2.1 LINK LAYER AND LOCAL AREA NETWORK

DATA LINK LAYER

Data link layer is most reliable node to node delivery of data. It forms frames from the packets that are received from network layer and gives it to physical layer.

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer is 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.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

SERVICES PROVIDED BY 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.

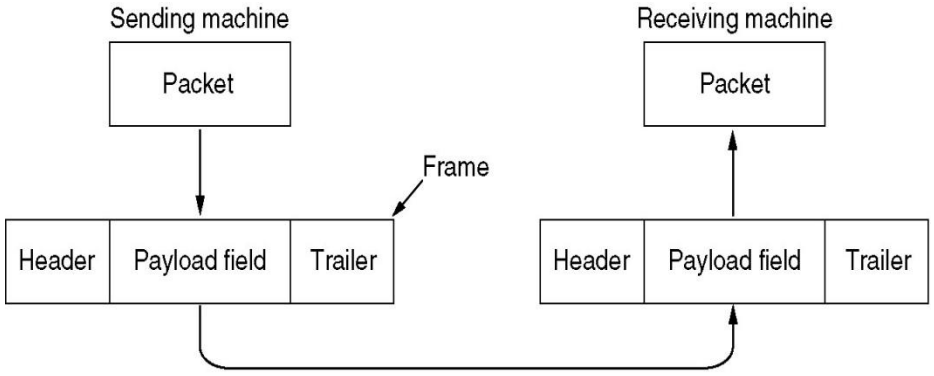
- **Flow Control**

  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**

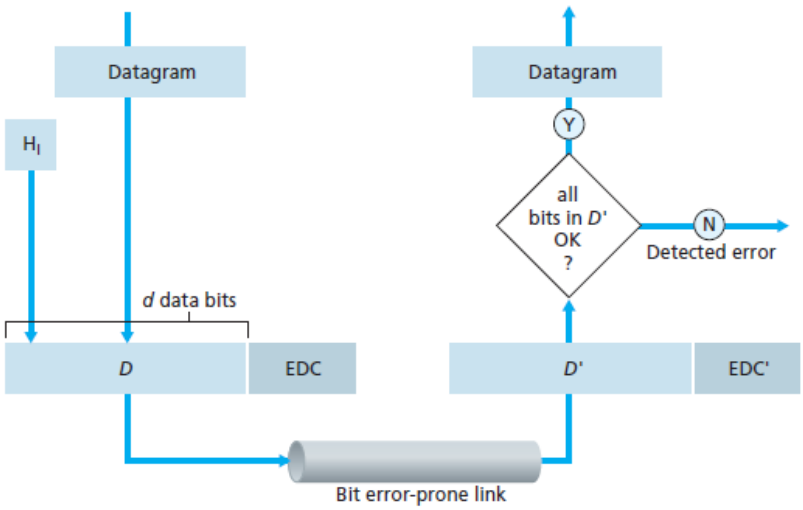
  When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

- **Reliable delivery**
  When a link-layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error.



ERROR DETECTION AND CORRECTION TECHNIQUES

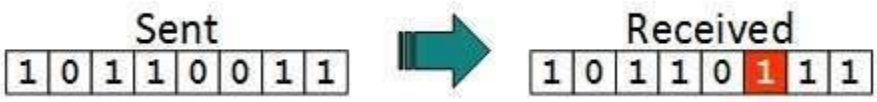
Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.



TYPES OF ERRORS

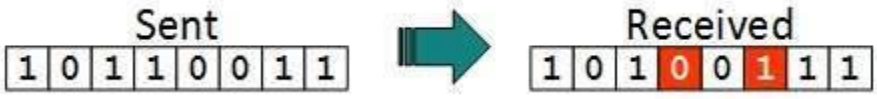
There may be three types of errors:

- **Single bit error**



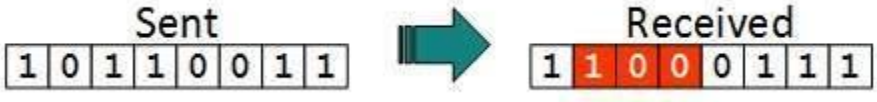
In a frame, there is only one bit, anywhere though, which is corrupt.

- **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
- Error correction

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.

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.

