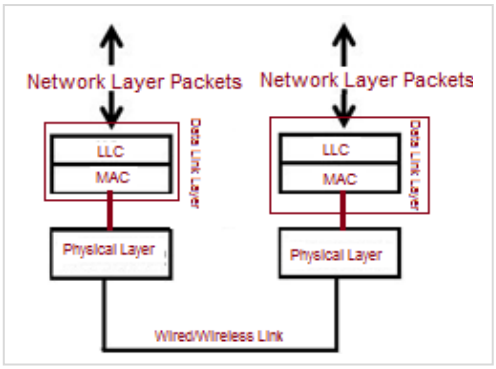
1. Functions of Data link layer
2. Framing
3. Error Detection and Corrections,
4. Flow Control
5. Examples of Data Link Protocol, HDLC, PPP
6. The Medium Access Sub-layer
7. The channel allocation problem
8. Multiple Access Protocols
9. Ethernet,
10. Networks: FDDI, ALOHA, VLAN, CSMA/CD, IEEE 802.3(Ethernet), 802.4(Token Bus), 802.5(Token Ring), 802.1(Wireless LAN).



- Second layer of OSI Layered Model.
- Ensures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully.
- responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.
- To detect the errors at the data link layer efficiently and easily, transmitting a small size data is a better approach.
- Data link layer has two sub-layers:
  - **Logical Link Control (LLC):** It deals with protocols, flow-control, and error control
    - Interface to upper layer, flow control and error control, management functions
  - **Media Access Control (MAC):** It deals with actual control of media
    - Construct header and trailer, assembles frames, address and error check, access the medium

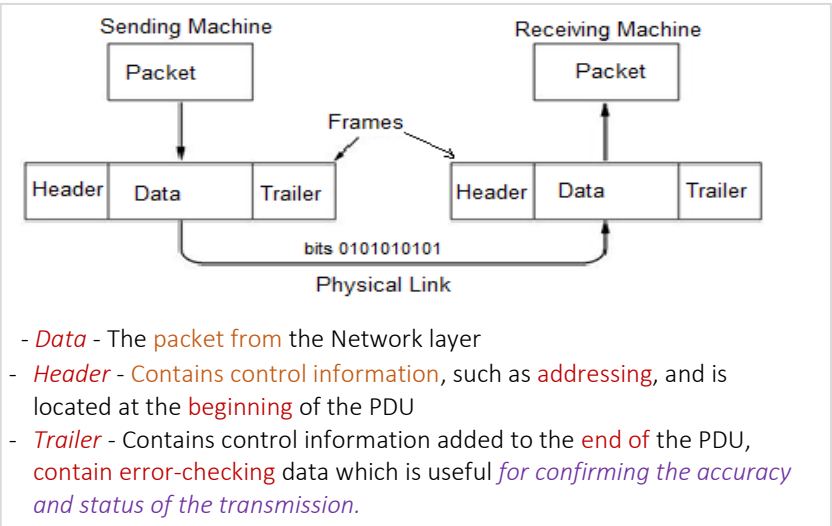
3.1. Functions of Data Link Layer

Data link layer does many tasks on behalf of upper layer. These are:

- Framing: Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.
- Addressing *:* Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- Synchronization *:* When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
- Error Control*:* Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- Flow Control : Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.
- Multi-Access *:* When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

3.2. Framing

The frame is made by breaking down a stream of packets into smaller, digestible chunks. A frame typically includes frame synchronization features consisting of a sequence of bits or symbols arrangement such that it indicates to the receiver the beginning and end of the payload data within the stream of symbols or bits it receives.



- *Data* - The packet from the Network layer
- *Header* - Contains control information, such as addressing, and is located at the beginning of the PDU
- *Trailer* - Contains control information added to the end of the PDU, contain error-checking data which is useful *for confirming the accuracy and status of the transmission.*

In the OSI model of computer networking, a frame is the protocol data unit at the data link layer. Frames are the result of the final layer of encapsulation before the data is transmitted over the physical layer. A frame is "the unit of transmission in a link layer protocol, and consists of a link layer header followed by a packet." Each frame is separated from the next by an interframe gap. A frame is a series of bits generally composed of framing bits, the packet payload, and a frame check sequence. Examples are Ethernet frames, Point-to-Point Protocol (PPP) frames, Fiber Channel frames, and V.42 modem frames.

- Encapsulate datagram into frame, adding header, trailer
- Chanel access if shared medium
- "MAC" addresses used in frame headers to identify source, destination and its different from IP address!

Methods of Framing: Frames can be of fixed or variable size

1. **Fixed-Size or Static Framing :** Frames size are fixed and there is no need for defining the boundaries of the frames or no need to specify the start of the frame; 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 or Dynamic Framing :** Frames size are changed and it is necessary to specify the start and end of each frame. It is prevalent in local- area networks.

Fixed-Size or Static Framing	Variable-size or Dynamic Framing
1.Every record in the file has exactly same size (in byte) 2.It take huge memory. 3.Access become fast. 4.Computer knows exact location of records so easy access. 5.slow in transferring the records it has large size.	1.Different record in the file have different size. 2.It take least memory. 3.access become slow. 4.computer does not know exact location of record so slow access. 5.fast transferring as it is small in size.

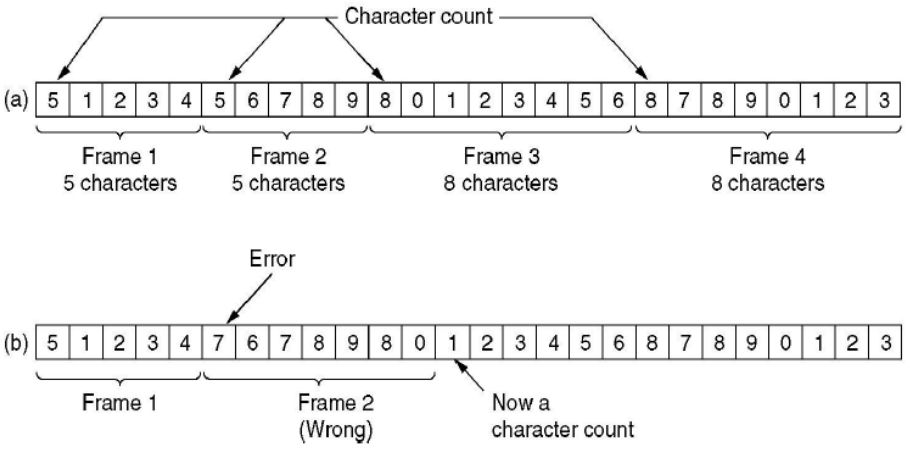
Approaches of Variable size framing:

2.1) Character-Oriented Approach and

2.2) Bit-Oriented Approach.

*** Character Count:**

This method uses a field in the header to specify the number of characters in the frame. But the *problem can occur if the count is distorted in transit due to which the receiver will not know where to pick up and the sender will not know how much to resend*. This method is rarely used.

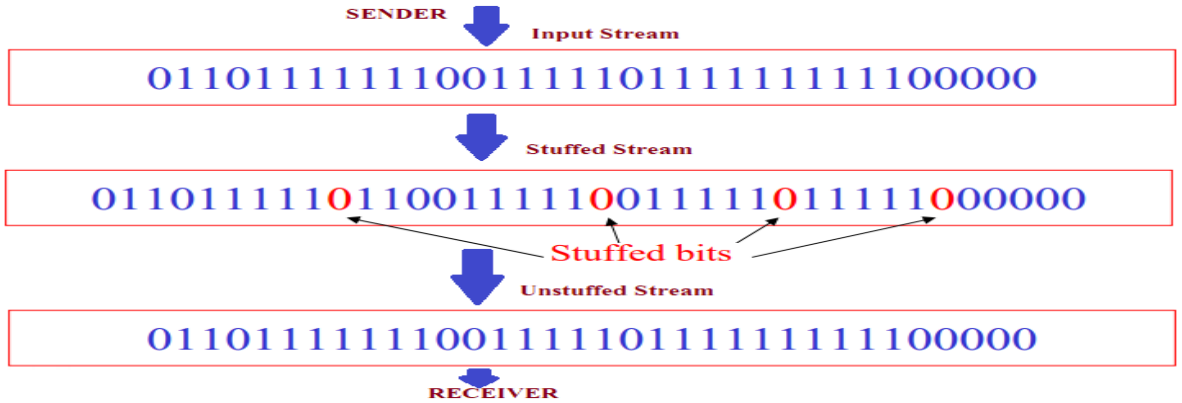


A character stream. (a) Without errors. (b) With one error.

Fig: Character Count

*** Bit stuffing:** Bits are sent

- Allows frame to contain arbitrary number of bits and arbitrary character size. The frames are separated by separating flag.
- Each frame begins and ends with a special bit pattern, **01111110** called a flag byte. When five consecutive 1's are encountered in the data, it automatically stuffs a **'0'** bit into outgoing bit stream.
- In this method, frames contain an arbitrary number of bits and allow character codes with an arbitrary number of bits per character. In his case, each frame starts and ends with a special bit pattern, **01111110**.
- In the data a **0** bit is automatically stuffed into the outgoing bit stream whenever the sender's DLL finds five consecutive **1s**.
- This bit stuffing is similar to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.
- When the receiver sees five consecutive incoming **1's** bits, followed by a **0's** bit, it automatically destuffs (i.e., deletes) the **0** bit. Bit Stuffing is completely transparent to network layer as byte stuffing. The figure1 below gives an example of bit stuffing.
- This method of framing finds its application in networks in which the change of data into code on the physical medium contains some repeated or duplicate data. For example, some LANs encodes bit of data by using 2 physical bits.



*** Byte stuffing or Character Stuffing:** ASCII characters are sent

- In this method, start and end of frame are recognized with the help of one flag bytes. Each frame starts with and ends with a flag byte. Two consecutive flag bytes indicate the end of one frame and start of the next one is named as escape character "**ESC**" flag byte.
- A frame delimited by flag bytes. This framing method is only applicable in 8-bit character codes which are a major disadvantage of this method as not all character codes use 8-bit characters e.g. Unicode.
- During data transmission, if the receiver gets lost, it just looks for the pair of flag bytes to *denote the end of one frame and the start of the next.*
- The escape "**ESC**" characters have a predefined pattern.
- At Fig.(1)(3) At the sender an ESC character is inserted just before the FLAG byte present in the data. At the receiver the ESC is removed from the data. At Fig.(2)(3)(4) an ESC is present in the data then an extra ESC is inserted before it in the data. This extra ESC is removed at the receiver.

Fig. Frame

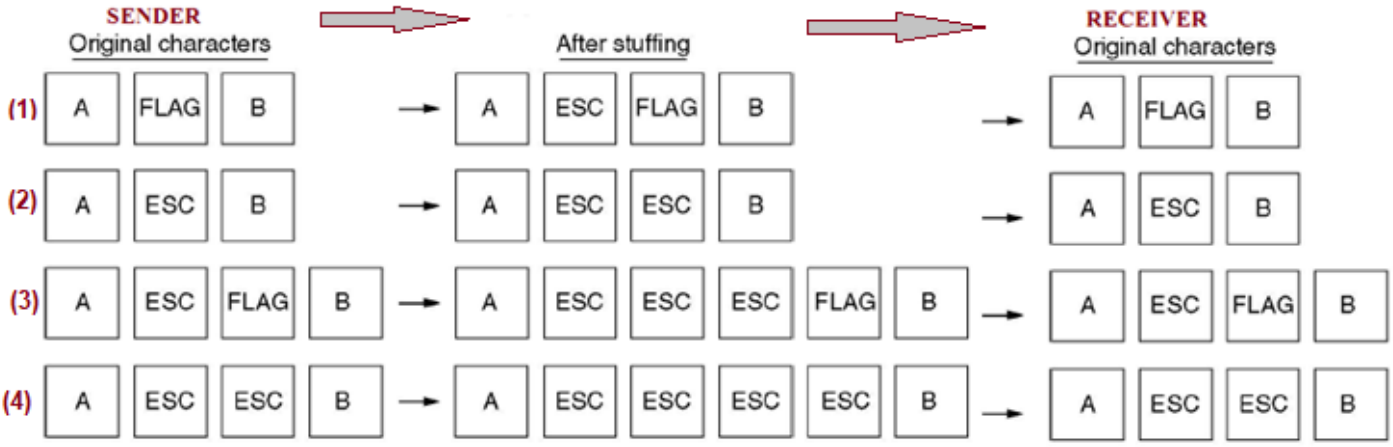


Fig. Four example of byte sequences before and after stuffing:

*** Physical Layer Coding Violations:**

- This method is only applicable to network in which the encoding on the physical medium contains some redundancy .
- **1** bit of data may encode using two physical bits like **0** and **1** .
- **1** bit represents high to low and **0** represents low to high .
- The combinations like high to high or low to low are not used for data .by using this the receiver easily locates bit boundaries .

3.3. Error Detection and Corrections

There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive wrong data. *Applications such as voice and video may not be that affected and with some errors they may still function well.*

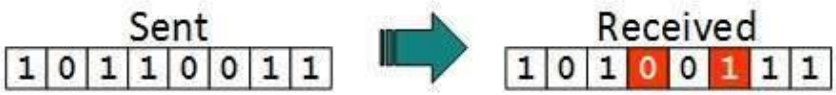
Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

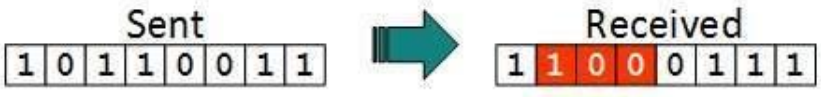
There may be three types of errors:

- **Single bit error :** In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error :** Frame is received with more than one bits in corrupted state.

