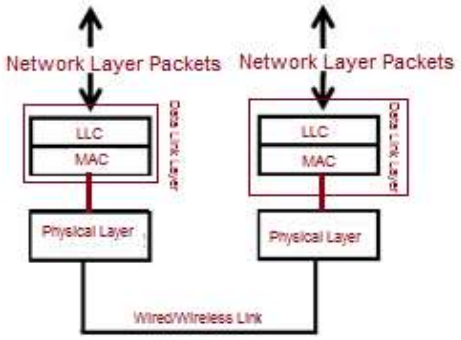
Introduction, Data link layer: the services provided by the link layer, Error detection and Error correction techniques, Multiple access protocols, LAN addresses and Address Resolution Protocol, Ethernet, Wireless Links: IEEE 802.11b, Bluetooth, Point to point protocol (PPP), Asynchronous Transfer Mode (ATM), Frame Relay

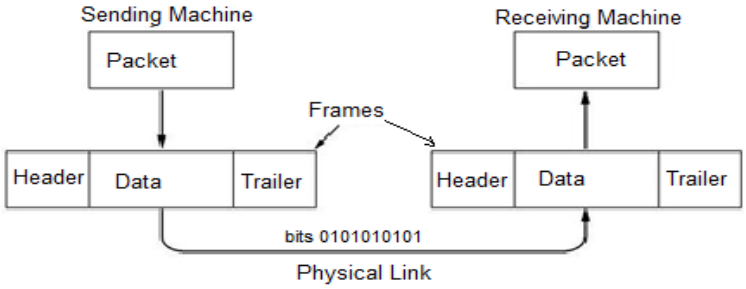
Introduction

- 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



Functions of DLL

- **Framing** :- The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical Addressing** :- If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
- **Flow Control** :- The data rate must be constant on both sides else the data may get corrupted.
- **Error control** :- Error control is normally achieved through a trailer added to the end of the frame and to detect and retransmit damaged or lost frames.
- **Access control** :- When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.



- *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.*

Data Link Layer : the services provided by the link layer

The data link layer has three specific functions:

- Provide a well-defined interface to the network layer.

  - Deal with transmission errors.
  - Regulate the flow of data (so that slow receivers are not overloaded).
- The Data Link Layer sits between the Network Layer and the Physical Layer.
- The DLL provides an interface for the Network Layer to send information from one machine to another.
- To the Network Layer, it looks as though the path to the new machine happens at the DLL level, when it is really happening at the physical level.

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.

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.

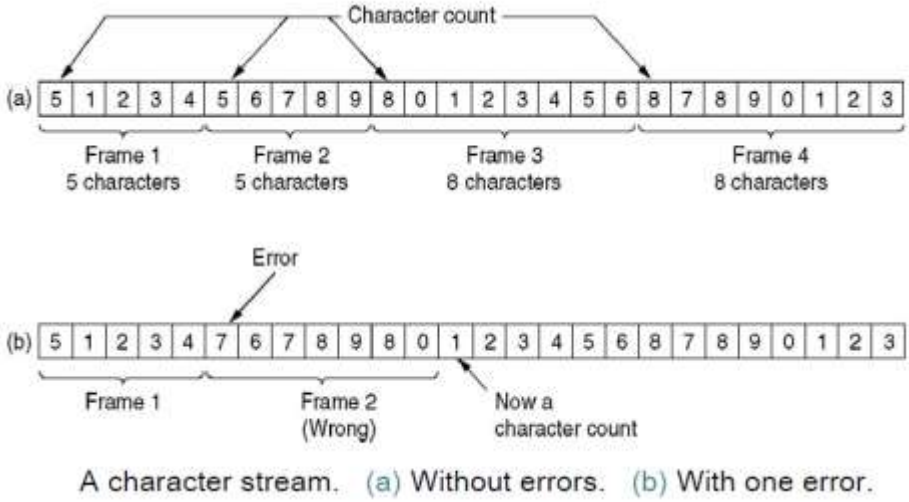
Fixed-Size or Static Framing	Variable-size or Dynamic Framing
1.Every record in the file has exactly same size (in byte) 2.It take huge memory. 3.Access become fast. 4.Computer knows exact location of records so easy access. 5.slow in transferring the records it has large size.	1.Different record in 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.



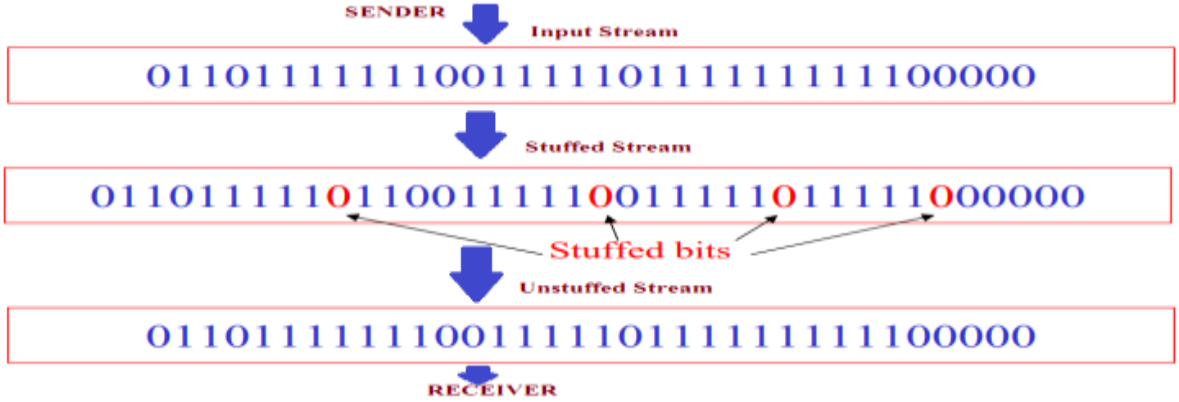
A character stream. (a) Without errors. (b) With one error.

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.

FLAG	Header	Payload	Tailor	FLAG

Fig. Frame

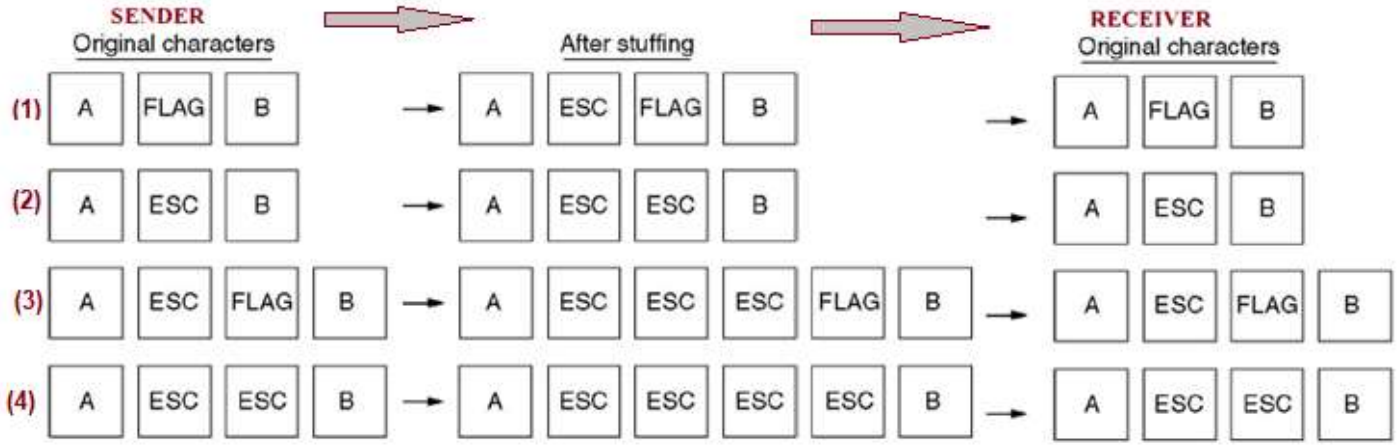


Fig. Four example of byte sequences before and after stuffing:

*** 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.

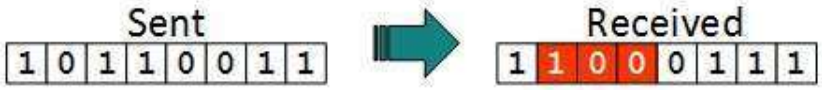
Types of Errors

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.