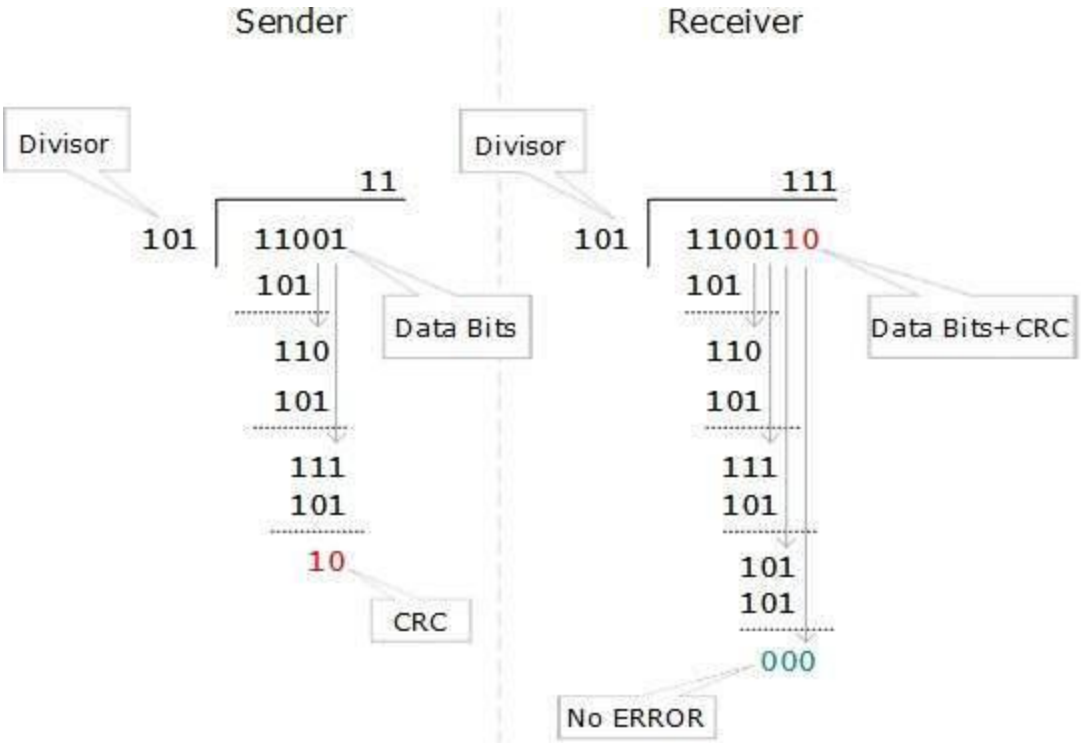
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

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 erroneous, then it is very hard for the receiver to detect the error.

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 codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords 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.

The Cyclic Redundancy Check (CRC)

Consider a message having many data bits which are to be transmitted reliably by appending several check bits as shown below.

message bits	parity bits

The exact number of extra bits and their makeup depends on a generating polynomial. For example one such polynomial is:

$$x^{16} + x^{12} + x^5 + 1$$

A Standard Generating Polynomial - CRC(CCITT)

The number of CRC bits corresponds to the order of the generating polynomial. The above polynomial of order 16 generates a 16-bit CRC. Typically, the CRC bits are used for error *detection* only.

CRC Computation

Consider a message represented by some polynomial M(x), and a generating polynomial G(x).
In this example, let M(x) represent the binary message 110010, and let $G(x) = x^3 + x^2 + 1$; (binary **1101**).
The polynomial G(x) will be used to generate a (3-bit) CRC called R(x) which will be appended to M(x). Note that G(x) is prime.

110010	CRC

The polynomial G(x) defines the CRC bits.

Step 1 - Multiply the message M(x) by x^3, where 3 is the number of bits in the CRC.
Add three zeros to the binary M(x).
Step 2 - Divide the product x^3 [M(x)] by the generating polynomial G(x).
We wish to find "the remainder, modulo M(x)"
Compute the following:

```
        100100 (ignore this quotient)
      ------------
1101) 110010000
      1101
      ----
        1100
        1101
        ----
          100   = remainder = R(x)
```

Observe that if R(x) were in place of the appended zeros, the remainder would become 000.
Step 3 - Disregard the quotient and add the remainder R(x)to the product x^3 [M(x)] to yield the code message polynomial T(x), which is represented as:
$T(x) = x^3 [M(x)] + R(x)$
Put the remainder R(x)=100 in place of the three zeros added in Step 1.

110010	100

The message may now be transmitted

CRC Error Checking - No Errors
Upon reception, the entire received T(x) = "message + crc" can be checked simply by dividing T(x)/G(x) using the same generating polynomial. If the remainder after division equals zero, then no error was found.

```
           100100 (ignore this quotient)
         ------------
1101) 110010100
      1101
      ----
        1101
        1101
        ----
          000   = remainder (no error)
```

CRC Error Checking - Single Bit Error

A single bit error in bit position K in a message T(x) can be represented by adding the term E(x) = x^K, (binary 1 followed by K-zeros).

sent: 110010100 = T(x)
error: 000001000 = E(x) = x^3
---
received: 110011100 = T(x) + E(x) (error in bit 3)

