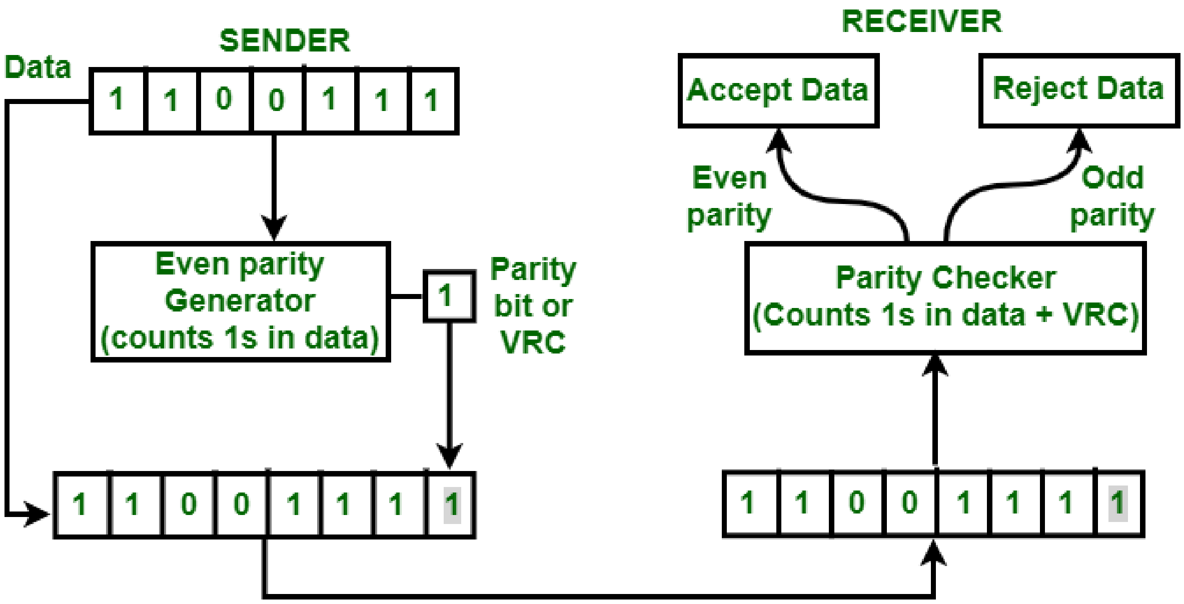
A simple method that adds a single bit to data to ensure the total number of 1s is even (even parity) or odd (odd parity).

Even Parity

- If the total number of 1s is even, the parity bit is set to 0.
- If the total number of 1s is odd, the parity bit is set to 1.

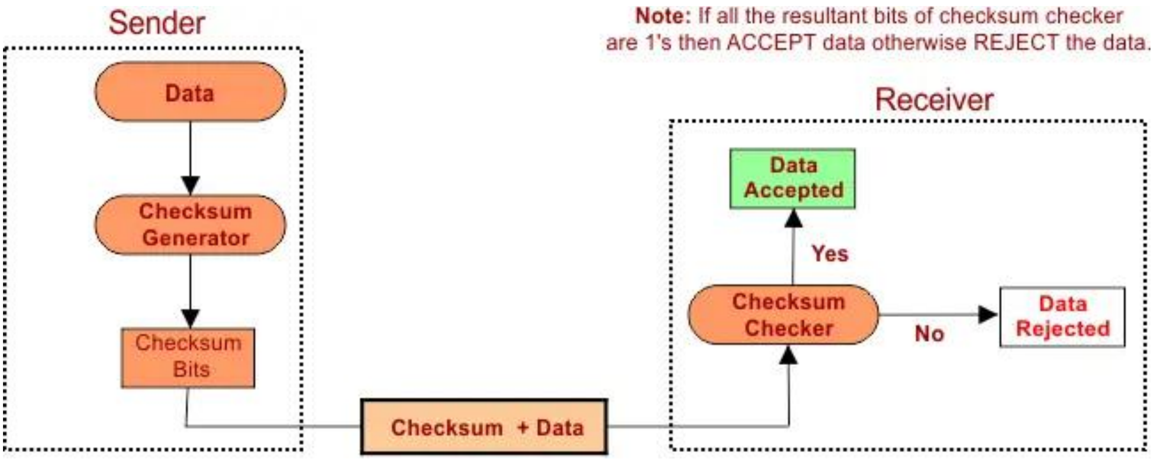
Odd Parity

- If the total number of 1s is even, the parity bit is set to 1.
- If the total number of 1s is odd, the parity bit is set to 0.



Checksums: A mathematical sum of data values calculated before transmission and verified at the destination. If the checksum doesn't match, an error is detected.

A Checksum is a redundancy of bits that are appended with actual data for error detection. At the sender side, the checksum is generated, and at the receiver side, the checksum is validated. The block diagram of the Checksum is given below.



1. Checksum at Sender Side

At the sender side, checksum is generated through the following steps

Step 01: Break the original data into the “K” number of blocks with “N” bits in each block.

Step 02: Sum all the “K” data blocks

Step 03: Add the carry bit if it exists.

Step 04: Find the 1st Complement

The result after 4th step, Checksum, is ready to append with data.

