UNIT – 4

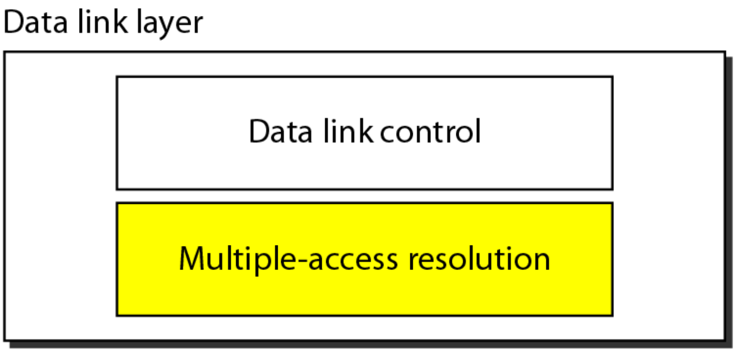
MULTIPLE ACCESS

4.1 Medium Access Control:

It defines which device has control over communication path when two (or) more devices connected to a link at a time.

Data Link Layer provides **Access Control** to avoid conflicts between stations. In that context, data link layer is divided into two sub layers:

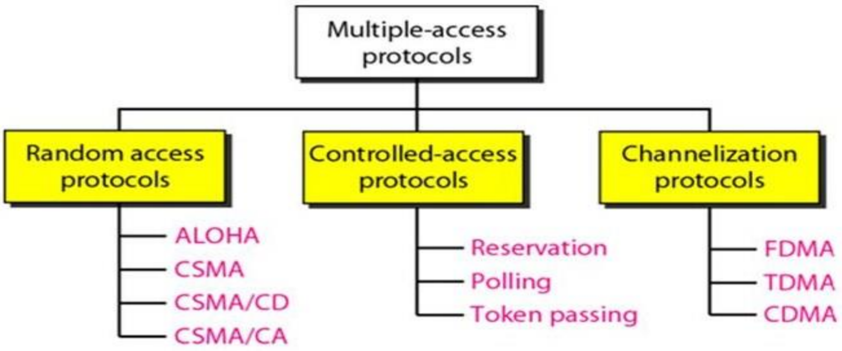
1. Data Link Control
2. Multiple Access Control



The **upper sub layer**, Data Link Control provides both flow and error control. It is called Logical Link control.

The **lower sub layer**, Multiple Access Control provides **access control** especially if devices are connected as Multipoint. It is called Media Access Control.

4.2 Taxonomy of Multiple Access Protocols:



Medium access protocols are divided into three broad categories as Random access, Controlled access, and Channelization Protocols. Each category of protocols follows different mechanisms to provide channel to a device at a time to minimize collisions among data.

4.3 Random Access:

In random access method, any station that has a data to send can access medium randomly. Random access is especially occurred in **Multipoint transmission mode**.

Two features give this method its name:

1. There is no scheduled time for a station to transmit i.e. Transmission is random among the stations.
2. There are no rules to specify which station should send next. Stations compete with one another to access the medium.

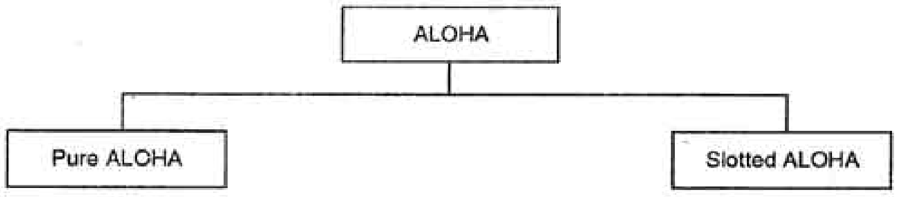
However, if more than one station tries to send, there is an access **conflict-collision**-and the frames will be either destroyed or modified. I.e. collision is occurred, so that station again needs to resend the sent frame.

To **overcome collision** in a shared medium random access uses different protocols

1. ALOHA
2. CSMA (Carrier Sense Multiple Access)
3. CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
4. CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

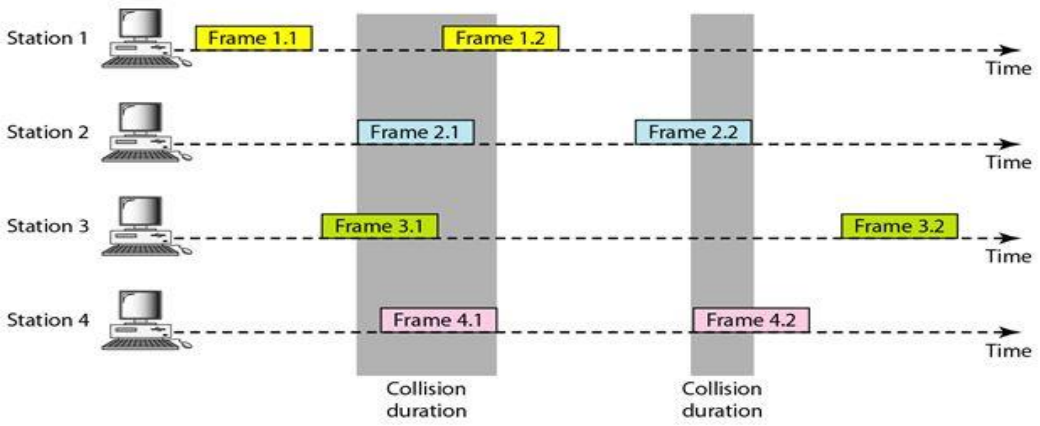
4.3.1 ALOHA

It provides a simple mechanism called Multiple Access (**MA**) to control collisions on a communication link.

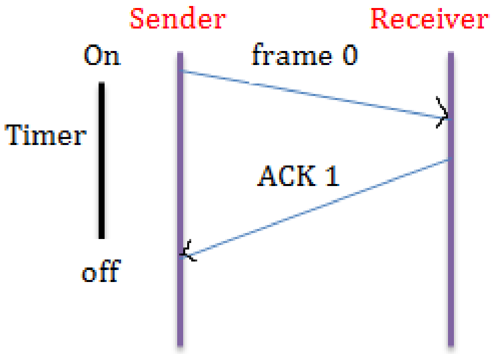


4.3.1.1 Pure ALOHA

- The **original ALOHA** protocol is called Pure ALOHA. This is a simple, but elegant protocol.
- The idea is that Pure ALOHA uses a **random amount of time** to send frame for each station whenever it has a frame to send.
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations.



- The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a **time-out period,** the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.



$$\boxed{\text{Time-out period} = 2 * \mathbf{T_p}}$$

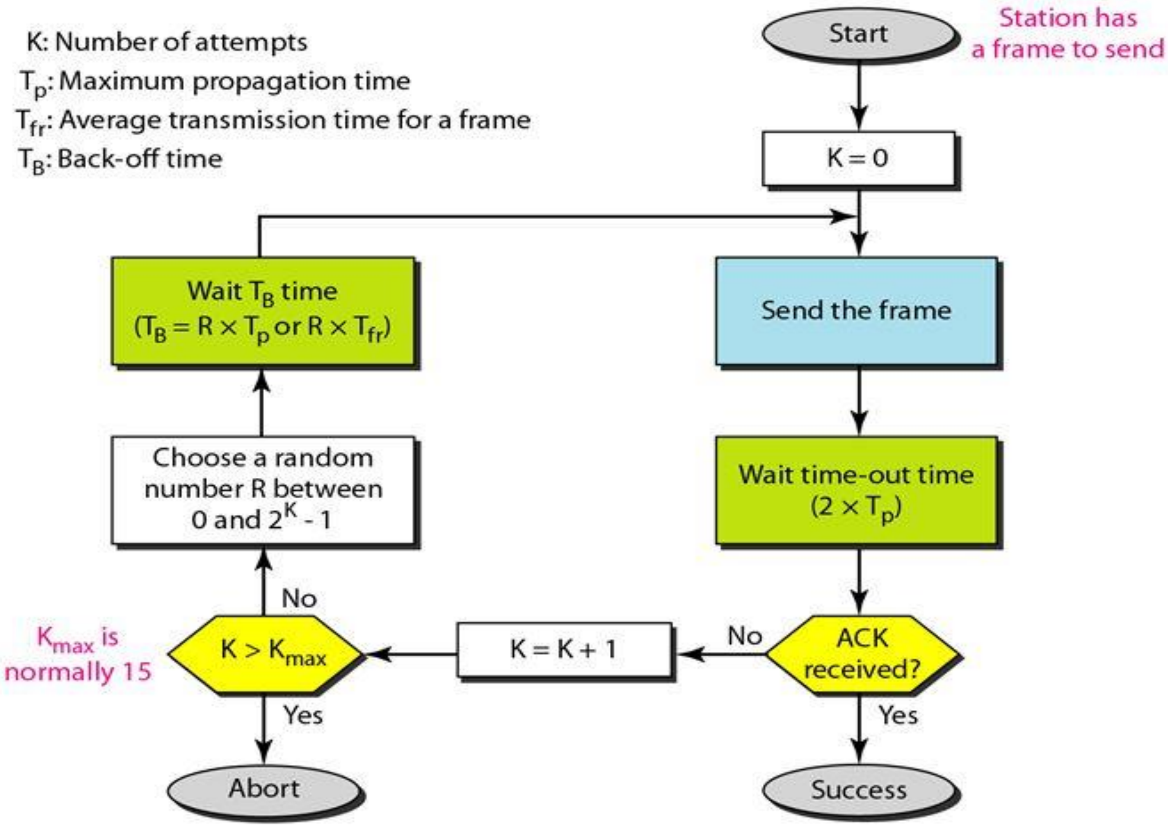
Where $\mathbf{T_p}$, is **Propagation time**, the time taken to transmit single bit from one station to other station

- If two or more stations tries to transmit at a time, a collision occurs. In those cases, the stations effected with collisions will wait for random time and starts resend their frames. The randomness will help avoid more collisions. This random time is called **Back-off time (T_B).** This procedure continues until the frame is successfully transmitted to the destination.
- Back-off time is different for any two stations to avoid collision between resending frames.
- To avoid congesting the channel with retransmission frames, A station must give up after a maximum number of retransmission attempts **K_{max}.**

Algorithm:

1. Send a frame
2. Check Time-out
   - ACK Received (**Success**), Continue for next frame.
   - ACK not received (**Failure**), Go to Step 3.
3. Wait for back-off time to resend a frame

Flow chart for pure ALOHA protocol:


K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Start
Station has a frame to send
K = 0
Send the frame
Wait time-out time ($2 \times T_p$)
ACK received?
Yes
Success
No
K = K + 1
$K > K_{max}$
K_{max} is normally 15
Yes
Abort
No
Choose a random number R between 0 and $2^K - 1$
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)

Maximum Propagation Time (T_P):

If we consider to calculate back – off time (**T_B**), as

$$\boxed{T_B = R * T_P}$$

Here ‘R’ a random value that can be chosen from **0 to 2^k - 1**

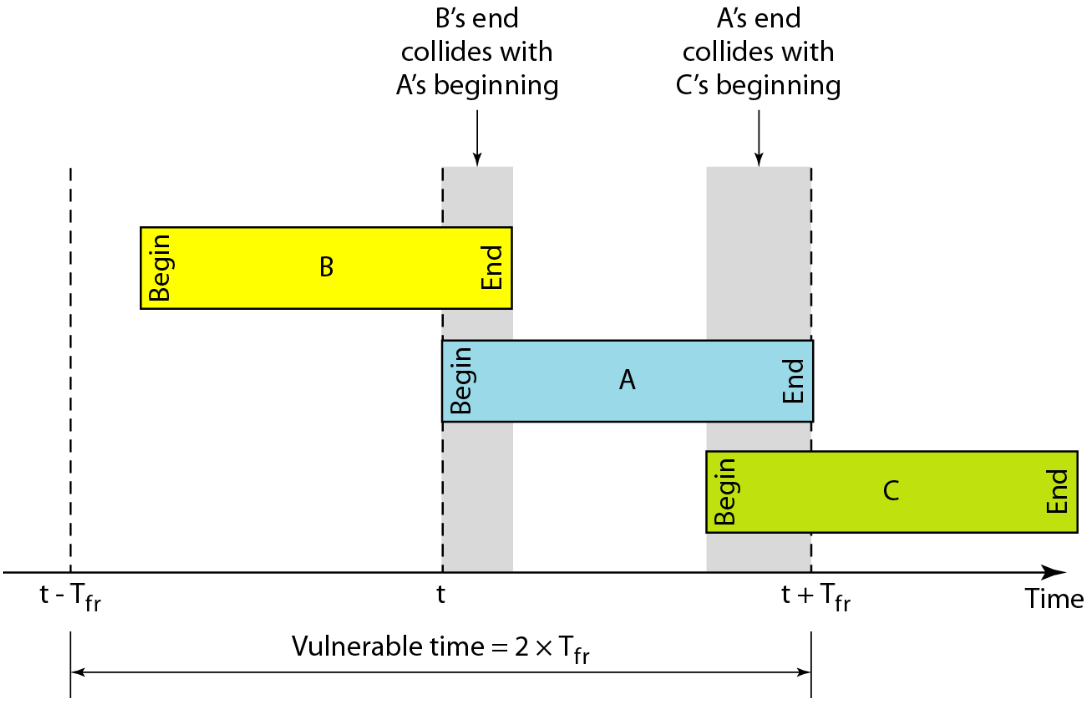
Average Frame Transmission time (T_{fr}):

Time taken to send an entire frame **T_{fr}.** It can be calculated as,

$$\boxed{T_B = R * T_{fr}}$$

Vulnerable Time:

If a station uses average frame transmission time to calculate back-off time then each station must $\boxed{2 * T_{fr}}$ time to send a frame. When a station starts its transmission if any other station tries to send the frames with in thi $\boxed{2 * T_{fr}}$ time then there is a collision is happened between two stations. The collision occurring time is called Vulnerable time.


