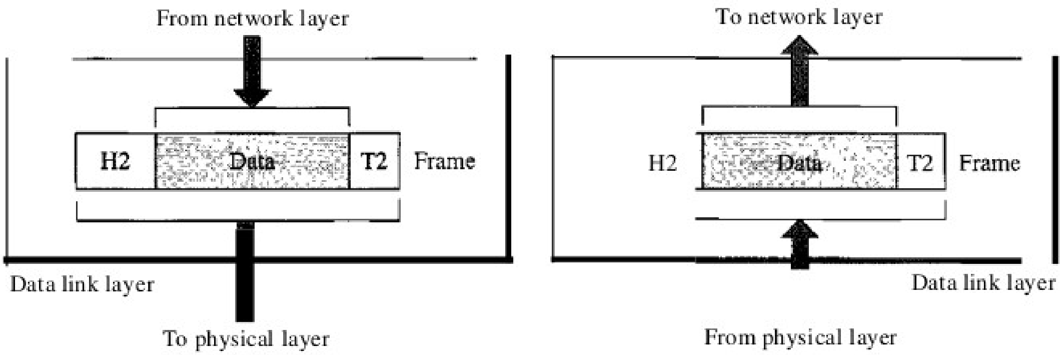
Module 4: The Data Link Layer

- Design Issues in Data Link Layer
- Framing–Concept
- Methods–Character Count, Flag bytes with Byte Stuffing, Starting & ending Flags with Bit Stuffing, Physical Layer Coding Violations
- Flow and Error Control, Error detection code CRC

- **Data Link Layer :**

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

Following figure shows the relationship of the data link layer to the network and physical layers.



The data link layer is responsible for moving frames from one hop (node) to the next.

Other responsibilities of the data link layer include the following:

Framing. The data link layer divides the stream of bits received from the network

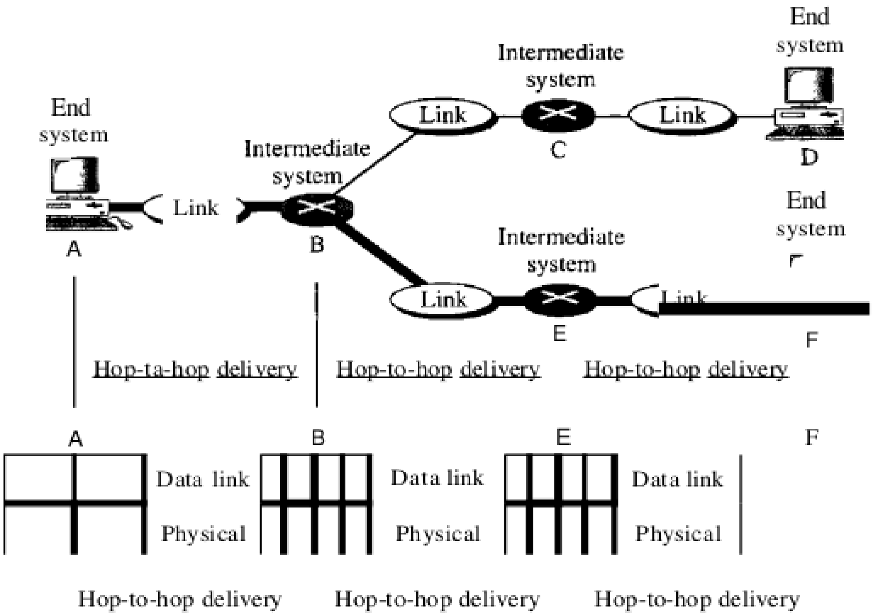
layer into manageable data units called frames. Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

Flow control. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

Access control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Following figure illustrates hop-to-hop (node-to-node) delivery by the data link layer.



As the figure shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made.

First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F. Note that the frames that are exchanged between the three nodes have different values in the headers.

The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of the frame.

- The two main functions of the data link layer are data link control and media access control. The first, data link control, deals with the design and procedures for communication between two adjacent nodes: node-to-node communication.

- Data link control functions include framing, flow and error control, and software-implemented protocols that provide smooth and reliable transmission of frames between nodes.

Data-link layer is the second layer after the physical layer. The data link layer is responsible for maintaining the data link between two hosts or nodes.
Before going through the design issues in the data link layer. Some of its sub-layers and their functions are as following below.

The data link layer is divided into two sub-layers :

1. **Logical Link Control Sub-layer (LLC) –** Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer. Functions are –

(i) Error Recovery.
(ii) It performs the flow control operations.
(iii) Useraddressing.

2. **Media Access Control Sub-layer (MAC) –** It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card. Functions are –

(i) To perform the control of access to media.
(ii) It performs the unique addressing to stations directly connected to LAN.
(iii) Detection of errors.

