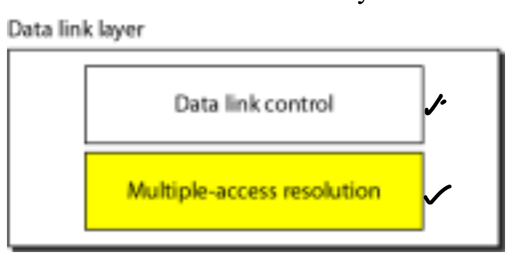
Network and Communication

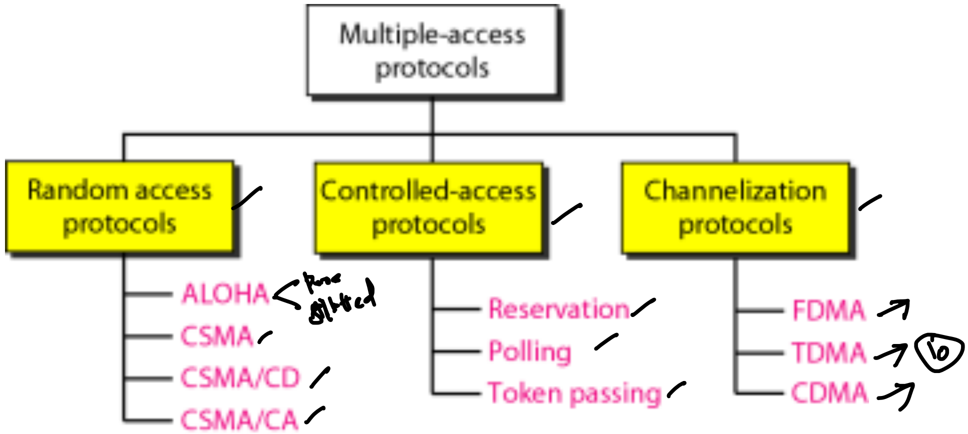
C. Sathiya Kumar
Associate Professor / SCOPE
VIT University

Multiple Access

- Data link layer divided into two functionality-oriented sublayers

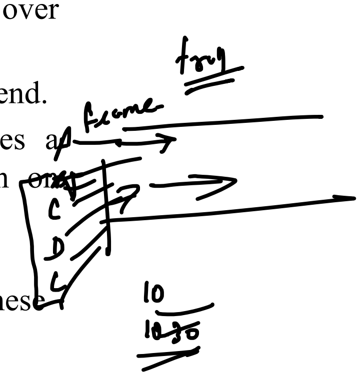


- IEEE has actually made this division for LANs.
- The upper sublayer that is responsible for flow and error control is called the logical link control (LLC) layer
- The lower sublayer that is mostly responsible for multiple access resolution is called the media access control (MAC) layer



Random Access or Contention

- In random access or contention methods, no station is superior to another station and none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.
- First, 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*.
- Second, 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.



ALOHA

- Earliest Random Access methods
- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

Pure ALOHA

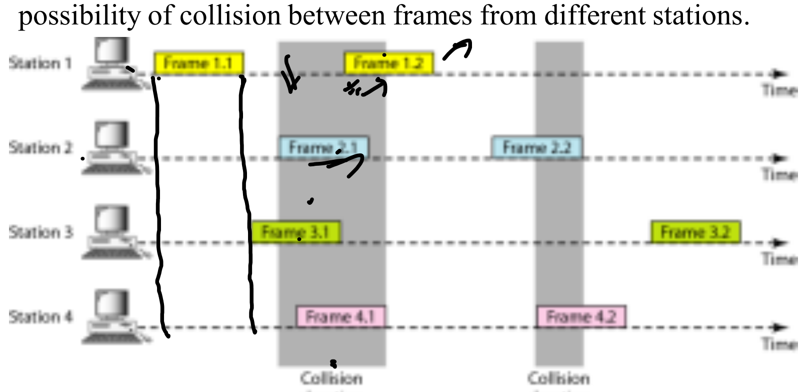
- The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol.

Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

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.



Pure ALOHA

- It is obvious that we need to resend the frames that have been destroyed during transmission.
- The pure ALOHA protocol relies on acknowledgments from the receiver.
- When a station sends a frame, it expects the receiver to send an acknowledgment.
- If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.
- A collision involves two or more stations.
- 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 a random amount of time before resending its frame

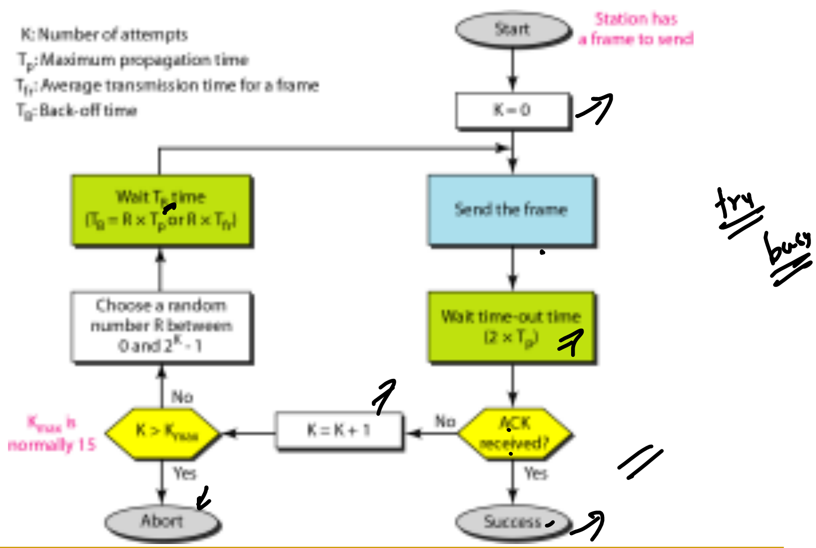
Data | Ack → resend

Pure ALOHA

- The randomness will help avoid more collisions. We call this time the back-off time *TB*.
- Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames.
- After a maximum number of retransmission attempts Kmax' a station must give up and try later.

K=0 ↑ ≤ Kmax

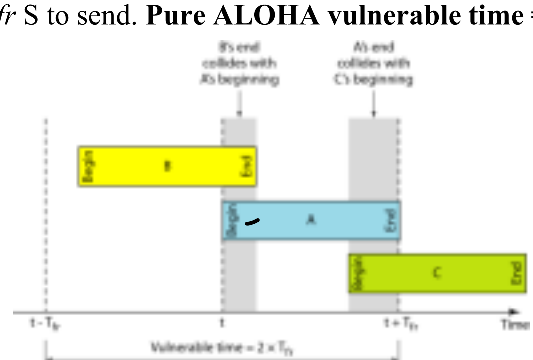
Pure ALOHA Procedure



Pure ALOHA

Vulnerable time

- The length of time, the **vulnerable time,** in which there is a possibility of collision.
- Assume that the stations send fixed-length frames with each frame taking *Tfr* S to send. **Pure ALOHA vulnerable time = 2 x Tfr**



Pure ALOHA - Throughput

Note

The throughput for pure ALOHA is

$S = G \times e^{-2G}$.