B’s end collides with A’s beginning
A’s end collides with C’s beginning
Begin
B
End
Begin
A
End
Begin
C
End
t - T_{fr}
t
t + T_{fr}
Time
Vulnerable time = 2 × T_{fr}

Throughput:

Throughput of pure ALOHA is $\boxed{S = G * e^{-2G}}$

Where **S =** Successful transmission of frames on average

G = Generation of frames during frame transmission time

For example, G = 1/2 (i.e. frame sent for 2 milli-seconds)

$S = 1/2 \times e^{-2 * 1/2}$

$S = 1/2 \times e^{-1}$

$S = 1/2 \times 0.3678$

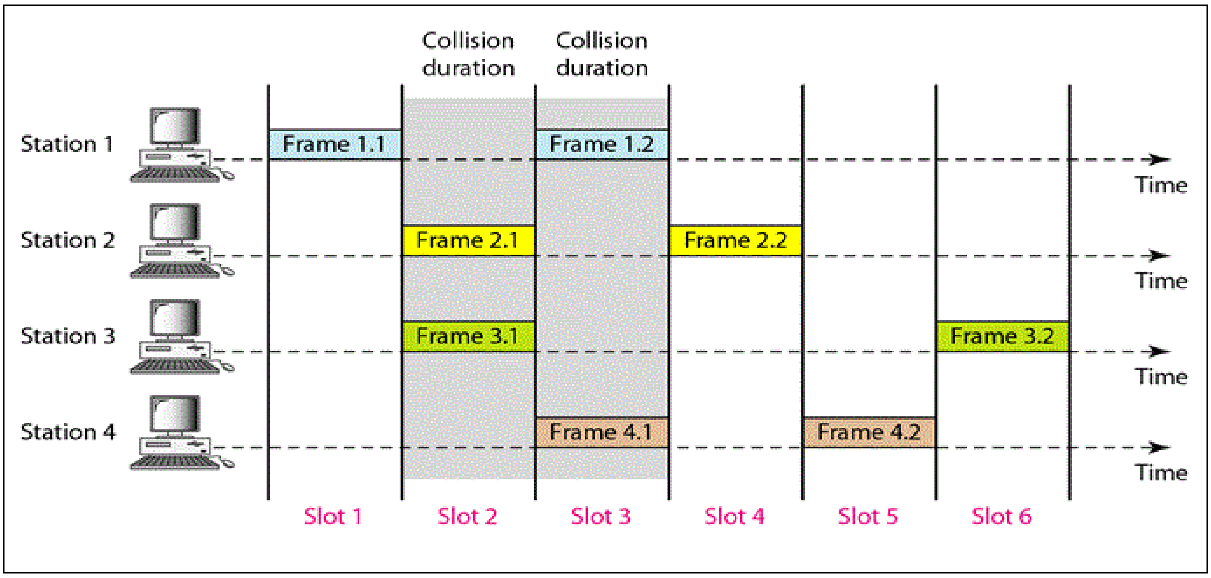
$S = 0.1839$

$S = 0.184$

So, **18.4 %** frames are transmitting successfully, when half of frame is generated during frame transmission time T_{fr} in **Pure ALOHA.** This is the maximum throughput we can achieve using Pure ALOHA.

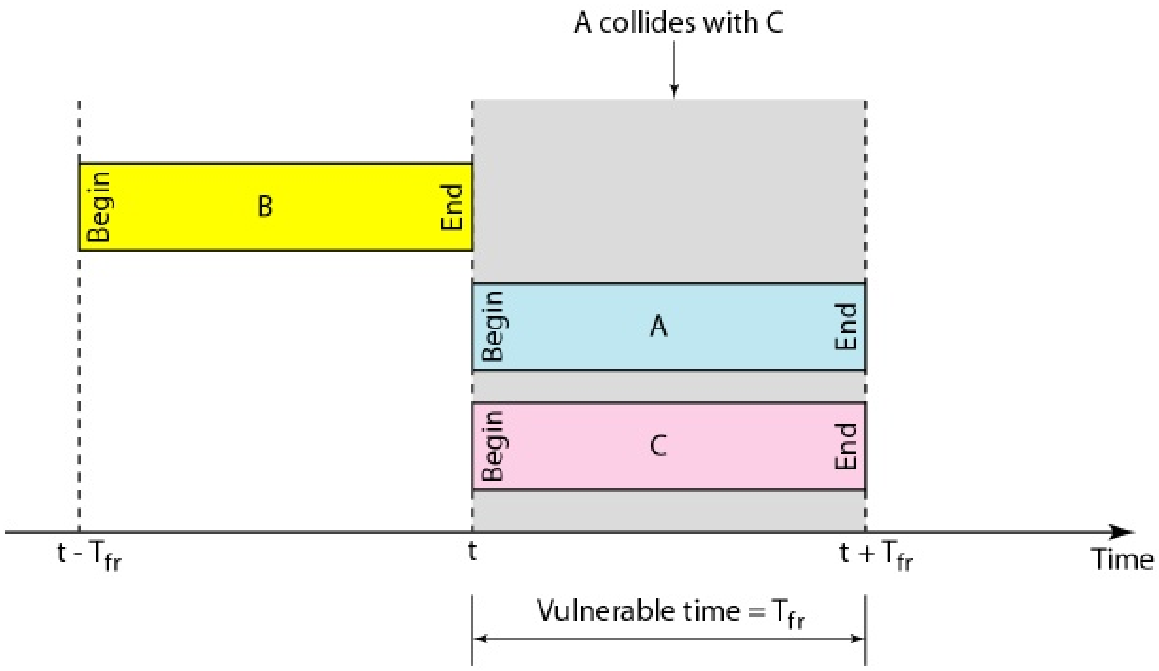
4.3.1.2 Slotted ALOHA

- In Slotted ALOHA bandwidth time is divided into different time slots.
- To improve the efficiency of Pure ALOHA, Slotted ALOHA is invented.



A station can send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame before the next time slot starts. There is still the possibility of collision if two stations try to send at the beginning of the same time slot.

Vulnerable Time:



Slotted ALOHA vulnerable time =$\mathbf{T_{fr}}$

Throughput:

The throughput for slotted ALOHA is $\boxed{\mathbf{S = G \times e^{-G}}}$

When G =1,

S = 1 x $\mathbf{e}^{-1}$

S = 0.3678

i.e. The maximum throughput $\mathbf{S}_{\mathbf{max}}$ = 0.368 when G=1

36 % frames are transmitted successfully in **slotted ALOHA**

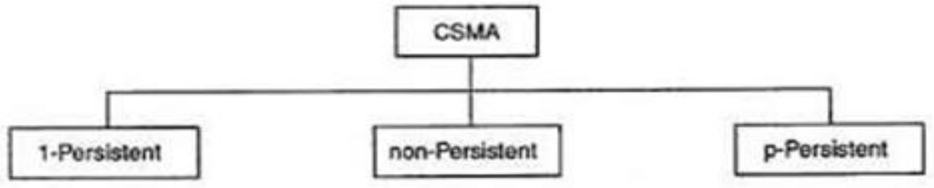
4.3.2 Carrier Sense Multiple Access (CSMA):

- 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".**

Persistence Methods

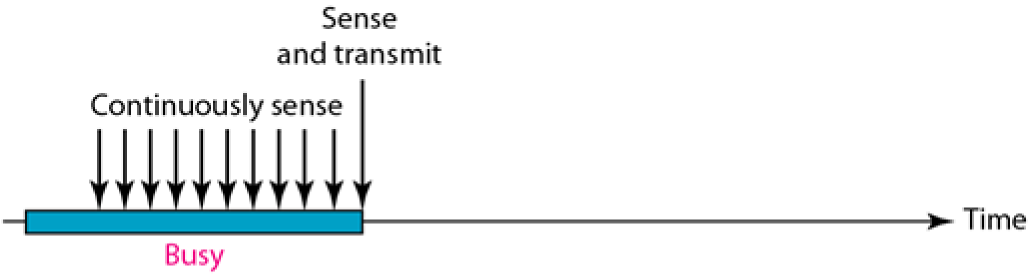
There are 3 types of transmission methods are used in CSMA those are called Persistence methods. These methods explain:

- What should a station do if the channel is busy
- What should a station do if the channel is idle

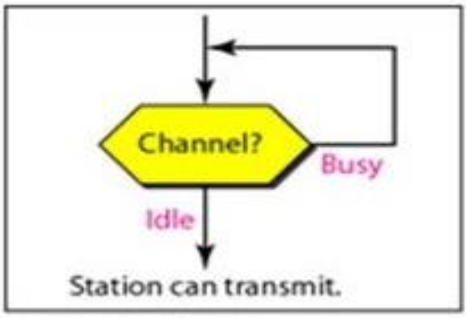


1-Persistent

- The 1-persistent method is simple and straight forward**.** Whenever **line is busy**, station **continuously sense** that busy line, if line is free then station sense that line and transmit its frame immediately (with probability 1).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

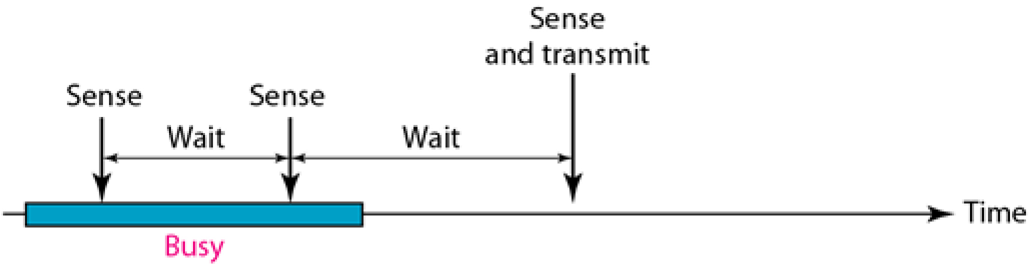


Flow Chart

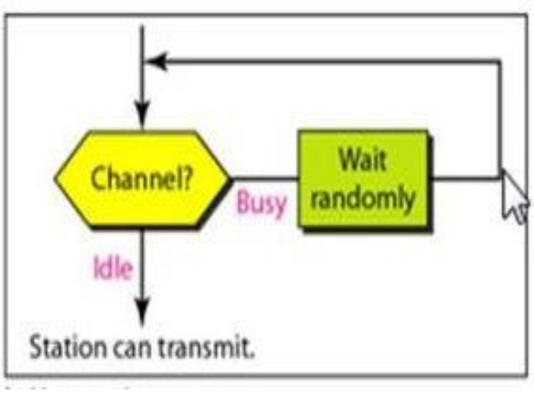


Non-Persistent

- In the Non-Persistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.
- The Non-Persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.

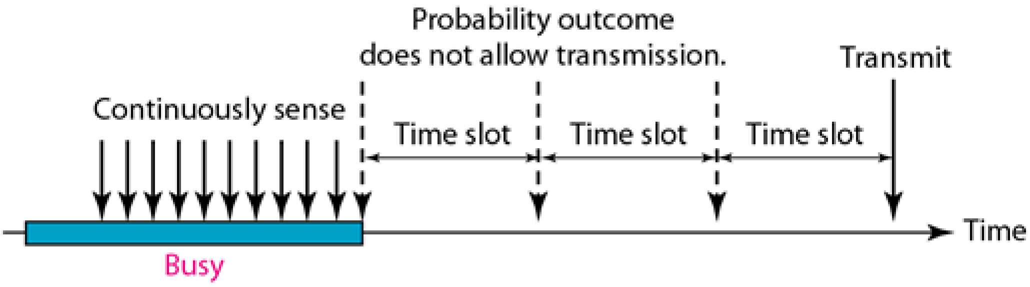


Flow Chart:



P-Persistent:

- The p-persistent method is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach reduces the chance of collision and improves efficiency.