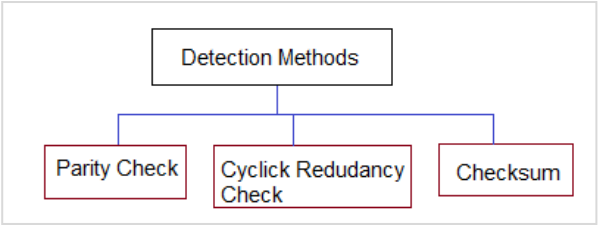


- **Burst error :** Frame contains more than1 consecutive bits corrupted.



Error control mechanism may involve two possible ways:

- **Error detection** : It allows a receiver to check whether received data has been corrupted during transmission. It can, for example, request a retransmission.
- **Error correction** : This type of error control allows a receiver to reconstruct the original information when it has been corrupted during transmission.



* Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

1. Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity. The sender while creating a frame counts the number of 1s in it. *For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.*

The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are error, then it is very hard for the receiver to detect the error.

Example for Parity bit :-

- Suppose the sender wants to send the word "world" in ASCII the five characters are coded as

1110111 1101111 1110010 1101100 1100100 => 1110111**0** 1101111**0** 1110010**0** 1101100**0** 1100100**1**

- Now suppose the word "world" in example 1 is received by receiver without corrupted in transmission.

The receiver counts the one(1's) in each character and comes up with even numbers (6,6,4,4,4). The data are accepted

- Now suppose the word "world" in example 1 is corrupted during transmission, The receiver counts the one(1's) in each character and comes up with even and odd numbers (7,6,5,4,4).

The receiver knows that the data are corrupted, discards them and asks for re-transmission.

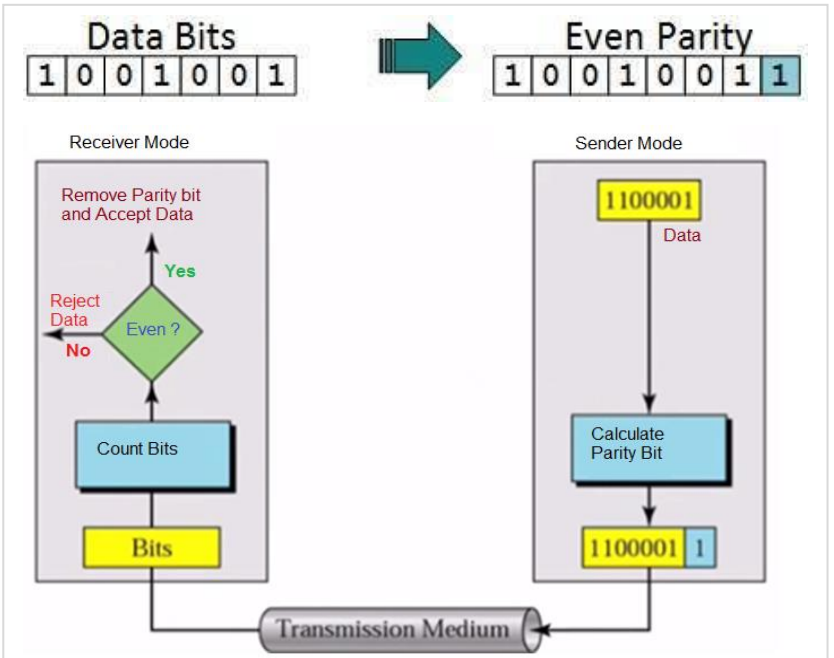


Fig.Parity Check

2. Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a code word. The sender transmits data bits as code words.

At the other end, the receiver performs division operation on code words using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Performance of CRC

CRC is a very effective error detection method. If the divisor is chosen according to the previously mentioned rules,

1.CRC can detect all burst errors that affect an odd number of bits.

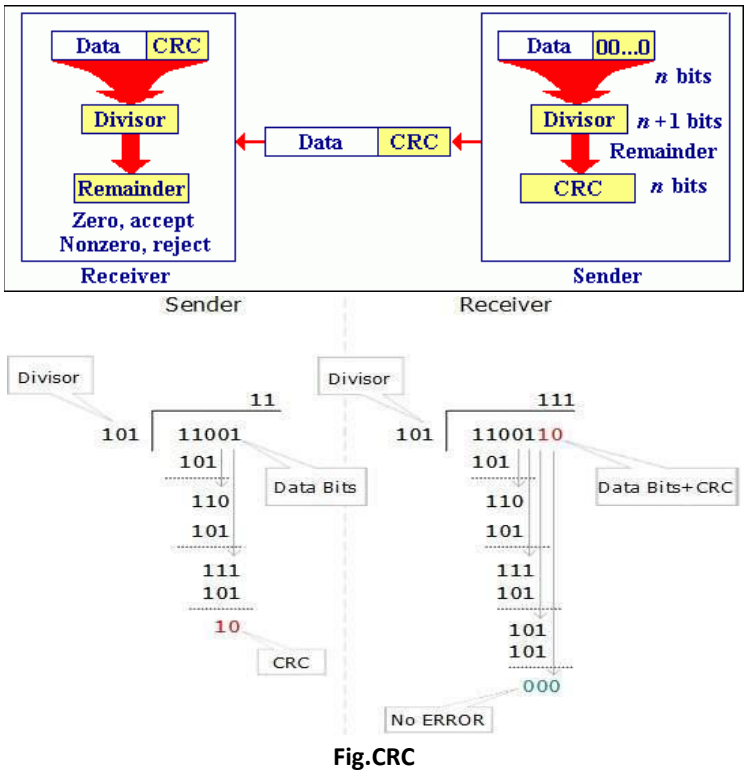


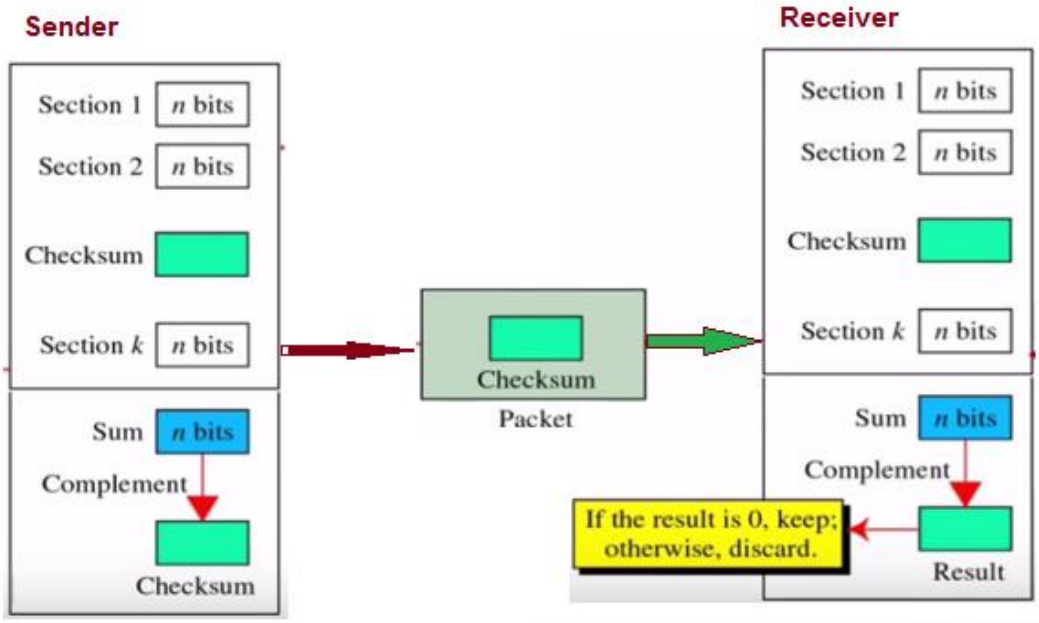
Fig.CRC

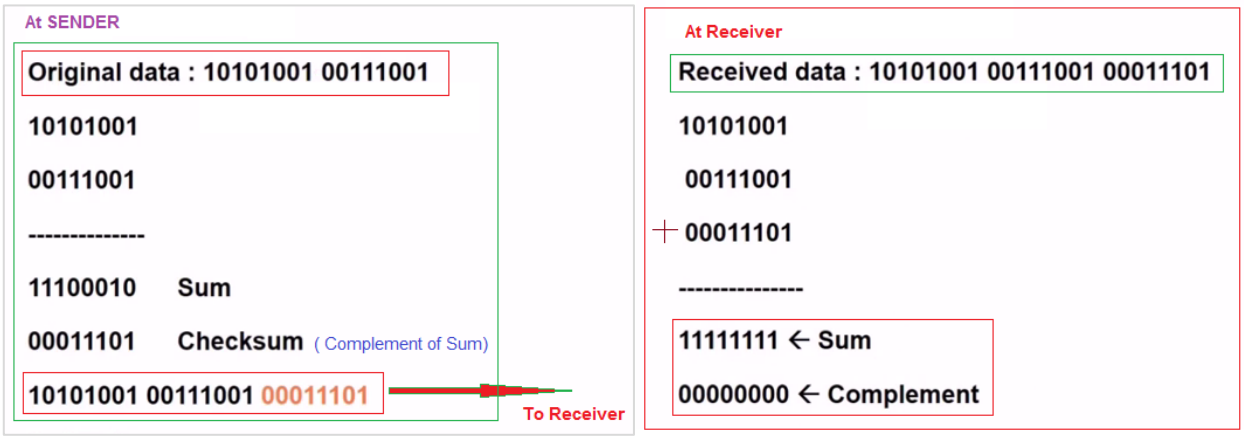
2.CRC can detect all burst errors of length less than or equal to the degree of the polynomial
3.CRC can detect, with a very high probability, burst errors of length greater than the degree of the polynomial.

3. Checksum:

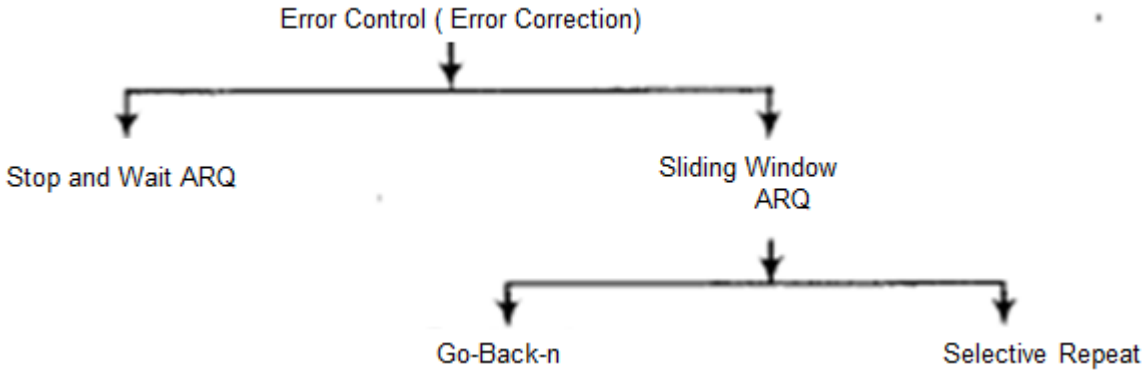
The checksum is used in the Internet by several protocols although not at the data link layer.
To create checksum, the sender does the following :-

- The unit is divided into **K** sections, each of **n** bits
- Section **1** and **2** are added together using **1's** complement.
- Section **3** is added to the result of the previous step.
- Section **4** is added to the result of the previous step.
- The process repeats until section k is added to the result of previous step.
- The final result is complemented to make checksum.





Error Correction



- An error is detected in an exchange, a negative acknowledgement **NAK** is returned and the specified frames are retransmitted. This process is called Automatic Repeat Request (**ARQ**).
- Retransmission of data happens in three Cases: Damaged frame, Lost frame and Lost acknowledgement.

In the digital world, error correction can be done in two ways:

- Automatic repeat request *(ARQ) or* Backward Error Correction - When the receiver *detects an error in the data received*, it requests back the sender to *retransmit the data unit*.
- Forward Error Correction (FCC) - When the receiver detects some error in the data received, it executes error-correcting code, which helps it to *auto-recover and to correct* some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive e.g. fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.
To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. *To locate the bit in error, redundant bits are used as parity bits for error detection.* For example, we take ASCII words (7 bits data), then there could *be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.*

Requirements for error control mechanism:

- Error detection - The sender and receiver, either both or any, must detect that there is some error in the transit.
- Positive ACK - When the receiver receives a correct frame, it should acknowledge it.
- Negative ACK - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- Retransmission: The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

Error control in the data link layer is based on automatic repeat request(ARQ), which is the retransmission of data.