2. Checksum at the Receiver Side

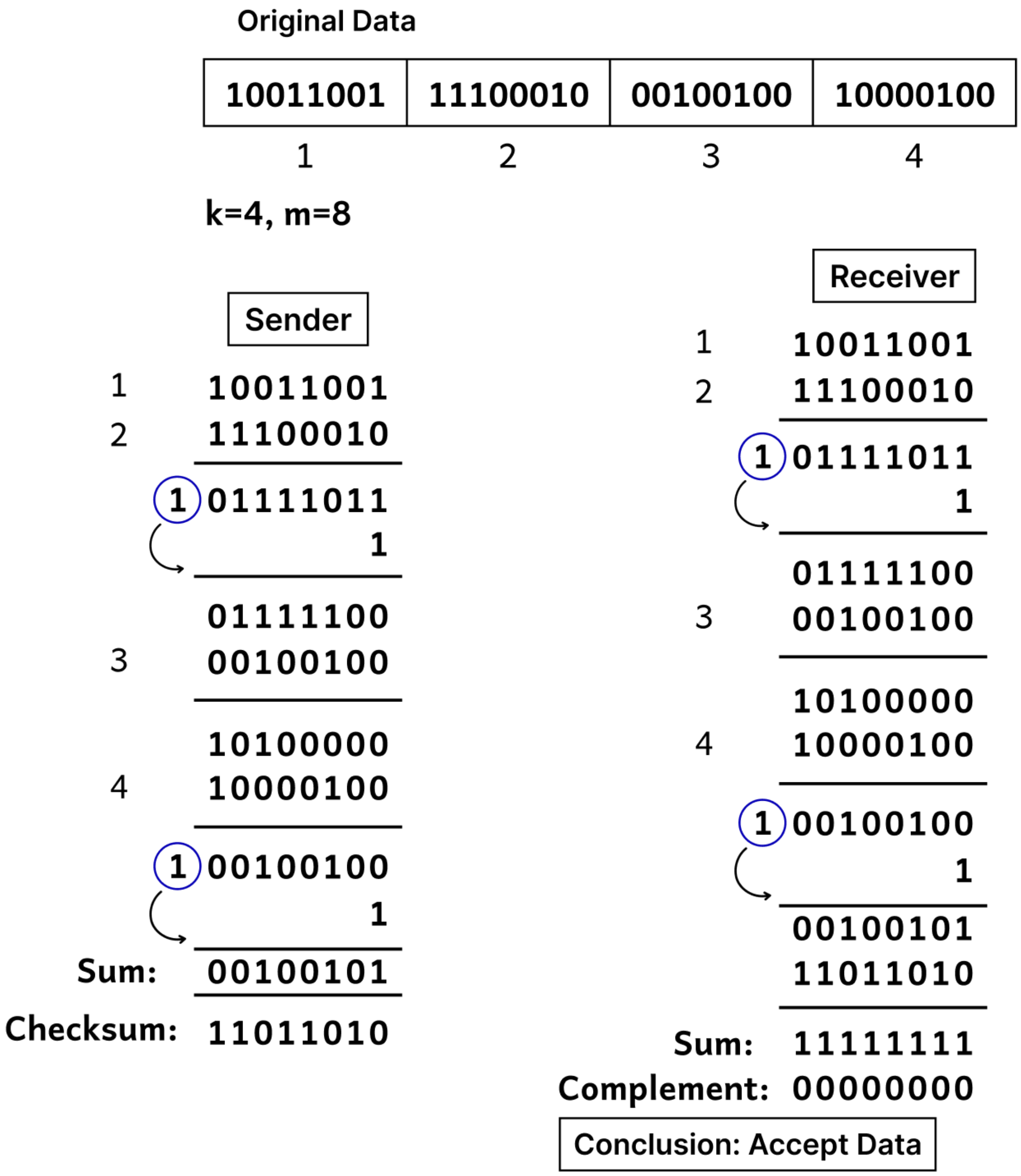
For validation of data at the sender side, follow the following steps

Step 01: Sum all the “K” data blocks and Checksum

Step 02: Add carry bits if any

Step 03: If the result is all 1s, ACCEPT data; otherwise, REJECT the data.

Consider the data unit 100110011110001000100100100000100. Now apply the above steps



Original Data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

Sender

```
1            10011001
2            11100010
           ----------
         (1) 01111011
                    1
           ----------
             01111100
3            00100100
           ----------
             10100000
4            10000100
           ----------
         (1) 00100100
                    1
           ----------
Sum:         00100101
           ----------
Checksum:    11011010
```

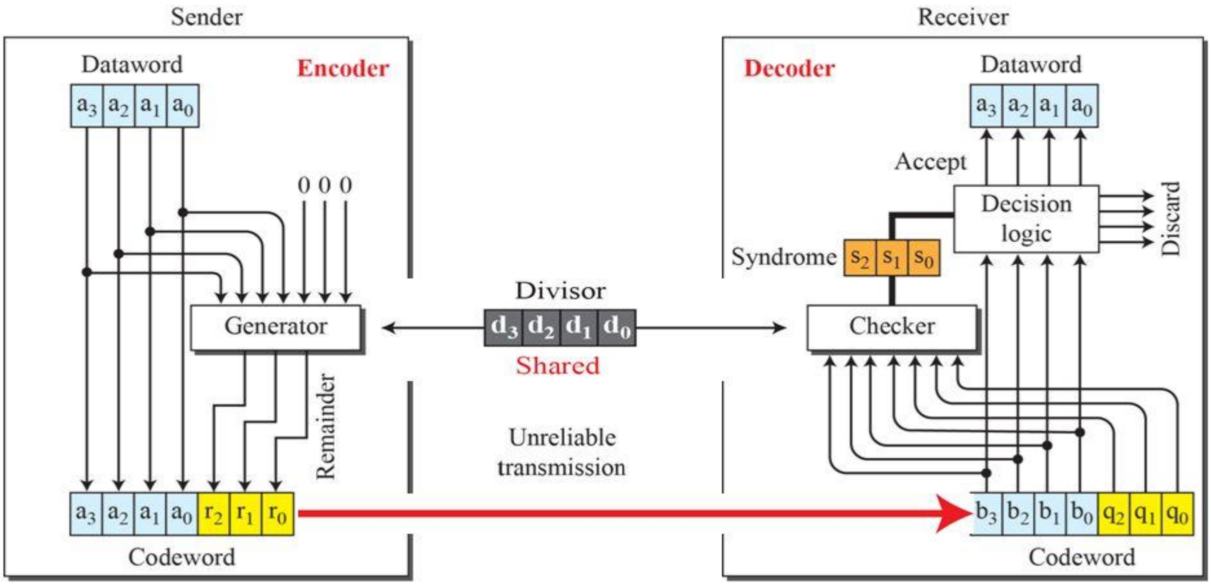
Receiver

```
1            10011001
2            11100010
           ----------
         (1) 01111011
                    1
           ----------
             01111100
3            00100100
           ----------
             10100000
4            10000100
           ----------
         (1) 00100100
                    1
           ----------
             00100101
             11011010
           ----------
Sum:         11111111
Complement:  00000000
```