Design issues with data link layer are:

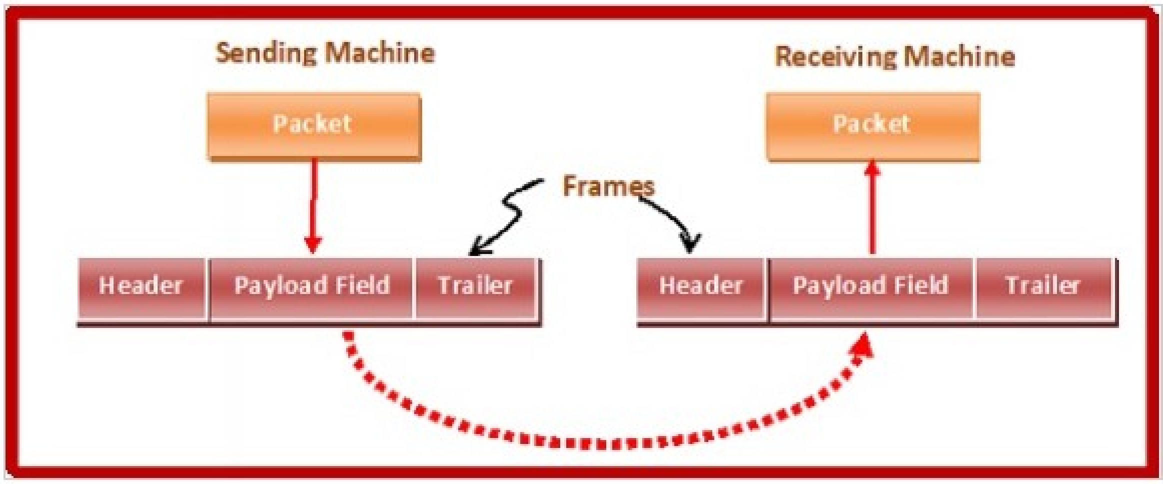
1. **Services provided to the network layer –** The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on

sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).

2. **Frame synchronization –** The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.
3. **Flow control –** Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.
4. **Error control –** Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Framing – Concept

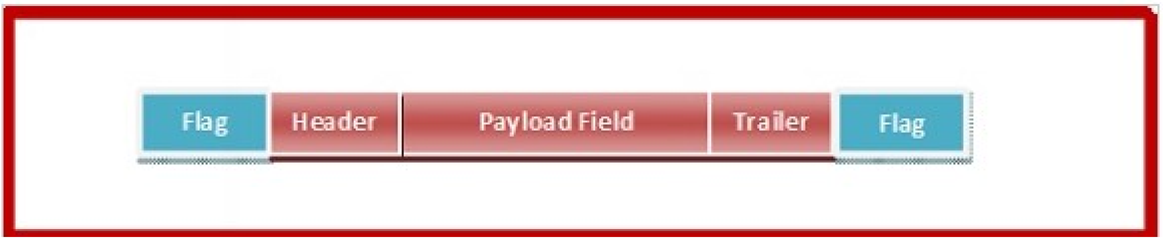
- Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing.
- The data link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another.
- Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.
- Although the whole message could be packed in one frame, that is not normally done. One reason is that a frame can be very large, making flow and error control very inefficient.
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole message. When a message is divided into smaller frames, a single-bit error affects only that small frame.



Parts of a Frame

A frame has the following parts −

Frame Header − It contains the source and the destination addresses of the frame.
Payload field − It contains the message to be delivered.
Trailer − It contains the error detection and error correction bits.
Flag − It marks the beginning and end of the frame.



Problems in Framing

- **Detecting start of the frame:** When a frame is transmitted, every station must be able to detect it. Station detects frames by looking out for a special sequence of bits that marks the beginning of the frame i.e. SFD (Starting Frame Delimiter).

- **How does the station detect a frame:** Every station listens to link for SFD pattern through a sequential circuit. If SFD is detected, sequential circuit alerts station. Station checks destination address to accept or reject frame.

- **Detecting end of frame:** When to stop reading the frame.

Types of Framing

1. Fixed-Size Framing

In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.

2. Variable- Size Framing

In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

Two ways to define frame delimiters in variable sized framing are −

- **Length Field −** Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).
- **End Delimiter −** Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situation −
    - **Byte – Stuffing −** A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.
    - **Bit – Stuffing −** A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

Methods of Framing

There are basically four methods of framing as given below.

1. Character Count
2. Flag Byte with byte stuffing
3. Starting and Ending Flags, with bit stuffing
4. Physical Layer coding violations.