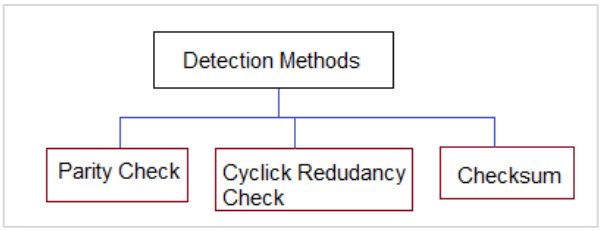


Error control mechanism may involve two possible ways:

- **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

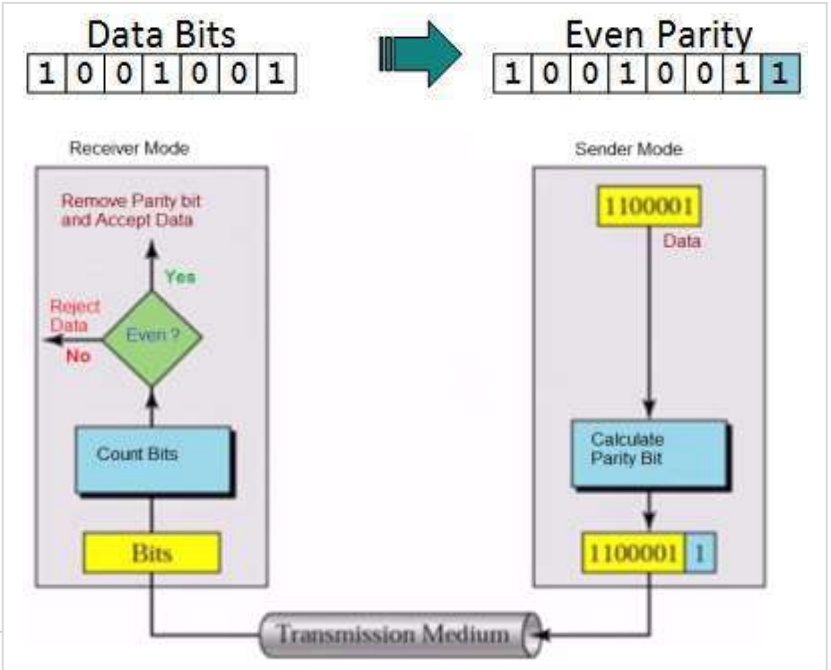


Fig.Parity Check

1110111 1101111 1110010 1101100 1100100 => 11101110 11011110 11100100 11011000 11001001

- 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.

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.

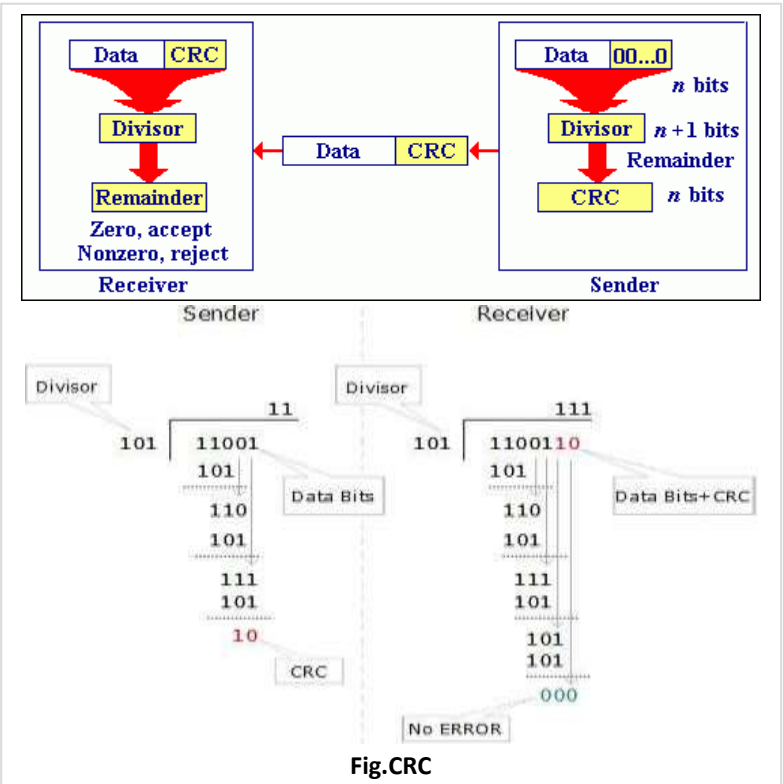


Fig.CRC

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.

2.CRC can detect all burst errors of length less than or equal to the degree of the polynomial

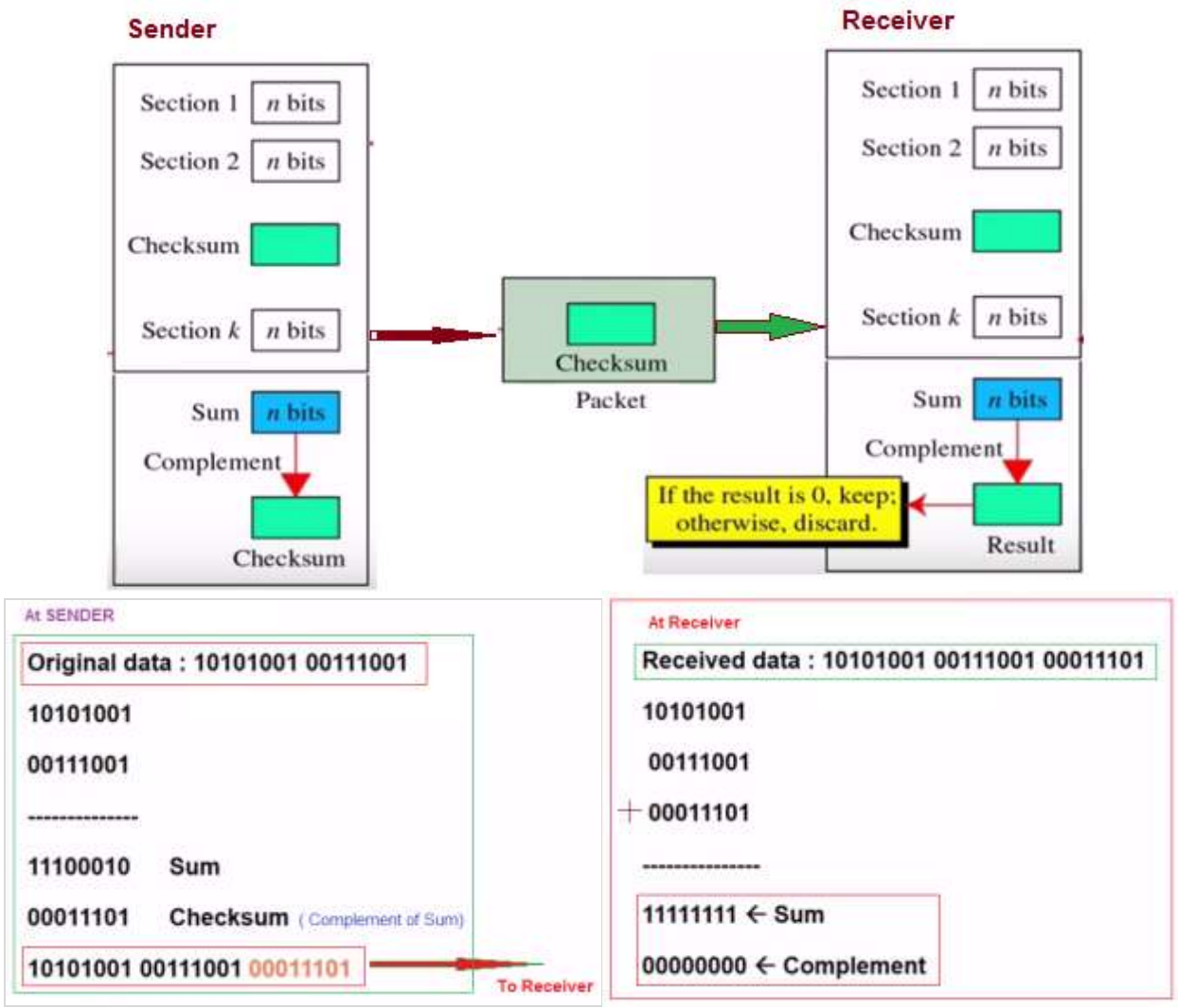
3.CRC can detect, with a very high probability, burst errors of length greater than the degree of the polynomial.