Conclusion: Accept Data

Cyclic Redundancy Check (CRC): CRC is an error-checking technique used in computer networks to detect data transmission errors. It involves appending a fixed-size, checksum value to the data, which the receiver recalculates upon arrival; if the calculated and received values differ, an error is detected, triggering retransmission. CRC is based on binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of a data unit such as byte.

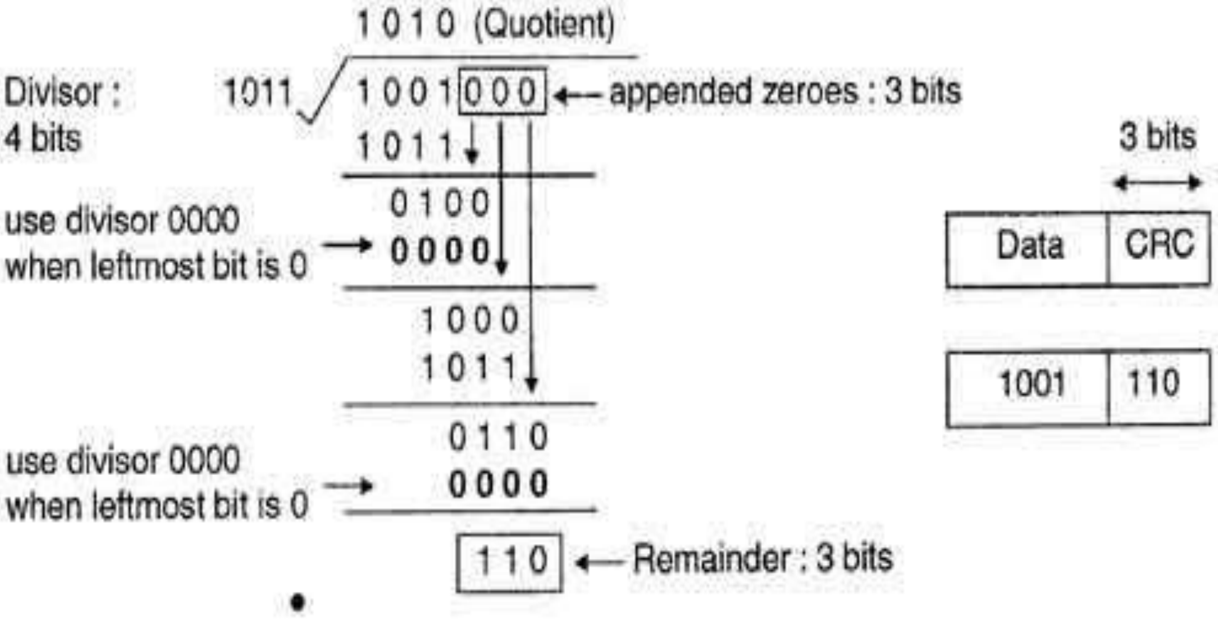
Figure : CRC encoder and decoder



10.13

Suppose we want to transmit the message 1001and protect it from errors using the CRC polynomial x^3+x+ 1. Use polynomial long division to determine the message that should be transmitted.

1. Data unit 1011000 is divided by 1011



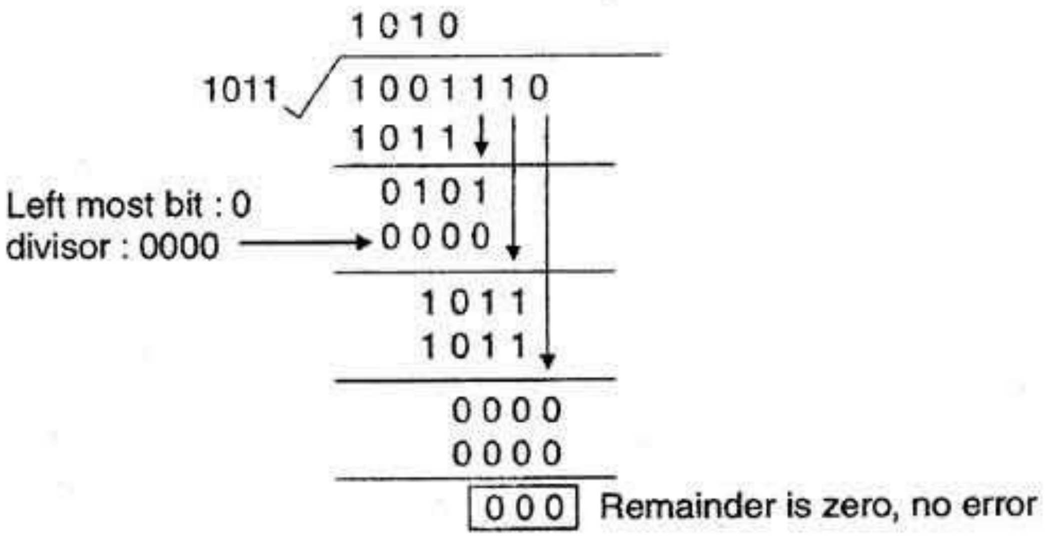
CRC generated (Binary division)