The maximum throughput

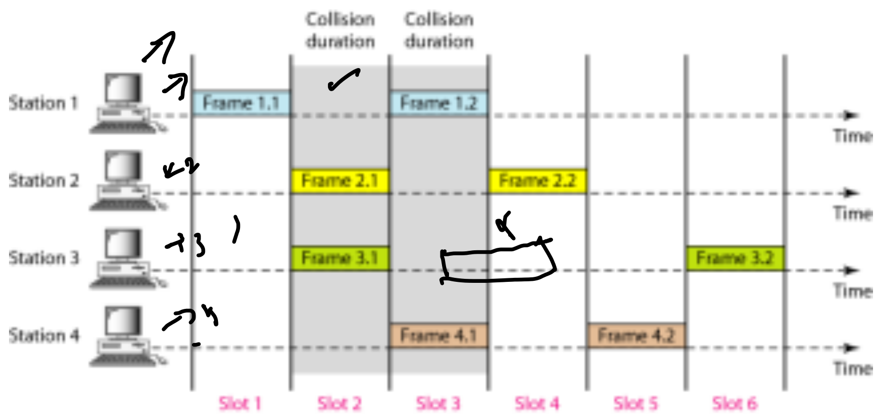
$S_{max} = 0.184$ when G= (1/2).

Slotted ALOHA

- Pure ALOHA has a vulnerable time of 2 x *Tfr* . This is so because there is no rule that defines 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 Tfr's and force the station to send only at the beginning of the time slot.

10:30

Slotted ALOHA



Slotted ALOHA

- 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.
- This means that the station which started at the beginning of this slot has already finished sending its frame.
- There is still the possibility of collision if two stations try to send at the beginning of the same time slot.
- However, the vulnerable time is now reduced to one-half, equal to

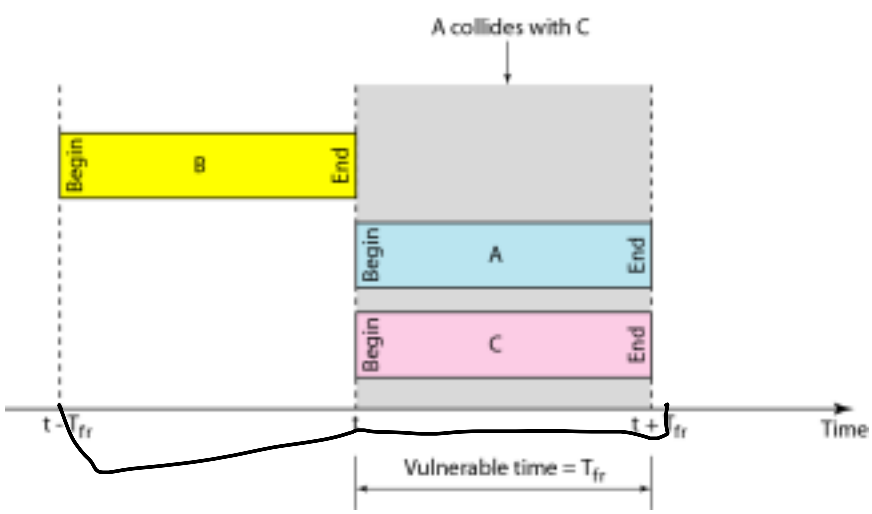
2xTfr

Slotted ALOHA vulnerable time = Tfr

Note

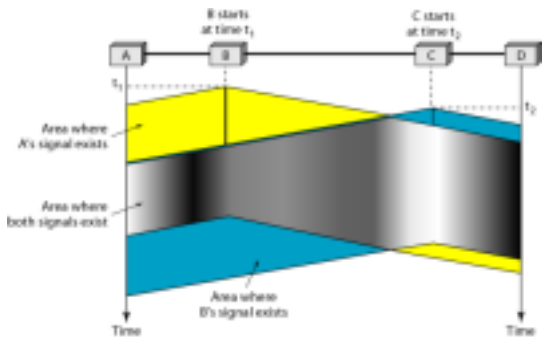
The throughput for slotted ALOHA is $S = G \times e^{-G}$.
The maximum throughput $S_{max} = 0.368$ when $G = 1$.

Slotted ALOHA – Vulnerable Time



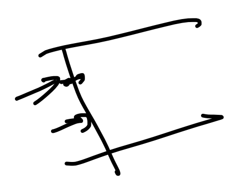
Carrier Sense Multiple Access (CSMA)

- (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.

