MAC SUB LAYER

Networks are divided into two categories, point to point and broadcast. Here we concentrate about broadcast networks. In any broadcast network, the key issue is assigning a channel to a user when there is a competition. Consider a conference call with 5 people on 5 different telephones, are all connected together so that each one can hear and talk to others. It may happen sometimes when one of them stops speaking, two or more may start talking at once. This leads to collisions. In a face to face meeting, these are avoided by raising hands to get permission to talk. But when we have a single channel, channel allocation is very hard. Broadcast channels are sometimes known as multi-access channels or random access channels. Protocols used to determine who goes next on a multi access channel belongs to a sub layer of data link layer called Medium Access Control Sub Layer.

Channel Allocation Problem:

Static Channel Allocation: The general way of allocating a single channel among multiple users is Frequency Division Multiplexing. According to this, if there are N users, the bandwidth is divided into N equal portions. Each user is given a portion.

When the number of users is large and continuously varying or the traffic is bursty, FDM has some problems.

1. If the spectrum is cut into N regions, and if users are less than N, lot of bandwidth will be wasted.
2. If number of users is greater than the available N regions, then some of them will be denied permissions to transmit, for lack of bandwidth. According to the performance of the channel, when there is a single user.

Let us assume that T is a minimum time delay, for a channel of capacity C bps, with an arrival rate of λ frames/sec, each frame has $1/\mu$ bits/sec.

$$T=1/(\mu c-\lambda)N \quad = N/\mu c-\lambda=NT$$

So the performance is degraded when number of users increases

Dynamic Channel Allocation:

Station Model: This model has n independent stations and the work generated is at a constant rate. Once a frame is generated, the station is blocked and does nothing until the frame has been successfully transmitted.

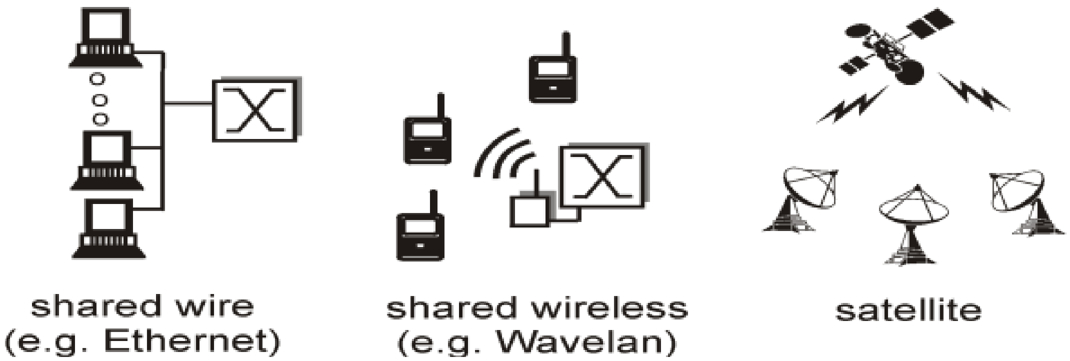
Single Channel Assumption: A single channel is available for communication. All stations can transmit on and receive from it.

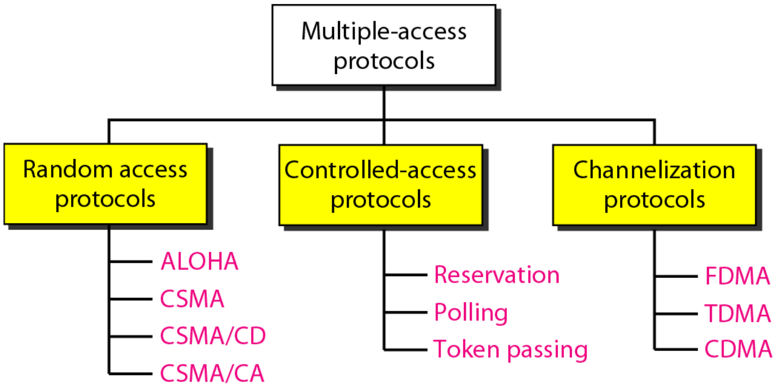
Collision Assumption: if two frames are transmitted simultaneously. They overlap in time and the resulting signal is garbled. This event is called a collision. All stations can detect collisions. A collided frame must be retransmitted. There are no errors other than these collided frames.

Continuous Time: Frame transmissions can begin at any instant. There is no master clock to divide the time into discrete intervals.

Slotted Time: Time is divided into discrete intervals. Frame transmissions always begin at the start of a slot. A slot may contain 0, 1 or more frames, corresponding to an idle slot, a successful transmission or a collision, respectively.
Carrier Sense: Before trying to use the channel, station can sense either channel us idle or it is using by some other station. If the channel is busy, no station will try to use it until it goes idle.
No carrier sense: Stations cannot sense the channel. They just transmit whenever they want. Latter they identify whether the transmission was successful or not.

Multiple Access Protocols:
When more than two nodes send at the same time , the transmitted frames collide.
All collide frames are lost and the bandwidth of the broadcast channel will be wasted.
We need multiple –access protocol to coordinate access to multipointor broadcast link (Nodes or stations are connected to or use a common link)
Multiple access protocols are needed in wire and wireless LANs and satellite networks





ALOHA:
In the year 1970, Norman Abramson and his colleagues devised a new elegant method to solve the channel allocation problem at the University of Hawaii for use with satellite communication systems in the Pacific. In a wireless broadcast system or a half-duplex two-way link, Aloha works perfectly. But as networks become more complex, for example in an Ethernet system involving multiple sources and destinations in which data

travels many paths at once, trouble occurs because data frames collide (conflict). The heavier the communications volume, the worse the collision problems become. The result is degradation of system efficiency, because when two frames collide, the data contained in both frames is lost.

To minimize the number of collisions, thereby optimizing network efficiency and increasing the number of subscribers that can use a given network, a scheme called slotted Aloha was developed. This system employs signals called beacons that are sent at precise intervals and tell each source when the channel is clear to send a frame. Further improvement can be realized by a more sophisticated protocol called Carrier Sense Multiple Access with Collision Detection (CSMA).

The two versions of Aloha are :

1. Pure Aloha
2. Slotted Aloha

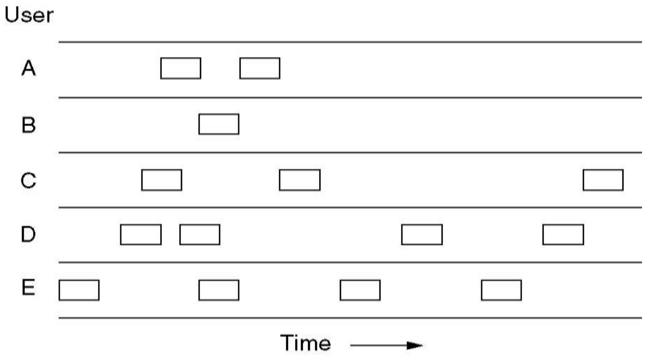


Fig: Frames are transmitted completely at arbitrary(random) times

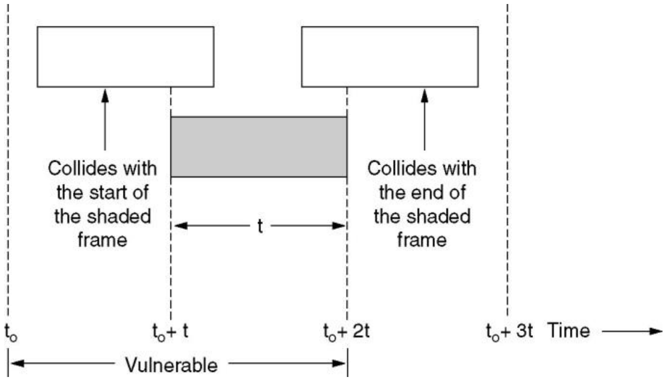
In the above architecture, all frames are of fixed length because the throughput of the Aloha systems is maximized by having a uniform frame size rather than allowing variable length frames. Whenever two stations wants to transfer their frames in the same time interval there will be a collision and both will be garbled. If the first bit of a new frame overlaps with the last bit of old frame, both frames will be totally destroyed and both will be retransmitted latter. The checksum algorithm cannot distinguish between a total or near loss.
Frame time: the amount of time required to transmit the standard fixed length frame
According to Poisson distribution S is the mean number of frames that can be distributed during a frame time.

If s>1 the user is generating more number of frames than the channel can handle, in this case every frame will suffer a collision
So the reasonable throughput is 0<s<1

In addition to new frames, stations must also generate retransmission of frames that

suffered collisions.
So, Let K be the number transmission attempts during a frame time(old and new combined)
Where G is the mean probability of transmission attempts per frame time
So G>=S
At low load(s=0) there will be few collisions and hence few transmissions, So G=S
At high load there will be many collisions, So G>s
At all loads, the throughput is just the offered load G.
The probability of transmission being successful is **$S=GP_0$**
Where P_0 is the probability of a frame that does not suffer collision

A frame will not suffer a collision if no other frames are sent within one frame time of its start.


Collides with the start of the shaded frame
Collides with the end of the shaded frame
t
t_o
t_o+ t
t_o+ 2t
t_o+ 3t
Time
Vulnerable

Now, let us see the various conditions at what rate, the shaded frame arrives undamaged. Let t be the time required to send a frame. if any other user has generated a frame between t_0 and t_0+t, the end of that frame will collide with the beginning of the shaded frame.
Similarly, anyn other frame started between t_0+t and t_0+2t collides with the end of the shaded frame. the probability of K framws generated during a frame time is given by the Poisson distribution

Prob[k transmissions in time t] = $(G^k \times e^{-G})/(k!)$

So the probability of 0 frames is just **e^{-G},**

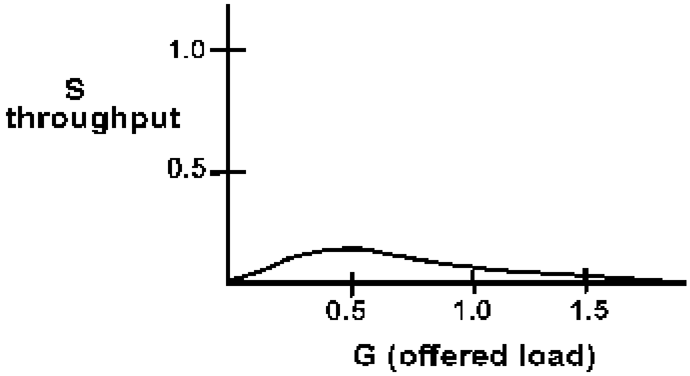
In an interval of two frames long the mean no of frames generated is 2G

So the probability of no other traffic being initiated during the entire vulnerable period is

$$P_0 = e^{-2G}$$

Using $s=GP_0$, we get $s=G\, e^{-2G}$

When G=0.5 and s=1/2e which is about 0.184 means we are utilizing 18% of the channel.



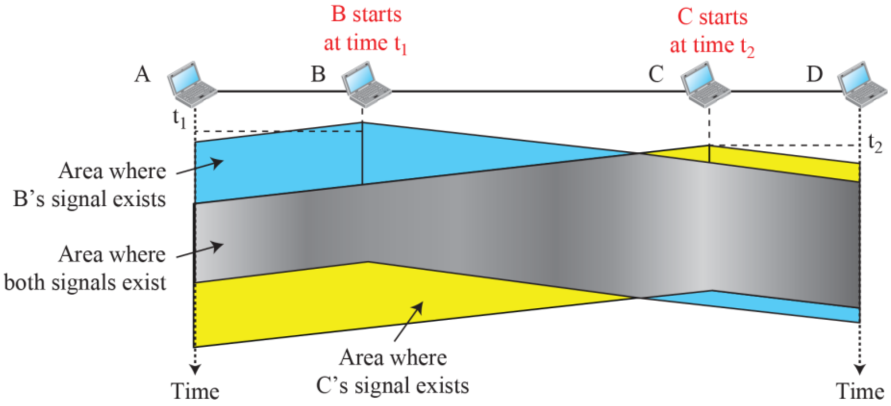
Slotted Aloha: In 1972 Roberts devised a method to double the capacity of an ALOHA system. According to his proposal, channel has to divide time into discrete time intervals. Each interval corresponds to one frame. This process requires the users to agree of slot boundaries. Now the continuous pure aloha is turned into discrete one.

So S=G $\mathbf{e}^{-G}$

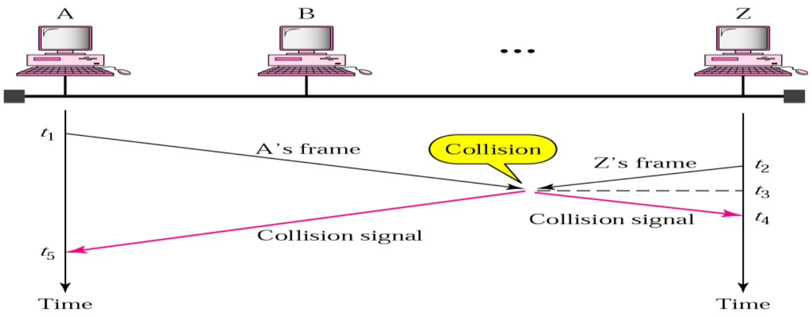
Slotted aloha peaks at G=1 with a throughput of s=1/e, i.e, 36% channel is utilized.

Carrier sense Multiple Access Protocols

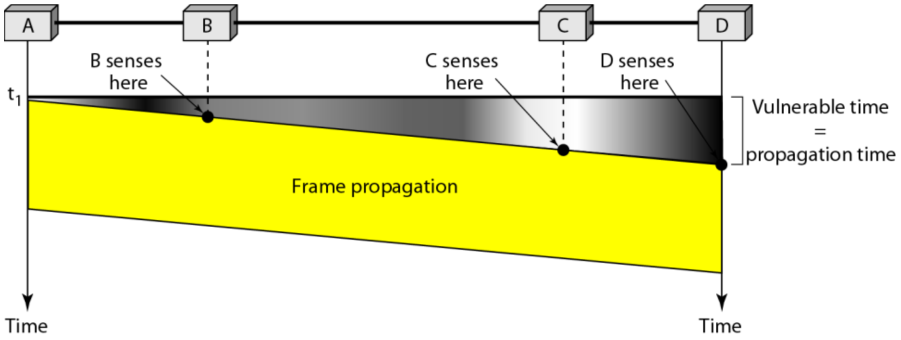
To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle “sense before transmit” or “listen before talk.”



