Unit III

Medium Access Control

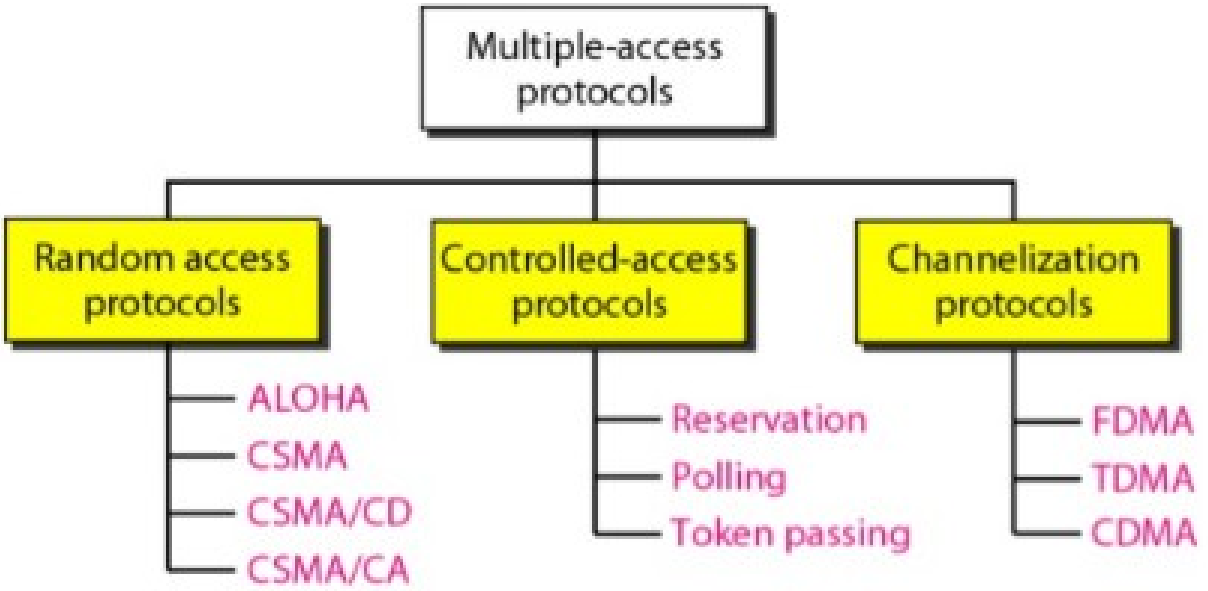
Introduction

- 2 types of networks
  - Point to point
  - Broadcast Network
- Broadcast n/w uses multi-access channel or randon access channel.In broadcast n/w it is important to decide to whom access of channel is granted when more than one users are compete for it.
- Protocol makes this decision.
- Protocol belongs to a sublayer of data link layer called the MAC(medium access control)

DLL

- It has 2 sublayers
  - LLC:Logical Link Control(flow and error Control)
  - MAC:Media access control(Multiple Access)

Protocols used for Media access control



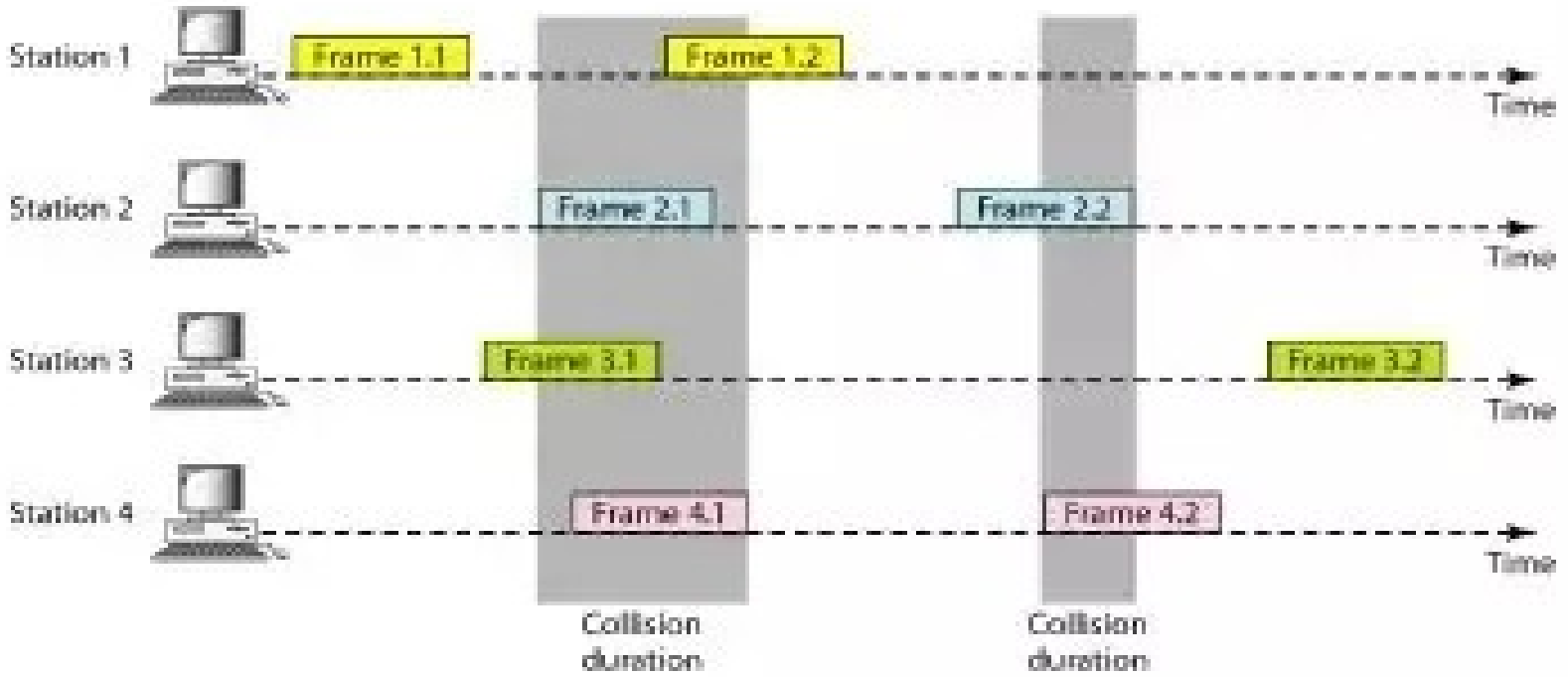
Random Access

- No station is superior to another station and none is assigned the control over another.
- No station permits another station to send.
- Station wants to send makes decision depending on the state of the medium (idle or busy).
- There is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access.
- There is no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods.

1.Pure ALOHA

- The original ALOHA protocol is called pure ALOHA.
- This is a simple protocol.
- The idea is that each station sends a frame whenever it has a frame to send(no rule).
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations

Figure 12.3 *Frames in a pure ALOHA network*

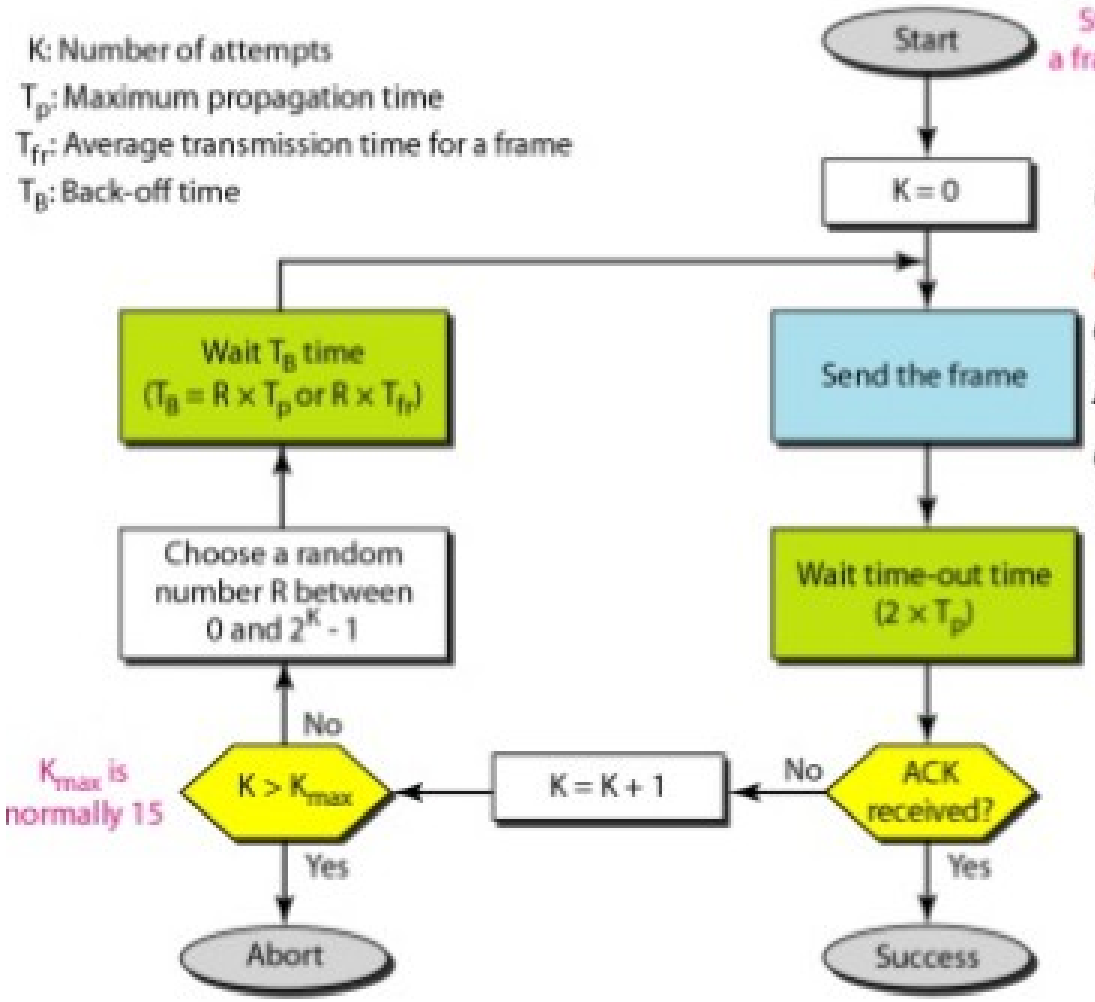


- There are four stations compete with one another for access to the shared channel.
- There are a total ofeight frames on the shared medium. Some of these frames collide and only frame 1.1 from station 1 and frame 3.2 from station 3 are survived.
- if one bit of a one frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.
- It is needed to resend the frames that have been destroyed during transmission.
- The pure ALOHA protocol is based on acknowledgments from the receiver when a station sends a frame.
- But 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.

- If all these stations try to resend their frames after the time-out, the frames will collide again.
- Pure ALOHA dictates that when the time-out period passes, each station waits for a random amount of time before resending its frame. The randomness will help avoid more collisions.
- This random waiting time is the back-off time TB.

Congestion Control In PURE ALOHA

Figure 12.4 *Procedure for pure ALOHA protocol*

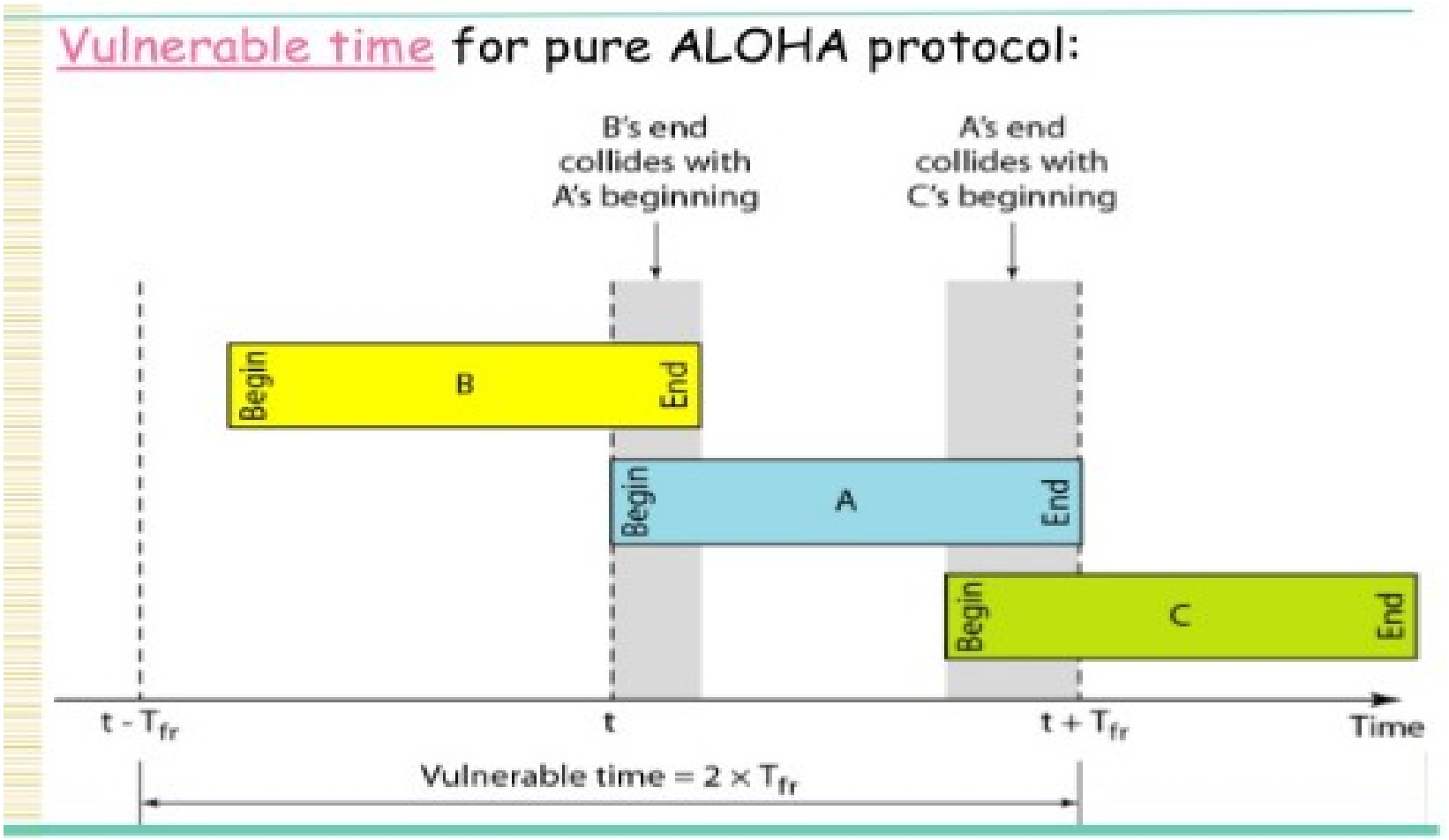


TB depends on the implementation. One common formula is the binary exponential back-off, for each retransmission, a multiplier in the range 0 to 2K - 1 is random chosen and multiplied by Tp or Tfr.

- The time-out period = The maximum possible round-trip propagation delay(which is twice the amount of time required to send a frame between the two most widely separated stations (2 x T_p))
- The back-off time T_B is a random value that normally depends on K (the number of attempted unsuccessful transmissions). The formula for TB depends on the implementation. One common formula is the binary exponential back-off.
- For each retransmission, a multiplier in the range 0 to $2^{\overline{K}}$ - 1 is randomly chosen and multiplied by T_p (maximum propagation time) or T_{fr} (the average time required to send out a frame) to find $T_{B'}$ In this procedure, the range of the random numbers increases after each collision. The value of K_{max} is usually chosen as 15.
-

Vulnerable Time

-
-



- Vulnerable time is the time in which there is a possibility of collision.
- Lets the stations send fixed-length frames with each frame taking T_{fr} seconds to send.
- Suppose station A send packet at a time t.B sends packet before time $t+t_{fr}$, then there is colision between ending of frame B and starting of frame A.
- Pure ALOHA vulnerable time= $2 \times T_{fr}$
- The throughput for pure ALOHA is $S = G \times e^{-2G}$.

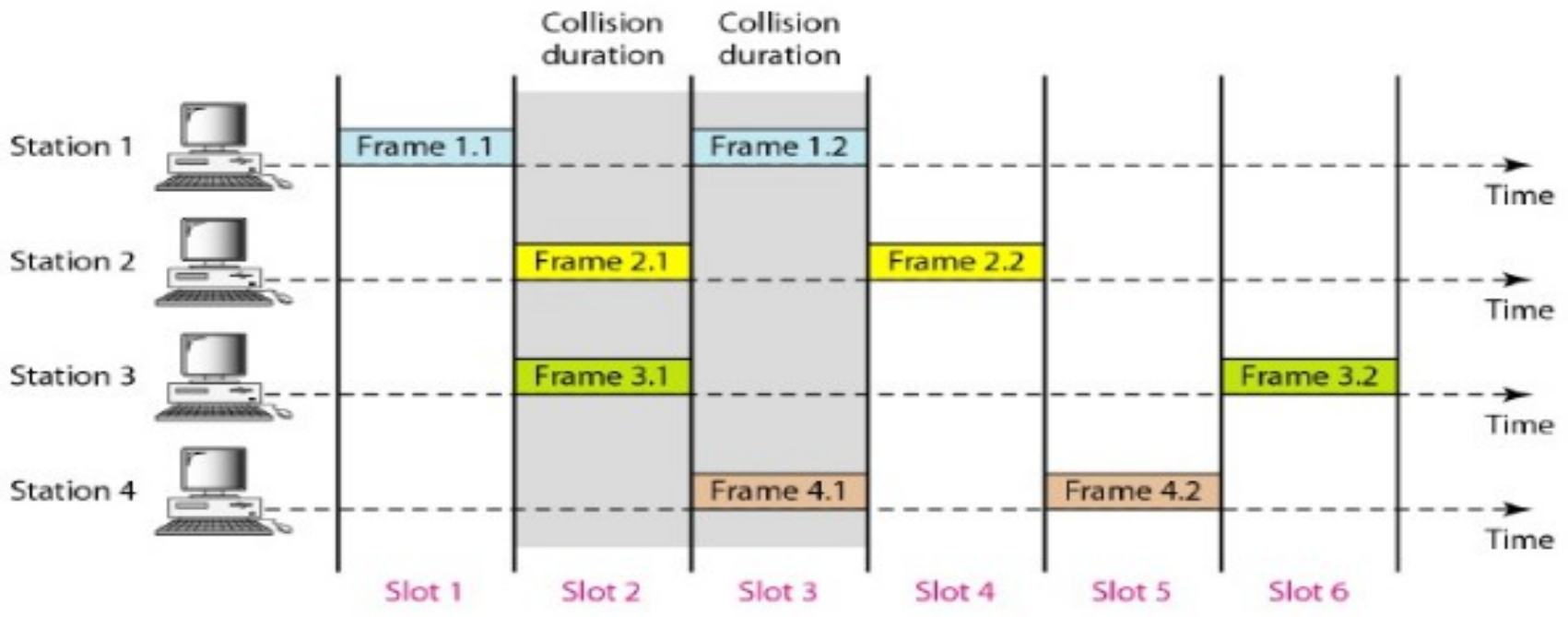
  Where G is average number of frames generated by the system during one frame transmission time.

- The maximum throughputSmax =0.184 when G=(1/2).