2. During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.

3. At the receiver side, data received is 1001110.

4. This data is again divided by a divisor 1011.

5. The remainder obtained is 000; it means there is no error.



CRC decoded (binary division)

CRC can detect all the burst errors that affect an odd number of bits.
The probability of error detection and the types of detectable errors depends on the choice of divisor.

High-level Data Link Control (HDLC)

With the increased exchange of multiple information and data units across distinct network models, the need for High-Level Data Link Control (HDLC) protocol arises in the network channel. The HDLC protocols are a part of the data link layer and are applied between multiple endpoints or nodes in a communication channel.

HDLC is a protocol of the data link layer. Since it works at the data link layer, it organizes the data in the form of frames. HDLC is a bit-oriented protocol and is applicable for point-to-point and multipoint connections.

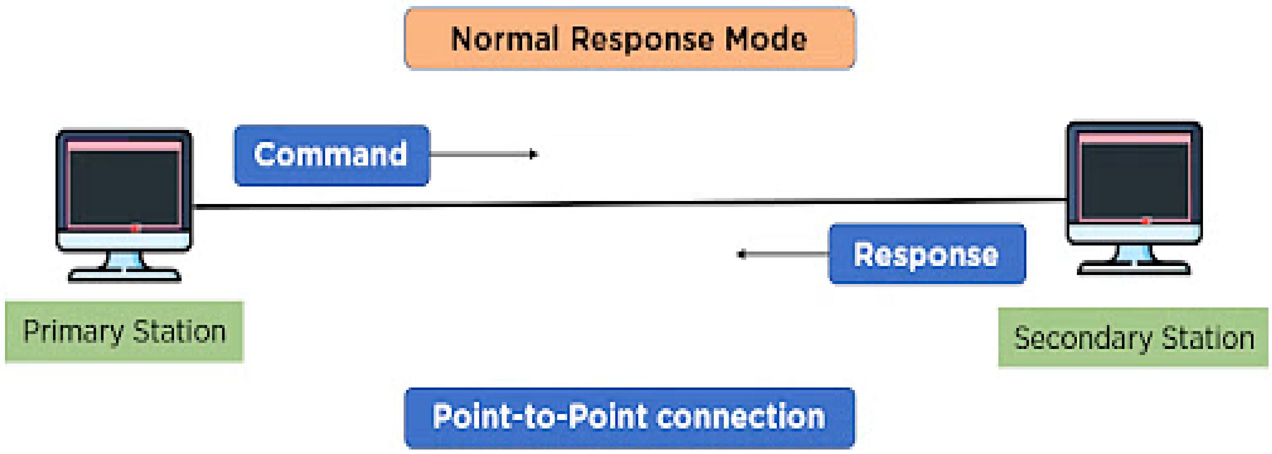
- Flag bytes with bit stuffing, a well-known framing method, were created only for the HDLC protocol.
- Generally, HDLC is a set of protocols of the data link layer that ensure communication for transmitting frames between network devices.
- HDLC implements Automatic Repeat Request (ARQ) in the sliding window protocol. Automatic Repeat Request (ARQ) is a technique to resend lost or damaged frames.

HDLC Transfer Modes

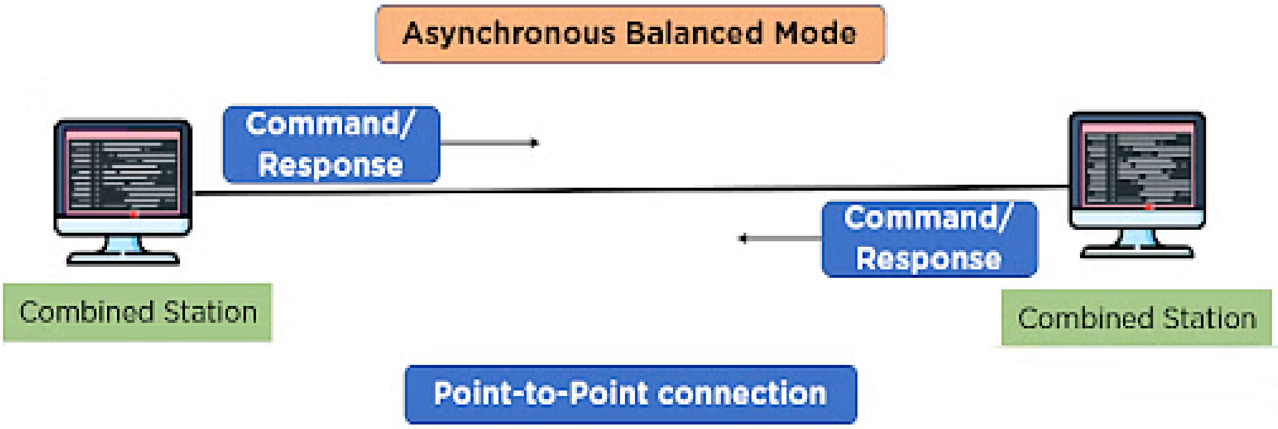
Two types of transfer modes are provided by HDLC that can be used in various configurations:

1. Normal Response Mode (NRM)
2. Asynchronous Balanced Mode (ABM)

Normal Response Model (NRM) - This transfer model combines primary and secondary stations in point-to-point or multipoint network configurations to exchange commands from primary stations and responses from secondary stations.