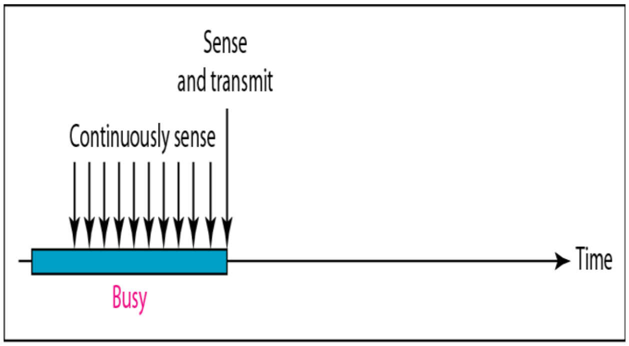
CSMA can reduce the possibility of collision, but it can not eliminate it because of the propagation delay (a station may sense the medium and find it idle, only because the first bit of a frame sent by another station has not been received)



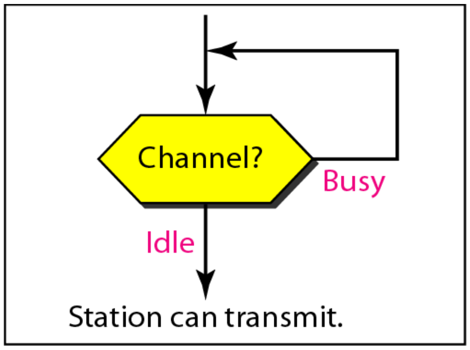
Vulnerable time: time in which there is a possibility of collision
Vulnerable time for CSMA is the **max propagation time Tp**needed for a signal to propagate from one end of the medium to the other



1 **Persistance Method:**
When the sender (station) is ready to transmit data, it checks if the medium is busy. If so, it senses the medium continually until it becomes idle. If line is idle, sends the frame immediately (with probability of 1).Chances of collision is high**.**



a. 1-persistent

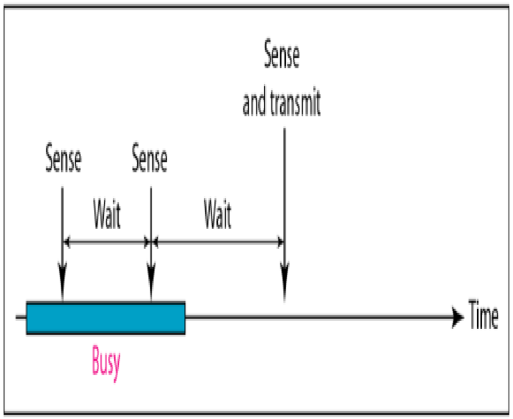


a. 1-persistent

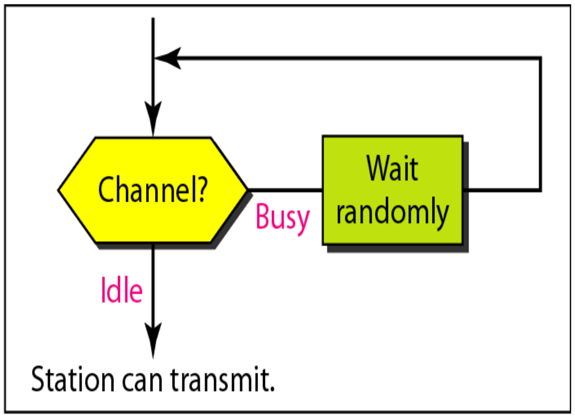
Non Persistence Methods:

- If a station has a frame to send, it senses the line.
- If the line is idle station sends frame immediately.
- If a line is not idle, station waits a random period of time and then senses the channel again.
- With this chances of collisions are reduced

- Reduces efficiency of the network (because the medium remain idle when there may be stations with frames to send



b. Nonpersistent



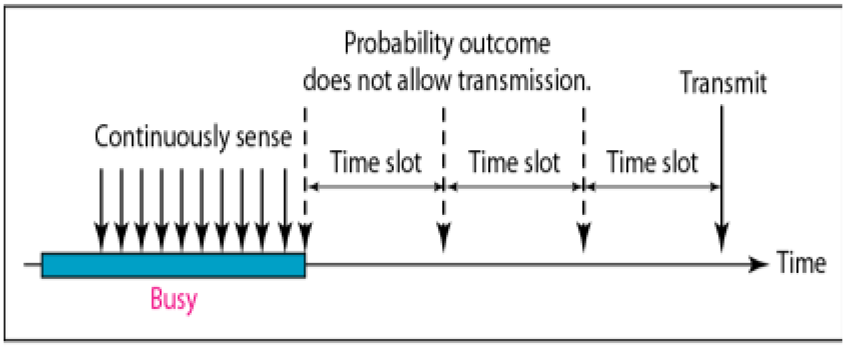
b. Nonpersistent

P-Persistence:

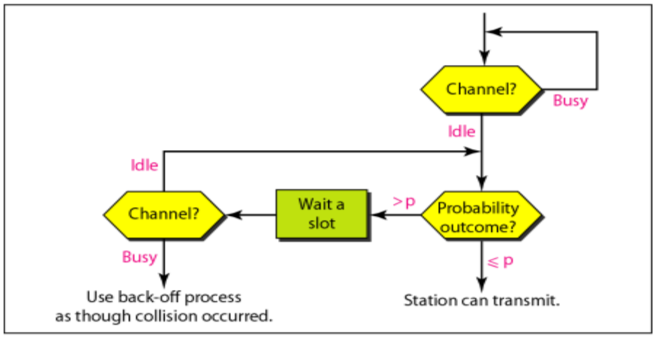
It is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.

When the sender (station) is ready to transmit data, it checks if the medium is busy. If so, it senses the medium continually until it becomes idle.

- If line is idle it may or may not send. It sends with probability p.
- Reduces the chance of collision and improves the efficiency by combining the other two strategies



c. p-persistent

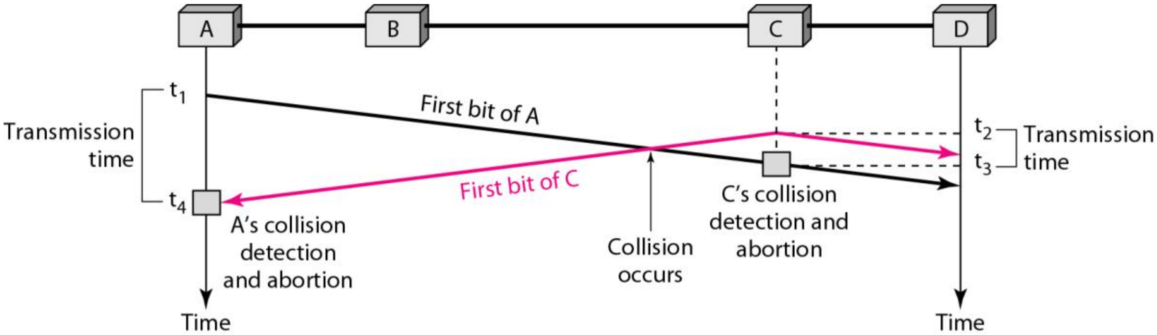


c. p-persistent

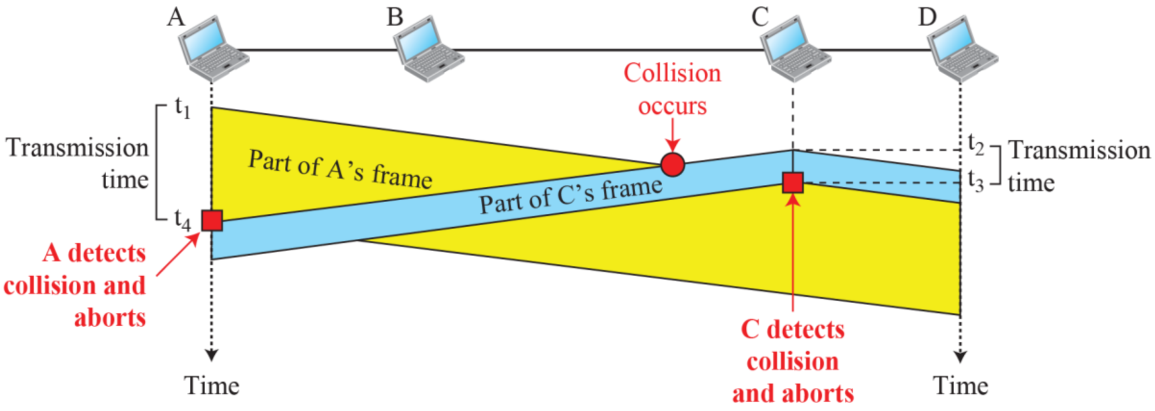
CSMA/CD :

A station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision. The following fig shows what happens when the first bits of A and C collide.



At time t1, station A has executed its persistence procedure and starts sending the bits of its frame. at time t2, station C has not yet sensed the first bit sent by A. station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t2 . station C detects a collision at time t3 when it receives the first bit of A's frame. station C immediately aborts transmission. Station A detects collision at time t4 when it receives the first bit of C's frame and also immediately aborts transmission.



Minimum Frame Size

For CSMA/CD to work correctly we need to restrict the minimum frame size. Before sending the last bit of a frame, the sending station must detect a collision and abort the transmission.

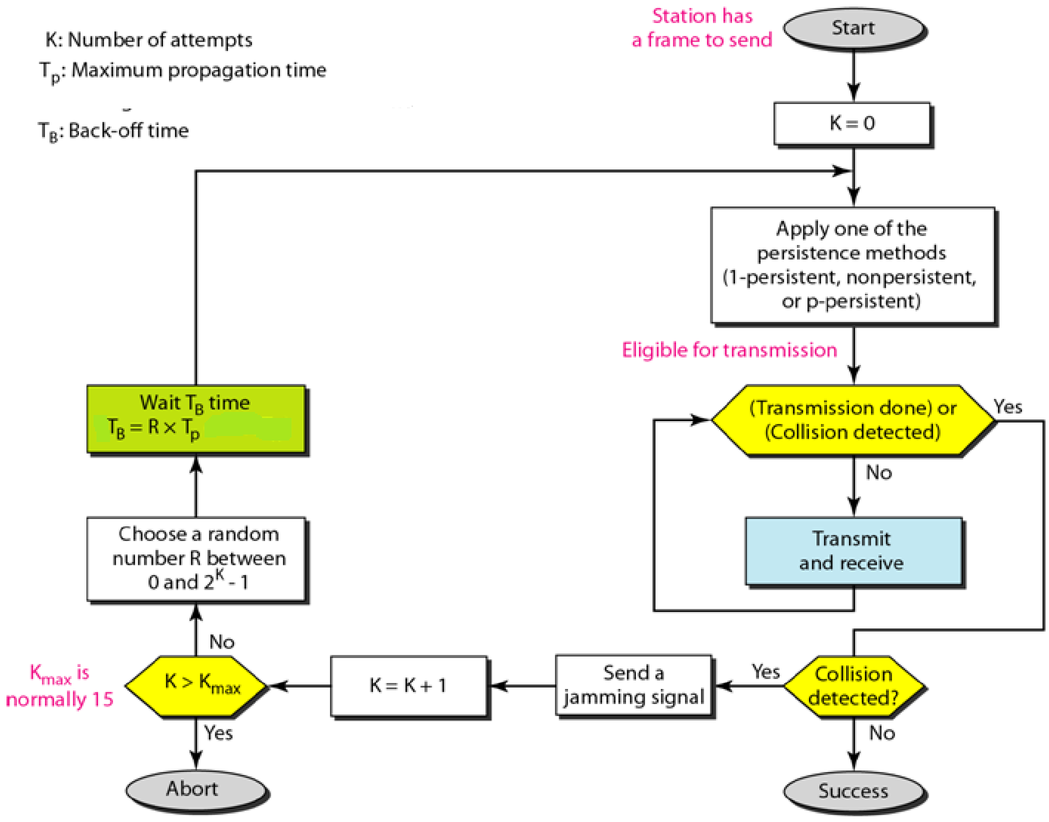
This is so because the station, once the entire frame is sent does not keep a copy of the frame and does not monitor the line of collision detection.

For the worst cases cenario ;if the two stations involved in a collision are the max distance apart transmission time > = 2 x max. propagation timeTfr> =2 X Tp(MinFrame size)/B-W = 2 X Tp

Ex: A network using CSMA/CD has a bandwidth of 10Mbps .If the maximum propagation time(including the delays in the devices and ignoring the time needed to send a jamming signal)is25.6µs,what is the minimum size of the frame?

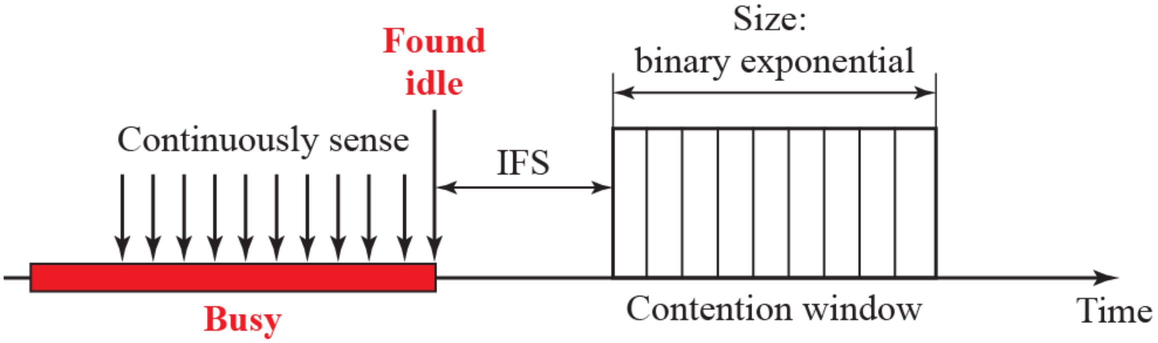
Solution:

The frame transmission time is Tfr=2×Tp=51.2µs. This means, in the worstcase, a station needs to transmit for a period of 51.2µs to detect the collision. The minimum size of the frame=10Mbps×51.2µs=512bitsor64bytes.This is actually the minimum size of the frame for Standard Ethernet.


K: Number of attempts
T_p: Maximum propagation time
T_B: Back-off time
Station has a frame to send
Start
K = 0
Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)
Eligible for transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Collision detected?
Yes
No
Success
Send a jamming signal
K = K + 1
K > K_{max}
K_{max} is normally 15
No
Yes
Abort
Choose a random number R between 0 and 2^K - 1
Wait T_B time
$T_B = R \times T_p$

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies: the inter frame space, the contention window, and acknowledgments.



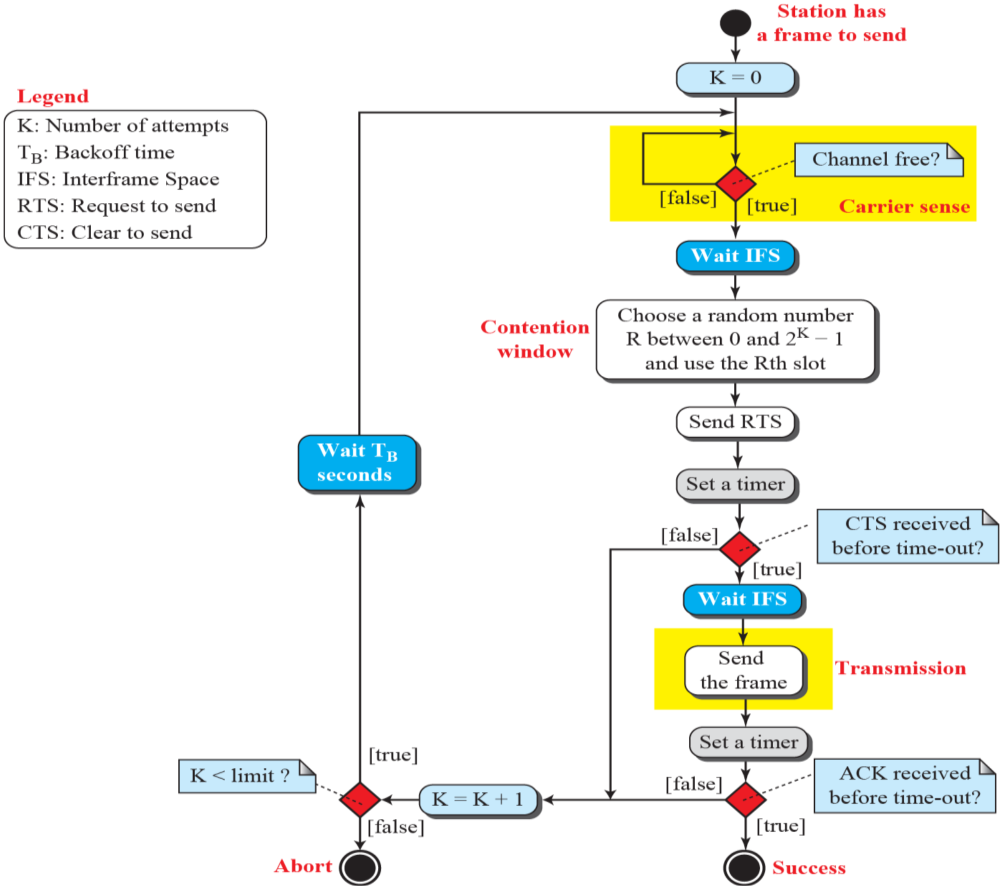
Inter Frame Space(IFS):

Collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called inter fame space or IFS. Even though the channel may appear idle when it is sensed, a distant station may have already started transmission. The distant stations signal has not yet reached to his station. The IFS time allows the transmitted signal by the distant station to reach this station. If after the IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time.