The above error would be detected when the CRC division is performed:

```
      100101 (ignore this quotient)
   ------------
1101) 110011100 = T(x) + E(x)
      1101
      ----
       1111
       1101
       ----
        1000
        1101
        ----
         101   = remainder (error!)
```

Note that division by G(x) revealed the error. On the other hand, since T(x)/G(x) = 0 by definition, the remainder is a function only of the error. An error in this same bit would give the same non-zero remainder *regardless of the message bits*.

$$\frac{T(x)+E(x)}{G(x)} = \frac{T(x)}{G(x)} + \frac{E(x)}{G(x)} = \frac{E(x)}{G(x)}$$

The remainder is a function only of the error bits E(x).

```
        1 (ignore this quotient)
   ------------
1101) 000001000   = E(x) alone
      1101
      ----
       101   = remainder (error!)
```

Since E(x) = x^K has no factors other than x, a single bit error will never produce a term exactly divisible by G(x). **All single bit errors will be detected.**

Checksum

A checksum is an error-detection method in a the transmitter computes a numerical value according to the number of set or unset bits in a message and sends it along with each message frame. At the receiver end, the same checksumfunction (formula) is applied to the message frame to retrieve the numerical value.

A checksum "adds" together "chunks" of data – The "add" operation may not be normal integer addition – The chunk size is typically 8, 16, or 32 bits

Example Part 1

- Suppose the following block of 16 bits is to be sent using a checksum of 8 bits.
- 10101001 00111001
- The numbers are added using one's complement
- 10101001
- 00111001

Sum 11100010

- Checksum **00011101**
- The pattern sent is 10101001 00111001 **00011101**

Error Correction

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

- **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** 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. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

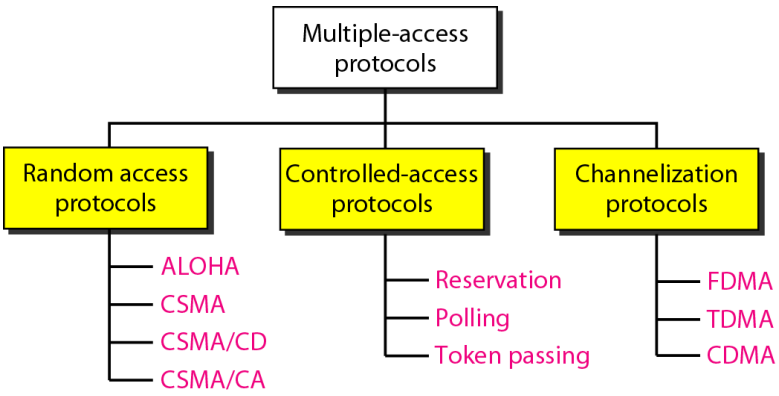
To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

MULTIPLE ACCESS PROTOCOLS

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

collision: if node receives two or more signals at the same time



Channelization

The term channelization refers to the sharing of a point-to-point communications medium. For example, many telephone conversations (or in our context, computer-to-computer network transactions) can be submitted simultaneously on a single wire, with each conversation being on a separate channel. The notion of a channel is very closely related to the household concept of radio and TV channels. The frequency spectrum for television, for instance, is divided into subranges called channels, and these correspond to our everyday concept of TV channels. Each channel is used to transmit different information, all simultaneously. There are three main ways of doing this:

• In time-division multiplexing (TDMA), different sources transmit on the line at different times, each taking (very short) turns. This is used in long-distance phone lines

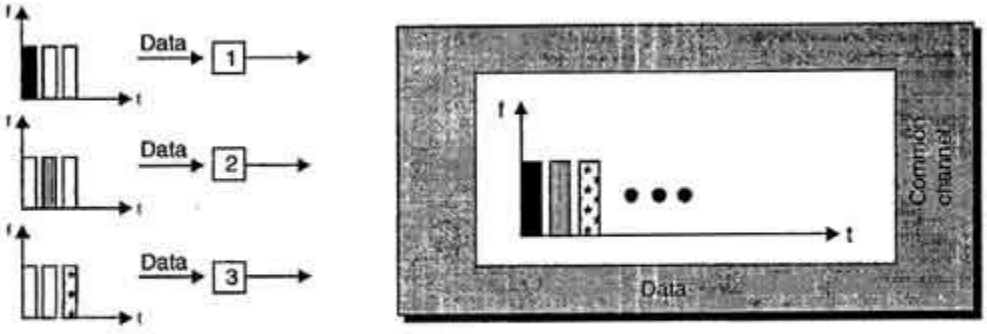
• In frequency-division multiplexing (FDMA), the different sources attached to the line send on different frequencies (e.g. different radio frequencies, or different light frequencies, i.e. different colors). This is

used for radio and television transmission, and increasingly for computer-to-computer network transactions.

