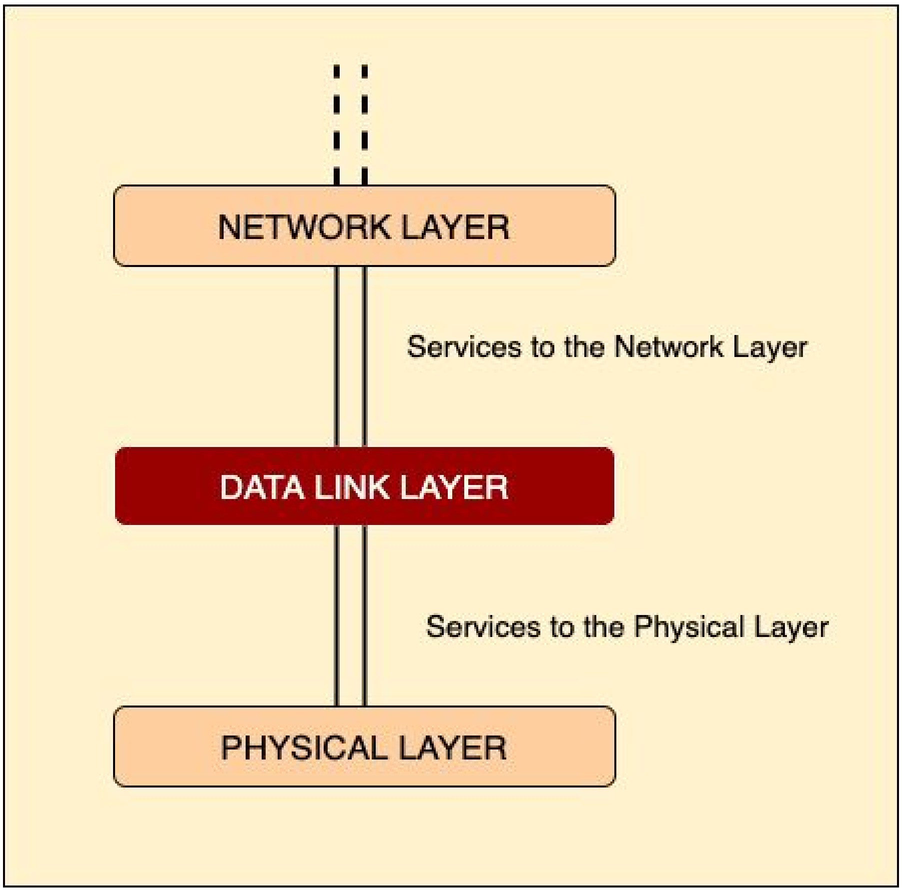
Discuss data link layer design issues

Data Link Layer Design Issues

The Data Link Layer is the second layer of the OSI Model, its function is to transmit data within a physical network link. It is also the most Complicated and Complex among all the Layers. The data link layer works between two hosts that are connected directly to each other in some way.

Services to the Network Layer

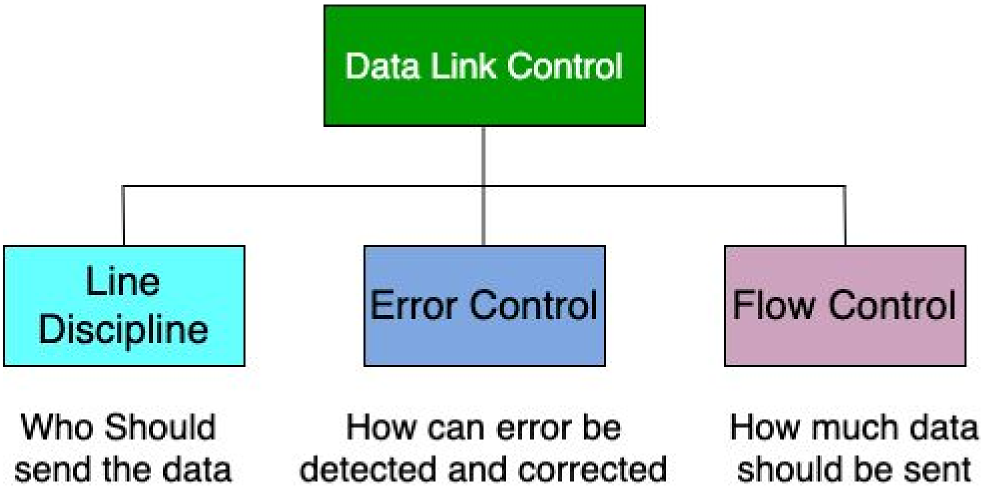
The Data Link Layer uses the services provided by the Physical Layer. The primary function of this layer is to provide a well defined service interface over the network layer.