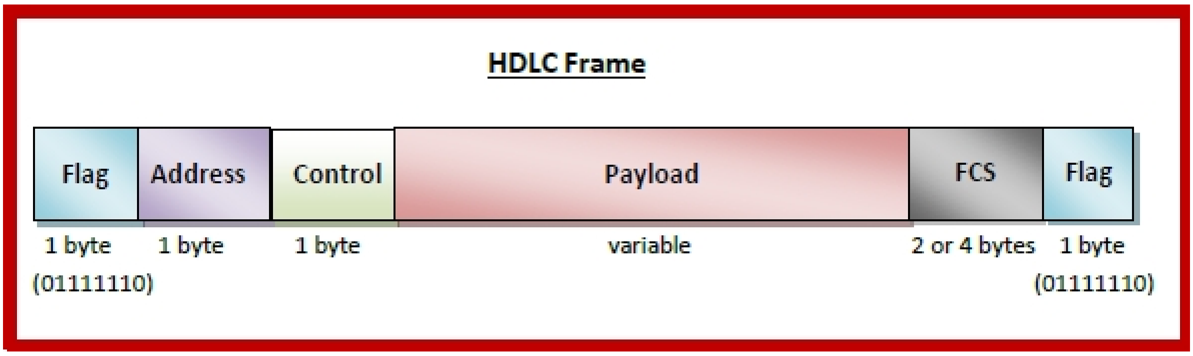


Asynchronous Balanced Model (ABM) - In this transfer model, combined stations are installed in a point-to-point configuration for exchange commands and responses in a balanced format.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are –



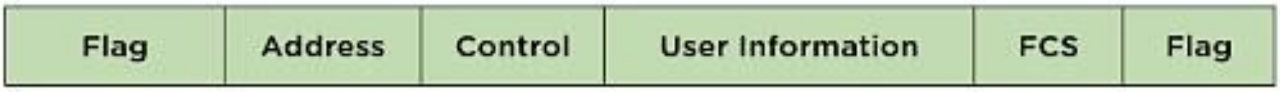
- Flag – It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- Address – It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- Control – It is 1- or 2-bytes containing flow and error control information.
- Payload – This carries the data from the network layer. Its length may vary from one network to another.
- FCS – It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

Types of HDLC Frames

Information Frames (I-Frames)
Supervisory Frames (S-Frames)
Unnumbered Frames (U-Frames)

.

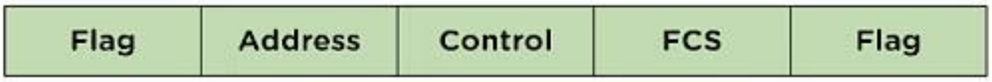
Information frame or I-frame is applied to encapsulate the user information from the upper layer in the model and then transmit it in the network channel and contains 0 in the control field.



Flag	Address	Control	User Information	FCS	Flag

I-Frame Format

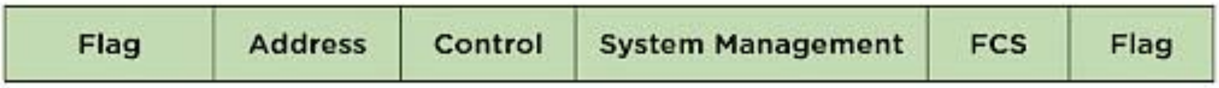
S-Frame - The supervisory frame or S-frames are used for error and data flow control and do not contain the information field in the frame format. The control field is 1 and 0 for the first two bits.



Flag	Address	Control	FCS	Flag

S-Frame Format

U-Frame - The un-numbered frame or U-frames are used for system management and exchanging control information between the connected network devices.



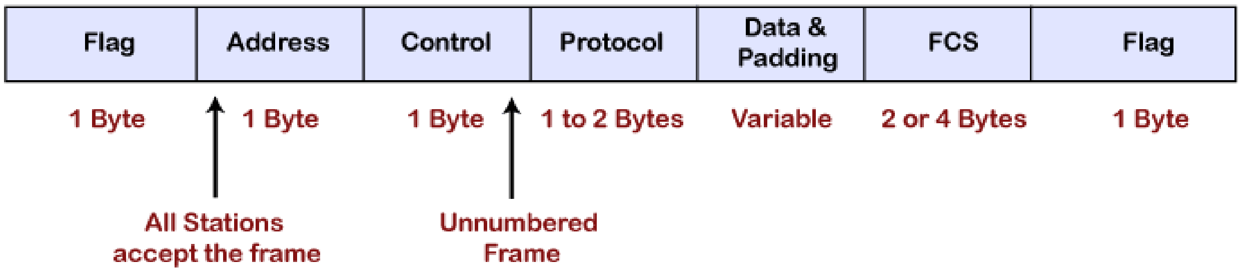
Flag	Address	Control	System Management	FCS	Flag

U-Frame Format

Point-to-Point Protocol (PPP)

The Point-to-Point Protocol (PPP) directly connects two network devices at the data link layer. It is typically used for internet connections and connecting remote networks via a Wide Area Network (WAN) link. PPP is adaptable, working with different physical layers protocols like serial lines, ISDN, and DSL

Frame format of PPP protocol



Flag: The flag field is used to indicate the start and end of the frame. The flag field is a 1-byte field that appears at the beginning and the ending of the frame. The pattern of the flag is similar to the bit pattern in HDLC, i.e., 01111110.

