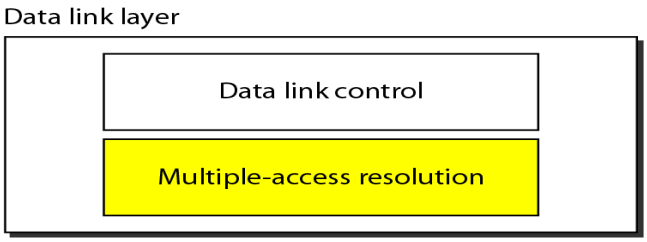
# UNIT – 4
# The Medium Access Control Sublayer

Data link layer is sub divided into 2 sublayers.

1. Data Link Control
2. MAC (Medium Access Control) sublayer




Data Link Control is responsible for flow and error control. MAC sub layer is responsible for resolving the access to shared media.

When two or more nodes transmit at the same time using a shared single media, their frames will collide and the link bandwidth is wasted during collision. The solution is we need a protocol to determine who goes next on a shared media. These protocols are called **Medium or Multiple Access Control (MAC) Protocols** belong to a **sublayer** of the data link layer called **MAC** (Medium Access Control).

MAC is important in LAN which use a multiaccess channel as the basis for communication.

## Channel Allocation Problem

There are 2 schemes to allocate a single channel among competing users.

1. Static Channel Allocation.
2. Dynamic Channel Allocation.

## Static Channel Allocation:

In this scheme FDM (Frequency Division Multiplexing) is used for allocating a single channel among competing users. If there are N users, the bandwidth is divided into N equal-sized portions, with each user being assigned one portion. Since each user has a private frequency band, there is now no interference among users.

When there is only a small and constant number of users, each of which has a steady stream or a heavy load of traffic, this division is a simple and efficient allocation mechanism. A wireless example is FM radio stations. Each station gets a portion of the FM band and uses it most of the time to broadcast its signal.

However, when the number of senders is large and varying or the traffic is bursty, FDM presents some problems. If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. And if more than N users want to communicate, some of them will be denied permission for lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever transmit or receive anything.

Even assuming that the number of users could somehow be held constant at *N*, dividing the single available channel into some number of static sub channels is inherently inefficient. The basic problem is that when some users are idle or inactive, their bandwidth is simply lost. They are not using it, and no one else is allowed to use it either. Consequently, most of the channels will be idle most of the time.

The poor performance of static FDM can easily be seen with a simple queueing theory calculation. Let us start by finding the mean time delay, T, to send a frame onto a channel of capacity C bps. We assume that the frames arrive randomly with an average arrival rate of $\lambda$ frames/sec, and that the frames vary in length

with an average length of 1/μ bits. With these parameters, the service rate of the channel is μC frames/sec. A standard queueing theory result is

$$T = \frac{1}{\mu C - \lambda}$$

This is only when there is no contention in the channel.

Now let us divide the single channel into N independent subchannels, each with capacity C/N bps. The mean input rate on each of the subchannels will now be λ/N. Recomputing T, we get

$$T_N = \frac{1}{\mu\left(\frac{C}{N}\right) - \left(\frac{\lambda}{N}\right)} = \frac{N}{\mu C - \lambda} = \mathrm{NT}$$

The mean delay for the divided channel is *N* times worse than if all the frames were somehow magically arranged orderly in a big central queue.

The other way of statically dividing the channel is TDM (Time Division Multiplexing). Allocate each user every $N^{th}$ time slot, if a user does not use allocated slot, it would be waste.

None of the traditional static channel allocation methods work well at all with bursty traffic.

## Assumptions for Dynamic Channel Allocation

1. Independent traffic
2. Single channel
3. Observable Collisions
4. Continuous or slotted time
5. Carrier sense or no carrier sense

- **Independent Traffic:**

– The model consists of *N* independent **stations** (e.g., computers, telephones, or personal communicators), each with a program or user that generates frames for transmission. Stations are sometimes called **terminals**.

– The probability of a frame being generated in an interval of length $\Delta t$ is $\lambda \Delta t$, where λ is a constant (the arrival rate of new frames).

– Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

- **Single Channel:**

– The single channel is available for all communication.
– All stations can transmit on it and all can receive from it.
– The stations are assumed to be equally capable though protocols may assign then different roles (i.e., priorities)

- **Observable Collisions:**

– If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled.
– This event is known as **collision**.
– All stations can detect that a collision has occurred. A collided frame must be retransmitted.

- **Continuous or Slotted Time:**

– Time may be assumed continuous. In which case frame transmission can begin at any instant.
– Alternatively, time may be slotted or divided into discrete intervals (called slots).
– Frame transmission must then 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 collision, respectively.

- **Carrier Sense or No Carrier Sense:**

– With the carrier sense assumption, stations can tell if the channel is in use before trying to use it.
– No station will attempt to use the channel while it is sensed as busy.
– If there is no carrier sense, stations cannot sense the channel before trying to use it.
– They will transmit then. Only later they can determine whether the transmission was successful.

## Multiple Access Protocols

- ALOHA
- Carrier Sense Multiple Access protocols
- Collision-free protocols
- Limited-contention protocols
- Wireless LAN protocols

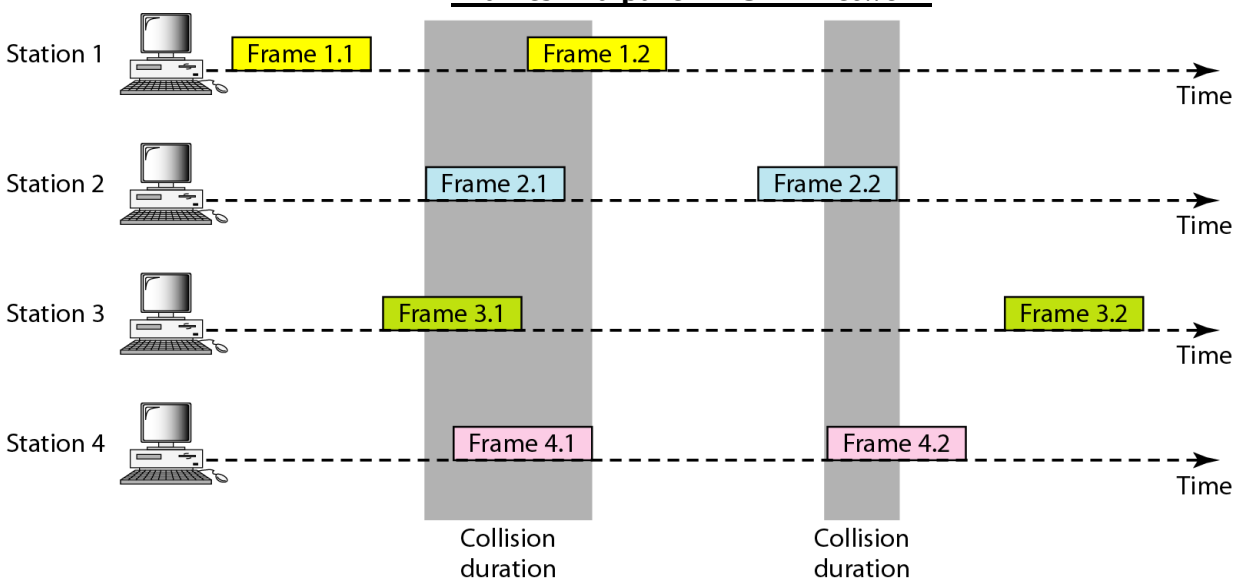
## ALOHA

- ALOHA is the random access method.
- It was developed at the University of Hawaii in early 1970.
- It was designed for radio (Wireless) LAN, but it can be used for any shared medium.
- There are two versions of ALOHA
    a) Pure ALOHA
    b) Slotted ALOHA

### Pure ALOHA

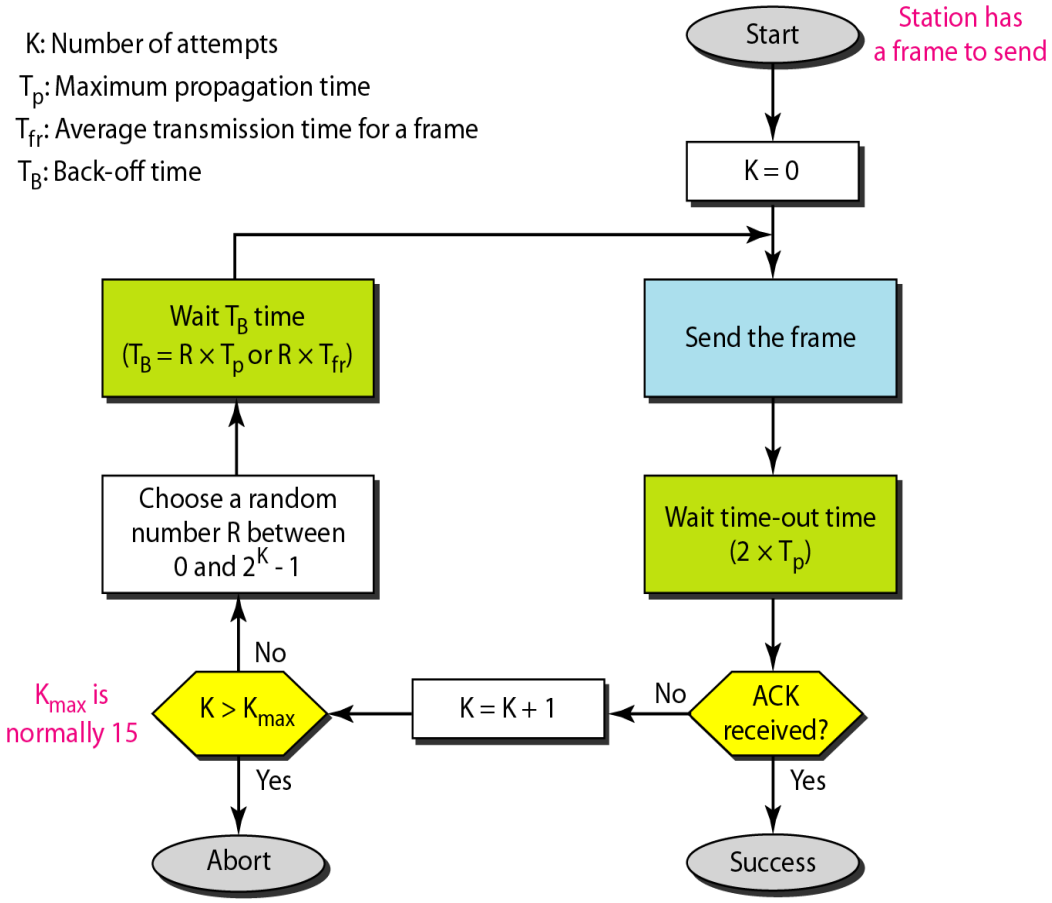
The original ALOHA protocol is called pure ALOHA. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations. The following figure shows an example of frame collisions in pure ALOHA.

**Frames in a pure ALOHA network**

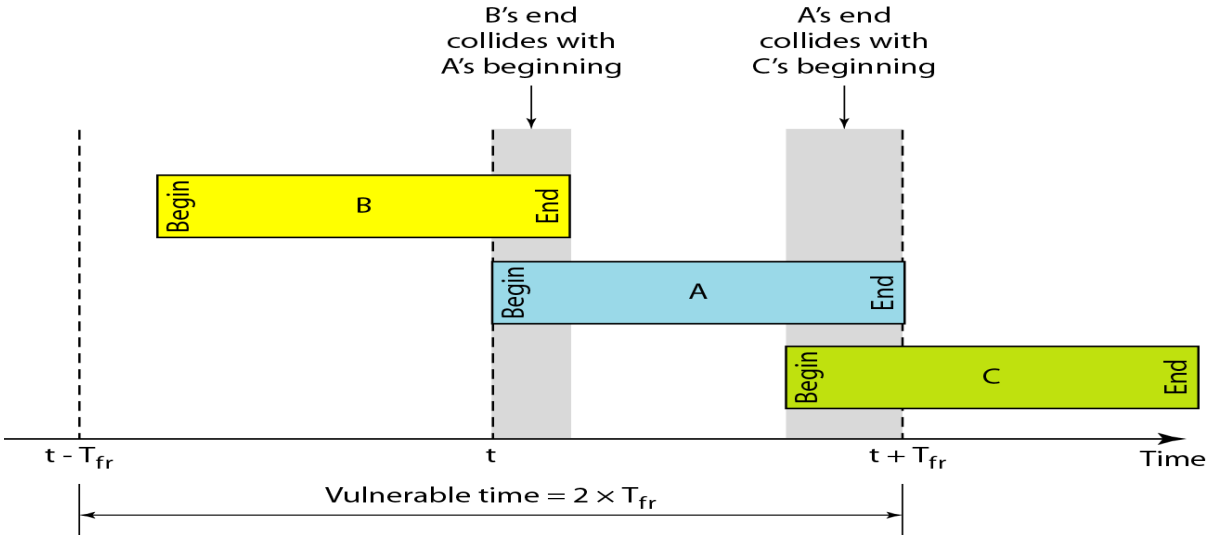


The colliding frames will be destroyed and we won't get acknowledgment regarding these destroyed frames. When all stations attempt to send again similar collisions will occur again. To avoid more collisions after timeout, each station waits for a random amount of time before resending the frame. This time is called as back-off time ($T_B$). To prevent congesting the channel with retransmitted frame, after a maximum number of transmissions $K_{max}$, a station must give up and try later.