In this method, after the station finds the line idle it follows these steps:

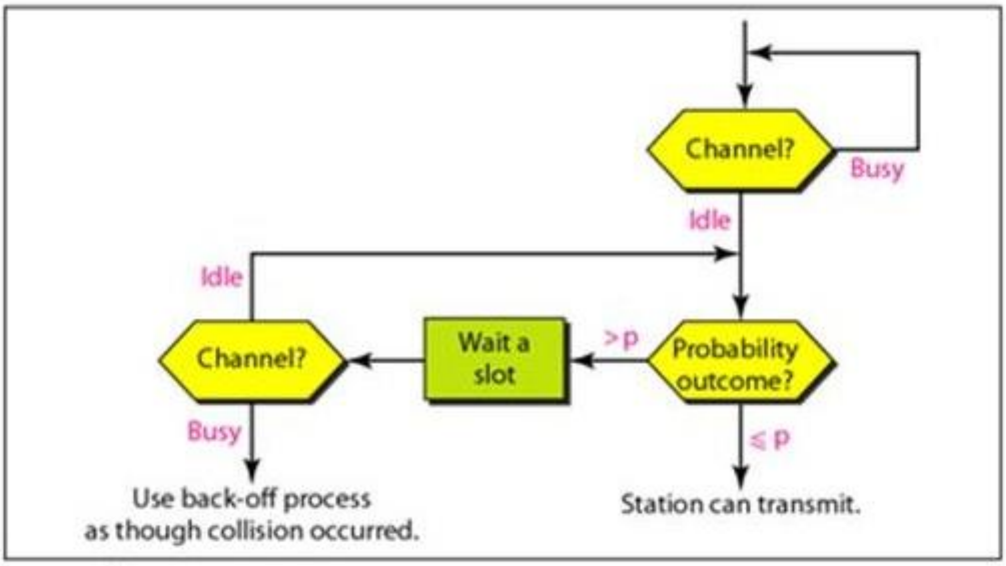
1. With probability p, the station sends its frame.

2. With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.

   a) If the line is idle, it goes to step 1.

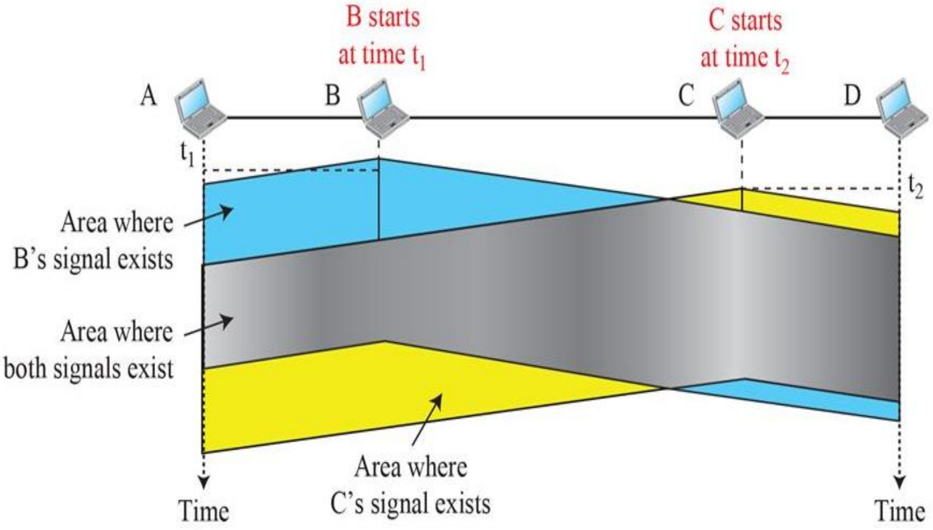
   b) If the line is busy, it acts as though a collision has occurred and uses the back- off procedure

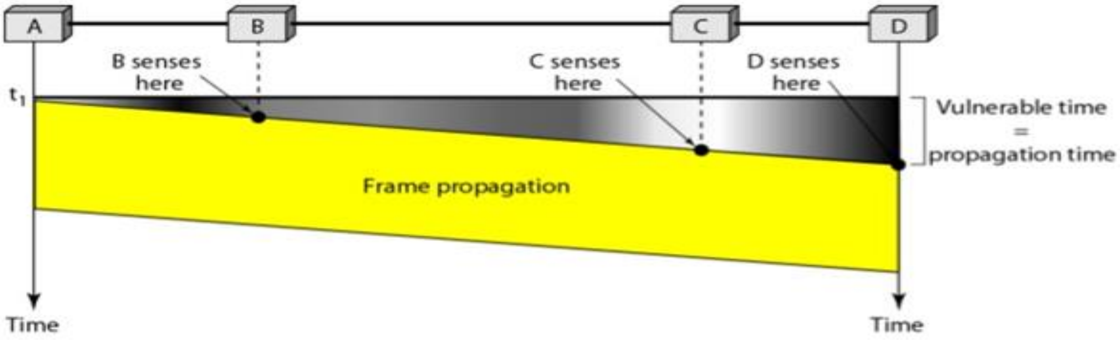
Flow Chart:



Vulnerable time in CSMA

Let us consider a scenario where four stations A, B, C, and D are connected to a shared channel. At the time t_1 Station B wants to transmit data to Station D. So, Station B senses the channel and finds that channel is idle and starts transmitting the frame to Station D. Before the first bit in Station B's frame reaches the intermediate Station C, at the time t_2 Station C also wants to send data to the same Station D. So, Station C senses the channel between Station C and Station D, finds it idle and starts transmitting the data to Station D. Now, Station B and Station C are communicating the same Station D, collision occurs among them.

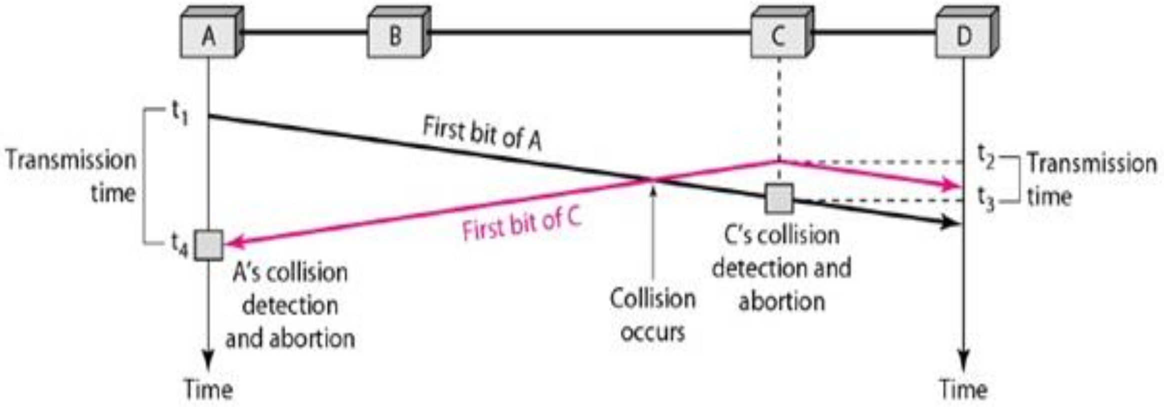

B starts at time t_1
C starts at time t_2
A
B
C
D
t_1
t_2
Area where B's signal exists
Area where both signals exist
Area where C's signal exists
Time
Time



4.3.3 *CSMA/Collision Detection (CD)*

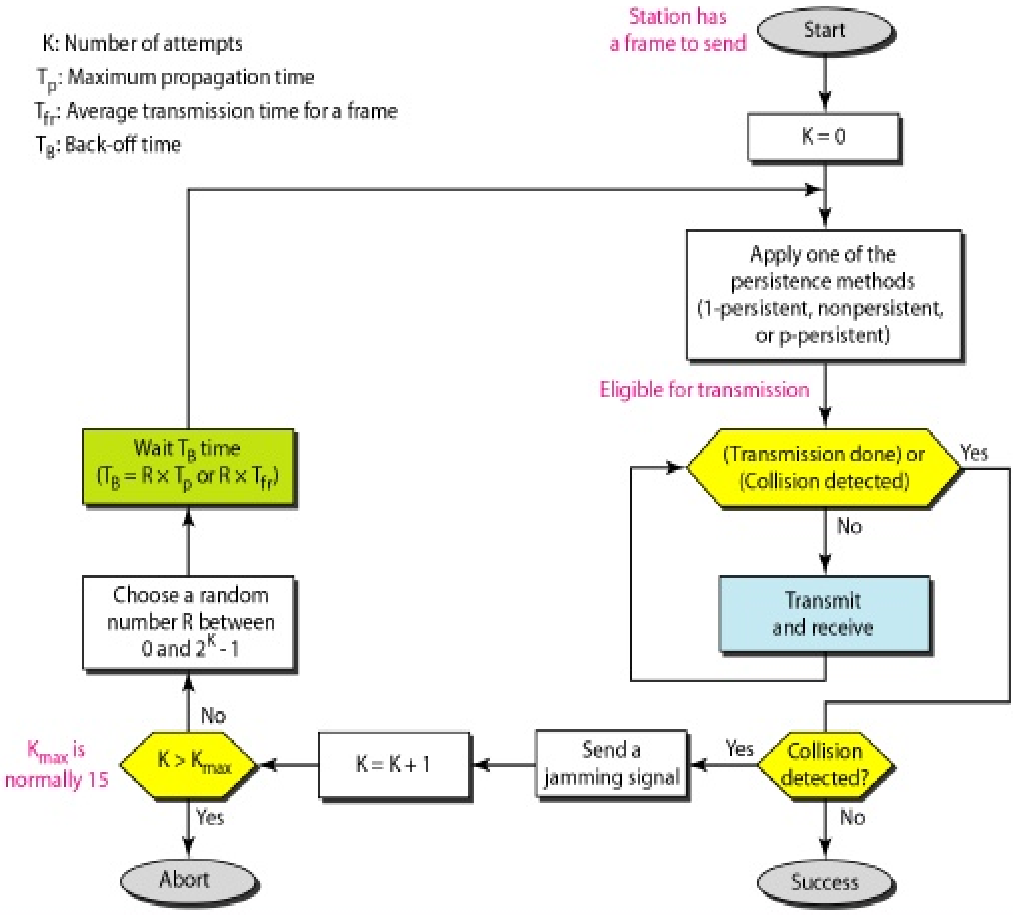
- Carrier Sense Multiple Access with collision detection (CSMA/CD) augments the algorithm to handle the collision used only in **Wired Communications**.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, 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, we show what happens as the first bits collide.

Collision and Abortion in CSMA/CD:



- 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 (or after a short time, but we assume immediately) aborts transmission.
- Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission.

Flow Chart:


K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
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 ($T_B = R \times T_p$ or $R \times T_{fr}$)

Procedure:

1. The first difference is the **addition of the persistence process**. We need to sense the channel before we start sending the frame by using one of the persistence processes (1-Persistence, Non-Persistence, P-Persistence).
2. The second difference is the **frame transmission**. In ALOHA, we first transmit the entire frame and then wait for an acknowledgment. In CSMA/CD, transmission and collision detection is a continuous process so **no need to send the entire frame** and then look for a collision. The station transmits and receives continuously and simultaneously.
3. The third difference is the **sending of a short jamming signal** that enforces the collision in case other stations have not yet sensed the collision.

As CSMA/CD is used in Wired Communications, because the signal does not loss its energy due to short distance between sender and receiver, **Repeaters** are generally used to amplify a signal.

Throughput:

The throughput of CSMA/CD is **greater** than that of pure or slotted ALOHA.

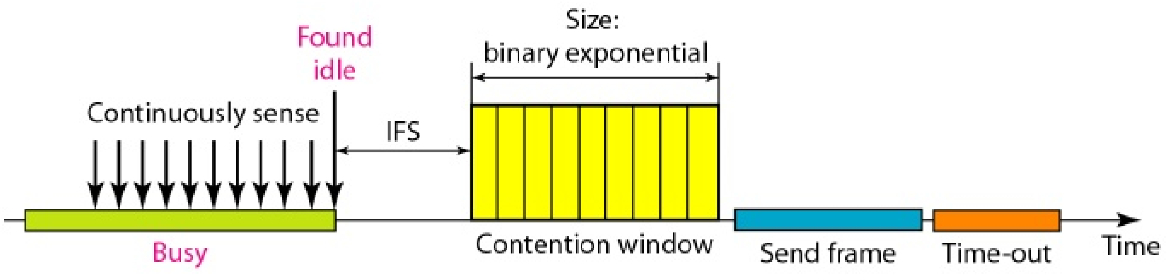
The maximum throughput occurs at a different value of G and is based on the persistence methods.

- For **I-persistent** method the maximum throughput is around **50 percent** when G =1.
- For **non-persistent** method, the maximum throughput can go up to **90 percent** when G is between 3 and 8.

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

In a wireless network, a signal lost its energy during transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. So the sender cannot identify the collision with its strength of the returned signal. So, it is difficult to identify the collision in wireless communication.

Timing Diagram:



CSMA/CA is used in wireless communication for avoiding the collisions use of **'3' strategies:**

1. IFS (Inter-Frame Space)
2. Contention window
3. Acknowledgement

Inter-Frame Space (IFS):

- When an idle channel is found, the station does not send immediately. It waits for a period of time called the inter-frame space or IFS.