Types of Automatic Repeat Requests (ARQ) techniques: -

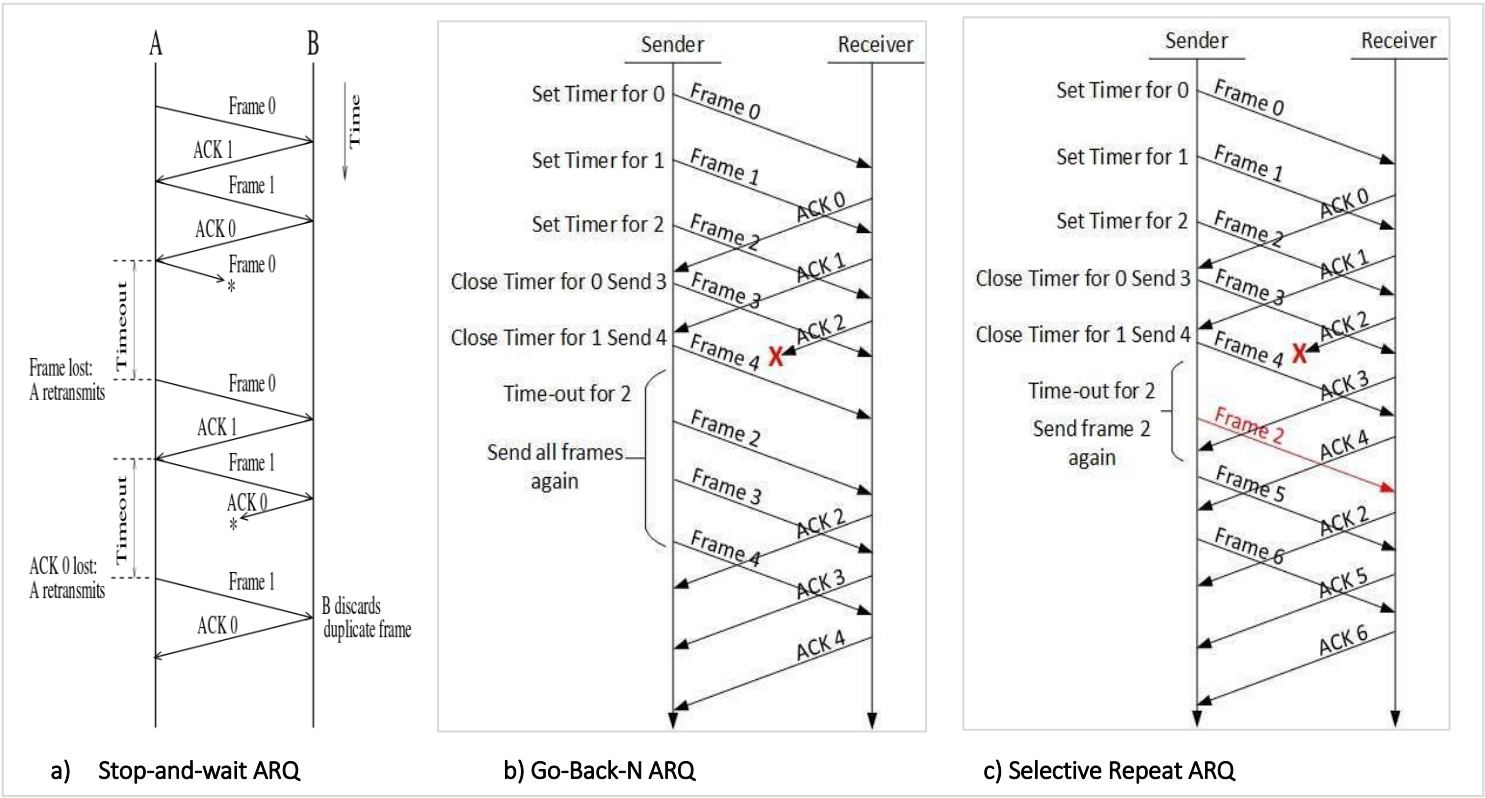
1. Stop-and-wait ARQ
   - The sender maintains a timeout counter. When a frame is sent, the sender starts the timeout counter.
   - If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
   - If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter. If a negative acknowledgement NAK is received, the sender retransmits the frame.
   - The sender has to wait for an acknowledgment of every frame that it sends. Only when an acknowledgment has been received is the next frame sent. This process continues until the sender transmits an End of Transmission (EOT) frame.
     - Advantages of Stop and Wait: It's simple and each frame is checked and acknowledged well.
   - Disadvantages of Stop and Wait:
     - Only one frame can be in transmission at a time.
     - It is inefficient, if the distance between devices is long. Reason is propagation delay is much longer than the transmission delay.
     - The time spent for waiting acknowledgements between each frame can add significant amount to the total transmission time.
   - Piggybacking: In bidirectional communications, both parties send & acknowledge data, i.e. both parties implement flow control. Outstanding ACKs are placed in the header of information frames, piggybacking can save bandwidth since the overhead from a data frame and an ACK frame (addresses, CRC, etc) can be combined into just one frame.
2. Go-Back-N ARQ

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.
The sending-window size *enables the sender to send multiple frames without receiving the acknowledgement of the previous ones.*
The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

- When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames.
- If sender finds that it has received NACK or has *not receive any ACK for a particular frame, it retransmits all the frames* after which it does not receive any positive ACK.

3. Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.
In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged. The sender in this case, sends only packet for which NACK is received.



a) Stop-and-wait ARQ b) Go-Back-N ARQ c) Selective Repeat ARQ

3.4. Flow Control

Flow Control deals with the issue where the sender sends data at the higher rate than the receiver can receive. Flow control can be done by using the buffer on the receiver side. But, the main problem that occurs, in this case, is that the slower receiver cannot handle with the faster sender which causes overflow and loss of data.

Approaches to Flow Control:

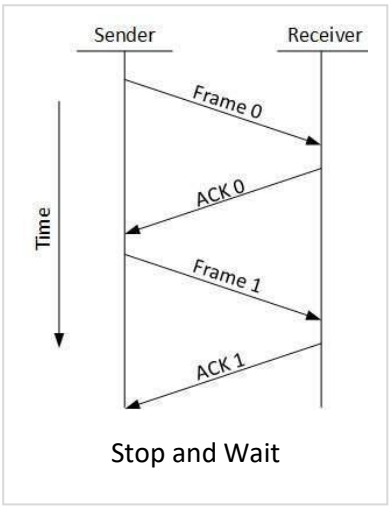
1. **Feedback-based Flow Control**: Receiver sends feedback to the sender telling how it is doing.
2. **Rate-based Flow Control**: In this approach, pre-communication occurs between sender and receiver and the data transfer occurs at the rate which the receiver can receive without overflow.

- In data communications, *flow control is the process of* managing the rate of data transmission *between two nodes to prevent a fast sender from* overwhelming *a slow receiver.*
- It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node.
- Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. This can happen if the receiving computers have a heavy traffic load in comparison to the sending computer, or if the receiving computer has less processing power than the sending computer.

Types of mechanisms can be deployed to control the flow:

1. Stop and Wait

- This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.
-, the receiver indicates its readiness to receive data for each frame, the message is broken into multiple frames. The sender waits for an ACK (acknowledgement) after every frame for specified time (called time out).
- It is sent to ensure that the receiver has received the frame correctly. It will then send the next frame only after the ACK has been received.



Stop and Wait

Operations

1. Sender: Transmits a single frame at a time.
2. Receiver: Transmits acknowledgement (ACK) as it receives a frame.
3. Sender receive ACK within time out.
4. Go to step 1.

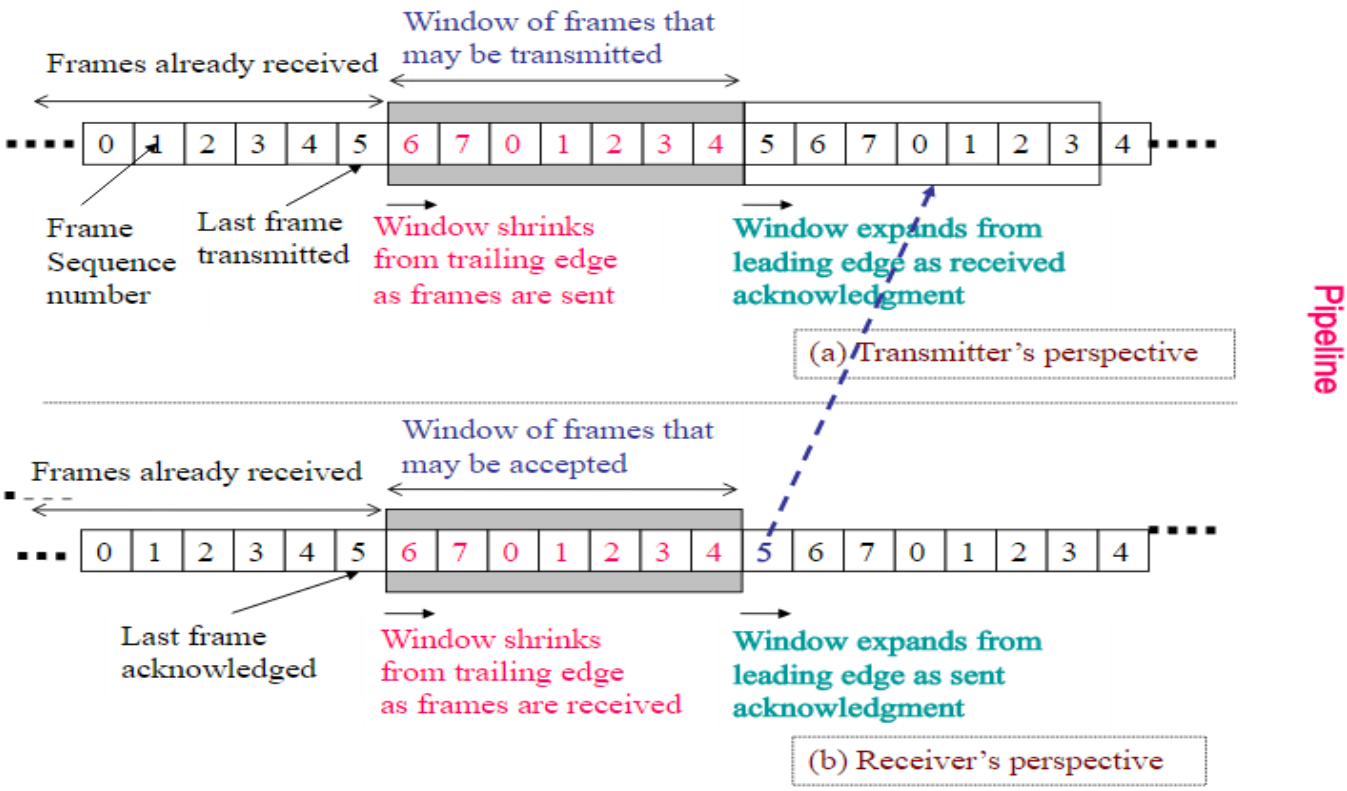
- If a frame or ACK is lost during transmission, then it has to be transmitted again by sender. This re-transmission process is known as ARQ (automatic repeat request).
- The problem with Stop-and wait is that only one frame can be transmitted at a time, and that often leads to inefficient transmission, because until the sender receives the ACK it cannot transmit any new packet. During this time both the sender and the channel are unutilized.

2. Sliding Window

- Major Drawback of Stop-and-Wait Flow Control: - Only one frame can be in transmission at a time - This leads to inefficiency if propagation delay is much longer than the transmission delay
- Sliding Window Flow Control - Allows transmission of multiple frames - Assigns each frame a k-bit sequence number - Range of sequence number is [0..2k -1], i.e., frames are counted modulo 2k
- **Window size**: No of frames which sent at a time
- In this flow control mechanism, *both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent.* As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.
- A method of flow control in which a receiver gives a transmitter permission to transmit data until a window is full. *When the window is full, the transmitter must stop transmitting until the receiver advertises a larger window.*
- Sliding-window flow control is best utilized when the buffer size is limited and pre-established. During a typical communication between a sender and a receiver the receiver allocates buffer space for n frames (n is the buffer size in frames). The sender can send and the receiver can accept n frames without having to wait for an acknowledgement.
- A **sequence number** is assigned to frames in order to help keep track of those frames which did receive an acknowledgement.
- The receiver acknowledges a frame by sending an acknowledgement that includes the sequence number of the next frame expected. This acknowledgement announces that the receiver is ready to receive n frames, beginning with the number specified.
- Both the sender and receiver maintain what is called a window. The size of the window is less than or equal to the buffer size. Sliding window flow control has a far better performance than stop-and-wait flow control.

  For example, in a wireless environment if data rates are low and noise level is very high, waiting for an acknowledgement for every packet that is transferred is not very feasible. Therefore, transferring data as a bulk would yield a better performance in terms of higher throughput.

  The window maintained by the sender indicates which frames he can send. The sender sends all the frames in the window and waits for an acknowledgement (as opposed to acknowledging after every frame). The sender then shifts the window to the corresponding sequence number, thus indicating that frames within the window starting from the current sequence number can be sent.