**Procedure for pure ALOHA protocol**




**Vulnerable time:** Vulnerable time is the length of the time in which there is a possibility of collision.




The vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.

The throughput ( S) for pure ALOHA is $S = G \times e^{-2G}$ . Throughput means average number of successful transmissions.

The maximum throughput $S_{max} = 0.184$ when G= (1/2).

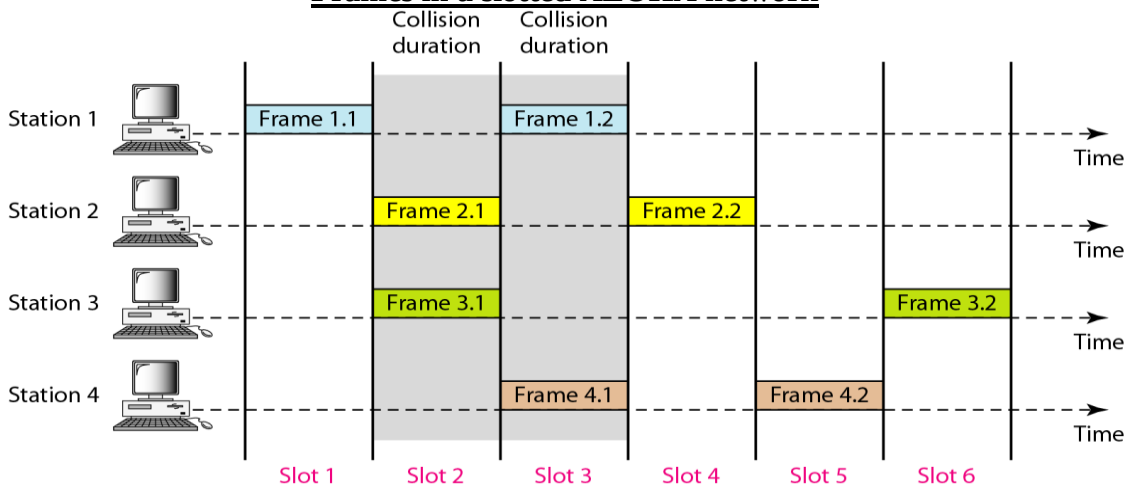
G = Average number of frames generated by the system (all stations) during one frame transmission time.

## Slotted ALOHA

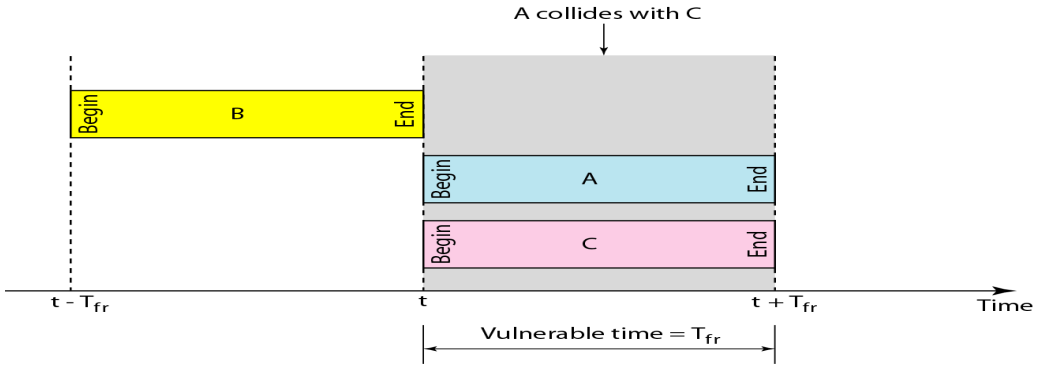
Pure ALOHA has a vulnerable time of 2 X $T_{fr}$. This is so because there is no rule that defined when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

In slotted ALOHA we divide the time into slots of $T_{fr}$ and force the station to send only at the beginning of the time slot. The following figure shows an example of frame collisions in slotted ALOHA.

**Frames in a slotted ALOHA network**




Because a station is allowed to 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. There is still possibility of collision if two stations try to send at the beginning of the same time slot. The **vulnerable time** is reduced to one-half that of pure ALOHA i.e $T_{fr}$.




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

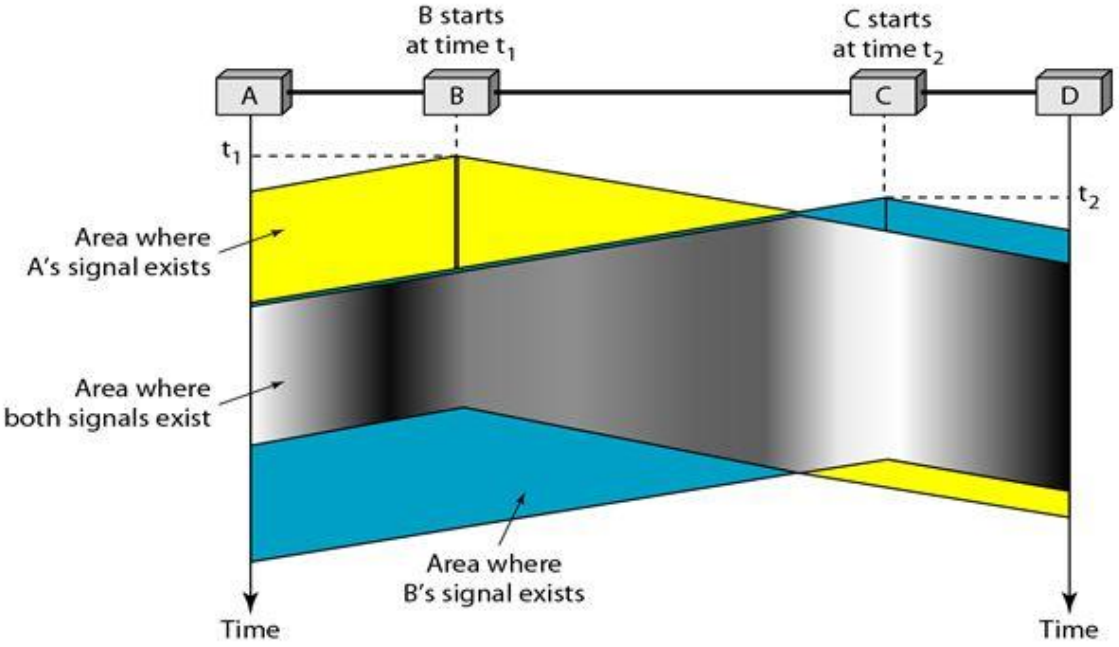
The maximum throughput $S_{max} = 0.368$ when G = 1.

## 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 cannot eliminate it. The reason for this is shown in Figure

The possibility of collision still exists because of propagation delay. When a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. In other words, a

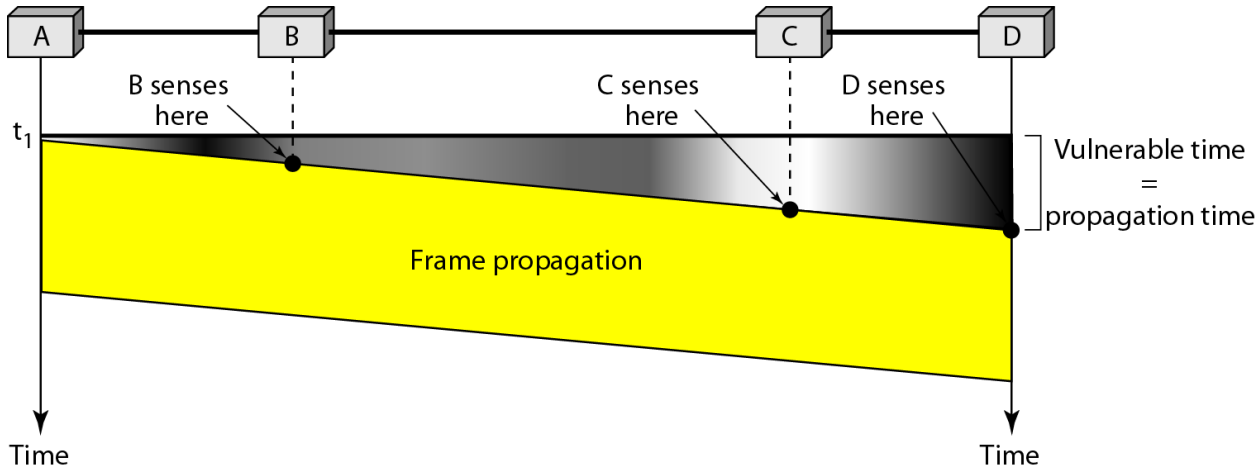
station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received. At time t1 station B senses the medium and finds it idle, so it sends a frame. At time t2 *(t2> t1)* station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.




## Vulnerable Time

The vulnerable time for CSMA is the propagation time Tp . This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.

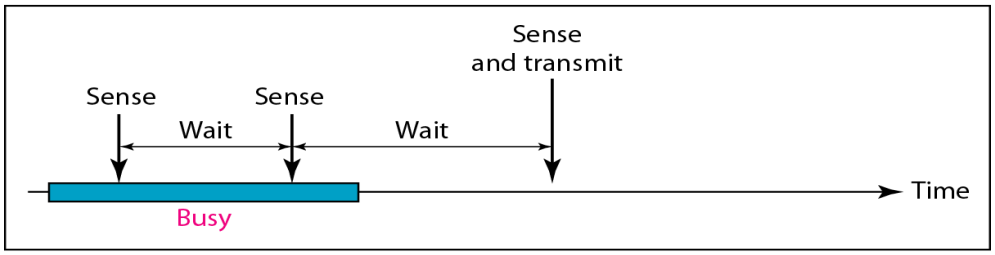
**Vulnerable time in CSMA**



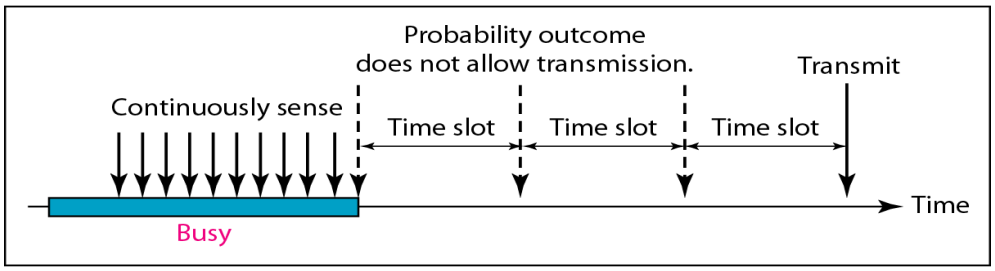

## Persistence Methods

What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been designed to answer these questions: the 1-persistent method, the nonpersistent method, and the p-persistent method. The following Figure shows the behavior of three persistence methods when a station finds a channel busy.


a. 1-persistent




b. Nonpersistent




c. p-persistent

**1-Persistent:** The **1-persistent method** is simple and straightforward. In this method, after the station finds the line idle, it sends 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.