- Even though the channel may appear idle when it is sensed, other station also starts at same time so there may be a chance of collision. To avoid collision a station should wait for IFS time.
- IFS can also be used to define the priority of a station or a frame.
- If IFS is very small to a station i.e. sender and receiver are in shorter distance so that sender has higher priority to send.
- CSMA/CA exactly working as a combination of both non-persistence and P-Persistence methods. In non-persistence wait is nothing but IFS time.
- In CSMA/CA, there is more chance of collisions due to wireless channel transmission medium.

Contention window:

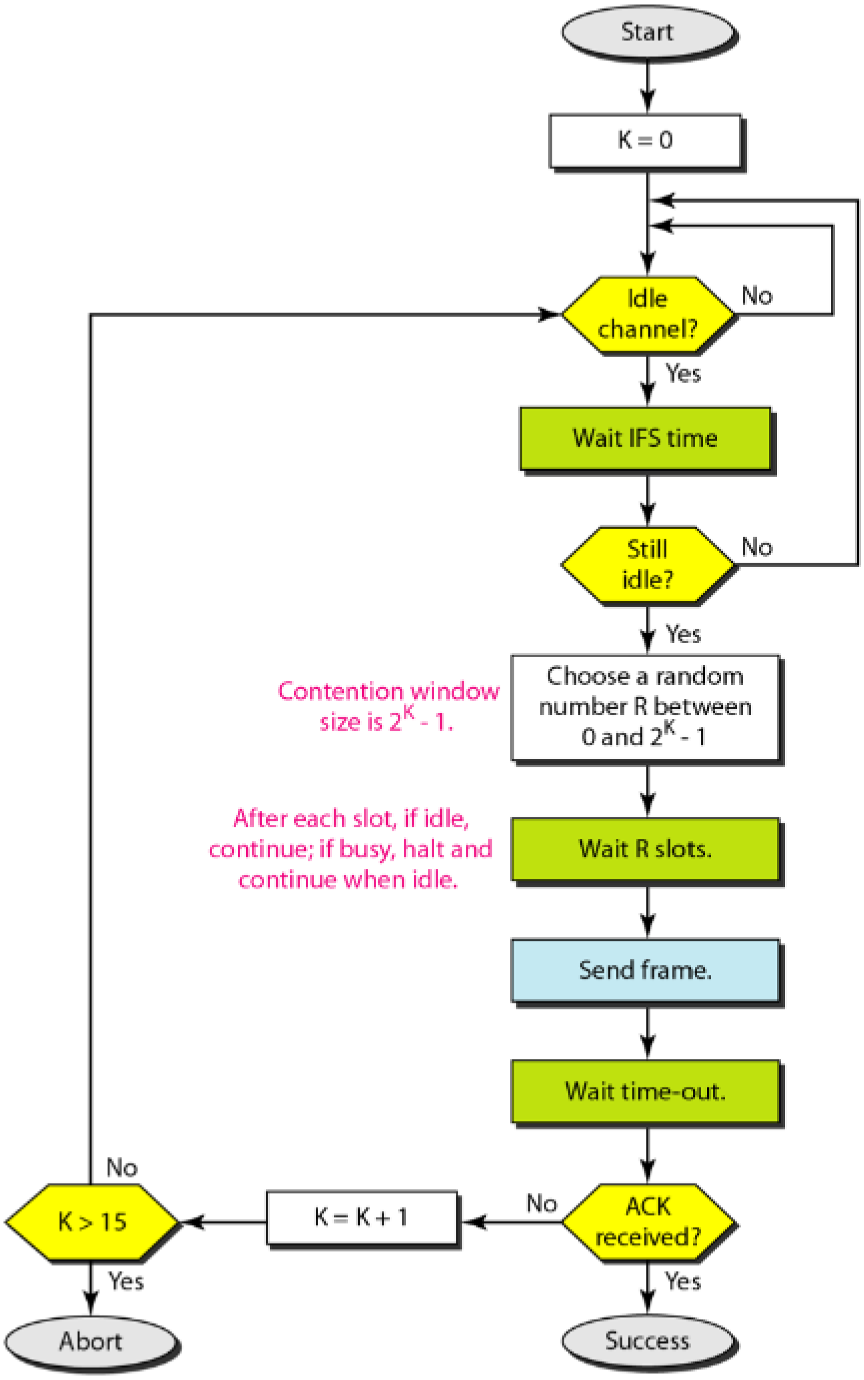
In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

Acknowledgment:

In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

Flow Chart:

In CSMA/CA there is a more chance of collisions due to wireless channel transmission medium.


Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Choose a random number R between 0 and $2^K - 1$
Contention window size is $2^K - 1$.
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
ACK received?
No
Yes
Success
K = K + 1
K > 15
No
Yes
Abort

4.4 Controlled Access

- 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.

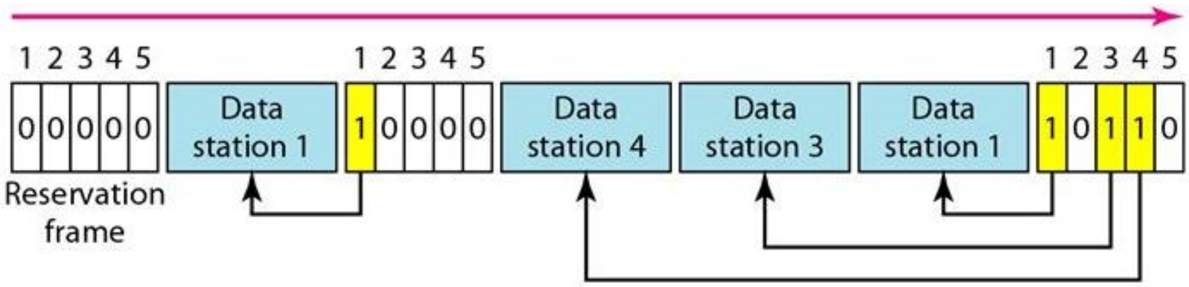
The three-popular controlled-access methods are:

1. Reservation
2. Polling
3. Token Passing

4.4.1 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 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.
- Data transmission can be done by one station at a time as **First Come First Serve** manner.

Figure below shows a situation with five stations and a five-mini slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



4.4.2 Polling

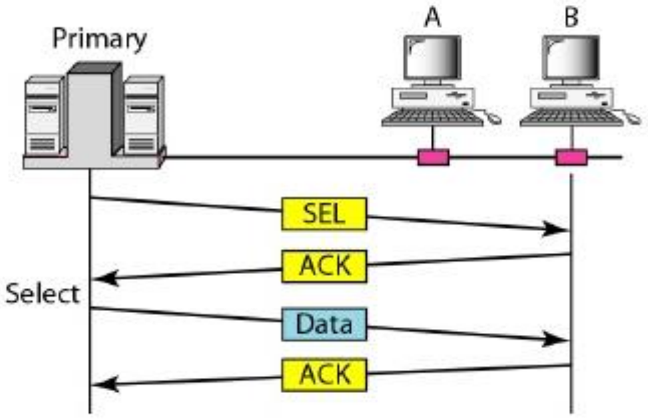
- Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations.
- In polling method all the stations can be controlled by one station that is called **primary station.**
- All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.
- It is up to the primary device to determine which device is allowed to use the channel at a given time.

Primary station uses 2 methods for Data transfer:

1. Select
2. Poll

4.4.2.1 Select

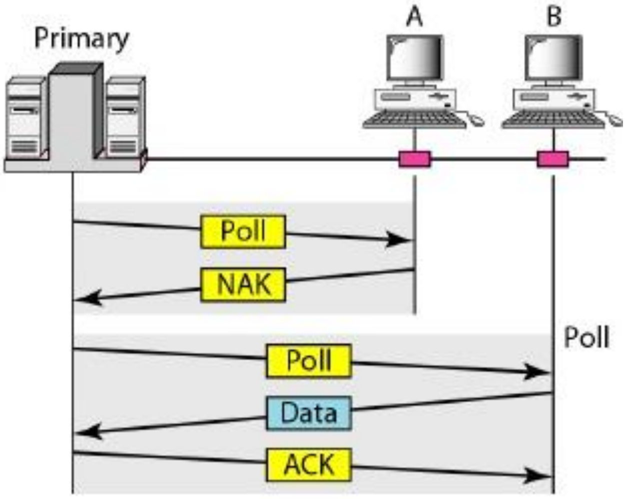
- The select function is used whenever the primary device has something to send.
- If the primary is neither sending nor receiving data, it knows the link is available. If it has something to send, the primary device sends it.
- Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.



4.4.2.2 Poll

- The poll function is used when the primary station is ready to receive data 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.
- If the response from the secondary device is negative (a NAK frame), then the primary polls the next secondary station 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.



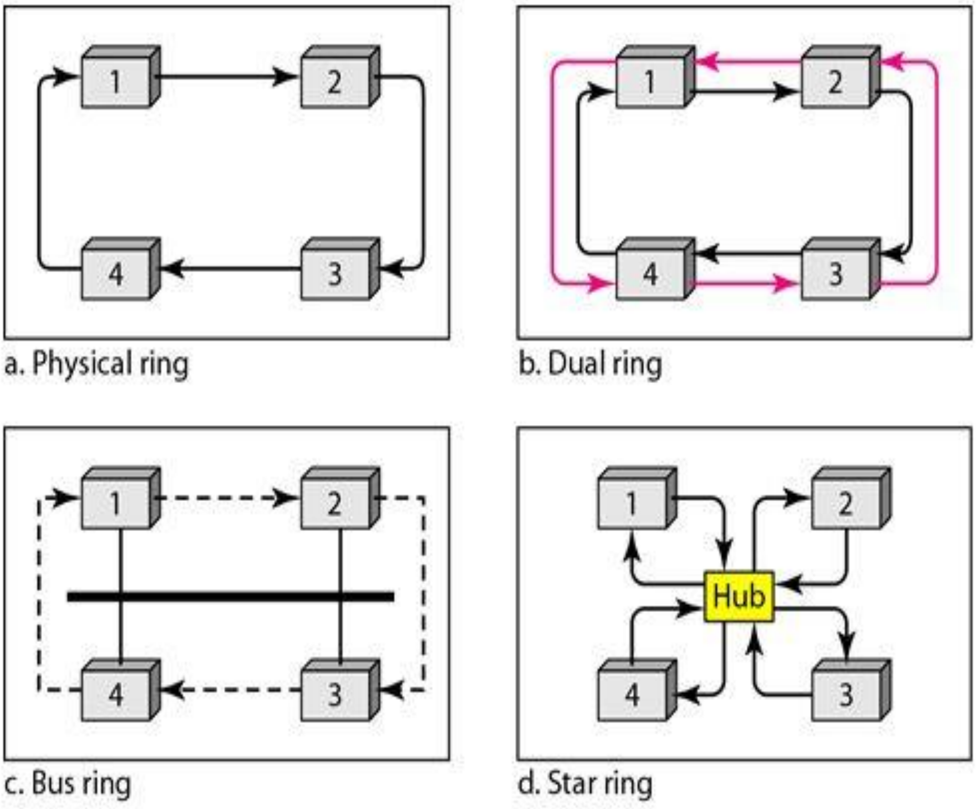
4.4.3 Token Passing

- 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.
- **Token management** is needed for this access method. The token must be monitored to ensure it has not been lost or destroyed.

- 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.

Logical ring and physical topology in token-passing access method

In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one.



a. Physical ring

b. Dual ring

c. Bus ring

d. Star ring

4.4.3.1 Physical ring topology

- In this topology, when a station sends the token to its successor, other stations cannot see the token; the successor is the next one in line. This means that the token does not have to have the address of the next successor.
- The problem with this topology is that if one of the links-the medium between two adjacent stations- fails, the whole system fails.

4.4.3.2 Dual ring topology

- This topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring.
- The second ring is for emergencies only. If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring.
- The high-speed Token Ring networks called FDDI (Fiber Distributed Data Interface) and CDDI (Copper Distributed Data Interface) use this topology.

4.4.3.3 Bus ring topology

- It is also called a token bus; the stations are connected to a single cable called a bus. They, however, make a logical ring, because each station knows the address of its successor (and also predecessor for token management purposes).
- When a station has finished sending its data, it releases the token and inserts the address of its successor in the token. Only the station with the address matching the destination address of the token gets the token to access the shared media.
- The Token Bus LAN, standardized by IEEE, uses this topology.

4.4.3.4 Star ring topology

- In a star ring topology, the physical topology is a star. There is a hub, however, that acts as the connector.
- The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections.
- This topology makes the network less prone to failure because if a link goes down, it will be bypassed by the hub and the rest of the stations can operate.

4.5 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.