The types of services provided can be of three types.

- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

The main functions and the design issues of this layer.



- Framing
- Error Control
- Error Detection Code
- Error Correcting Code
- Flow Control

1. Framing

The data link layer takes packages from the network layer and divides them into a few frames. Then it bit by bit sends all these frames to the hardware. The data link layer then takes the signals from the hardware and converts them into frames.

The Frame Contains

- Frame Header
- Payload field for holding packet
- Frame Trailer

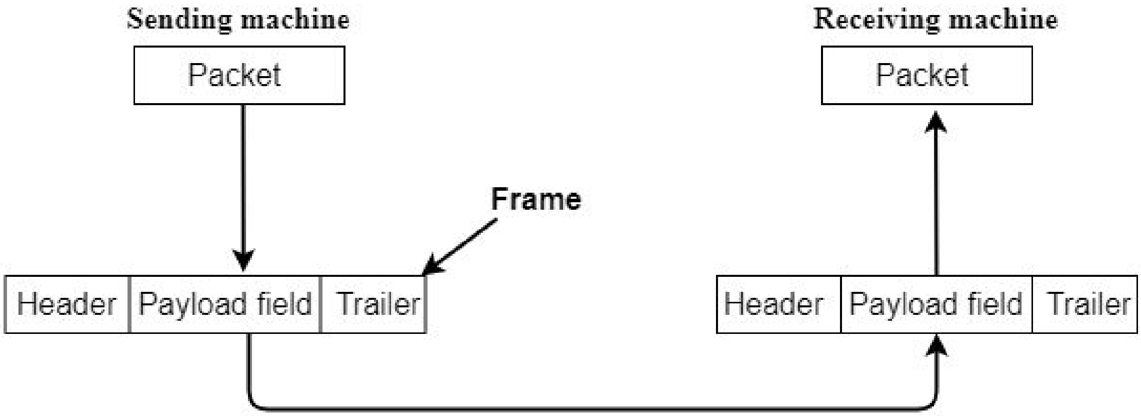


Fig :- Relationships Between Packets and Frames

2. Error Control

Error Control is a process when the receiver's information does not match the information of the sender. Then this process occurs. The Data Link Layer uses two methods to control the error.

- Error Detecting Code

  Whenever a message is transmitted, the data gets corrupted many times due to noise. To remove this problem, we use the Error Detection Code. In this process, it sends a digital data with Messege so that it can understand if there is an error in this Message.
- Error Correction Code

  We use this Process to remove the correct Message from the corrupt Message. We know such code by the name of Error Correcting Code. It also works to identify the correct location of corrupt Bit.

3. Flow Control

Flow control is a technique. Which allows the two stations to communicate with each other and work at different speeds. The data link layer regulates the flow control so that when a fast sender sends a data, a slow receiver can receive the data at the same speed. There are 2 common approaches to control flow, even if the transmission is error free.

- Feedback Based Flow Control
- Rate Based Flow Control

2)What is pure ALOHA and slotted ALOHA

In the computer networks, the devices access the common underlying shared medium (e.g LAN cable) to communicate. Aloha protocol provides an access control mechanism, for shared channel/medium. For example, a local area network connects multiple computers to each other over a common physical network, using wires, hubs, switches, routers, etc.

In other networks like peer to peer, no need for Aloha protocol, as there is no sharing of a medium, so no collision.

What is pure aloha and slotted aloha?

The first version of the aloha protocol is named Pure Aloha. After that, a more efficient version was developed which named slotted aloha. Both pure aloha and slotted aloha works for a shared broadcast network, as LAN or WiFi LAN.

What is Pure Aloha?

As the name suggests pure aloha is the original version of the aloha protocol.
Following is the procedure in pure aloha for communication.

- **When a network station needs to send the frame, it sends immediately and waits for the acknowledgment.**
- **If the sender receives an acknowledgment, the sender may send the next frame.**
- **If no acknowledgment sender assumes the frame has been garbled and retransmit the same frame after a random time to avoid collision again.**

What is slotted Aloha?