3. Checksum:

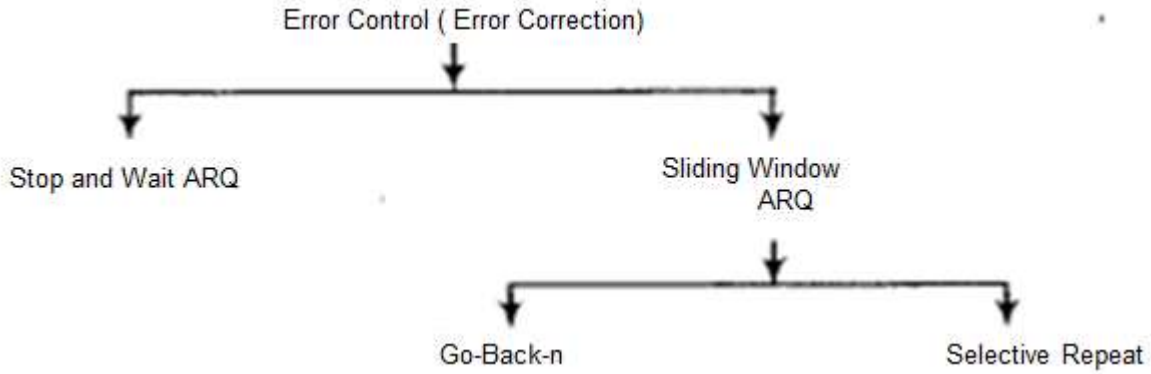
The checksum is used in the Internet by several protocols although not at the data link layer.

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 (it is a process of converting two way process to one way process i.e. sender sends both (data+ack) to receiver). Data and ACK are sent in a single frame is called piggybacking. 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

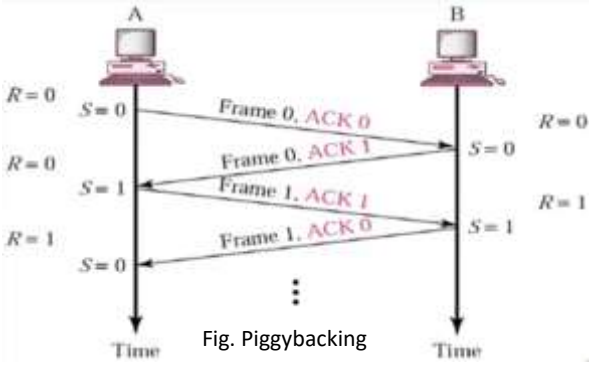


Fig. Piggybacking

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.

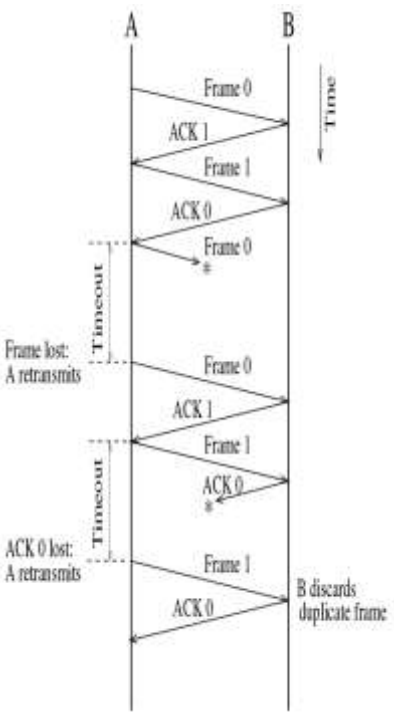
The **sending**-window size *enables the sender to send multiple frames without receiving the acknowledgement of the previous ones.* The **receiving**-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

- 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.**

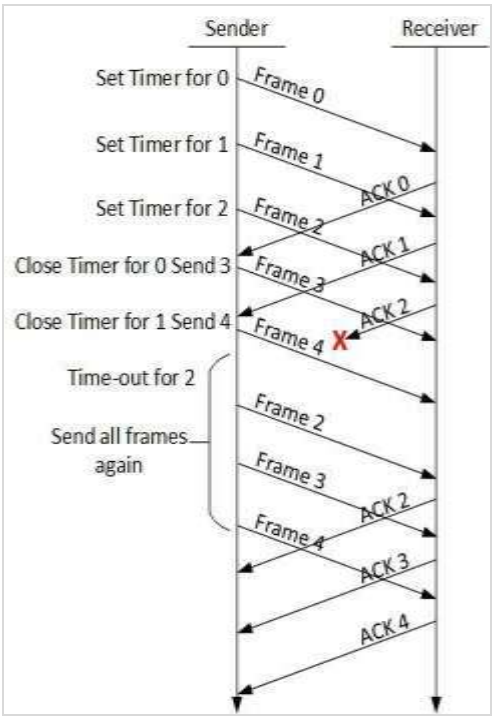
3. Selective Repeat ARQ

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.