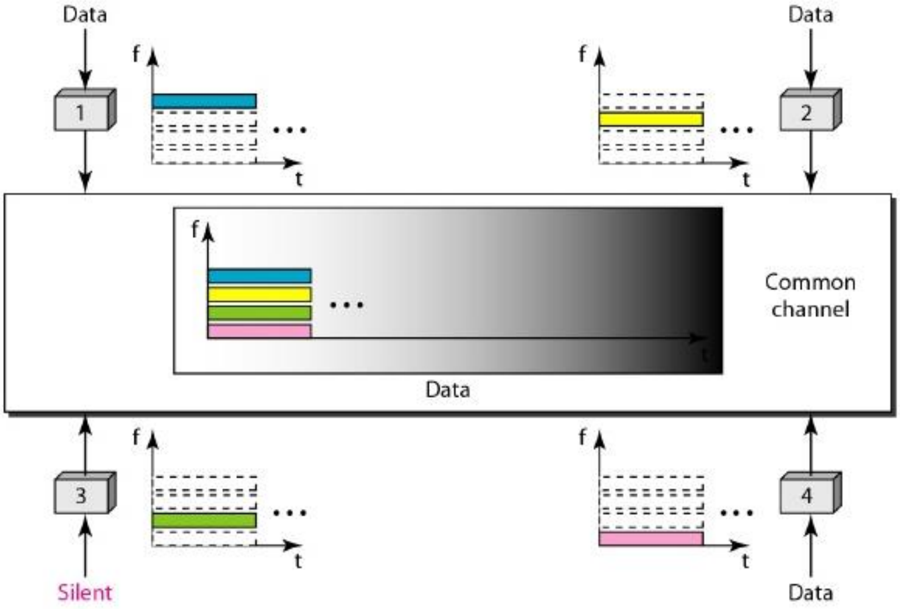
Three protocols are used for Channelization:

1. FDMA
2. TDMA

3. CDMA

4.5.1 Frequency Division Multiple Access (FDMA)

- In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data.
- In other words, each band is reserved for a specific station, and it belongs to the station all the time.
- Each station also uses a band pass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.



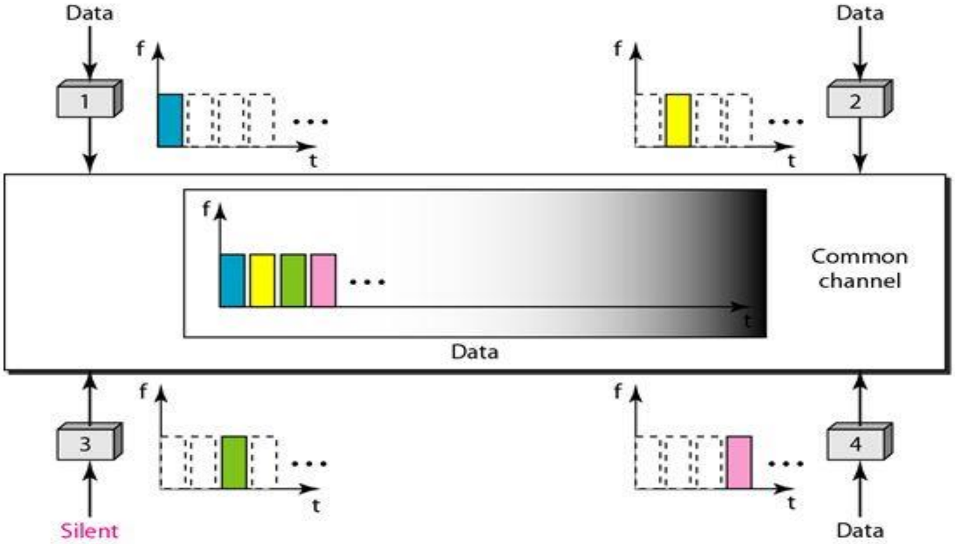
Difference between FDM and FDMA:

Frequency Division Multiplexing (FDM)	Frequency Division Multiple Access (FDMA)
1. FDM is a **Physical layer** technique.	FDMA is an access method in the **data link layer.**
2. FDM at physical layer combines the loads from low-bandwidth channels and transmits them by using a high-bandwidth channel.	The 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.
3. It **requires multiplexers.**	It **doesn't require multiplexers**

4.5.2 Time Division Multiple Access (TDMA)

- In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data. Each station transmits its data in is assigned time slot.



- The **main problem with TDMA** lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot. To compensate for the delays, we can insert guard times.
- **Synchronization** is normally accomplished by having some synchronization bits (normally referred to as preamble bits) at the beginning of each slot.

Difference between TDM and TDMA:

Time Division Multiplexing (TDM)	Time Division Multiple Access (TDMA)
1. TDM is a **Physical layer** technique.	TDMA is an access method in the **data link layer.**
2. TDM at physical layer, that combines the data from slower channels and transmits them by using a faster channel.	The data link layer in each station tells its physical layer to use the allocated time slot.

3. It **requires multiplexers.**	It **doesn't require multiplexers**

4.5.3 Code Division Multiple Access (CDMA):

- In CDMA, one channel carries all transmissions simultaneously.
- It differs from FDMA because only one channel occupies the entire bandwidth of the link.
- It differs from TDMA because all stations can send data simultaneously and there is no timesharing.
- CDMA simply means communication with different codes

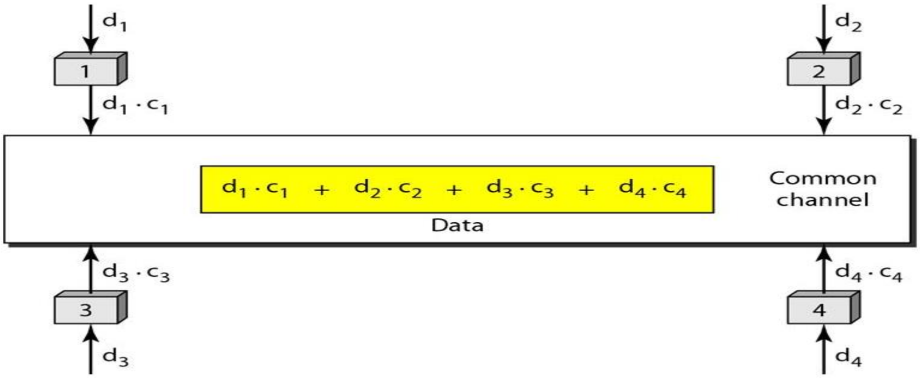
4.5.3.1 Idea of CDMA

Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel. The data from station 1 are d1, from station 2 are d2, and so on. The code assigned to the first station is c1, to the second is c2, and so on. We assume that the assigned codes have two properties.

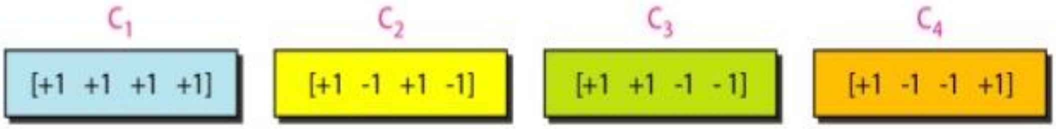
1. If we multiply each code by another, we get 0.
2. If we multiply each code by itself, we get 4 (the number of stations).

4.5.3.2 Simple idea of communication with code

- Here **Station 1** multiplies its data by its code to get **d1.c1** and **Station 2** multiplies its data by its code to get **d2.c2** and so on. The data that go on the channel are the **sum of all** these terms, as shown in the box.
- 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. For example, suppose stations 1 and 2 are talking to each other. Station 2 wants to hear what station I is saying. It multiplies the data on the channel by cl' the code of station 1.

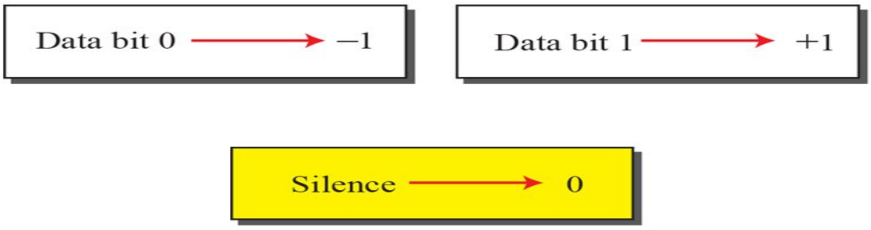


- CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips.
- Each station is assigned a unique chip sequence whose length is 'N' (Number of stations)
- Chip sequences are orthogonal vectors i.e. the inner product of any pair must be zero.



Some rules are followed for encoding and decoding process:

- If a station needs to send a **0 bit**, it encodes it as **-1**;
- If a station needs to send a **1 bit**, it encodes it as **+1**.
- When a station is **idle**, it sends **no signal**, which is interpreted as a 0 (**zero**).



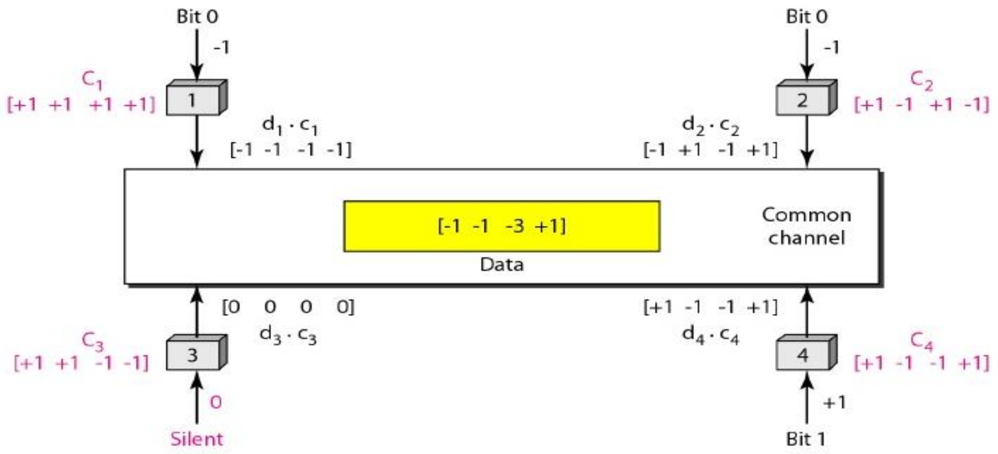
For **station1** data bit is -1 and code, c1 = [+1 +1 +1 +1] so d1.c1 = [-1 -1 -1 -1]

For **station2** data bit is -1 and code, c1 = [+1 -1 +1 -1] so d1.c1 = [-1 +1 -1 +1]

For **station3** data bit is 0 and code, c1 = [+1 +1 -1 -1] so d1.c1 = [0 0 0 0]

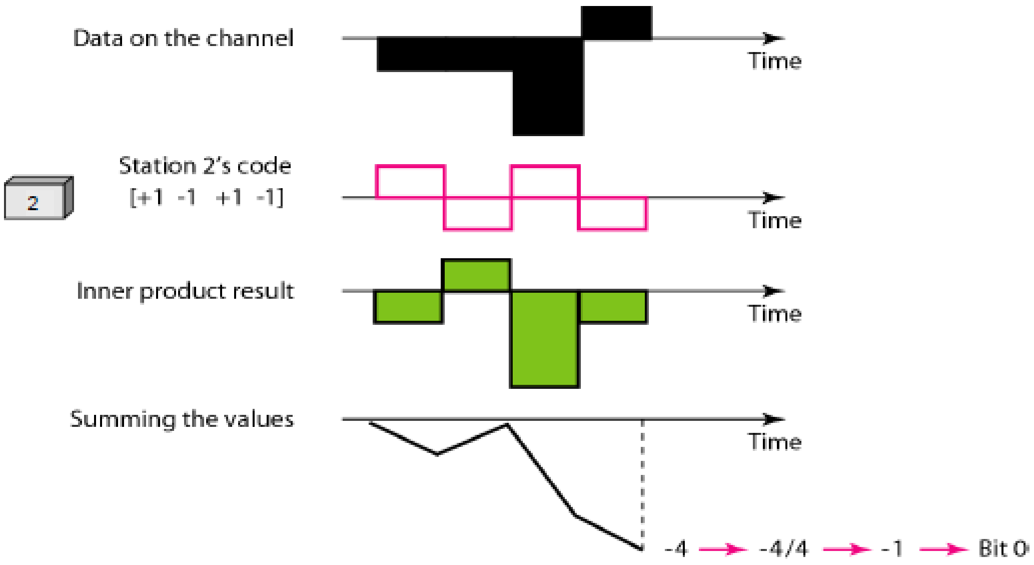
For **station4** data bit is +1 and code, c1 = [+1 -1 -1 +1] so d1.c1 = [+1 -1 -1 +1]

Data Transmitted is [-1 -1 -3 +1] (By adding d1.c1 + d2.c2+ d3.c3+ d4.c4)

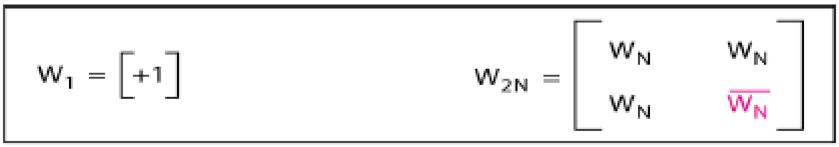


The shared channel will transfer the addition of the signals coming from all the devices connected to the network as in the above example it is [-1 -1 -3 +1].