2. Slotted ALOHA

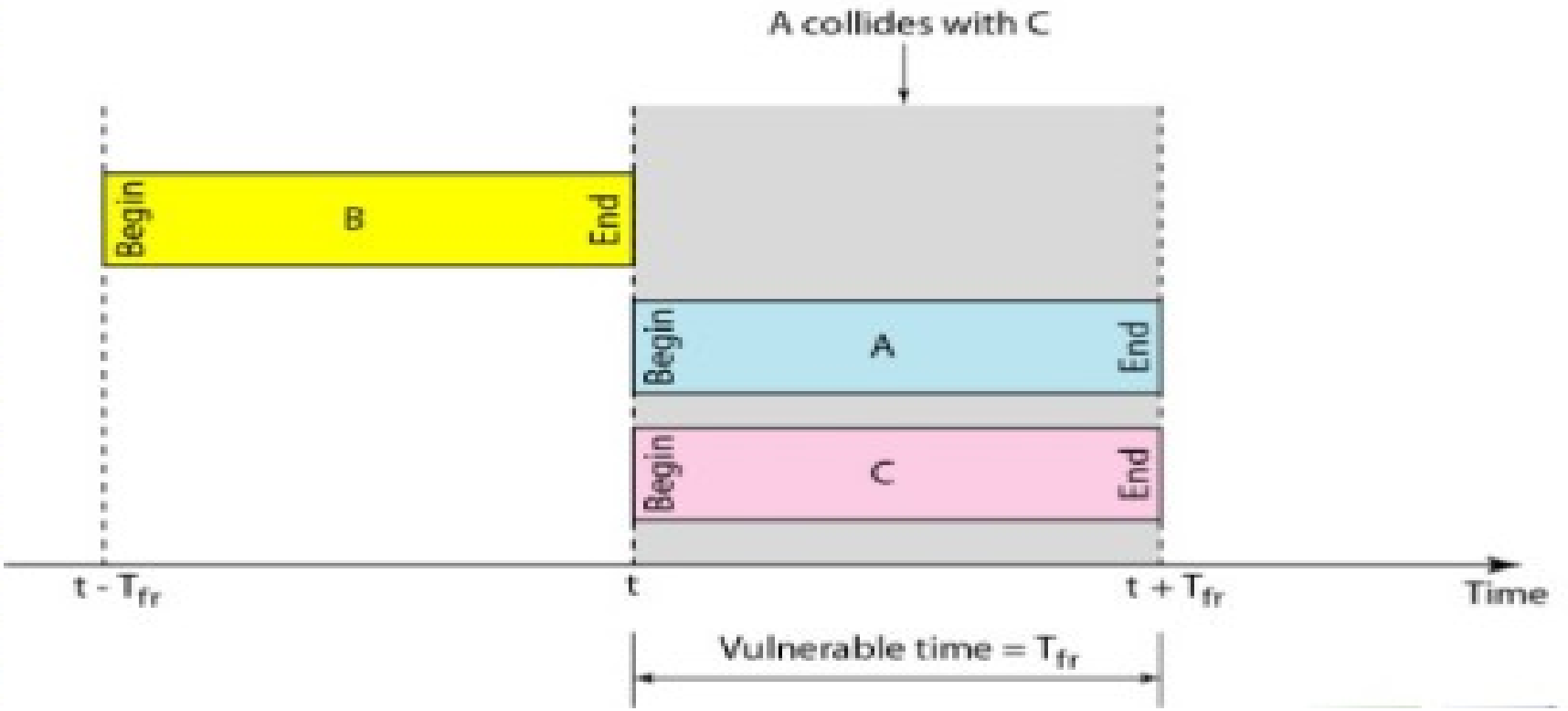
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA we divide the time into slots of T_{fr} s and force the station to send only at the beginning of the time slot.
-

Figure 12.6 *Frames in a slotted ALOHA network*



- 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 the possibility of collision if two stations try to send at the beginning of the same time slot.
- The vulnerable time is now reduced to one-half i.e. equal to T_{fr}
- Slotted ALOHA vulnerable time =T_{fr}
- Throughput of slotted ALOHA is $S = G \times e^{-G}$
- The maximum throughput Smax == 0.368 when G=1.
-

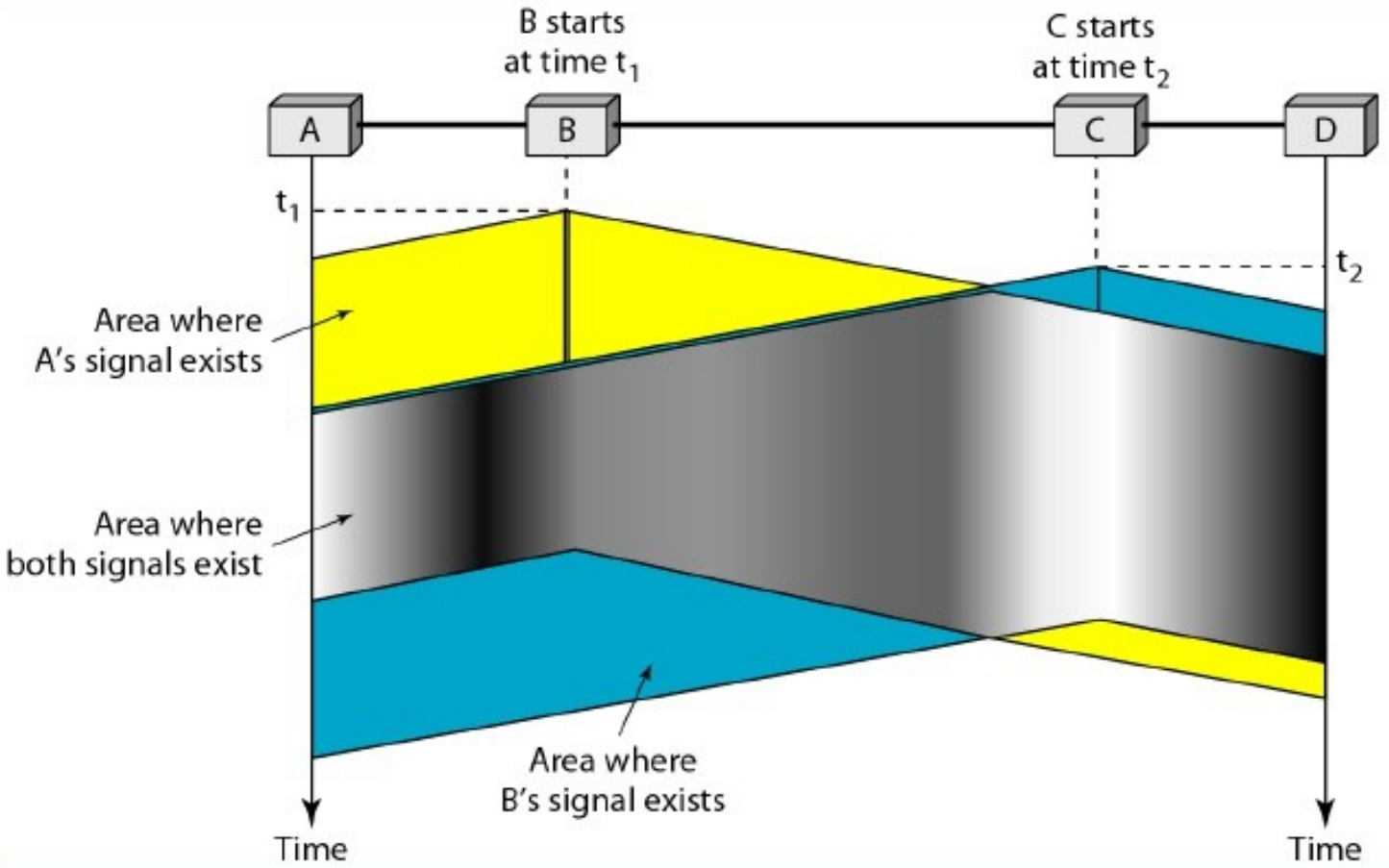
Vulnerable time for slotted ALOHA protocol



3. CSMA

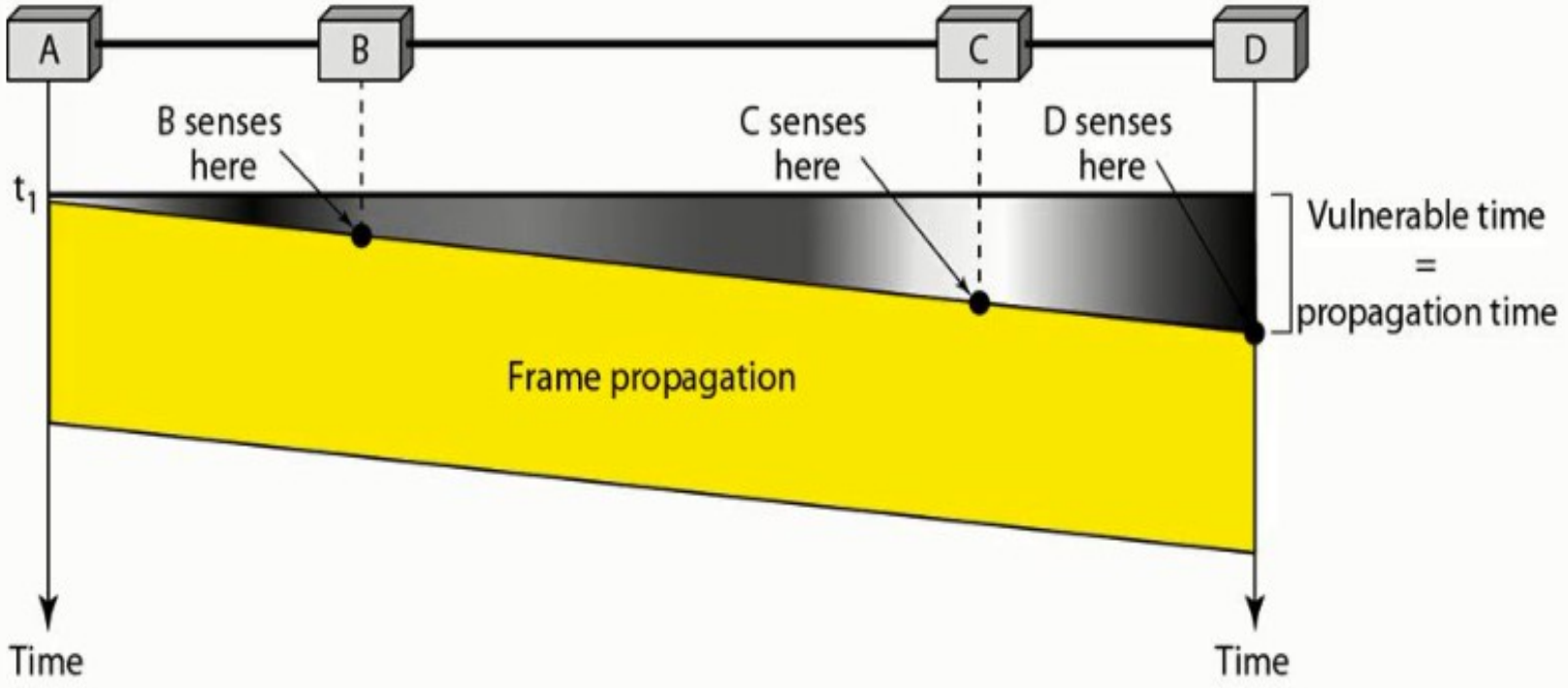
- It is Carrier Sense Multiple Access.
- It is used to minimize the chance of collision and therefore increase the performance.
- CSMA based on, each station first listen/senses to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle "sense before transmit" or"listen before talk."
- CSMA can reduce the possibility of collision, but it cannot eliminate it.
- The possibility of collision still exists because of propagation delay. when a station senses the medium as free , it still takes time (although very short) for the first bit to reach every station and for every station to sense it.

Figure 12.8 *Space/time model of the collision in CSMA*



- At time t1' station B senses the medium and finds it idle, so it sends a frame. At time t2 (t2> tI)' 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.

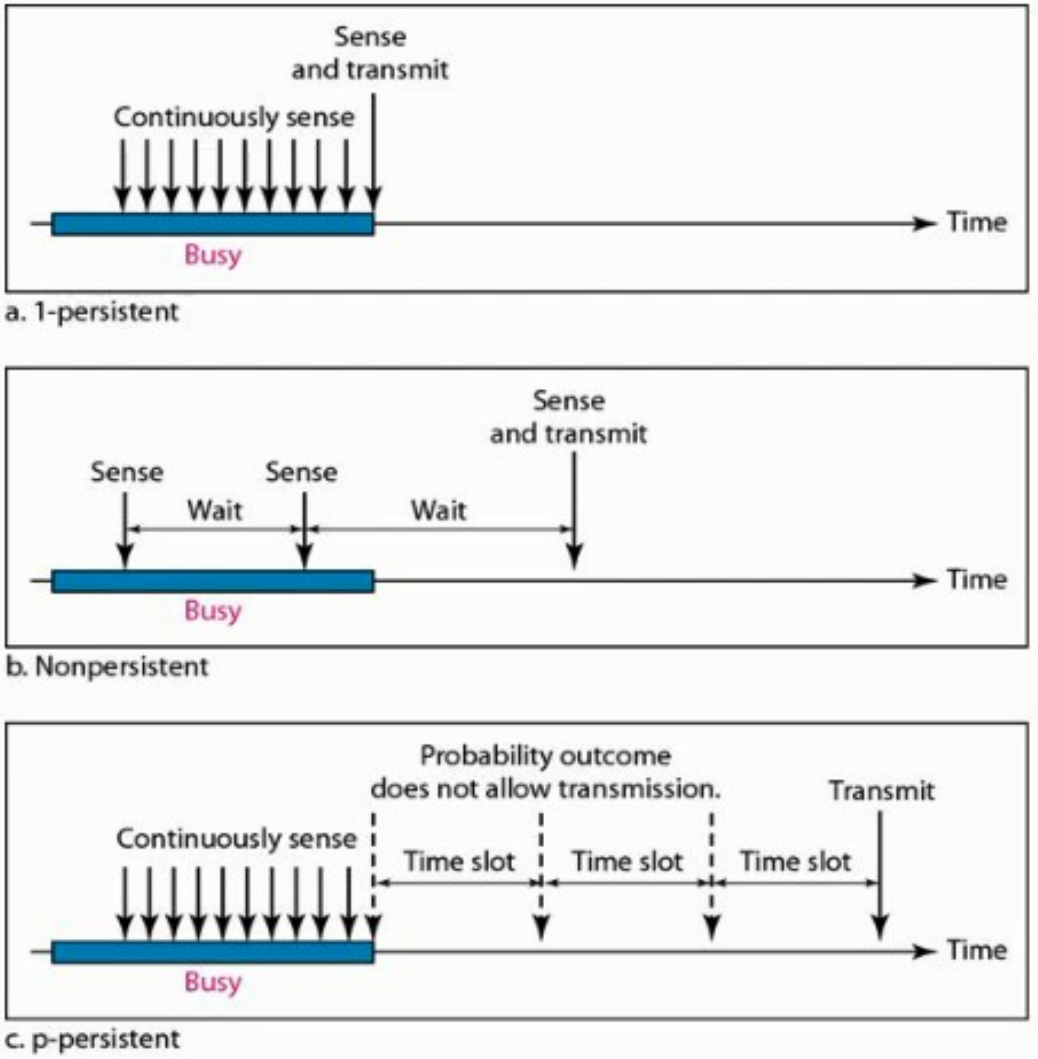
Figure 12.9 *Vulnerable time in CSMA*



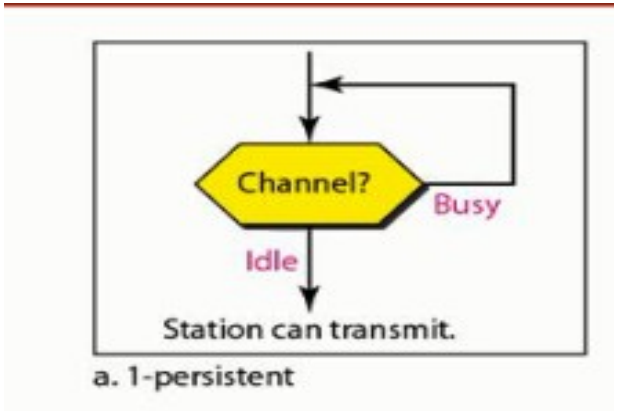
CSMA Methods

- What should a station do if the channel is busy or idle? It depends upon the 3 Methods.
  - Persistent method
  - Nonpersistent method
  - P-persistent method.

Figure 12.10 *Behavior of three persistence methods*



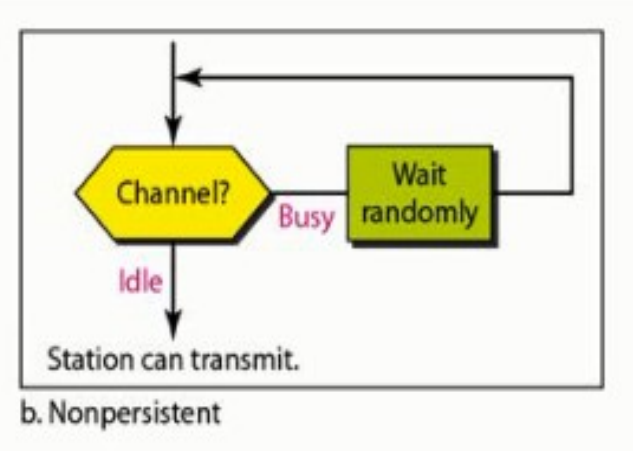
I-persistent method



a. 1-persistent

- The persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability I).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

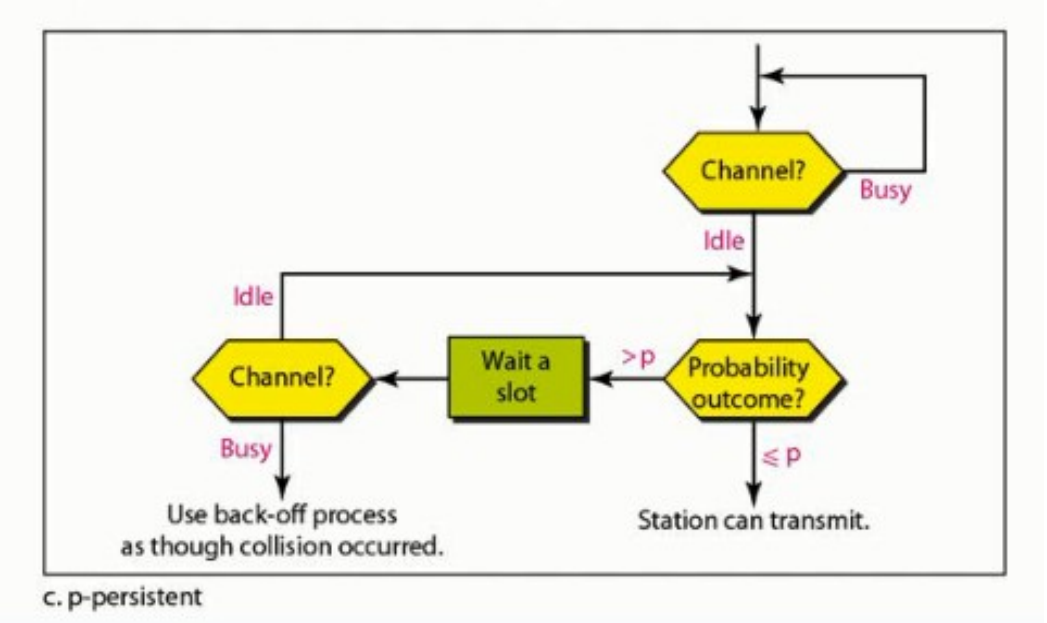
Nonpersistent method



b. Nonpersistent

- 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 method



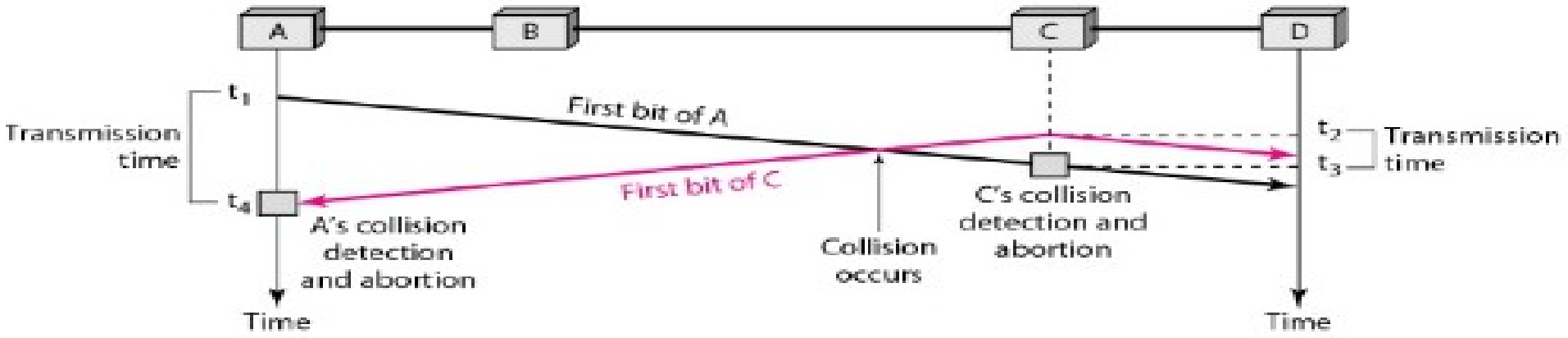
c. p-persistent

- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.
  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.
  3. If the line is idle, it goes to step 1.
  4. If the line is busy or a collision has occurred , it uses the back- off procedure.
- e.g. If p=1/6 then among 6 stations 1 is transmitting and others will wait.