• In code-division multiplexing (CDMA), all nodes on the network send at the same time, on the same frequency, but using different codes. (Think of one node using a 4B/5B code, another using a second kind of code, and so on.) This is used in some cellular telephone systems.

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.



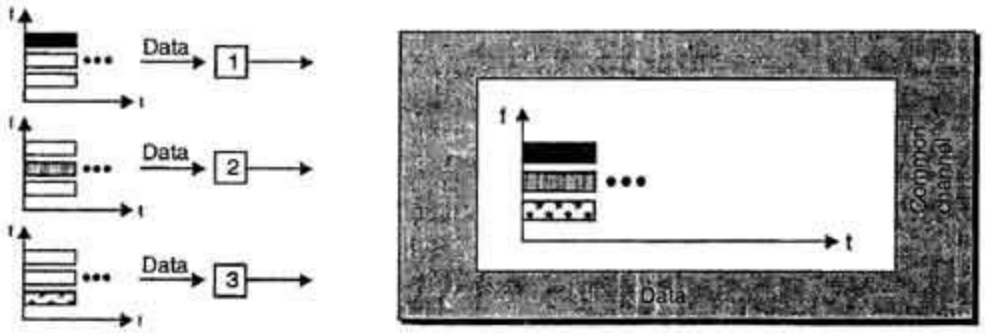
TDMA

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)

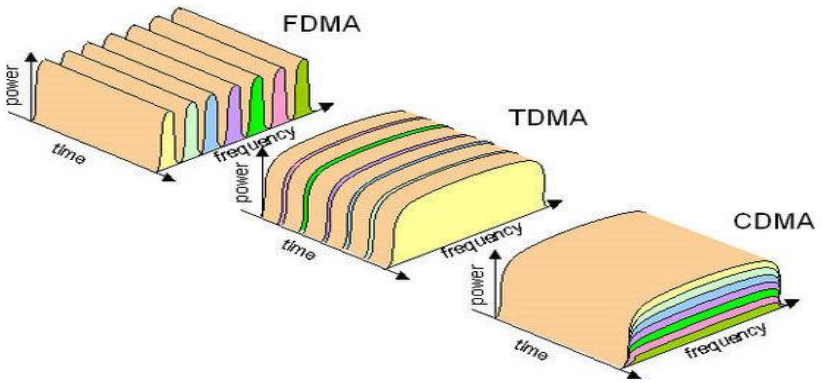
CDMA (Code Division Multiple Access) also called *spread-spectrum* and *code division multiplexing*, one of the competing transmission technologies for digital MOBILE PHONES. The transmitter mixes the packets constituting a message into the digital signal stream in an order determined by a PSEUDO-RANDOM 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 PROTOCOLS

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.

There are two different versior.s/types of ALOHA:

(i)PureALOHA
(ii) Slottecl ALOHA

(i) Pure ALOHA

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

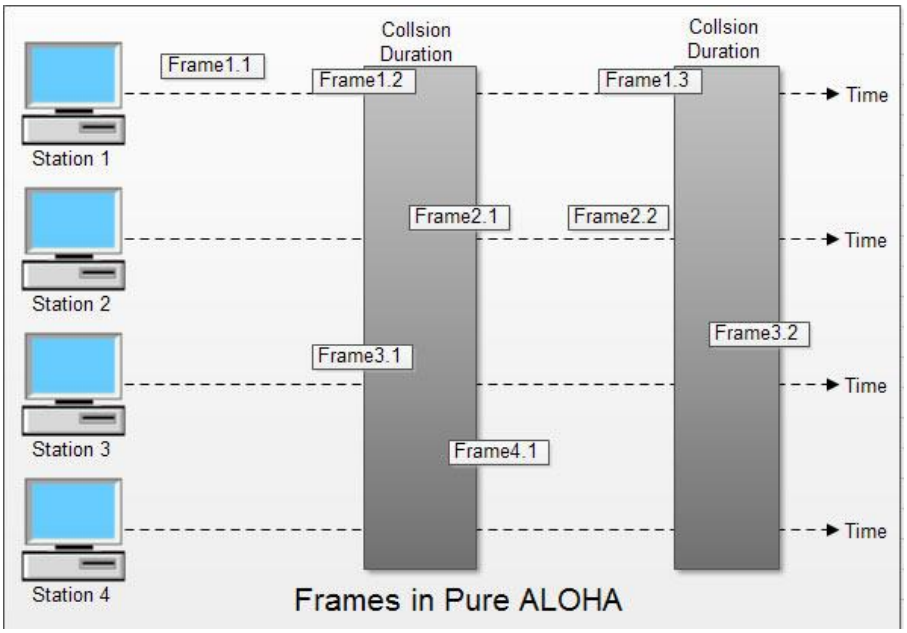
• When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

• 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.

• • 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.