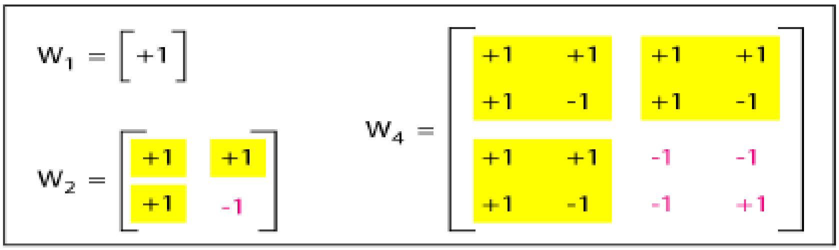
When the respective destination arrives it reads the signal in the shared channel [-1 -1 -3 +1], multiplies with the source's code and adds all the values in the signal. The resultant is then divided with the number of devices in the networks. This is clearly depicted below.



To generate the orthogonal codes, we use a Walsh table, a two dimensional table with an equal number of rows and columns. Each row is a sequence of chips. General rule and examples of creating Walsh tables are shown below.



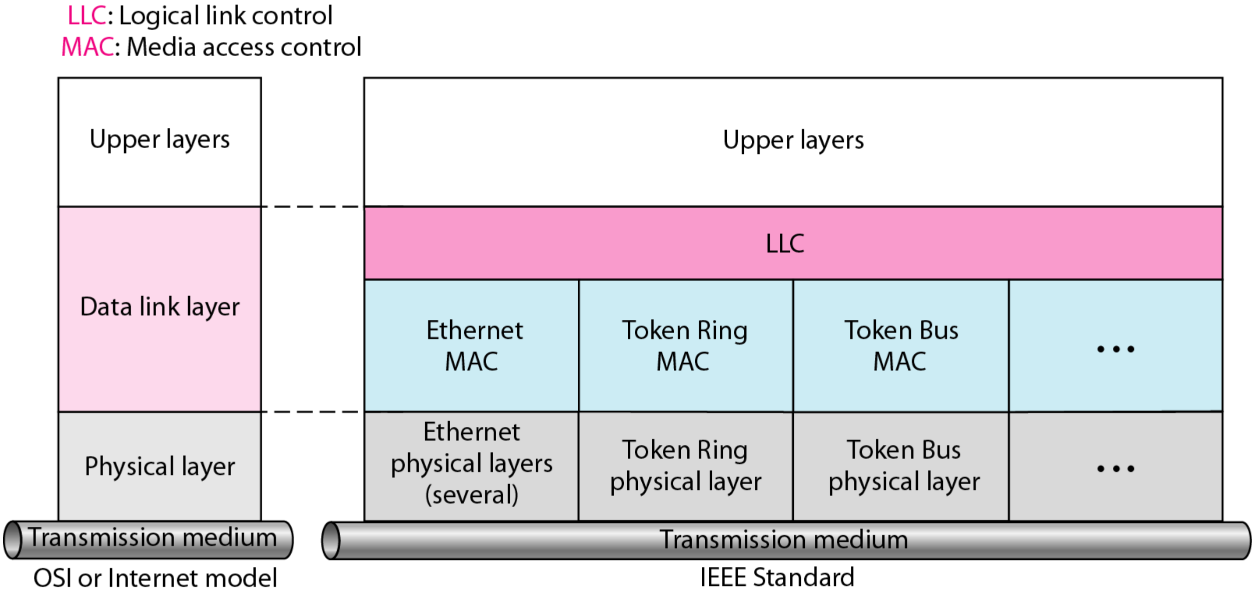
a. Two basic rules



4.6 Wired LANs

In 1985, the computer society, IEEE started a project called Project 802, to set standards that enable intercommunication among equipment from a variety of manufacturers. Project 802 doesn't seek to replace any part of OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802. The relationship of 802 standards to the traditional OSI model is shown below figure.



The IEEE has subdivided the data link layer into two sub layers

1. Logical Link Control (LLC) and

2. Medium Access Control (MAC)

IEEE has also created several physical layer standards for different LAN protocols.

4.6.1 Data Link Layer

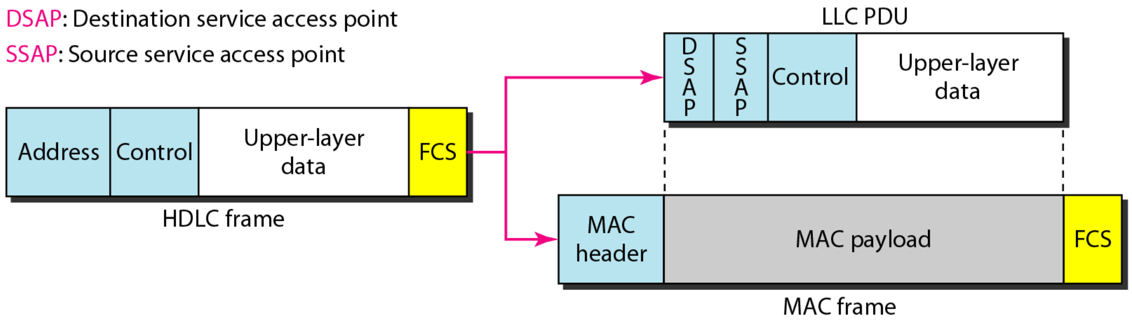
As we mentioned before, the data link layer in the IEEE standards is divided into two sublayers: LLC and MAC.

Logical Link Control (LLC)

We said that data link control handles framing, flow control, and error control. In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC and MAC sublayer

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent. The above figure shows one single LLC protocol serving several MAC protocols. Framing LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The 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 destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP). The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In otherwords, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in below figure.

Need for LLC: The purpose of the LLC is to provide flow and error control for the upper layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper layer protocols such as IP, do not use the services of LLC.

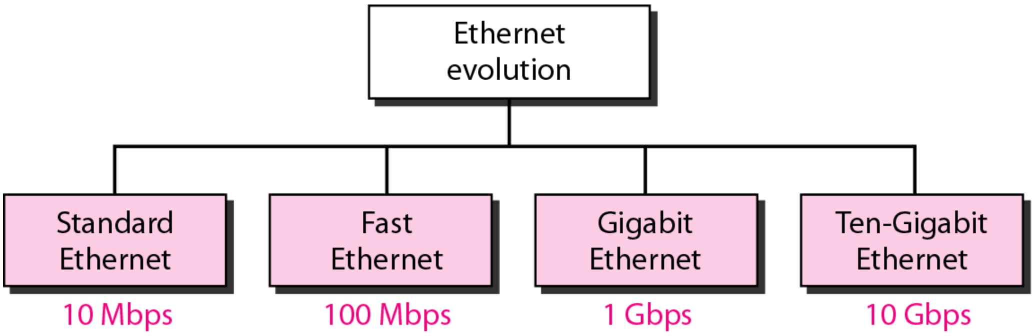


Medium Access Control (MAC)

IEEE Project 802 has created a sublayer called Medium Access Control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the medium access method for Ethernet LANs and the tokenpassing method for Token Ring and Token Bus LANs. As we discussed in the previous section, part of the framing function is also handled by the MAC layer. In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

4.6.2 Physical Layer

The physical layer is dependent on the implementation and type of physical medium used. IEEE defines detailed specifications for each LAN implementation. For example, although there is only one MAC sublayer for Standard Ethernet, there is a different physical layer specification for each Ethernet implementations.



4.6.2.1 Standard Ethernet

MAC Sublayer:

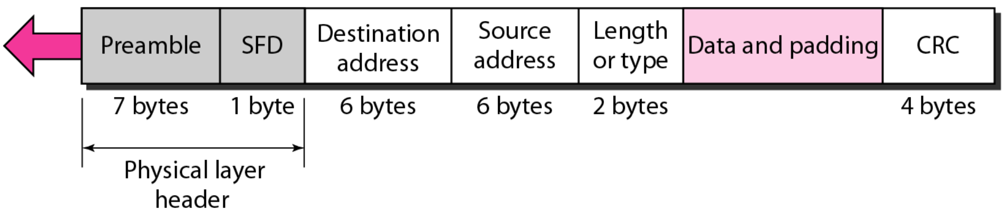
In Standard Ethernet, the MAC sublayer governs the operations of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Frame Format:

The Ethernet frame contains seven fields: Preamble, SFD, DA, SA, Length or Type of Protocol Data Unit (PDU, upper layer data, and the CRC. Ethernet doesn’t provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.

Acknowledgments must be implemented at the higher layers. The format of the MAC frame is shown in Figure below.

Preamble: 56 bits of alternating 1s and 0s.
SFD: Start frame delimiter, flag (10101011)



i. Preamble: The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56 bit pattern allows the stations to miss some bits at the beginning of the frame. The Preamble is actually added at the physical layer and is not part of the frame.

ii. Start Frame Delimiter (SFD): The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

iii. Destination Address (DA): The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.

iv. Source Address (SA): The SA field is also 6 bytes and contains physical address of the sender of the packet.

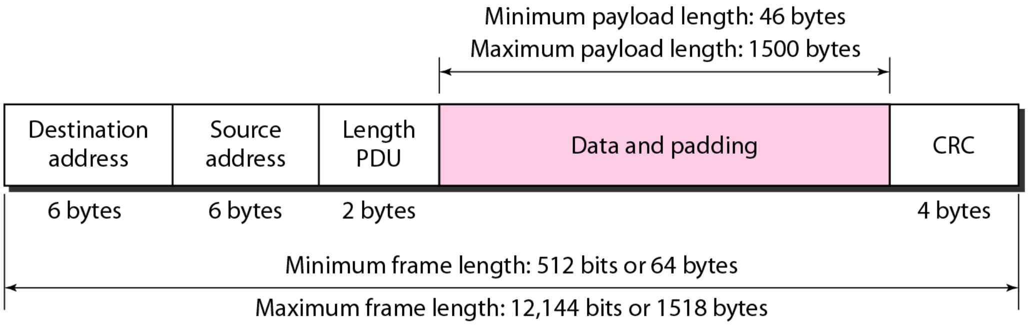
v. Length or Type: This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.

vi. Data: The field carries data encapsulated from the upper layer protocols. It is a minimum of 46 bytes and maximum of 1500 bytes.

vii. CRC: The last field contains error detection information, in this case a CRC – 32

Frame Length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame, as shown in below figure

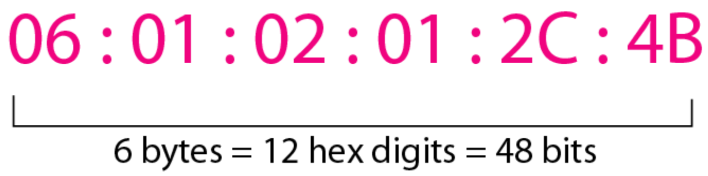

Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

The minimum length restrictions are required for the correct operation of CSMA/CD. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 – 18 = 46 bytes. If the upper layer packet is less than 46 bytes, padding is added to make up the difference.

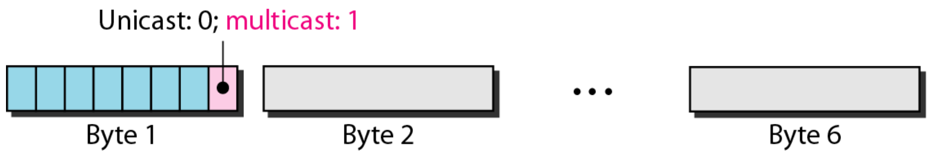
The Standard defines the maximum length of a frame as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet was designed. A maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Addressing:

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address. As shown in Figure below, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.


06 : 01 : 02 : 01 : 2C : 4B
6 bytes = 12 hex digits = 48 bits

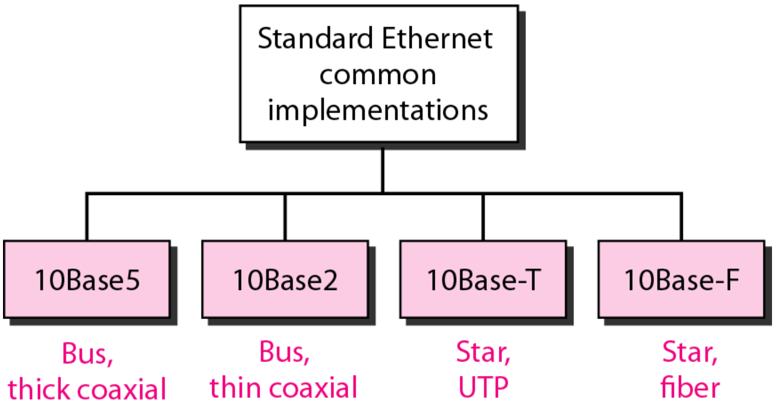
Unicast, Multicast, and Broadcast address: A source address is always a unicast address; the frame comes from only one station. The destination address, however, can be unicast, multicast or broadcast. Figure below shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise it is multicast.



A unicast destination address defines only one receiptant; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of address; the relationship between the sender and the receiver is one-to-many. The broadcast address is a special case of the multicast address; the receiptants are all the stations on the LAN. A broadcast destination address is 48 bits.