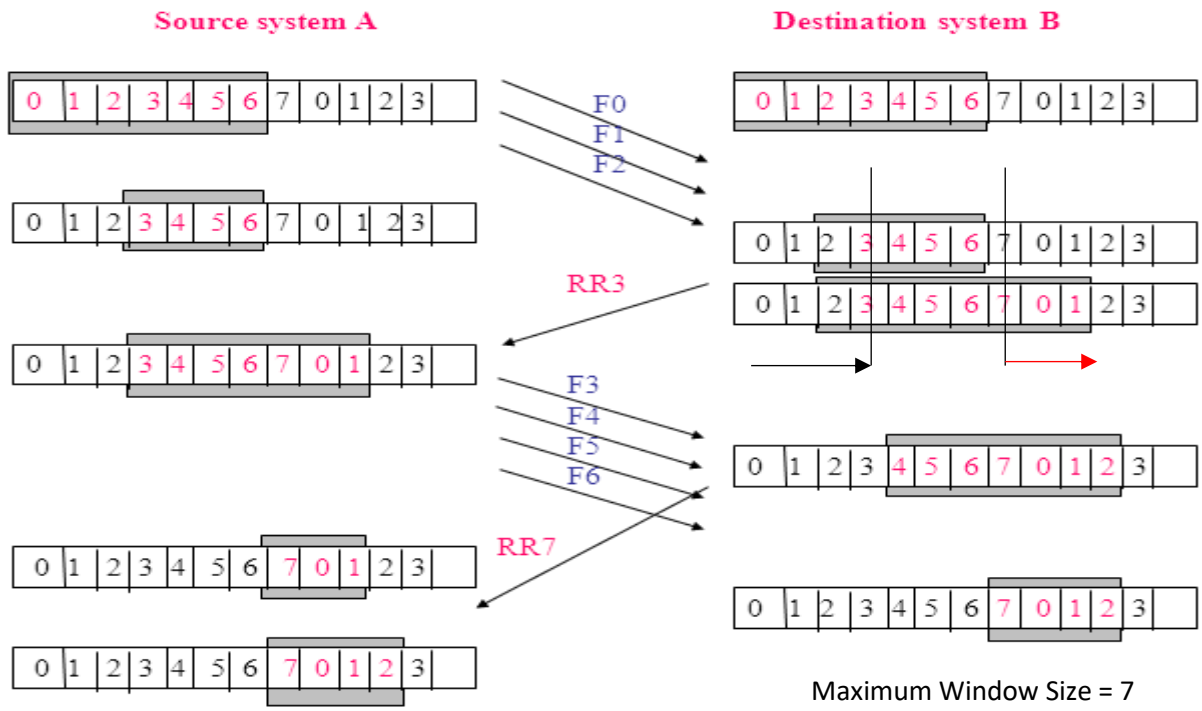


How Flow control is achieved?

• Receiver can control the size of the sending window.

• By limiting the size of the sending window data flow from sender to receiver can be limited .

*The example assumes a **3-bit** sequence number field and a maximum window size of **2^n-1= 7** frames. Initially, Source and Destination have windows indicating that Source may transmit **7** frames, beginning with frame **0 (FO).** After transmitting **3** frames **(FO, F1, F2)** without acknowledgment, Source has contracted its window to **4** frames. The window indicates that Source may transmit **4** frames, beginning with frame number **3**. Destination then transmits an **RR (receive-ready) 3(RR3),** which means: "I have received all frames up to frame number **2(F2)** and am ready to receive frame number **3(F3);** in fact, I am prepared to receive **7** frames, beginning with frame number **3(F3)."** With this acknowledgment, Source is back up to permission to transmit **7** frames, still beginning with frame **3(F3**). Source proceeds to transmit frames **3, 4, 5 , and 6**. Destination returns an **RR 7,** which allows Source to send up to and including frame **F2.***



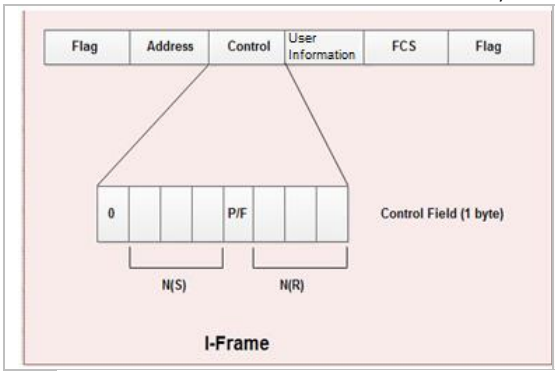
3.5. Examples of Protocol: HDLC, PPP

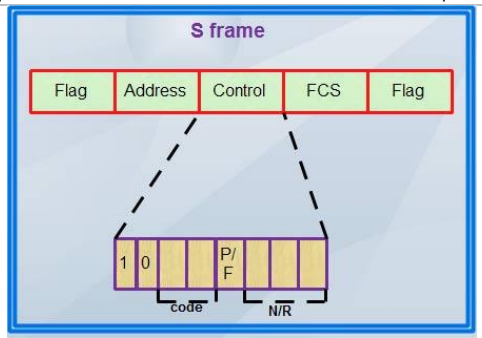
* HDLC:

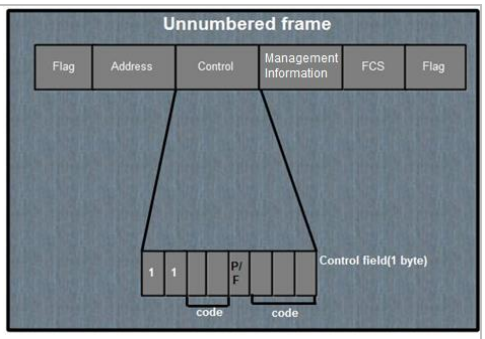
- **SDLC** is a data link layer transmission protocol developed by IBM in the 1970s. This protocol is used to makes sure if the data successfully transmits or not. It is also a modification of SDLC protocol. Data is organized into frames and sent across a network to a destination node. The data frame contains Address, Control, Data and checksum where the **Address** is used to identify terminal, **Controls** are the different type of control signal, etc. and **Checksum** are for the error detection purpose.
- HDLC (High-level Data Link Control) is a group of protocols or rules for transmitting data between network points (sometimes called nodes). In HDLC, data is organized into a unit (called a frame) and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent.
- Variations of HDLC are also used for the public networks that use the X.25 communications protocol and for frame relay, a protocol used in both and wide area network, public and private.

Types of HDLC frames:

- Information frames/User data (I-frames) : carry user's data and control information about user's data. The first bit of control field is always zero, i.e. the presence of zero at this place indicates that it is I-frame.
- Supervisory frames/Control data (S-frames) : carries control information, primarily data link layer flow and error controls. It does not contain information field. The first two bits in the control field of S-frame are always 10.
- Unnumbered frames (U-frames) : are used to exchange session management and control information between the two connected devices. Information field in U-frame does not carry user information rather, it carries system management information. U-frame is identified by the presence of 11 in the first and second bit position in control field.







N(S) = specifies the sequence number of the frame.
P/F i.e. Poll/Final = used for these two purposes. It has, meaning only when it is set i.e. when P/F=1. It can represent the following two cases.
(i) It means poll when frame is sent by a primary station to secondary (when address field contains the *address of receiver*).
(ii) It means final when frame is sent by secondary to a primary station (when the address field contains the *address of the sender*).
N(R) i.e. the receive sequence number of the frame expected in return in two-way communication.
If last frame received was error-free then N(R) number will be that of the next frame is sequence. If the last frame was not received correctly, the N(R) number will be the number of the damaged frame, asking for its retransmission.

N(S): Send Sequence Number

Flag Field: Flag fields define the frame at both ends with the unique pattern 01111110. A single flag may be used as the closing flag for one frame and the opening flag for the next. On both sides of the user-network interface, receivers are continuously hunting for the flag sequence to synchronize on the start of a frame. While receiving a frame, a station continues to hunt for that sequence to determine the end of the frame. Since the pattern 01111110 may appear in the frame as well, a procedure know and bit stuffing is used. After detecting a starting flag, the receiver monitors the bit stream.

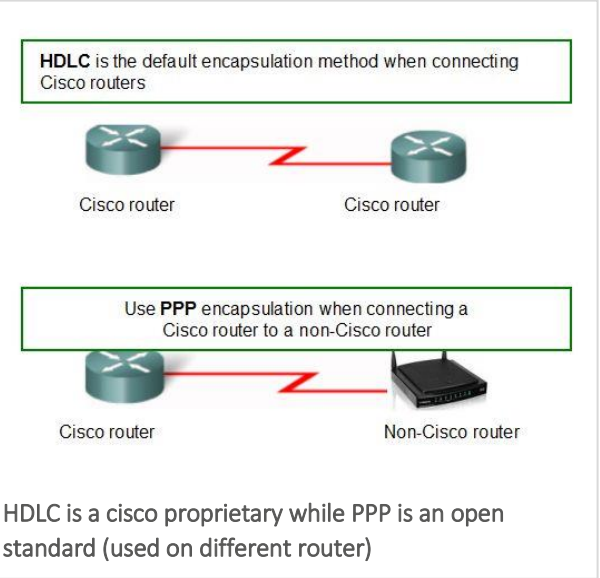
- When a pattern of **five 1s** appears, the **sixth bit** is examined. If this bit is **0**, it is deleted.
- If the **sixth bit** is a **1** and the seventh bit is a **0**, the combination is accepted as a flag.
- If the **sixth and seventh bits** are both 1, the sender is indicating an abort condition.

Address Field: The address field identifies the secondary station that transmitted or is to receive the frame.

Control Field: It defines the three types of frames I,U and S Frame for HDLC.

Information Field: This field is present only in I frame and some U Frame.

Frame Check Sequence Field(FCS): Its and error detecting code calculated from the remaining bits of the frame, exclusive of flags.



HDLC is a cisco proprietary while PPP is an open standard (used on different router)

*** PPP:** This protocol is used for the point-to-point connection between terminals within the internet. It is often used to connect home users to the internet. E.g. user connect with remote server

- In computer networking, Point-to-Point Protocol (PPP) is a data link (layer 2) protocol used to establish a direct connection between two nodes.
- It can provide connection authentication, transmission encryption (using ECP, RFC 1968), and compression.
- PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET.
- PPP is also used over access connections. Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol.

PPP connections are used to connect LANs to service provider WANs, and to connect LAN segments within an organization network. A LAN-to-WAN point-to-point connection is also referred to as a serial connection or leased-line connection, because the lines are leased from a carrier (usually a telephone company) and are dedicated for use by the company leasing the lines.

PPP provides several services:

- PPP defines the format of the frame to be exchanged between devices.
- PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP defines how network layer data are encapsulated in the data link frame.
- PPP defines how two devices can authenticate each other.
- PPP provides multiple network layer services supporting a variety of network layer protocols.
- PPP provides connections over multiple links.
- PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

On the other hand, to keep PPP simple, several services are missing:

- PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver.
- PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order.
- PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

PPP is used to carry out the following Functions:

- **-Data Encapsulations:** this is a method used to encapsulate multi-protocol datagrams. Different network-layer protocols are simultaneously transported and encapsulated over the same link, the flexibility of the PPP design enables it to be compatible to most supporting network devices.
- **-Link Control Protocol**: The LCP is used to establish, configure, and test the data link connection. It's flexible in *handling different sizes of packets, detect a looped-back link, configuration errors, and terminate the link.*
- **-Network Control Protocol:** NCP is used for establishing and configuring different Network layer protocols. *PPP enables the simultaneous use of multiple Network layer protocols.*

01111110	11111111	11000000				01111110
FLAG	ADDRESS	CONTROL	PROTOCOL	PAYLOAD	FCS	FLAG
1 Byte	1 Byte	1 Byte	1 or 2 Byte	Variable	2 or 4 Byte	

Fig. PPP Frame Format

Flag. A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110. Although this pattern is the same as that used in HDLC, there is a big difference. PPP is a byte-oriented protocol; HDLC is a bit-oriented protocol. The flag is treated as a byte, as we will explain later.

Address. The address field in this protocol is a constant value and set to 11111111 (Broadcast Address).

Control. This field is set to the constant value 11000000 (imitating unnumbered frames in HDLC). PPP does not provide any flow control. Error control is also limited to error detection. This means that this field is not needed at all, and again, the two parties can agree, during negotiation, to omit this byte.

Protocol. The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

Payload. This field carries either the user data or other information. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte- stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.

FCS. The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

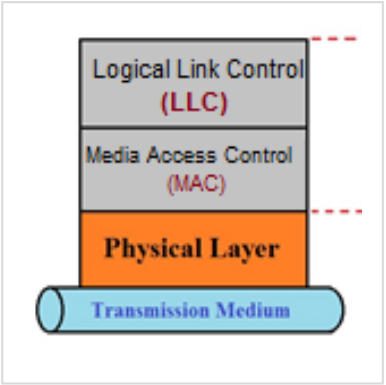
Difference between HDLC and PPP protocols.

HDLC	PPP
Operates at layer-2 (i.e. Data link layer)	Operates at layer-2 and layer-3 (i.e. network layer)
bit oriented protocol	byte oriented protocol
It does not have method to detect the errors.	It detects the errors while transmitting the data.
HDLC protocols have two types viz. ISO HDLC and Cisco HDLC	It uses HDLC format as defined by ISO.
It used to perform encapsulation of data without using other encapsulation protocols.	PPP can not encapsulate data without the help of other encapsulation protocols such as HDLC, SDLC(synchronous data link control)
It does not support authentication i.e. it fails to provide authentication between two nodes.	It supports authentication using protocols such as PAP and CHAP
It provides a frame format which contains a proprietary field. The other 6 fields are similar to PPP protocol frame fields. ISO HDLC do not have proprietary field and hence has only 6 fields.	It provides a frame format which contains a protocol field. The other 6 fields are similar to HDLC frame field.
It fails to check for quality of a link established.	It uses link control protocol(LCP) to check for quality of the established link.

3.6. The Media Access Sub Layer

In the Open Systems Interconnection (OSI) model of communication, the Media Access Control layer is one of two sublayers of the Data Link Control layer and is concerned with sharing the physical connection to the network among several computers. Each computer has its own unique MAC address. **Ethernet** is an example of a protocol that works at the Media Access Control layer level. MAC is responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel.