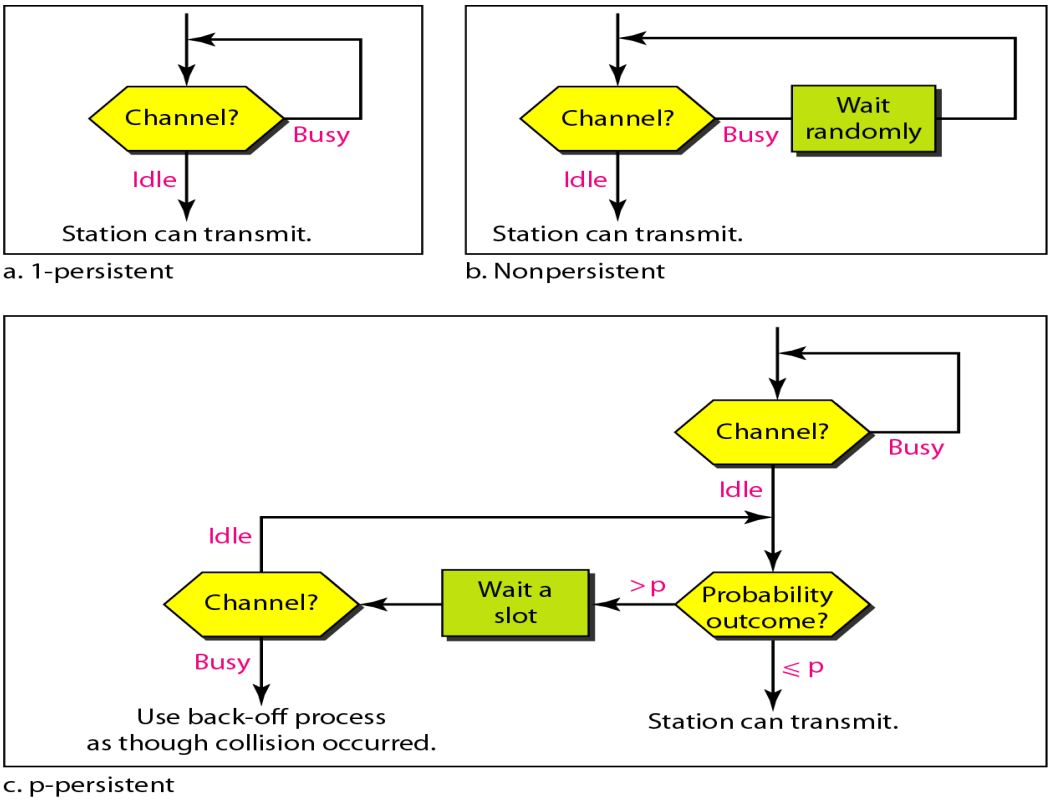
**Nonpersistent:** In the **nonpersistent method,** a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

**p-Persistent:** The **p-persistent method** is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It 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.

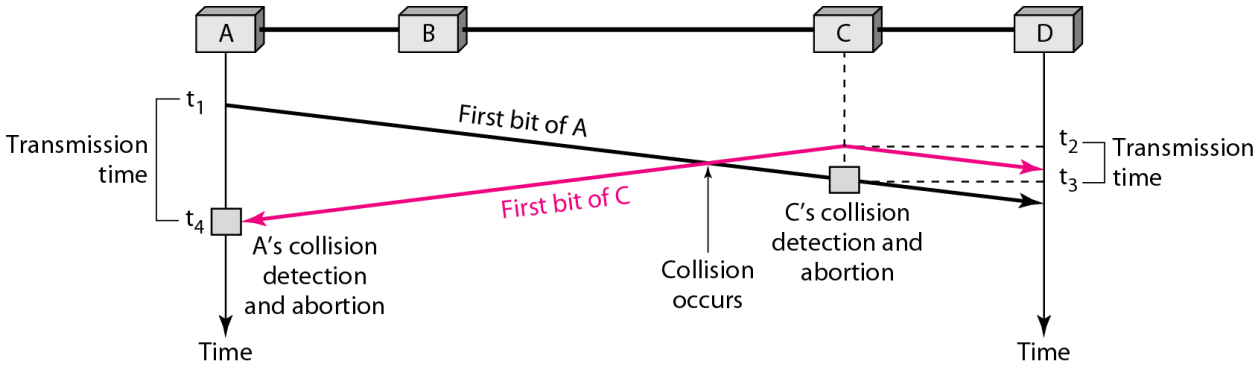
    a. If the line is idle, it goes to step 1.
    b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

## Flow diagram for three persistence methods



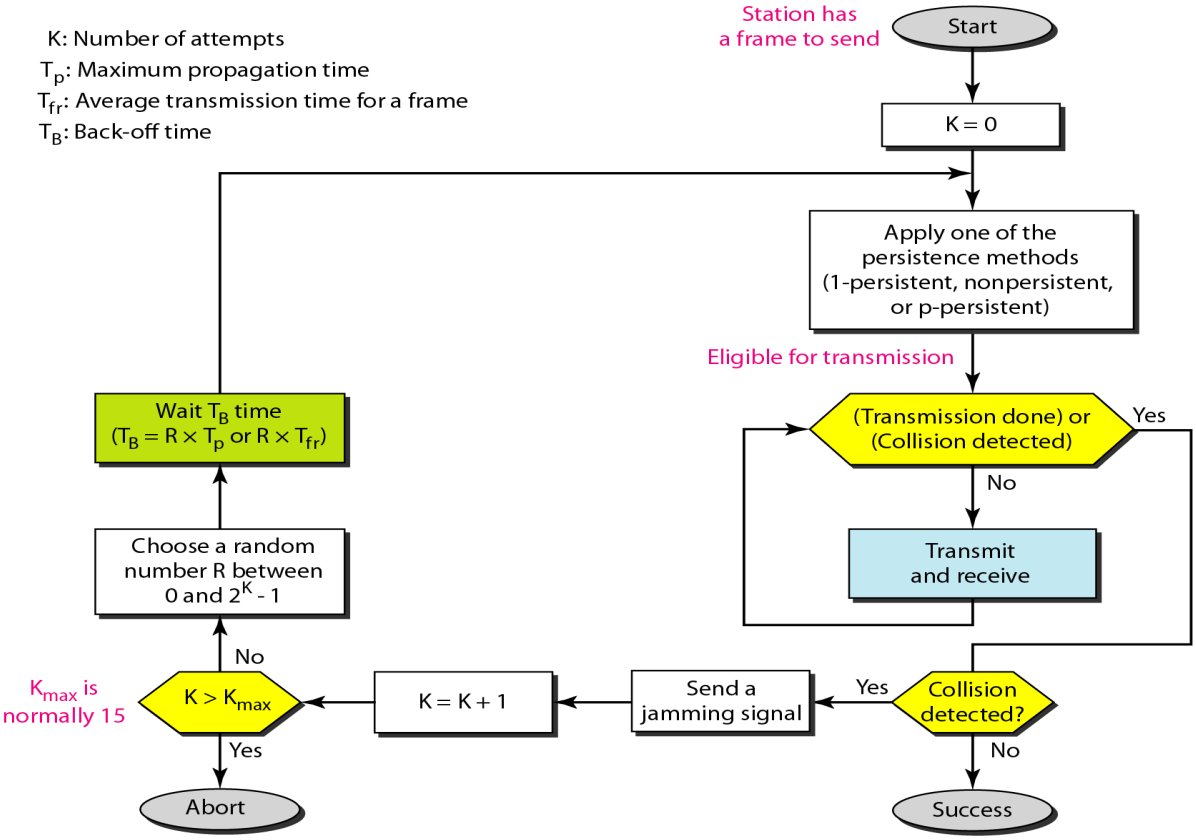

## Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

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.




At time *t* 1, 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 diagram for the CSMA/CD



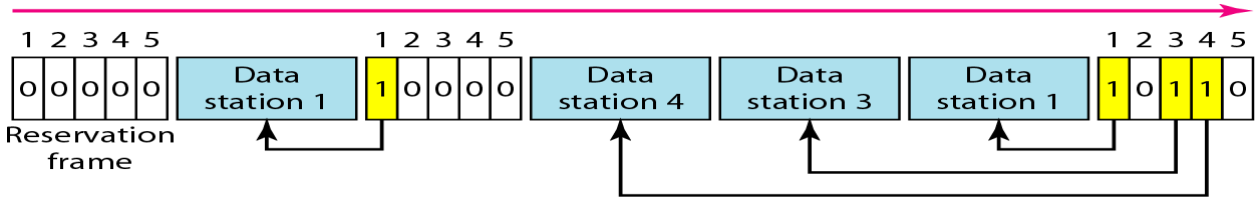

## Collision-Free Protocols

### A Bit-Map Protocol or Reservation:

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

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

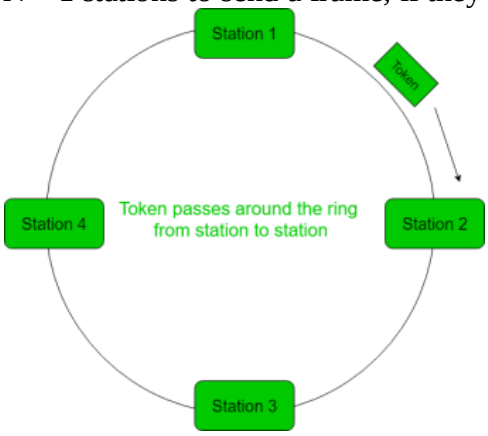
The following Figure shows a situation with five stations and a five-minislot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.




### Token Passing:

- In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in the some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas in case of Token bus, each station uses the bus to send the token to the next station in some predefined order.

- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbors and the other N – 1 stations to send a frame, if they have one.




**Binary Countdown:**

In this protocol, a node which wants to signal that it has a frame to send does so by writing its address into the header as a binary number. The arbitration is such that as soon as a node sees that a higher bit position that is 0 in its address has been overwritten with a 1, it gives up. The final result is the address of the node which is allowed to send. After the node has transmitted the whole process is repeated all over again. Given below is an example situation.

| Nodes | Addresses |
|---|---|
| A | 0010 |
| B | 0101 |
| C | 1010 |
| D | 1001 |
| | ---- |
| | 1010 |

Node C having higher priority gets to transmit. The problem with this protocol is that the nodes with higher address always wins. Hence this creates a priority which is highly unfair and hence undesirable.

## Limited Contention Protocols

Both the type of protocols described above - Contention based and Contention - free has their own problems. Under conditions of light load, contention is preferable due to its low delay. As the load increases, contention becomes increasingly less attractive, because the overload associated with channel arbitration becomes greater. Just the reverse is true for contention - free protocols. At low load, they have high delay, but as the load increases, the channel efficiency improves rather than getting worse as it does for contention protocols.

Obviously it would be better if one could combine the best properties of the contention and contention - free protocols, that is, protocol which used contention at low loads to provide low delay, but used a contention-free technique at high load to provide good channel efficiency. Such protocols do exist and are called Limited contention protocols.

It is obvious that the probability of some station acquiring the channel could only be increased by decreasing the amount of competition. The limited contention protocols do exactly that. They first divide the stations up into (not necessarily disjoint ) groups. Only the members of group 0 are permitted to compete for slot 0. The competition for acquiring the slot within a group is contention based. If one of the members of that group succeeds, it acquires the channel and transmits a frame. If there is collision or no

node of a particular group wants to send then the members of the next group compete for the next slot. The probability of a particular node is set to a particular value (optimum).

**Adaptive Tree Walk Protocol**

The following is the method of adaptive tree protocol. Initially all the nodes are allowed to try to acquire the channel. If it is able to acquire the channel, it sends its frame. If there is collision then the nodes are divided into two equal groups and only one of these groups compete for slot 1.

If one of its member acquires the channel then the next slot is reserved for the other group. On the other hand, if there is a collision then that group is again subdivided and the same process is followed. This can be better understood if the nodes are thought of as being organized in a binary tree as shown in the following figure.

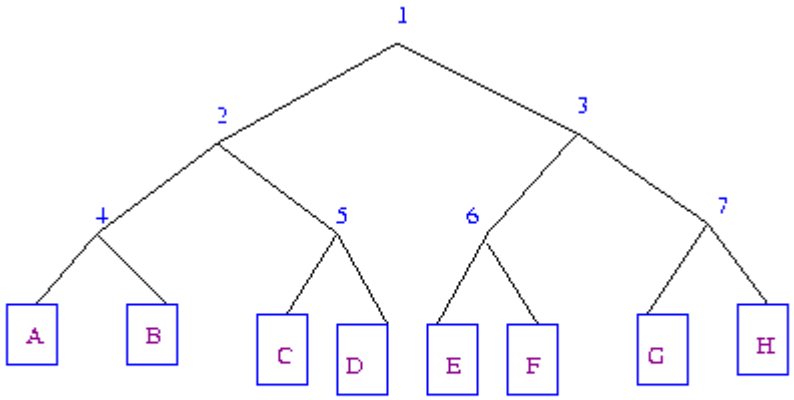
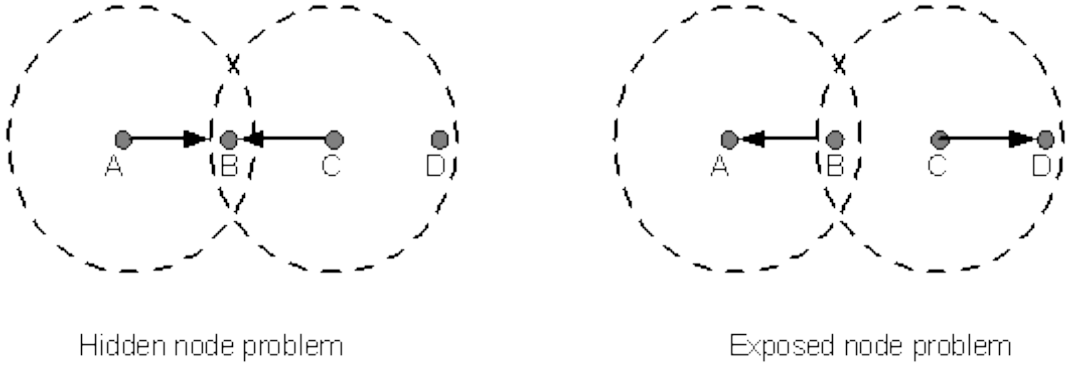



Fig. Adaptive Tree Walk abstraction of nodes in binary tree.