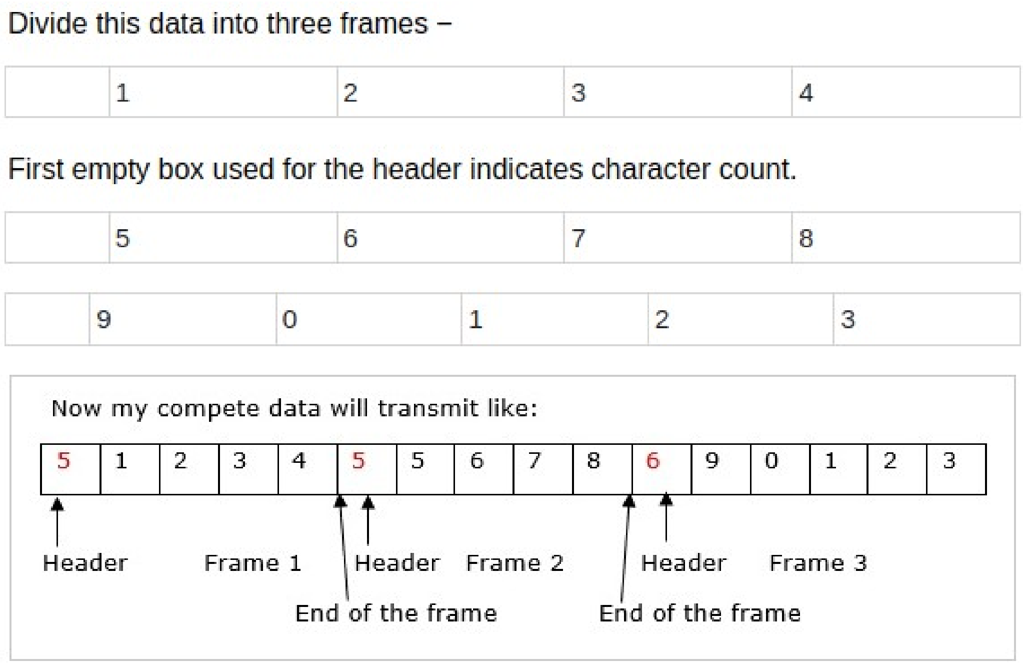
1. **Character Count :**
   - This method is rarely used and is generally required to count total number of characters that are present in frame. This is be done by using field in header. Character count method ensures data link layer at the receiver or destination about total number of characters that follow, and about where the frame ends.

   - There is disadvantage also of using this method i.e, if anyhow character count is disturbed or distorted by an error occurring during transmission, then destination or receiver might lose synchronization. The destination or receiver might also be not able to locate or identify beginning of next frame.

   - First framing method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is.

Example:

Consider a data – 1234567890123



Divide this data into three frames –

	1	2	3	4

First empty box used for the header indicates character count.

	5	6	7	8

	9	0	1	2	3

Now my compete data will transmit like:

5	1	2	3	4	5	5	6	7	8	6	9	0	1	2	3

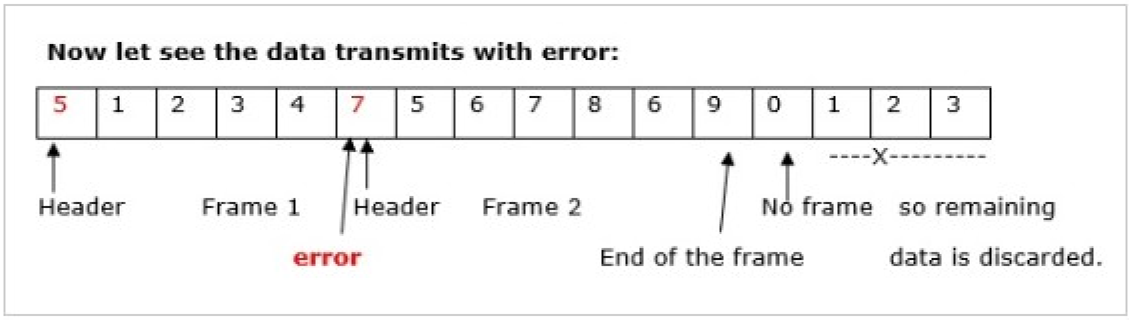
Explanation

Step 1 − Starting header in the frame indicate the character count, so first frame consists of 5 units of data including that number,

Step 2 − Second frame header consists of 5 units of data including that number, so second frame consists of data 5,6,7,8. 8 indicate the end of the frame here.

Step 3 − Third frame header consists of character count 6 that means the frame consists of 6 characters including 6. So the data in the third frame is 9,0,1,2,3.

Step 4 − My data transfer to the receiver side without any errors.



Now let see the data transmits with error:

Explanation

Step 1 − Starting header in the frame indicates the character count, so the first frame consists of 5 units of data including that number.

Step 2 − Second frame header consists of 7 character count including that number actually it is an error, even though error is there the data will be transmitted, so second frame consists of data 5,6,7,8,6,9. Here, 9 indicate the end of the frame here.

Step 3 − Third frame header consists of character count 0 that means the frame consists of 0 characters. The last frame data is discarded.

Step 4 − My data transfer to the receiver side with errors.

2. Flag Byte with byte stuffing

Data link layer is responsible for something called Framing, which is the division of stream of bits from the network layer into manageable units (called frames). Each frame consists of the sender's address and a destination address. The destination address defines where the packet is to go and the sender's address helps the recipient acknowledge the receipt.

Frames could be of fixed size or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames as the size itself can be used to define the end of the frame and the beginning of the next frame. But, in variable-size framing, we need a way to define the end of the frame and the beginning of the next frame.