Medium Access Sub Layer deals with broadcast networks and their protocols. In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it. So, a controlling unit should be defined which permits only one request to access the single channel, this is done by sub layer of the data link layer called the MAC (Medium Access Control) sub-layer.



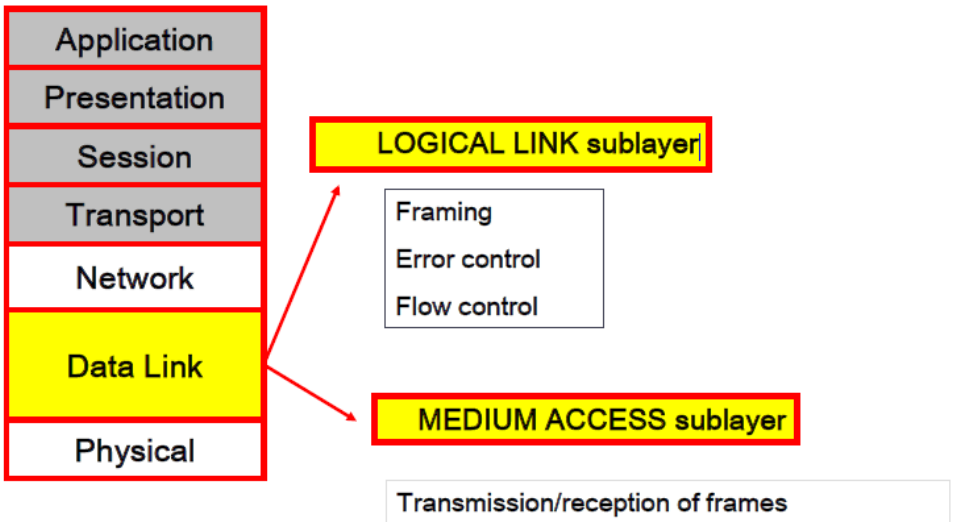


Fig: Medium Access Sub-Layer

Medium Access Layer deals with:

- Broadcast networks and their protocols (*group of radio stations, television stations, or other electronic media outlets, that form an agreement to air, or broadcast, content from a centralized source. E.g. BBC U.K.*)
- Channel allocation problem (*How to allocate a single broadcast channel among competing users*)
- Multiple access protocols (*protocol is used to coordinate access to the link. Or Single shared broadcast channel, determines how nodes share channel, i.e., determine when node can transmit)*
- IEEE standards 802 for LANS (*802.3-Ethernet, 802.11-Wireless LAN etc*)
- Datalink Switching(*tunneling protocol designed to tunnel unrouteable, non-IP based protocols such as IBM Systems Network Architecture (SNA) and NBF over an IP network.)*
- VLANs (is *broadcast domain that is partitioned and isolated in a computer network)*

What MAC layer does?

- (ON SENDERS END) It receives packet form network layer and attach header to it, header includes 48-bit MAC address *(which is unique to each machine provided by manufacturer unlike IP address which is provided by network provider)*, also includes Error correction bits
- (ON RECIVERS END) It receives frame from physical layer, verify if frame has destination MAC address of this computer only if yes accept that frame, removes frame header and forward remaining pay load to Network layer
- It also ensures a collision free transmission of frames in some of the protocol like 802.3(Ethernet LAN) or 802.11(Wireless LAN)

The primary functions performed by the MAC layer are:

- acts as an interface between the Logical Link Control sublayer and the network's physical layer
- provides an addressing mechanism called physical address or MAC address. This is a unique serial number assigned to each network adapter, making it possible to deliver data packets to a destination within a subnetwork, i.e. a physical network without routers, e.g. Ethernet network.
- provides the protocol and control mechanisms that are required for a certain channel access method. This makes it possible for several stations connected to the same physical medium to share it. E.g. bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links.

Protocols are used by Medium Access Layer :

- **ALOHA (Advocates of Linux Open-source Hawaii Association or Additive Links On-line Hawaii Area):** ALOHA is a system for coordinating and arbitrating access to a shared communication channel.
- **Carrier Sensed Multiple Access (CSMA) :** CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
- **CSMA/CD (Carrier Sense Multiple Access/Collision Detection) :** CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time.
- **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) :** In CA collision avoidance), collisions avoided because each node signals its intent to transmit before actually doing so.
- **Ethernet : IEEE 802.3 Local Area Network (LAN) Protocols :** Ethernet protocols refer to the family of local-area network (LAN)covered by the IEEE 802.3.
- **IEEE 802.4 Token Bus :** In token bus network station must have control of a token before it can transmit on the network. The topology of the network can include groups of workstations connected by long trunk cables.
- **IEEE 802.5 Token Ring :** Token ring is the IEEE 802.5 standard for a token-passing ring network with a star-configured physical topology

3.7. Channel Allocation Problem

The channel allocation problem is "How to allocate a single broadcast channel among competing users". There are two schemes that can be applied to allocate a single channel among competing users and they are:

1. **Static Channel Allocation :** Static channel allocation can be done by using the static multiplexing method; FDM and TDM (Frequency/Time Division Multiplexing). FDM is used in Radio or TV broadcasting whereas TDM is POTS (Plain Old Telephone System). These channel allocation techniques waste bandwidth as they cannot handle with the dynamic environment.
2. **Dynamic Channel Allocation :** Dynamic Channel Allocation is done by using Pure/Slotted ALOHA Protocol or Carrier Sense Multiple Access (CSMA) Protocols. It is more efficient than static channel allocation as it uses collision free protocols and doesn't waste bandwidth.

In Detail …

Static Channel Allocation(Synchronous) in LANs and MANs

With static Channel Allocation, a specific capacity is dedicated to a connection; this is the *same approach used in circuit switching, frequency-division multiplexing (FDM), and synchronous time-division multiplexing (TDM)*. Such techniques are generally not suitable in LANs and MANS because the needs of the stations are random.

If any connection is not transferring information, then the channel is wasted which is allocated to particular connection. Therefore, it is better for bulky and heavy data.

- The traditional way of allocating a single channel, such as a **telephone trunk**, among multiple competing users is Frequency Division Multiplexing (FDM). If there are N users, the bandwidth is divided into N equal-sized portions each user being assigned one portion. Since each user has a private frequency band, there is no interference between users.

- When there are only a small and constant number of users, each of which has a heavy (buffered) load of traffic (e.g., carriers' switching offices), FDM is a simple and efficient allocation mechanism. However, when the number of senders is large and continuously varying or the traffic is bursty, FDM presents some problems.
- If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. If more than N users want to communicate, some of them will be denied permission for lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever transmit or receive anything.

Dynamic Channel Allocation (Asynchronous)

In dynamic channel allocation, capacity is given whenever there is any need. It is divided into 3 groups,

- ROUND ROBIN: With round robin each turn is given the opportunity to transmit. During that opportunity the station may decline to transmit or may transmit subject to a specific upper bound.
  When many stations have data to transmit, round robin technique can be efficient. If only a few stations have data to transmit, then, there is a considerable overhead in passing the turn from station to station, because most of the stations can't transmit but simply pass their turns.
- RESERVATION: It is used for stream traffic, in reservation techniques time on the medium is divided into slots, much as with TDM. Reservation can be made in centralized or distributed fashion.
- CONTENTION: It is used for bursty traffic, with contention, no control is exercised to determine whose turn it is, all stations contend for time in a way that can be.

3.8. Multiple Access Protocol

Multiple access protocol is used to control/coordinate access to the link or link in a shared connection. Nodes can regulate their transmission within the shared broadcast channel by using Multiple Access Protocol. All the nodes can transmit a frame at the same time. This may arise to the collision, so to overcome this Multiple Access protocol is implemented.

Generally, there are two types of Network Links: point-to-point links, and broadcast links.

- A **Point-to-Point link** consists of a single sender on one end of the link, and a single receiver at the other end of the link. Many link-layer protocols have been designed for point-to-point links; PPP (the point-to-point protocol) and HDLC are two such protocols
- A **Broadcast link,** can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel. The term "broadcast" is used here because when any one node transmits a frame, the channel broadcasts the frame and each of the other nodes receives a copy.

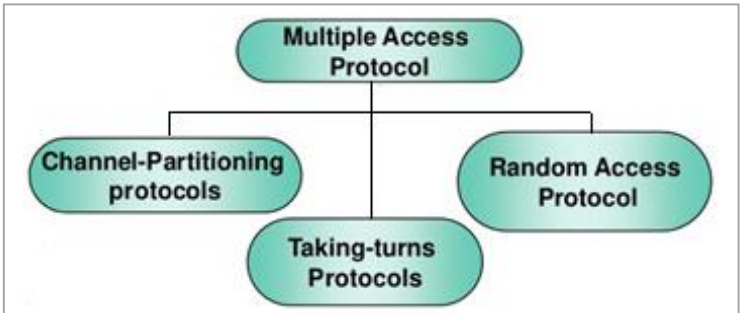


Fig: Types of Multiple Access Protocol

  - Ethernet is probably the most widely deployed broadcast link technology first examine a problem of central importance to the data link layer: how to coordinate the access of multiple sending and receiving nodes to a shared broadcast channel - the so-called multiple access problem.
  - Broadcast channels are often used in Local Area Networks (LANs), networks that are geographically concentrated in a single building (or on a corporate or university campus).

Classification of Multiple Access Protocols

1. Random Access Protocols
   When node has packet to send
   a. transmit at random at full channel data rate R.
   b. no a priori coordination among nodes
   If two or more nodes are transmitting at once, we get a "collide", then they retransmit at random times, random access MAC protocol specifies:
   c. how to detect collisions
   d. how to recover from collisions (e.g., via delayed retransmissions)
   Examples of random access MAC protocols: slotted ALOHA, ALOHA, CSMA and CSMA/CD
2. **Channel partitioning protocol:** channel is divided **e.g.** TDMA, FDMA and CDMA (Code Division Multiple Access) where
   - TDMA shares the channel according to time slots,
   - FDMA share channel in different frequency range and
   - CDMA divide the channel by providing unique codes.
3. Controlled Access Protocols
   In controlled access, A station cannot send unless it has been authorized by other stations. The stations consult one another to find which station has the right to send.

3.9. Ethernet

Ethernet is a computer networking technology used in LANs and MANs. It is the most widely used for local area network (LAN) technology. Ethernet is a link layer protocol in the TCP/IP stack, describing how networked devices should format data for efficient transmission between other network devices on the same network segment, and how to put that data out on the network connection.

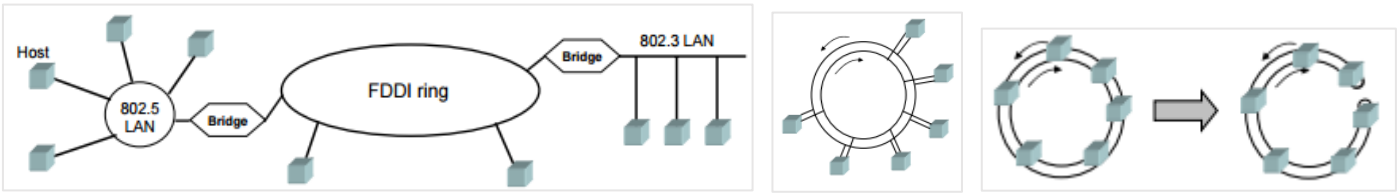
3.10. Networks

* Fiber Distributed Data Interface (FDDI)

The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper. FDDI (Fiber Distribution Data Interface) is similar to Token ring as it shares several characteristics including token passing and a ring architecture. FDDI uses a dual-ring connection architecture. Traffic on each ring in the interface flows in opposite directions (called counter-rotating). The dual rings have a primary and a secondary ring. The **primary ring** is used for data transmissions during normal operation while the **secondary ring** remains idle. The secondary ring is only used when the primary ring fails or to send some special information. The primary purpose of the dual rings is to make the network reliable and robust.

FDDI provides multiple ways to connect devices to the ring. FDDI defines three types of devices that can be connected: Single Attachment Station (SAS)- attached to one ring. like PCs, Dual Attachment Station (DAS)- attached to both rings like routers, servers, and a concentrator.

- FDDI is a high-performance token ring LAN based on optical fibers
- ANSI standard X3T9.5
- Data rates of 100 MBit/s
- Range of up to 200 km
- Support of up to 1000 stations, with distances of maximally 2 km
- Often used as Backbone for small LANs



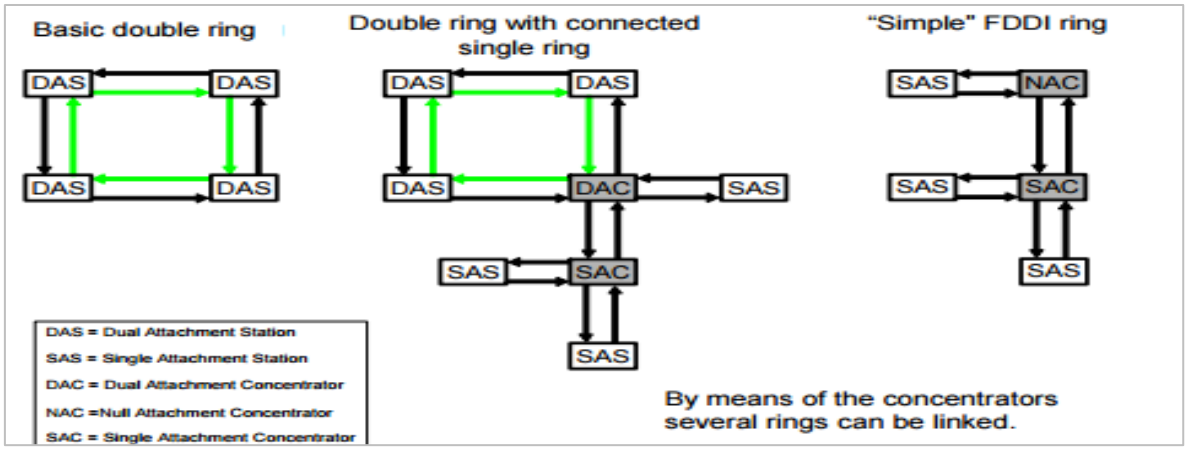
Structure of FDDI - Wiring within FDDI: 2 optical fiber rings with opposite transmission direction.