The next version of aloha, more efficient. The following describes the protocol procedure for slotted aloha protocol.

- **In slotted aloha, time is divided into slots. A sender may send a frame at the start of the time slot.**
- **If the sender does not send at the start then it will wait for the next slot.**
- **If two sender sends the frames at the beginning of the time slot, there will be a collision and the frame will be garbled.**
- **If the acknowledgment is not received, the frame is retransmitted in a new slot.**

3)Explain about selective repeat sliding window protocol and go back N protocol

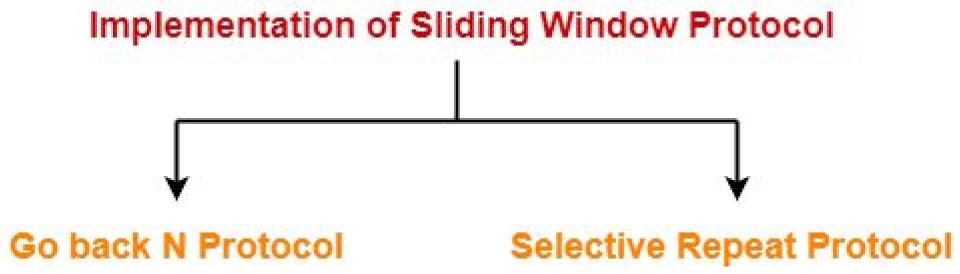
Sliding Window Protocol

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

Sliding window protocol has two types:


Implementation of Sliding Window Protocol
Go back N Protocol
Selective Repeat Protocol

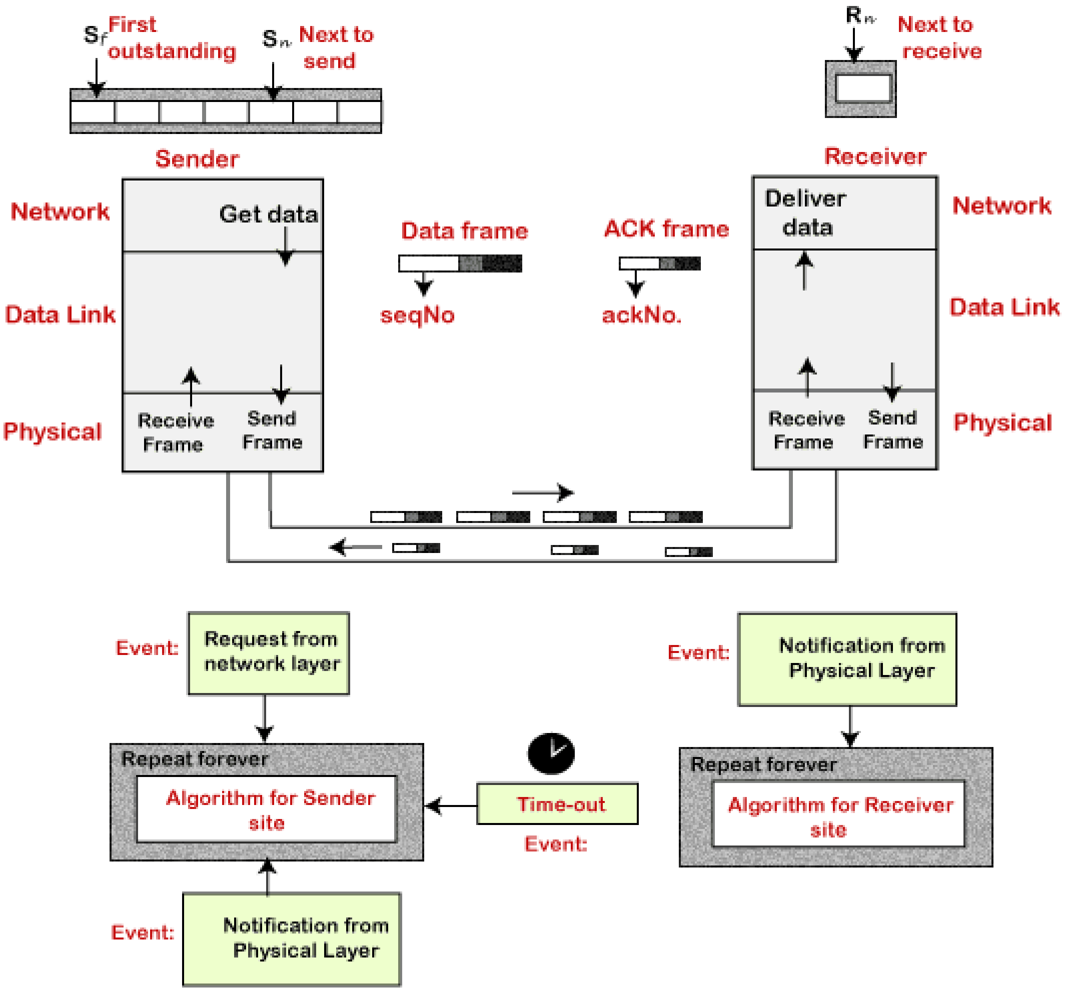
1. **Go-Back-N ARQ**
2. **Selective Repeat ARQ**

