## Flow Control

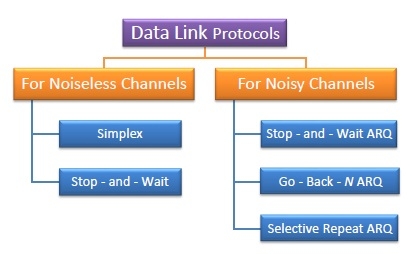
* It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
* The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
* It requires a buffer, a block of memory for storing the information until they are processed.

**Elementary Data Link Protocols**

Protocols in the data link layer are designed so that this layer can perform its basic functions: framing, error control and flow control. Framing is the process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes. Error control mechanisms deals with transmission errors and retransmission of corrupted and lost frames. Flow control regulates speed of delivery and so that a fast sender does not drown 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**

The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong. It has distinct procedures for sender and receiver. The sender simply sends all its data available onto the channel as soon as they are available its buffer. The receiver is assumed to process all incoming data instantly. It is hypothetical since it does not handle flow control or error control.

**Stop – and – Wait Protocol**

Stop – and – Wait protocol is for noiseless channel too. It provides unidirectional data transmission without any error control facilities. However, it provides for flow control so that a fast sender does not drown a slow receiver. The receiver has a finite buffer size with finite processing speed. The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.

A----------------------------------------------------------------B

**Sliding Window protocol**

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.

• In sliding window method, multiple frames are sent by sender at a time before needing an acknowledgment.

• Multiple frames sent by source are acknowledged by receiver using a single ACK frame.

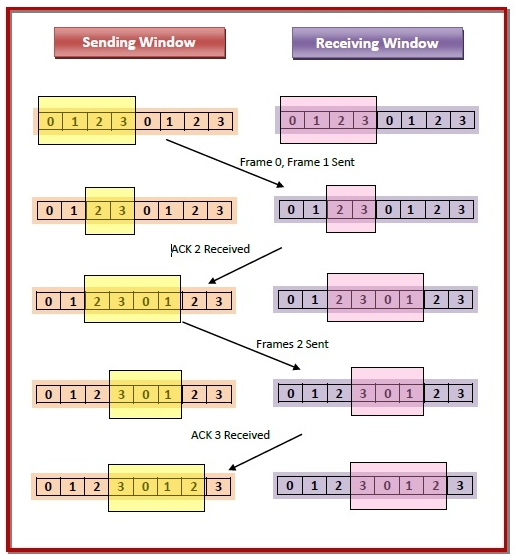
• Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.

• It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.

• Frames may be acknowledged by receiver at any point even when window is not full on receiver side.

• Frames may be transmitted by source even when window is not yet full on sender side.

**Sliding window of size =4**



# Stop and Wait ARQ

* Used in Connection-oriented communication.
* It offers error and flow control
* It is used in Data Link and Transport Layers
* Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1

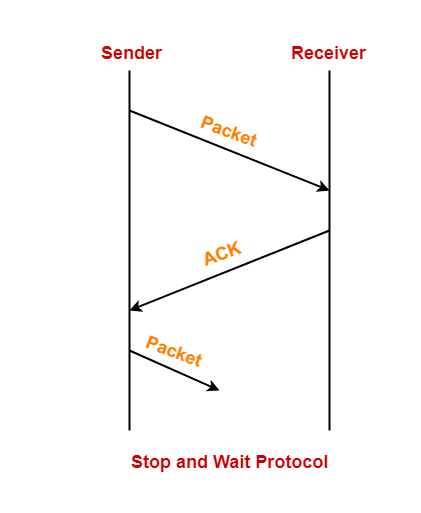
### Simple Stop and Wait

Sender:

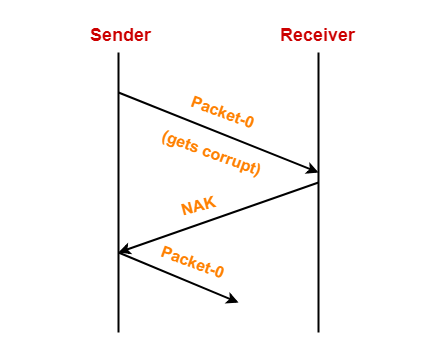
* Send one data packet at a time.
* Send next packet only after receiving acknowledgement for previous.