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

- It is used to handle the collision in wired network.
- 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 transmission otherwise there is a collision, the frame is resent again.

Collision in CSMA/CD



- At time t1, station A starts sending the bits of its frame.
- At time t2, station C has not yet sensed the first bit sent by A and starts sending the bits of its frame, which propa- gate 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 and immediately aborts transmission.
- Station A detects collision at time t4 when it receives the first bit of C's frame and immediately aborts transmission.
- A transmits for the duration t4 – tl and C transmits for the duration t3 - t2'

For CSMA/CD to work

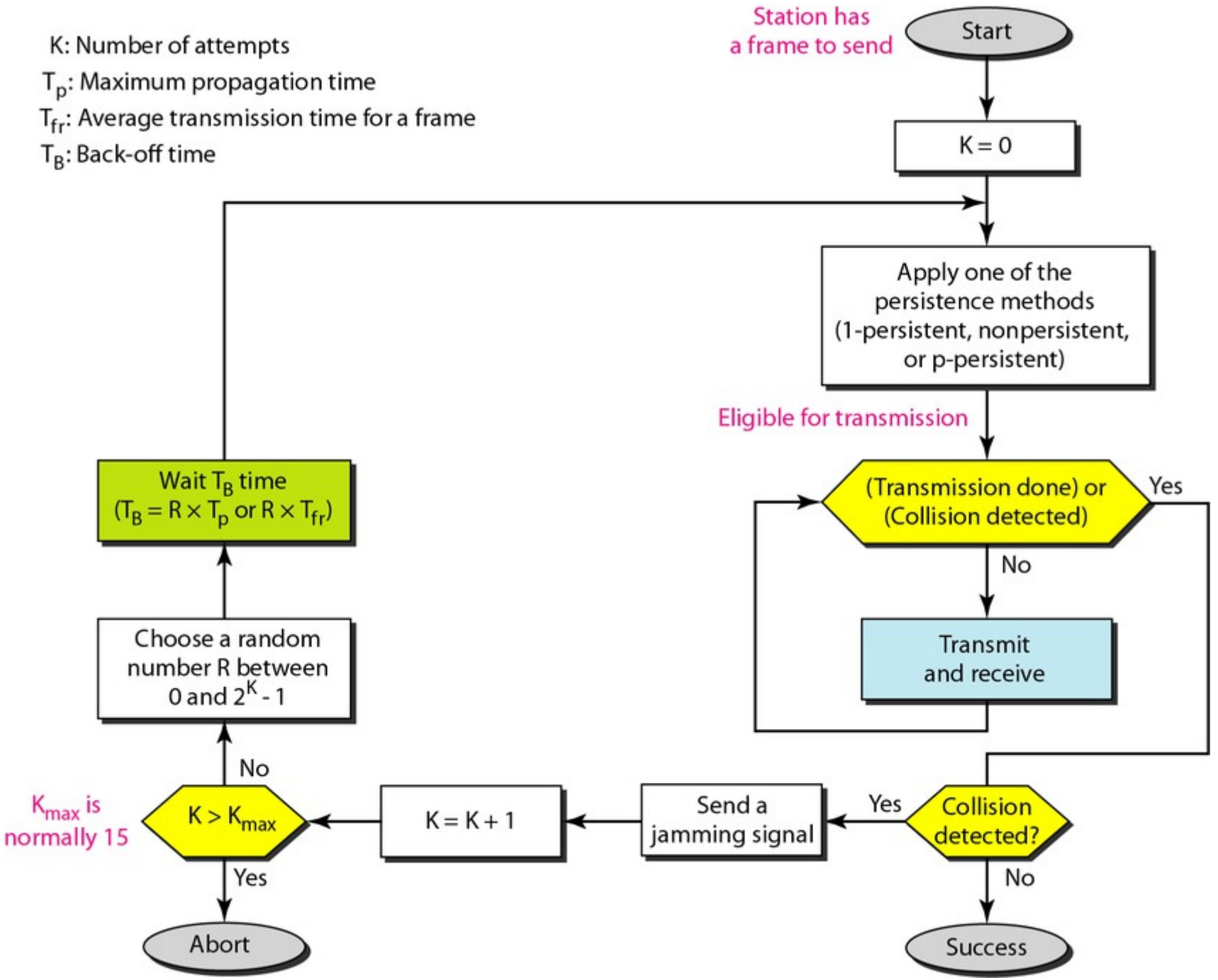
- For CSMAICD to work, it is required a restriction on the frame size.
- Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission .
- The frame transmission time T_{fr} must be at least two times the maximum propagation time T_p.**($T_{fr} = 2T_p$)** If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second, and the effect of the collision takes another time Tp to reach the first. So the requirement is that the first station must still be transmitting after 2Tp.

For CSMA/CD to work

- For CSMAICD to work, it is required a restriction on the frame size.
- Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission .
- The frame transmission time T_{fr} must be at least two times the maximum propagation time T_p.**($T_{fr} = 2T_p$)** If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second, and the effect of the collision takes another time Tp to reach the first. So the requirement is that the first station must still be transmitting after 2Tp.

For CSMA/CD to work

- For CSMAICD to work, it is required a restriction on the frame size.
- Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission .
- The frame transmission time T_{fr} must be at least two times the maximum propagation time T_p.**($T_{fr} = 2T_p$)** If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second, and the effect of the collision takes another time Tp to reach the first. So the requirement is that the first station must still be transmitting after 2Tp.


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
Send a jamming signal
K = K + 1
K > K_{max}
No
Yes
K_{max} is normally 15
Choose a random number R between 0 and 2^K - 1
Wait T_B time (T_B = R × T_p or R × T_{fr})
No
Success
Abort

Throughput of CSMA/CD

- The throughput of CSMAlCD is greater than that of pure or slotted ALOHA.
- The maximum throughput occurs at a different value of G and the value of p in the p-persistent approach.
- For 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.

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

- It is invented to avoid collision in wireless network.
- Collisions are avoided through the three strategies:
  - The interframe space.
  - The contention window
  - Acknowledgments.

Interframe Space (IFS)

- Collisions are avoided by , When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS.
- If after the IFS time the channel is still idle, the station can send.
- The IFS can also be used to define the priority of a station or a frame.For example, a station that is assigned a shorter IFS has a higher priority.

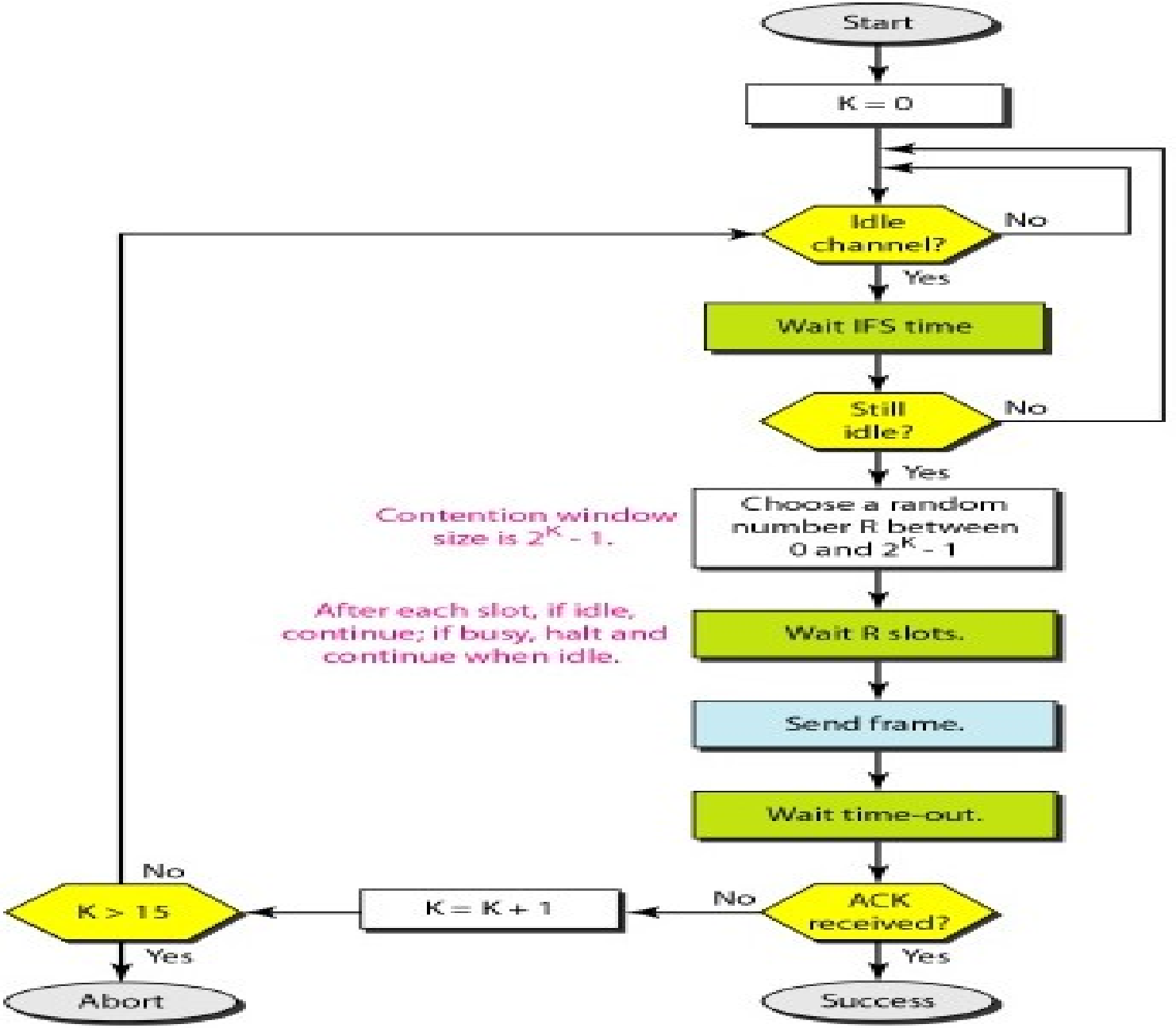
Contention Window

- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy.
- Back-off strategy:This means that contention window is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This gives priority to the station with the longest waiting time

Acknowledgment

- 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 Dig. CSMA/CA

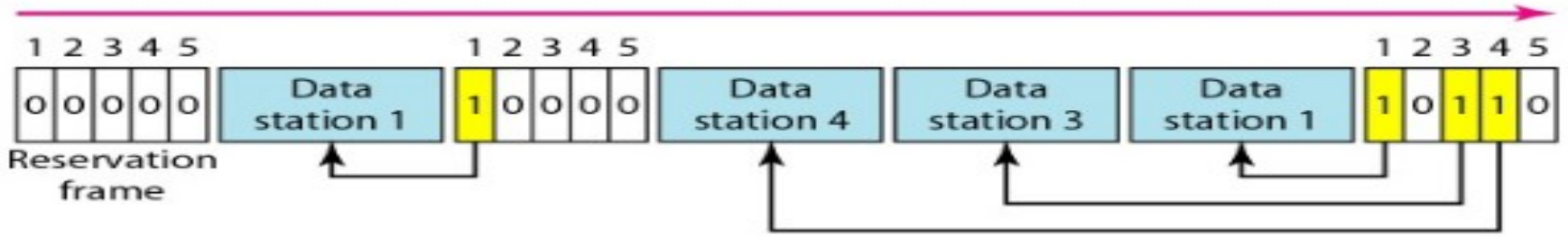


2. CONTROLLED ACCESS

- 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.
- 3 methods are used
  - Reservation.
  - Polling.
  - Token Passing.

Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.
- If there are N stations in the system, there are exactly N reservation minislots in the reservation frame. Each minislot belongs to a station.
- When a station needs to send a data frame, it makes a reservation in its own minislot.
- The stations that have made reservations can send their data frames after the reservation frame.
-

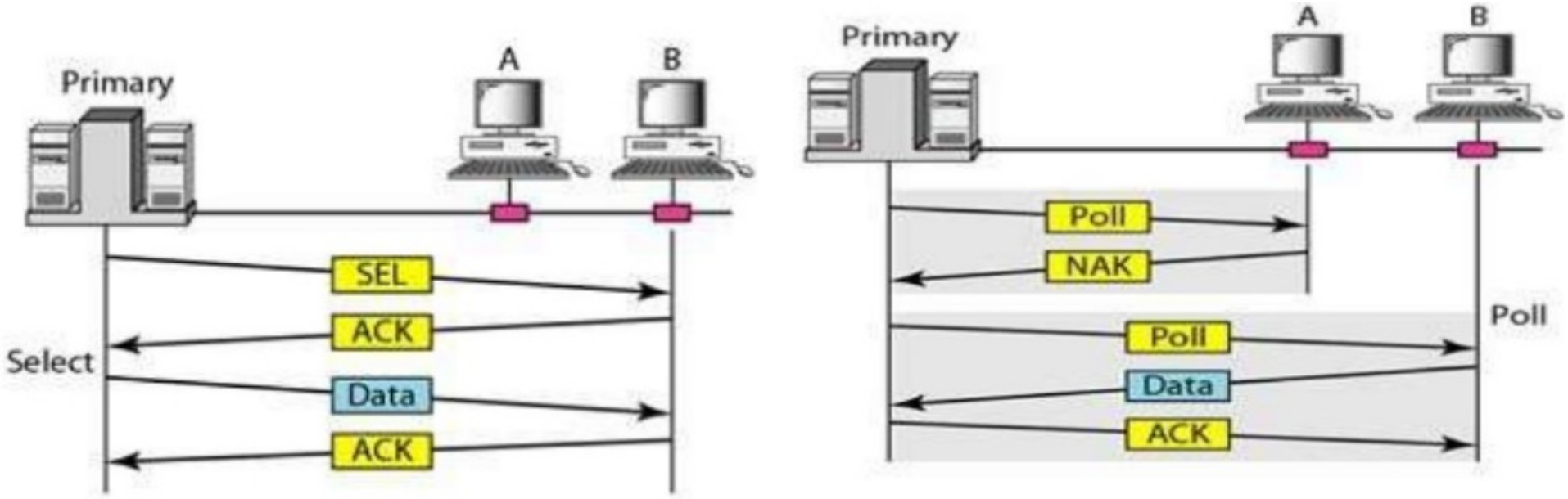


- five stations and a five-minislot reservation frame.
- In the first interval, only stations 1, 3, and 4 have made reservations.
- In the second interval, only station 1 has made a reservation.

Polling

- Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations.
- All data exchanges must be made through the primary device .
- The primary device controls the link and the secondary devices follow its instructions.
- It is up to the primary device to determine which device is allowed to use the channel at a given time.
- The primary device, therefore, is always the initiator of a session

Contd...



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

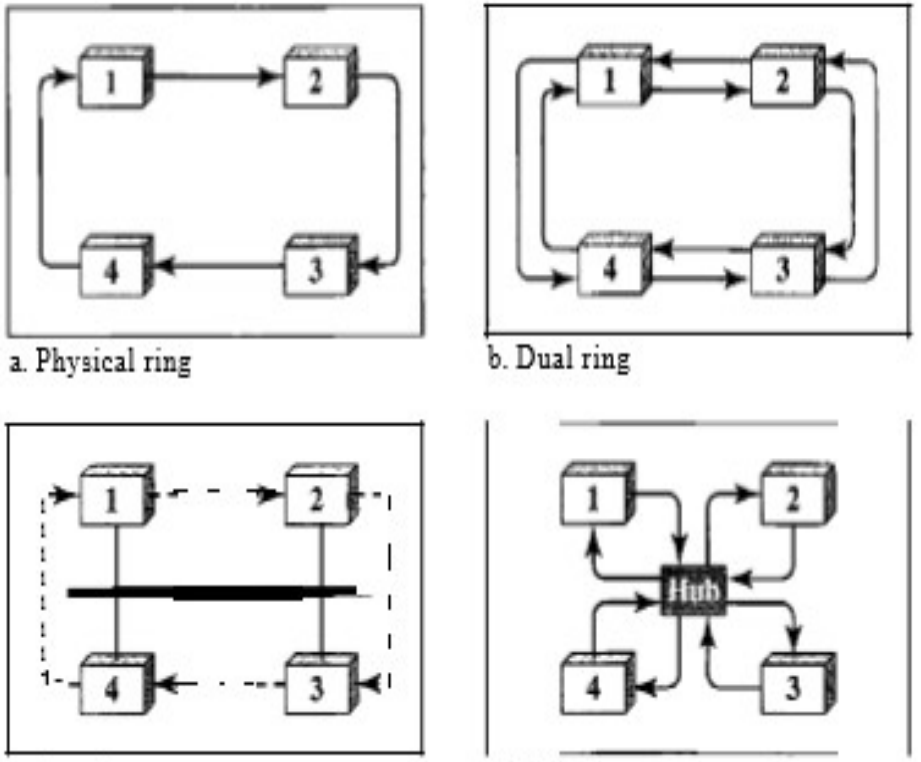
- **Select:** If primary has something to send, the primary device sends it. But it does not know, whether the target device is prepared to receive.
- So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the secondary's ready status. Before sending data.
- The primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.
- **Poll:** When the primary is ready to receive data, it must ask (poll) each secondary if it has anything to send.
- When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data
- If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send.
- When primary receives a data frame, the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.