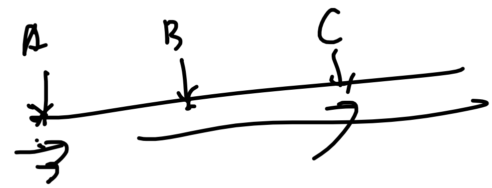


CSMA – Reason For Not Eliminate Collison

- Stations are connected to a shared channel (usually a dedicated medium).
- 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.

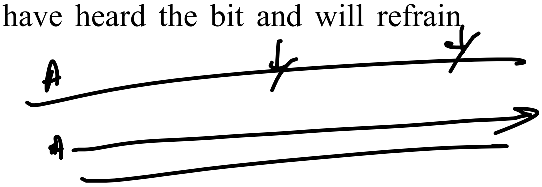


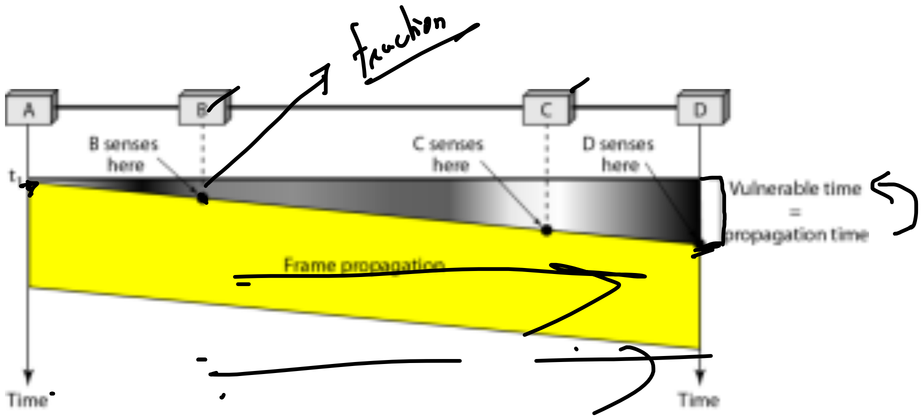
- At time *t1* station B senses the medium and finds it idle, so it sends a frame. At time
- *t2 (t2> t1)'* station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C.
- Station C also sends a frame. The two signals collide and both frames are destroyed.



CSMA - *Vulnerable Time*

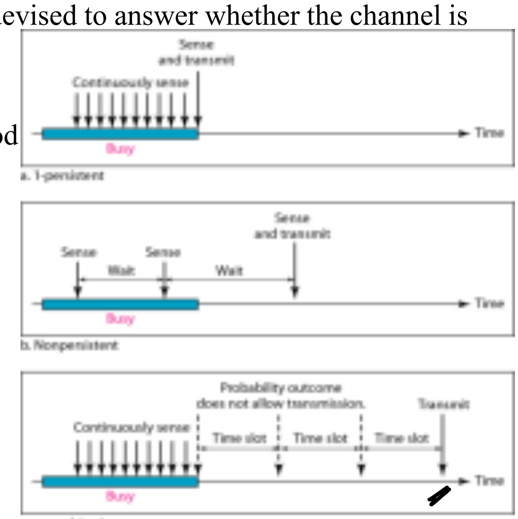
- The vulnerable time for CSMA is the propagation time *Tp* .
- The time needed for a signal to propagate from one end of the medium to the other.
- When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.
- If the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.





CSMA - *Persistence Methods*

- Three methods have been devised to answer whether the channel is busy or idle:
  - the I-persistent method
  - the non-persistent method
  - the p-persistent method



I-Persistent

- simple and straightforward. **A**fter 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.