Contention Window: An amount of time is 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 algorithm. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

Acknowledgement: with all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive ack and the time-out timer can held guarantee that the receiver has received the frame.

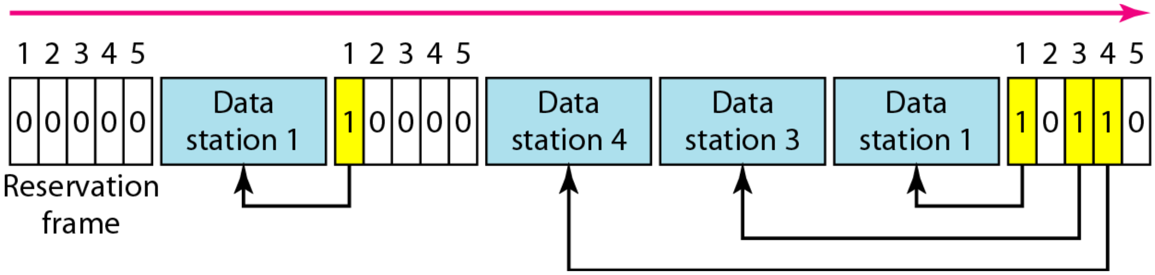
Procedure: The channel needs to be sensed before and after the IFS. The channel also needs to be sensed during the contention time. For each time slot of the contention window, the channel is sensed. If is found idle, the timer continues; if the channel is found busy, the timer is stopped and continues after the time becomes idle again



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.

Reservation: 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 reserved mini slots in the reservation frame. Each mini slot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own mini slot. The stations that have made reservations can send their data frames after the reservation frame. In the following figure station 1,3 and 4 have made reservations in the first slot. In the second slot only station 1 has made a reservation.

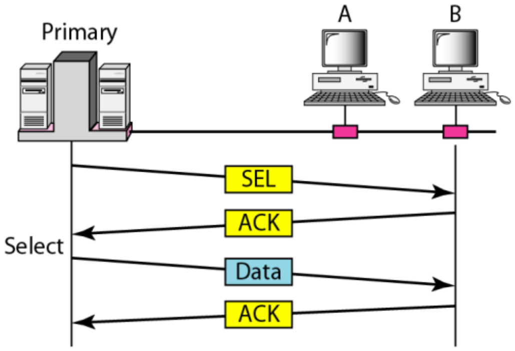


Polling:

It 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 station is a secondary device. The primary device controls the link: the secondary device 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.

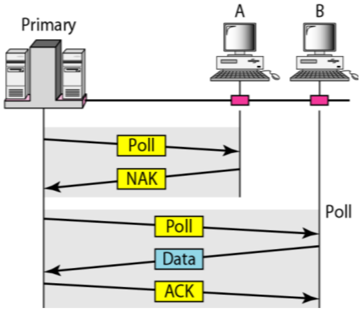
If the primary wants to receive data, it asks the secondaries if they have anything to send. This is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function:

Select: It is used whenever the primary device has something to send. If the primary is neither sending nor receiving data, it knows the link is available. If it has something to send, the primary sends. The primary alerts the secondary to the upcoming transmission and wait for an ack of the secondary's ready status. Before sending data, the primary creates and transmits a select (SEL) frame



Poll: 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 if it does. If the response is NAK, the primary polls the next secondary. If it receives data, it sends ACK frame



Token Passing:

In the token-passing, the stations are organized in a logical ring. For each station there is a predecessor and a successor. Predecessor is the station which is logically before the station in the ring. The successor is the station which is logically after the station in the ring. The current station is the one that accessing the channel now.

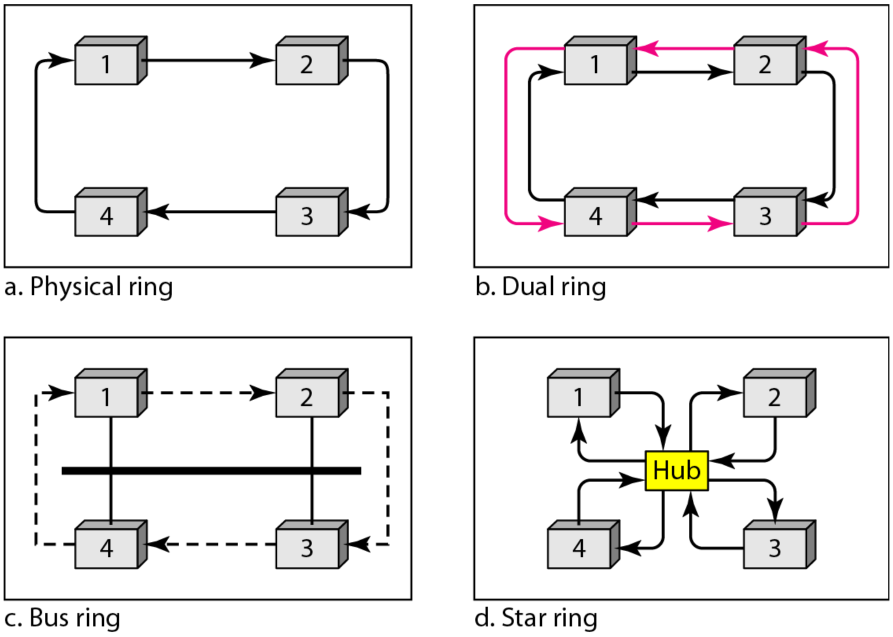
How is The right to access channel passed from one station to another?

Station is authorized to send data when it receives a special frame called a token

- Stations are arranged around a ring.
- When no data are being sent, a token circulates the ring.
- If a station needs to send data, it waits for the token.
- The station captures the token and sends one or more frames (as long as it has frames to send or the allocated time has not expired), and finally it releases the token to be used by next station (successor).
- The maximum time any station can hold the token is limited.
- Since there is only one token, only one station transmits at a time, and collisions never occur.

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(if the station that is holding the token fails, the token will disappear from the network)
- Assign priorities to the stations , to make low-priority stations release the token to high priority stations.
- Stations do not have to be physically connected in a ring ; the ring can be logical one.



a. Physical ring

b. Dual ring

c. Bus ring

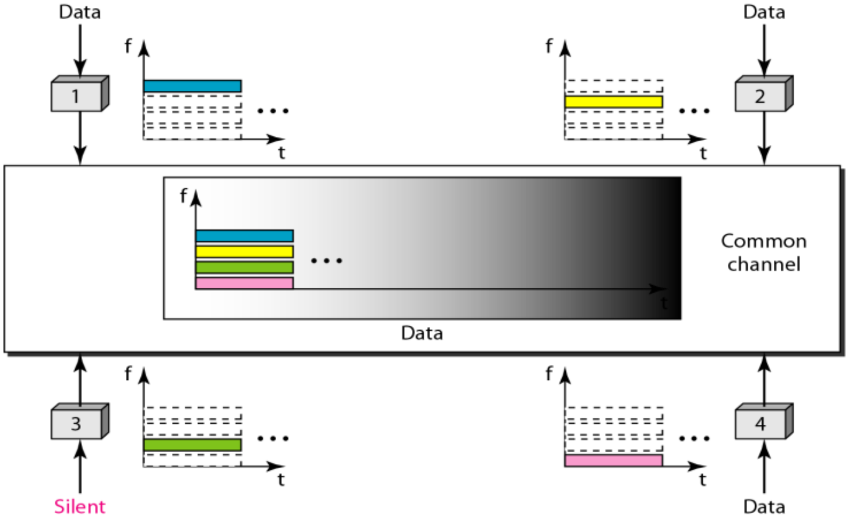
d. Star ring

Channelization:

Channelization is a multiple access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.

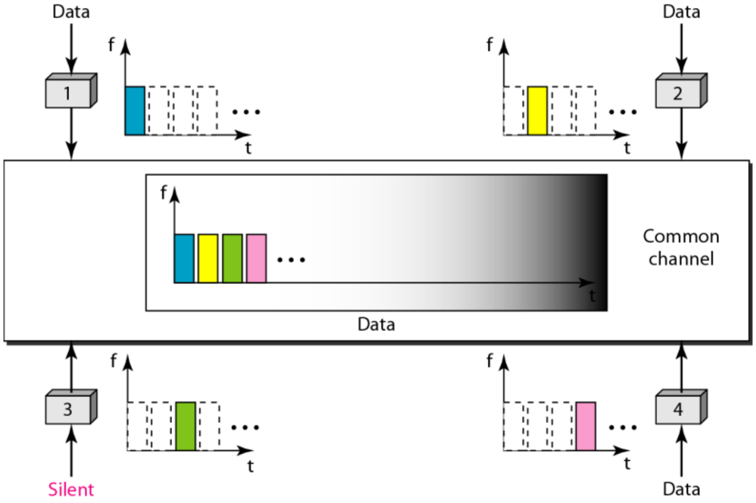
FDMA:

In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands. The bandwidth is just one channel that is timeshared between different stations.



TDMA:

The bandwidth is just one channel that is timeshared between different stations

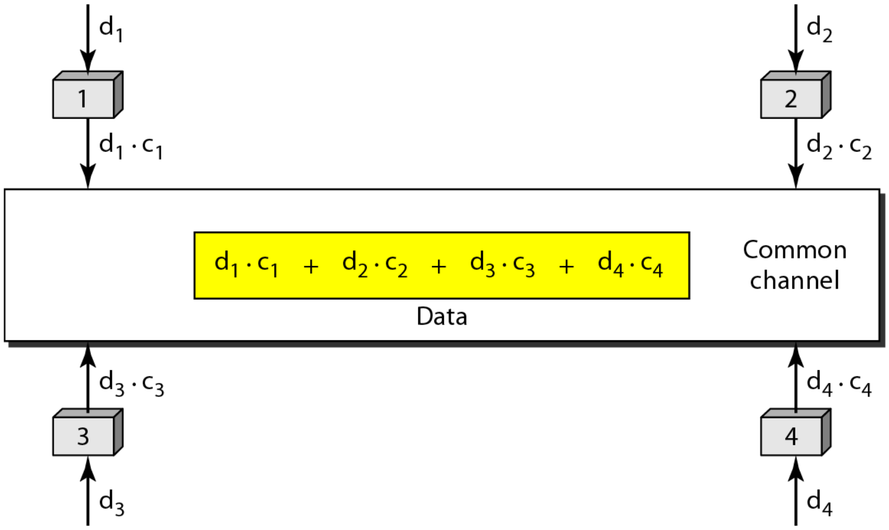


CDMA:

In CDMA, one channel carries all transmissions simultaneously. CDMA simple means communication with different codes. Four stations namely 1,2,3,4 are connected to some channel. The data from station 1 is d1, from station 2 is d2, and so on. The code assigned to the first station is c1, to the second is c2, and so on. Assigned codes have the following properties.

1. If we multiply each code by another code, we get 0.
2. If we multiply each code by itself, we get 4.

Station 1multiplies its data by its code to get d1.c1. station 2 multiplies its data by its code to get d2.c2 and so on. The data that go on the channel is sum of all these products.

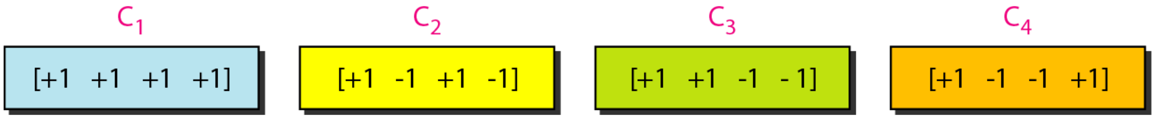


Any station that wants to receive data from one of the other three multiplies the data on the channel by the code of the sender.

Ex: suppose stations 1 and 2 are talking to each other. Station 2 wants to hear what station 1 is saying. It multiplies the data on the channel by c1.

Data=(d1.c1+d2.c2.+d3.c3+d4.c4).c1
=(d1.c1.c1+d2.c2.c1+d3.c3.c1+d4.c4.c1)
=(d1.4+0+0+0)
=4d1

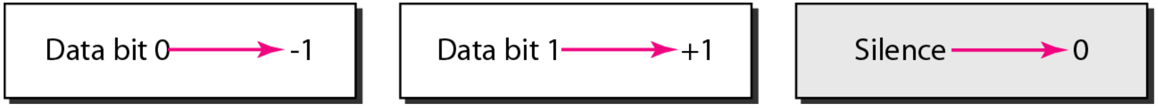
Chips: CDMA is based on the coding theory. Each station is assigned a chip code., which is a sequence of numbers called chips.



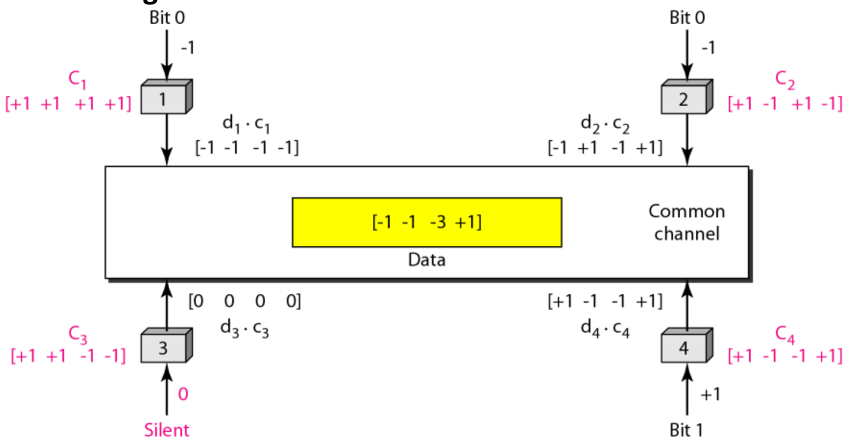
These codes are called orthogonal sequences.

- Each sequence is made of N elements, where N is the number of stations.
- If we multiply a sequence by a number, every element in the sequence is multiplied by that element. This is called multiplication of a sequence by a scalar.
  2[+1 +1 -1 -1] = [+2 +2 -2 -2]
- If we multiply two equal sequences, element by element, and add the results, we get N, where N is the number of elements in each sequence. This is called the inner product of two equal sequences.
  [+1 +1 -1 -1].[+1 +1 -1 -1] = 1+1+1+1 =4
- If we multiply two different sequences, element by element and add the results, we get 0, this is called inner product of two different sequences.
  [+1 +1 -1n -1].[+1 +1 +1 +1] = 1+1-1-1= 0
- Adding two sequences means adding the corresponding elements. The result is another sequence.
  [+1 +1 -1 -1]+[+1 +1 +1 +1]= [+2 +2 0 0]

Data Representation: If a station needs to send a 0 bit, it encodes it as -1; if it needs to send a 1 bit, it encodes it as a +1. When a station is idle, it sends no signal which is interpreted as a 0.



Encoding and Decoding:

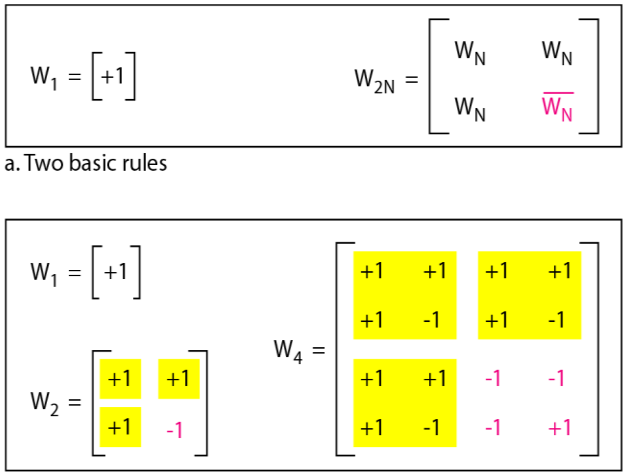


Here station 3 is silent and is listening to station 2. Station 3 multiplies the total data on the channel by the code for station 2, to get.