Token Passing

- In the token-passing method, the stations in a network are organized in a logical ring i.e. for each station, there is a predecessor and a successor.
- 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 and from current station to the successor.
- To pass this access right a special packet called a token circulates through the ring.
- Station that holds the token can sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring
- Token management is needed for this access method. -
- Token Management :
  - Stations can hold token for limited time period.
  - The token must be monitored to ensure it has not been lost or destroyed.
  - assign priorities to the stations and to the types ofdata being transmitted.
  - It make low-priority stations release the token to high- priority stations.
-

Logical Ring

Figure 12.20 *Logical ring and physical topology in token-passing access method*



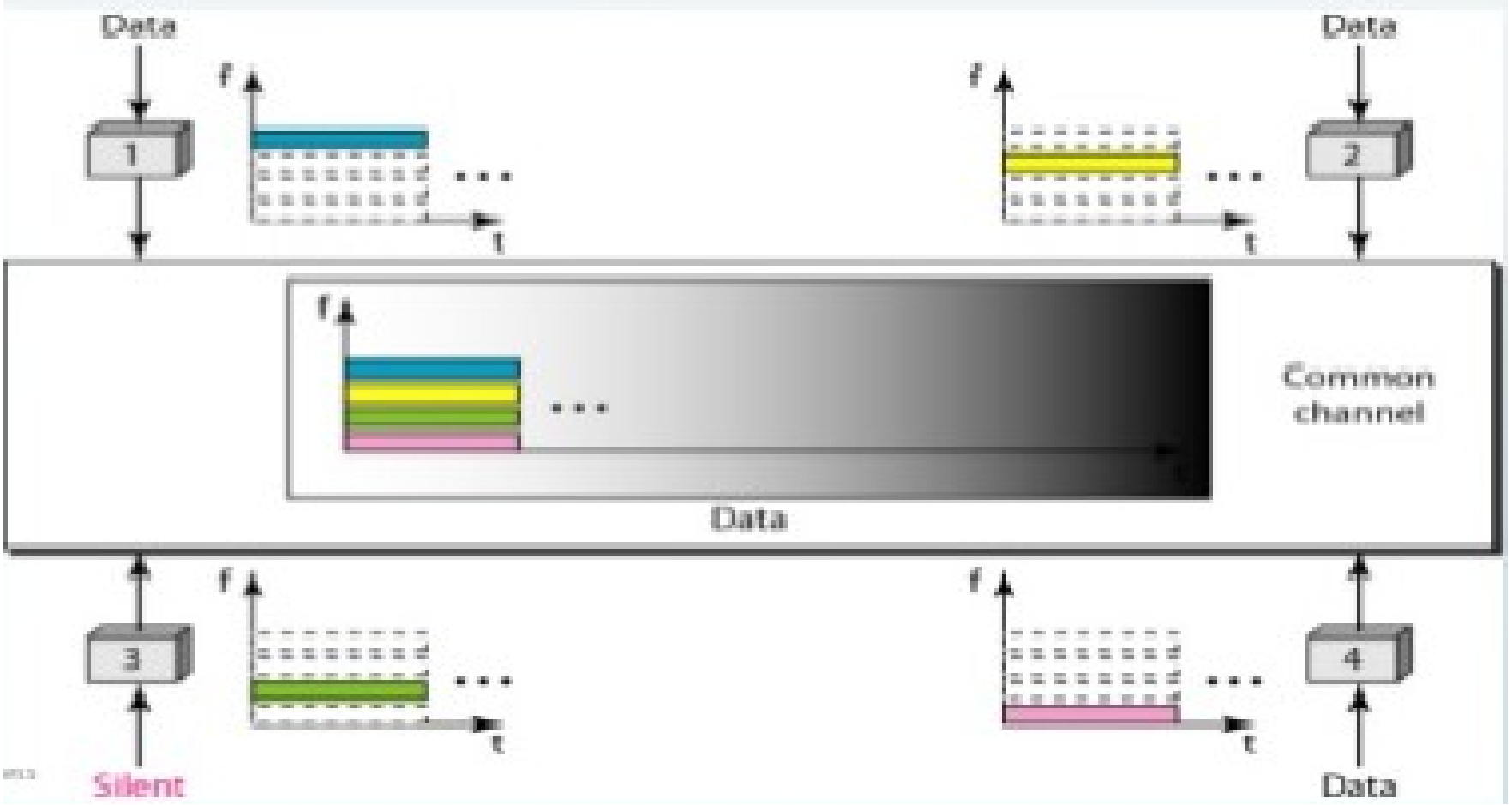
CHANNELIZATION

- 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.
- 3 channelization protocol are there
  - FDMA (Frequency Division Multiple Access)
  - TDMA (Time Division Multiple Access)
  - CDMA. (Code Division Multiple Access)

Frequency-Division MultipleAccess (FDMA)

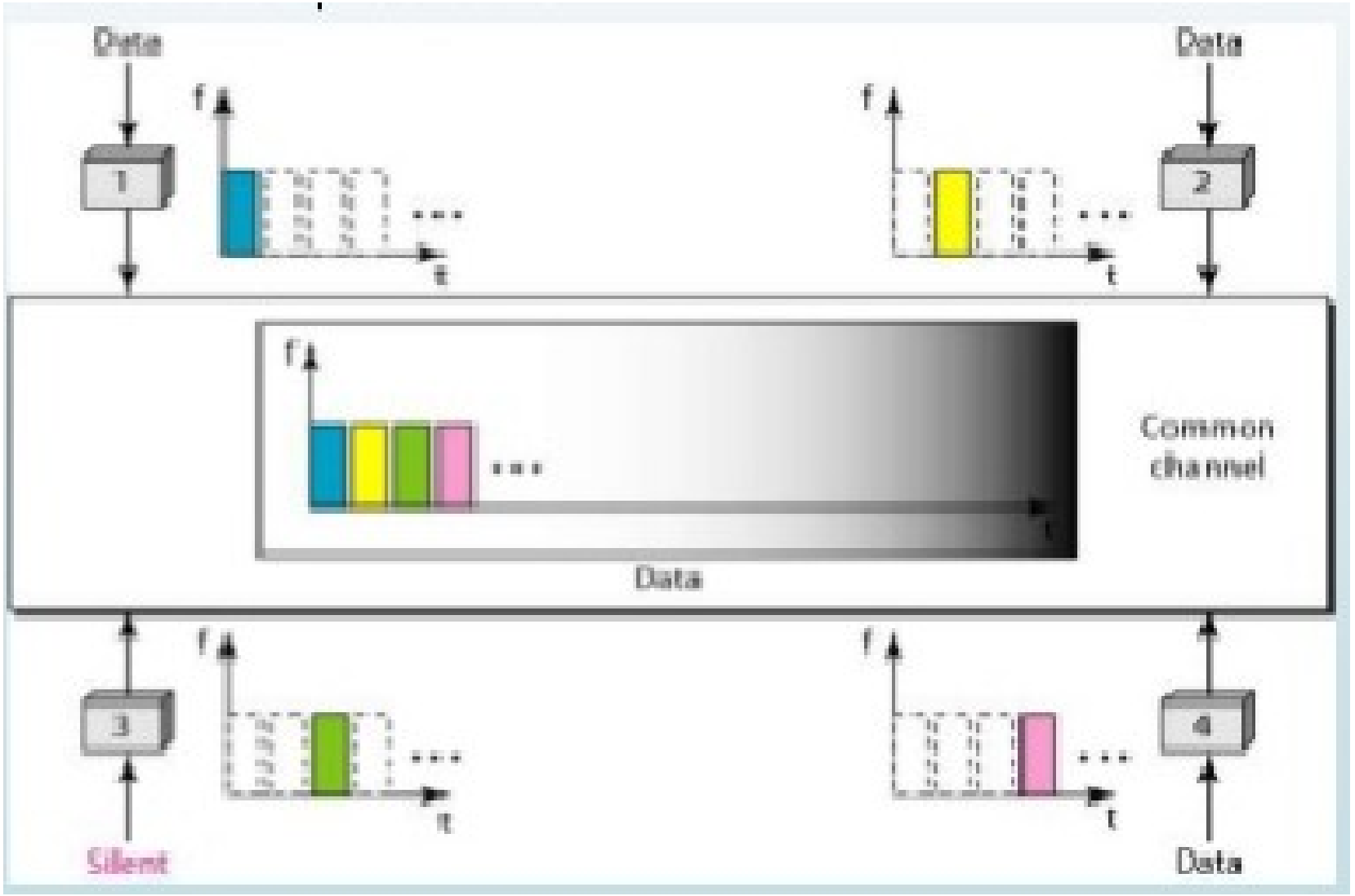
- In FDMA, the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data.
- It means each band is reserved for a specific station, and it belongs to the station all the time.
- Each station also uses a bandpass filter to confine the transmitter frequencies.
- To prevent station interferences, the allocated bands are separated from one another by small guard bands.
- FDMA specifies a predetermined frequency band for the entire period of communication.

FDMA



Time-Division Multiple Access (TDMA)

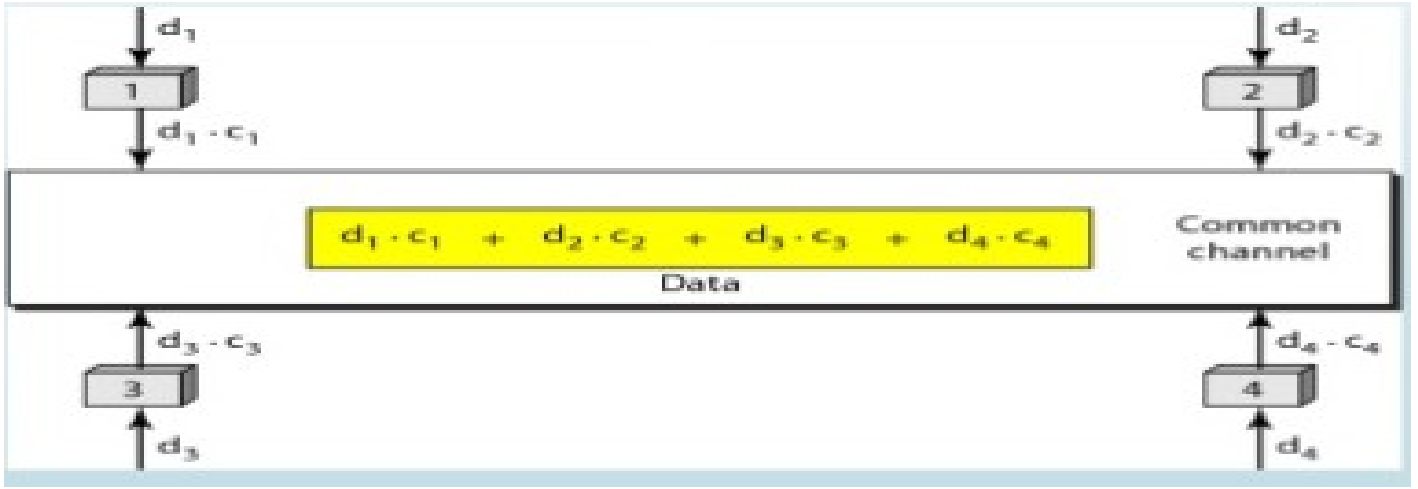
- In time-division multiple access (TDMA), the stations share the whole bandwidth of the channel in time slot. Each station is allocated a time slot during which it can send data. Each station transmits its data in is assigned time slot only.


Data
Data
f
f
1
2
t
t
f
Common
channel
Data
f
f
3
4
t
t
Silent
Data

- 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.
- This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area.
- To compensate for the delays, we can insert guard times between two time bands.
- Synchronization is normally accomplished by having some synchronization bits (preamble bits) at the beginning of each slot.
-

Code-Division MultipleAccess (CDMA)

- CDMA 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; there is no timesharing.
- CDMA simply means communication with different codes.
- For example, in a large room with many people, two people can talk in English if nobody else understands English. Another two people can talk in Chinese if they are the only ones who understand Chinese, and so on.
- In other words, the common channel, the space of the room in this case, can easily allow communication between several couples, but in different languages (codes).
-



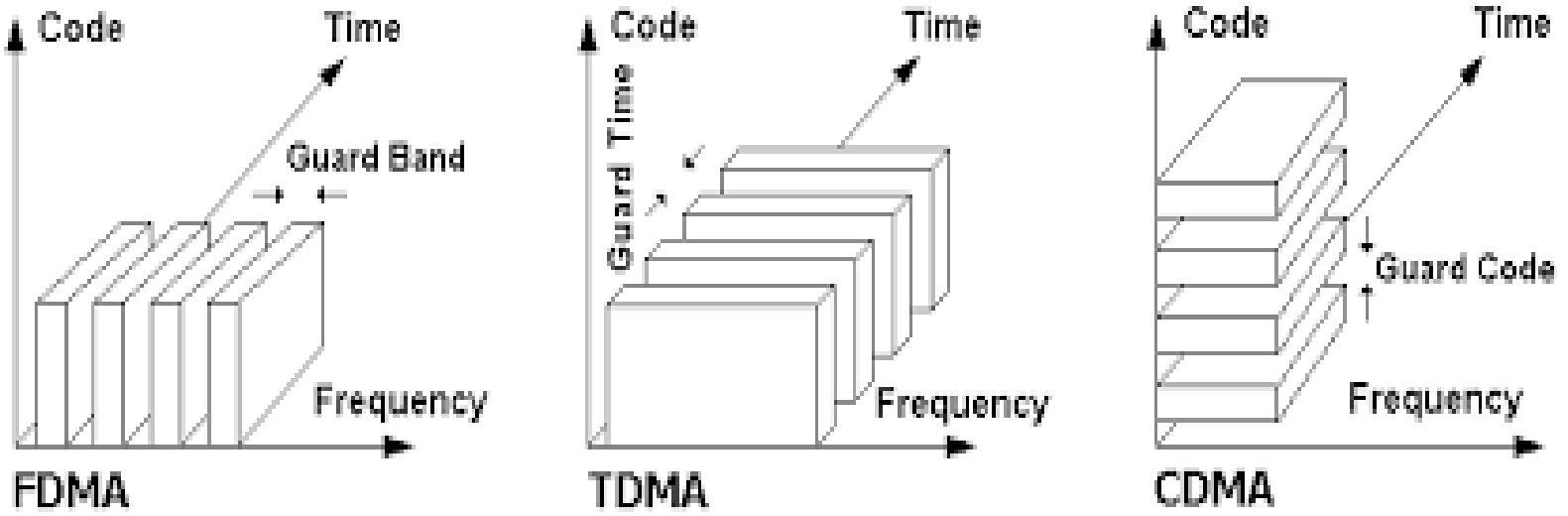
- Let us assume we have four statins 1, 2, 3, and 4 connected to the same channel. The data from station 1 are d1 , from station 2 are d2, and so on. The code assigned to the first station is c1, to the second is c2, and so on.

- The Codes are assigned have two properties.
  - 1. If we multiply each code by another, we get O.
  - 2. If we multiply each code by itself, we get 4 (the number of stations).
- Station 1 multiplies its data by its code c1 ,Station 2 multiplies its data by its code c2 . And so on.
- Data that go on the channel are the sum of all these terms.
- suppose stations 1 and 2 are talking to each other.
- Station 2 wants to hear what station 1 is saying. It multiplies the data on the channel by c1 the code of station 1.
- Because (c1 * c1) is 4, but (c2 * c1), (c3 * c1), and (c4 * c1) are all Os, station 2 divides the result by 4 to get the data from station 1.

  Data=(c1*d1*c1)+(c2*d2*c1)+(c3*d3*c1)+(c4*d4*c1)

  = d1*4
- D1*4/4 = d1 i.e. Station 2 hears station 1's data
- Actually, code is sequence of numbers called as chip

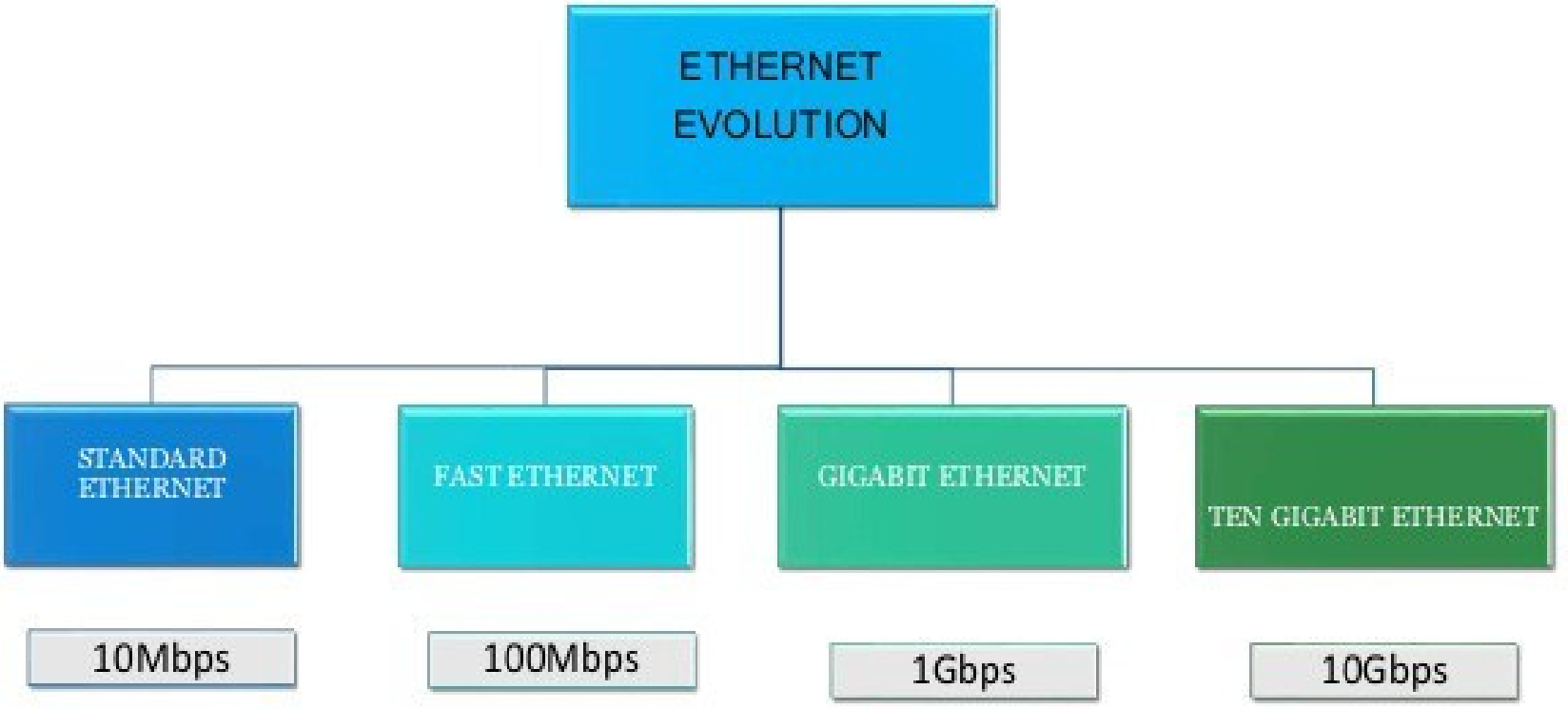
FDMA	TDMA	CDMA
Bandwidth is shared between stations	Time is shared between stations	Bandwidth and time are shared between stations
Synchronization is not necessary	Synchronization is necessary	Synchronization is not necessary
Code word is not used	Code word is not used	Code word is used
Guard Band between Adjacent channel are necessary	Guard times between Adjacent channel are necessary	Guard Band and Guard Times between Adjacent channel are necessary
B/W=30 KHz	B/W=31 KHz	B/W=1.25 MHz


Code
Time
Guard Band
Frequency
FDMA
Code
Time
Guard Time
Frequency
TDMA
Code
Time
Guard Code
Frequency
CDMA

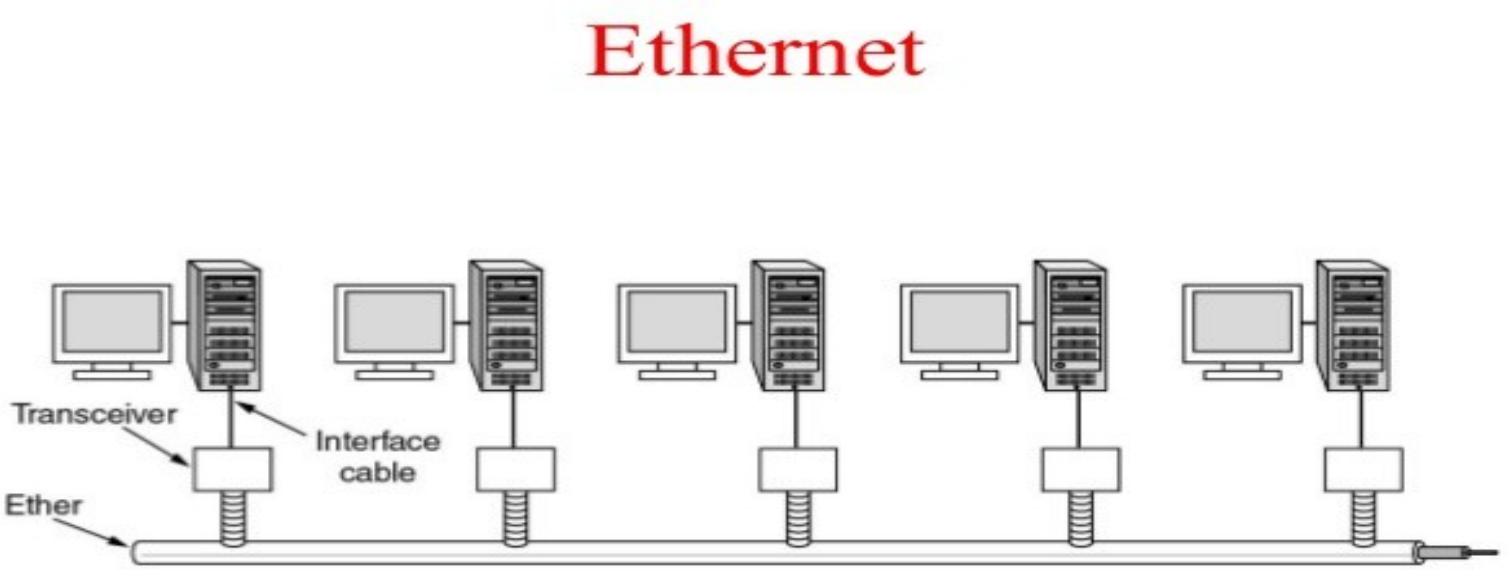
Ethernet

- The LAN market has uses 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.

Ethernet evolution



Architecture of Ethernet



Architecture of the original Ethernet.