## Wireless LAN Protocols

A system of laptop computers that communicate by radio can be regarded as a wireless LAN. Wireless systems cannot normally detect a collision while it is occurring. A station on a wireless LAN may not be able to transmit frames to or receive frames from all other stations because of the limited radio range of the stations. In wired LANs, when one station sends a frame, all other stations receive it. The absence of this property in wireless LANs causes a variety of complications.




Hidden node problem  Exposed node problem

**Hidden Node Problem**

Consider the situation depicted in the figure, where each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right. For example, B can exchange frames with A and C but it cannot reach D, while C can reach B and D but not A. (A and D's reach is not shown in the figure.) Suppose both A and C want to communicate with B and so they each send it a frame. A and C are unaware of each other since their signals do not carry that far. These two frames collide with each other at B, but unlike an Ethernet, neither A nor C is aware of this collision. A and C are said to be hidden nodes with respect to each other.

Hidden node problem can be defined as "In wireless networking, the **hidden node problem or hidden terminal problem** occurs when a node is visible to a wireless access point (AP), but not to other nodes communicating with that AP."

**Collision cannot be detected in hidden node problem**

This is because the nodes **A** and **C** are out of range of each other(and so cannot detect a collision while transmitting). Thus, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur. The data received by the access point is corrupted due to the collision. To overcome the hidden node problem, RTS/CTS handshaking (IEEE 802.11 RTS/CTS) is implemented in addition to the Carrier sense multiple access with collision avoidance (CSMA/CA) scheme.

**Exposed Node Problem**

A related problem, called the exposed node problem, occurs under the following stated circumstances:
Suppose B is sending to A (as in the above Figure). Node C is aware of this communication because it hears B's transmission. It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission. For example, suppose C wants to transmit to node D. This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.

We address these problems by an algorithm known as Multiple Access with Collision Avoidance (MACA). The sender and receiver exchange frames with each other before transmitting data. This informs all nearby nodes that a transmission is about to begin. Sender transmits **Request to Send (RTS)** frame to receiver. The receiver then replies with **clear to send (CTS)** frame back to the sender. Any node that receives CTS frame knows that it is close to the receiver, therefore, cannot transmit a frame. Any node that receives RTS frame but not the CTS frame knows that is not close to the receiver to interfere with it, so it is free to transmit data.

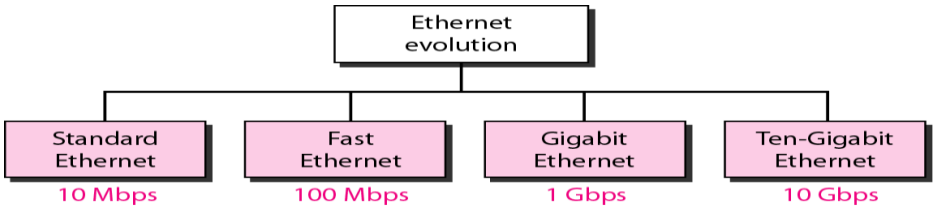
## ETHERNET

The LAN market has seen several technologies such as Ethernet, Token Ring, Token Bus, FDDI, and ATM LAN. Some of these technologies survived for a while, but Ethernet is by far the dominant technology. The most important of the survivors are IEEE 802.3(Ethernet) and IEEE 802.11(Wireless LAN).

Two kinds of Ethernet exist

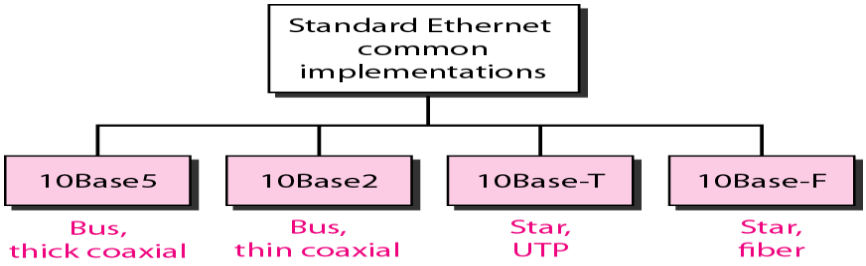
a) Classic Ethernet or Standard Ethernet.
b) Switched Ethernet.

Classic Ethernet run at 3 to 10Mbps. Switched Ethernet, in which devices called switches are used to connect different computers. It runs at 100,1000,10000 Mbps in the form of Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet.



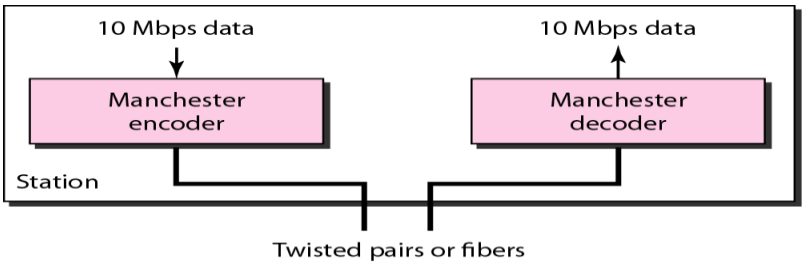

**Classic Ethernet Physical Layer:**

The Standard Ethernet or Classic Ethernet defines several physical layer implementations. Four of the most common, are shown in the following Figure.



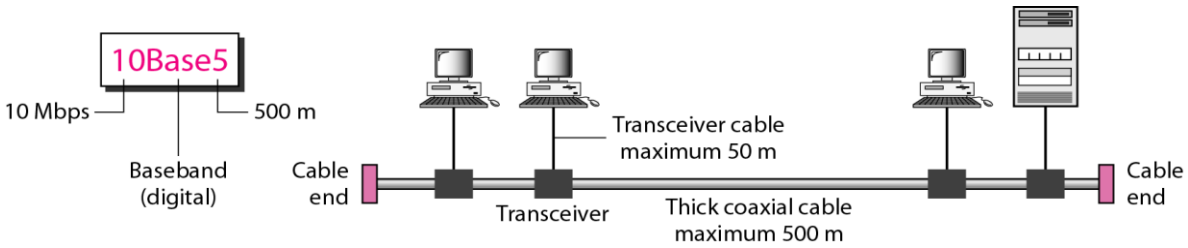
**Encoding and Decoding**

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 following Figure shows the encoding scheme for Standard Ethernet.




**10Base5:** Thick Ethernet

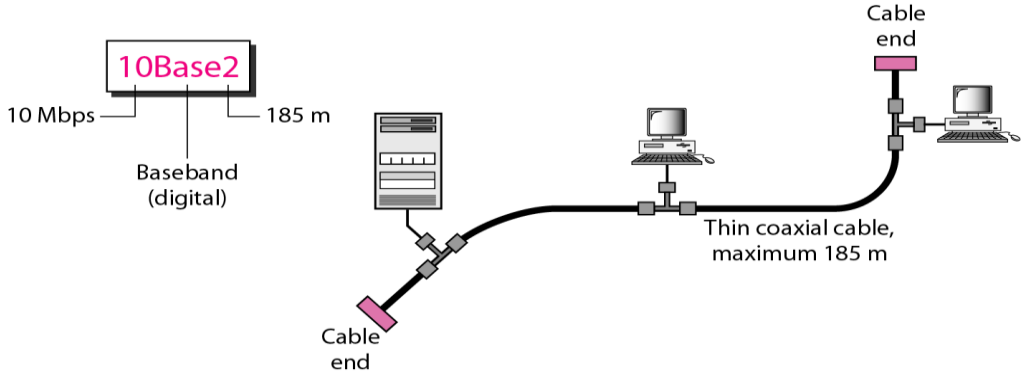
The first implementation is called 10Base5, thick Ethernet, or Thicknet. The nickname derives from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands. 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable.




The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable. The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive degradation of the signal. If a length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

**10Base2: Thin Ethernet**

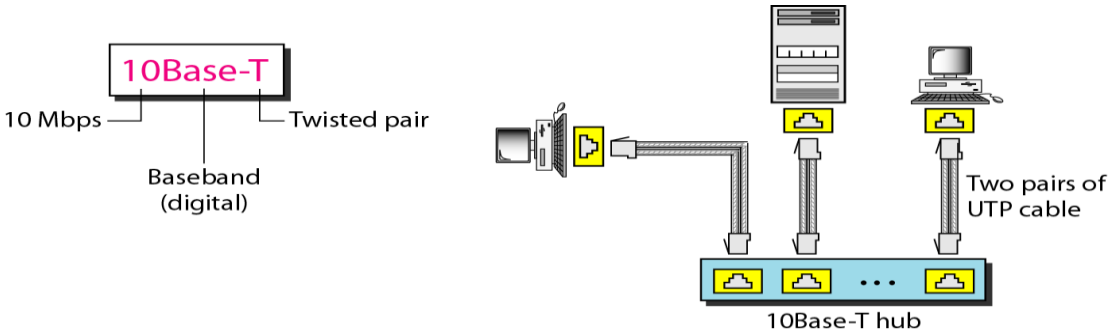
The second implementation is called 10Base2, thin Ethernet, or Cheapernet. 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.




Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

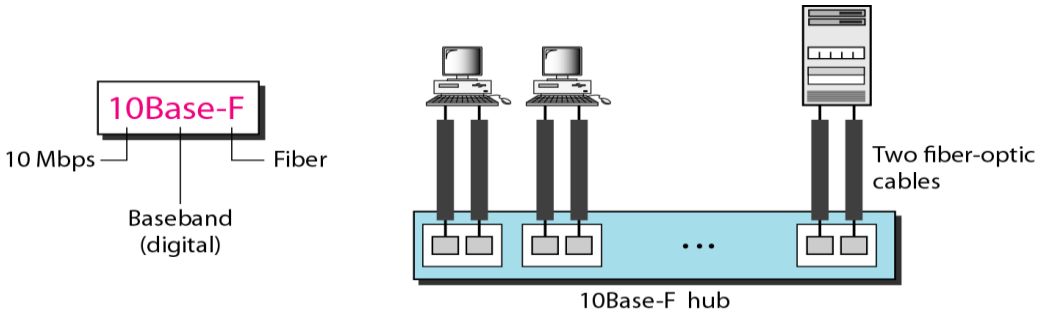
**10Base-T: Twisted-Pair Ethernet**

The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable, as shown in the following Figure. Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.




**10Base-F: Fiber Ethernet**

Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F. 10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables, as shown in Figure.




## Summary of Standard Ethernet implementations

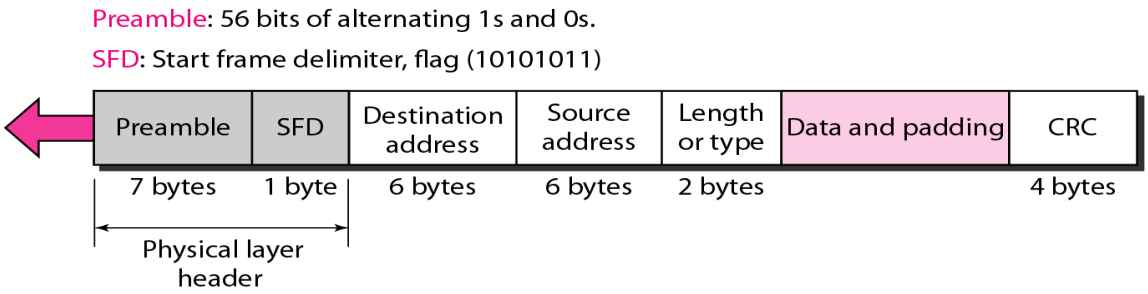
| *Characteristics* | *10Base5* | *10Base2* | *10Base-T* | *10Base-F* |
|---|---|---|---|---|
| Media | Thick coaxial cable | Thin coaxial cable | 2 UTP | 2 Fiber |
| Maximum length | 500 m | 185 m | 100 m | 2000 m |
| Line encoding | Manchester | Manchester | Manchester | Manchester |

## MAC Sublayer

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

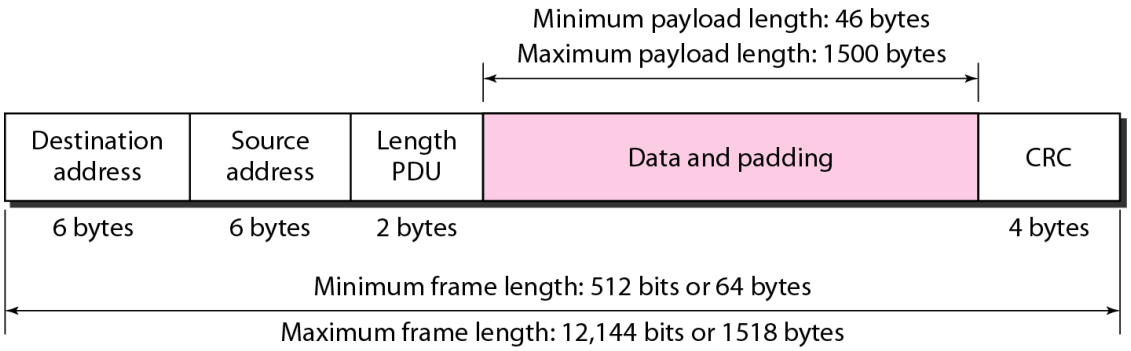
**Frame Format:**

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. The format of the MAC frame is shown in the following Figure.