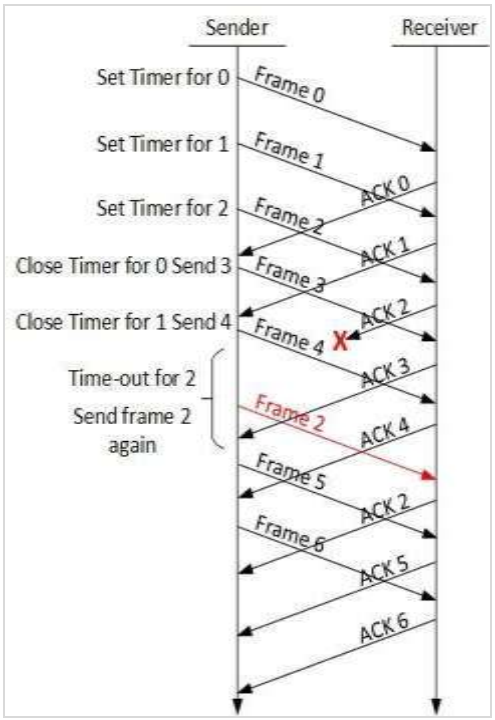
In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged. The sender in this case, sends only packet for which NACK is received.



a) **Stop-and-wait ARQ**



b) Go-Back-N ARQ



c) Selective Repeat

ARQ

Multiple Access Protocols (CHANNEL-PARTITIONING, RANDOM ACCESS, TAKING-TURNS)

- single shared broadcast channel
- two or more simultaneous transmissions by nodes:
  Interference
  – collision: if node receives two or more signals at the same time

Multiple access protocol

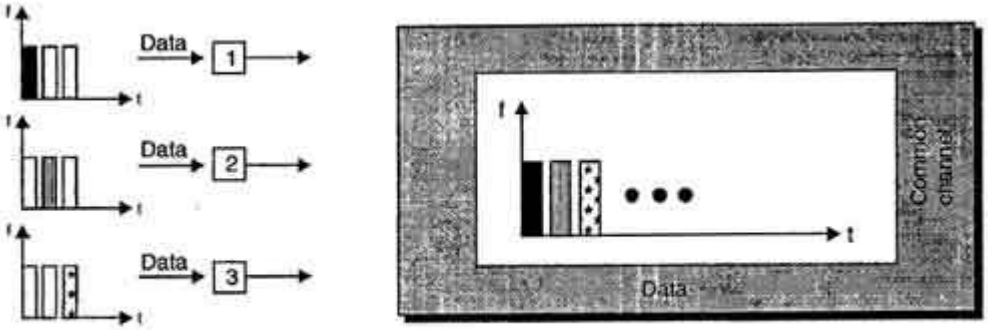
- distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit.
- communication about channel sharing must use channel itself!
  – no out-of-band channel for coordination

CHANNEL PARTITIONING PROTOCOL

I. **TDMA** (Time Division Multiple Access)

- In TDMA, the bandwidth of channel is dividend amongst various stations on the basis of time.
- Each station is allocated a time slot during which it can send its data *i.e.* each station can transmit its data in its allocated time slot only.
- Each station must know the beginning of its slot and the location of its slot.
- TDMA requires synchronization between different stations.
- Synchronization is achieved by using some synchronization bits (preamble bits) at the beginning of each slot.

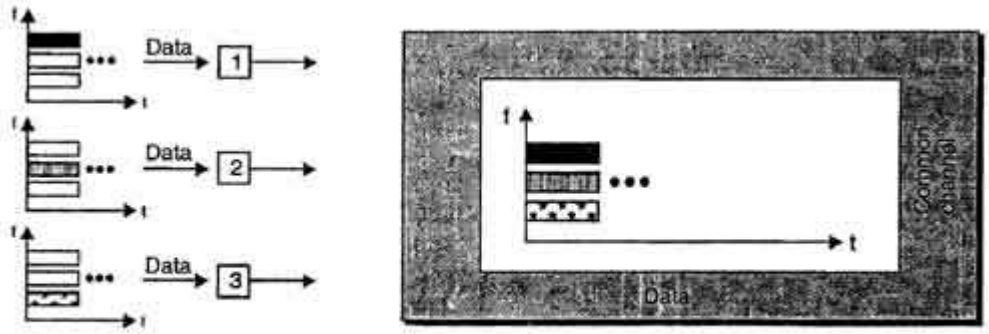
- TDMA is different from TDM, although they are conceptually same.
- TDM is a physical layer technique that combines the data from slower channels and transmits then by using a faster channel. This process uses physical multiplexer.
- TDMA, on other hand, is an access method in the data link layer. The data link layer in each station tells its physical layer to use the allocated time slot. There is no physical multiplexer at the physical layer.



TDMA

II. FDMA (Frequency Division Multiple Access)

- In FDMA, the available bandwidth is divided into various frequency bands.
- Each station is allocated a band to send its data. This band is reserved for that station for all the time.
- The frequency bands of different stations are separated by small bands of unused frequency. These unused frequency bands are called guard bands that prevent station interferences.
- FDMA is different from frequency division multiplexing (FDM).
- FDM is a physical layer technique whereas FDMA is an access method in the data link layer.
- FDM combines loads from different low bandwidth channels and transmit them using a high bandwidth channel. The channels that are combined are low-pass. The multiplexer modulates the signal, combines them and creates a band pass signal. The bandwidth of each channel is shifted by the multiplexer.
- In FDMA, data link layer in each station tells its physical layer to make a band pass signal from the data passed to it. The signal must be created in the allocated band. There is no physical multiplexer at the physical layer.



FDMA

III. **CDMA** (Code Division Multiple Access)

CDMA (Code Division Multiple Access) also called *spread-spectrum* and *code division multiplexing,* one of the competing transmission technologies for digital MOBILE PHONES. The transmitter mixes the packets constituting

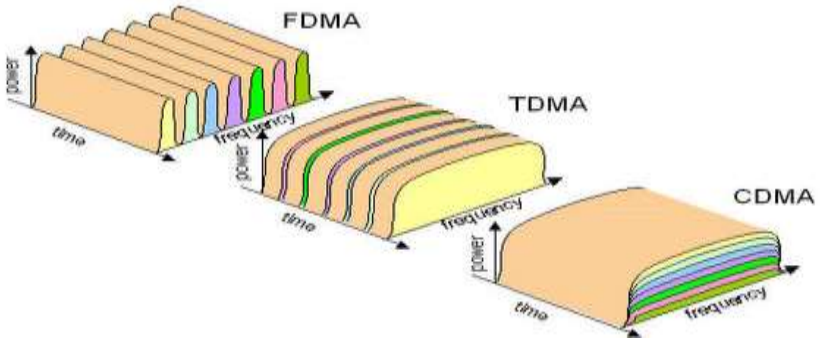
a message into the digital signal stream in an order determined by a PSEUDO-RANDOM NUMBER sequence that is also known to the intended receiver, which uses it to extract those parts of the signal intended for itself. Hence, each different random sequence corresponds to a separate communication channel. CDMA is most used in the USA.

• Unlike TDMA, in CDMA all stations can transmit data simultaneously, there is no timesharing.

• CDMA allows each station to transmit over the entire frequency spectrum all the time.

• Multiple simultaneous transmissions are separated using coding theory.

• In CDMA, each user is given a unique code sequence.



RANDOM ACCESS PROTOCOL

I. Aloha

ALOHA: ALOHA is a system for coordinating and arbitrating 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 data link layer and proposes how multiple terminals access the medium without interference or collision. In 1972, Roberts developed a protocol that would increase the capacity of aloha two fold. 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.

There are two different versions/types of ALOHA:

a) Pure Aloha

• **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.