[-1 -1 -3 +1].[+1 -1 +1 +1]=-4/4=-1 → means bit 0

Sequence Generation:

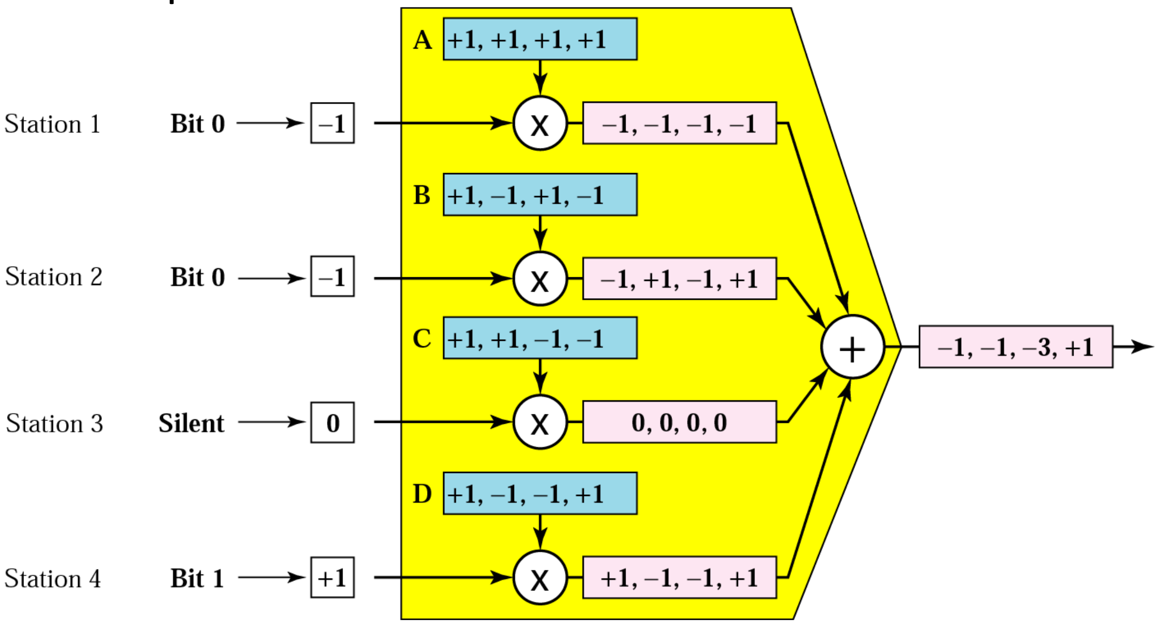
To generate chip sequences, we use a walsh table, a two dimensional table with an equal number of rows and columns.


$W_1 = \begin{bmatrix} +1 \end{bmatrix}$
$W_{2N} = \begin{bmatrix} W_N & W_N \\ W_N & \overline{W_N} \end{bmatrix}$
$W_1 = \begin{bmatrix} +1 \end{bmatrix}$
$W_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$
$W_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$

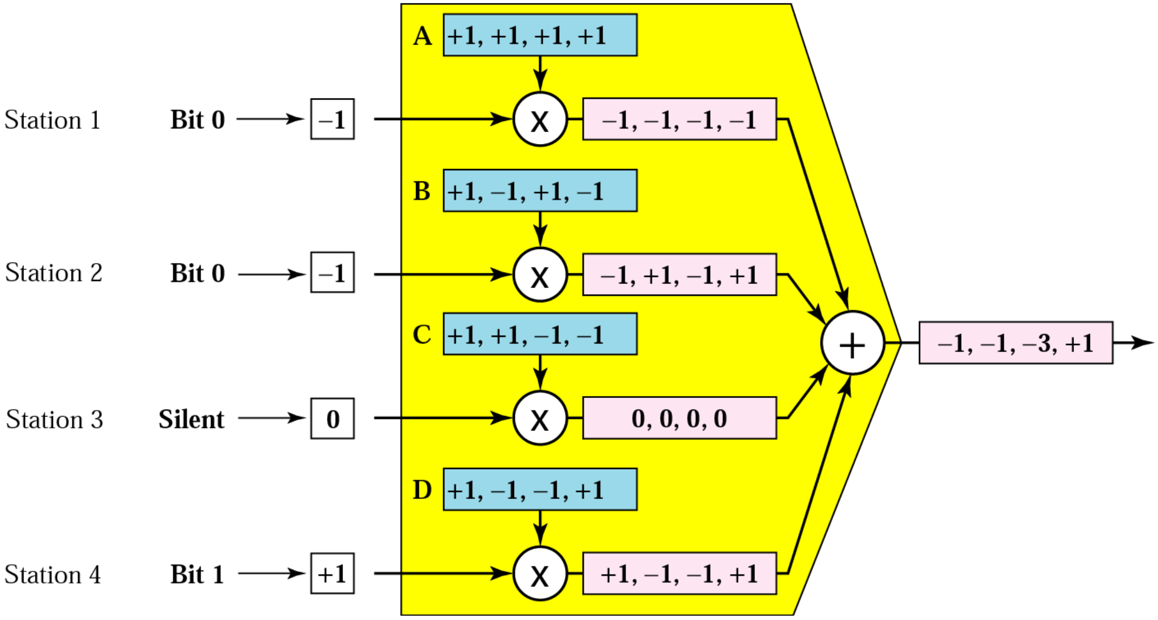
a. Two basic rules

b. Generation of W_1, W_2, and W_4

CDMA Multiplexer



CDMA Demultiplexer



IEEE Standards

In 1985, the computer society of the IEEE started a project, called project 802 to set standards to enable intercommunication among equipment from a variety of manufacturers. The IEEE has subdivided the data link layer into two sub layers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.

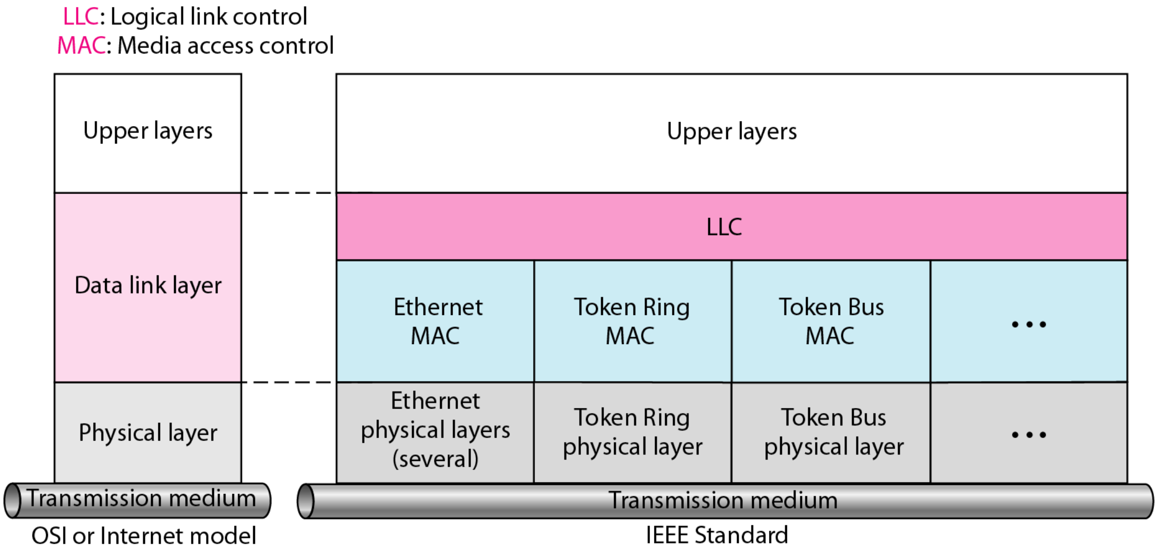


Fig: IEEE standards for LANs

Data Link Layer: Divided into two sub layers: MAC and LLC

Logical Link Control (LLC): In IEEE project 802, flow control, error control and part of the framing duties are collected into one sub layer called the logical link control. Framing is handled in both LLC sub layer and the MAC sub layer. The LLC provides one single data link control protocol for all IEEE LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes MAC sub layer transparent.

Framing: LLC defines a protocol data unit that is similar to HDLC.

Comparison of HDLC with LLC and MAC: LLC header contains a control field like the one in HDLC. This field is used for flow and error control. The two other header fields define the upper layer protocol at the source and the destination that uses LLC. These fields are called destination service access point and source service access point. The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sub layer. A frame defined in HDLC is divided into a PDU at the LLC sub layer and a frame at the MAC sub layer.

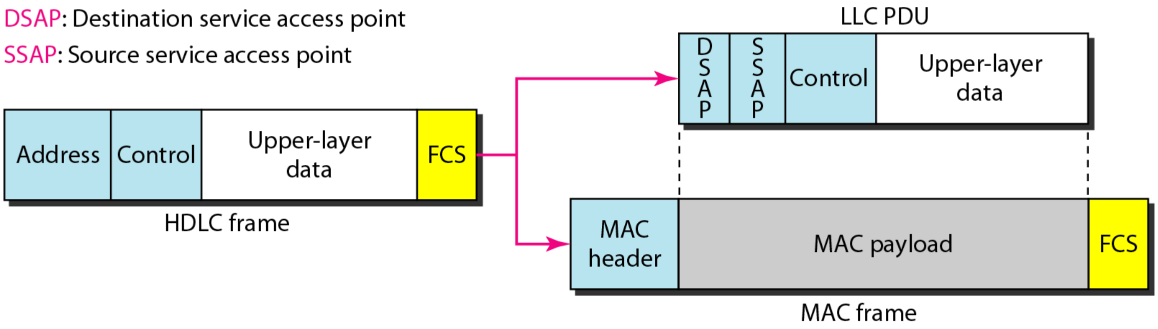


Fig: HDLC frame is compared with LLC and MAC

Need for LLC: The purpose of LLC is to provide flow and error control for upper layer protocols. However, most upper layer protocols such as IP, do not use the services of LLC.

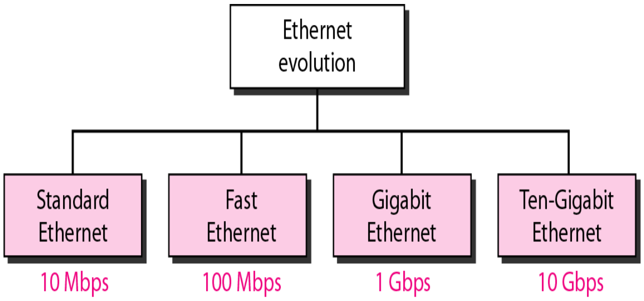
MAC: 802 has created a sub layer called media access control that defines the specific access method (like random access, controlled access, and channelization) for each LAN. For example it defines CSMA/CD as the media access method for Ethernet LANs and token passing method for Token Ring and Token Bus LANs. In contrast to LLC sub layer, the MAC sub layer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

IEEE 802 standard for LAN, MAN and WLANs

These standards are divided into various parts. 802.1 standard gives an introduction to the set of standards and defines the interface primitives. 802.2 standard describes the upper part of the data link layer which uses the LLC protocol. 802.3 to 802.5 describes about LAN standards, CSMA/CD. Token bus and token ring architectures.

IEEE 802.3 Standard Ethernet

The original Ethernet was created in 1976 at Xerox Palo Alto Research Center (PARC). Since then it has gone through four generations: Standard Ethernet (10Mbps), Fast Ethernet (100Mbps), Gigabit Ethernet (1Gbps), and Ten-Gigabit Ethernet (10Gbps).

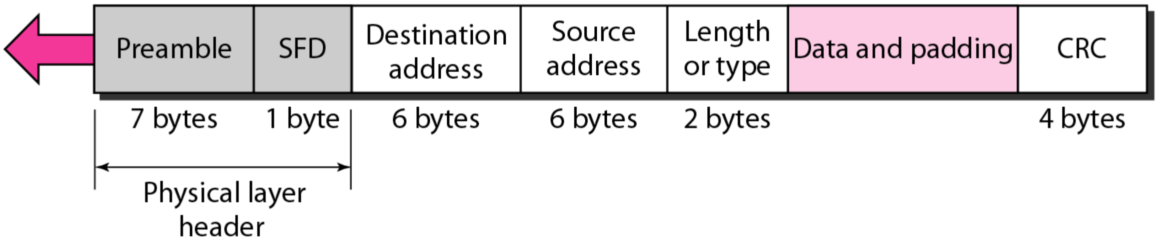


The 802.3 MAC sub layer protocol

The IEEE802.3 based Ethernet frame consists of preamble of 56 bit-size, start of the frame delimiter of 8bit size, destination address of 48 bit-size, sources address of 48 bit-size, type field to identify higher layer protocol of 16 bit-size, data field of variable bit-size, and frame check sequence field of 32 bit size. The figure below explains better.

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Preamble: Each frame starts with this field. Length of this field is 7 bytes, each byte contains the bit pattern 10101010. It alerts the receiving device to synchronize its time clock with the source.

Start Frame Delimiter: Length of this field is 1 byte which contains 10101011 to denote the start of the frame. The SFD warns the station that this is the last chance to synchronize. The last two bits are 11 and alerts the receiver that the next field is destination address.

Source and Destination Address: Represents the 6 byte MAC address of source and destination stations. Each station on an Ethernet has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6 byte physical address. It is written in hexadecimal colon notation.

Ex: 06:01:2A:4C:F0:3B

Length: Determines how many bytes can be inserted in a single frame. The maximum size is 1500 bytes. To make it easier to distinguish valid frames from garbage, 802.3 states that valid frames must be at least 64 bytes long, from destination address to CRC.

The maximum length of a frame is 1500 bytes and minimum length is 64 bytes. If we subtract the MAC layer header 18 bytes (destination address + source address + length + CRC) from minimum length, then the data from the upper layer is 46 bytes. If the upper layer data is less than 46 bytes then required number of random bits are padded to make up a frame.

CRC: contains error detection information and is used to find damaged frames. CRC-32 algorithm is used to generate this 32 bit code.

Access Method: It is 1-persistent CSMA/CD LAN. According to the scheme, when a station wants to transmit it listens to the channel. If the channel is busy, the station waits until it goes idle; otherwise it transmits immediately. If two or more station simultaneously begin transmitting on an idle channel, they will collide each other. All collided stations terminate their transmissions and wait a random time. The XEROX Ethernet was so successful at 10Mbps. This standard forms the basis for 802.3

Physical Layer:

802.3 cabling:

Name	Cable	Max Segment	Nodes/segment	Advantages
10 Base 5	Thick Coax	500 m	100	Good for backbones
10 Base 2	Thin Coax	200 m	30	Cheapest System
10 Base T	Twisted Pair	100 m	1024	Easy maintenance
10 Base F	Fiber Optics	2000 m	1024	Best between buildings

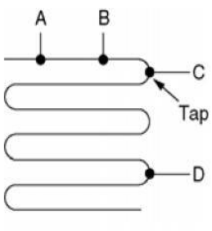
10 Base 5: Also called thick Ethernet. It looks like a yellow garden hose with markings over every 2.5 meters to show where the connections should go. Connections to it are generally made using vampire taps. 10 Base 5 means it operates at 10 Mbps, uses base band signaling, and can support segments of up to 500 meters

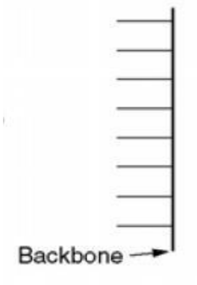
10 Base 2: Historically it is known as thin Ethernet. It bends easily. Connections to it are made using industry standard BNC connectors to form T junctions. But it can run only 200m and can handle only 30 machines per cable segment.