- The transmission medium is a thick co-axial cable upto 2.5 km long.
- Repeater is placed after every 500 meters.
- Upto 256 machines can be attached to multidrop cable.
- The original Ethernet was standardized as IEEE 802.3 standard.

IEEE standards

- **IEEE 802.1**: Standards related to network management.
- **IEEE 802.2:** General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sub-layers -- the logical link control (LLC) layer and the media access control (MAC) layer.
- **IEEE 802.3:** Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard.
- **IEEE 802.4**: Defines the MAC layer for bus networks that use a token-passing mechanism (token bus networks).
- **IEEE 802.5**: Defines the MAC layer for token-ring networks.
- **IEEE 802.6:** Standard for Metropolitan Area Networks (MANs).

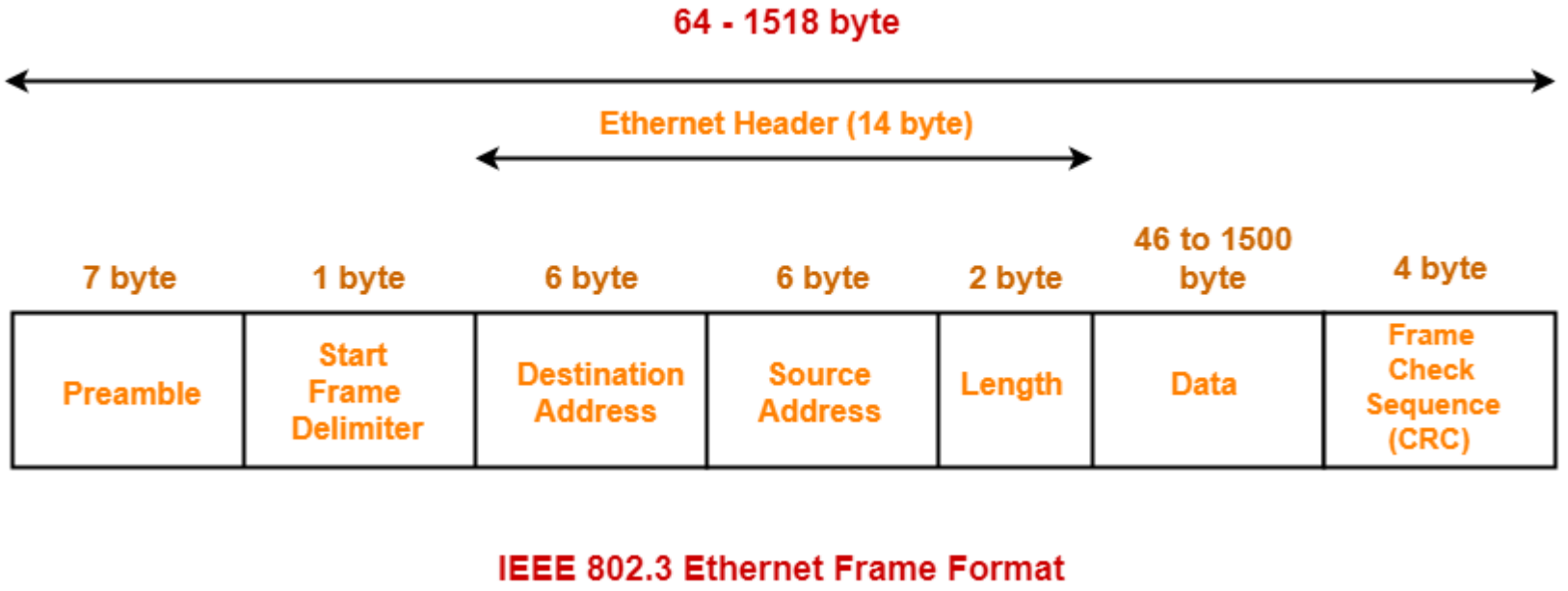
Topology

- Bus topology
- Ring topology
- Star topology
- Tree topology

Traditional Ethernet (IEEE 802.3)

- It is oldes version of Ethernet created in 1976
- It supports data rates of 10 Mbps.
- MAC uses CSMA/CD to share media between all stations.

Frame Format



IEEE 802.3 Ethernet Frame Format

- The Ethernet frame contains seven fields:
- **Preamble**. It is 7 bytes (56 bits) long.
- It is sequence of 0's and 1's and it used for synchronization i.e. alerts about the coming frame.
- The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD).** It is of a 1 byte: 10101011
- It 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 it alerts the receiver that the next field is the destination address.

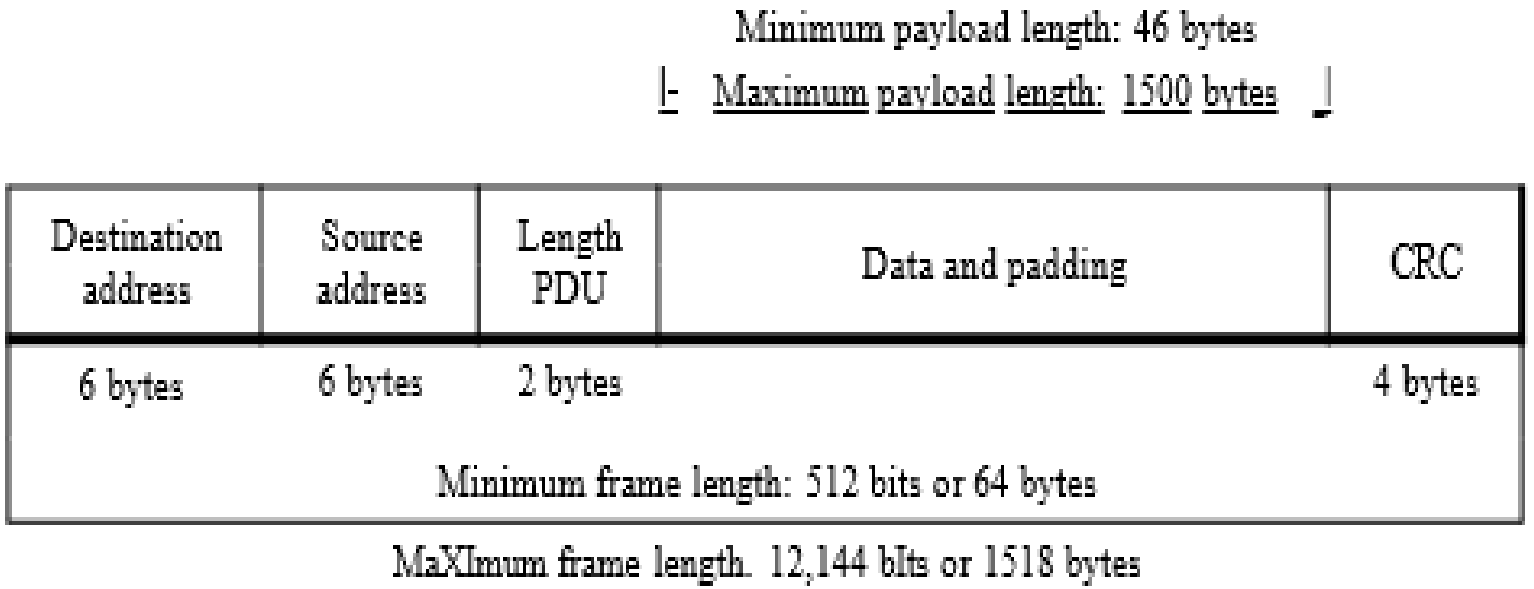
- **Destination address (DA)**. The DA field is of 6 bytes
- It contains the physical address of the destination station or stations.
- **Source address (SA).** The SA field is of 6 bytes
- It contains the physical address of the sender of the packet.
- **Length or type**. This field is defined as a type field or length field.
- **Data.** This field carries data encapsulated from the upper-layer protocols.

  It is a minimum of 46 and a maximum of 1500 bytes
- **CRC**. The last field contains error detection information, in this case a CRC-32 bit long

Frame Length

- Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame.
-

Figure 13.5 *Minimum and maximum lengths*



Ethernet Address

- Each station on an Ethernet network has its own network interface card (NIC).
- The NIC fits inside the station and provides the station with a 6-byte physical address.
- Etherrnet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.
- e.g. **06:01 :02:01:2C:4B**
- MAC addresses can be Unicast, Multicast, and Broadcast Addresses
- . 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.

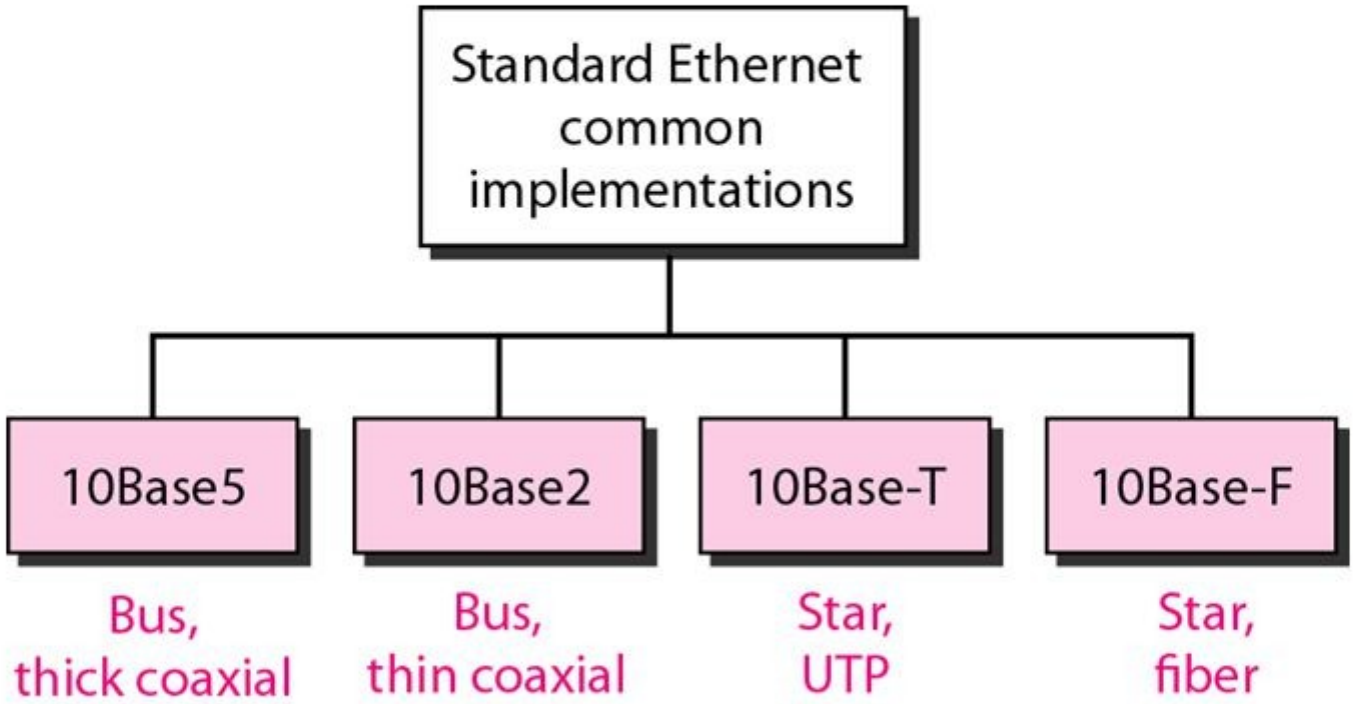
- If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.
- If all the bits are 1's then address is broadcast.
-
-

Figure 13.7 *Unicast and multicast addresses*

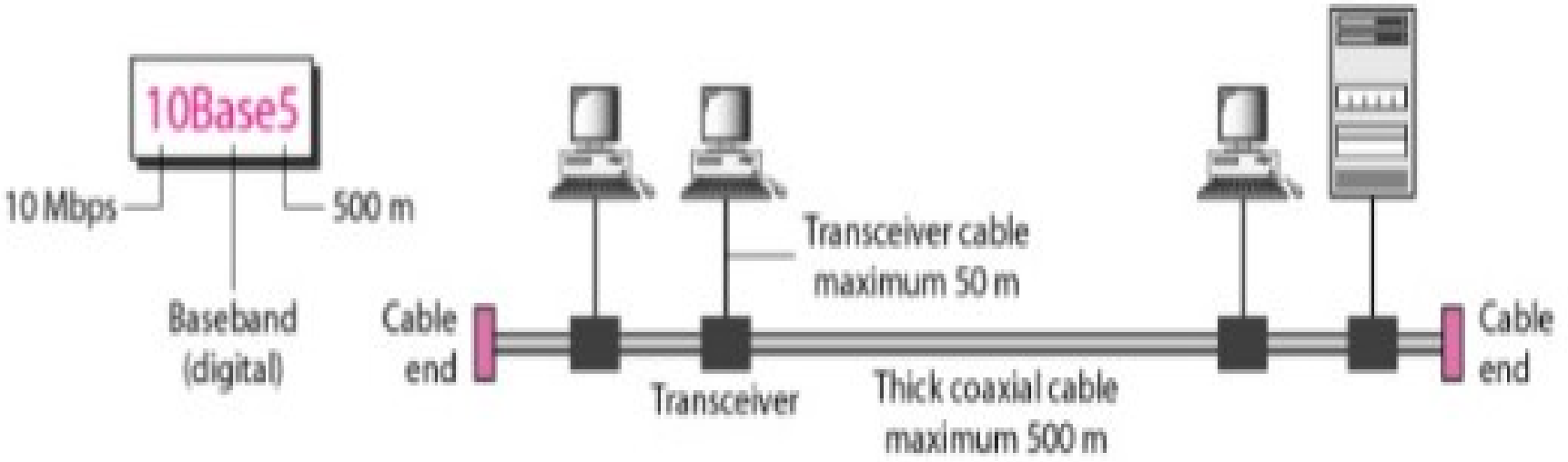
- Define the type of the following destination addresses:
- a. 4A:30:10:21:1O:1A
- b. 47:20:1B:2E:08:EE
- c. FF:FF:FF:FF:FF:FF
-

- a. This is a unicast address because A in binary is 1010 (even).
- b. This is a multicast address because 7 in binary is 0111 (odd).
- c. This is a broadcast address because all digits are F's.

Figure 13.8 *Categories of Standard Ethernet (PHYSICAL LAYER)*



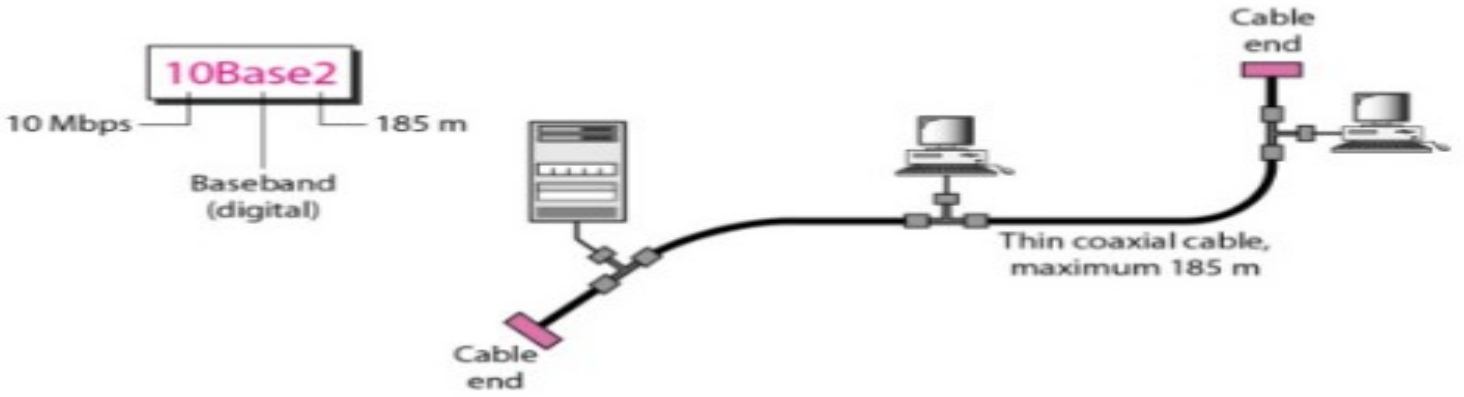
1O Base 5 implementation (Thick-ethernet)



- The first implementation is called 10Base5, thick Ethernet, or Thicknet(cable is thick and rough).
- It uses 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

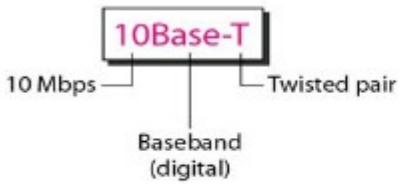
10Base2: Thin Ethernet

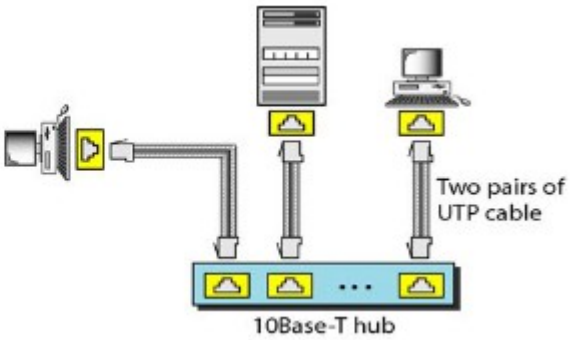
- The second implementation is called 1OBase2, thin Ethernet, or Cheapernet.
- 1OBase2 also uses a bus topology, but the cable is much thinner and more flexible.
- The transceiver is normally part of the network interface card (NIC), which is installed inside the station.
- It is cheaper beause of use of thin coaxial cable and tee.