- **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 preamble is actually added at the physical layer and is not (formally) part of the frame.
- **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.
- **Destination address (DA**): The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Source address (SA**): The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **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.
- **Data:** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes, as we will see later.
- **CRC**: The last field contains error detection information, in this case a CRC-32.

## Frame Length




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 (without preamble and SFD field) 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.

## 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.

## Goals of Fast Ethernet:

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.

## MAC Sublayer:

- Main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched.
- **Drop bus topologies** and keep only the **star topology**.
- For the star topology, there are two choices, as we saw before: **half duplex** and **full duplex**.

In Half-duplex approach:

- The stations are connected via a hub.
- The access method is CSMA/CD

Full-duplex approach

- The connection is made via a switch with buffers at each port.
- No need for CSMA/CD

## Autonegotiation:

- A new feature added to Fast Ethernet is called autonegotiation.
- It allows a station or a hub a range of capabilities.
- Autonegotiation allows two devices to negotiate the mode or data rate of operation.
- It was designed particularly for the following purposes:
    1. To allow incompatible devices to connect to one another. For example, a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but can work at a lower rate).
    2. To allow one device to have multiple capabilities.
    3. To allow a station to check a hub's capabilities.

## Physical layer:

- The physical layer in Fast Ethernet is more complicated than the one in Standard Ethernet.

## Topology:

- Fast Ethernet 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.

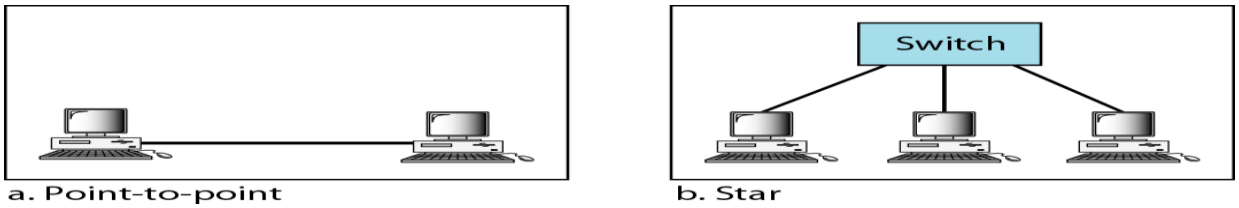



**Figure: Fast Ethernet topology**

## Fast Ethernet implementations:

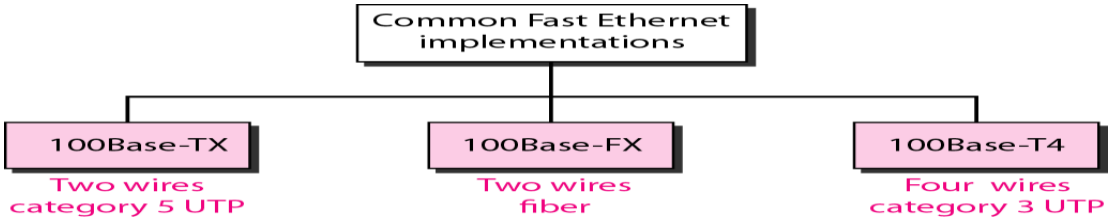



**Figure: Fast Ethernet implementations**

### 100Base-TX:

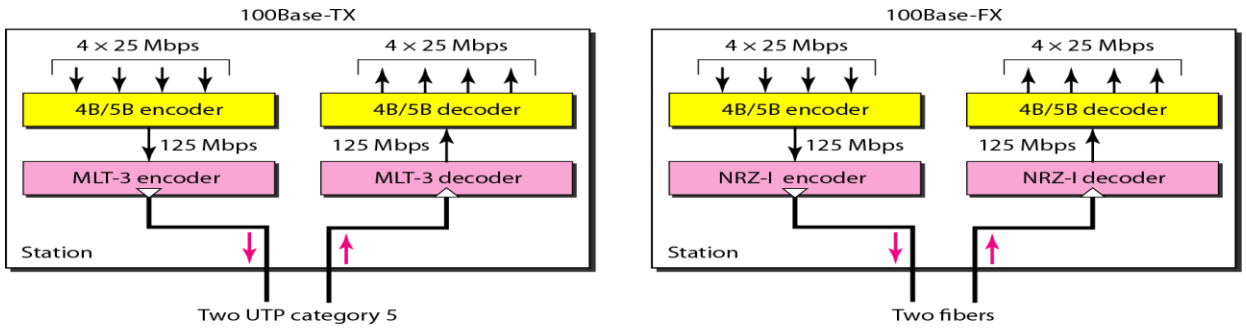
- It uses two pairs of twisted-pair cable (either category 5 UTP or STP (Shielded twisted pair).
- For this implementation, the MLT-3(Multi Level Transmit) scheme was selected since it has good bandwidth performance.
- 4B/5B block coding is used to provide bit synchronization by preventing the occurrence of a long sequence of 0s and 1s.
- This creates a data rate of 125 Mbps, which is fed into MLT-3 for encoding.

### 100Base-FX:

- Uses two pairs of fiber-optic cables.
- Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes.
- Uses NRZ-I(Non-Return-to-Zero Inverted) encoding scheme ( bit synchronization problem.)
- To overcome this problem, 4B/5B block coding is used.
- A 100Base-TX network can provide a data rate of 100 Mbps, but it requires the use of category 5 UTP or STP cable. It is cost effective.

### 100Base-T4:

- Uses four pairs of category 3 or higher UTP.(not cost efficient compared to Category 5)
- Transmit 100 Mbps.
- Uses 8B/6T encoding.
- Each twisted pair cannot easily handle more than 25 Mbaud.
- As one pair switches between sending and receiving, three pairs of UTP category 3 can handle only 75 Mbaud (25 Mbaud each).
- Thus it requires an encoding scheme that converts 100 Mbps to a 75 Mbaud signal. This is done by using 8B/6T (eight binary/six ternary) encoding scheme.



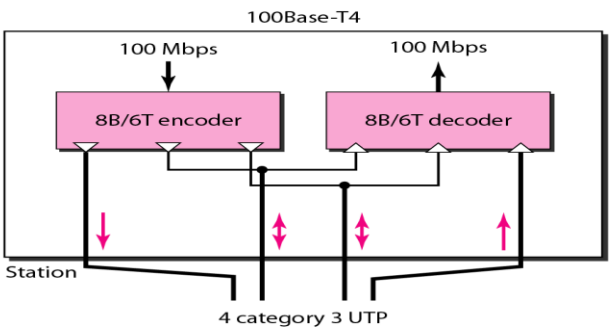



**Figure: Encoding for Fast Ethernet implementation**

| *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 |

**Table:** ***Summary of Fast Ethernet implementations***

## 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 802.3z.

### The goals of the Gigabit Ethernet

- Upgrade the data rate to 1 Gbps.
- Make it compatible with Standard or Fast Ethernet.
- Use the same 48-bit address.
- Use the same frame format.
- Keep the same minimum and maximum frame lengths.
- To support auto negotiation as defined in Fast Ethernet.

### MAC Sublayer

MAC sub layer remains almost same in Gigabit Ethernet. There are two distinct approaches for medium access: half-duplex and full duplex.

**In full duplex mode**

a) There is no collision and CSMA/CD is not used.
(b) Each computer is connected to central switch or other switches as shown in fig.
(c) In this mode, each switch has buffers for each input port in which data are stored until they are transmitted.
(d) The maximum length of the cable is determined by the signal attenuation in the cable.

**• In Half duplex mode**

(a) Switch is not used rather a hub is used.
(b) All the collisions occur in this hub.
(c) To control this, CSMA/CD approach is used.
(d) The maximum length of the network in this approach is totally dependent on the minimum frame size.

Three methods have been defined

1. Traditional
2. Carrier Extension
3. Frame Bursting

**Traditional** In the traditional approach, we keep the minimum length of the frame as in traditional Ethernet (512 bits). However, because the length of a bit is 1/100 shorter in Gigabit Ethernet than in 10-Mbps Ethernet, the slot time for Gigabit Ethernet is 512 bits × 1/1000 μs, which is equal to 0.512 μs. The reduced slot time means that collision is detected 100 times earlier. This means that the maximum length of the network is 25 m. This length may be suitable if all the stations are in one room, but it may not even be long enough to connect the computers in one single office.

**Carrier Extension** To allow for a longer network, we increase the minimum frame length. The **carrier extension** approach defines the minimum length of a frame as 512 bytes (4096 bits). This means that the minimum length is 8 times longer. This method forces a station to add extension bits (padding) to any frame that is less than 4096 bits. In this way, the maximum length of the network can be increased 8 times to a length of 200 m. This allows a length of 100 m from the hub to the station.

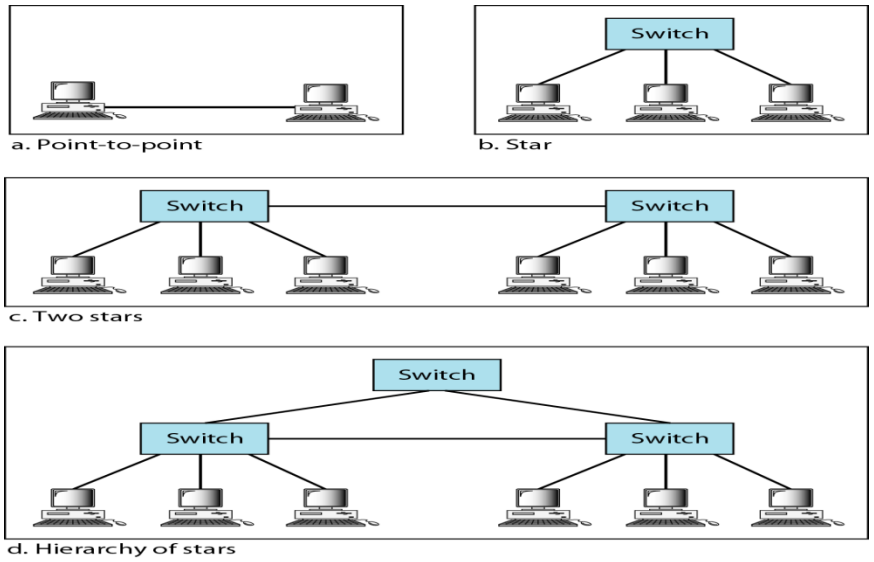
**Frame Bursting** Carrier extension is very inefficient if we have a series of short frames to send; each frame carries redundant data. To improve efficiency, **frame bursting** was proposed. Instead of adding an extension to each frame, multiple frames are sent. However, to make these multiple frames look like one frame, padding is added between the frames (the same as that used for the carrier extension method) so that the channel is not idle. In other words, the method deceives other stations into thinking that a very large frame has been transmitted.

## Physical layer

The Physical layer in Gigabit Ethernet is more complicated than in Standard or Fast Ethernet.

### Topology

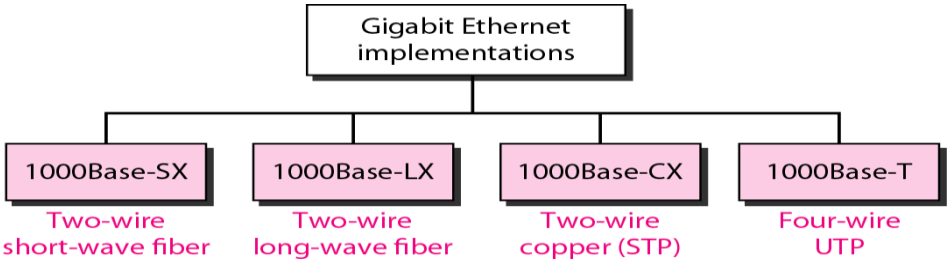
- In Gigabit Ethernet, two or more stations can be connected.
- Only two stations can be connected in point to point mode as shown in fig.
- Multiple stations (two or more) can be connected in a star topology with a switch or hub.
- The various possible implementations are shown in fig.




a. Point-to-point
b. Star
c. Two stars
d. Hierarchy of stars

**Physical layer implementation**

- Two different implementation of Gigabit Ethernet are two wires and a four Wire.
- Two wire implementation uses fiber optic cable. The various two Wire implementations are 1000Base-SX, 1000Base-LX, 1000Base-CX
- Four wire implementation uses category 5 twisted pair cable. It includes 100 Base-T.