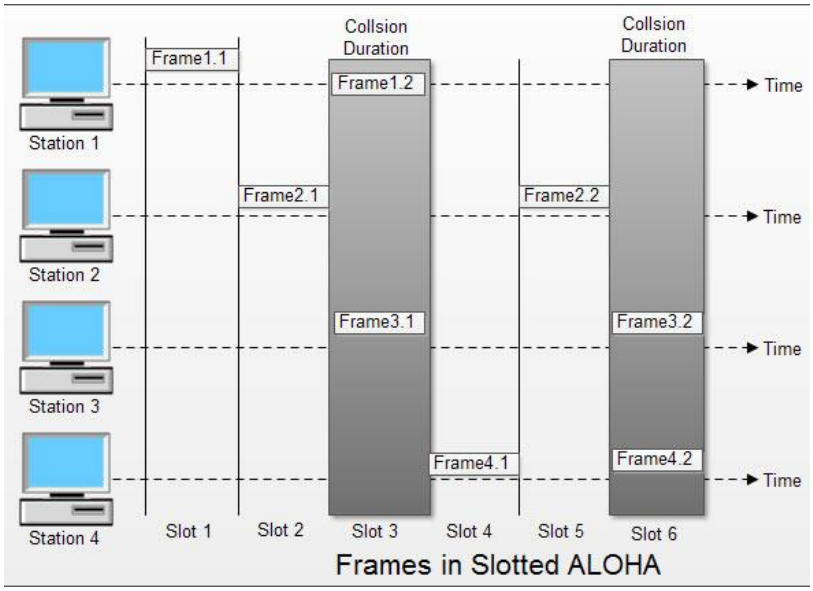
• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

(ii) Slotted ALOHA

• Slotted ALOHA 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.



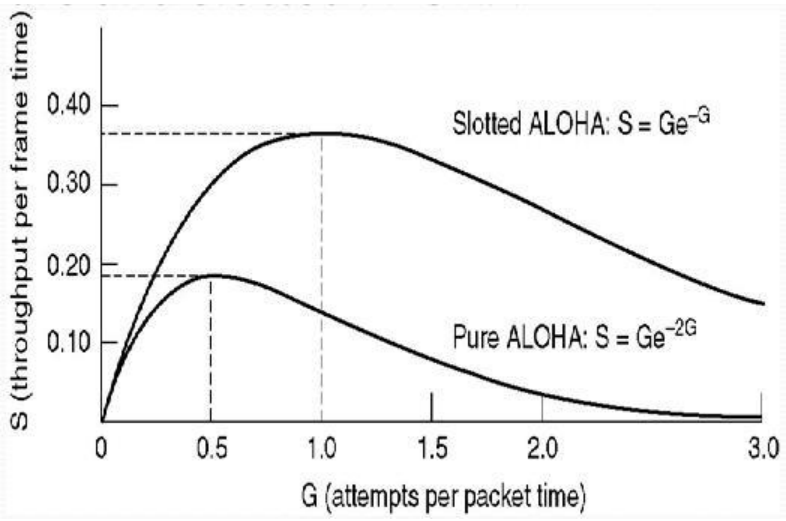
• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.

• 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 fig.

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

Key Differences Between Pure ALOHA and Slotted ALOHA

1. Pure ALOHA was introduced by Norman and his associates at the university of Hawaii in 1970. On the other hand, Slotted ALOHA was introduced by Roberts in 1972.
2. In pure ALOHA, whenever a station has data to send it transmits it without waiting whereas, in slotted ALOHA a user wait till the next time slot beings to transmit the data.
3. In pure ALOHA the time is continuous whereas, in Slotted ALOHA the time is discrete and divided into slots.
4. In pure ALOHA the probability of successful transmission is S=G*e^-2G. On the other hand, in slotted ALOHA the probability of successful transmission is S=G*e^-G.
5. The time of sender and receiver in pure ALOHA is not globally synchronized whereas, the time of sender and receiver in slotted ALOHA is globally synchronized.
6. The maximum throughput occurs at G=1/2 which is 18 % whereas, the maximum throughput occurs at G=1 which is 37%.



CSMA, or listen with random access carrier

Technical CSMA (Carrier Sense Multiple Access) is to listen to the channel before transmitting. This significantly reduces the risk of collision, but does not eliminate them completely. If during the propagation time between the couple of the more remote stations (vulnerability period), a coupler does not detect the transmission of a frame, and there may be signal superposition. Therefore, it is necessary to subsequently retransmit lost frames.

Numerous variations of this technique have been proposed, which differ by three Features:

• The strategy followed by the module after detecting the channel status.

• The way collisions are detected.

• The message retransmission after collision policy.

Its main variants are:

• **Non-persistent CSMA**. The coupler the listening channel when a frame is ready to be sent. If the channel is free, the module emits. Otherwise, it starts the same process after a random delay.