1OBase-T: Twisted-Pair Ethernet

- The third implementation is called lOBase-T or twisted-pair Ethernet.
- 1OBase-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.
- 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.
- The maximum length of the twisted cable here is defined as 100 m





1OBase-F: Fiber Ethernet

- 1OBase-F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables.
-

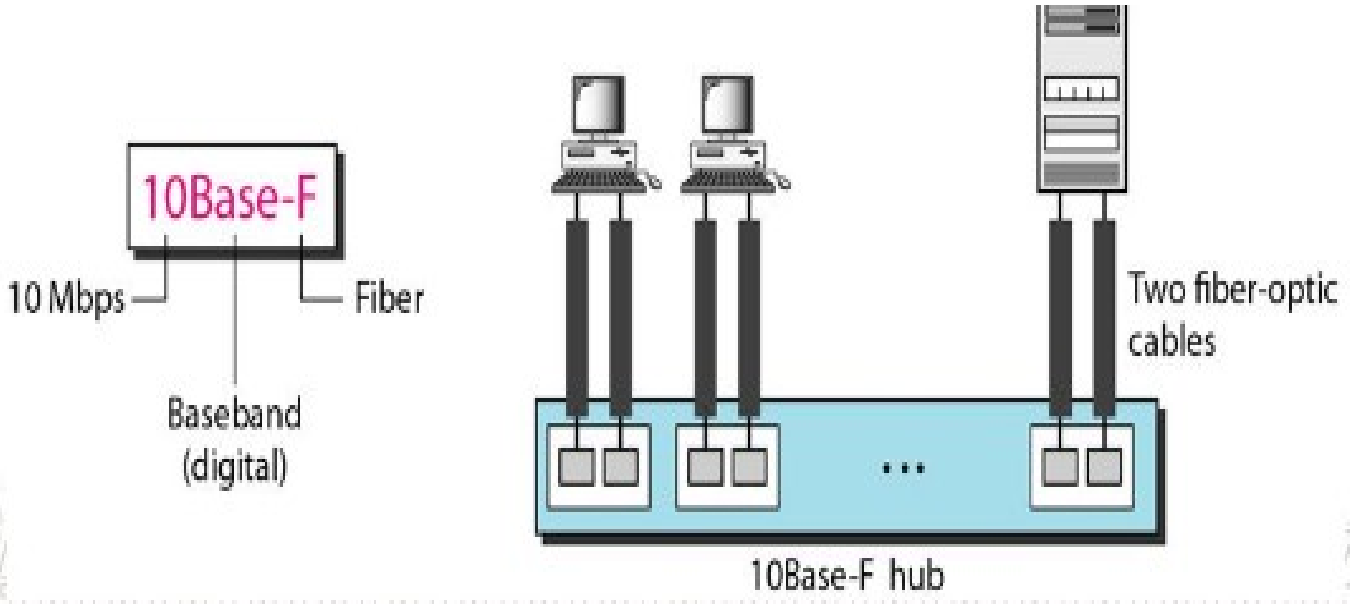
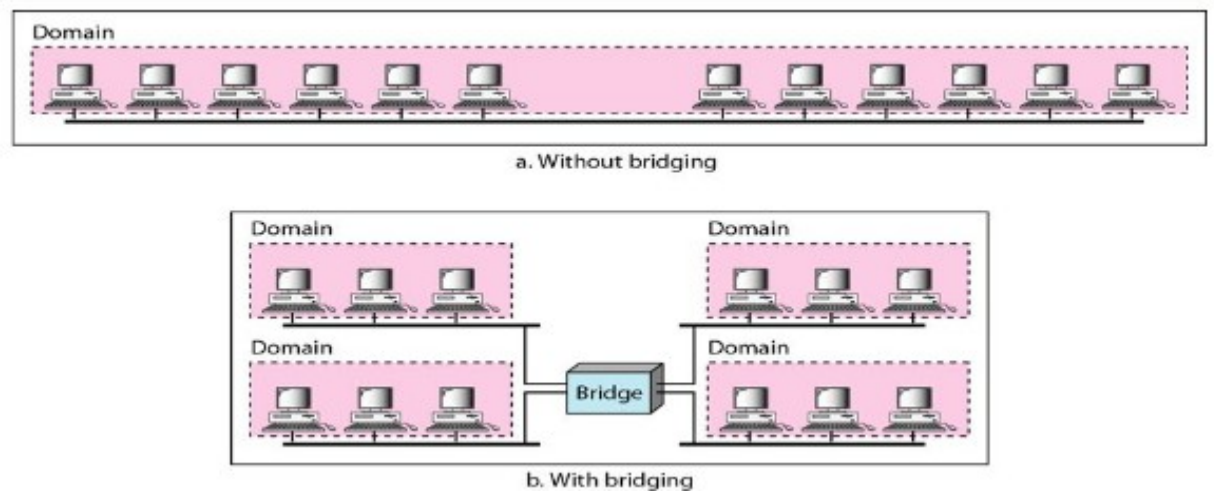


Table 13.1 *Summary of Standard Ethernet implementations*

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

Bridged Ethernet

- It means division of a LAN by bridges.
- Bridges have two effects on an Ethernet LAN: They raise the bandwidth and they separate collision domains.
- **Raising the Bandwidth:**

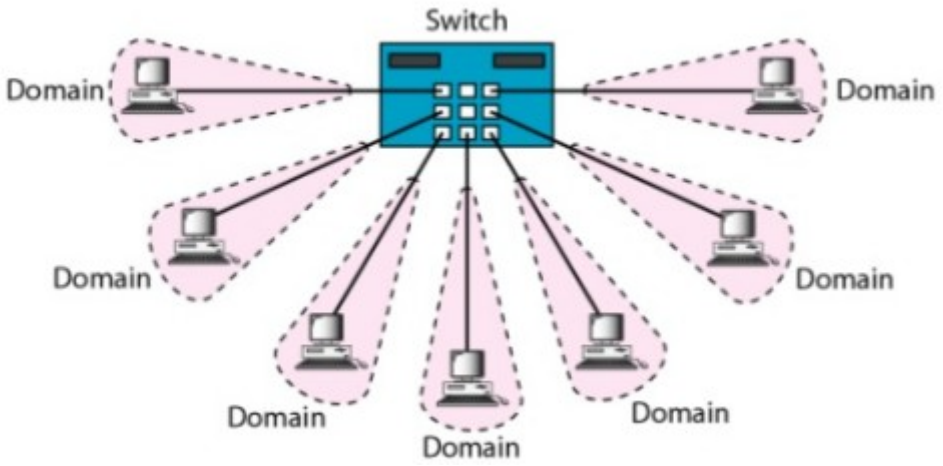


- A bridge divides the network into two or more networks and Bandwidth-wise, each network is independent.
- For example, as shown in figure,a network with 12 stations is divided into two networks,
- Each with 6 stations. Now each network has a capacity of 10 Mbps. The 1O-Mbps capacity in each segment is now shared between 6 stations (actually 7 because the bridge acts as a station in each segment).
- In a network with a heavy load, each station theoretically is offered 10/6 Mbps
- In unbridged network , 10 Mbps B/W is shared between 12 stations ,so it offers 10/12 Mbps Bandwidth.

- **Separating Collision Domains:** Another advantage of a bridge is the separation of the collision domain
- The collision domain becomes much smaller and the probability of collision is reduced tremendously.
- Without bridging, 12 stations contend for access to the medium; with bridging only 3 stations contend for access to the medium.

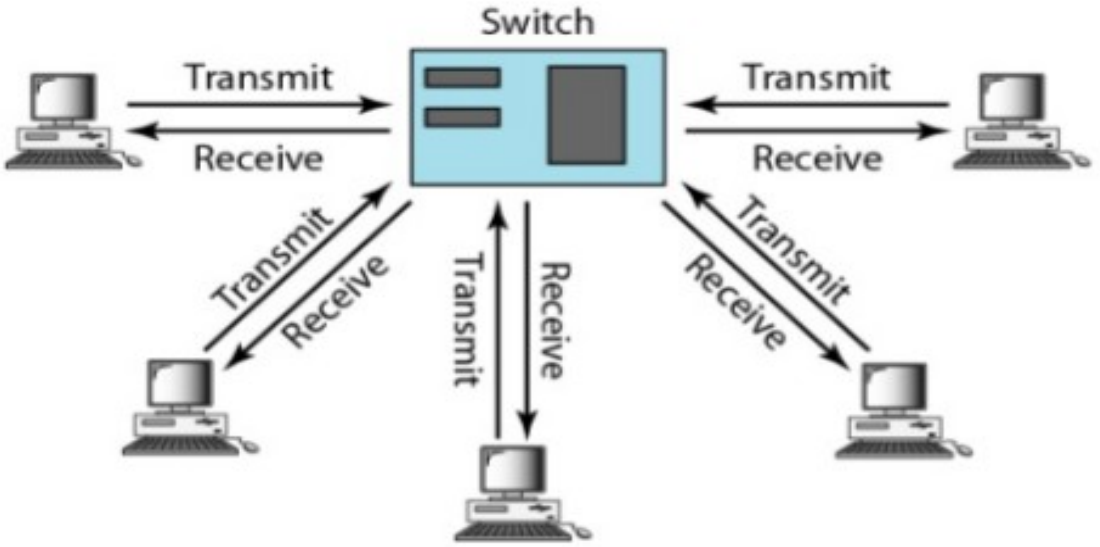
Switched Ethernet

- The idea of a bridged LAN can be extended to a switched LAN.
- Instead of having two to four networks using bridge,it has N networks(N is no. of stations)
- The bandwidth is shared only between the station and the switch (5 Mbps each).
- The collision domain is divided into N domains.
- It allows faster handling of the packets.
-



Full-Duplex Ethernet

- Switched Ethernet is extended to full-duplex switched Ethernet.
- The full-duplex mode increases the capacity of each domain from 10 to 20 Mbps.
- Instead of using one link between the station and the switch, the con-figuration uses two links: one to transmit and one to receive.
- There is no need for the CSMA/CD method
- **One of the limitations of 10Base5 and 10Base2 is that communication is half-duplex And 10Base-T is always full-duplex.**



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.
6. It uses star topology with 2 choices such as half duplex and full duplex.
7. CSMA/CD is used in half duplex and not in a full duplex mode.
8. Autonegotiation:A new feature added to Fast Ethernet is called autonegotiation.

- **Autonegotiation:**
- Autonegotiation allows two devices to negotiate the mode or data rate of operation.
- It 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).
- It allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.
-

Fast Ethernet Implementation

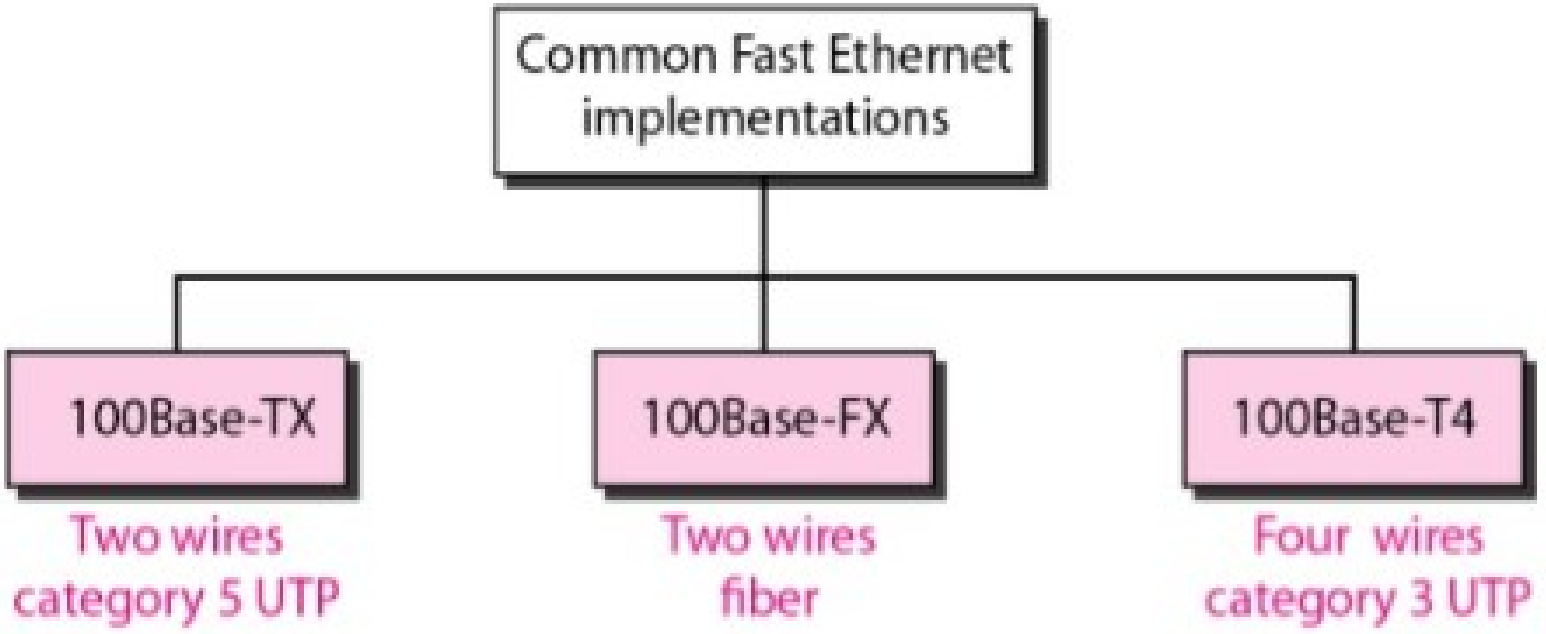


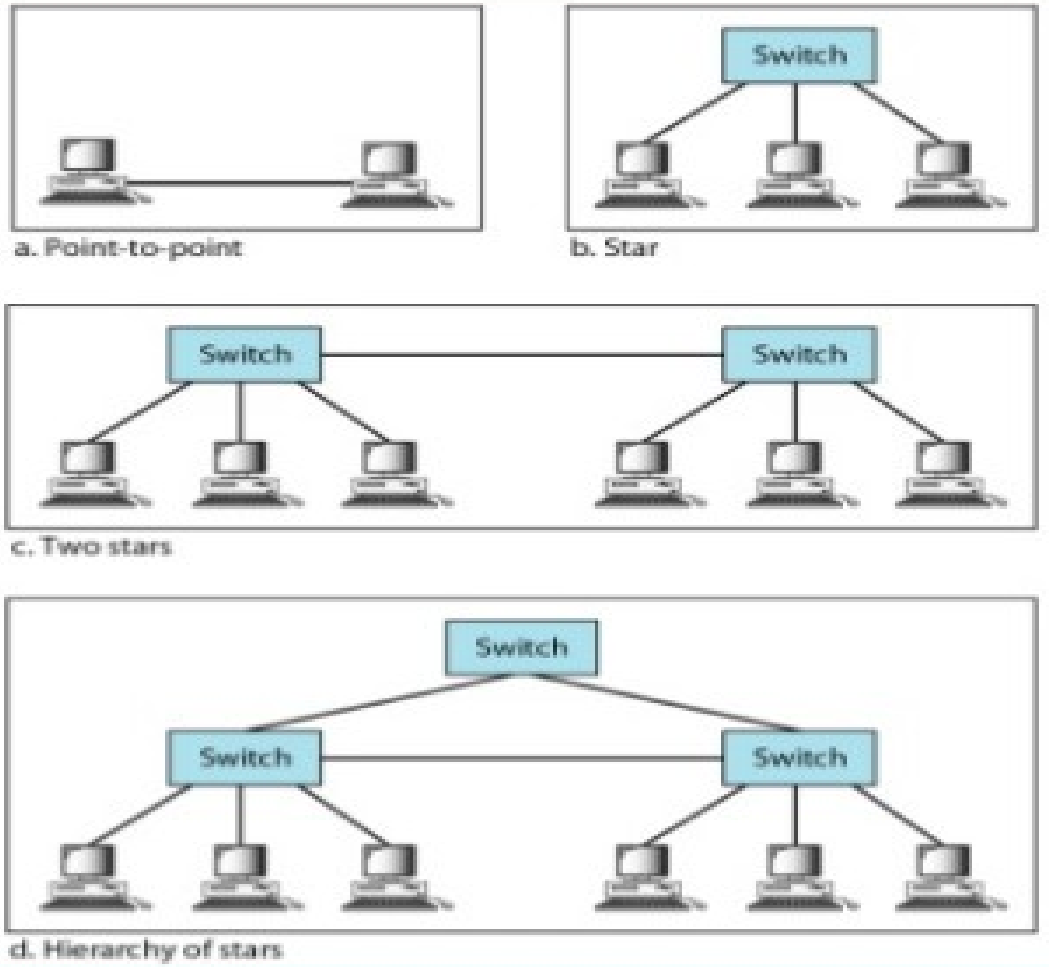
Table 13.2 *Summary of Fast Ethernet implementations*

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

GIGABIT ETHERNET

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address(mac addres).
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support autonegotiation as defined in Fast Ethernet.
7. It uses 2 approaches for medium access: half-duplex and full-duplex but mainly full-duplex is used.

Figure 13.22 *Topologies of Gigabit Ethernet*



a. Point-to-point

b. Star

c. Two stars

d. Hierarchy of stars

Implementation of Gigabit Ethernet

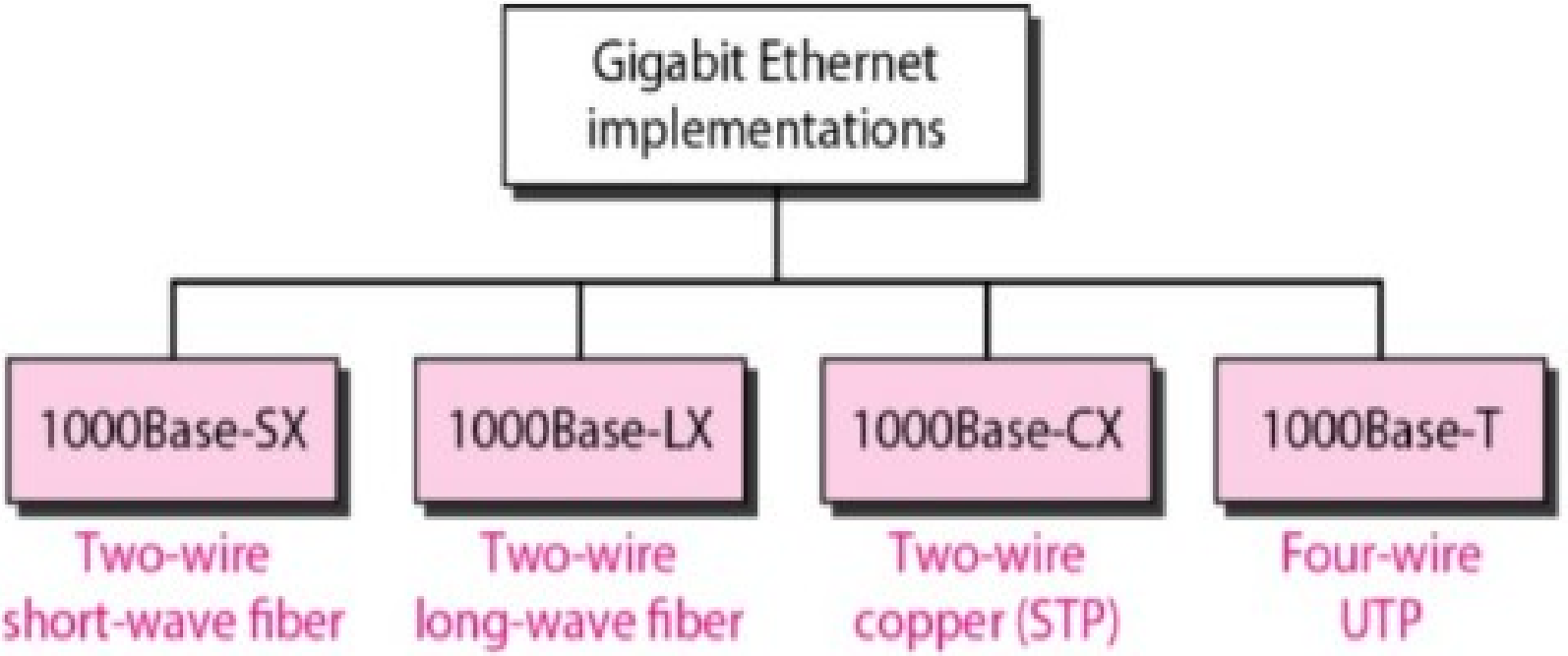


Table 13.3 *Summary of Gigabit Ethernet implementations*

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	550m	5000m	25m	100m
Block encoding	8B/10B	*8B/10B*	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Ten-Gigabit Ethernet

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

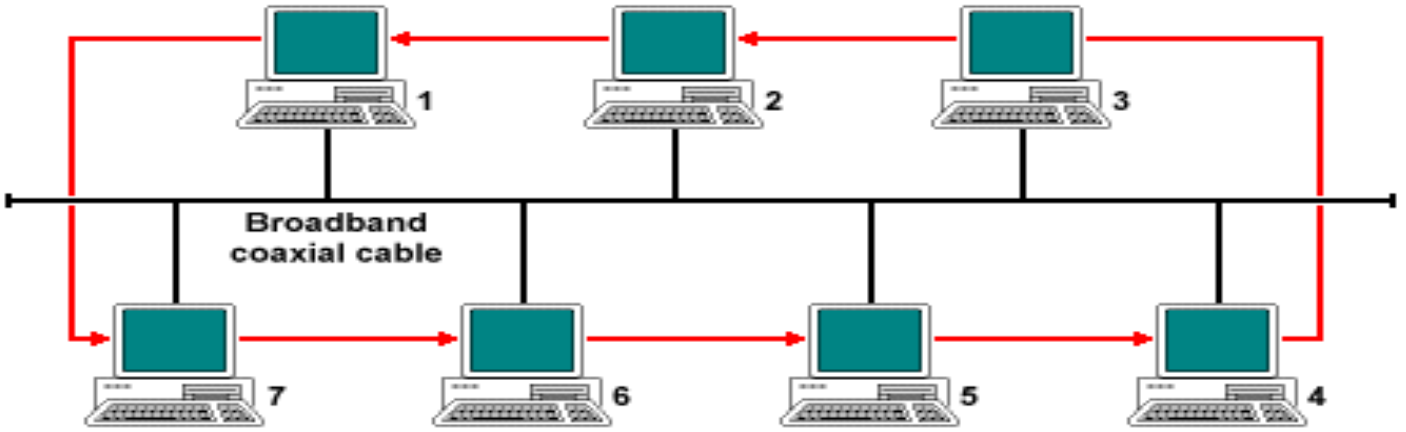
Gigabit Ethernet Implementations.

Table 13.4 *Summary ofTen-Gigabit Ethernet implementations*

Characteristics	*lOGBase-S*	*lOGBase-L*	*lOGBase-E*
Media	Short-wave S50-nrn rnultimode	Long-wave 131O-nrn single mode	Extended 1550-mrn single mode
Maximum length	300m	lOkm	40km

Token Bus (IEEE 802.4)

- It is a Local Area Network (LAN) in which the stations on the bus or tree form a logical ring.
- All stations are placed in an ordered sequence like bus topology.
- It operates at 1,5, 10 Mbps.
- It uses FSK modulation tech.
- Uses carrier band(single channel) or broadband(multiple channel) transmission.