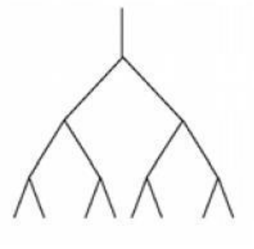
But in both the schemes, detecting cable breaks is difficult. The problems associated with finding cable breaks have a cable running to a central hub. Usually these wires are telephone company twisted pairs. This scheme is called 10Base T.

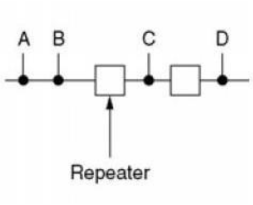
10Base F : it is highly expensive due to the cost of the connectors and terminators, but it has excellent noise immunity and is the method of choice when running between buildings or widely separated hubs. The different ways wiring up a building are shown below:

Linear: The linear topology is like a single cable running in all portions of building. The stations are connected to the cable through tapping.









Spine: It looks like our back bone spinal cord, where multiple numbers of horizontal cables are connected to a vertical line through special amplifiers or repeaters.

Tree: This is most general topology because a network with two paths between some pairs of stations would suffer from interference between the signals.

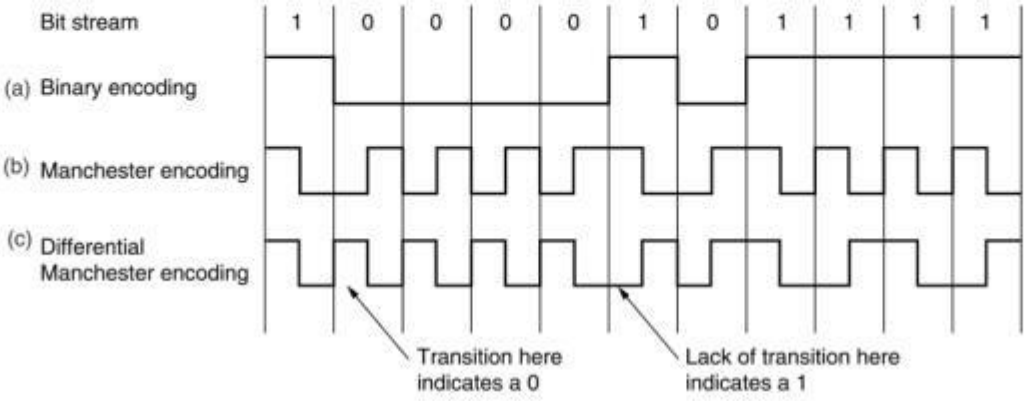
Segmented: Since each version of 802.3 has maximum cable length per segment, to allow larger networks, repeaters can connect multiple cables.

Manchester Encoding: The normal binary logics of one and zero are no more used to send data from one station to other station. The reason of not using plain binary signal is they cause ambiguities resulting in false interpretation of sent data. The major culprit is zero, where even no data is sent the receiver can assume it as zero. So to clear out the ambiguity or to ensure proper interpretation of data, a coding technique called Manchester coding is employed in IEEE802.3 standards. There are two types of Manchester coding: simple Manchester coding and differential Manchester coding.

Each bit is transmitted in a fixed time (the "period").
A 0 is expressed by a low-to-high transition, a 1 by high-to-low transition (according to G.E. Thomas' convention -- in the IEEE 802.3 convention, the reverse is true).
The transitions which signify 0 or 1 occur at the midpoint of a period.
Transitions at the start of a period are overhead and don't signify data.

Manchester code always has a transition at the middle of each bit period and may (depending on the information to be transmitted) have a transition at the start of the period also. The direction of the mid-bit transition indicates the data. Transitions at the period boundaries do not carry information. They exist only to place the signal in the correct state to allow the mid-bit transition. Although this allows the signal to be self-clocking, it doubles the bandwidth requirement compared to NRZ coding schemes (or see also NRZI). In the Thomas convention, the result is that the first half of a bit period matches the information bit and the second half is its complement.

If a Manchester encoded signal is inverted in communication, it is transformed from one convention to the other. This ambiguity can be overcome by using differential Manchester encoding.

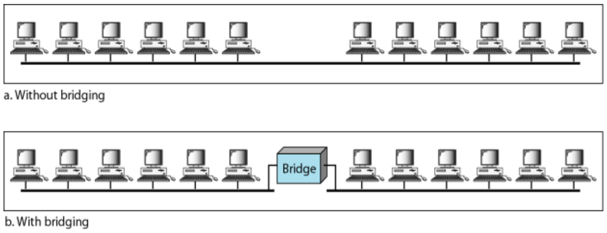

Bit stream
1
0
0
0
0
1
0
1
1
1
1
(a) Binary encoding
(b) Manchester encoding
(c) Differential Manchester encoding
Transition here indicates a 0
Lack of transition here indicates a 1

Differential Manchester Encoding Shown in above figure is a variation of basic Manchester encoding. A '1' bit is indicated by making the first half of the signal equal to the last half of the previous bit's signal i.e. no transition at the start of the bit-time. A '0' bit is indicated by making the first half of the signal opposite to the last half of the previous bit's signal i.e. a zero bit is indicated by a transition at the beginning of the bit-time. In the middle of the bit-time there is always a transition, whether from high to low, or low to high. A reversed scheme is possible, and no advantage is given by using either scheme. All 802.3 baseband systems use Manchester encoding due to its simplicity. The high signal is +0.85 Volts and low signal is -0.85 V giving a DC value of 0 volts.

Changes in the standards:

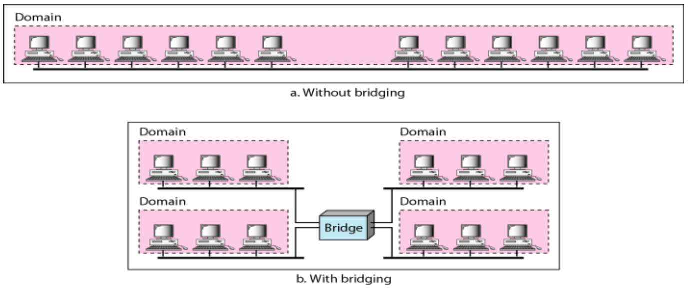
1. **Bridged Ethernet**: The first evolution in Ethernet is dividing LAN by bridges. Bridges have two effects on Ethernet LAN; they raise the bandwidth and they separate collision domain.

Raising the Bandwidth: In an unbridged Ethernet network, the total capacity(10Mbps) is shared among all stations with a frame to send: the stations share the bandwidth of network. If only one station has a frame to send then it can use the total capacity (10Mbps). But if more than one station needs to use the network, the capacity is shared.

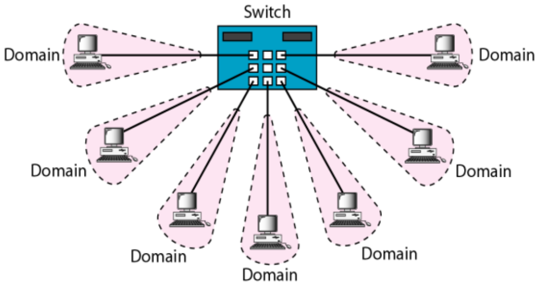


A bridge divides the network into two or more networks. Bandwidth wise each network is independent. A network with 12 stations is divided into two parts each with 6 stations. Now each network has a capacity of 10Mbps. The 10 Mbps capacity is now shared by 6 stations only. If we further divide the network, more bandwidth can be achieved.

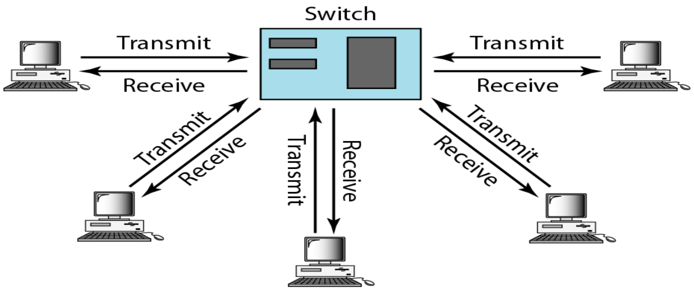
Separating Collision Domains: The following figure shows the collision domain for bridged and unbridged network. Collision domain becomes much smaller and the probability of collision is reduced tremendously.



Switched Ethernet: The idea of bridged LAN can be extended to switched LAN. Instead of having two or four networks, if we have N networks, where N is the number of stations on the LAN. A layer 2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.



Full-Duplex Ethernet: One of the limitations of 10Base5 and 10Base2 is that communication is half duplex; a station can either send or receive, but may not do both at the same time. The next step in the evolution was to move from switched Ethernet to full-duplex switched Ethernet. The full duplex mode increases the capacity of each domain from 10 to 20 Mbps. Instead of using one link between the station and the switch, the configuration uses two links: one to transmit and one to receive.



FAST ETHERNET: This was deigned to compete with LAN protocols such as FDDI or Fiber Channel. IEEE uses fast Ethernet standard as 802.3u. Fast Ethernet is backward compatible with standard Ethernet. But it transmits data 10 times faster than standard Ethernet at a rate of 100 Mbps.

Features:

1. Upgrade the data rate to 100Mbps

2. Make it compatible with standard Ethernet

3. Uses the same 48 bit address

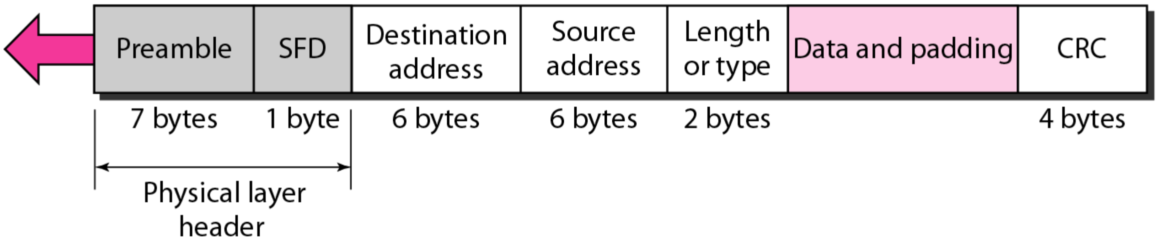
4. Uses the same frame format

5. Keep the same minimum and maximum frame lengths

MAC Sub layer:

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Preamble: Each frame starts with this field. Length of this field is 7 bytes, each byte contains the bit pattern 10101010. It alerts the receiving device to synchronize its time clock with the source.

Start Frame Delimiter: Length of this field is 1 byte which contains 10101011 to denote the start of the frame. The SFD warns the station that this is the last chance to synchronize. The last two bits are 11 and alerts the receiver that the next field is destination address.

Source and Destination Address: Represents the 6 byte MAC address of source and destination stations. Each station on an Ethernet has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6 byte physical address. It is written in hexadecimal colon notation.

Ex: 06:01:2A:4C:F0:3B

Length : Determines how many bytes can be inserted in a single frame. The maximum size is 1500 bytes. To make it easier to distinguish valid frames from garbage, 802.3 states that valid frames must be at least 64 bytes long, from destination address to CRC.

The maximum length of a frame is 1500 bytes and minimum length is 64 bytes. If we subtract the MAC layer header 18 bytes (dest address+source address+length+CRC) from minimum length, then the data from the upper layer is 46 bytes. If the upper layer data is less than 46 bytes then required number of random bits are padded to make up a frame.

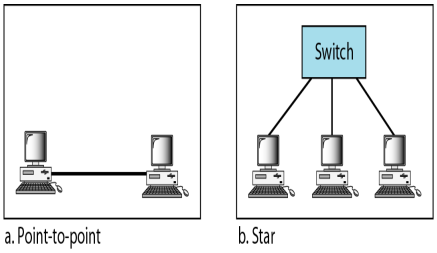
CRC: contains error detection information and is used to find damaged frames. CRC-32 algorithm is used to generate this 32 bit code.

Access Method: It is 1-persistent CSMA/CD LAN. According to the scheme, when a station wants to transmit it listens to the channel. If the channel is busy, the station waits until it goes idle; otherwise it transmits immediately. If two or more station simultaneously begin transmitting on an idle channel, they will collide each other. All collided stations terminate their transmissions and wait a random time.

Physical Layer: The physical layer in fast Ethernet is more complicated than the one in standard Ethernet

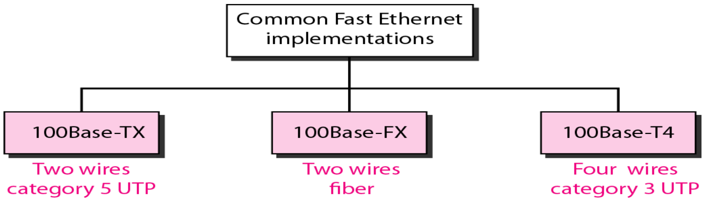
Topology

It is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center.



a. Point-to-point b. Star

Implementation: Fast Ethernet implementation at physical layer can be categorized as either two-wire or four-wire. The two wire implementation can be either category 5 UTP(100Base-TX) or fibre-optic cable (100BASE-FX). The four wire implementation is designed only for category 3 UTP(100Base-T4)



Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

Gigabit Ethernet:

The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000Mbps). The IEEE committee assigned the standard as 802.3z.

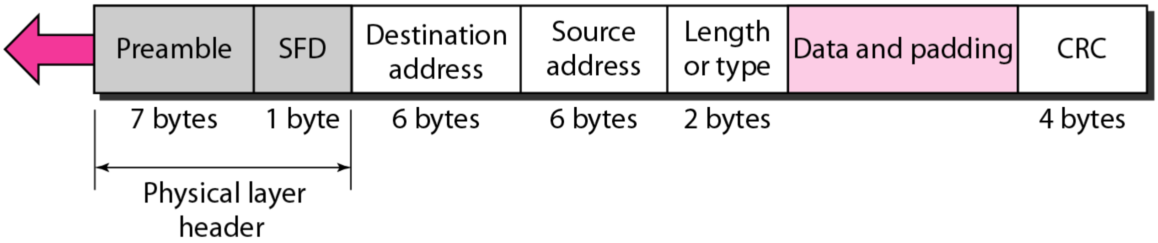
Features:

1. Upgrade the data rate to 1Gbps
2. Make it compatible with standard or fast Ethernet
3. Use the same 48 bit address
4. Use the same frame format
5. Keep the same minimum and maximum frame lengths

Mac Sublayer:

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Preamble: Each frame starts with this field. Length of this field is 7 bytes, each byte contains the bit pattern 10101010. It alerts the receiving device to synchronize its time clock with the source.

Start Frame Delimiter: Length of this field is 1 byte which contains 10101011 to denote the start of the frame. The SFD warns the station that this is the last chance to synchronize. The last two bits are 11 and alerts the receiver that the next field is destination address.

Source and Destination Address: Represents the 6 byte MAC address of source and destination stations. Each station on an Ethernet has its own network interface card(NIC). The NIC fits inside the station and provides the station with a 6 byte physical address. It is written in hexadecimal colon notation.

Ex: 06:01:2A:4C:F0:3B

Length : Determines how many bytes can be inserted in a single frame. The maximum size is 1500 bytes. To make it easier to distinguish valid frames from garbage, 802.3 states that valid frames must be at least 64 bytes long, from destination address to CRC.