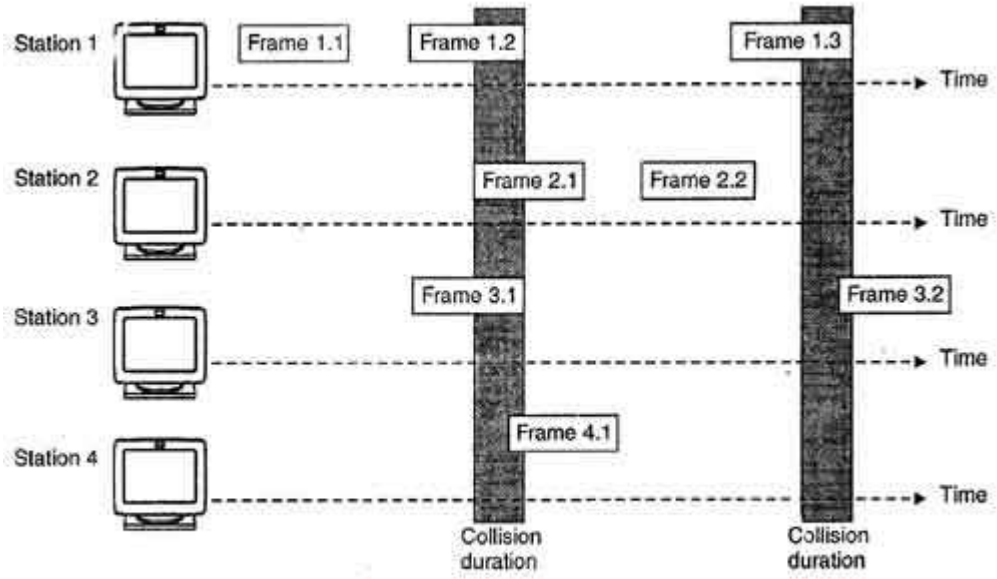
• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• 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.



Frames in Pure ALOHA

• In figure, 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.

b) Slotted Aloha

• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

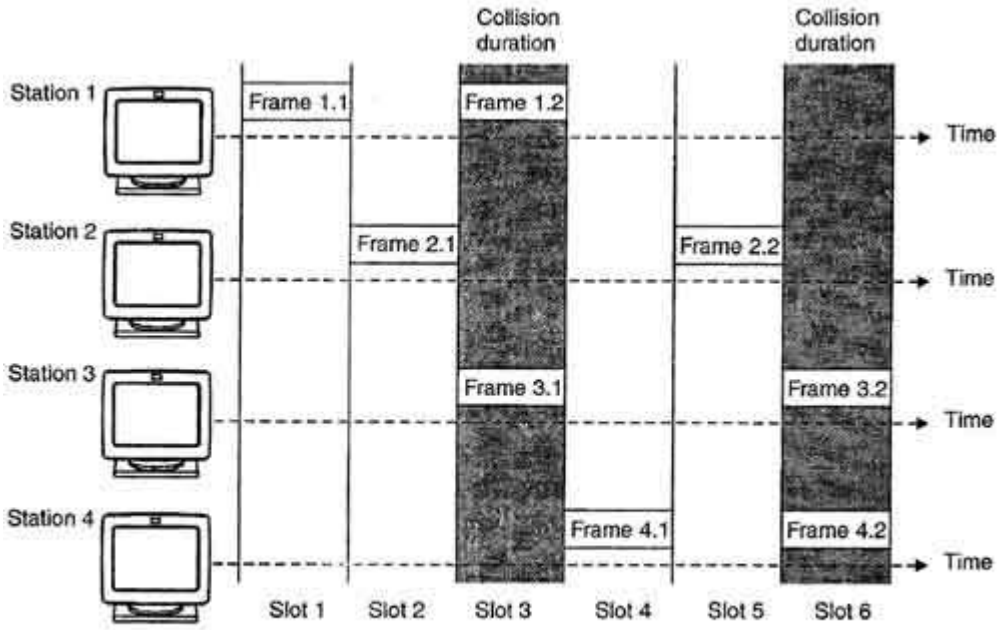
• In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.

• 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 as shown in figure.

• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.



Frames in Slotted ALOHA

Suppose there is only one channel and two computers C1 and C2 are willing to send data through it. If C1 is transmitting data, it sends signals to all the other computers notifying that C1 is about to send data. After the time slot has completed, only then C2 can transmit data through that channel.

II. CSMA

Carrier Sense Multiple Access (CSMA): CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

Consider computers C1, C2, and C3 are willing to send data through a channel. At first, C1 transmits data. In the due course of transmission, C2 and C3 check the status of the channel at the same time. Both find the channel to be busy, so they wait for time T. After time T, both C2 and C3 check the channel and find it free, so they start to initiate the process of data transmission which can lead to collision.

CSMA modes:

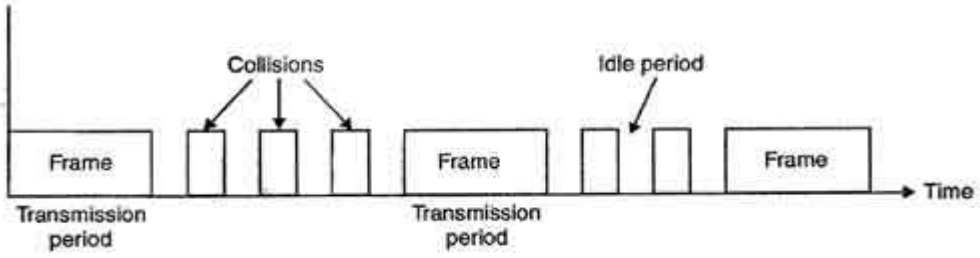
1-persistent

Non-persistent

P-persistent

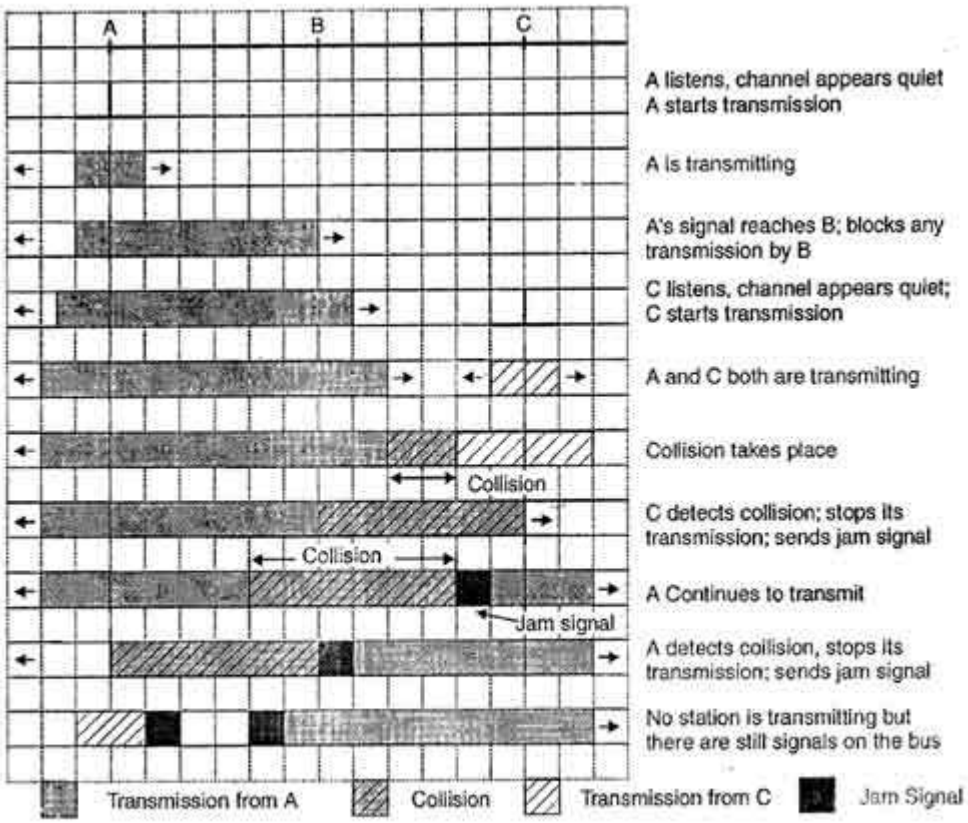
a) CSMA/CD

- *CSMA/CD* is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA. If the channel is busy, the station waits.
- Additional feature in *CSMA/CD* is that the stations can detect the collisions. The stations abort their transmission as soon as they detect a collision. In CSMA, this feature is not present. The stations continued their transmission even though they find that the collision has occurred. This leads to the wastage of channel time.
- However, this problem is handled in *CSMA/CD.* In *CSMA/CD,* the station that places its data onto the channel after sensing the channel continues to sense the channel even after the data transmission. If collision is detected, the station aborts its transmission and waits for predetermined amount of time & then sends its data again.
- As soon as a collision is detected, the transmitting station releases a jam signal.
- Jam signal will alert the other stations. The stations are not supposed to transmit immediately after the collision has occurred. Otherwise, there is a possibility that the same frames would collide again.
- After some back-off delay time, the stations will retry the transmission. If the collision occurs again then the back-off delay time is increased progressively.
- Therefore, the CSMA/CD method consists of alternating transmission period and collisions with idle periods when none of the stations is transmitting.