A Token Bus network

Media access control in Token Bus

- Station which holds the token only can transmits it's data frame on the bus.
- Data frame contains source and destination address, so destined station accept frame and other will discard it.
- Once station finish it's transmission, will pass the token to it's neighbour.
- i.e. Token circulates through the ring and each station will get apportunity to transmit.

Token Ring(IEEE 802.5)

- Consists of a set of nodes connected in a ring.
- Data flows in a particular direction only.
- Data received from upstream neighbour and forwarded to downstream neighbour.
- Token – access to the shared ring

  – a special sequence of bits

  – circulates around the ring.
- Each node receives and forwards token.
- Frame makes its way back to sender .That frame removed by sender and sender reinsert token.
- As token circulates around ring, each station gets a chance to transmit
- Date rate: 4 Mbps or 16 Mbps
- encoding: differential manchester
- 802.5 connects upto 250 station

Wireless LAN(IEEE 802.11)

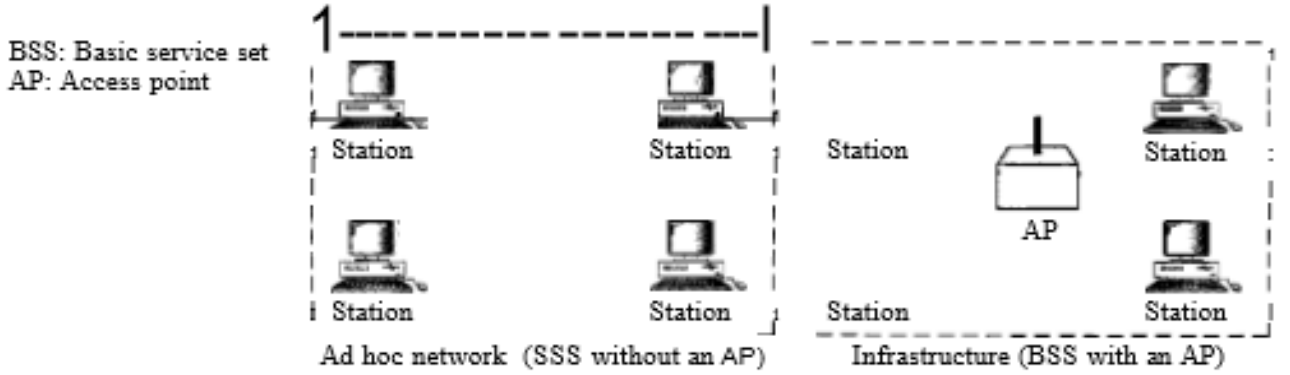
Architecture:

The standard defines two kinds of services:

1. The basic service set (BSS)
2. The extended service set (ESS).

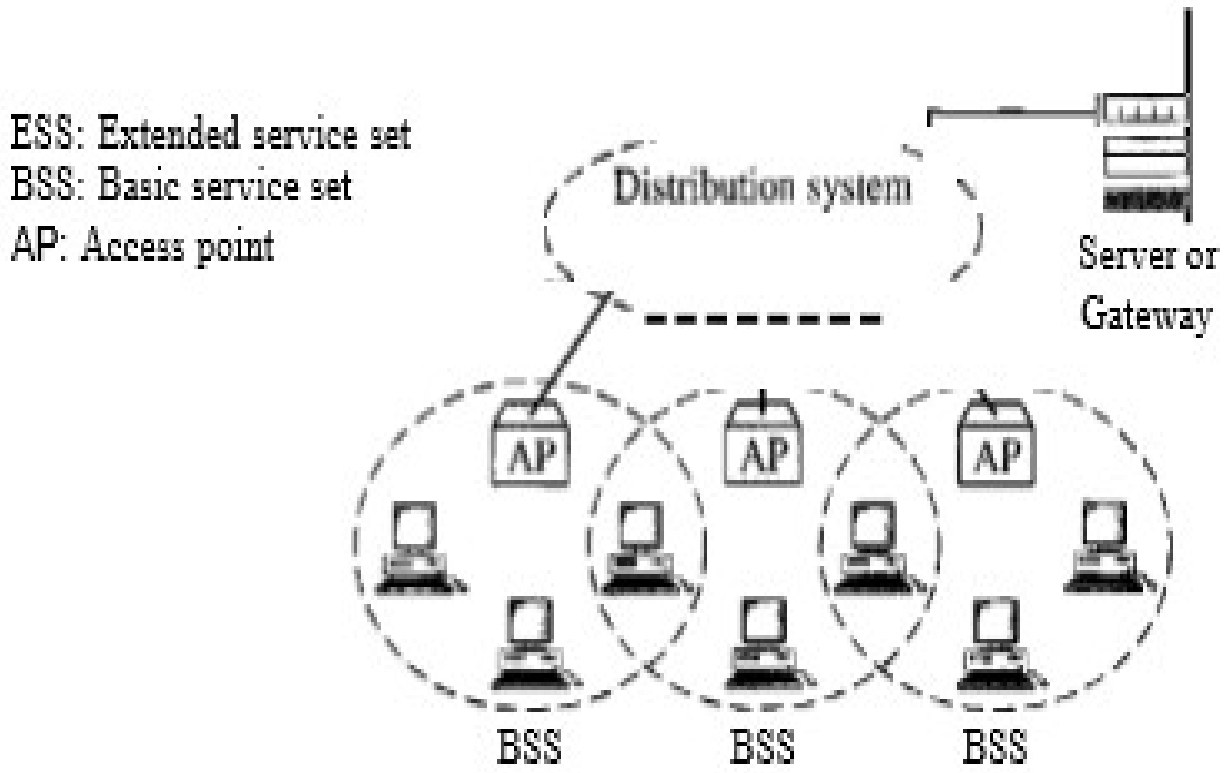
- **Basic Service Set:**
- It is building block of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
- A BSS without an AP is called an ad hoc network; a BSS with an AP is called an infrastructure network.
-

Figure 14.1 *Basic service sets (BSSs)*



- **Extended Service Set:**
- An extended service set (ESS) is made up of two or more BSSs with APs.
- The BSSs are connected through a distribution system, which is usually a wired LAN.(Ethernet)
- The distribution system connects the APs in the BSSs.
- 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 14.2 *Extended service sets (ESSs)*



Station Types

- IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN.

1. **No-transition:**A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
2. **BSS·transition:** A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
3. **ESS-transition mobility:** A station with ESS-transition mobility can move from one ESS to another.

	802.11	802.11a	802.11b	802.11g
Operating Frequency	2.4 GHz	5 - 6 GHz	2.4 GHz	2.4 GHz
Data rates	1 to 2 Mbps (PSK Modulation)	6 Mbps, 12 Mbps, or 24 Mbps (OFDM -54 Mbps)	11 Mbps complementary code keying (CCK)	54 Mbps
Specification	WLAN	Wi-Fi 5	Wi-Fi	offers the best features of both 802.11a and 802.11b
	No longer used		backward compatible with the 802.11	backward compatible with the 802.11b
Coverage Distance		400 feet	60 feet (need more access point)	

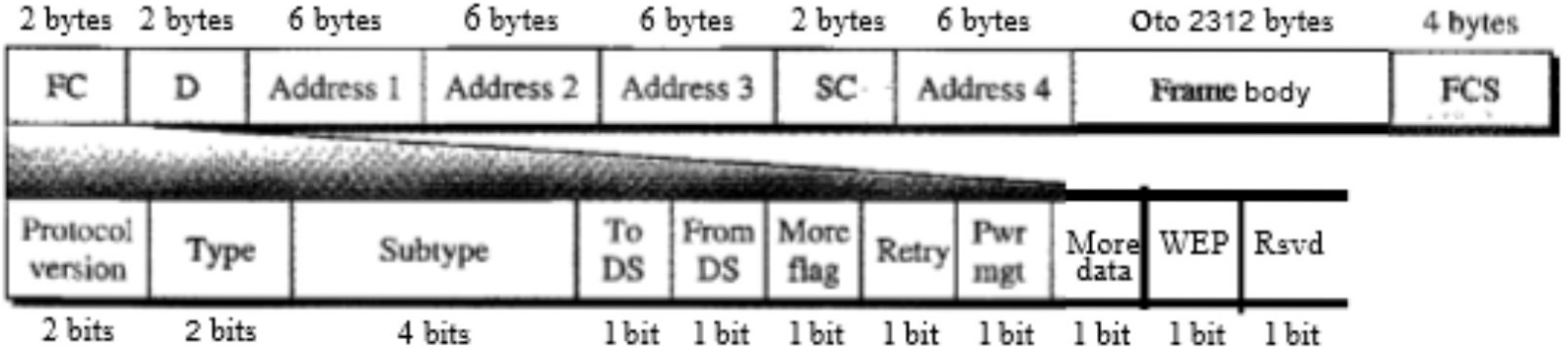
Table 2. Comparison Between IEEE 802.11a,b,g,n and ac[2]

802.11 network PHY standards								
802.11 protocol	**Release date**	**Frequency**	**Band-width**	**Stream Data Rate**	**Allowable MIMO streams**	**Modulation Antenna Tech.**	**Approx. range**	
							In	**Out**
		(GHz)	**(MHz)**	**Min-Max (Mbit/s)**			**(m)**	**(m)**
802.11	Jun 1997	2.4	22	1-2	1	DSSS, FHSS	20	100
a	Sep 1999	5	20	6-54	1	OFDM	35	120
		3.7				(SISO)	—	5K
b	Sep 1999	2.4	22	1-11	1	DSSS (SISO)	35	140
g	Jun 2003	2.4	20	6-54	1	OFDM, DSSS (SISO)	38	140
n	Oct 2009	2.4/5	20	7.2 -72.2 (6.5- 65)	4	OFDM (MIMO)	70	250
			40	15 - 150 (13.5 - 135)			70	250
ac	**Dec 2013**	**5**	**20**	**7.2 - 96.3 (6.5 - 86.7)**	**8**	**OFDM (MU-MIMO)**	**35**	
			40	**15 - 200 (13.5 - 180)**			**35**	
			80	**32.5 - 433.3 (29.2 - 390)**			**35**	
			160	**65 - 866.7 (58.5 - 780)**			**35**	

Fragmentation

- The wireless environment is very noisy; a corrupted frame has to be re-transmitted.
- The protocol, therefore, recommends fragmentation-the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.
-

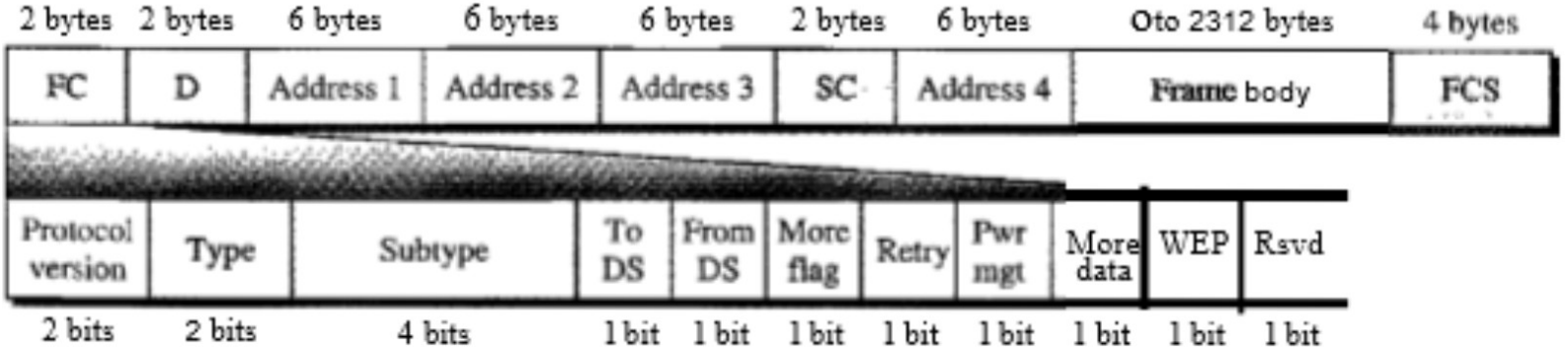
Figure 14.7 *Frameformat*



Fragmentation

- The wireless environment is very noisy; a corrupted frame has to be re-transmitted.
- The protocol, therefore, recommends fragmentation-the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.
-

Figure 14.7 *Frameformat*



- **Frame control (FC).** The FC field is 2 bytes long and defines the type of frame and some control information.

Table 14.1 *Subfields in FC field*

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)
ToDS	Defined later
FromDS	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:** This field defines the duration of the transmission.
- **D 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 sub fields
- **D Sequence control:** This field defines the sequence number of the frame to be used in flow control.
- **D Frame body.:**This field, which can be between 0 and 2312 bytes, contains information based on the type and the sub type defined in the FC field.
- **D 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:
  1. M**anagement frames:** used for the initial communication

  2**. Control frames :** used for accessing the channel and acknowledging frames.

  3. **Data frames.**

-

Table 14.2 *Values of subfields in control frames*

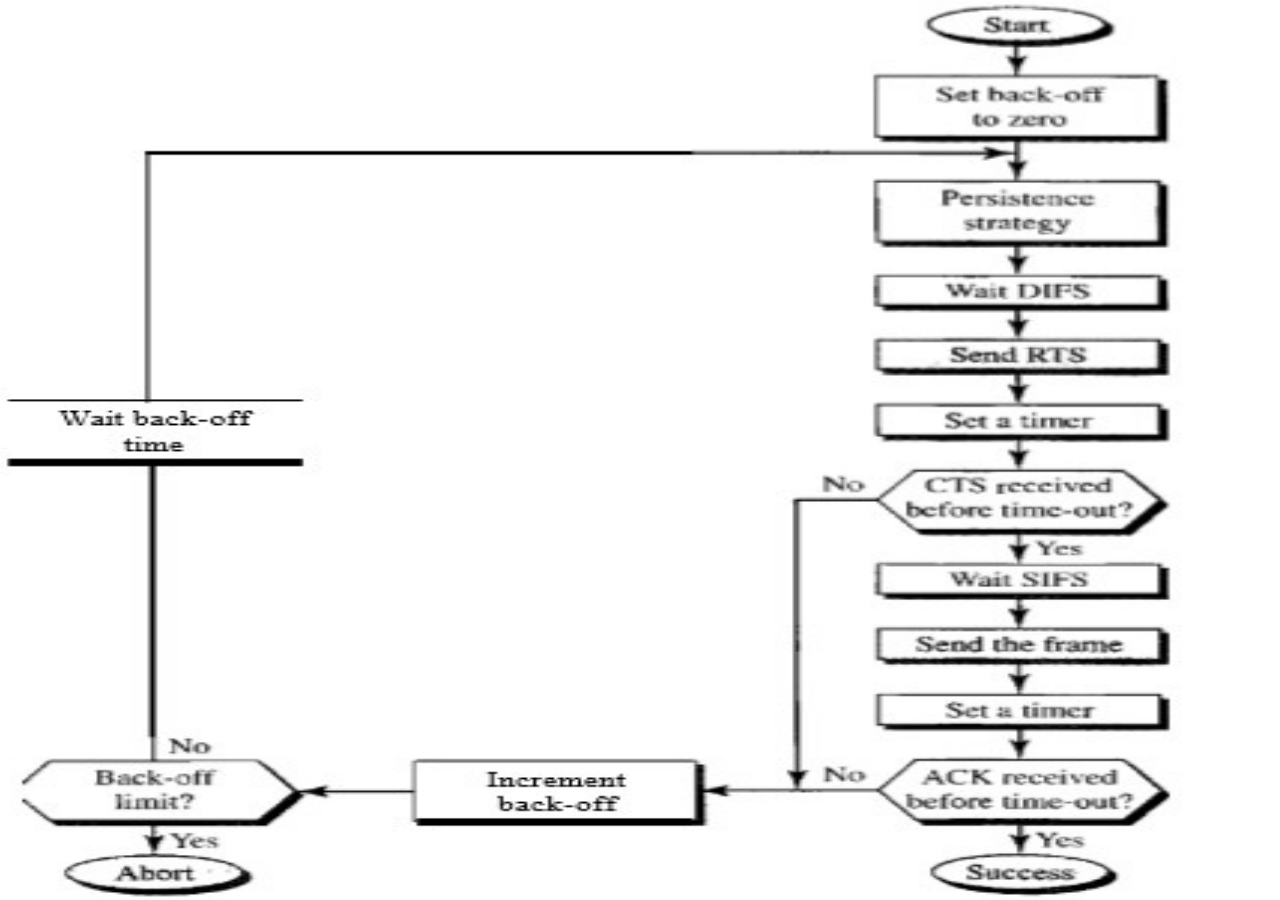
Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Media Access Control Methods

- Wireless Lan(802.11n) uses 2 techniques for media access control.
  - DCF: Distributed Coordination Function.
  - PCF: Point Co-ordination Function

Distributed Coordination Function(DCF)

- It is the protocol defined by IEEE at MAC sub layer.
- DCF uses CSMAICA to handle the collision.
- **Figure 14.4** *CSMAICA flowchart*



- Before sending a frame, the source station senses the medium by checking the energy level.
- The channel uses a persistence strategy with back-off until the channel is idle.
- After the station is found to be idle, the station waits for a period of time called the distributed inter-frame space (DIFS) and then the station sends a control frame called the request to send (RTS).
- After receiving the RTS and waiting a period of time called the short inter-frame 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.
- The source station sends data after waiting an amount of time equal to SIFS.
- The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.

Point Coordination Function (PCF)

- The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network).
- It is used mostly for time sensitive transmission.
- PCF has a centralized, contention-free polling access method.
- The AP performs polling for stations one after another, sending any data they have to the AP.
- PCF has more priority than DCF.

Inter Frame Spacing(IFS)

- IFS refers to the time interval between the transmission of two successive frames by any station.
- Types of IFS
  - Short Inter Frame spacing(SIFS)
  - PCF Inter Frame Spacing(PIFS)
  - DCF Inter Frame Spacing(DIFS)
  - Extended Inter Frame Spacing(EIFS)

- **SIFS:** It is shortest of all IFS and denotes highest priority to access the medium. It is defined for short control message such as acknowledgement and polling responses.

- **DIFS:**It is used by station that are operating under DCF mode to transmit packet. This is for asynchronous data transfer within contention period.
- **PIFS:**It is used by station that are operating under PCF mode to transmit packet. It's value lies between SIFS and DIFS .This is used for real time services.
- **EIFS:**It is longest of all the IFS and denotes the least priority to access the medium. It is used for re synchronization whenever physical layer detects incorrect MAC frame reception.