Go-Back-N ARQ

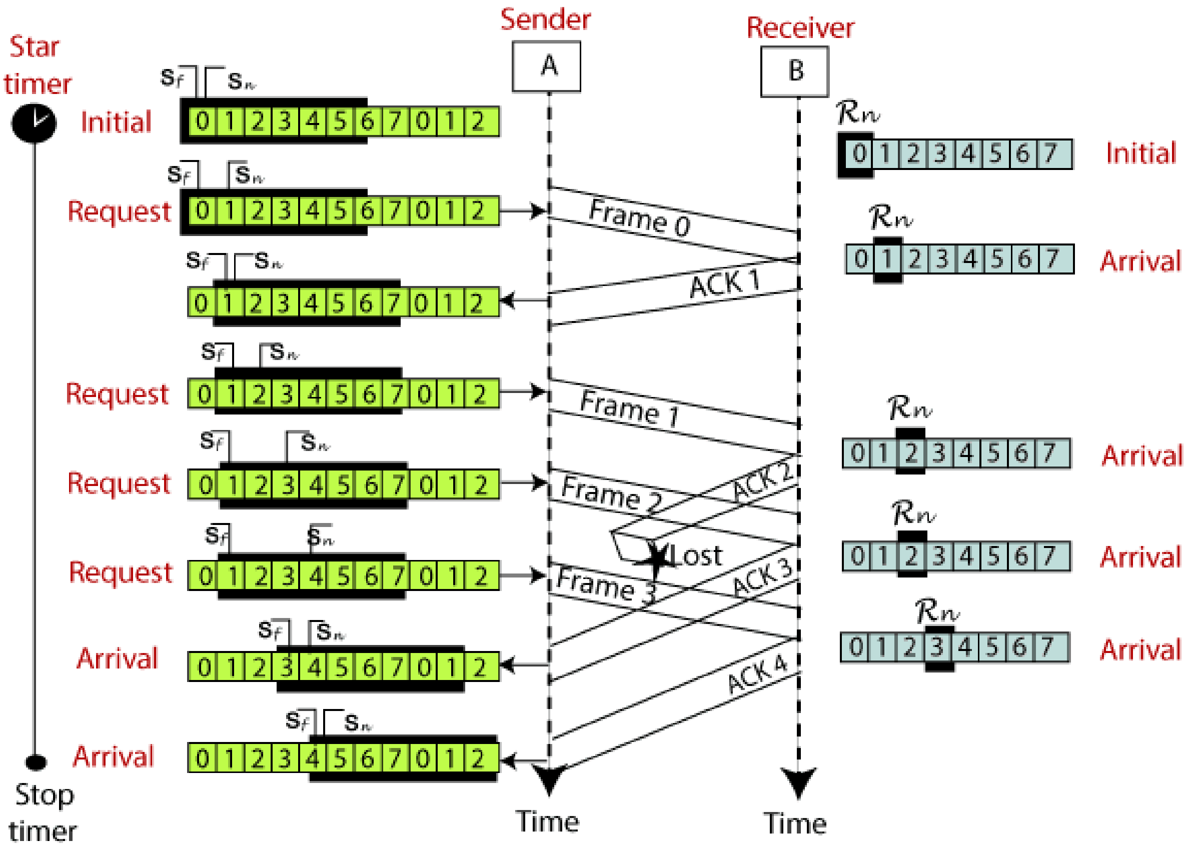
Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.