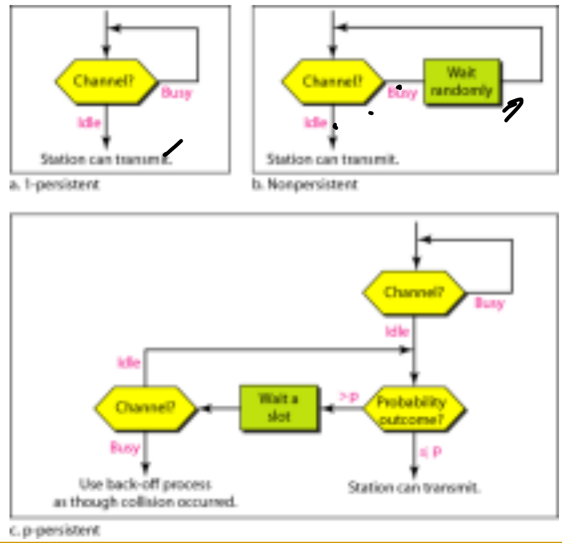
Non-persistent

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

p-Persistent

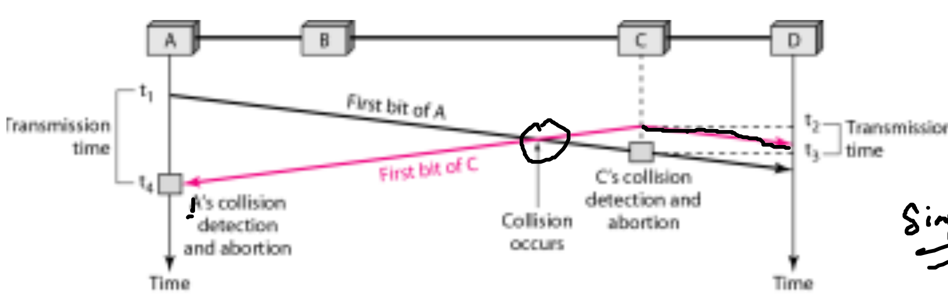
- the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.
- In this method, after the station finds the line idle it follows these steps:
  - With probability *p*, the station sends its frame.
  - With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.
    - If the line is idle, it goes to step 1.
    - If the line is busy, it acts as though a collision has occurred and uses the backoff
- procedure.

Flow Diagram For Persistant Methods



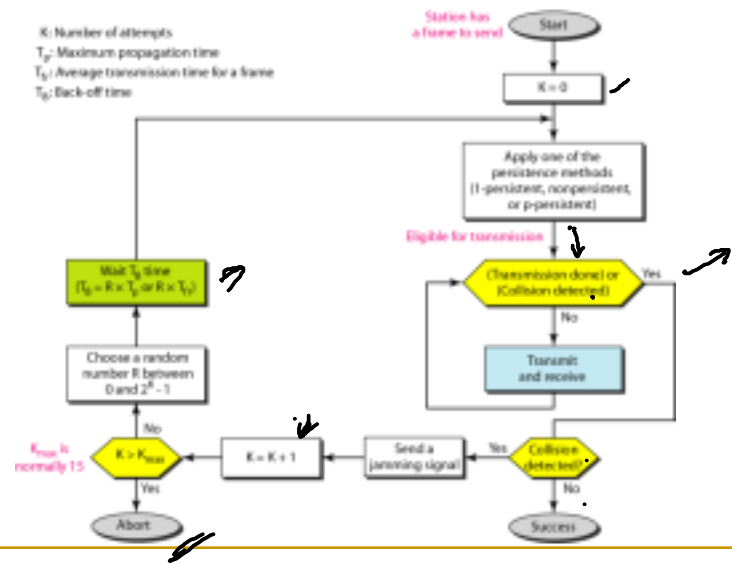
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- 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.