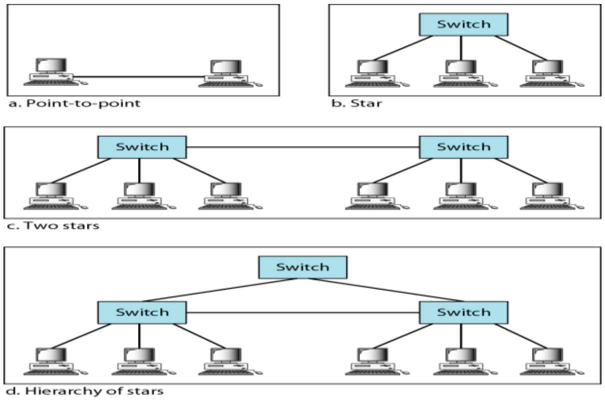
The maximum length of a frame is 1500 bytes and minimum length is 64 bytes. If we subtract the MAC layer header 18 bytes (dest address+source address+length+CRC) from minimum length, then the data from the upper layer is 46 bytes. If the upper layer data is less than 46 bytes then required number of random bits are padded to make up a frame.

CRC: contains error detection information and is used to find damaged frames. CRC-32 algorithm is used to generate this 32 bit code.

Access Method: It is 1-persistent CSMA/CD LAN. According to the scheme, when a station wants to transmit it listens to the channel. If the channel is busy, the station waits until it goes idle; otherwise it transmits immediately. If two or more station simultaneously begin transmitting on an idle channel, they will collide each other. All collided stations terminate their transmissions and wait a random time.

Physical Layer:

Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. Another possible configuration is to connect several star topologies or let a star topology be part of another.



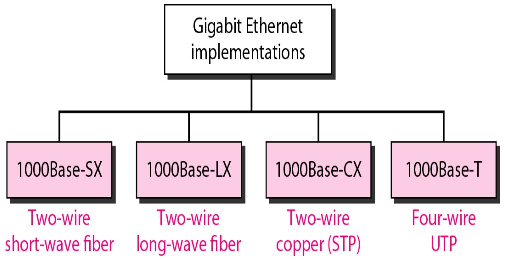
a. Point-to-point

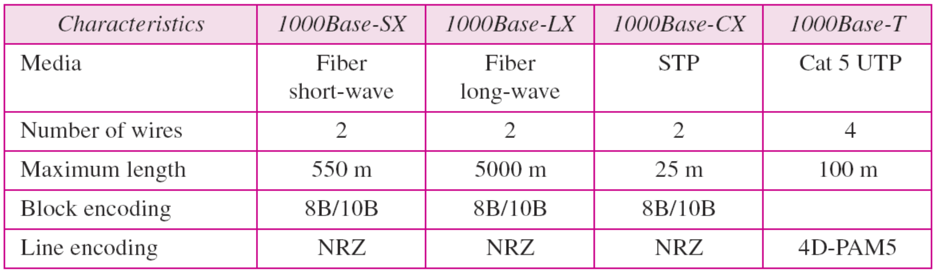
b. Star

c. Two stars

d. Hierarchy of stars

Implementation: Gigabit Ethernet can be categorized as either two wire or four wire implementation. The two wire implementations use fiber optic cable (1000Base-SX short wave, or 1000Base-Lx,Long wave) or STP(1000Base-CX). The four wire version uses category 5 twisted pair cable (1000Base-T).





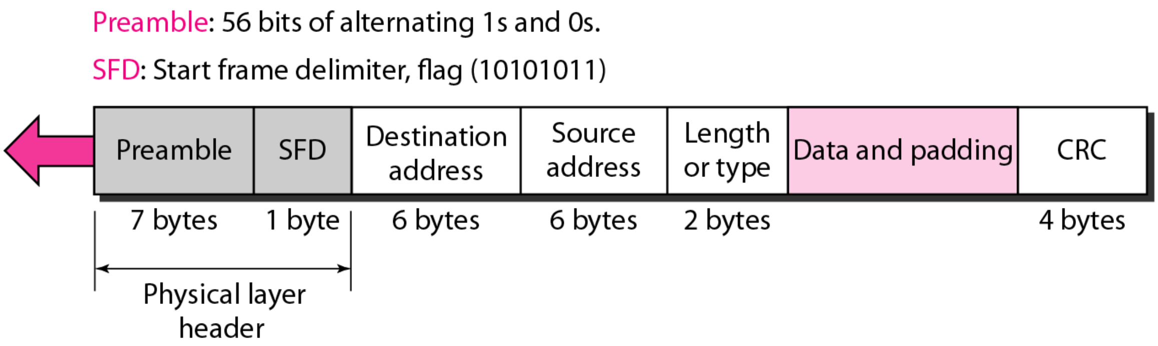
Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Ten-Gigabit Ethernet: The IEEE committee create Ten-Gigabit Ethernet and called it standard 802.3ae

Features:

1. Upgrade the data rate to 10Gbps
2. Make it compatible with standard, fast and Gigabit Ethernet
3. Use the same 48 bit address
4. Use the same frame format
5. Keep the same minimum and maximum frame lengths
6. Allow the interconnection of existing LANs into a MAN or a WAN
7. Make Ethernet compatible with technologies such as Frame Relay and ATM

Mac Sub Layer: Ten Gigabit Ethernet operates only in full duplex, mode which means there is no need for contention. CSMA/Cd is not used on Ten-Gigabit Ethernet.


Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)

Preamble: Each frame starts with this field. Length of this field is 7 bytes, each byte contains the bit pattern 10101010. It alerts the receiving device to synchronize its time clock with the source.

Start Frame Delimiter: Length of this field is 1 byte which contains 10101011 to denote the start of the frame. The SFD warns the station that this is the last chance to synchronize. The last two bits are 11 and alerts the receiver that the next field is destination address.

Source and Destination Address: Represents the 6 byte MAC address of source and destination stations. Each station on an Ethernet has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6 byte physical address. It is written in hexadecimal colon notation.

Ex: 06:01:2A:4C:F0:3B

Length: Determines how many bytes can be inserted in a single frame. The maximum size is 1500 bytes. To make it easier to distinguish valid frames from garbage, 802.3 states that valid frames must be at least 64 bytes long, from destination address to CRC.

The maximum length of a frame is 1500 bytes and minimum length is 64 bytes. If we subtract the MAC layer header 18 bytes (destination address +source address + length + CRC) from minimum length, then the data from the upper layer is 46 bytes. If the upper layer data is less than 46 bytes then required number of random bits are padded to make up a frame.

CRC: contains error detection information and is used to find damaged frames. CRC-32 algorithm is used to generate this 32 bit code.

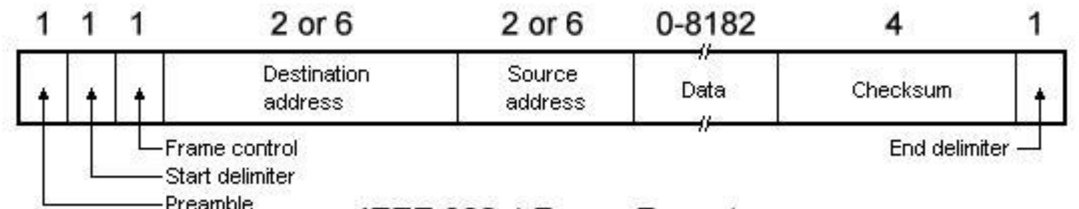
Physical Layer: The physical layer in Ten-Gigabit Ethernet is designed for using fibre optic cable over long distances. Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase-E.

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

IEEE Standard 802.4 Token Bus:

802.3 was widely used in small offices. The companies who are interested in factory automation and large organizations prefer this standard. In this system, the nodes are physically connected as a bus, but logically form a ring with tokens passed around to determine the turns for sending. It has the robustness of the 802.3 broadcast cable and the known worst case behavior of a ring. The structure of a token bus network is as follows:

Frame Structure:



IEEE 802.4 Frame Format

A 802.4 frame has the following fields:

Preamble: The Preamble is for synchronizing the receiver's clock. **Starting Delimiter (SD) and End Delimiter (ED)**: The SD and ED fields are used to mark frame boundaries. Both contain analog encoding of symbols other than 1 or 0 so that they cannot occur accidentally in the user data. Lengthy field is no more needed. **Frame Control (FC)**: FC is used to distinguish data frames from control frames. Data frames carries the frame's priority as well as a bit which the destination can set as an acknowledgement. For control frames, the Frame Control field is used to specify the frame type. Token passing and various ring maintenance frames are the allowed frame types.
Destination and Source Address: The Destination and Source address fields may be of 2 bytes (for a local address) or 6 bytes (for a global address).

Data: This is the actual data and it is of 8182 bytes when 2 byte addresses are used and 8174 bytes for 6 byte addresses.

Checksum: A 4-byte checksum of the data for error detection

Token bus or 802.4 is more robust and reliable than 802.3 frames. The standard 802.4 is a linear or tree shaped cable onto which the stations are attached. Network is a physical bus but a logical ring. The stations are numbered and are allowed to access the medium sequentially. If there are n stations, and packet transmission time is bounded to T, then the maximum waiting time is nXT. Token bus MAC is simple and robust. Token bus is mostly used in automation systems.

Data is subdivided into four priority classes. Each station has four packet queues, one for each priority. When a station receives token, it is allowed to transmit certain fixed time. During that time it transmits packets in the decreasing order of priorities.

Ring Maintenance:

The various control frames used for ring maintenance are shown below:

Frame Control Field	Name	Meaning
00000000	Claim_token	Claim token during ring maintenance
00000001	Solicit_successor_1	Allow stations to enter the ring
00000010	Solicit_successor_2	Allow stations to enter the ring
00000011	Who_follows	Recover from lost token
00000100	Resolve_contention	Used when multiple stations want to enter
00001000	Token	Pass the token
00001100	Set_successor	Allow the stations leave the ring

Whenever the first node on the token bus comes up, it sends a **Claim_token** packet to initialize the ring. If more than one station send this packet at the same time, there is a collision. Collision is resolved by a contention mechanism.

Once the ring is set up, new nodes which are powered up may wish to join the ring. For this a node sends **Solicit_successor_1** packets from time to time, inviting bids from new nodes to join the ring. This packet contains the address of the current node and its current successor, and asks for nodes in between these two addresses to reply. If more than one nodes respond, there will be collision. The node then sends a **Resolve_contention** packet, and the contention is resolved using a similar mechanism as described previously. Thus at a time only one node gets to enter the ring. The last node in the ring will send a **Solicit_successor_2** packet containing the addresses of it and its successor. This packet asks nodes not having addresses in between these two addresses to respond.

There may be problems in the logical ring due to sudden failure of a node. What happens if a node goes down along with the token? After passing the token, a node, say node A, listens to the channel to see if its successor either transmits the token or passes a frame. If neither happens, it resends a **token**. Still if nothing happens, A sends a Who_follows packet, containing the address of the down node. The successor of the down node, say node C, will now respond with a Set_successor packet, containing its own address. This causes A to set its successor node to C, and the logical ring is restored. However, if two successive nodes go down suddenly, the ring will be dead and will have to be built afresh, starting from a Claim_token packet.

When a node wants to shutdown normally, it sends a Set_successor packet to its predecessor, naming its own successor. The ring then continues unbroken, and the node goes out of the ring.

IEEE 802.5: Token Ring Network

Token Ring is formed by the nodes connected in ring format. The principle used in the token ring network is that a token is circulating in the ring and whichever node grabs that token will have right to transmit the data. Whenever a station wants to transmit a frame it inverts a single bit of the 3-byte token which instantaneously changes it into a normal data packet. Because there is only one token, there can be at most one transmission at a time. Since the token rotates in the ring it is guaranteed that every node gets the token with in some specified time. So there is an upper bound on the time of waiting to grab the token so that starvation is avoided. There is also an upper limit of 250 on the number of nodes in the network. To distinguish the normal data packets from token (control packet) a special sequence is assigned to the token packet. When any node gets the token it first sends the data it wants to send, then recirculates the token.

If a node transmits the token and nobody wants to send the data, the token comes back to the sender. If the first bit of the token reaches the sender before the transmission of the last bit, then error situation arises. So to avoid this we should have: propagation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time

A station may hold the token for the token-holding time. Which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well. After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring.

If a node transmits the token and nobody wants to send the data the token comes back to the sender. If the first bit of the token reaches the sender before the transmission of the last bit, then error situation arises. So to avoid this we should have: propagation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time

A station may hold the token for the token-holding time. which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well. After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring.

Modes of Operation

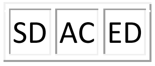
Listen Mode: In this mode the node listens to the data and transmits the data to the next node. In this mode there is a one-bit delay associated with the transmission.

Transmit Mode: In this mode the node just discards the any data and puts the data onto the network.

By-pass Mode: The node reaches to this mode when the node is down. Any data is just bypassed. There is no one-bit delay in this mode. One problem with a ring network is that if the cable breaks somewhere, the ring dies. This problem is elegantly addressed by using a ring concentrator. A Token Ring concentrator simply changes the topology from a physical ring to a star wired ring. But the network still remains a ring logically. Physically, each station is connected to the ring concentrator (wire center) by a cable containing at least two twisted pairs, one for data to the station and one for data from the station. The Token still circulates around the network and is still controlled in the same manner, however, using a hub or a switch greatly improves reliability because the hub can automatically bypass any ports that are disconnect0ed or have a cabling fault. This is done by having bypass relays inside the concentrator that are energized by current from the stations. If the ring breaks or station goes down, loss of the drive current will release the relay and bypass the station. The ring can then continue operation with the bad segment bypassed.

Token Format

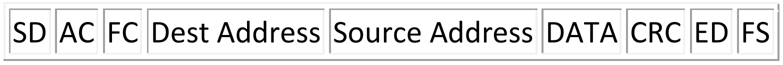
The token is the shortest frame transmitted (24 bit). MSB (Most Significant Bit) is always transmitted first - as opposed to Ethernet



SD	AC	ED

SD = Starting Delimiter (1 Octet)
AC = Access Control (1 Octet)

ED = Ending Delimiter (1 Octet)
Frame Format:



1	**1**	**1**	**2or6**	**2or6**	**no limit**	**4**	**1**	**1**
SD	AC	FC	Dest Address	Source Address	DATA	CRC	ED	FS

SD=Starting Delimiter (1 octet)
ED = Ending Delimiter (1 Octet)
AC=Access Control (1 octet)
FC = Frame Control (1 Octet)
DA = Destination Address (2 or 6 Octets)
SA = Source Address (2 or 6 Octets)
DATA = Information 0 or more octets up to 4027
CRC = Checksum (4 Octets)
FS=Frame Status

When a station with a Frame to transmit detects a token which has a priority equal to or less than the Frame to be transmitted, it may change the token to a start-of-frame sequence and transmit the Frame.

Bits Priority Bits indicate tokens priority, and therefore, which stations are allowed to use it. Station can transmit if its priority as at least as high as that of the token.

The monitor bit is used to prevent a token whose priority is greater than 0 or any frame from continuously circulating on the ring. if an active monitor detects a frame or a high priority token with the monitor bit equal to 1, the frame or token is aborted. This bit shall be transmitted as 0 in all frame and tokens. The active monitor inspects and modifies this bit. All other stations shall repeat this bit as received.

R = Reserved bits the reserved bits allow station with high priority Frames to request that the next token be issued at the requested priority. The description is similar to as above.

Data Format:

No upper limit on amount of data as such, but it is limited by the token holding time.
Checksum:

The source computes and sets this value. Destination too calculates this value. If the two are different, it indicates an error, otherwise the data may be correct.
Frame Status: It contains the A and C bits. A bit set to 1: destination recognized the packet. C bit set to 1: destination accepted the packet.

Ring Maintenance

Each token ring has a monitor that oversees the ring. Among the monitor's responsibilities are seeing that the token is not lost, taking action when the ring breaks, cleaning the ring when garbled frames appear and watching out for orphan frames. An orphan frame occurs when a station transmits a short frame in it's entirety onto a long ring and then crashes or is powered down before the frame can be removed. If nothing is done, the frame circulates indefinitely.