Address: It is a 1-byte field that contains the constant value which is 11111111. These 8 ones represent a broadcast message.

Control: It is a 1-byte field which is set through the constant value, i.e., 11000000. It is not a required field as PPP does not support the flow control and a very limited error control mechanism. The control field is a mandatory field where protocol supports flow and error control mechanism.

Protocol: It is a 1 or 2 bytes field that defines what is to be carried in the data field. The data can be a user data or other information.

Payload: The payload field carries either user data or other information. The maximum length of the payload field is 1500 bytes.

Checksum: It is a 16-bit field which is generally used for error detection.

PPP Architecture

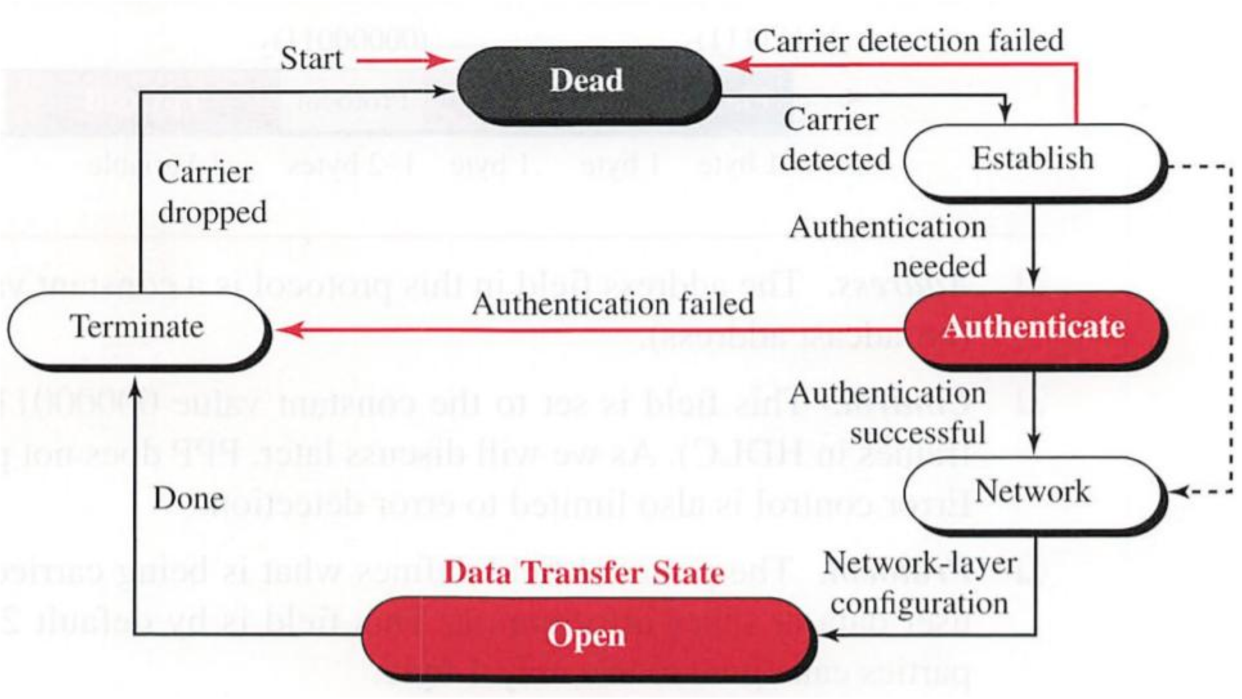
PPP is a layered protocol that operates at the data link layer of the OSI (Open Systems Interconnection) model. The PPP protocol consists of a layered protocol with three primary components:

- The Link Control Protocol (LCP): responsible for establishing, configuring, and testing the link between the two devices. It negotiates link parameters like the maximum frame size and compression type while monitoring the link for errors and drops
- The Authentication Protocol (AP): responsible for verifying the identities of the two devices using a range of authentication methods, including passwords, digital certificates, and biometrics
- The Network Control Protocol (NCP): responsible for negotiating the network layer protocol used to transmit data over the connection, supporting a variety of network layer protocols such as IP, IPX, and AppleTalk

Transition phases of PPP protocol

Dead: Dead is a transition phase which means that the link is not used or there is no active carrier at the physical layer.

Establish: If one of the nodes starts working then the phase goes to the establish phase. In short, we can say that when the node starts communication or carrier is detected then it moves from the dead to the establish phase.



Authenticate: It is an optional phase which means that the communication can also moves to the authenticate phase. The phase moves from the establish to the authenticate phase only when both the communicating nodes agree to make the communication authenticated.

Network: Once the authentication is successful, the network is established or phase is network. In this phase, the negotiation of network layer protocols take place.