Receiver:

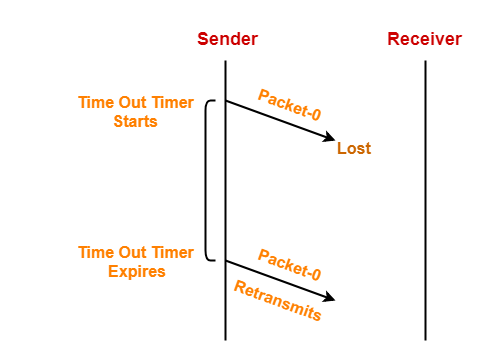
* Send acknowledgement after receiving and consuming of data packet.
* After consuming packet acknowledgement need to be sent (Flow Control)



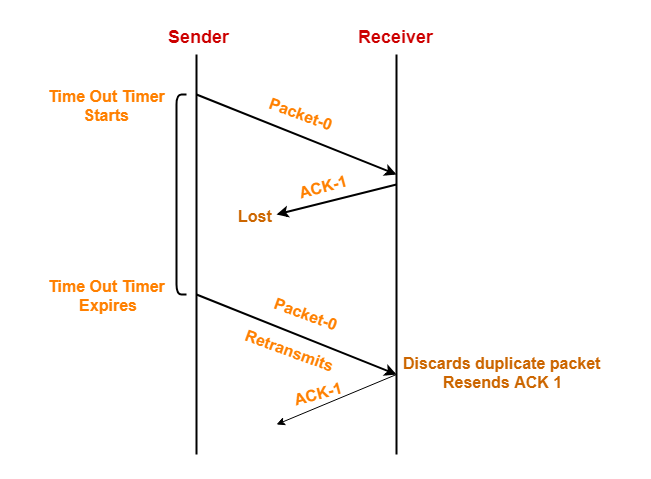
**Stop and Wait ARQ for damaged frame**



**Stop and Wait ARQ for lost data frame**

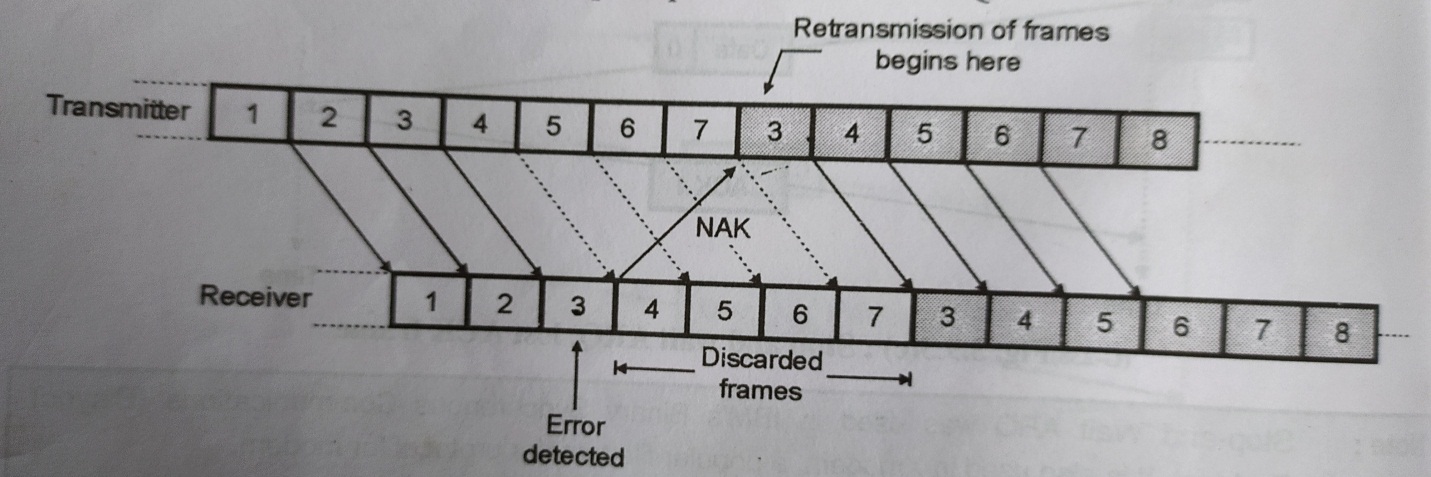


**Stop and Wait ARQ for lost acknowledgment**



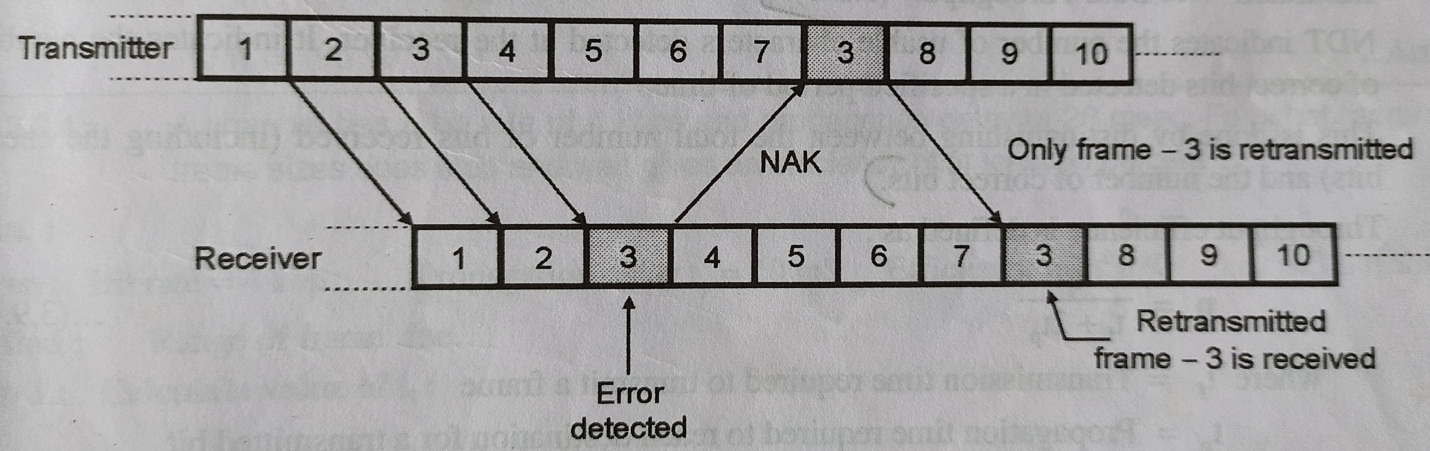
# GO Back n

* This is an improved protocol compared to Stop and Wait protocol. It is a method to overcome the inefficiency of Stop and Wait protocol by allowing the transmitter to continue sending enough frames so that the cannel kept busy while the transmitter wait for acknowledgments.
* It transmits the frames continuously as long as it does not receive the NAK signal.
* When receiver detects an error it sends the NAK signal to the sender.
* But this signal takes some time to reach the transmitter by that time transmitter has transmit the frames.



# Selective Repeat ARQ

* This is a better technique compare to Go Back n.
* Selective Repeat protocol provides for sending multiple frames depending upon the availability of frames in the sending window, even if it does not receive acknowledgement for any frame in the interim.
* The maximum number of frames that can be sent depends upon the size of the sending window.