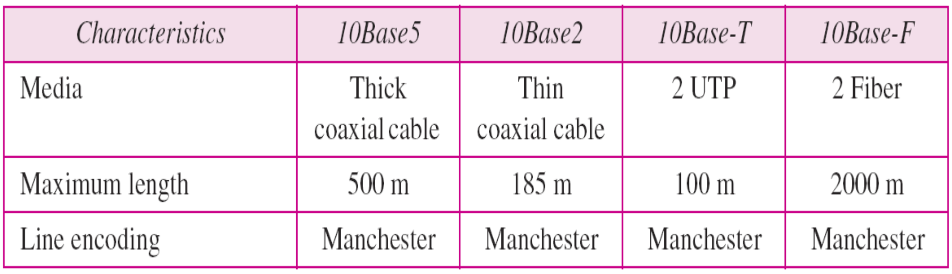
Physical Layer

The Standard Ethernet defines several physical layer implementations. Four of the most common are shown in figure below.



All standard implementations use digital signaling (Baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme. At the receiver, the received signal is interpreted as Manchester and decoded into data. Manchester encoding is self-synchronous, providing a transition at each bit interval.

The comparisons between different Standard Ethernet standards are shown in below table.



Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

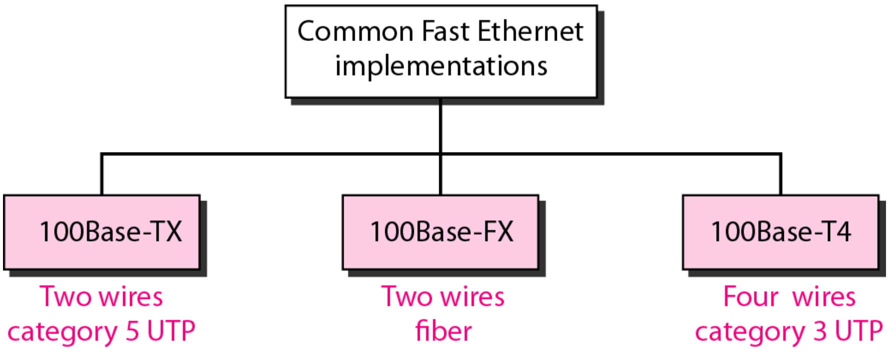
4.6.2 Fast Ethernet

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.

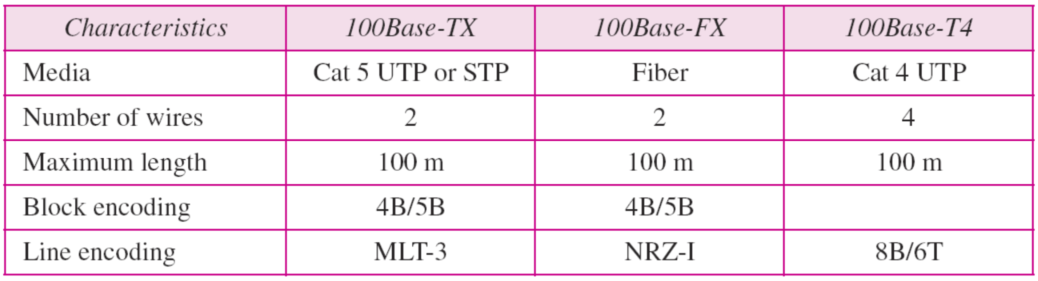
The goals of Fast Ethernet can be summarized as follows

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48 bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths

The implementations of Fast Ethernet are shown in figure below.



The Comparison between Fast Ethernet standards are shown in table below.

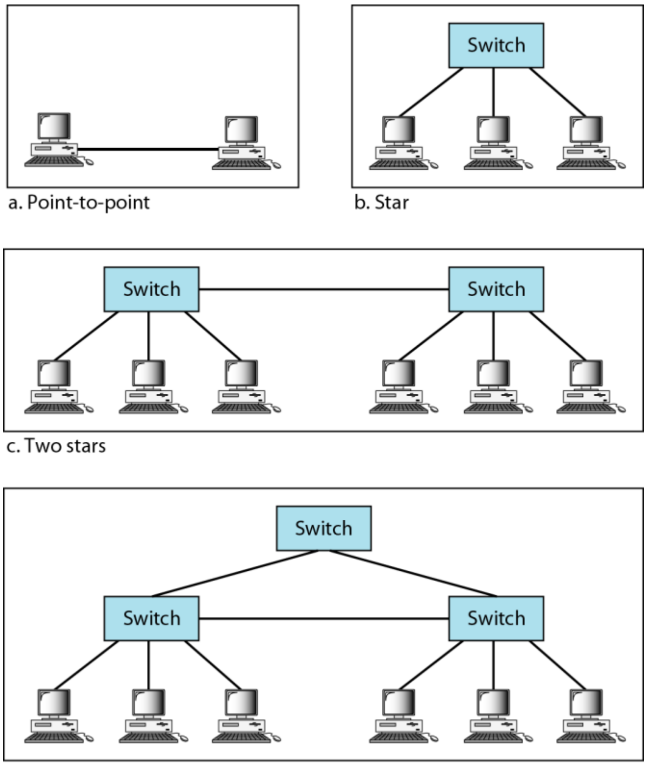


Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

4.6.3 Gigabit Ethernet

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the standard as 802.3z. In the full duplex mode of Gigabit Ethernet, there is no collision. The maximum length of the cable is determined by the signal attenuation in the cable.

The topologies of Gigabit Ethernet are 1. Point to Point, 2. Star, 3. Two Stars, 4. Hierarchy of Stars.



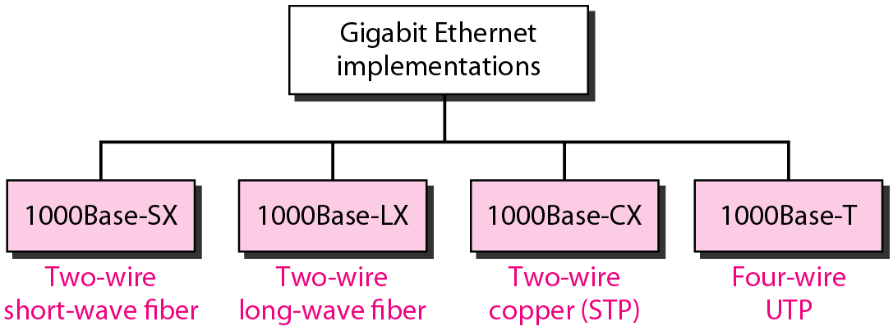
a. Point-to-point

b. Star

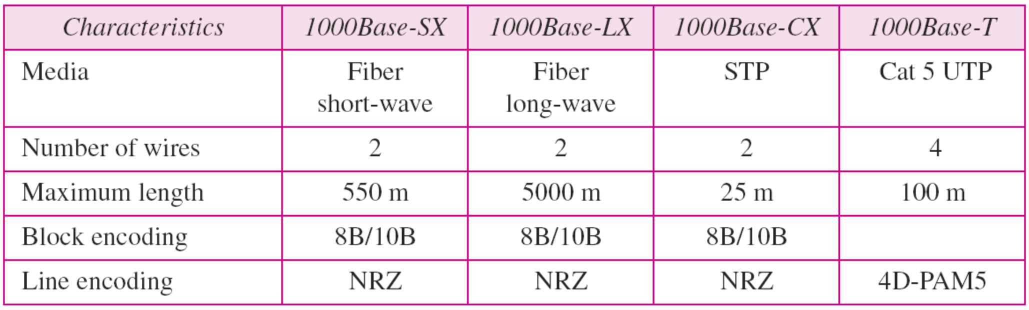
c. Two stars

d. Hierarchy of stars

The Gigabit Ethernet implementations are clearly shown in below picture.



The comparison among these Gigabit Ethernet are shown below.



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

4.6.4 Ten Gigabit Ethernet

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

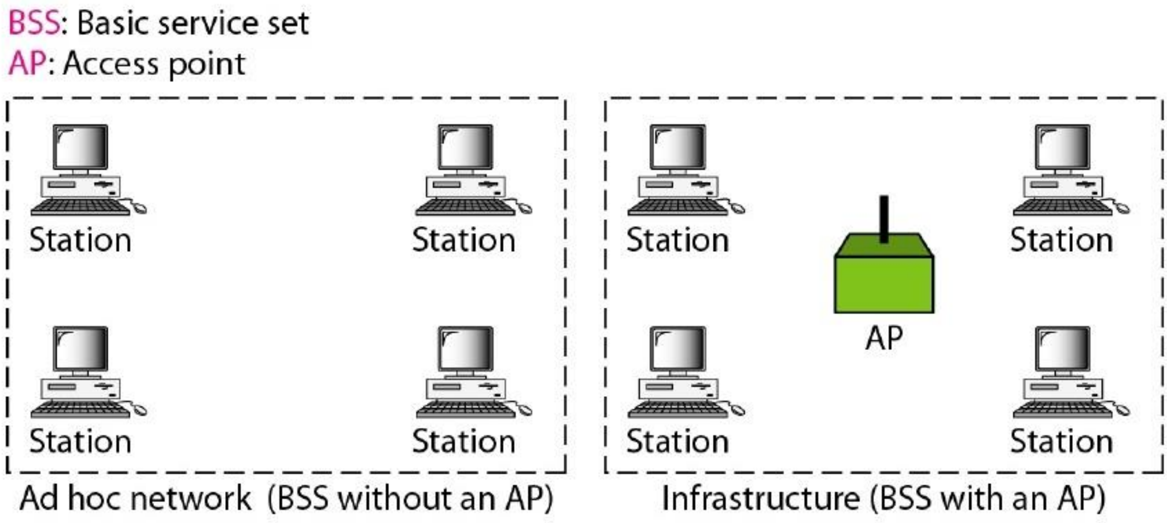
4.7 IEEE 802.11

4.7.1 Architecture

The standard defines two kinds of services: The Basic Service Set (BSS) and the Extended Service Set (ESS).

Basic Service Set

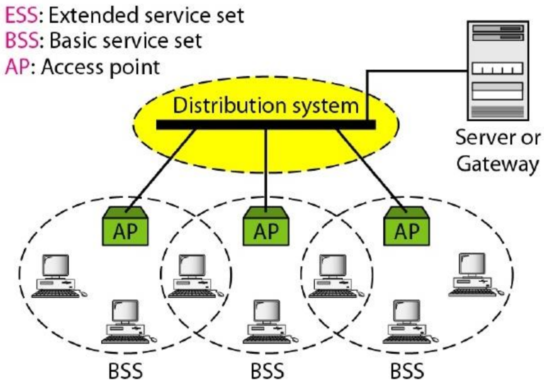
IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure below shows two sets in this standard.



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 (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.



4.7.2 Layered Architecture of IEEE 802.11

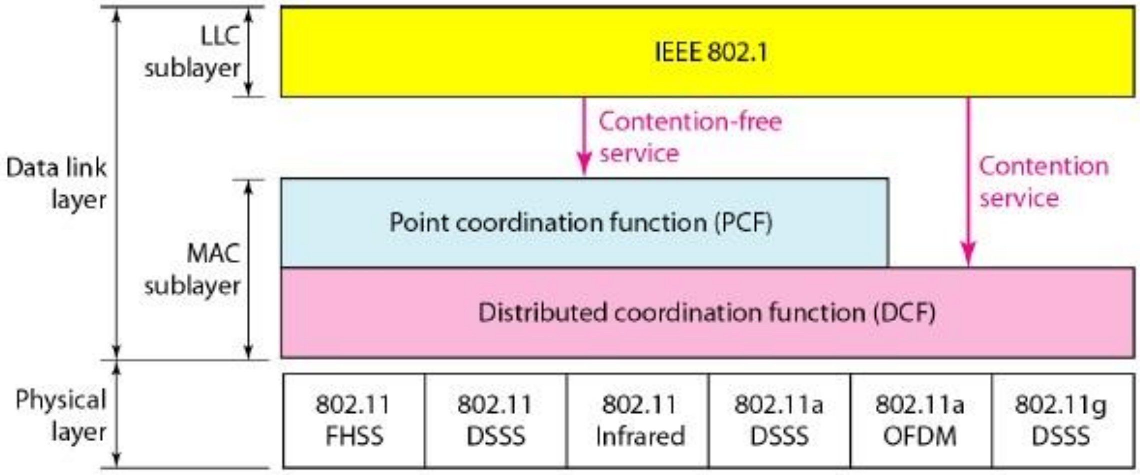
IEEE 802.11 defines different signalling systems and protocols in Physical and Data link Layers. Physical layer consists of different multiplexing techniques like Frequency Hoping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DHSS), Orthogonal Frequency Division Multiplexing (OFDM) and Infrared frequencies.