CSMA/CD with three states : collisions, transmission, or idle

The entire scheme of CSMA/CD is depicted in the figure:



CSMA/CD

i. IEEE 802.3 Ethernet

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

Preamble	Destination Address	Source Address	Type	Data	Frame Check Status (FCS)
Bytes 8	6	6	2	46 to 1500 bytes	2 or 4

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.

Destination Address (DA): It is six byte field that contains physical address of packet's destination.

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).

Length: This two byte field specifies the length or number of bytes in data field.

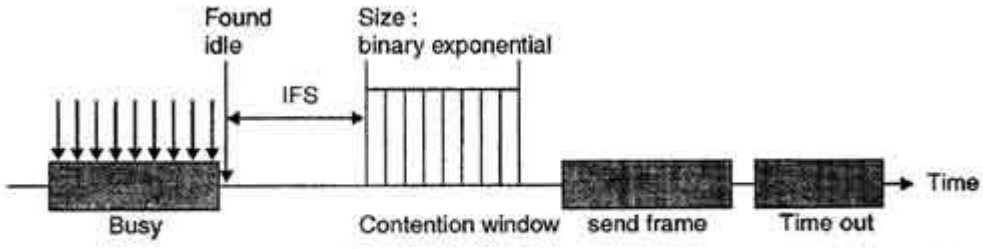
Data: It can be of 46 to 1500 bytes, depending upon the type of frame and the length of the information field.

Frame Check Sequence (FCS): This is for byte field, contains CRC for error detection.

b) CSMA/CA

- CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.
- CSMA/CA avoids the collisions using three basic techniques.

a. Interframe space
b. Contention window
c. Acknowledgements



CSMA/CA

a. Interframe Space (IFS)

• Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).

• When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.

• Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.

• If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.

• IFS variable can also be used to define the priority of a station or a frame.

b. Contention Window

• Contention window is an amount of time divided into slots.

• A station that is ready to send chooses a random number of slots as its wait time.

• The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

• This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.

• In contention window the station needs to sense the channel after each time slot.

• If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

c. Acknowledgement

• Despite all the precautions, collisions may occur and destroy the data.

• The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.

i. IEEE 802.11 Wireless LAN (WiFi)

Wireless communication is one of the fastest growing technologies these days. Wireless LANs are commonly found in office buildings, college campuses, and in many public areas.

Types

Standard	**Frequency Range (US)**	**Data Rate**
IEEE 802.11b	2.4 – 2.485 GHz	Up to 11 Mbps

IEEE 802.11a	5.1 – 5.8 GHz	Up to 54 Mbps
IEEE 802.11g	2.4 – 2.485 GHz	Up to 54 Mbps

IEEE 802.11n is on the process of standardization, uses Multiple Input Multiple Output (MIMO) antennas.

IEEE 802.11 standard provides wireless communication with the use of infrared or radio waves.

- Two configurations:

➢ Ad-hoc: no central control, no connection to the outside world

➢ Infrastructure: uses fixed network access point to connect to the outside world.

- It doesn't implement collision detection because it can't detect collisions at the receiver end (hidden terminal problem)
- To avoid collisions, the frames contains field containing the length of the transmissions. Other stations defer transmissions.
- 802.11 lives in physical layer and data link layer in the OSI.
- IEEE 802.11b (Wi-Fi) is a wireless LAN technology that is growing rapidly in popularity. It is convenient, inexpensive and easy to use.

  Uses: airports, hotels, bookstores, parks etc.

  Estimates: 70% of WLANs are insecure.
- 802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.
- 802.11b devices experience interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include microwave ovens, Bluetooth devices, baby monitors, cordless telephones and some amateur radio equipment.

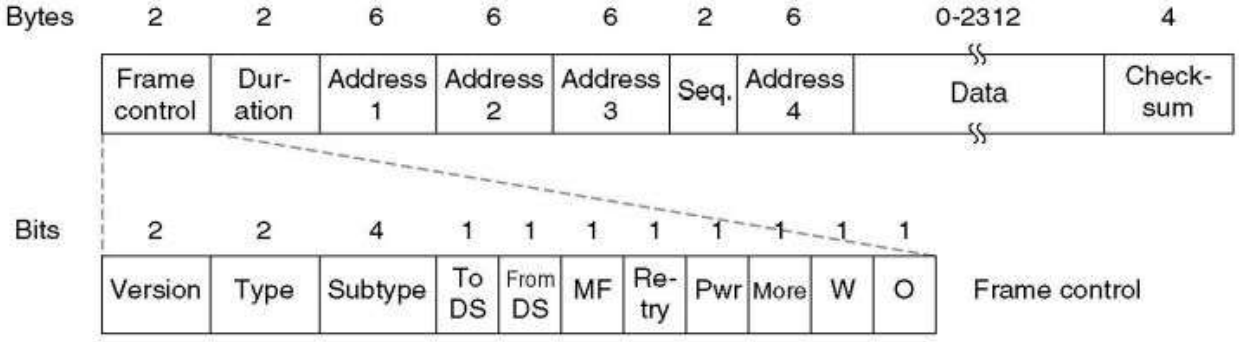


Fig: the 802.11 frame structure

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 (e.g. 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 destination. Add, of sender and receiver, other two are that of base stations for intercell traffic.

TAKING-TURNS PROTOCOL

I. Polling Protocol

The polling protocol requires one of the nodes to be designated as a master node which polls each of the nodes in a round-robin fashion. In particular, the master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum number of frames. After node 1 transmits some frames, the master node tells node 2 that it (node 2) can transmit up to the maximum number of frames. (The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel.) The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.

a) Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 20,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. Bluetooth was standardized as IEEE 802.15.1, but the standard is no longer maintained. The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks. To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG. A network of patents is required to implement the technology, which is licensed only for that qualifying device.

II. Token-passing Protocol

This protocol, also called Token-Passing Protocol, relies on a control signal called the token. A token is a 24-bit packet that circulates throughout the network from NIC to NIC in an orderly fashion. If a workstation wants to transmit a message, first it must seize the token. At that point, the workstation has complete control over the communications channel. The existence of only one token eliminates the possibility of signal collisions. This means that only one station can speak at a time.

a) IEEE 802.5 Token Ring

Ring technology is a collection of point-to-point links that happen to a form of circle, not a broadcast medium, which supports to run twisted pair, coax and fiber optic cables. Each bit arriving at an interface of the ring is copied into a 1-bit buffer and then copied out onto the ring again. While in the buffer, the bit can be inspected and possibly modified before being written out. This copying step introduces 1-bit delay at each interface.