Single

Flow Diagram CSMA/CD

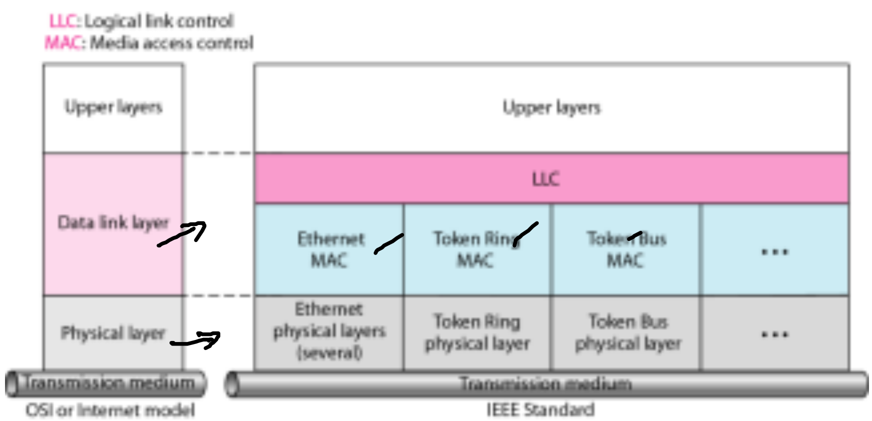


IEEE Standards

IEEE

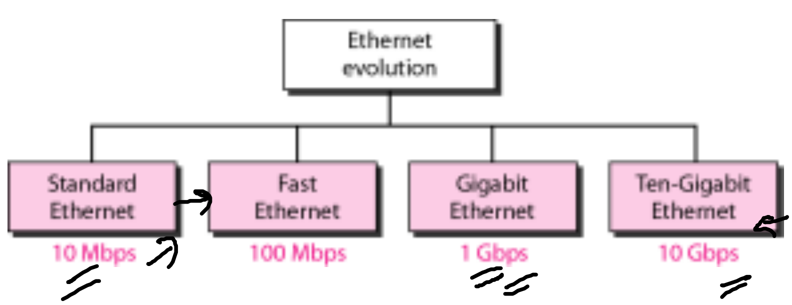
- In 1985, the Computer Society of the IEEE started a project, called Project 802,
- To set standards to enable intercommunication among equipment from a variety of manufacturers.
- Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

IEEE Standards for LAN



Standard Ethernet

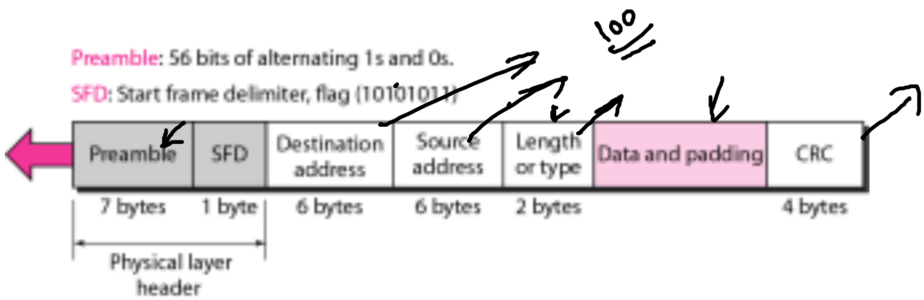
- The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations.



LAN

10Mb 100Mb

802.3 Ethernet MAC Frame



- **Preamble**. 7 bytes (56 bits) of alternating 0's and 1's that alerts the receiving system 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.

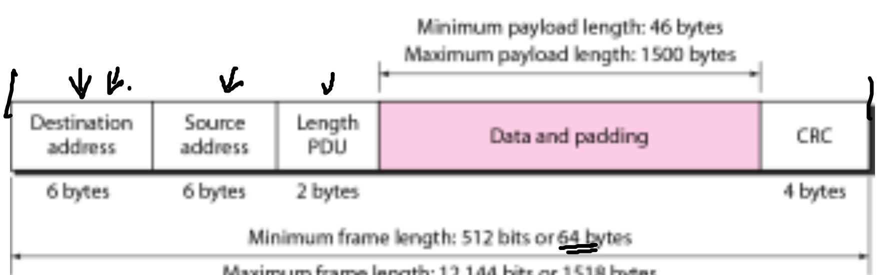
10101011 ← dest

- **Destination address (DA).** The DA field is 6 bytes and contains the physical address of the destination station
- **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