To separate one frame from the next, an 8-bit (or 1-byte) flag is added at the beginning and the end of a frame. But the problem with that is, any pattern used for the flag could also be part of the information. So, there are two ways to overcome this problem:

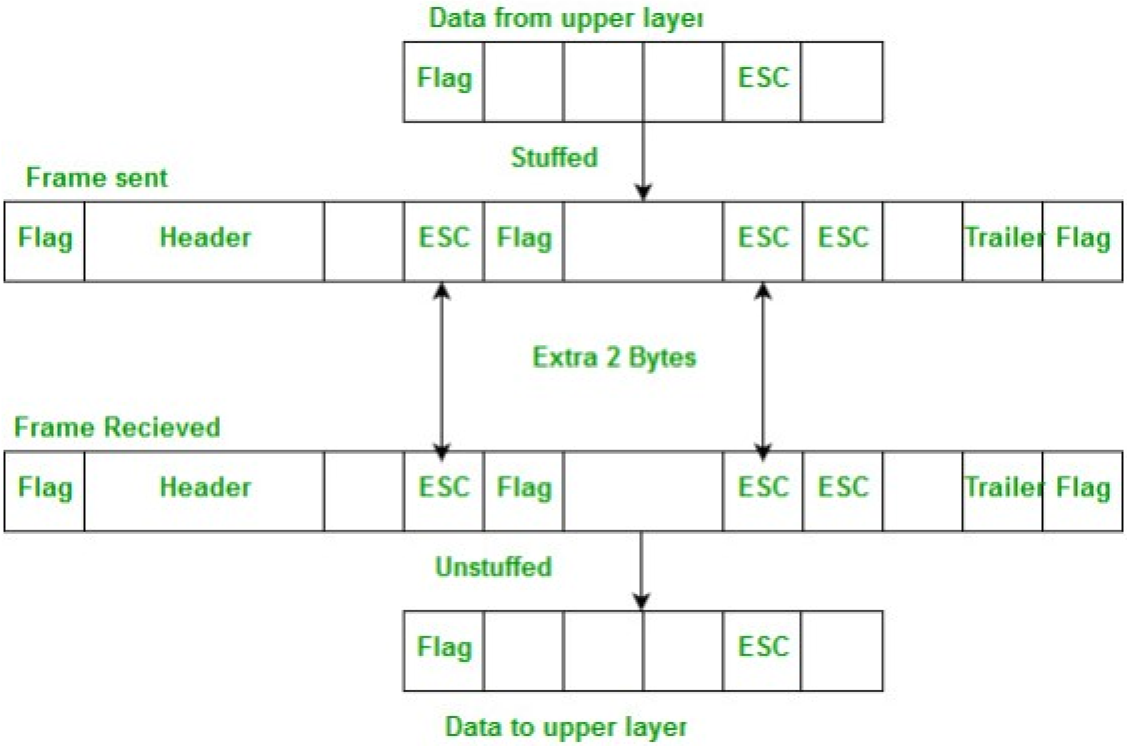
1.Using Byte stuffing (or character stuffing)

2.Using Bit stuffing

1. Using Byte stuffing

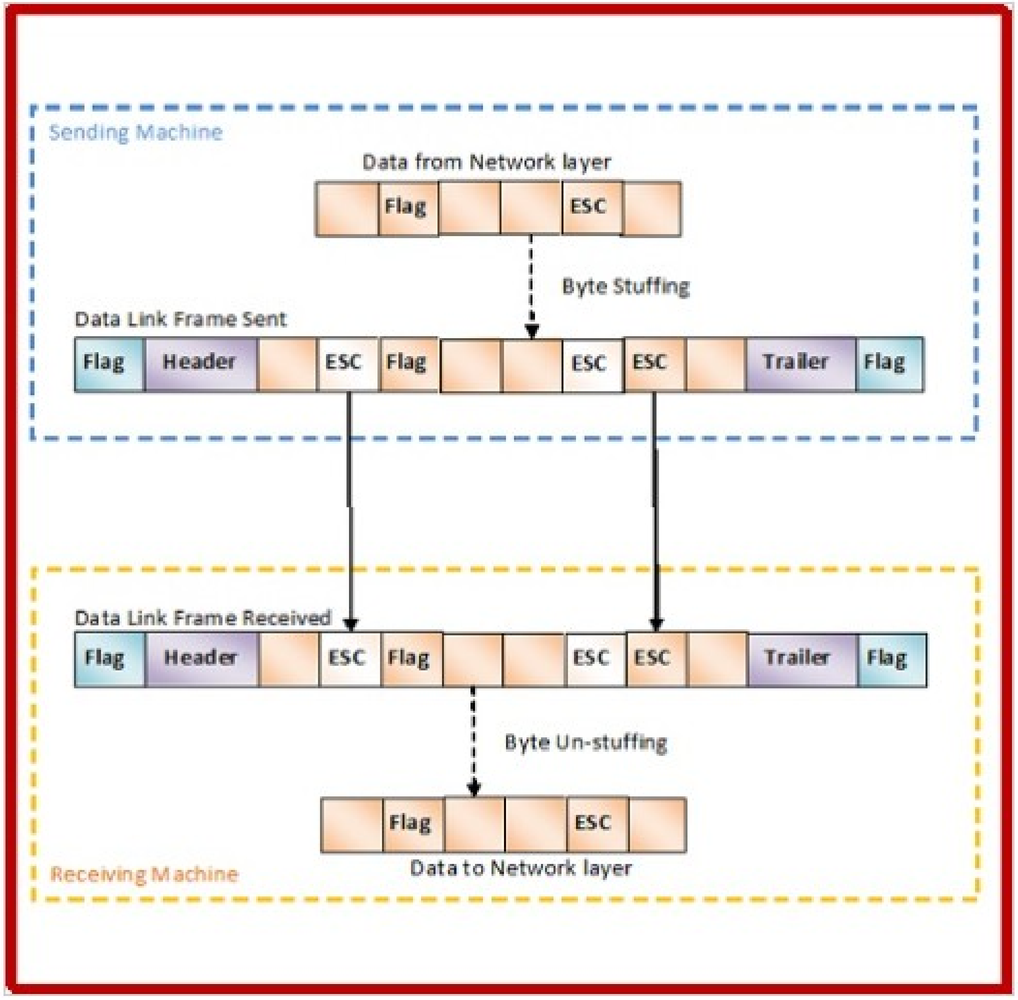
A byte (usually escape character (ESC)), which has a predefined bit pattern is added to the data section of the frame when there is a character with the same pattern as the flag. Whenever the receiver encounters the ESC character, it removes from the data section and treats the next character as data, not a flag.