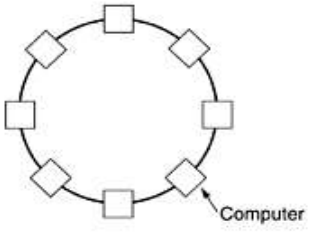


Fig: Token Ring

In token ring special bit pattern, called the token, circulates around the ring whenever all stations are idle. When a station wants to transmit a frame, it is required to seize the token and remove it from the ring before transmitting. This action is done by inverting a single bit in the 3 byte token, which instantly changes it into the first 3 bytes of normal data. Because there is only one token, only one station can transmit at a given instant, thus solving the channel access problem the same way token bus solves it.

A station may hold the token for the token holding time, which is 10 ms unless an installation sets a different value. After all frames transmitted or the transmission of another frame would exceed the token holding time, the station regenerates the token.

Token ring frame format:

	SD	AC	FC	DA	SA	Data	Checksum	ED	FS
Bytes	1	1	1	2 or 6	2 or 6	>=0	4	1	1

Data/ Command

Start Delimiter	Access Control	End Delimiter
1	1	1

Token

Token Frame Fields

• Start delimiter—Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

• Access-control byte—Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

• End delimiter—Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

• Start delimiter—Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

• Access-control byte—Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

• Frame-control bytes—Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.

• Destination and source addresses—Consists of two 6-byte address fields that identify the destination and source station addresses.

• Data—Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
• Frame-check sequence (FCS)—Is filed 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 data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
• Frame Status—Is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

b) FDDI

- Fiber Distributed Data Interface
- Similar to Token ring in the sense that it share some features such as topology(ring) and media access technique(token-passing)
- High performance Fiber Optic token ring running at 100 mbps over distance 200 KM and permits up to 1000 stations
- FDDI deals with network reliable issues as mission-critical applications were implemented on high speed networks. It is frequently used as a backbone technology, and to connect high speed computer on LAN
- Based on two counter–rotating fiber rings, only one used at a time and next is for backup. So if there is any problem in one ring, next ring works automatically
- It allows 16 to 48 bits address and maximum frame size is 4500 bytes
- It prefers multimode fiber optic cable rather than single mode as multimode reduces cost for high data transmission
- It prefers LEDs instead of Laser for light source not only for cheaper but also to remove accidental chances at user end connector (if user open connector and sees cable by naked eye, eye may damage on laser light)
- It operates at low error (1 bit error for 2.5×10^{10})
- It uses 4B/5B encoding in place of Manchester encoding in Token Ring
- It capture token before transmitting and does not wait for acknowledgement to regenerate token as ring might be very long and may occurs much delay to wait for ACK.
- In normal operation, the token and frames travel only on the primary ring in a single direction. The second ring transmits idle signals in the opposite direction
- If a cable or device becomes disabled, the primary ring raps back around onto the secondary ring
- Stations may be directly connected to FDDI dual ring or attached to FDDI concentrator. There are three types of nodes:
  - -DAS (Dual attachment station)
  - -SAS (Single attachment station)
  - -DAC (Dual attachment concentrator)
- FDDI deploys following timers:
  - -Token holding time: upper limit on how long a station can hold token
  - -Token Rotation time: how long it takes the token to traverse the ring or the interval between two successive arrivals of the token
- There are four specifications in FDDI.
  - *Media Access control*- deals with how medium is accessed, frame format, token handling, addressing, fair and equal access of the ring through the use of the timed token, guarantee bandwidth for special traffic etc.
  - *Physical layer protocol*-deals with data encoding/decoding procedures, establish clock synchronization, data recovery from incoming signal etc.
  - *Physical layer medium*- defines characteristics of transmission medium, fiber optic link type: single mode, multimode; power levels, bit error rates, optical components: connectors, switches, LEDs, Pin etc.
  - *Station Management*- defines FDDI station configuration, ring configuration, ring control features, station insertion and removal, initialization etc.

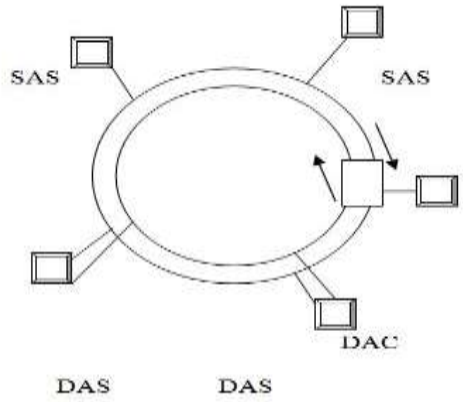


Fig: FDDI Dual Ring

FDDI Frame format:

	Preamble	SD	FC	DA	SA	Data	Checksum	ED	FS
8 B	1 B	1 B	2 or 6 B	2or 6B	4500 B	4 B	1 B	1B	

FDDI Frame can be as long as 4500bytes.
Preamble: Unique sequence that prepares each station for an upcoming frame.
Start Delimiter: Indicates beginning of the frame.
Frame Control: Indicates size of address field and whether the frame contains synchronous or asynchronous data, among other control information
Destination Address: Contains a unicast, multicast or broadcast address. FDDI uses 6 byte address
Source Address: 6 byte address source Address.
Data: Contains either information destined for upper layers or control information
Frame Check Sequence: For Error detection.
End Delimiter: End of Frame.
Frame status: Allows the source station to determine whether an error occurred; identifies whether the frame was recognized and copied by a receiving station.

ARP

- Address Resolution Protocol
- Used to convert an IP address into a physical address (called a *DLC address*), such as an Ethernet address.

RARP

- Reverse ARP
- used by a host to discover its IP address
- to convert physical address into IP address

PPP – the Point-to-Point Protocol

- PPP was devised by IETF (Internet Engineering Task Force) to create a data link protocol for point to point lines that can solve all the problems present in SLIP (serial line internet protocol).
- PPP is most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem.

This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

i. PPP defines the format of the frame to be exchanged between the devices.
ii. It defines link control protocol (LCP) for:-

(a) Establishing the link between two devices.

(b) Maintaining this established link.

(c) Configuring this link.

(d) Terminating this link after the transfer.

iii. It defines how network layer data are encapsulated in data link frame.

iv. PPP provides error detection.

v. Unlike SLIP that supports only IP, PPP supports multiple protocols.

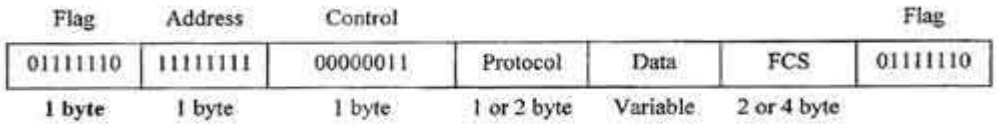
vi. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

vii. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

viii. It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:



PPP frame format

Flag field: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

Address field: This field is of 1 byte and is always 11111111. This address is the broadcast address *i.e.* all the stations accept this frame.

Control field: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.

Protocol field: This field specifies the kind of packet in the data field *i.e.* what is being carried in data field.