* The receiver records the sequence number of the earliest incorrect or un-received frame. It then fills the receiving window with the subsequent frames that it has received. It sends the sequence number of the missing frame along with every acknowledgement frame.
* The sender continues to send frames that are in its sending window. Once, it has sent all the frames in the window, it retransmits the frame whose sequence number is given by the acknowledgements. It then continues sending the other frames.



# 

# Medium Access Control Sublayer (MAC sublayer)

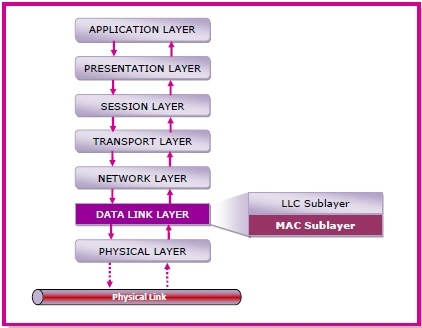
The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

## MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers −

* The logical link control (LLC) sublayer
* The medium access control (MAC) sublayer

The following diagram depicts the position of the MAC layer −



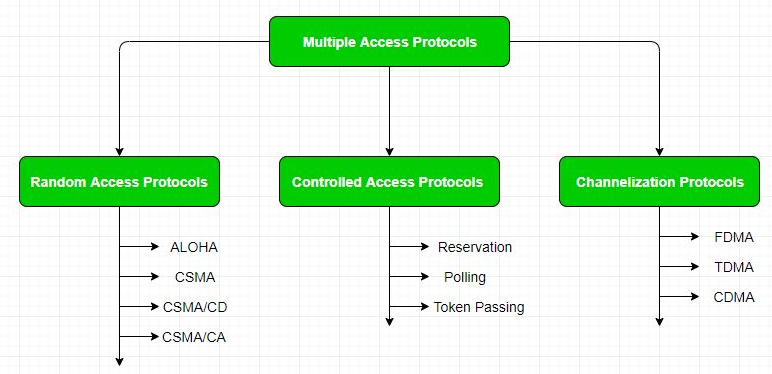
## Functions of MAC Layer

* It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
* It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
* It resolves the addressing of source station as well as the destination station, or groups of destination stations.
* It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
* It also performs collision resolution and initiating retransmission in case of collisions.
* It generates the frame check sequences and thus contributes to protection against transmission errors.