But the problem arises when the text contains one or more escape characters followed by a flag. To solve this problem, the escape characters that are part of the text are marked by another escape character i.e., if the escape character is part of the text, an extra one is added to show that the second one is part of the text.



Note – Point-to-Point Protocol (PPP) is a byte-oriented protocol.

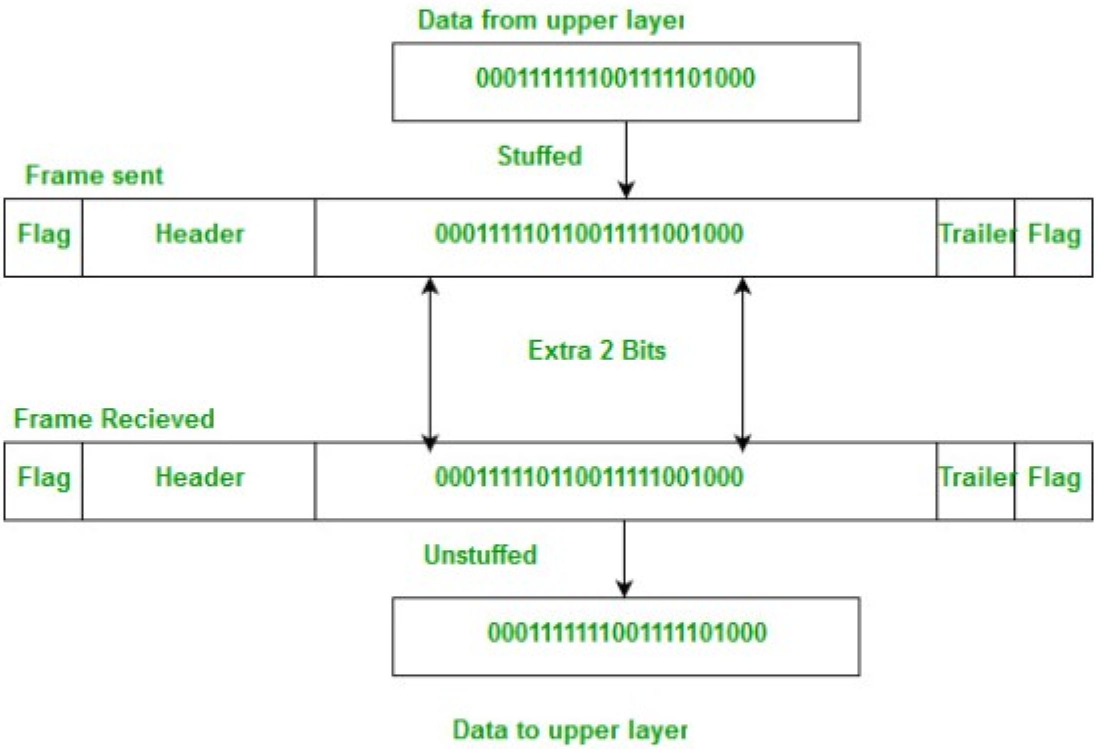
In byte stuffing, a special byte called the escape character (ESC) is stuffed before every byte in the message with the same pattern as the flag byte. If the ESC sequence is found in the message byte, then another ESC byte is stuffed before it.



3. Bit stuffing –

Mostly flag is a special 8-bit pattern “01111110” used to define the beginning and the end of the frame. Problem with the flag is the same as that was in case of byte stuffing. So, in this protocol what we do is, if we encounter 0 and five consecutive 1 bits, an extra 0 is added after these bits. This extra stuffed bit is removed from the data by the receiver.

The extra bit is added after one 0 followed by five 1 bits regardless of the value of the next bit. Also, as the sender side always knows which sequence is data and which is flag it will only add this extra bit in the data sequence, not in the flag sequence.



Note – High-Level Data Link Control(HDLC) is a bit-oriented protocol.

4. Physical Layer Coding Violation

Encoding violation is method that is used only for network in which encoding on physical medium includes some sort of redundancy i.e., use of more than one graphical or visual structure to simply encode or represent one variable of data.