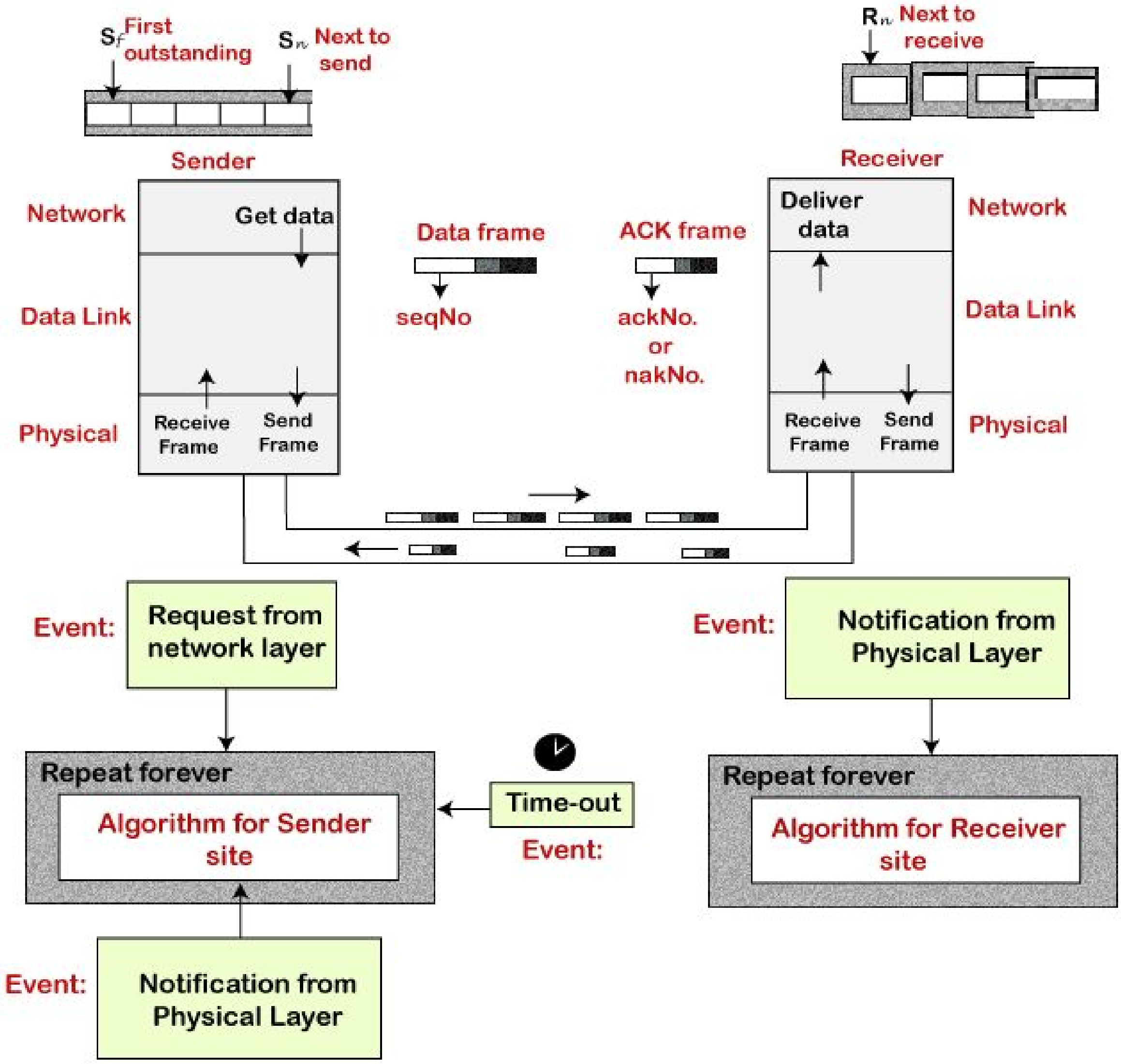
The example of Go-Back-N ARQ is shown below in the figure.