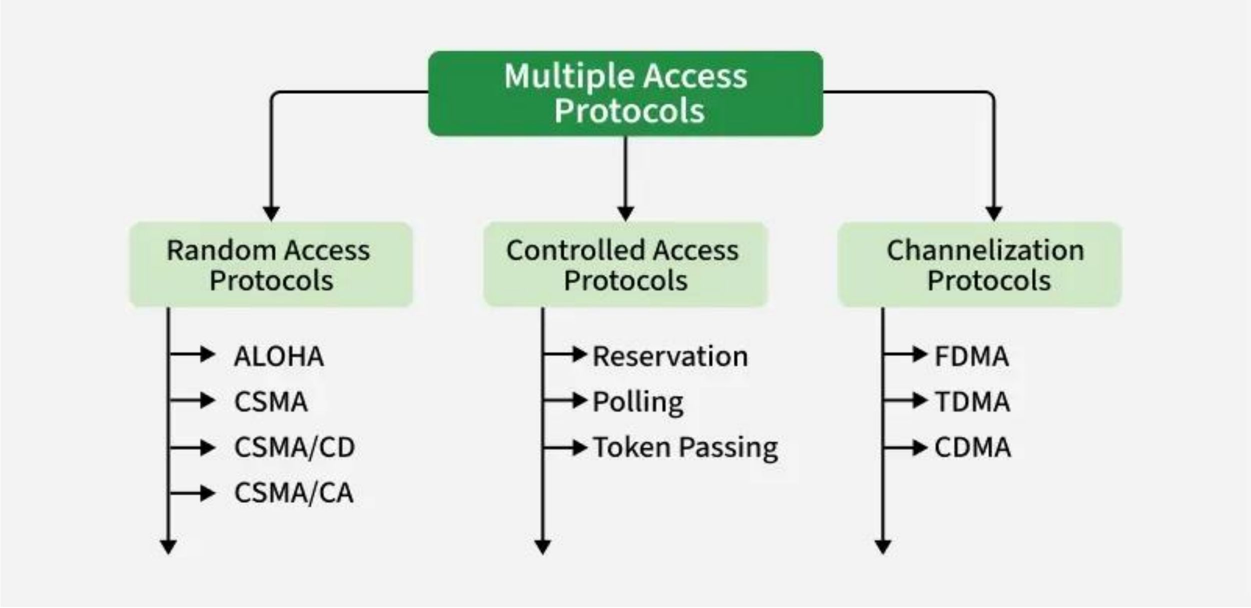
Open: After the establishment of the network phase, it moves to the open phase. Here open phase means that the exchange of data takes place. Or we can say that it reaches to the open phase after the configuration of the network layer.

Terminate: When all the work is done then the connection gets terminated, and it moves to the terminate phase

Multiple Access Protocols:

Multiple access protocols are methods used to manage data transmission in networks where multiple devices share the same communication channel. These protocols ensure that data is transmitted efficiently without collisions or interference. Without these protocols, network communication would face significant challenges, such as data loss, inefficiency, and system failures. By organizing how devices share resources, these protocols enable smooth and error-free communication.

- **Channel Sharing**: Facilitates multiple users accessing the same network medium.
- **Collision Management**: Reduces or resolves data collisions.
- **Efficiency**: Maximizes bandwidth utilization.



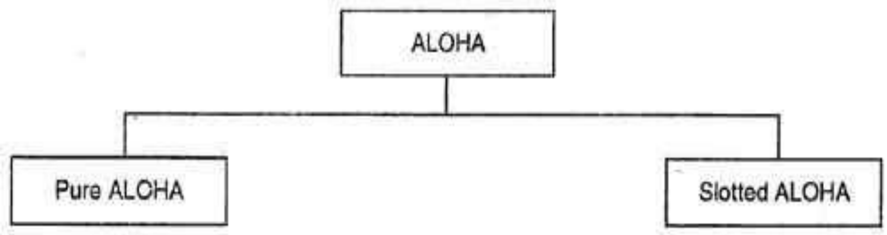
Random Access Protocol:

In random access, no device is superior to any other device connected to a channel, and no device has control over the other device. Any device can transmit whenever it wants, so the transmission between devices is random. Hence, these methods are known as random access.

- At any time, the device uses the protocol when it wants to send a frame. Depending on the protocol, the device will decide whether to send or not.
- Here, there is no scheduled time for a device to transmit the frame. Transmission occurs randomly over a channel between devices.
- In random access, there is no rule as to which device is next to send the frame. So, the devices compete with each other to access the channel to transmit the frame.
- Frames will either be lost or modified if more than one device sends over a shared channel. So, devices use a protocol to overcome this problem

ALOHA is an early random-access protocol used in computer networks. The basic operation of the ALOHA protocol is as follows:

- Devices can transmit data whenever they have a message to send
- If two or more devices transmit simultaneously, their messages will collide and be corrupted
- Devices that detect a collision will wait for a random amount of time before trying to transmit again



Types of ALOHA

Pure ALOHA

We use Pure Aloha whenever data is available for sending over a channel at stations. When each station transmits data to a channel without first checking whether the channel is idle or not, there is a risk of collision and the data frame being lost in pure Aloha.

Controlled Access Protocol.