**Multiple Access**

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

Thus, protocols are required for sharing data on non-dedicated channels. Multiple access protocols can be subdivided further as –



**Random Access Protocol:** In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium’s state (idle or busy).

It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

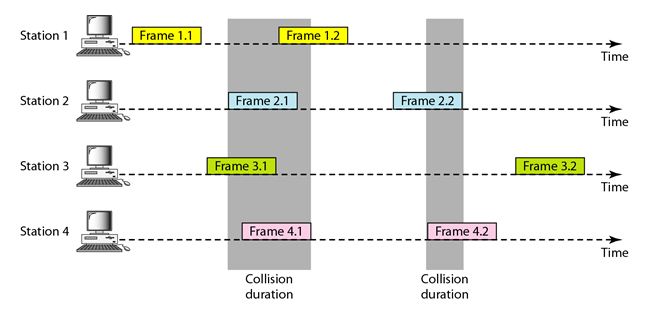
**ALOHA Protocols**

ALOHA, the earliest random access method was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

**Pure ALOHA**

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations. The following figure shows an example of frame collisions in pure ALOHA.

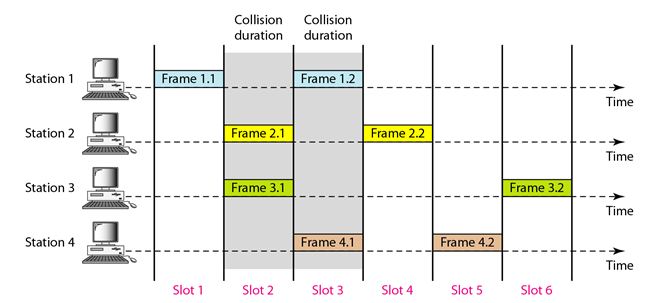


There are four stations (unrealistic assumption) that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel.

## Slotted ALOHA:

Pure ALOHA has a vulnerable time of 2 x Tfr. This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency.

In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot. The following figure shows an example of frame collisions in slotted ALOHA.



**CSMA**

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However, there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes-

* **1-persistent:**The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally (with 1 probability) as soon as the channel gets idle.
* **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
* **P-persistent:**The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.

**CSMA/CD**

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free. The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

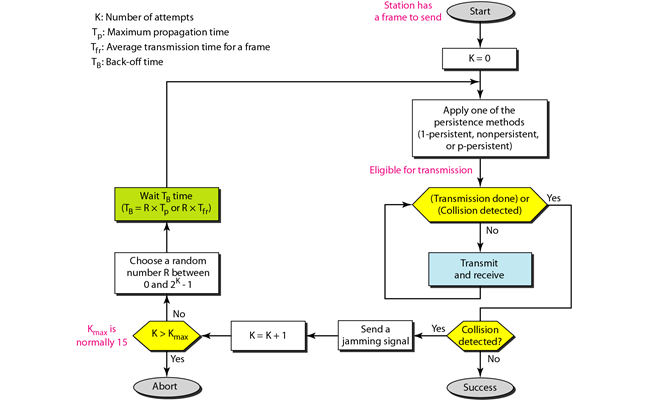
## Algorithms

The algorithm of CSMA/CD is:

* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is busy, the station waits until the channel becomes idle.
* If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
* If a collision is detected, the station starts the collision resolution algorithm.
* The station resets the retransmission counters and completes frame transmission.

The algorithm of Collision Resolution is:

* The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.
* The station increments the retransmission counters.
* If the maximum number of retransmission attempts is reached, then the station aborts transmission.
* Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restart main algorithm.



# CSMA with Collision Avoidance (CSMA/CA)

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. In contrast to CSMA/CD (Carrier Sense Multiple Access/Collision Detection) that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.

## Algorithm

The algorithm of CSMA/CA is:

* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is busy, the station waits until the channel becomes idle.
* If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
* After sending the frame, it sets a timer.
* The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
* Otherwise, it waits for a back-off time period and restarts the algorithm.