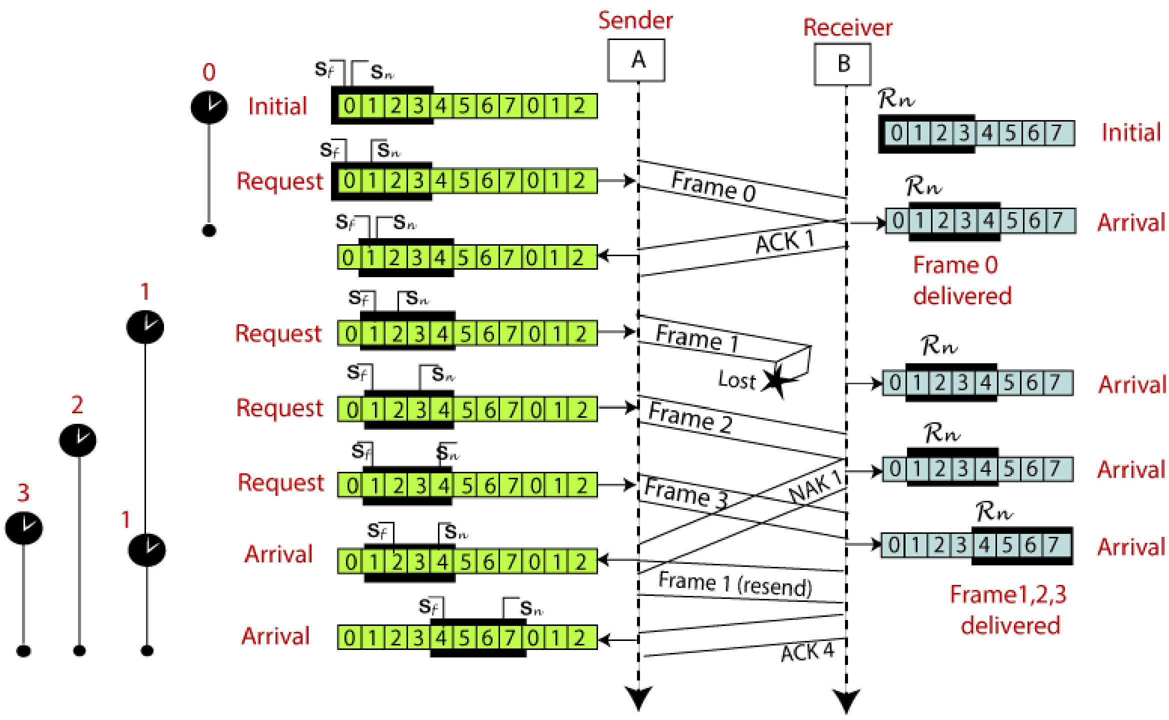
Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

The design of the Selective Repeat ARQ protocol is shown below.



The example of the Selective Repeat ARQ protocol is shown below in the figure.



Difference between the Go-Back-N ARQ and Selective Repeat ARQ?

Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	**In this, only the frame is sent again, which is corrupted or lost.**
If it has a high error rate,it wastes a lot of bandwidth.	**There is a loss of low bandwidth.**
It is less complex.	**It is more complex because it has to do sorting and searching as well. And it also requires more storage.**
It does not require sorting.	**In this, sorting is done to get the frames in the correct order.**

It does not require searching.	**The search operation is performed in it.**
It is used more.	**It is used less because it is more complex.**

SHORT QUESTIONS

Explain flow control,framing,piggy backing

Flow Control

Flow control tells the sender how much data should be sent to the receiver so that it is not lost. This mechanism makes the sender wait for an acknowledgment before sending the next data. There are two ways to control the flow of data:

1. Stop and Wait Protocol
2. Sliding Window Protocol

Stop and Wait Protocol

It is the simplest flow control method. In this, the sender will send one frame at a time to the receiver. Until then, the sender will stop and wait for the acknowledgment from the receiver. When the sender gets the acknowledgment then it will send the next data packet to the receiver and wait for the acknowledgment again and this process will continue.