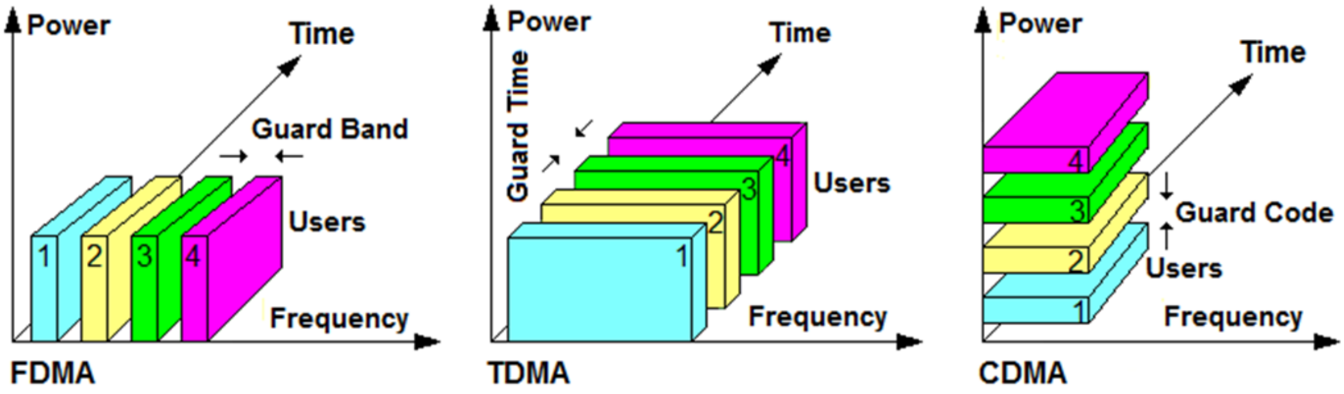
In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation,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

Channelization Protocols:

It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

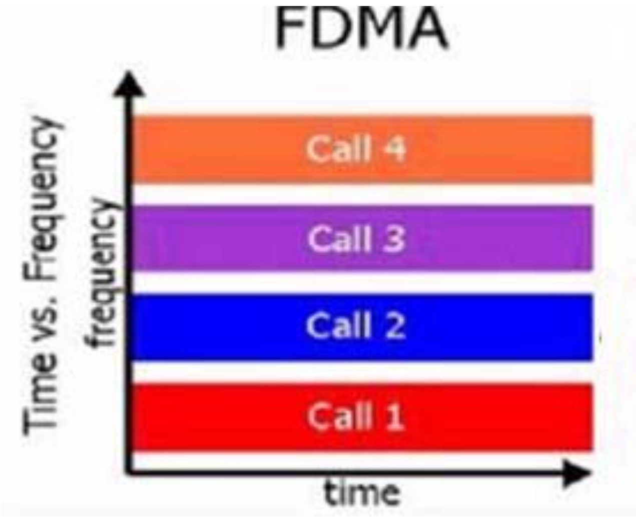
Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)



FDMA (Frequency Division Multiple Access)

FDMA works by dividing the frequency spectrum into separate channels or frequency bands. Each user or data stream is allocated a unique frequency band for communication. The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise. Users transmit and receive data using their assigned frequency band, ensuring minimal interference with other users.



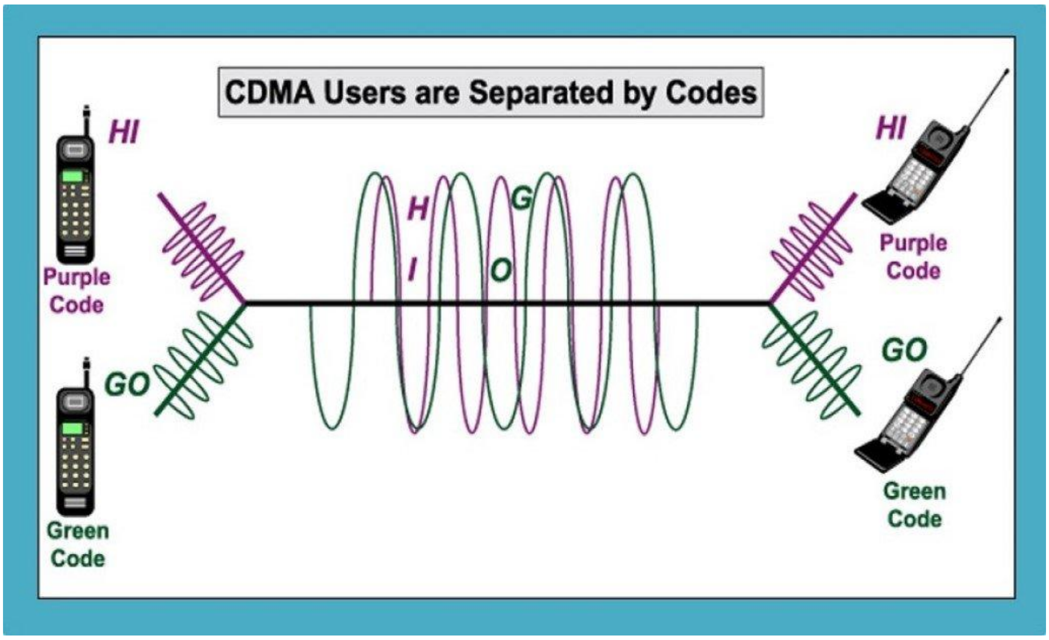
FDMA divides the given spectrum into channels by the frequency domain. Each phone call is allocated one channel for the entire duration of the call. In the above, each band represents one call.

TDMA (Time Division Multiple Access)

Time serves as the channel resource for this protocol. Using the TDMA protocol, we divide each user's signal into a different time slot and assign each time slot to a different user. This technique enables numerous users to share and use the same frequency channel. The global system of mobile communication (GSM) system, a 2G cellular system, is one significant application where we have used the TDMA protocol.

Code Division Multiple Access (CDMA) Protocol

The channel resource for this protocol is code. In the CDMA protocol, we allow multiple users to simultaneously transmit their data signals over the entire bandwidth of the common channel by assigning unique spreading codes to each user. This technique helps us utilize the channel more effectively. In CDMA, we use the spread spectrum principle to utilize unique transmission codes.



Spread spectrum is a technique that enables us to transfer signals via communication channels by purposefully extending the signal’s bandwidth beyond what is necessary for transmission