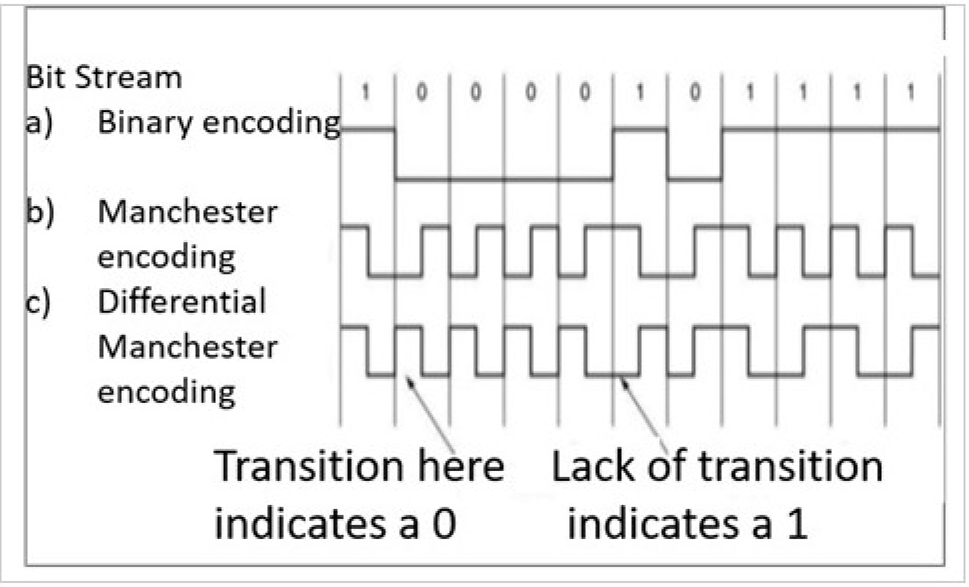
This framing method is used only in those networks in which encoding on the physical medium contain some redundancy.

Some LANs encode each bit of data by using two physical bits that Manchester coding uses.

Here, Bit 1 is encoded into a high-low (10) pair and Bit 0 is encoded into a low-high (01) pair.

The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries.

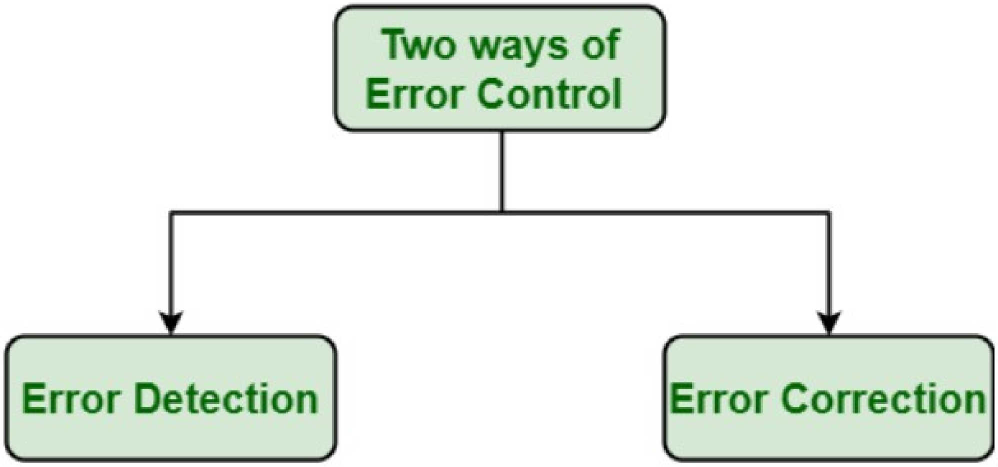
The combinations high-high and low-low are not used for data but are used for delimiting frames in some protocols.


Bit Stream
1 0 0 0 0 1 0 1 1 1 1
a) Binary encoding
b) Manchester encoding
c) Differential Manchester encoding
Transition here indicates a 0
Lack of transition indicates a 1