Data field: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

FCS field: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

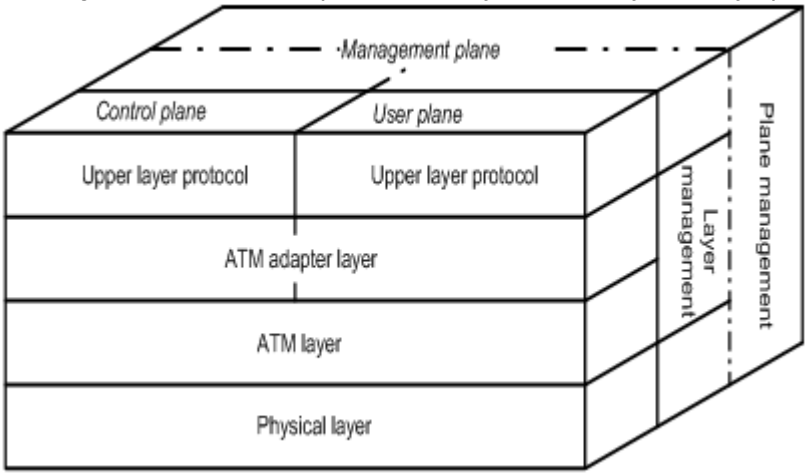
ATM

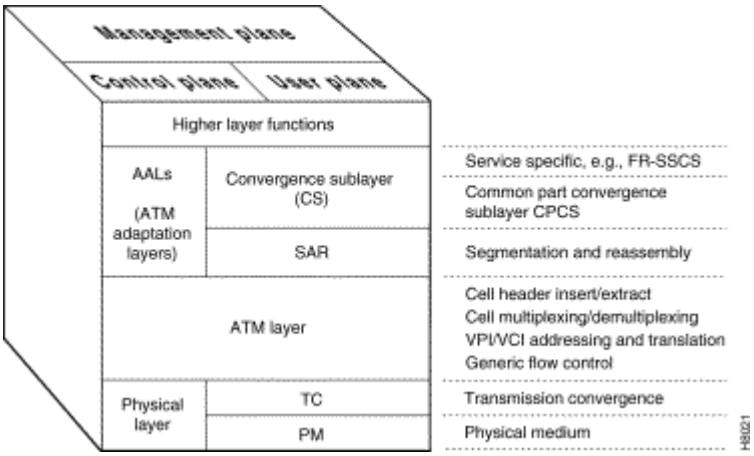
Asynchronous Transfer Mode (ATM) is also called *cell relay,* a high-speed switched network technology developed by the telecommunications industry to implement the next, BROADBAND generation of ISD. ATM was designed for use in WANS such as the public telephone system and corporate data networks, though it has also been applied to create super-fast LANS. It can carry all kinds of traffic - voice, video and data – simultaneously at speeds up to 155megabits per second.

ATM is a CONNECTION-ORIENTED scheme, in which switches create a VIRTUAL CIRCUIT between the sender and receiver of a call that persists for the duration of the call. It is a PACKET SWITCHING system, which breaks down messages into very small, fixed length packets called CELLS generally 53 bytes in length (48 bytes of data plus a 5-byte header). The advantage conferred by such small cells is that they can be switched entirely in hardware, using custom chips, which makes ATM switches very fast (and potentially very cheap).

The ASYNCHRONOUS part of the name refers to the fact that although ATM transmits a continuous stream of cells, some cells may be left empty if no data is ready for them so that precise timings are not relevant. This is ATM's greatest strength, as it enables flexible management of the QUALITY OF SERVICE so; an operator can offer different guaranteed service levels (at different prices) to different customers even over the same line. This ability will enable companies to rent VIRTUAL PRIVATE NETWORKS based on ATM that behave like private leased lines but in reality share lines with other users.

- **Layers** of ATM model (AAL, ATM Layer, ATM Physical Layer)





AAL (ATM Adaptation Layer): A software layer that accepts user data, such as digitized voice, video or computer data, and converts to and from cells for transmission over an ASYNCHRONOUS TRANSFER MODE network. AAL software mostly runs at the end-points of a connection, though in a few circumstances AAL software is run inside an ATM switch. AAL includes facilities to carry traffic that uses other network protocols, such as TCP/IP, over ATM.

Frame Relay

Frame relay has evolved from X.25 packet switching and objective is to reduce network delays, protocol overheads and equipment cost. Error correction is done on an end-to-end basis rather than a link -to-link basis *as* in X.25 switching. Frame relay can support multiple users over the same line and can establish a permanent virtual circuit or a switched virtual circuit.

Frame relay is considered to be a protocol, which must be carried over a physical link. While useful for connection of LANs, the combination of low throughput, delay variation and frame discard when the link is congested will limit its usefulness to multimedia.

Packet switching was developed when the long distance digital communication showed a large error rate.

- To reduce the error rate, additional coding bits were introduced in each packet in order to introduce redundancy to detect and recover errors.
- But in the modem high speed telecommunication a system, this overhead is unnecessary and infect counterproductive.
- Frame relay was developed for taking the advantage of the high data rates and low error rates in the modem communication system.
- The original packet switching networks were designed with a data rate at the user end of about 64 kbps.
- But the frame relay networks are designed to operate efficiently at the user's data rates up to 2 Mbps.
- This is possible practically because most of the overhead (additional bits) are striped off.
- Frame relay is a virtual circuit wide area network which was designed in early 1990s.
- Frame relay also is meant for more efficient transmission scheme than the X.25 protocol.
- Frame Relay is used mostly to route Local Area Network protocols such *as* IPX or *TCP/IP.*
- The biggest difference between Frame Relay and X.25 is that X.25 guarantees data integrity and network managed flow control at the cost of some network delays. Frame Relay switches packets end-to-end much faster, but there is no guarantee of data integrity at all.

Features of frame relay:

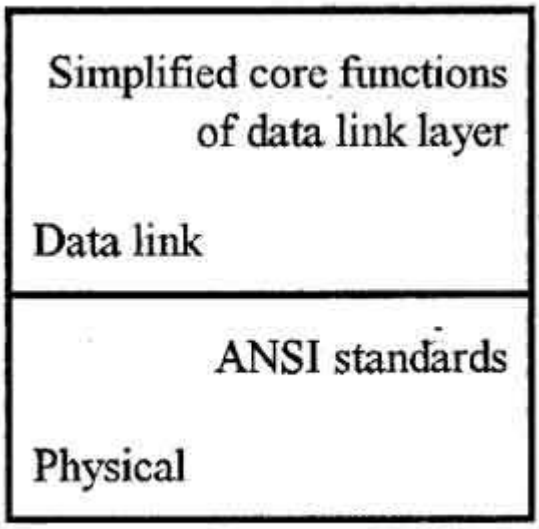
i. Frame relay operates at a high speed (1.544 Mbps to 44.376 Mbps).
ii. Frame relay operates only in the physical and data link layers. So it can be easily used in Internet.
iii. It allows the bursty data.
iv. It has a large frame size of 9000 bytes. So it can accommodate all local area network frame sizes.
v. Frame relay can only detect errors (at the data link layer). But there is no flow control or error control.
vi. The damaged frame is simply dropped. There is no retransmission. This is to increase the speed. So frame relay needs a reliable medium and protocols having flow and error control.

Frame Format

- The DLCI length is 10 bits
- There are two EA locations. The value of the first one is fixed at 0 and the second at
- 1 is set in the DE (Discard Eligibility) for the part that can be discarded first when congestion occurs
- The data size may vary up to 4096 bytes.

Frame relay layers

• Frame relay has only two layers i.e. physical layer and data link layer.



Frame relay layers

Physical layer

• Frame relay supports ANSI standards.

• No specific protocol is defined for the physical layer. The user can use any protocol which is recognized by ANSI.

Data link layer

• A simplified version of HDLC is employed by the frame relay at the data link layer.

• A simpler version is used because flow control and error correction is not needed in frame relay.