• **Persistent CSMA** - A loan coupler to transmit the channel and previously listening forwards if it is free. If it detects the occupation of carrier, it continues to listen until the channel is clear and transmits at that time. This technique allows lose less time than in the previous case, but it has the disadvantage increase the likelihood of collision, since the frames that accumulate during the busy time are all transmitted simultaneously.

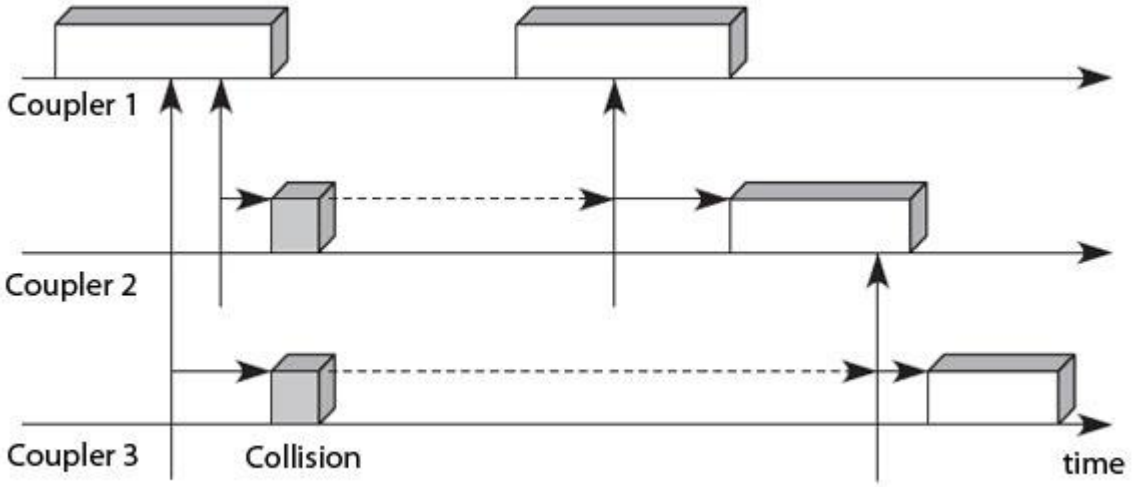
• **P-persistent CSMA** - The algorithm is the same as before, but when the

Channel becomes free; the module transmits with probability p. In other words, the coupler differs his show with probability 1 - p. This algorithm reduces the likelihood of collision. Assuming both terminals simply making the collision is inevitable in the standard case. With the new algorithm, there is a probability 1 - p that each terminal does not transmit, thereby avoiding the collision. However, it increases the time before transmission, since a terminal may choose not to transmit, with a probability 1 - p, while the channel is free.

• **CSMA / CD (Carrier Sense Multiple Access / Collision Detection)** - a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a *collision*). Standard Ethernet networks use CSMA/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular

station can transmit. If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval, the stations that collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off .If there is a collision, it interrupts its transmission as soon as possible and sends special signals, called padding bits so that all couplers are notified of the collision. He tries again his show later using an algorithm that we present later.

Figure shows the CSMA/CD. In this example, the couplers 2 and 3 attempt broadcasting for the coupler 1 transmits its own frame. The couplers 2 and 3 begin to listen and transmit at the same time, the propagation delay around, from the end of the Ethernet frame transmitted by the coupler 1. A collision ensues. Like the couplers 2 and 3 continue to listen to the physical media, they realize the collision, stop their transmission and draw a random time to start retransmission process.

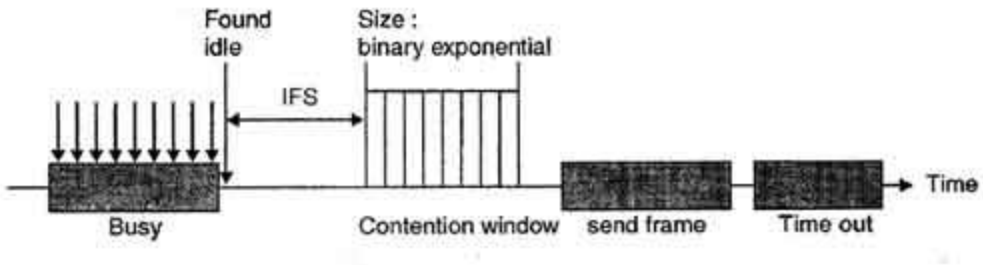


Operating Principle of CSMA / CD

The CSMA/CD create an efficiency gain compared to other techniques random access because there are immediate collision detection and interruption of current transmission. Issuers couplers recognize a collision by comparing the transmitted signal with the passing on the line. The collisions are no longer recognized by absence of acknowledgment but by detecting interference. This conflict detection method is relatively simple, but it requires sufficient performance coding techniques to easily recognize a superposition signal. It is generally used for this differential coding technique, such as differential Manchester code.