**1000 Base-SX**

- It uses multimode optical fiber with 2 wires.
- It uses short wave laser.
- The maximum length of segment supported by 1000Base-SX is 550 meters.
- It uses 8B/10B block encoding and NRZ line encoding as shown in Fig.

**1000 Base-LX**

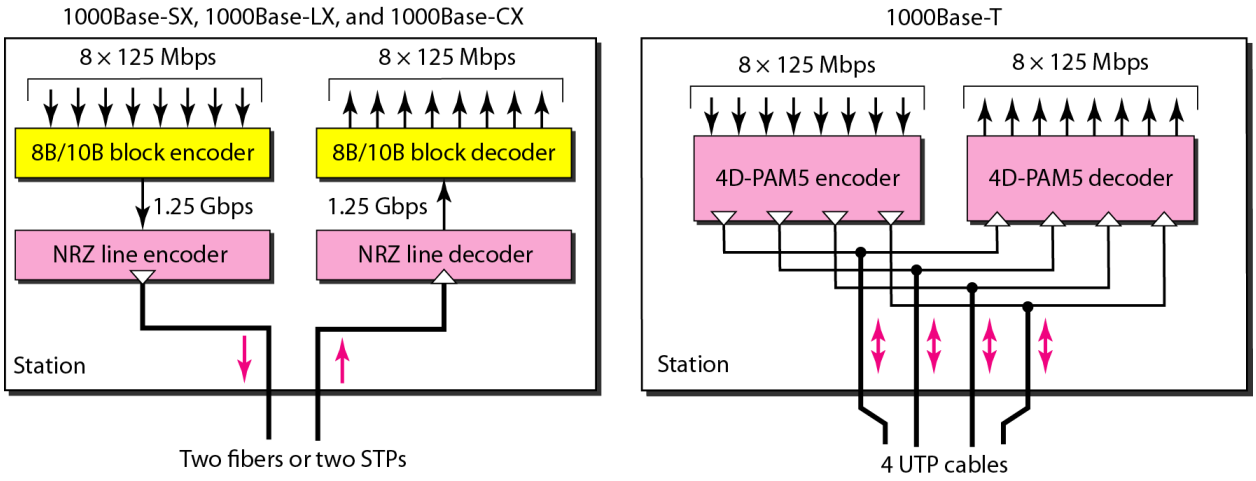
- It uses multimode or single mode optical fiber (2 wires).
- It makes use of long wave laser.
- The maximum length of segment supported is 550 meters (in multimode) and 5000 meters (in single mode).
- It also uses 8B/10B block encoding with NRZ line encoding.

**1000 Base-CX**

- It uses shielded twisted pair cable (2 wires) that carry electrical signal.
- The maximum length of segment supported by it is~5 meters.
- It also uses 8B/6B blocking encoding and NRZ line encoding.

**1000 Base-T**

- It uses category 5 UTP (4 wires).
- The maximum segment length supported is 100 meters.
- It makes use of 4D-P AM5 encoding to reduce the bandwidth.
- In 4D-PAM 5 encoding, are four wires are evolved input and output.
- Each wire carries 250 Mbps which is in the range for cat 5 UTP cable.




***Encoding in Gigabit Ethernet implementations***

| *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 |

**Summary of Gigabit Ethernet implementations**

## Ten-Gigabit Ethernet:

- The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae.

**The goals of the Ten-Gigabit Ethernet**

- Upgrade the data rate to 10 Gbps.
- Make it compatible with Standard, Fast, and Gigabit Ethernet.
- Use the same 48-bit address.
- Use the same frame format.
- Keep the same minimum and maximum frame lengths.
- Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
- Make Ethernet compatible with technologies such as Frame Relay and ATM.

### *MAC Sublayer*

Ten-Gigabit Ethernet operates only in full duplex mode which means there is no need for contention; CSMA/CD is not used in Ten-Gigabit Ethernet.

### *Physical Layer*

The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: **10GBase-S, 10GBase-L,** and 10G Base-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 |

**Summary of Ten-Gigabit Ethernet implementations**

## IEEE-802.11:

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

### Architecture:

- The standard defines two kinds of services:
  1. The basic service set (BSS)
  2. The extended service set (ESS)
- 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).
- 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**.

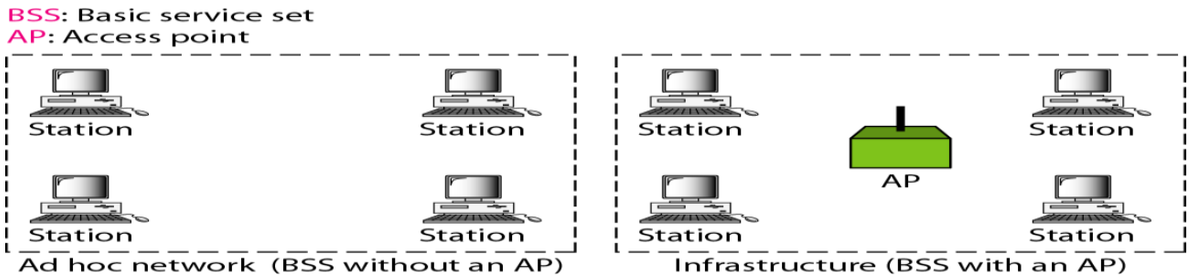



**FIGURE: BASIC SERVICE SETS (BSSS)**

### 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.

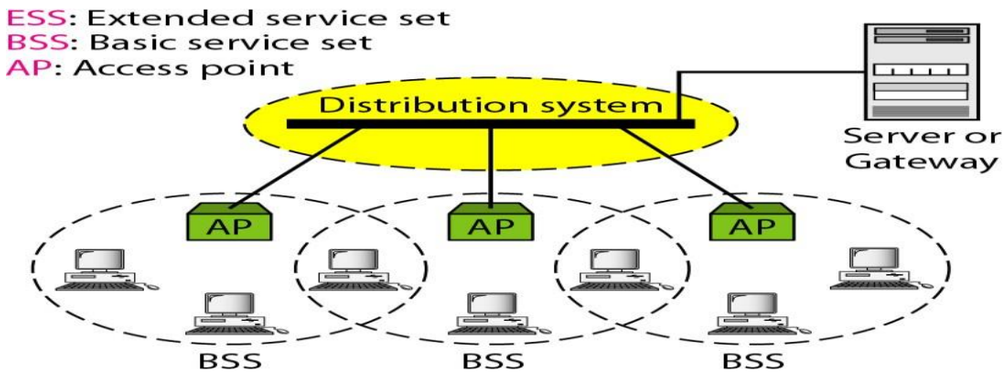



**Figure: Extended service sets (ESSs)**

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

### Station Types:

- IEEE 802.11 defines **three** types of **stations** based on their mobility in a wireless LAN:
  1. no-transition 2. BSS transition 3. ESS-transition mobility
- A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
- A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- A station with ESS-transition mobility can move from one ESS to another.
- However, IEEE 802.11 does not guarantee that communication is continuous during the move.

## MAC Sublayer:

- IEEE 802.11 defines **two** MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).

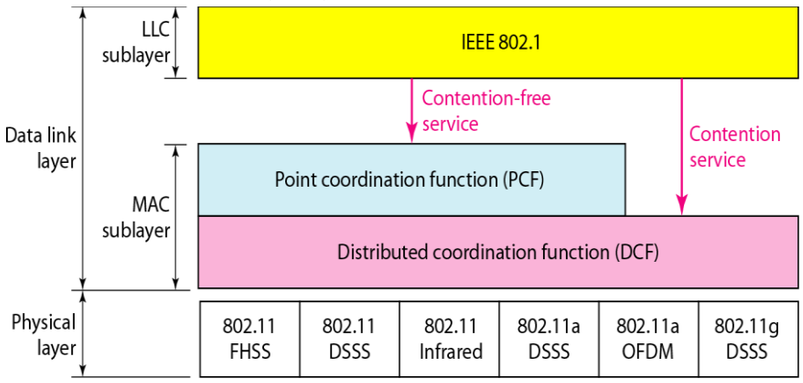
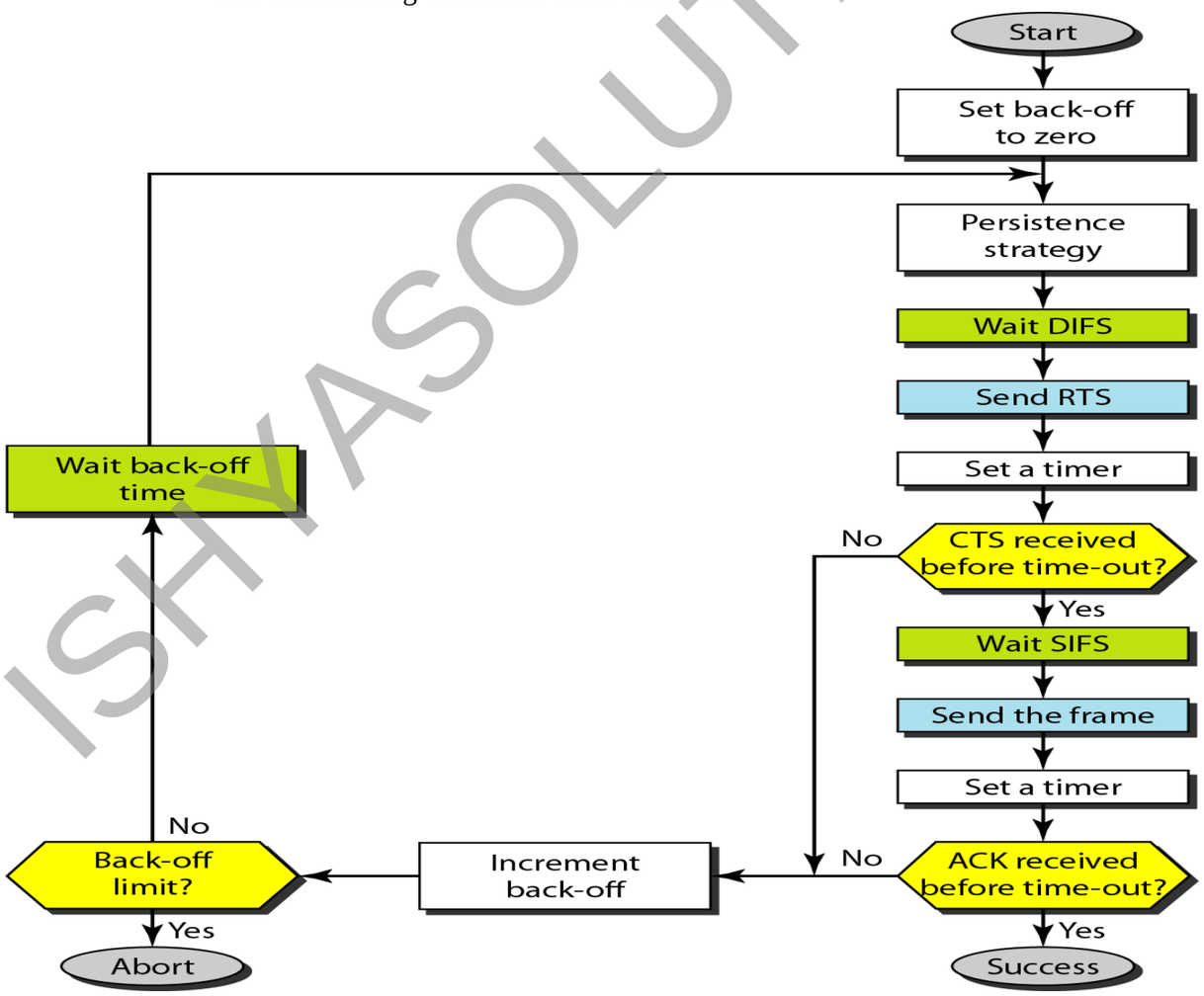


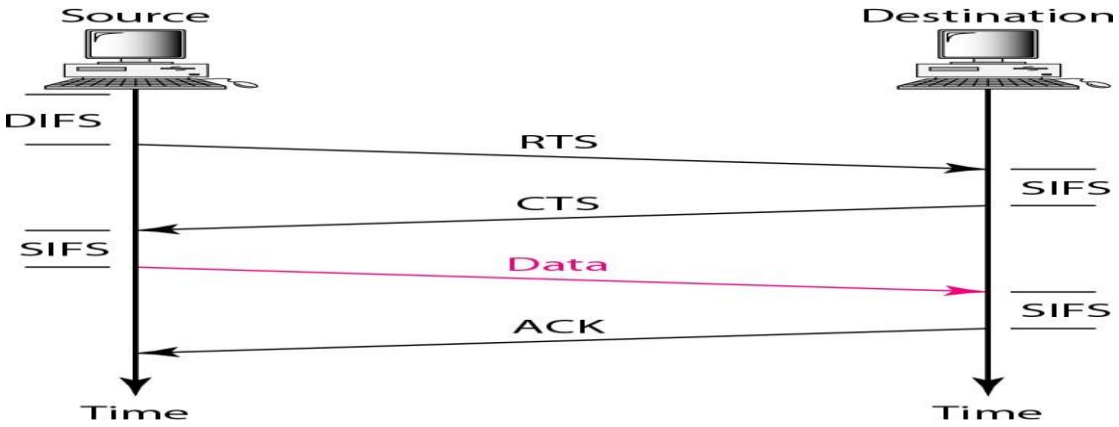

**Figure: MAC layers in IEEE 802.11 standard Distributed Coordination Function:**

- DCF uses CSMA/CA as the 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. This can mean costly stations and increased bandwidth requirements.
    2. Collision may not be detected because of the hidden station problem.
    3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.