- During normal operation, only the primary ring is used, the secondary ring remains in readiness
- If the ring breaks, the other one (also called protection ring) can be used.
- If both rings break or if a station precipitates, the rings can be combined into only one, which has double length:

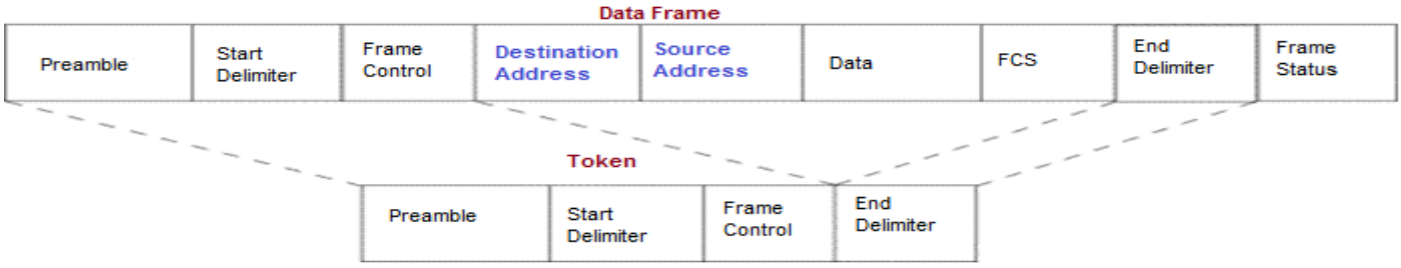
Two classes of stations exist:

i. DAS (Dual Attachment Station) can be attached to both rings, the cheaper
ii. SAS (Single Attachment Station) are only attached to one ring.

FDDI Configuration



FDDI Frame Format



FDDI that is completely compatible with the ANSI standard version.

- ***Preamble***---A unique sequence that prepares each station for an upcoming frame.
- ***Start Delimiter***---Indicates the beginning of a frame by employing a signaling pattern that differentiates it from the rest of the frame.

- *Frame Control*---Indicates the size of the address fields and whether the frame contains asynchronous or synchronous data, among other control information.
- *Destination Address*---Contains a unicast (singular), multicast (group), or broadcast (every station) address. As with Ethernet and Token Ring addresses, FDDI destination addresses are 6 bytes long.
- *Source Address*---Identifies the single station that sent the frame. As with Ethernet and Token Ring addresses, FDDI source addresses are 6 bytes long.
- *Data*---Contains either information destined for an upper-layer protocol or control information.
- *Frame Check Sequence (FCS)*---Filed by the source station with a calculated cyclic redundancy check value dependent on frame contents (as with Token Ring and Ethernet). The destination address recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- *End Delimiter*---Contains unique symbols, which cannot be data symbols, that indicate the end of the frame.
- *Frame Status*---Allows the source station to determine whether an error occurred and whether the frame was recognized and copied by a receiving station.

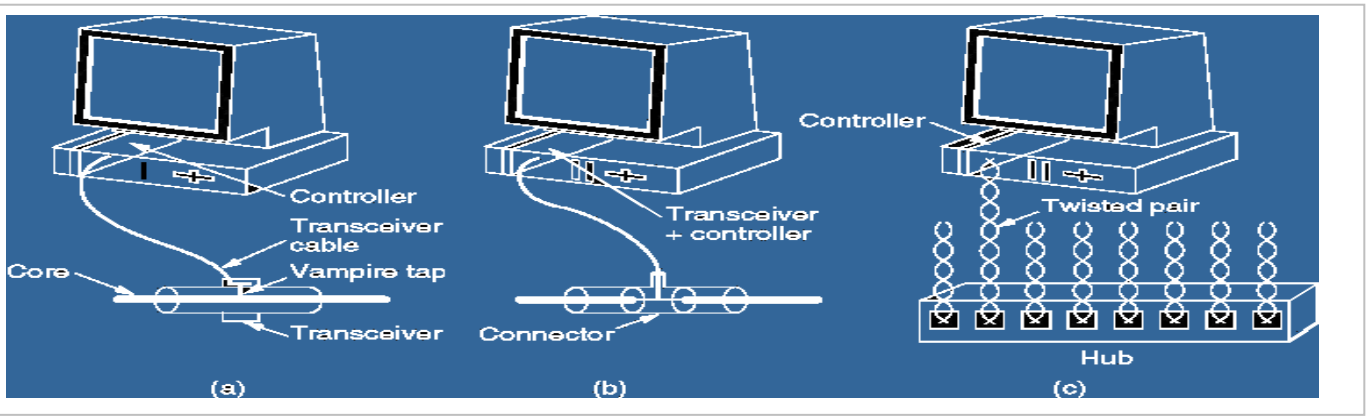
* Ethernet

Ethernet is a computer networking technology used in LANs and MANs. It is the most widely used for local area network (LAN) technology. Ethernet is a link layer protocol in the TCP/IP stack, describing how networked devices should format data for efficient transmission between other network devices on the same network segment, and how to put that data out on the network connection.

- IEEE has standardized a number of LANs and MANs under the name of **IEEE 802**. A few have survived but many have not.
- The most important of the survivors are **802.3** (Ethernet) and **802.11** (wireless LAN)
- For **802.15** (Bluetooth) and **802.16** (wireless MAN), it is too early to tell.
- Both 802.3 and 802.11 have different physical layers and different MAC sublayers but converge on the same logical link control sublayer (defined in 802.2), so they have the same interface to the **network layer**.

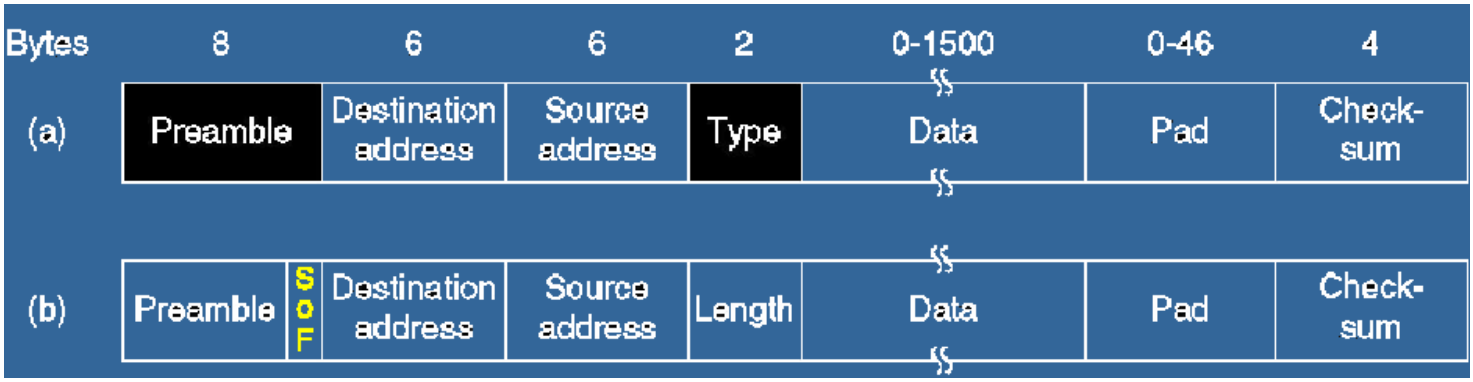
Ethernet Cabling

Name	Cable	Max seg.(m)	Nodes per segment	Advantages
10Base5	thick coax	500	100	The Original
10Base2	thin coax	185	30	no hub
10Base-T	twisted pair (UTP)	100	1024	cheapest
10Base-F	fiber	2000	1024	long distance



10Base5 10Base2 10Base-T

Ethernet Frame Format **DIX** (DEC, Intel, Xerox)



IEEE 802.3

- **Preamble**: Sequence of 10101010s. 8 bytes.
  - *(SOF, Start of Frame delimiter, for compatibility with 802.4 and 802.5)*
- **Addresses**: 2 or 6 bytes.
  - high-order bit of the destination address:
    - 0 for ordinary addresses
    - 1 for group addresses.
  - bit 46 - global or local address.
- **Type**: specifies which process to give the frame to.
  - *(Any number <=1500 is treated as length or as type otherwise.)*
- **Data**: up to 1500 bytes.
- **Pad**: (optional) The frame must be at least 64 bytes in total!
- **Checksum**: CRC based on this polynomial: $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

* ALOHA

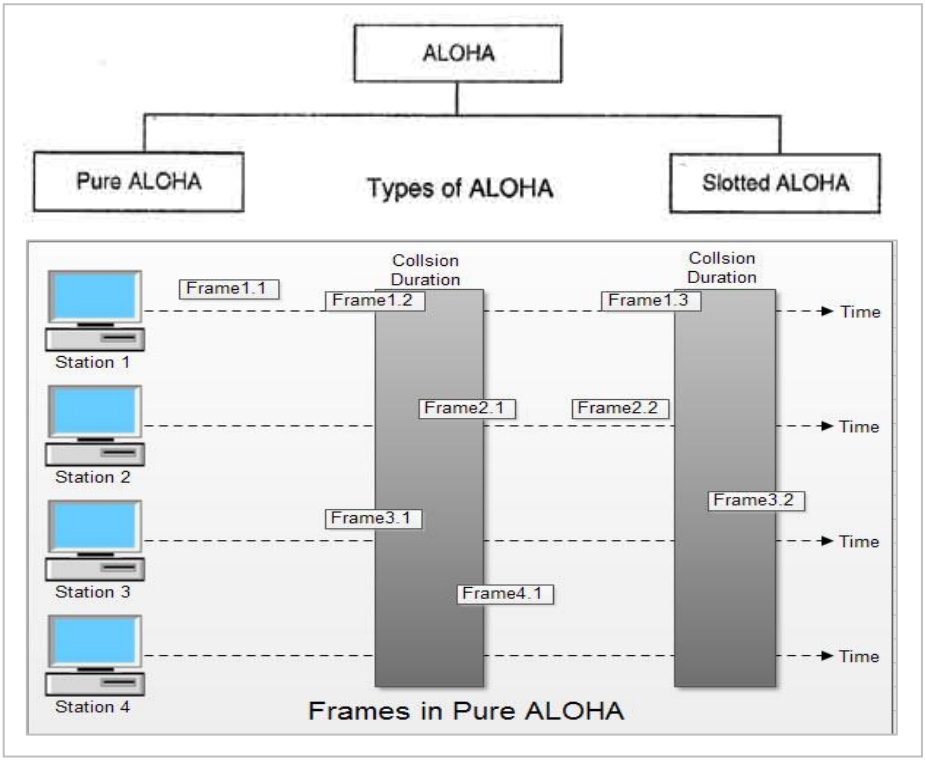
ALOHA is a system for coordinating and deciding access to a shared communication Networks channel. It was developed in the **1970s** by Norman Abramson and his colleagues at the **University of Hawaii**. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. The **Slotted Aloha** protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

- Abramson et. al., University of Hawaii, designed for early satellite systems in early 1970s.
- Nodes transmit whenever they have data to send
- Then listen to positive ACK on a separate link
- If timeout (collision), waits random time and then retransmits
- Free decentralized
- Slot synchronization reduces collision probability ⇒ Slotted ALOHA

Types of ALOHA:



(i) Pure ALOHA

The original ALOHA protocol is called pure ALOHA. This is a simple, but an elegant protocol. The idea is that each station can send a frame whenever it wants a frame to send. However, since only one channel is shared among stations, there is the chance of collision between frames send from different stations. When a station sends a frame, it waits for the receiver to send an acknowledgment. If the receiver doesn't acknowledge for a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed at the middle and resends the frame.

A collision can occur between two or more stations. If all the stations resend their frames after the time-out, the frames will collide again. So, each station waits for a random amount of time before resending its frame. The randomness will help to avoid further collisions.