Minimum and Maximum Length

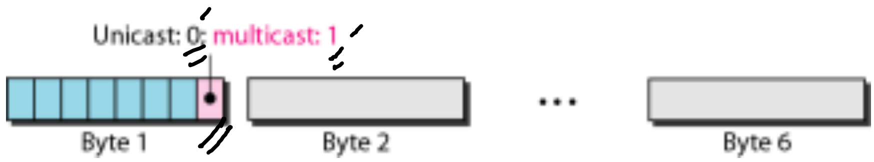
Pre & SFD



Note

Frame length:
Minimum: 64 bytes (512 bits)
Maximum: 1518 bytes (12,144 bits)

Unicast and Multicast Address



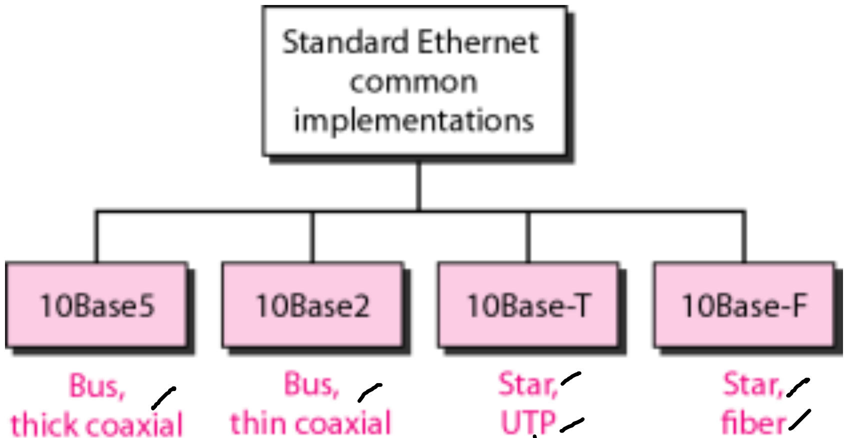
Note

The least significant bit of the first byte defines the type of address. If the bit is 0, the address is unicast; otherwise, it is multicast.

Note

The broadcast destination address is a special case of the multicast address in which all bits are 1s.