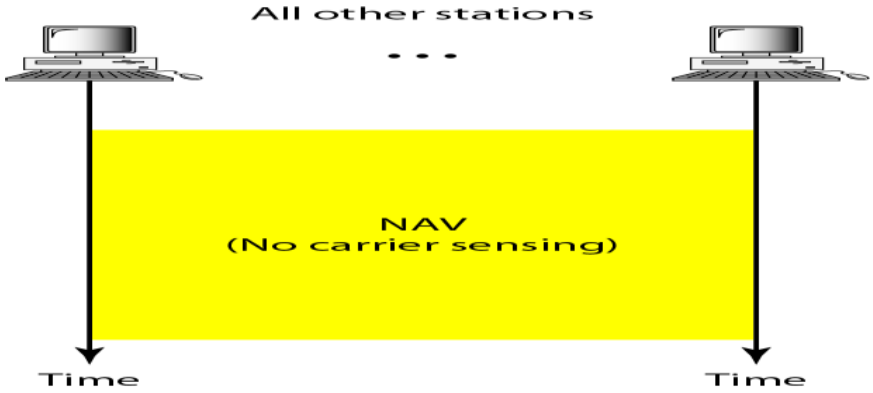

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
    a. The channel uses a persistence strategy with back-off until the channel is idle.
    b. After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).
2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in *CSMA/CD* is a kind of indication to the source that data have arrived.
   Following figure shows the Frame Exchange Time line




***Network Allocation Vector:***

- How do other stations defer sending their data if one station acquires access?
- The key is a feature called **NAV**.
- When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel.
- The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.
- Each time a station accesses the system and sends an RTS frame, other stations start their NAV.
- In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.

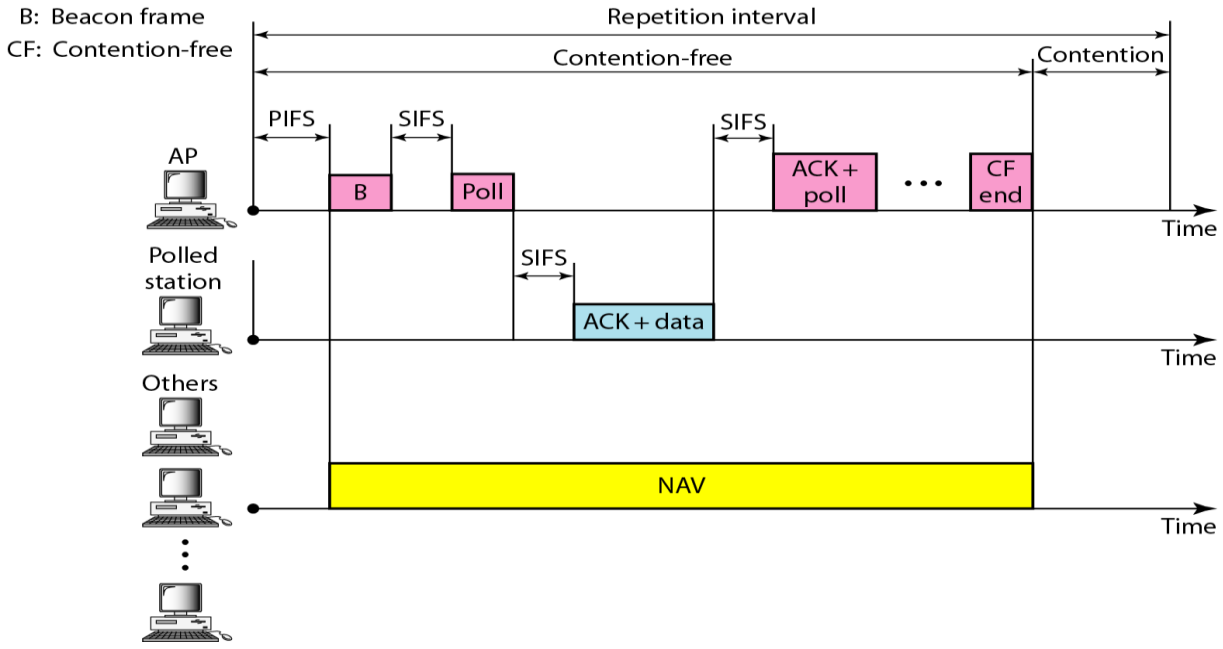


***Collision During Handshaking:***

- What happens if there is collision during the time when RTS or CTS control frames are in transition, often called the handshaking period?
- Two or more stations may try to send RTS frames at the same time.
- These control frames may collide.
- However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver.
- The back-off strategy is employed, and the sender tries again.

**Point Coordination Function (PCF):**

- The PCF is an optional access method that can be implemented in an infrastructure network.
- It is implemented on top of the 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.
- To give priority to PCF over DCF, another set of interframe spaces has been defined: PIFS and SIFS.
- The SIFS is the same as that in DCF, but the PIFS (PCF IFS) is shorter than the DIFS.
- Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium.
- To prevent this, a repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic.
- The repetition interval, which is repeated continuously, starts with a special control frame, called a **beacon frame**.
- When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval.



## Frame Format:

- The MAC layer frame consists of nine fields

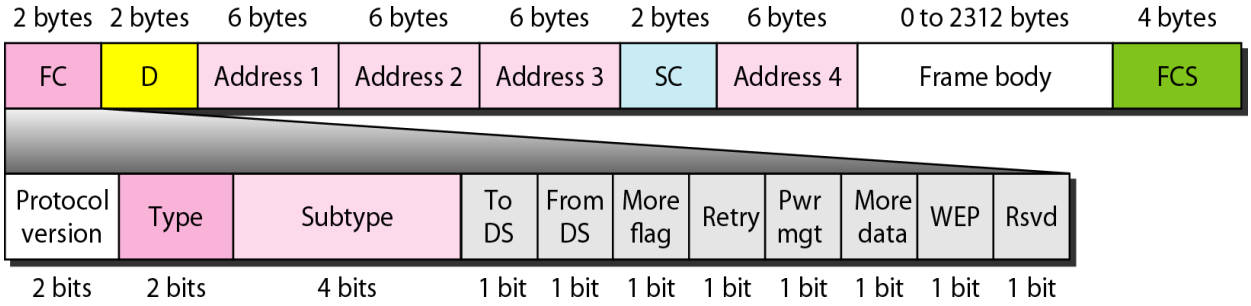



**Figure: Frame format**

✓ **Frame control (FC).** The FC field is 2 bytes long and defines the type of frame and some control 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 except one, this field defines the duration of the transmission that is used to set the value of NAV. In one control frame, this field defines the ID of the frame.

✓ **Addresses**. There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the To DS and From DS subfields

✓ **Sequence control**. This field defines the sequence number of the frame to be used in flow control.

✓ **Frame body**. This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.

✓ **FCS**. The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.

## Frame Types:

- A wireless LAN defined by IEEE 802.11 has three categories of frames: **management frames**, **control frames**, and **data frames**.
- Management frames are used for the initial communication between stations and access points.
- Data frames are used for carrying data and control information.

- Control frames are used for accessing the channel and acknowledging frames.

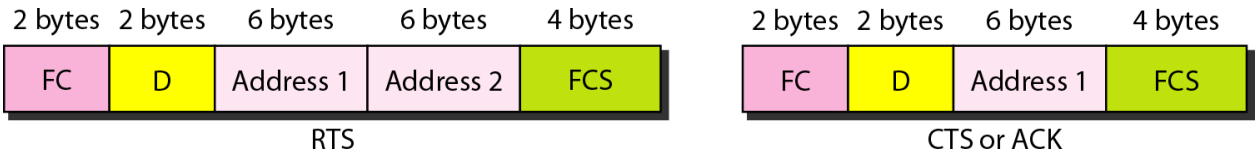



**Figure: Control frames**

- For control frames the value of the type field is 01; the values of the subtype fields for

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

frames

**Table: Values of subfields in control frames**

## Addressing Mechanism:

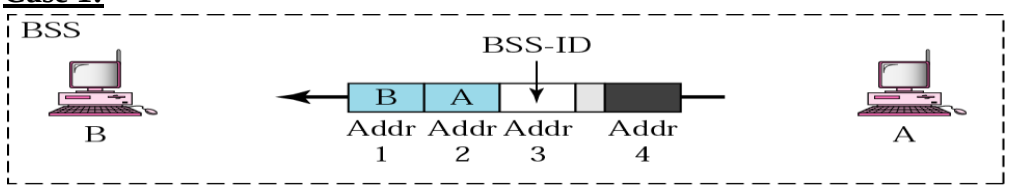
- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS.
- Each flag can be either 0 or 1, resulting in four different situations.
- The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags

| *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 |

**Table: Addresses**

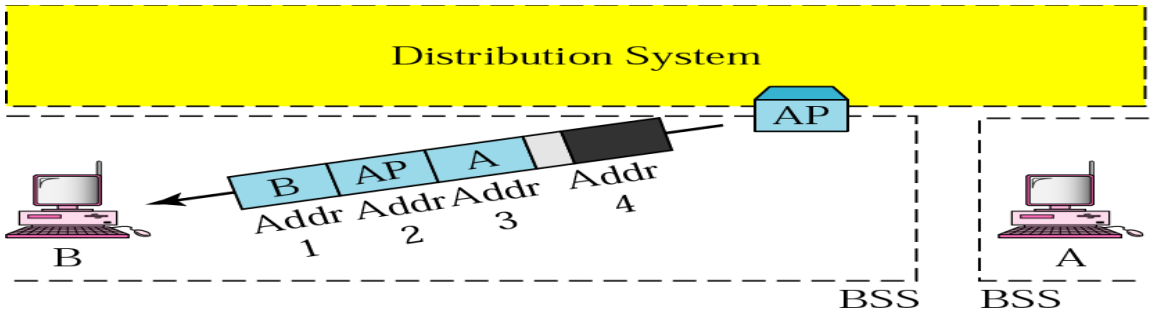
Address 1 is always address of next device
Address 2 is always address of previous device
Address 3 is address of final destination if not defined by Address 1
Address 4 is address of original source if not defined by Address 2

### Case 1:



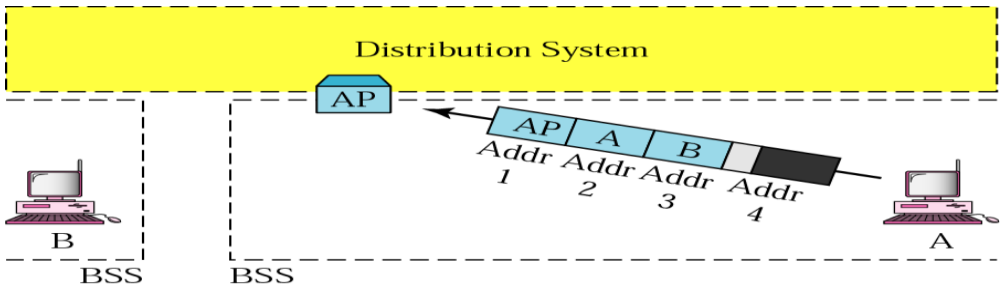

Frame is going directly from one client to another. No intervening distribution system. To DS = 0, From DS = 0

**Case 2:**



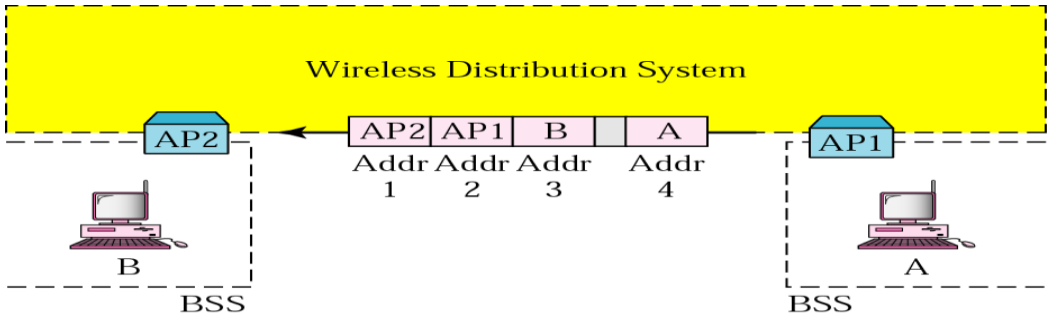

To DS = 0, From DS = 1 frame is coming from a DS (Access Point)

**Case 3:**




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

**Case 4**:




To DS = 1 and From DS = 1

**Hidden and Exposed Station Problems:**

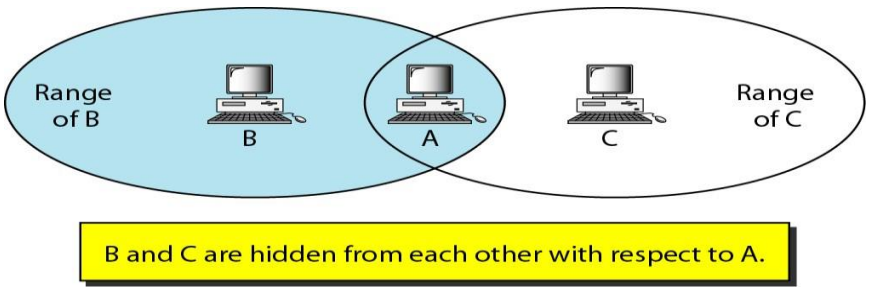



**Figure: Hidden station problem**

Above Figure shows an example of the hidden station problem. Station B has a transmission range shown by the left oval (sphere in space); every station in this range can

hear any signal transmitted by station B. Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C. Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C. Station A, however, is in the area covered by both Band C; it can hear any signal transmitted by B or C.

Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach

C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations 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 the hidden station problem is the use of the handshake frames (RTS and CTS) that we discussed earlier. Following Figure shows that the RTS message from B reaches A, but not C. However, because both Band C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

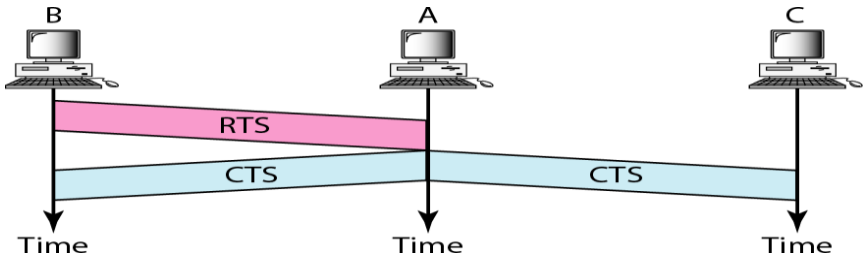



**Figure: Use of handshaking to prevent hidden station problem**

**Exposed Station Problem:**

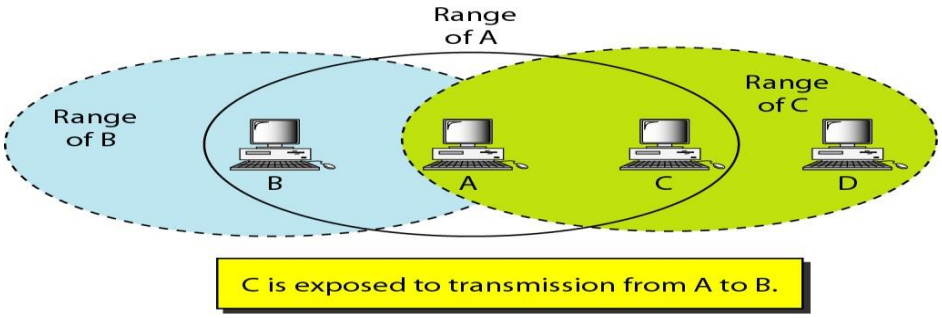



**Figure: Exposed station problem**

In this problem a station refrains from using a channel when it is, in fact, available. In the above figure, station A is transmitting to station B. Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B. However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

The handshaking messages RTS and CTS cannot help in this case, despite what you

might think. Station C hears the RTS from A, but does not hear the CTS from B. Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D. Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state. Station B, however, responds with a CTS. The problem is here. If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D. It remains exposed until A finishes sending its data as Following Figure shows.

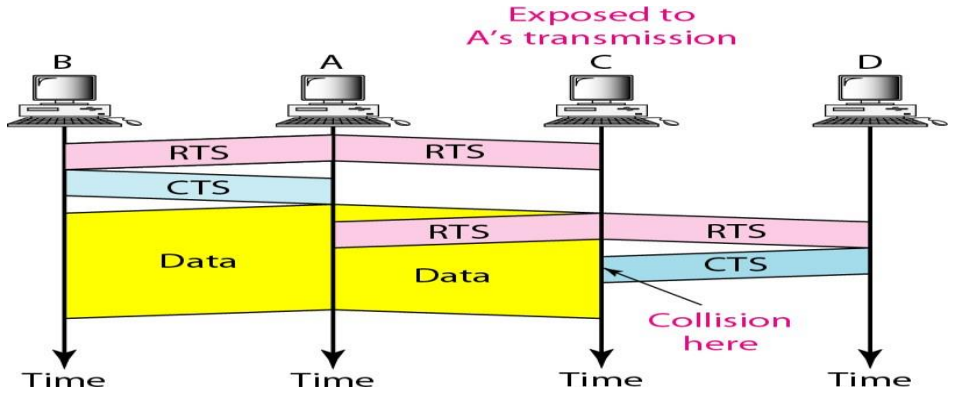



**Figure: Use of handshaking in exposed station problem**

## Physical Layer:

All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges 902-928 MHz, 2.400--4.835 GHz, and 5.725-5.850 GHz.

| *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 |

**Table : *Physical layers***

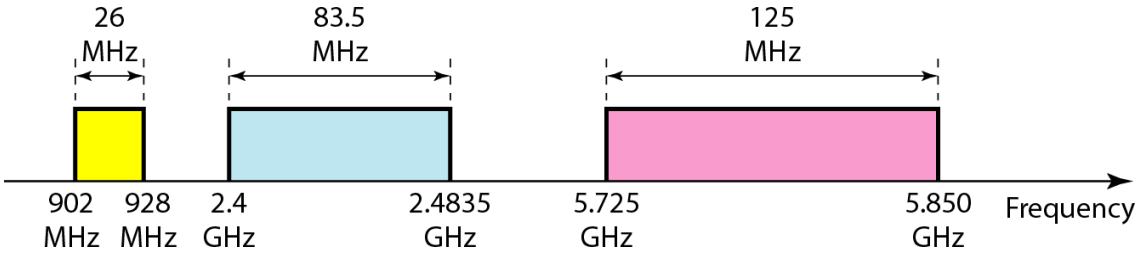



**Figure: Industrial, scientific, and medical (ISM) band**

## IEEE 802.11 FHSS:

- IEEE 802.11 FHSS uses the frequency-hopping spread spectrum (FHSS) method.
- FHSS uses the 2.4-GHz ISM band.
- The band is divided into 79 subbands of 1 MHz (and some guard bands).
- A pseudorandom number generator selects the hopping sequence.
- The modulation technique in this specification is either two-level FSK or four-level FSK with 1 or 2 bits/baud, which results in a data rate of 1 or 2 Mbps.

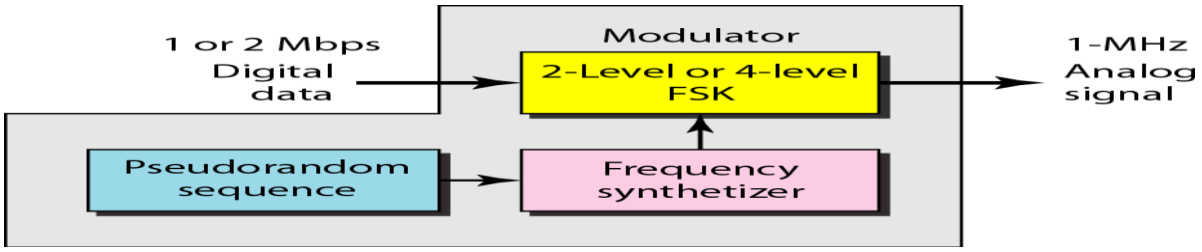



**Figure: Physical layer of IEEE 802.11 FHSS**

## IEEE 802.11 DSSS:

- IEEE 802.11 DSSS uses the direct sequence spread spectrum (DSSS) method.
- DSSS uses the 2.4-GHz ISM band. The modulation technique in this specification is PSK at 1 Mbaud/s. The system allows 1 or 2 bits/baud (BPSK or QPSK), which results in a data rate of 1 or 2 Mbps, as shown in Figure.

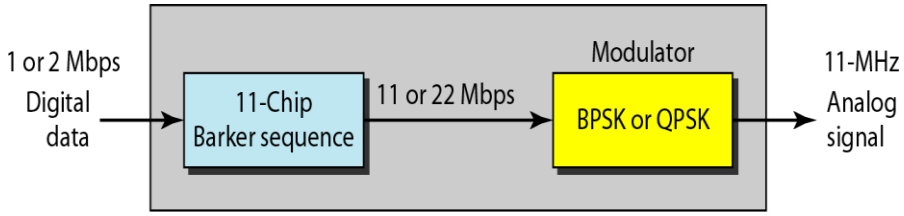



**Figure: Physical layer of IEEE 802.11 DSSS**

## IEEE 802.11 Infrared:

- IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm.
- The modulation technique is called pulse position modulation (PPM).
- For a 1-Mbps data rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and the rest are set to 0.
- For a 2-Mbps data rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bit is set to 1 and the rest are set to 0.
- The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

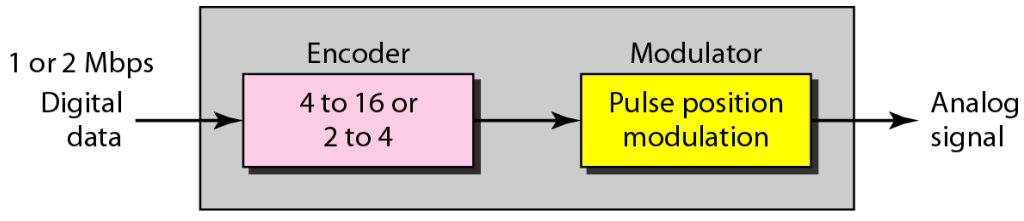


**Figure: Physical layer of IEEE**

## 802.11 infrared IEEE 802.11A

## OFDM:

- IEEE 802.11a OFDM describes the orthogonal frequency-division multiplexing (OFDM) method for signal generation in a 5-GHz ISM band.
- The band is divided into 52 subbands, with 48 subbands for sending 48 groups of bits at a time and 4 subbands for control information.
- Dividing the band into subbands diminishes the effects of interference.
- If the subbands are used randomly, security can also be increased.
- OFDM uses PSK and QAM for modulation. The common data rates are 18 Mbps (PSK) and 54 Mbps (QAM).

## IEEE 802.11b DSSS:

- IEEE 802.11 b DSSS describes the high-rate direct sequence spread spectrum (HRDSSS) method for signal generation in the 2.4-GHz ISM band.
- HR-DSSS is similar to DSSS except for the encoding method, which is called complementary code keying (CCK).
- CCK encodes 4 or 8 bits to one CCK symbol. To be backward compatible with DSSS, HR-DSSS defines four data rates: 1,2, 5.5, and 11 Mbps.
- The first two use the same modulation techniques as DSSS. The 5.5-Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding. The II-Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

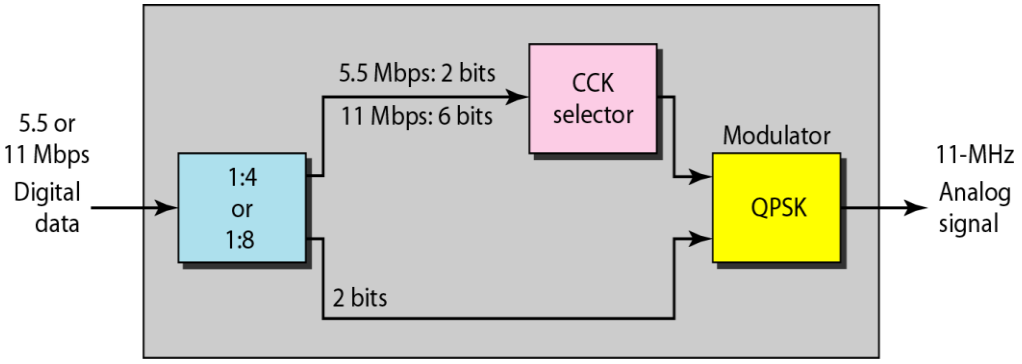



**Figure:** ***Physical layer of IEEE 802.11b***

## IEEE 802.11g:

- This new specification defines forward error correction and OFDM using the 2.4-GHz ISM band.
- The modulation technique achieves a 22- or 54-Mbps data rate. It is backward compatible with 802.11b, but the modulation technique is OFDM.