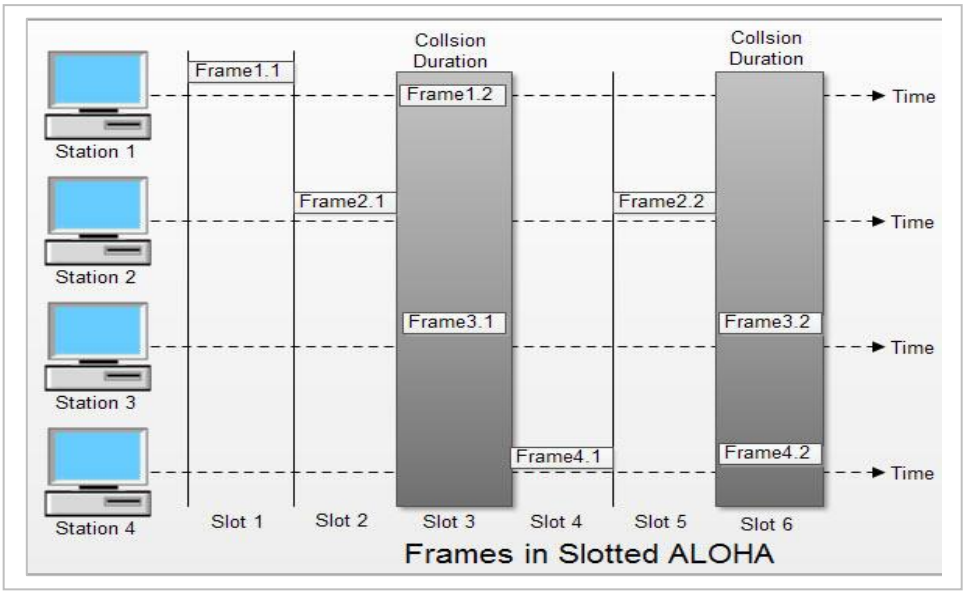
In pure ALOHA, the stations transmit frames whenever they have data to send.

- *When two or more stations transmit simultaneously, there is collision and the frames are destroyed.*
- In pure ALOHA, *whenever any station transmits a frame, it expects the acknowledgement from the receiver.*
- *If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.*
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore, pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

• Figure shows an example of frame collisions in pure ALOHA.
• In fig *there are four stations that. contended with one another for access to shared channel.* All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.
• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

(ii) Slotted ALOHA

Slotted ALOHA is an improvement over the pure ALOHA. *Pure ALOHA has no rule that defines when the station can send*. A station may send anytime: after another station has started before another station has finished. In slotted ALOHA time is divided into the slot and the station can send only at the beginning of every time slot. As a station is only allowed to send at the beginning of the time slot; if a station misses this moment, it has to wait until the next time slot begins. But, still, there is the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is reduced to one-half.



• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
• In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
• The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.
• In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot.
• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

*** VLAN -** Virtual local area network

- It is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain.
- systems on one VLAN don't see the traffic associated with systems on other VLANs on the same network.

VLANs are the new type of LAN/BN architecture that uses intelligent, high-speed switches. VLAN assigns computers to LAN segments by using software. VLANs are designed in two ways Single-switch VLANs or Multi-switch VLANs. **In Single switch** VLANs, computers are assigned to VLANs using special software but physically connected together using a larger physical switch. Computer can be assigned to VLANs in different ways and they are:

- according to their VLAN switch port
- according to their data link layer address
- according to their IP address
- on the basis of the application that the computer uses

To understand VLAN more clearly let's take an example.

Our company has three offices. All offices are connected with back links. Company has three departments Development, Production and Administration. Development department has six computers, Production department and Administration department has three computers. Each office has two PCs from development department and one from both production and administration department. Administration and production department have sensitive information and need to be separate from development department.

With default configuration, all computers share same broadcast domain. Development department can access the administration or production department resources. With VLAN we could create logical boundaries over the physical network. Assume that we created three VLANs for our network and assigned them to the related computers.

- VLAN Admin for Administration department
- VLAN Dev for Development department
- VLAN Pro for Production department

Physically we changed nothing but logically we grouped devices according to their function. These groups [VLANs] need router to communicate with each other. Logically our network look likes following diagram.

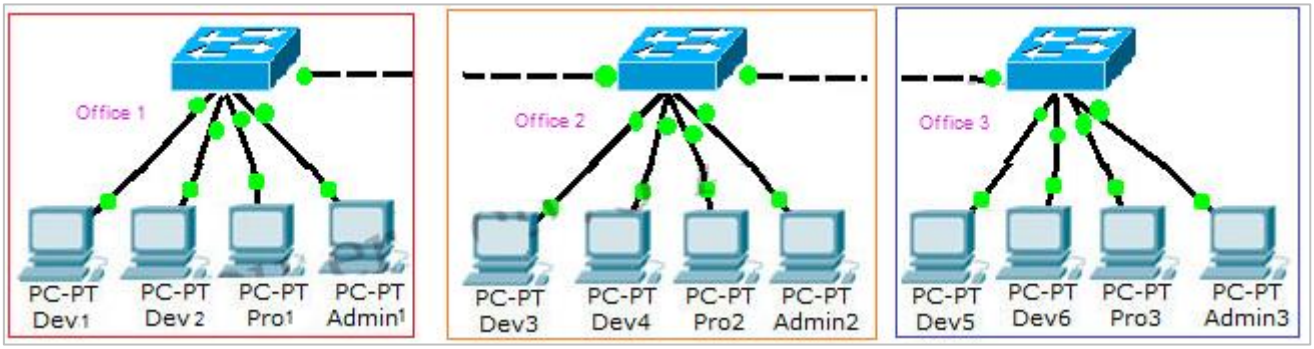


Fig . Same LAN with Different Departments

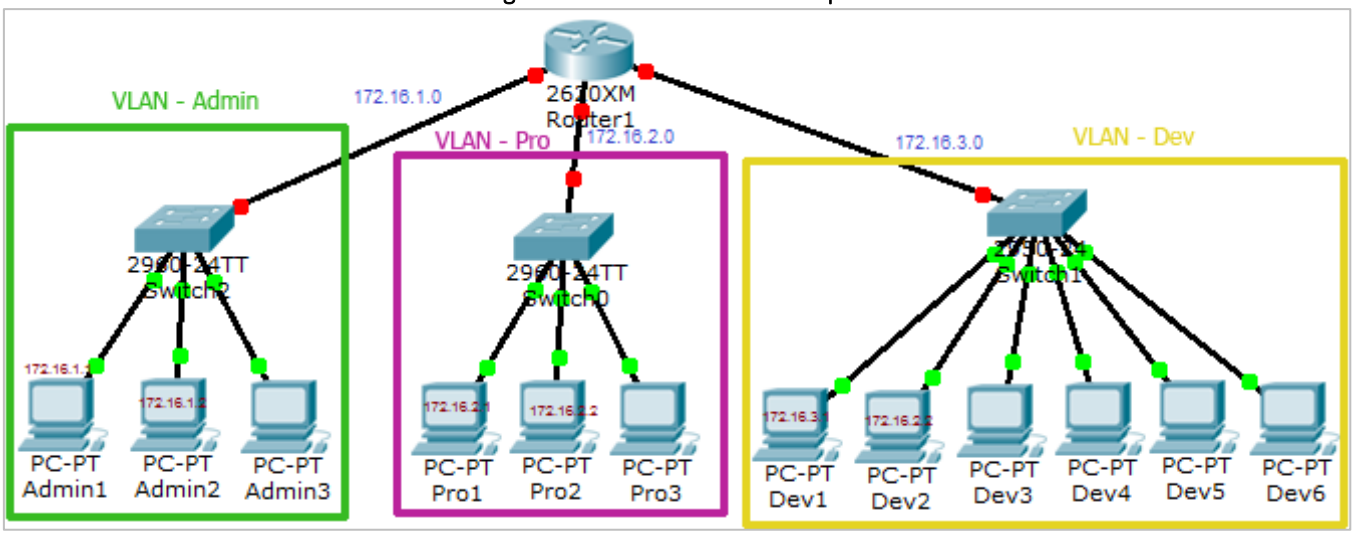


Fig. Different LAN with Different Departments

With the help of VLAN, we have separated our single network in three small networks. These networks do not share broadcast with each other improving network performance. VLAN also enhances the security. Now Development department cannot access the Administration and Production department directly. Different VLAN can communicate only via Router where we can configure wild range of security options.

VLAN membership can be assigned to a device by one of two methods. These methods decide how a switch will associate its ports with VLANs.

Static : Assigning VLANs statically is the most common and secure method. It is pretty easy to set up and supervise. In this method we manually assign VLAN to switch port. VLANs configured in this way are usually known as port-based VLANs.

As any switch port that we have assigned a VLAN will keep this association always unless we manually change it. It works really well in a networking environment where any user movement within the network needs to be controlled.

Dynamic : In dynamic method, VLANs are assigned to port automatically depending on the connected device. In this method we have configure one switch from network as a server. Server contains device specific information like MAC address, IP address etc. This information is mapped with VLAN. Switch acting as server is known as VMPS (VLAN Membership Policy Server). Only high end switch can configured as VMPS. Low end switch works as client and retrieve VLAN information from VMPS.

Dynamic VLANs supports plug and play movability. For example if we move a PC from one port to another port, new switch port will automatically be configured to the VLAN which the user belongs. In static method we have to do this process manually.

Why use VLAN's?

VLAN's offer a number of advantages over traditional LAN's.

1) Performance : In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic

2) Formation of Virtual Workgroups : Nowadays, it is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research. These workgroups are usually formed for a short period of time. During this period, communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them.

3) Simplified Administration : **70%** of network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, recalling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLAN's.

4) Reduced Cost : VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

5) Security : Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion

*** Carrier Sense Multiple Access/ Collision Detect (CSMA/CD)**

- ***Carrier sense*** *is the* ability of a network interface card (NIC) to check the network for any communication. Obviously if there is data being transmitted over the network, the NIC should not attempt to transmit data. If there is no traffic on the network, the NIC will then attempt to transmit the data.
- ***The MA (multiple access***) part of CSMA/CD tells us that there will be multiple devices using the same network. This, of course, means collisions are more than possible.
- The **CD (collision detect)** part of CSMA/CD states that we need a method for detecting a collision. After all, we need to tell other computers to hold off on transmissions until the problem is sorted.
- CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in ready and not-ready CSMA

Fig. Carrier Sense

Fig. Multiple Access

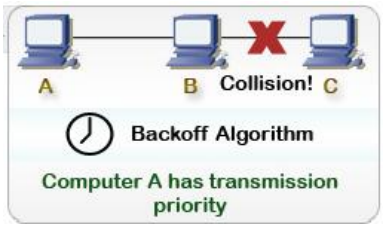
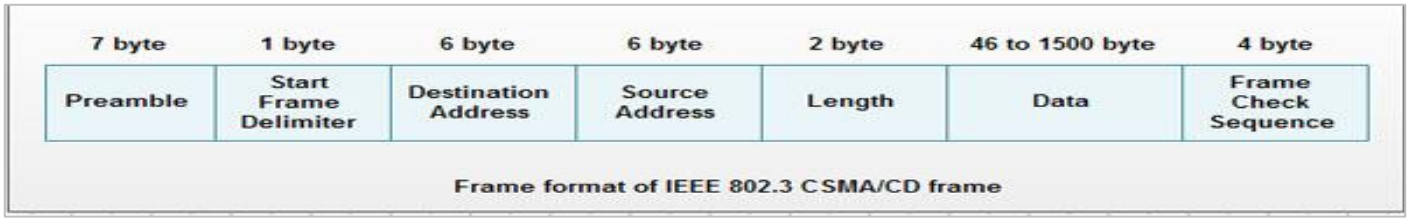


Fig. Collision Detect

Applications : *Now-obsolete shared media Ethernet variants (10BASE5, 10BASE2) and in the early versions of twisted-pair Ethernet which used repeater hubs. Modern Ethernet networks, built with switches and full-duplex connections*

Frame format of CSMA/CD

The frame format specified by IEEE 802.3 standard contains following fields.



1. **Preamble**: It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating 0s and 1s. The purpose is to provide alert and timing pulse.
2. **Start Frame Delimiter (SFD)**: It is one byte field with unique pattern: 10 10 1011. It marks the beginning of frame.
3. **Destination Address (DA)**: It is six byte field that contains physical address of packet's destination.
4. **Source Address (SA)**: It is also a six byte field and contains the physical address of source or last device to forward the packet (most recent router to receiver).
5. **Length**: This two byte field specifies the length or number of bytes in data field.
6. **Data**: It can be of 46 to 1500 bytes, depending upon the type of frame and the length of the information field.
7. **Frame Check Sequence (FCS)**: This for byte field contains CRC for error detection.

*** IEEE 802.3 (Ethernet)**

IEEE 802.3 is a working group and a collection of IEEE standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet. This is generally a local area network technology with some wide area network applications. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable.

- 802.3 is a technology that supports the IEEE 802.1 network architecture.
- 802.3 also defines LAN access method using CSMA/CD.
- 802.3 is a standard specification for Ethernet, a method of physical communication in a local area network (LAN), which is maintained by the Institute of Electrical and Electronics Engineers (IEEE). In general, 802.3 specifies the physical media and the working characteristics of Ethernet. The original Ethernet supports a data rate of 10 megabits per second (Mbps) and specifies these possible physical media:
    - 10BASE-2 (Thin wire coaxial cable with a maximum segment length of 185 meters)
    - 10BASE-5 (Thick wire coaxial cable with a maximum segment length of 500 meters)
    - 10BASE-F (optical fiber cable)
    - 10BASE-T (ordinary telephone twisted pair wire)
    - 10BASE-36 (broadband multi-channel coaxial cable with a maximum segment length of 3,600 meters)

The **"10"** in the media type designation refers to the transmission speed of 10 Mbps. The **"BASE"** refers to baseband signaling, which means that only Ethernet signals are carried on the medium (or, with 10BASE-36, on a single channel). The **"T"** represents twisted-

pair; the **"F"** represents fiber optic cable; and the **"2", "5", and "36"** refer to the coaxial cable segment length (the 185 meter length has been rounded up to "2" for 200).