Detection of orphan frames: The monitor detects orphan frames by setting the monitor bit in the Access Control byte whenever it passes through. If an incoming frame has this bit set, something is wrong since the same frame has passed the monitor twice. Evidently it was not removed by the source, so the monitor drains it.

Lost Tokens: The monitor has a timer that is set to the longest possible tokenless interval : when each node transmits for the full token holding time. If this timer goes off, the monitor drains the ring and issues a fresh token.

Garbled frames: The monitor can detect such frames by their invalid format or checksum, drain the ring and issue a fresh token.

The token ring control frames for maintenance are:

Control field	Name	Meaning
00000000	Duplicate address test	Test if two stations have the same address
00000001	Express Buffer	Verifies the buffer
00000010	Beacon	Used to locate breaks in the ring
00000011	Claim token	Attempt to become monitor
00000100	Purge	Reinitialize the ring
00000101	Active monitor present	Issued periodically by the monitor
00000110	Standby monitor present	Announces the presence of potential monitors

The monitor periodically issues a message "Active Monitor Present" informing all nodes of its presence. When this message is not received for a specific time interval, the nodes detect a monitor failure. Each node that believes it can function as a monitor broadcasts a "Standby Monitor Present" message at regular intervals, indicating that it is ready to take on the monitor's job. Any node that detects failure of a monitor issues a "Claim" token. There are 3 possible outcomes:

If the issuing node gets back its own claim token, then it becomes the monitor.
If a packet different from a claim token is received, apparently a wrong guess of monitor

failure was made. In this case on receipt of our own claim token, we discard it. Note that our claim token may have been removed by some other node which has detected this error.
If some other node has also issued a claim token, then the node with the larger address becomes the monitor.

In order to resolve errors of duplicate addresses, whenever a node comes up it sends a "Duplicate Address Detection" message (with the destination = source) across the network. If the address recognize bit has been set on receipt of the message, the issuing node realizes a duplicate address and goes to standby mode. A node informs other nodes of removal of a packet from the ring through a "Purge" message. One maintenance function that the monitor cannot handle is locating breaks in the ring. If there is no activity detected in the ring (e.g. Failure of monitor to issue the Active Monitor Present token.) , the usual procedures of sending a claim token are followed. If the claim token itself is not received besides packets of any other kind, the node then sends "Beacons" at regular intervals until a message is received indicating that the broken ring has been repaired.

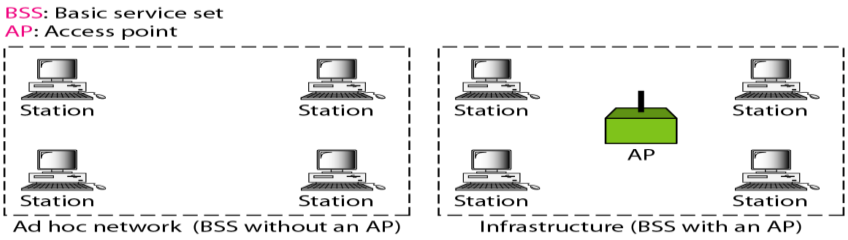
WIRELESS LANS

Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of any wires is increasing everywhere. Wireless LANs can be found in college campuses, office buildings, and in many public areas.

IEEE 802.11

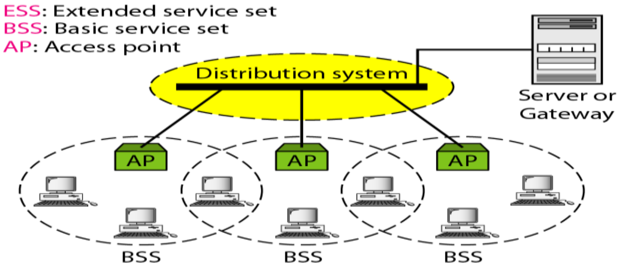
The standard defines two kinds of services: the basic service set(BSS) and extended service set (ESS).

Basic Service Set: IEEE 802.11 defines the basic service set as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station which is also known as the access point (AP).



The BSS without an AP is a stand alone network and cannot send data to other BSSs. It is called an ad-hoc architecture. In this architecture stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

Extended Service Set: An extended service set is made up of two or more BSSs with Aps. In this case the BSSs are connected through a distributed system which is usually a wired LAN.

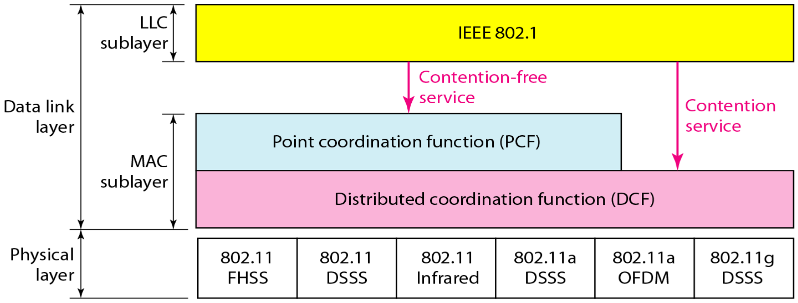


When BSSs are connected, the stations within reach of one anotehr can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs.

Station Types: 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS-transistion, ESS-transition. A station with no-transition is etiher stationary or moves only inside a BSS. A station with BSS-transition can move from one BSS to another BSS. A station with ESS-transition moves from ESS to another ESS.

MAC Sub Layer:

802.11defines two MAC sub layers: distributed coordination function(DCF), Point coordination function(PCF).

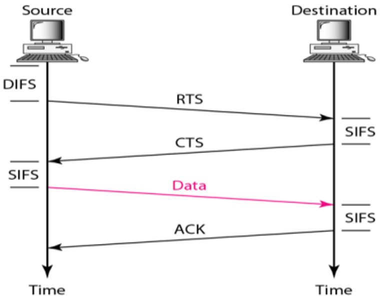


DCF: uses CSMA/CA as access method. Wireless LANs cannot implement CSMA/CD for three reasons.

1. For collision detection a station must be able to send data and receive collision signals at the same time. It is expensive and needs high bandwidth.
2. Collision may not be detected because of hidden terminal and exposed terminal problems.
3. The distance between stations can be great.

CSMA/CA:

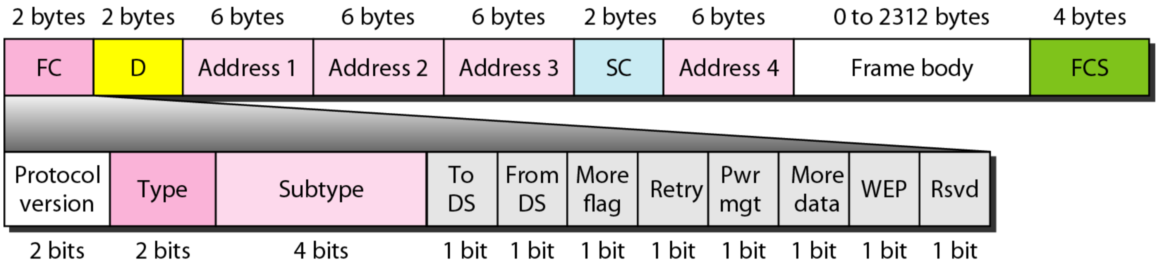
1. Before sending a frame, the source station senses the channel. Once a station finds the channel idle, station waits a period of time called the distributed inter frame space(DIFS); then it sends a control frame called request to send (RTS)
2. After receiving RTS, receiver waits for short inter frame space(SIFS) and sends a control frame called clear to send (CTS) to the sender. This control frame indicates that the receiver is ready to receive data.
3. The sender sends data after waiting a SIFS time
4. The receiver after waiting an SIFS, sends an ACK to show that the frame has been received.



PCF: This is an optional access method that can be implemented in an infrastructure network. It is implemented on the top of DCF and is used mostly for time sensitive transmission. PCF has a centralized, contention free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP

MAC Sub Layer:

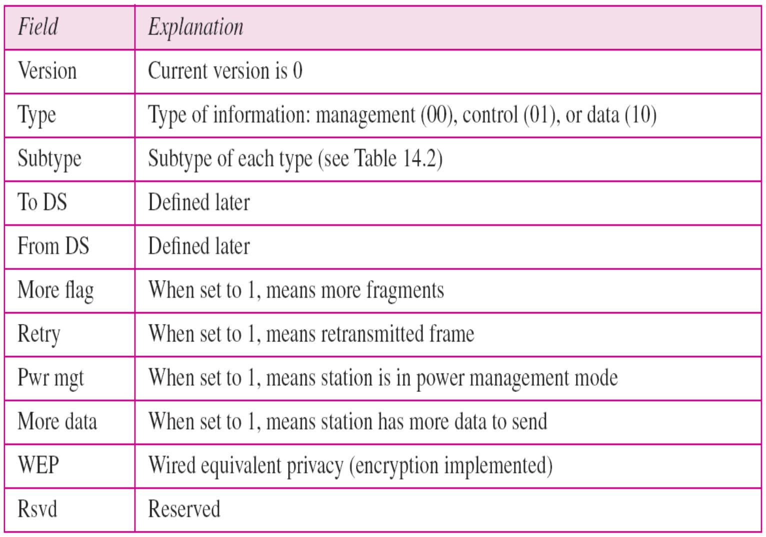
Frame Format:



2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	Frame body	FCS

Protocol version	Type	Subtype	To DS	From DS	More flag	Retry	Pwr mgt	More data	WEP	Rsvd
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

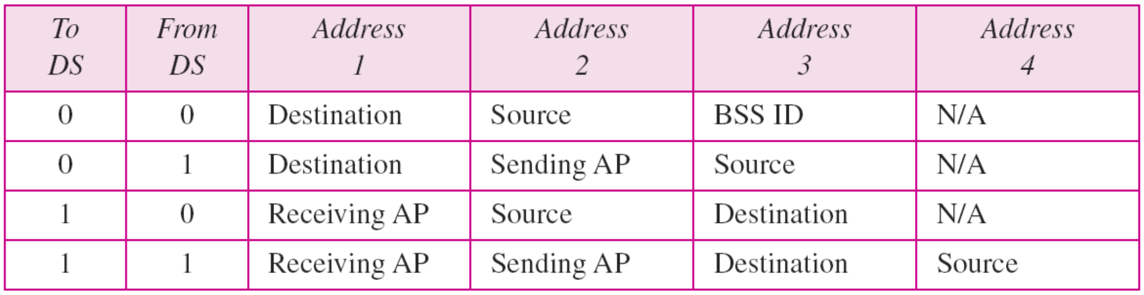
Frame Control(FC): The FC field is of length 2 bytes, and defines the type of frame and control information. These two bytes consits of following information:



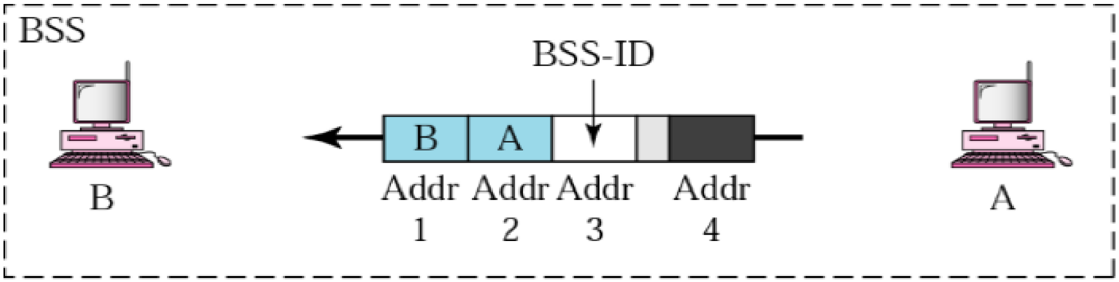
Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

D: In all frame types it defines the duration of transmission.But in control frames it contains the ID of the frame.

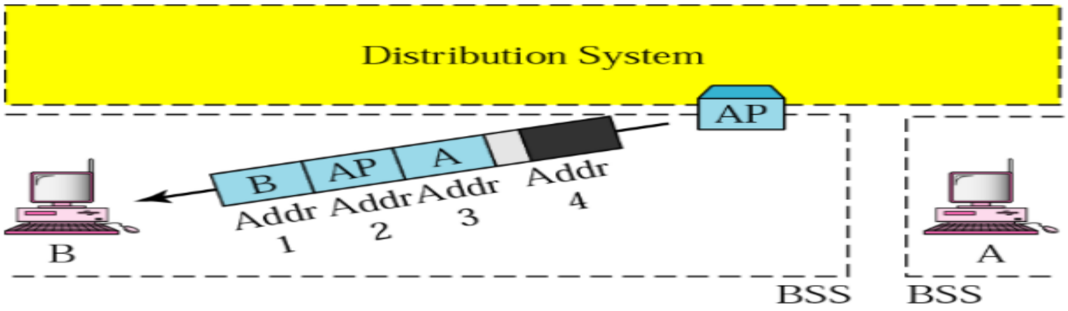
Addreses: There are four address fields, each is of length 6 bytes. The meaning of each address field depends on the value of the **To DS** and **From DS** fields.



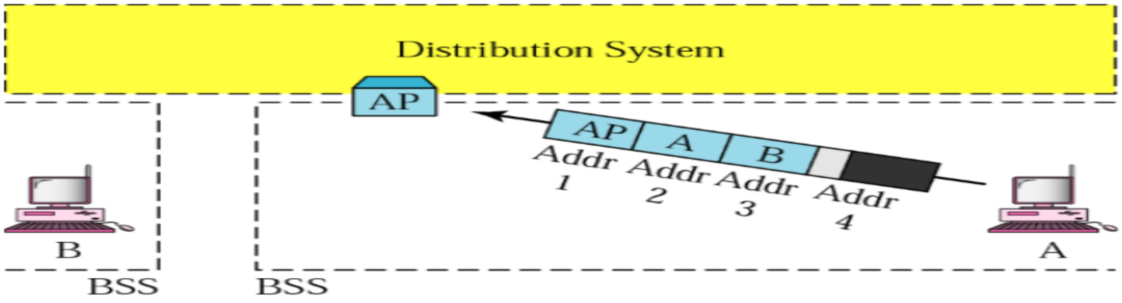
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source



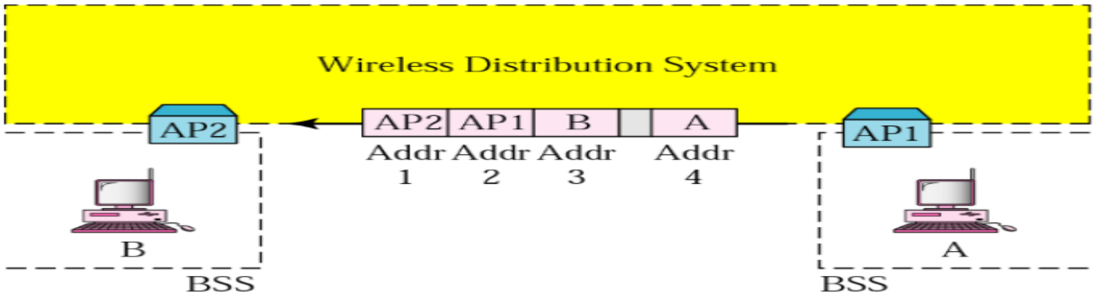
Frame is going directly from one client to another. No intervening distribution system. To DS = 0, From DS = 0



To DS = 0, From DS = 1 - frame is coming from a DS (Access Point)



To DS = 1, From DS = 0 - frame is going to a DS (or AP)



To DS = 1 and From DS = 1

Sequence Control: Defiens the sequence number of the frame to be used in flow control.

Frame body: The length is in between 0-2312 bytes.

FCS: It is oflength 4 bytes and contains CRC-32 error detection sequence.

Frame Types: There are three categories of frames, Management, Control and data frames.

Management frames: Used for the initial comunication between stations and access points.