RTS-CTS Mechanism

- It is four-way handshaking technique to be optionally used for a packet transmission.
- It is used to avoid collision in wireless Lan.
- A station that wants to transmit a packet, waits until the channel is sensed idle for a DIFS, follows the back-off rules .
- instead of the packet, preliminary transmits a special short frame called *Request To Send (RTS).*
- *When the receiving station* detects an RTS frame, it responds, after a SIFS, with a *Clear To Send (CTS) frame.*
-

RTS/CTS Mechanism

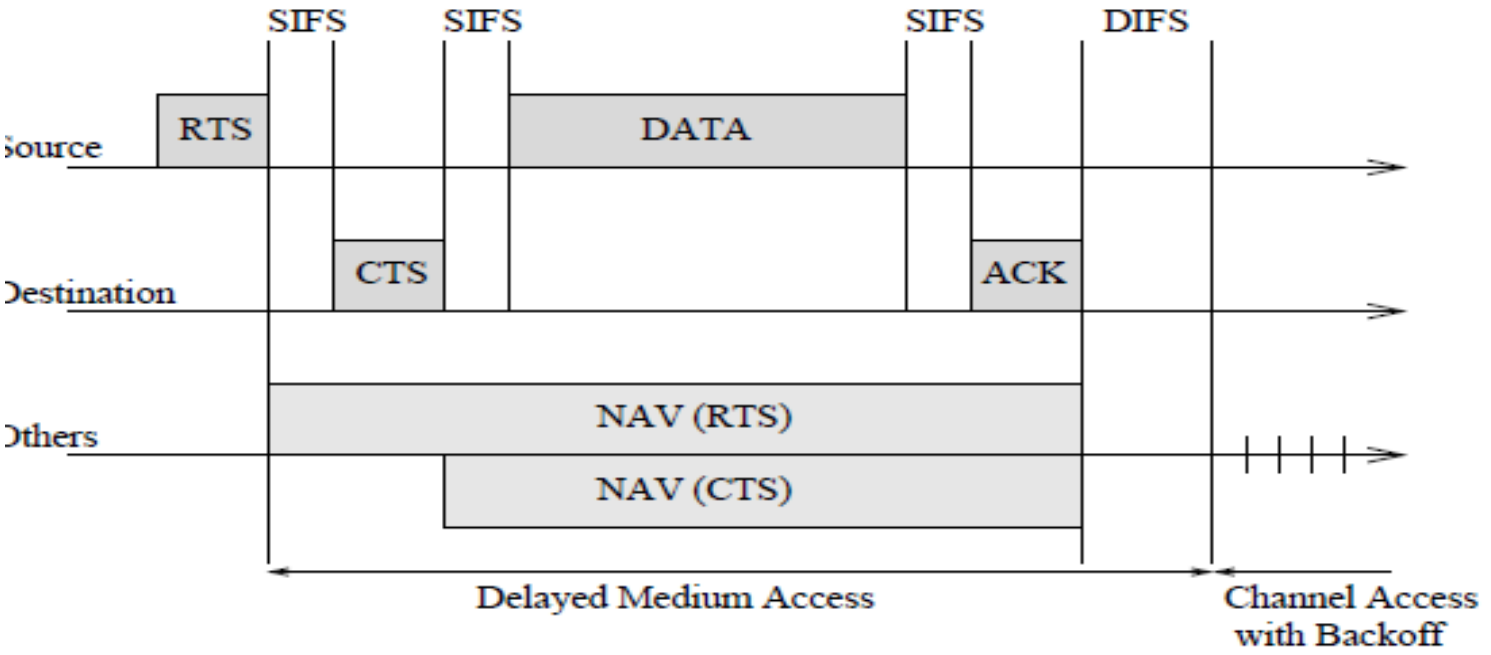


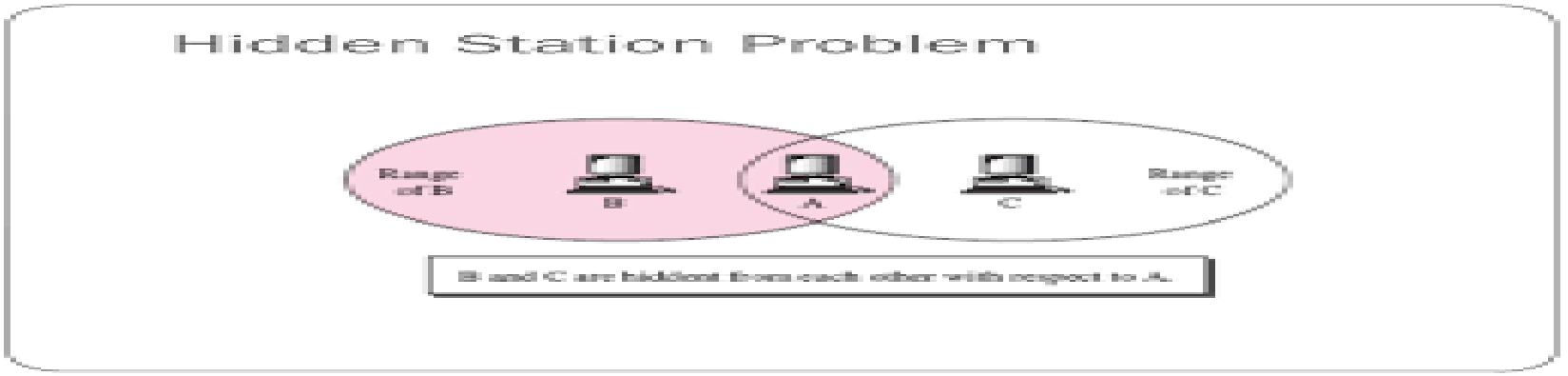
Fig. 2. *RTS/CTS Access Mechanism*

- The sender sends RTS packet to receiver.
- RTS is received by all the stations that can hear the sender.
- Every station that receives the RTS packet will set NAV (Network Allocation Vector) accordingly and it specifies earliest time at which the station is allowed to attempt transmission.(i.e. When transmission is completed)
- The intended receiver waits for SIFS and send CTS packet (it is ready to receive data)
- All stations receiving CTS will set their NAV.
- After receiving CTS, Sender waits for SIFS and then send the data.
- Once RTS is send and CTS is received then all nearby nodes of sender and receiver understand that medium has been reserved .
- After receiving data, the receiver waits for SIFS and send ACK.
- As soon as transmission is completed the NAV in each node will mark medium as free and process can repeat again.
- The collision can takes place only at the beginning i.e. when RTS and CTS are send.

Problems in WLAN

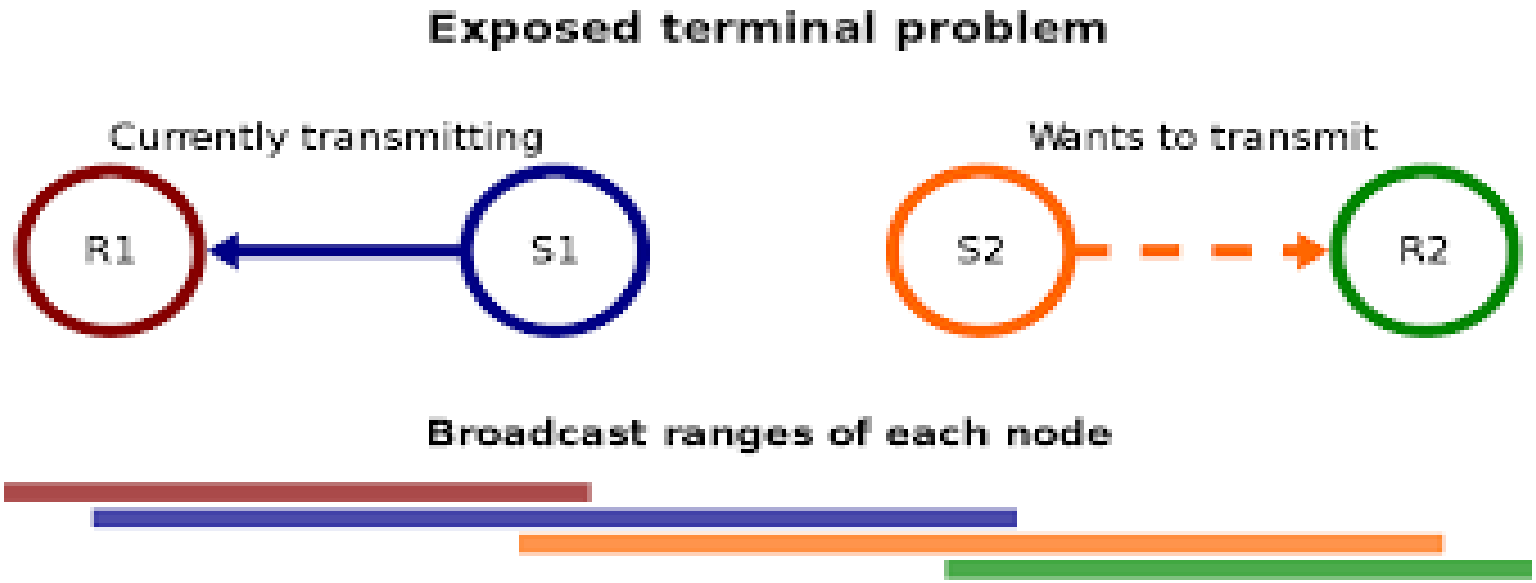
- Hidden Station Problem
- Exposed station problem
- Multi path Fading

Hidden Station Problem



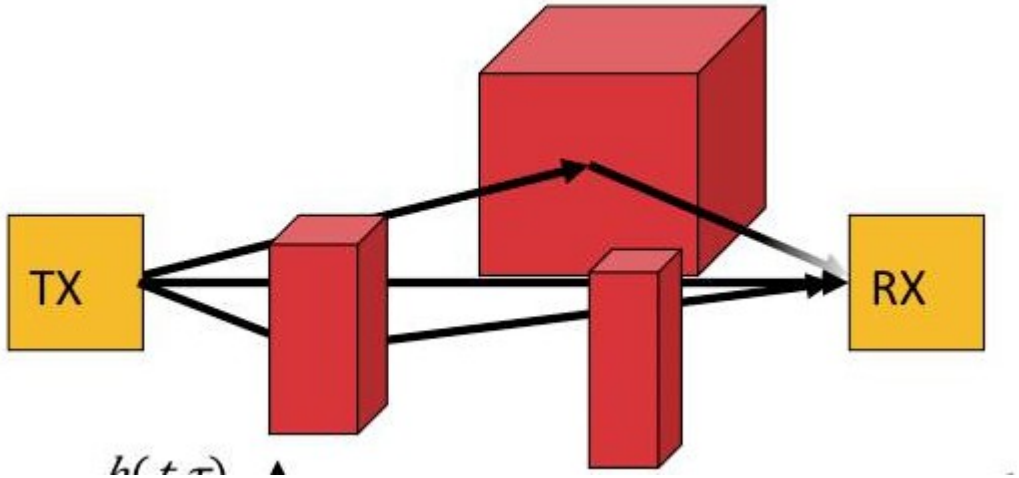
- B is transmitting to A.
- C wants to transmits to node A, C is unknown to B and starts transmission to node A
- Hence, Collision occurs and discards both the frames.

Exposed station problem



Multipath Fading

- In wireless N/w, signals gets reflected from solid material , so receiver will receives same signal multiple times from different path is known as multipath fading.
-



Advantages and Disadvantages of WLAN

- Advantages:
  - It is cheaper than wired LAN.
  - Used in Historical Buildings.
  - Possible to form WLAN using Laptops.
  - It uses WAP2 protocol which is secure.
- Disadvantages:
  - Spectrum assignments and operational conditions are not same worldwide.
  - Radiated power is limited to 100 mW.
  - WI-Fi has limited range of 35 m.
  - Wi-Fi n/w has less security and easily disrupted.

WPAN(IEEE 802.15)

- Examples of WPAN (802.15) are Bluetooth(IEEE 802.15.1), ZigBee (IEEE 802.15.4)

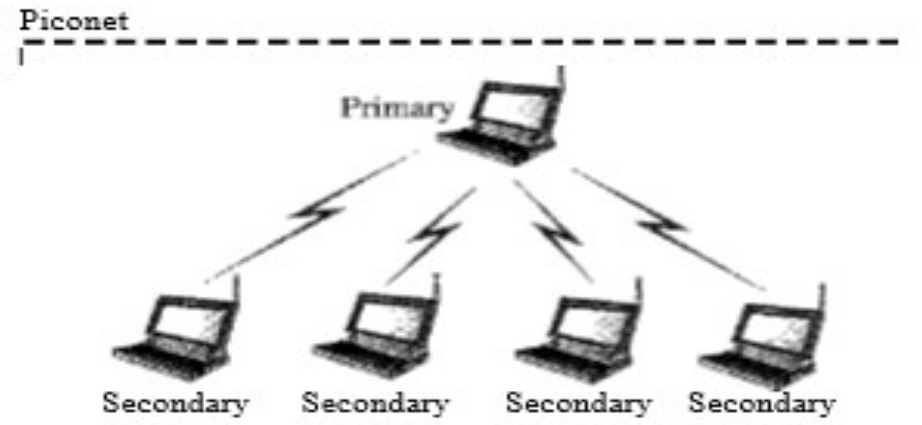
BLUETOOTH(IEEE 802.15.1)

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.
- A Bluetooth LAN, by nature, can- not be large.
- e.g. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.
- The current data rate is 1Mbps with a 2.4-GHz bandwidth

  Bluetooth defines two types of networks: piconet and scatternet.
-

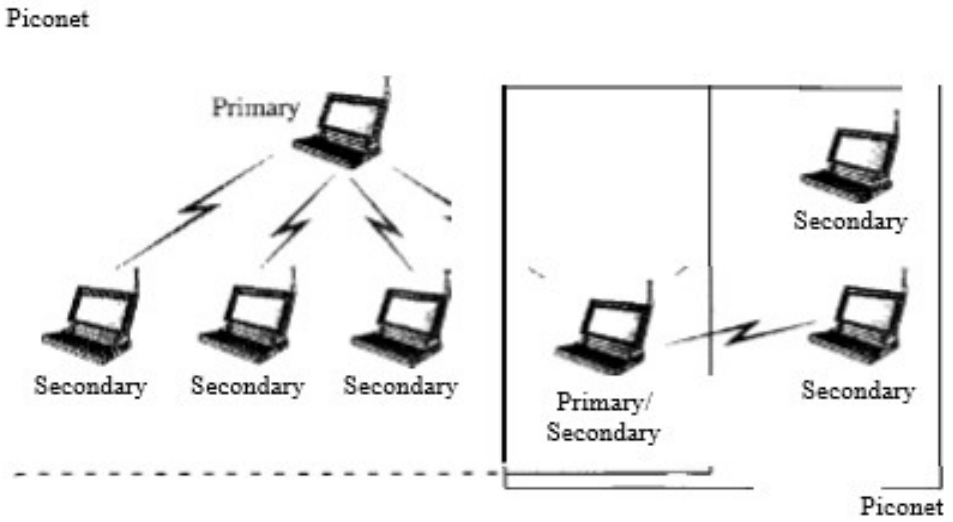
Piconets

- It is a small network.. A piconet can have up to eight stations.
- One of which is called the primary and the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- With seven secondaries, an additional eight secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state
- Only 8 nodes at a times takes place in communication.
-



Scatternet

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets.
- Figure 14.20 *Scatternet*



Link Manager Protocol(LMP)

- It is used to set and maintain the properties of Bluetooth Link.
- It has 2 main functions.
  - Power Management
  - Security Management.
- **Power Management:** For Power management Bluetooth operates in 4 modes.
  1. **Active Mode**:device participated actively and uses optimization techniques for power saving.
  2. **Sniff Mode**:This is Low power mode and listening activity of slave is reduced.
  3. **Hold Mode**: Slave temporarily stops supporting packets on channel.
  4. **Park Mode**:It is low power mode and slave goes into parking state.

- **Security Management:**
- Due to wireless nature, security is difficult to maintain.
- To maintain the security
  - Challenge response mechanism is provided for authenication.
  - Specific sequence of channel hopping is used and known to only sender and receiver.
  - 128 bit key encryption is used.

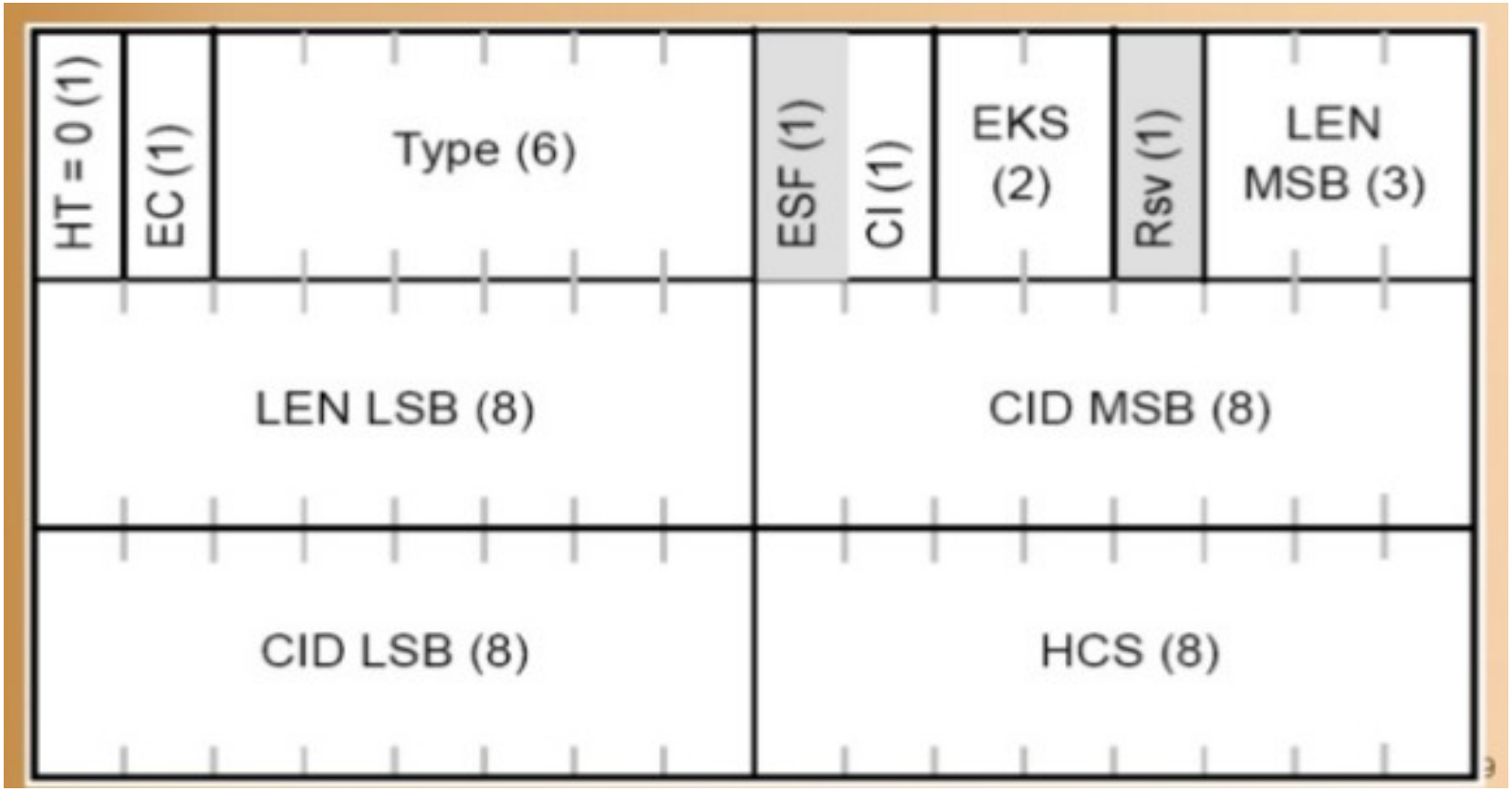
WI-MAX(IEEE 802.16)

- WI_MAX is Broadband wireless network.
- It is high-speed Internet service via wireless technology, available in Internet cafés, local “hot spots” within many cities, private businesses and many homes.
- A broadband wireless modem receives the service and transmits it via radio waves to the immediate surrounding area.
- **802.16 IEEE Standards**
- WIMax: 802.16.1 : (10-66 GHz, line-of-sight, up to 134Mbit/s).
- WMAN:802.16.2 : (minimizing interference between coexisting WMANs).
- 802.16a : (2-11 Ghz, Mesh, non-line-of- sight).
- 802.16b : (5-6 Ghz).| 802.16c : (detailed system profiles).| P802.16e : (Mobile Wireless MAN).
-

Features of WI-Max

- Use microwave signals for the wireless transfer of data.
- Specifies a frequency band in the range between 2 GHz to 66 GHz.
- Wimax is a wireless internet service that is capable of covering a wide geographical area by serving hundreds of users at a very low cost.
- Uses FDM ,good for multipath environments.
- Flexible channel sizes (3.5 MHz,5 MHz,10MHz)
- An easy and fast system to install.
- Leading to low installation cost, when compared to fiber ,cable or DSL deployments.

802.16 Frame Structure



- HT(Header type): For generic frame,HT=0
- EC (Encryption control) 0 = Payload is not encrypted ,1 = Payload is encrypted.
- Type : This field identifies the frame type ,whether packing and fragmentation is present.
- CI (CRC indicator) 1 = CRC is included . 0 = No CRC is included.
- EKS (Encryption key sequence) : Which encryption key is used.
- Length: Complete length of the frame including header.
- Connection ID: Which connection this frame belongs to
- Header CRC: Header check sequence. An 8-bit field used to detect errors in the header. Header check-sum using 100000111.
- ESF(Extended sub-header) ESF=0 ,absent:ESF=1.present