Flow and Error Control, Error detection

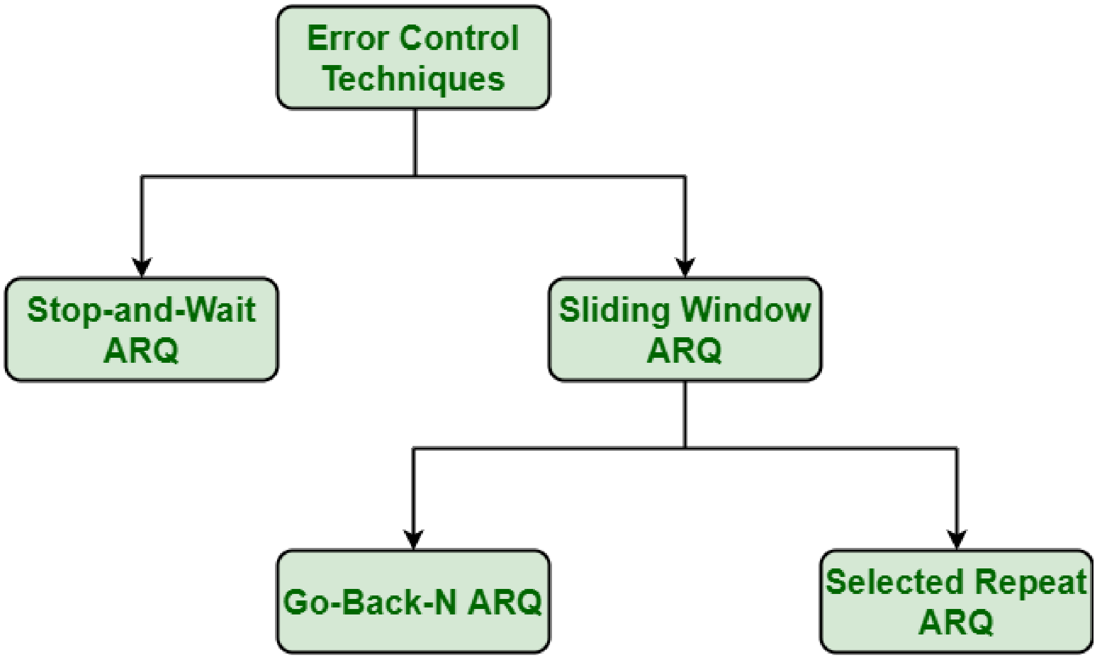
- Data-link layer uses the techniques of error control simply to ensure and confirm that all the data frames or packets, i.e. bit streams of data, are transmitted or transferred from sender to receiver with certain accuracy.

- Using or providing error control at this data link layer is an optimization, it was never requirement.
- Error control is basically process in data link layer of detecting or identifying and re-transmitting data frames that might be lost or corrupted during transmission.
- In both of these cases, receiver or destination does not receive correct data-frame and sender or source does not even know anything about any such loss regarding data frames.
- Therefore, in such type of cases, both sender and receiver are provided with some essential protocols that are required to detect or identify such type of errors like loss of data frames.
- The Data-link layer follows technique known as re-transmission of frames to detect or identify transit errors and also to take necessary actions that are required to reduce or remove such errors.
- Each and every time an effort is detected during transmission, particular data frames retransmitted and this process is known as ARQ (Automatic Repeat Request).



Ways of Error Control

1. Error Detection :Error detection, as name suggests, simply means detection or identification of errors. These errors may cause due to noise or any other impairments during transmission from transmitter to the receiver, in communication system. It is class of technique for detecting garbled i.e. unclear and distorted data or message.
2. Error Correction :Error correction, as name suggests, simply means correction or solving or fixing of errors. It simply means reconstruction and rehabilitation of original data that is error-free. But error correction method is very costly and is very hard.



1. Stop-and-Wait ARQ : Stop-and-Wait ARQ is also known as alternating bit protocol. It is one of simplest flow and error control techniques or mechanisms. This mechanism is generally required in telecommunications to transmit data or information among two connected devices. Receiver simply indicates its readiness to receive data for each frame. In these, sender sends information or data packet

to receiver. Sender then stops and waits for ACK (Acknowledgment) from receiver. Further, if ACK does not arrive within given time period i.e., time-out, sender then again resends frame and waits for ACK. But, if sender receives ACK, then it will transmit the next data packet to receiver and then again wait for ACK fro receiver. This process to stop and wait continues until sender has no data frame or packet to send.

2. Sliding Window ARQ : This technique is generally used for continuous transmission error control.

3. Go-Back-N ARQ : Go-Back-N ARQ is form of ARQ protocol in which transmission process continues to send or transmit total number of frames that are specified by window size even without receiving an ACK (Acknowledgement) packet from the receiver. It uses sliding window flow control protocol. If no errors occur, then operation is identical to sliding window.

4. Selective Repeat ARQ : Selective Repeat ARQ is also form of ARQ protocol in which only suspected or damaged or lost data frames are only retransmitted. This technique is similar to Go-Back-N ARQ though much more efficient than the Go-Back-N ARQ technique due to reason that it reduces number of retransmission. In this, the sender only retransmits frames for which NAK is received. But this technique is used less because of more complexity at sender and receiver and each frame must be needed to acknowledged individually.

1. Flow Control

It is an important function of the **Data Link Laye**. It refers to a set of procedures that tells the sender how much data it can transmit before waiting for acknowledgement from the receiver.

Purpose of Flow Control :
Any receiving device has a limited speed at which it can process incoming data and also a limited amount of memory to store incoming data. If the source is sending the data at a faster rate than the capacity of the receiver, there is a possibility of the receiver being swamped. The receiver will keep losing some of the frames simply because they are arriving too quickly and the buffer is also getting filled up.

This will generate waste frames on the network. Therefore, the receiving device must have some mechanism to inform the sender to send fewer frames or stop transmission temporarily. In this way, flow control will control the rate of frame transmission to a value that can be handled by the receiver.