Efficiency = Useful Time/ Total Time

$$\eta=Td / (Td+2Tp)$$

Advantages of Stop and Wait Protocol

1. It is very simple to implement.

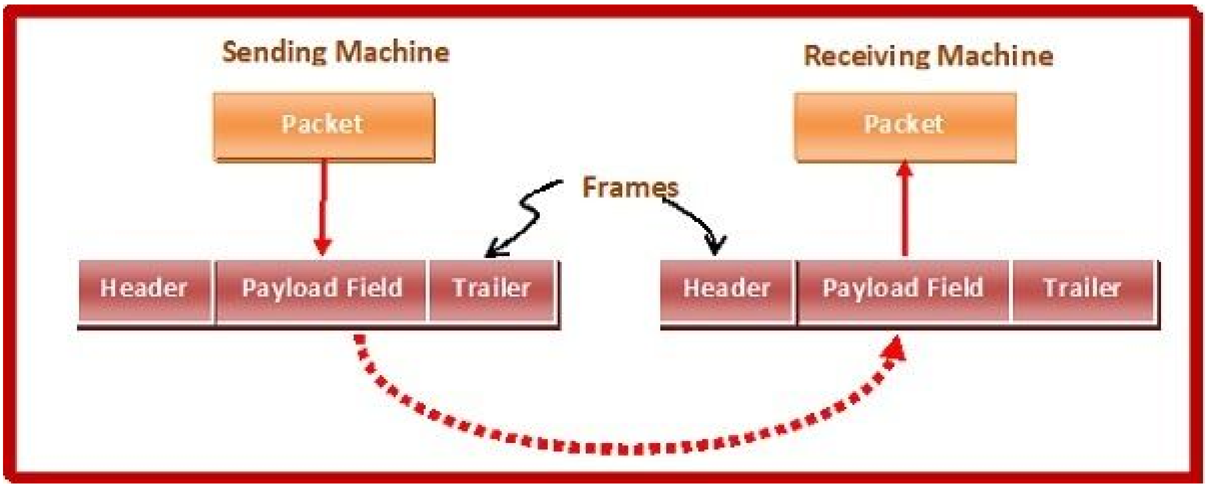
Disadvantages of Stop and Wait Protocol

1. We can send only one packet at a time.
2. If the distance between the sender and the receiver is large then the propagation delay would be more than the transmission delay. Hence, efficiency would become very low.
3. After every transmission, the sender has to wait for the acknowledgment and this time will increase the total transmission time.

Framing in Data Link Layer

Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames makes flow control and error control more efficient.

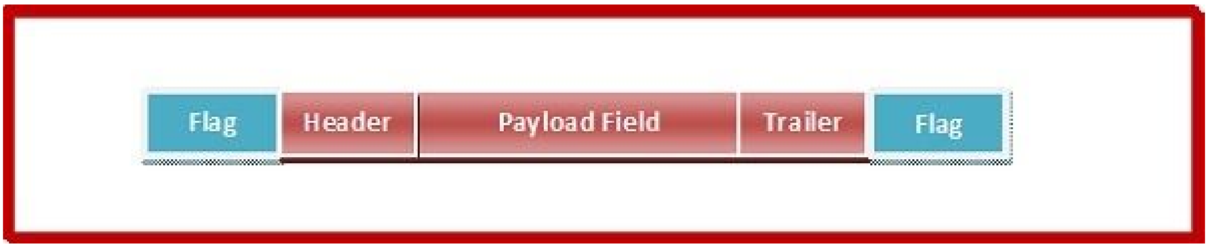
Then, it sends each frame bit-by-bit on the hardware.



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.



Types of Framing

Framing can be of two types, fixed sized framing and variable sized framing.

1.Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example − ATM cells.

2.Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.

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.**

Piggybacking (data transmission)

In two-way communication, whenever a frame is received, the receiver waits and does not send the control frame (acknowledgement or ACK) back to the sender immediately.

The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.

Working Principle

Piggybacking data is a bit different from Sliding Protocol used in the OSI model. In the data frame itself, we incorporate one additional field for acknowledgment (called ACK).

Whenever party A wants to send data to party B, it will carry additional ACK information in the PUSH as well.

For example, if A has received 5 bytes from B, which sequence number starts from 12340 (through 12344), A will place "ACK 12345" as well in the current PUSH packet to inform B it has received the bytes up to sequence number 12344 and expects to see 12345 next time.

Three rules govern the piggybacking data transfer.

- **If station A wants to send both data and an acknowledgment, it keeps both fields there.**
- **If station A wants to send the acknowledgment, after a short period of time to see whether a data frame needs to be sent, then decide whether send an ACK frame alone or attach a data frame with it.**
- **If station A wants to send just the data, then the previous acknowledgment field is sent along with the data. Station B simply ignores this duplicate ACK frame upon receiving.**

Advantages and Disadvantages[edit]

Advantages : Improves the efficiency, better use of available channel bandwidth.

Disadvantages : The receiver can jam the service if it has nothing to send. This can be solved by enabling a counter (Receiver timeout) when a data frame is received. If the count ends and there is no data frame to send, the receiver will send an ACK control frame. The sender also adds a counter (Emitter timeout), if the counter ends without receiving confirmation, the sender assumes packet loss, and sends the frame again.