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.

CONTROLLED ACCESS PROTOCOLS

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. The three popular controlled-access methods are as follows.

1. *Reservation:*

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

If there are N stations in the system, there are exactly N reservation minislots in the reservation frame. Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame.

2. *Polling:*

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session. Consider the following figure.

If the primary wants to receive data, it asks the secondaries if they have anything to send, this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

Select:

The select function is used whenever the primary device has something to send. If it has something to send, the primary device sends it. It has to know whether the target device is prepared to receive or not. So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the secondary's ready status. Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

Poll:

The poll function is used by the primary device to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send. When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data (in the form of a data frame) if it does. If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.

3. Token Passing:

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station which is logically

before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round.

Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed. For example, if a station that is holding the token fails, the token will disappear from the network. Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low- priority stations release the token to high priority stations.

Local Area Network (LAN)

a) IEEE 802.5 Token Ring

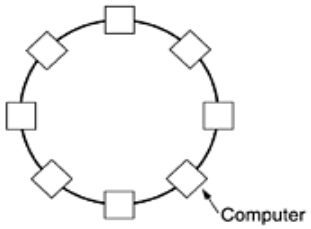


Fig: Token Ring

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.

a) 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.

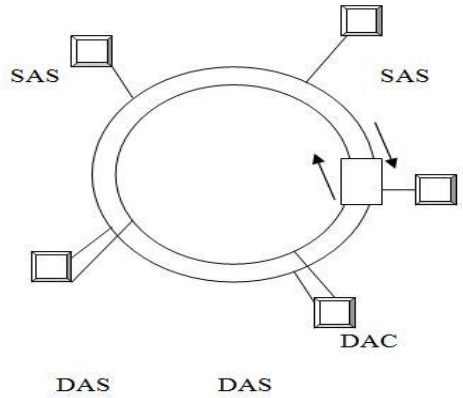


Fig: FDDI Dual Ring

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

LAN ADDRESS AND ARP

ARP

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

- Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

RARP

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

ETHERNET

Ethernet (IEEE 802.3)

Ethernet protocols refer to the family of local-area network (LAN) covered by the IEEE 802.3. In the Ethernet standard, there are two modes of operation: half-duplex and full-duplex modes. In the half duplex mode, data are transmitted using the popular Carrier-Sense Multiple Access/Collision Detection (CSMA/CD) protocol on a shared medium. The main disadvantages of the half-duplex are the efficiency and distance limitation, in which the link distance is limited by the minimum MAC frame size. This restriction reduces the efficiency drastically for high-rate transmission. Therefore, the carrier extension technique is used to ensure the minimum frame size of 512 bytes in Gigabit Ethernet to achieve a reasonable link distance.

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.

ETHERNET TECHNOLOGIES

Nomenclature	Speed (Mbps)	Distance (meters)	Media
10BaseT	10	100	Copper
100BaseTX	100	100	Copper
100BaseFX	100	2,000	Multimode fiber
1000BaseLX	1000	5,000	Single mode fiber
	1000	550	Multimode fiber
1000BaseSX	1000	550	Multimode fiber (50u)
	1000	275	Multimode fiber (62.5u)
1000BaseCX*	1000	25	Copper
1000BaseT	1000	100	Copper

**Not supported by industry products*

WIRELESS LINK

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.

- 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.

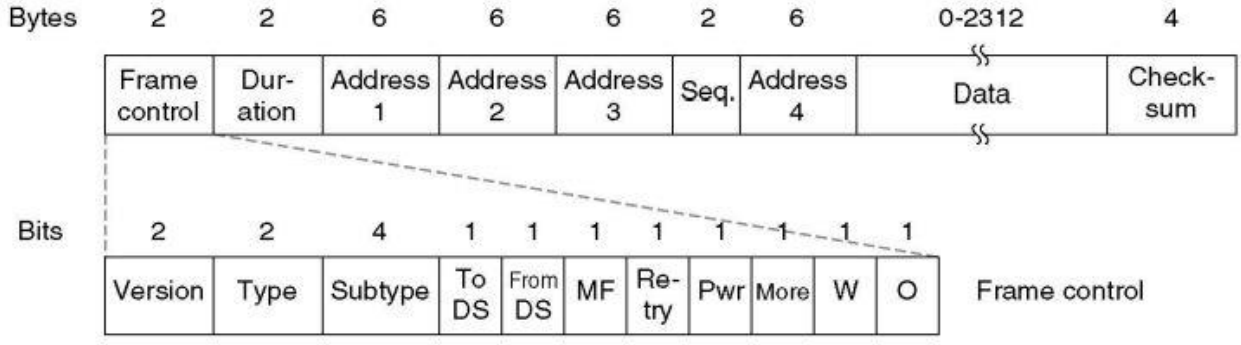


Fig: the 802.11 frame structure

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.

b) 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.