2. Error Control

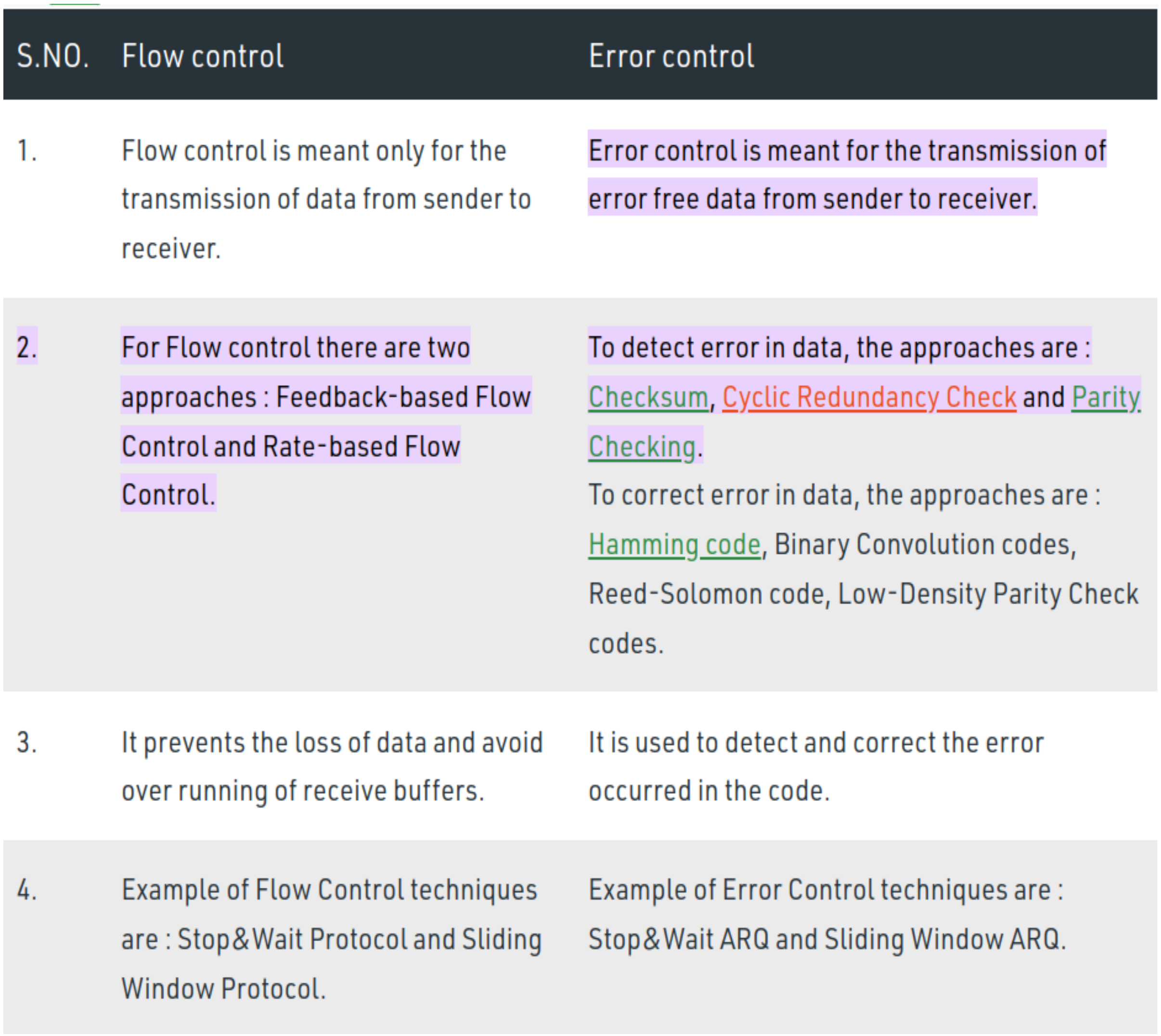
The error control function of data link layer detects the errors in transmitted frames and re-transmit all the erroneous frames.

Purpose of Error Control :

The function of the error control function of the data link layer helps in dealing with data frames that are damaged in transit, data frames lost in transit, and the acknowledgment frames that are lost in transmission.

The method used for error control is called Automatic Repeat Request which is used for the noisy channel.

Difference between Flow Control and Error Control :



S.NO.	Flow control	Error control
1.	Flow control is meant only for the transmission of data from sender to receiver.	Error control is meant for the transmission of error free data from sender to receiver.
2.	For Flow control there are two approaches : Feedback-based Flow Control and Rate-based Flow Control.	To detect error in data, the approaches are : Checksum, Cyclic Redundancy Check and Parity Checking. To correct error in data, the approaches are : Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes.
3.	It prevents the loss of data and avoid over running of receive buffers.	It is used to detect and correct the error occurred in the code.
4.	Example of Flow Control techniques are : Stop&Wait Protocol and Sliding Window Protocol.	Example of Error Control techniques are : Stop&Wait ARQ and Sliding Window ARQ.

References:

https://www.geeksforgeeks.org/design-issues-in-data-link-layer/

https://www.tutorialspoint.com/what-is-the-character-count-explain-with-an-example#

https://www.geeksforgeeks.org/difference-between-byte-stuffing-and-bit-stuffing/

https://www.geeksforgeeks.org/error-control-in-data-link-layer/

https://www.tutorialspoint.com/error-detection-and-correction-in-data-link-layer