The Datalink layer consists of two sublayers LLC & MAC, where MAC is again sub divided into two functions such as Point Coordination Function (PCF) and Distributed Coordination Function (DCF). The Point Coordination Function comes in to picture where an access point wants to communicate with an individual user device called secondary station. The Distributed Coordination Function (DCF) works in normal condition where two user devices want to communicate with the help of an access point. The alternative PCF and DCF is separated by a contention period.

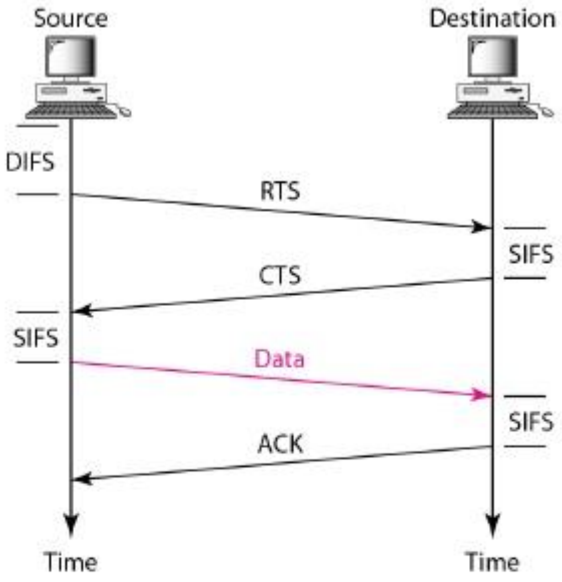
Distributed coordination function (DCF):

DCF is the normal communication duration in which two user devices communicate with each other with the help of an Access Point (AP). So, there is a requirement of

Medium Access Protocol to allocate shared channel to user devices. The MAC protocol used in IEEE 802.11 DCF is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

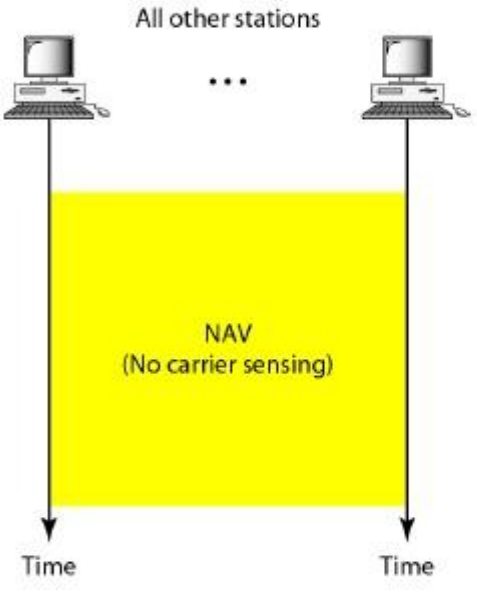


Two control frames Request to SEND (RTS) and Clear to SEND (CTS) are used to allocate the bandwidth between two users source & destination. The working of RTS and CTS are shown in the picture below.



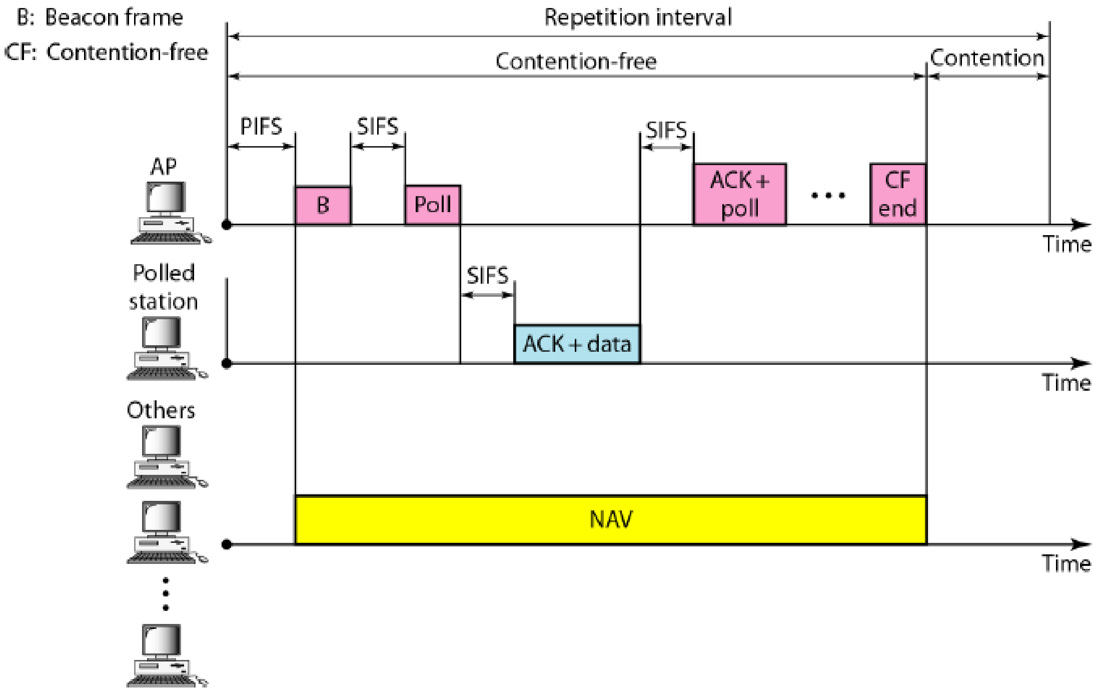
When the source wants to communicate to a particular destination, it sends an RTS frame to the destination through access point after the Distributed Interframe Space (DIFS). After receiving a RTS frame from source the destination waits for Separated Interframe Space (SIFS), and when it is ready for accepting the connection, transmits a CTS frame to the source. Thereafter, the source and destination exchanges data and acknowledgement frames for the data transfer.

When a RTS frame is transmitted from a source to destination a timer, Non Allocation Vector (NAT), is initiated in all other stations and the stations move to ‘No Carrier Sensing’ mode.

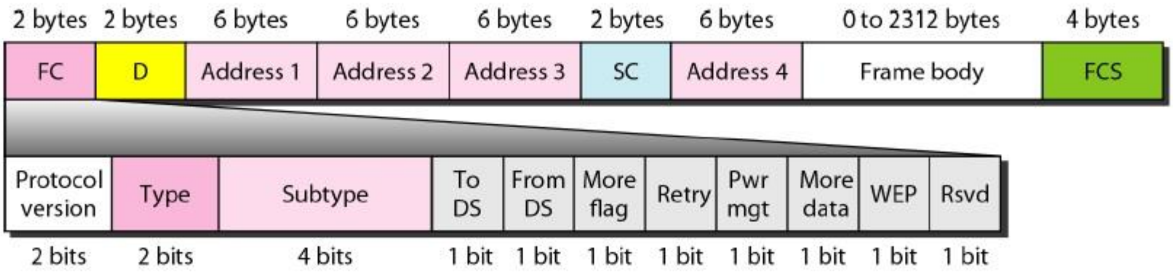


Point coordination function (PCF):

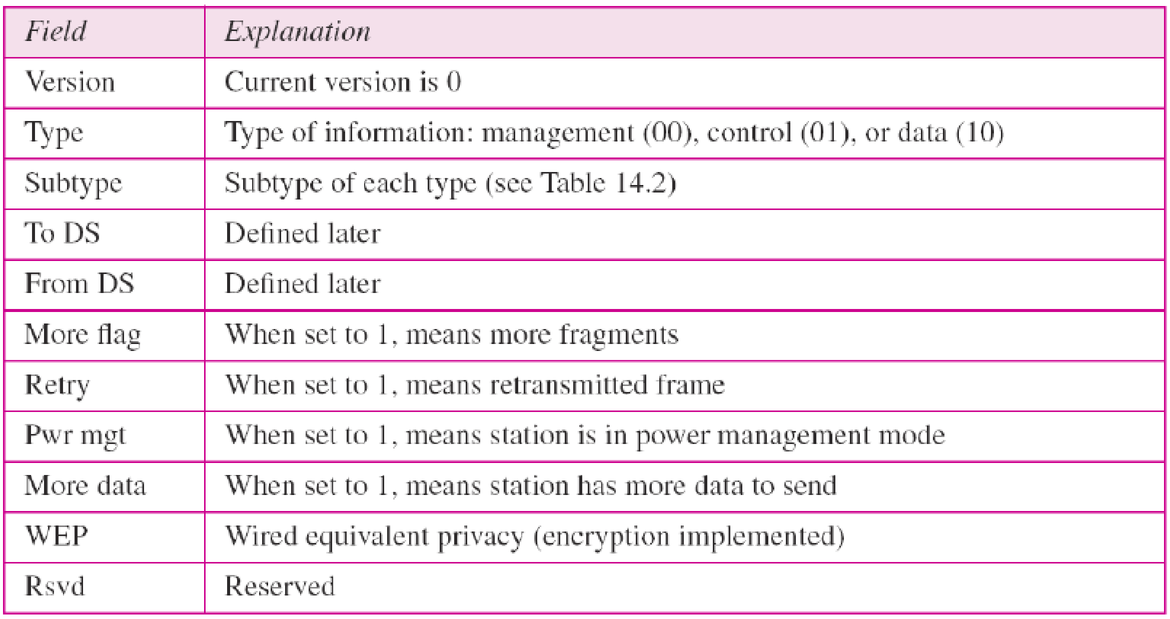
In the PCF, the Access point acting as a primary station, communicates with user device selecting as a secondary station. The primary station, AP sends a poll request for data and the secondary station responds with the data and acknowledgement for the poll request.



4.7.3 Frame format of IEEE 802.11



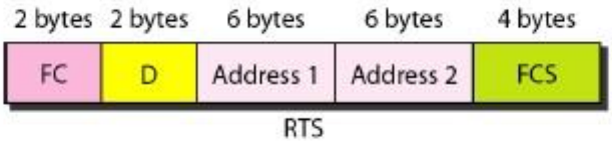
The Sub fields of Frame control (FC) is explained in the below table.

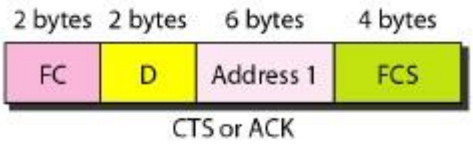


Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr 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

The second field ‘D’ represents 2 bytes of Delimiter where the destination is given with a sequence of ‘1’ to get synchronized with the source. The IEEE 802.11 has the frame body size vary from 0 bytes when the frame is meant of transferring control frames to 2312 bytes when the frame is used to transfer the user data. Last FCS, is used for error detection and correction purposes.

The format of three control frames RTS, CTS and ACK are as follows.





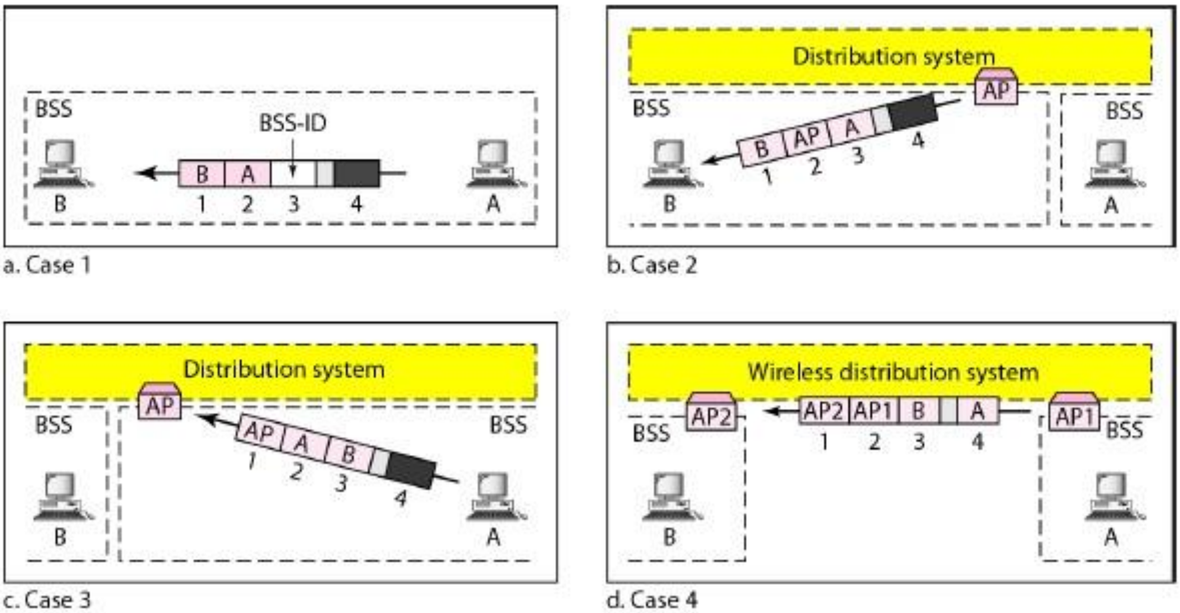
The values of subtype field in FC for control frames are represented as follows.

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

The values in addresses fields in IEEE 802.11 are as listed below.

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

The working of these addresses fields are shown in below figure.



a. Case 1

b. Case 2

c. Case 3

d. Case 4