7	1	6	6	2	46-1500bytes	4
Pre	SFD	DA	SA	Length Type	Data unit + pad	FCS

Fig: IEEE 802.3 header format

Preamble (Pre) : 7 Bytes bit pattern 10101010… used for synchronization
Start-of-frame delimiter(SFD) : 10101011 indicates Start of Frame
DA,SA : 6 bytes Destination and Source MAC Addresses
Length/Type : Length of data Field in bytes (but in Ethernet II, this field identifies the Type of Network Layer Protocol used.)
Data : Upper Layer Data (min. 46 bytes, max.1500 bytes)
FCS : 4 Bytes error detection CRC Calculated over DA, SA, Length and Data Fields

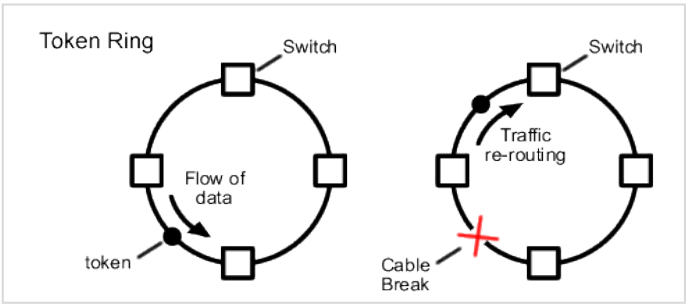
IEEE (Institute of Electrical and Electronics Engineers)

- **1984 AIEE** (American Institute of Electrical Engineers) was founded.
- **1963 IEEE** (Institute of Electrical and Electronics Engineers) was born, 1,50,500 members (1,40,000 members from US)
- **IEEE 802** standards deals in LAN and MAN

*** Token Ring (IEEE 802.5)**

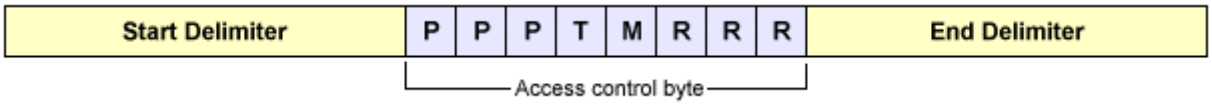
IEEE 802.5 uses token ring technique where a small frame called token is passed around the network. The node which passes the token can transmit data. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

- It requires that stations take turns to send data
- Each station may transmit only during its turn and may send only one frame during each turn.
- The mechanism that coordinates this rotation is called token passing.
- Token travel along the ring basis.



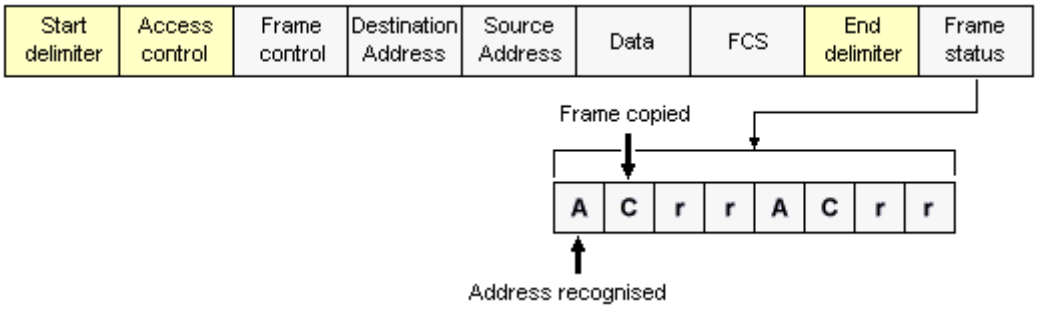
Frame format

Two basic frame types are used - tokens, and data/command frames. The token is three bytes long and consists of a *start delimiter*, an *access control byte*, and an *end delimiter*. The format of the token is shown below.



The Token Ring token

A data/command frame has the same fields as the token, plus several additional fields. The format of the data/command frame is shown below.



The Token Ring frame format

- ***Start delimiter*** - alerts each station of the arrival of a token or frame.
- ***Access control byte*** - contains the *priority field*, the *reservation field*, the *token bit* and a *monitor bit*.
- ***Frame control byte*** - indicates whether the frame contains data or control information. In a control frame, this byte specifies the type of control information carried.
- ***Destination and source addresses*** - two six-byte fields that identify the destination and source station MAC addresses.
- ***Data*** - the maximum length is limited by the ring *token holding time*, which defines the maximum time a station can hold the token
- ***Frame check sequence (FCS)*** - filled by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- ***End delimiter*** - signals the end of the token or frame, and contains bits that may be used to indicate a damaged frame, and to identify the last frame in a logical sequence.

- ***Frame status*** - a one-byte field that terminates a frame, and includes the one-bit *address-recognized* and *frame-copied* fields. These one-bit fields, if set, provide confirmation that the frame has been delivered to the source address and the data read.

*** Token Bus (IEEE 802.4)**

IEEE 802.4 was developed combining robustness of Linear Medium 802.3 and predictability of token passing. Stations are attached onto linear tree shaped cable. Each station knows the address of its left and right neighbors. A ring is first initialized by using a coordinator and the stations are inserted in the order of their address.

- The 802.4 IEEE standard defines the Token Bus protocol, combines features of Ethernet (Bus Topology) and Token Ring.
- Stations are logically organized into a ring. A token is passed among the stations. If a station wants to send data, it must wait and take the token
- The logical ring is formed based on the MAC address of the station in descending order.
- Each station considers the immediate lower address as next station and the station with immediate higher as the previous station.

Example :

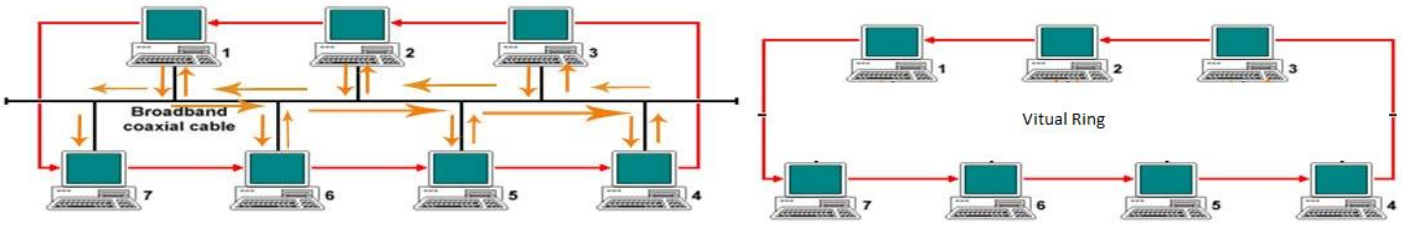
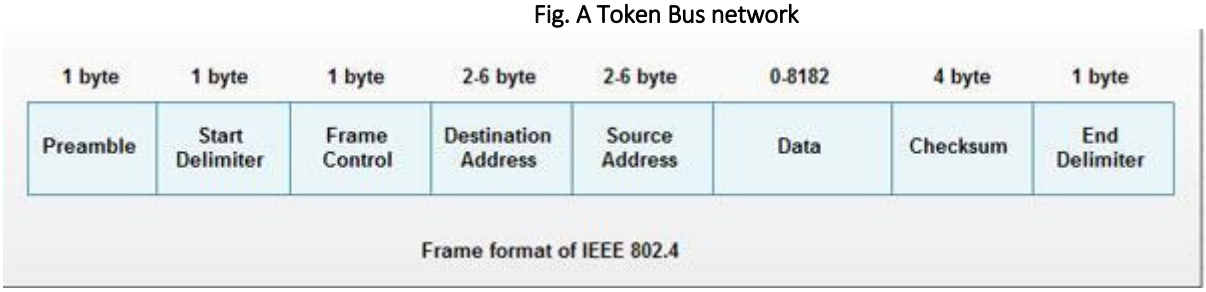


Fig. A Token Bus network



Frame format of IEEE 802.4

- **Preamble**: This. Field is at least 1 byte long. It is used for bit or clock synchronization.
- **Start Delimiter**: This one-byte field marks the beginning of frame.
- **Frame Control:** This one-byte field specifies the type of frame includes token passing and various ring maintenance frames, including the mechanism for letting new station enter the ring, the mechanism for allowing stations to leave the ring.
- **Destination address**: It specifies 2 to 6 bytes destination address.
- **Source address**: It specifies 2 to 6 bytes source address.
- **Data**: for 2 bytes addresses, up to 8182 bytes long are used and for 6 bytes address, up to 8174 bytes long is used.
- **Checksum**: This 4-byte field detects transmission errors.
- **End Delimiter**: This one-byte field marks the end of frame.

*** 802.11 IEEE wireless LAN standards**

802.11 and *802.11x* refers to a family of specifications developed by the IEEE for ***wireless LAN*** (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

A wireless LAN (WLAN or WiFi – Wireless Fidelity) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure

In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired network and a group of client computers, giving these users wireless access to the full resources and services of the corporate network across a building or campus setting.

802.11 standards focus on the bottom two levels the ISO model, the physical layer and link layer (see figure below). Any LAN application, network operating system, protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

The major motivation and benefit from Wireless LANs is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere.

Types of 802.11

1. **Infrastructure based**: Wire network to wireless network
2. **Ad-hoc**: wireless network to wireless networks

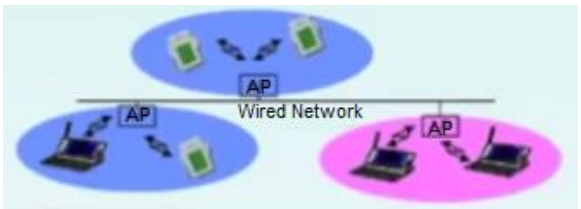


Fig. Infrastructure Based

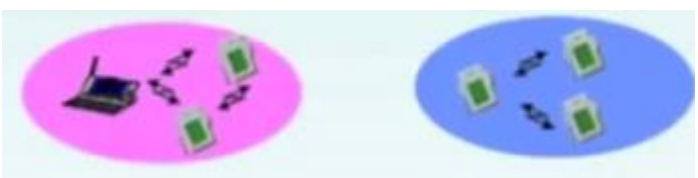


Fig. Ad-hoc based

The other advantages for WLAN include cost-effective network setup for hard-to-wire locations such as older buildings and solid-wall structures and reduced cost of ownership-particularly in dynamic environments requiring frequent modifications, thanks to minimal wiring and installation costs per device and user. WLANs liberate users from dependence on hard-wired access to the network backbone, giving them anytime, anywhere network access. This freedom to roam offers numerous user benefits for a variety of work environments, such as:

- Immediate bedside access to patient information for doctors and hospital staff
- Easy, real-time network access for on-site consultants or auditors or to study group meetings and research links for students
- Improved database access for roaming supervisors such as production line managers, warehouse auditors, or construction engineers
- Simplified network configuration with minimal MIS involvement for temporary setups such as trade shows or conference rooms
- Faster access to customer information for service vendors and retailers, resulting in better service and improved customer satisfaction
- Location-independent access for network administrators, for easier on-site troubleshooting and support

Protocol	Released Date	Data Rate (Max.)	Range (Indoor)	Range (Outdoor)
802.11	1997	2 Mbit/s		
802.11a	1999	54 Mbit/s	25 m	75 m
802.11b	1999	11 Mbit/s	35 m	100 m
802.11g	2003	54 Mbit/s	25 m	75 m
802.11n	2007	540 Mbit/s	50 m	125 m

802.11 is the collection of standards set up for wireless networking. 802.11 lives in the physical layer and data link layer in the OSI. There are three popular standards: 802.11a, 802.11b, 802.11g and the latest one is 802.11n. Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.

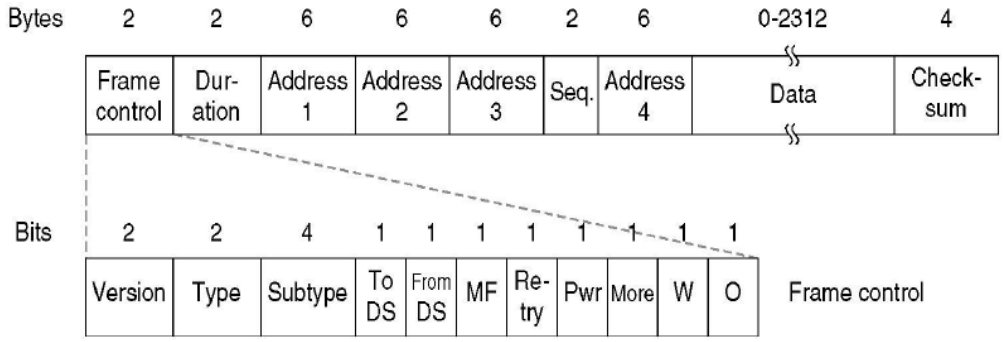


Fig: IEEE 802.11 header format

Frame Control: Contains following

- **Version**: Protocol version Type : data, control or mgmt. Subtype : RTS or CTS
- **To/From DS**: Going to or Coming from intercell distribution (eg. ethernet)
- **MF**: More fragments to follow Retry: Retransmission of earlier frame
- **Pwr**: used by base station to sleep or wake receiver
- **More**: sender has more frames for receiver W: WEP Encryption
- **O** : sequence of frames must be processed in order
- **Duration** : time to occupy channel, used by other stations to manage NAV
- **Addresses** : Two are source and design. Add. of sender and receiver, other two are that of base stations for intercell traffic.