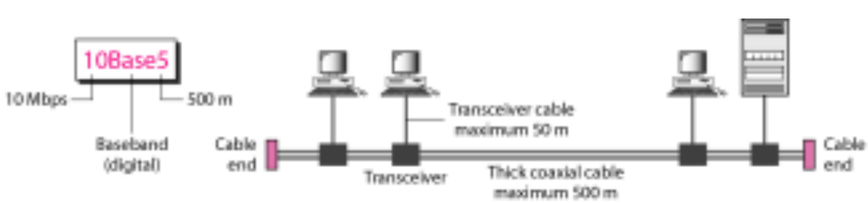
Categories of Standard Ethernet



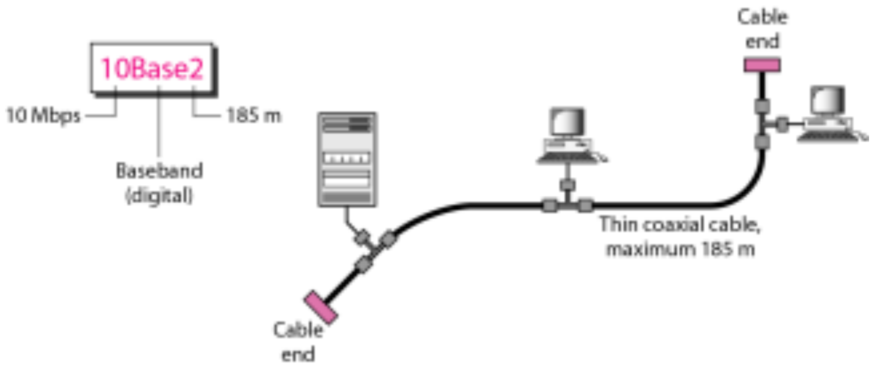
core cladding

light

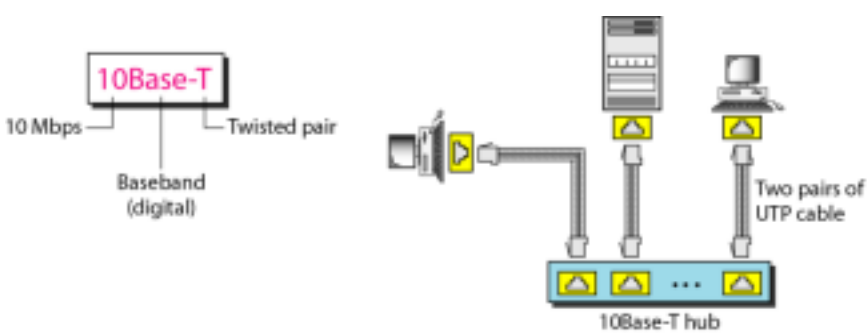
10Base5 Implementation



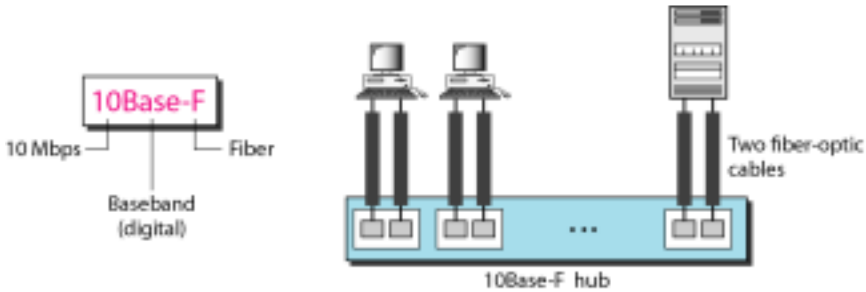
10Base2 Implementation



10Base – T Implementation



10Base – F Implementation



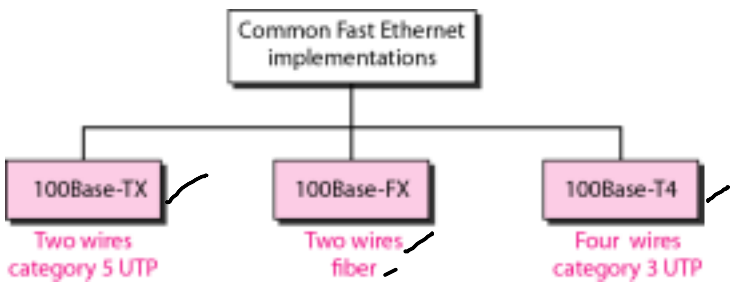
light

Repeated

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

Fast Ethernet

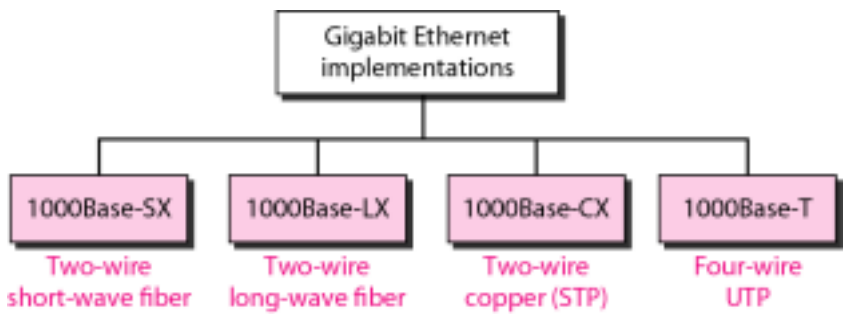
- Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.
- IEEE created Fast Ethernet under the name 802.3u.
- Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.



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

Gigabit Ethernet

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



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

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