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.

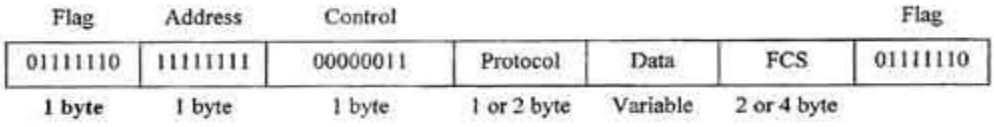
vi. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

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

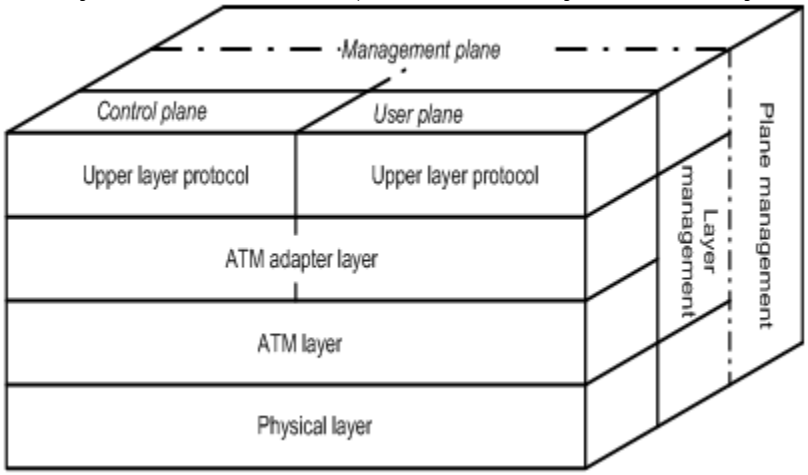
Asynchronous Transfer Mode (ATM) is also called *cell relay*, a high-speed switched network technology developed by the telecommunications industry to implement the next, BROADBAND generation of ISD. ATM was designed for use in WANS such as the public

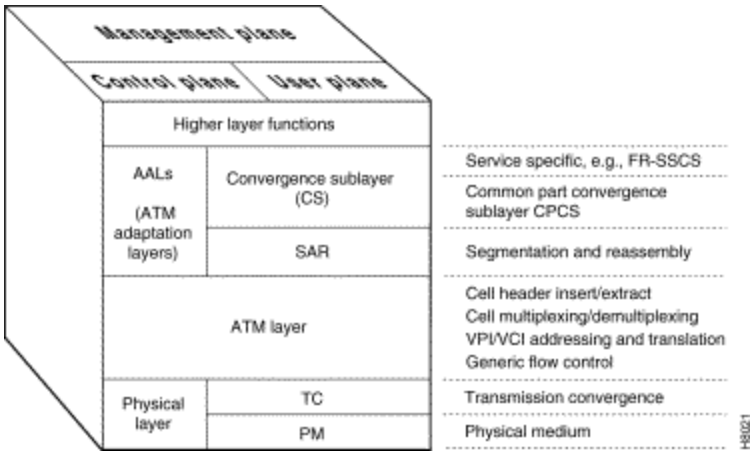
telephone system and corporate data networks, though it has also been applied to create super-fast LANS. It can carry all kinds of traffic - voice, video and data – simultaneously at speeds up to 155megabits per second.

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:

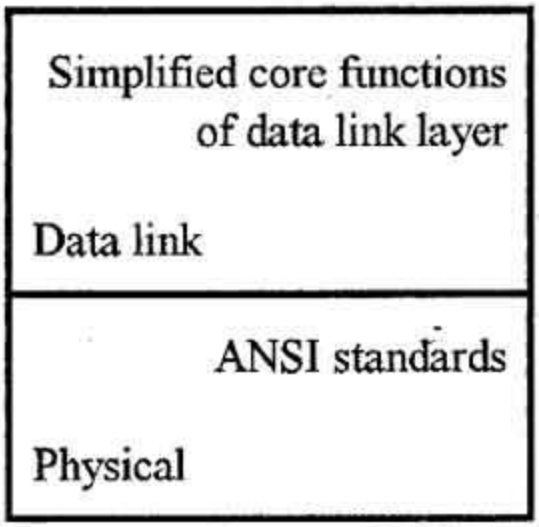
i. Frame relay operates at a high speed (1.544 Mbps to 44.376 Mbps).
ii. Frame relay operates only in the physical and data link layers. So it can be easily used in Internet.
iii. It allows the bursty data.
iv. It has a large frame size of 9000 bytes. So it can accommodate all local area network frame 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.