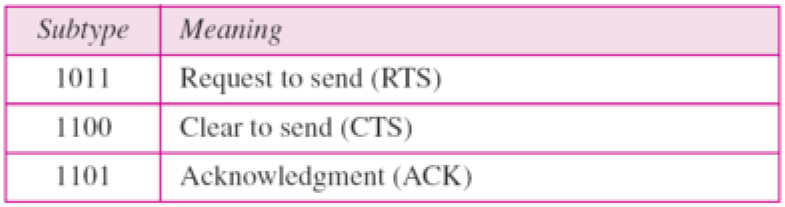
Control Frames: Used for accessing the channel and acknowledging frames

2 bytes	2 bytes	6 bytes	6 bytes	4 bytes
FC	D	Address 1	Address 2	FCS

RTS

2 bytes	2 bytes	6 bytes	4 bytes
FC	D	Address 1	FCS

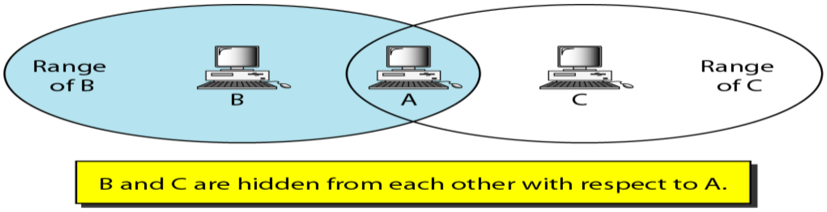
CTS or ACK



Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

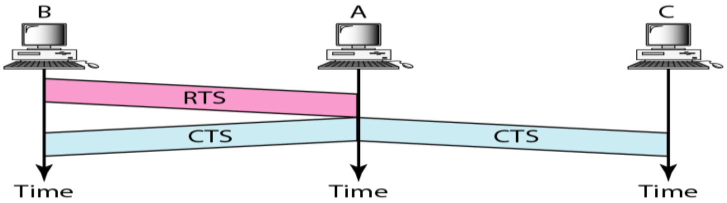
Hidden and Exposed Station Problem:

Hidden station Problem: Station B has a transmission range shown by the left oval; every station in this range can hear any signal transmitted by station B. Station C has a transmission range shown by the right oval; every station located in this range can hear any signal transmitted by C. Station C is outside the transmission range of B; similarly station B is outside the transmission range of C. Station A however is in the area converted by both B and C. It can hear any signal transmitted by B and C.

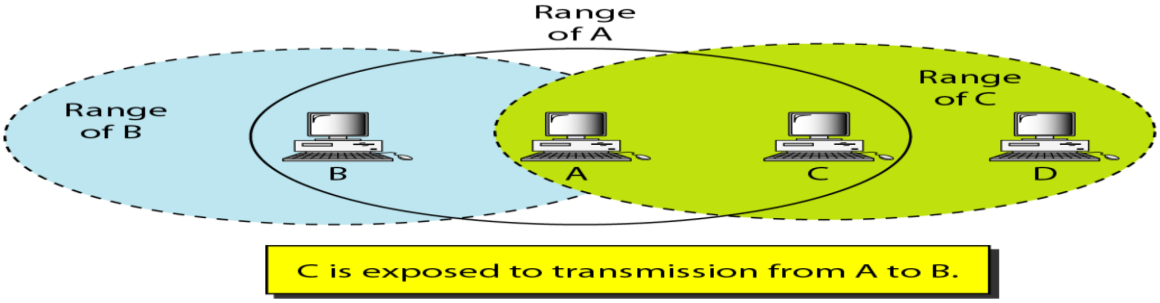


Assume that stastion B is sending data to station A. In the middle of this transmission, station C also has data to send station A. However station C is out of B's range and transmission from B can not reach C. Therefore C thinks the channel is free. Station C sends its data to A; which results a collision at A, because this station is receiving data from both B and c.Station B and C are hidden from each other with respect to A. Hidden stations can reduce the capacity of the network because of the possibility of collision,.

The solution to this problem is the use of hand shake frames (RTS,CTS). For example RTS message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS message which contains the duration of transmission from B to A reaches C. Station C knows some hidden sation is using the channel and refrains from transmitting until that duration is over.



Exposed Station Problem: This is the reverse of the hidden station problem. In this case a station refrains from using the channel when it is available. Assume that station A is transmitting to station B. Station C has some data to send to Station D, which can be sent without interferring with the transmission from A to B. However station C is exposed to transmission from A; it hears that A is sending and thus refrains from sending. It wastes the capacity of the channel.



The handshake messages RTS and CTS cannot held in this case.

Physical Layer:

All implementations, except the infrared, operate in the indusrial, scientific and medical(ISM) band, which defines three unlicensed bands.

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

BLUETOOTH:

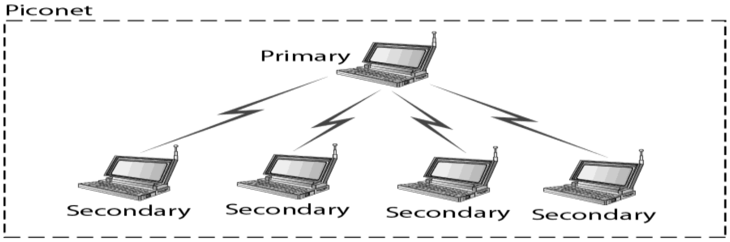
Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad-hoc network, which means that the network is formed spontaneously; the devices sometimes called gadgets. Bluetooth devices find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Herald Blataand, the king of Denmark who united Denmark and Norway. Blataand translates to Bluetooth in English.

Architecture:

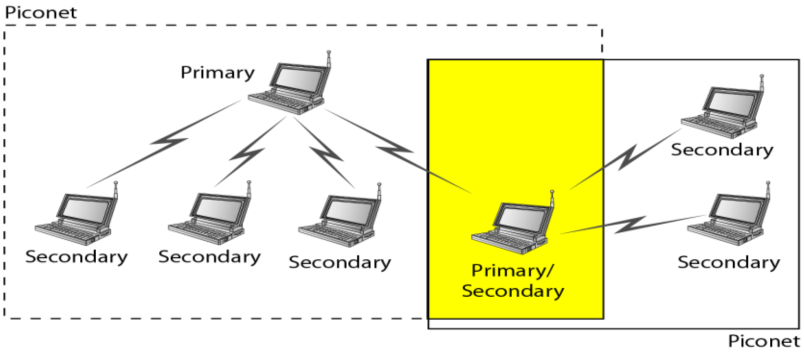
Bluetooth has two types of networks: Piconet and Scatternet

Piconet: A Bluetooth network is called a piconet or a small net. A piconet can have maximum 8 stations, one of which is called as primary and the rest are called secondaries. All the secondary stations synchronize their clocks with primary. The communication between primary and secondary can be one-to-one or one-to-many.



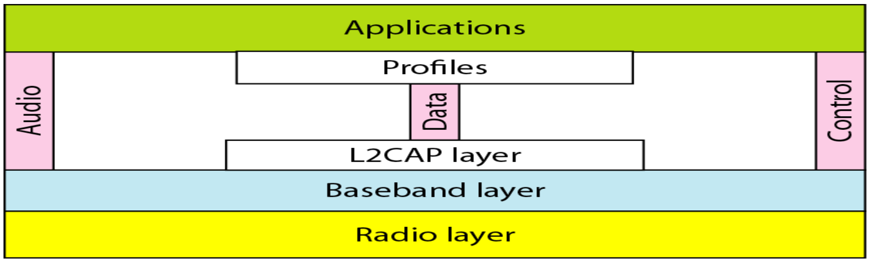
A piconet can have maximum 7 secondaries, and an additional 7 secondaries may be in the parked state. A secondary in a parked sate is synchronized with primary, but cannot take part in communication until it is moved from parked state.

Scatternet: Piconets can be combined to form a scatternet. A secondary station in one picoent can be the primary in another piconet. This station can receive messages from primary in the first piconet and forwards to second piconet stations.



Bluetooth Layers:

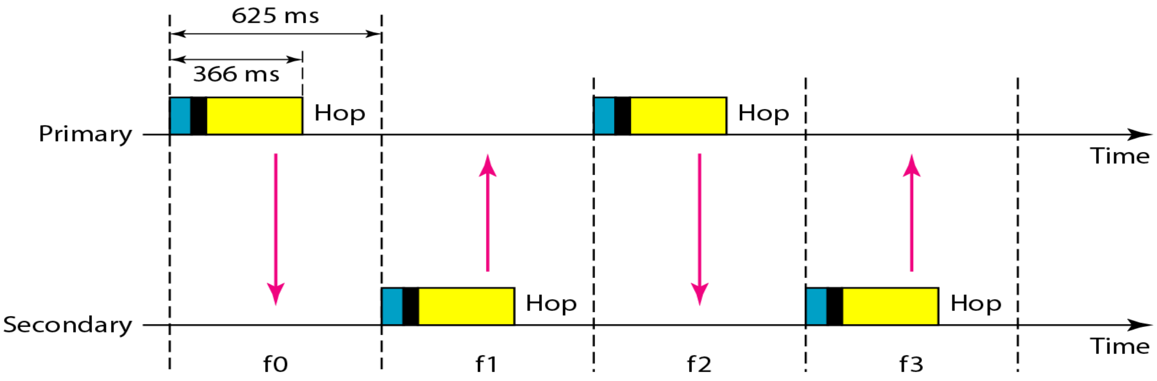
It uses several layers that do not exactly match those of the Internet mode.



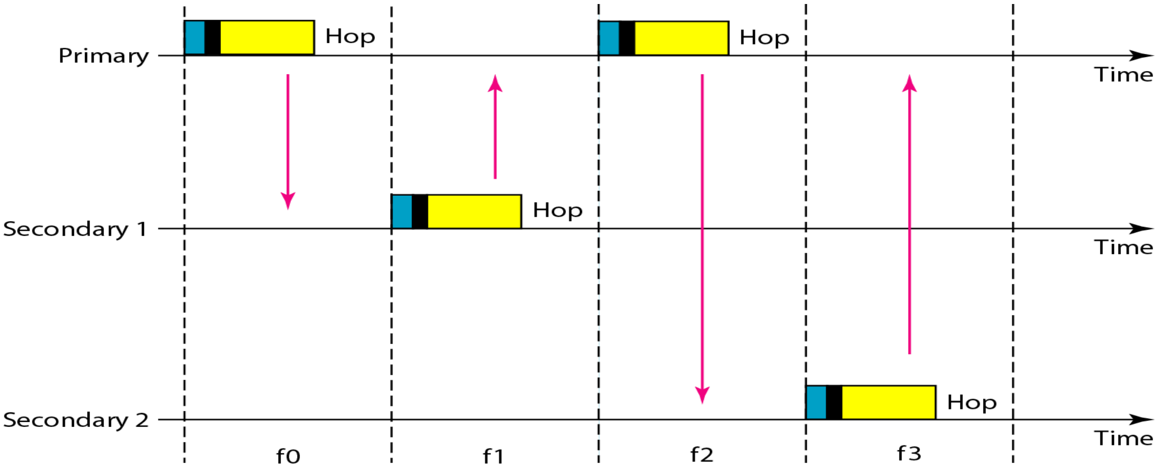
Radio Layer: Roughly equivalent to physical layer of the Internet model. Bluetooth devices are low power and have a range of 10m. it uses 2.4 GHz ISM band divided into 79 channels of 1MHz each. It uses Frequency Hopping Spread Spectrum in Radio layer to avoid interferences from other devices or networks.

Baseband Layer: It is roughly equivalent to MAC sub layer. The access method is TDMA. The primary and secondary communicate each other in time slots. The length of a time slot is 625 µs. There are two types of communication in MAC layer:

Single-Secondary Communication: if the piconet has only one secondary, the TDMA operation is very simple. The time is divided into time slots of 625 µs. the primary uses even numbered slots(0,2,4,6,8…), and the secondary uses odd-numbered slots(1,3,5,…)

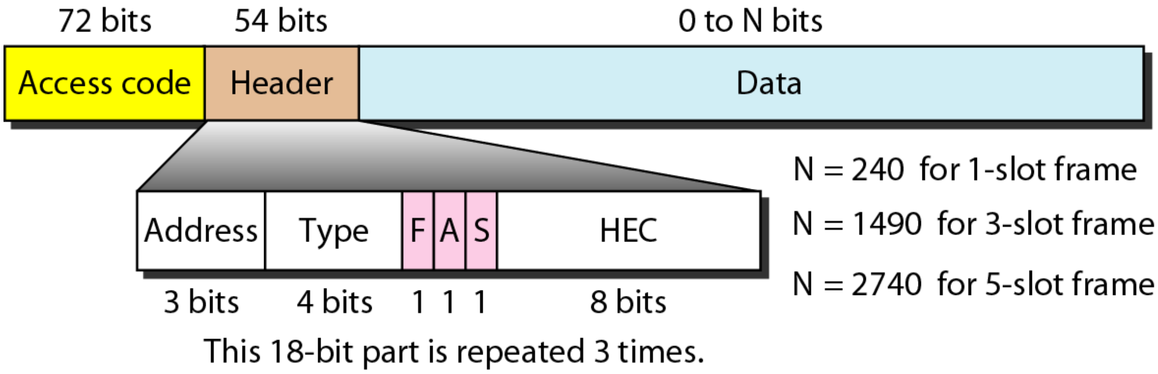


Mutilple-Secondary Communication: If there is more than one secondary in the piconet, the primary uses all even numbered slots but a secondary sends in the next odd numbered slot if it receives a packet in the previous slot. All secondaries listen on even numbered slots but only one secondary sends in any odd numbered slot.



Frame Format: A frame in the baseband layer can be one of three types: one-slot, three-slot, or five-slot. A one slot is equal to 625 µs. in a one slot frame exchange, 259 µs is required for hopping and control mechanisms. Means a one slot frame can last only 625-259=366 µs.

A three slot frame occupies three slots, and the length of frame is 3x625-259=1616 µs or 1616 bits. A five slot frame has 5x625-259=2866 µs or bits.



Access Code: This 72 bit field contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.

Header: This 54-bit field is a repeated 18-bit pattern. Each pattern has the following information

Address: This 3-bit field can define up to seven secondaries. If the address is 0 then it is considered as broadcaster or primary to communicate with all secondaries.

Type: The 4-bit type indicates the type of data coming from the upper layers.

F: 1-bit field is used for Flow Control. When it is set to 1, indicates that the device is unable to receive more frames (buffer is full)

A: This I bit field indicates acknowledgement. Bluetooth uses stop and wait ARQ. 1 bit is sufficient for acknowledgement.

S: This 1 bit field is a sequence number.

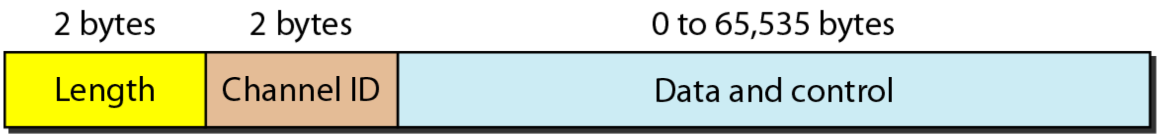
HEC: This 8 bit field is used for error detection.

The header has 3 identical 18 bit sections. The receiver compares these three sections bit by bit. If each of the corresponding bit is same, the bit is accepted; If not the majority opinion rules out. This is a form of forward error detection.

Payload: This of length 0 to 2740 bits. It contains data or control information coming from the upper layers.

L2CAP :

The Logical Link Control and Adaptation Protocol is roughly equivalent to LLC sub layer in LANs. It is sued for data exchange on asynchronous connection less channels. Synchronous connection oriented channels do not use L2CAP.



The 16 bit length field defines the size of data in bytes coming from the upper layers. The channel ID (CID) defines a unique identifier for the virtual channel created at this level. L2CAP provides multiplexing, segmentation and reassembly, quality of service and group management.