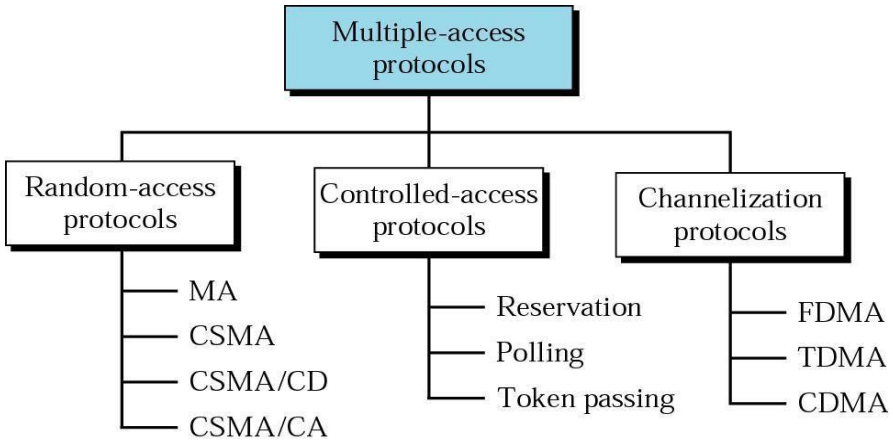
Introduction:

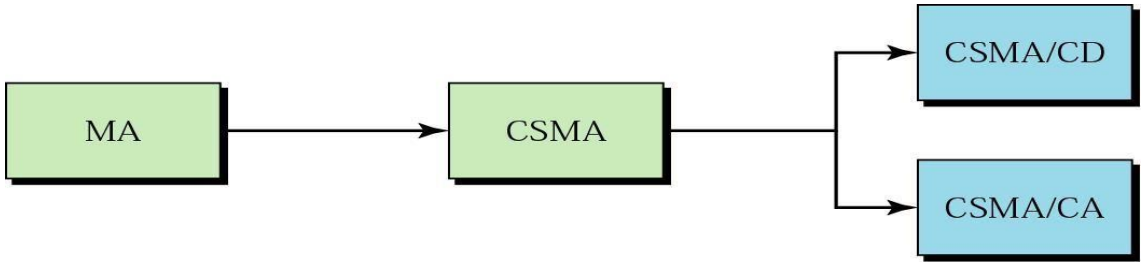
- Data link layer has two sub layers: Upper sub layer – Data link Control & Lower sub layer – Multiple access Control.
- The upper sub layer is responsible for flow and error control.
- The lower sub layer is responsible for multiple access resolution.
- When the nodes are connected using a dedicated link, lower sub layer is not required, but when the nodes are connected using a multipoint link (broadcast), multiple access resolution is required.

Taxonomy of Multiple access protocols

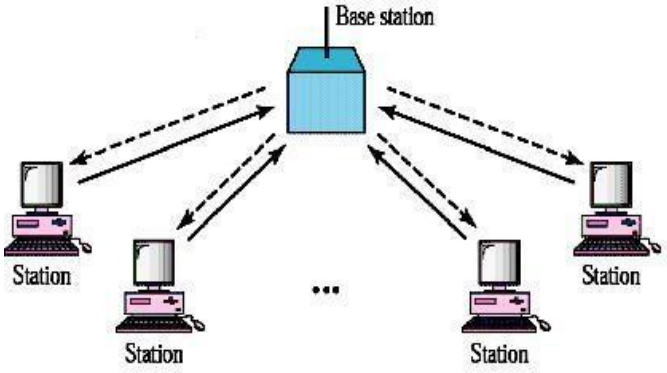


RANDOM ACCESS

- No station is superior to another station and none is assigned 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.
- Transmission is random among the stations.
- Each station has the right to the medium without being controlled by any other station. All stations compete with one another to access the medium. Random access methods are also called as contention methods.
- If more than one station tries to send, there is an access conflict – collision, frames will be either destroyed or modified.



i) ALOHA

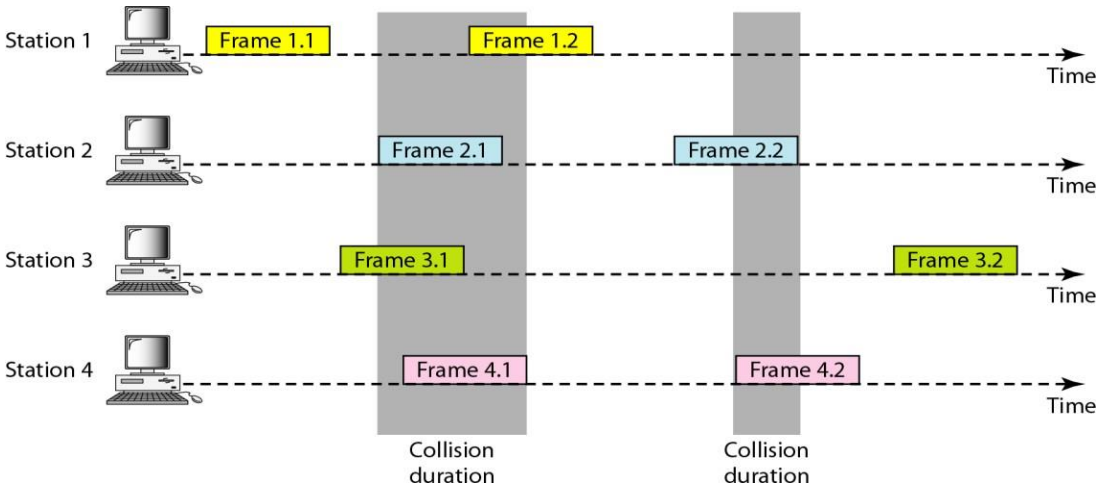


- The earliest random access method, was developed at the university of Hawaii in early 1970.
- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

PURE ALOHA

- The original ALOHA protocol is called pure ALOHA.
- Each station sends a frame whenever it has a frame to send.
- Since there is only one channel to share, there is possibility of collision between frames from different stations.

Frames in a pure ALOHA network



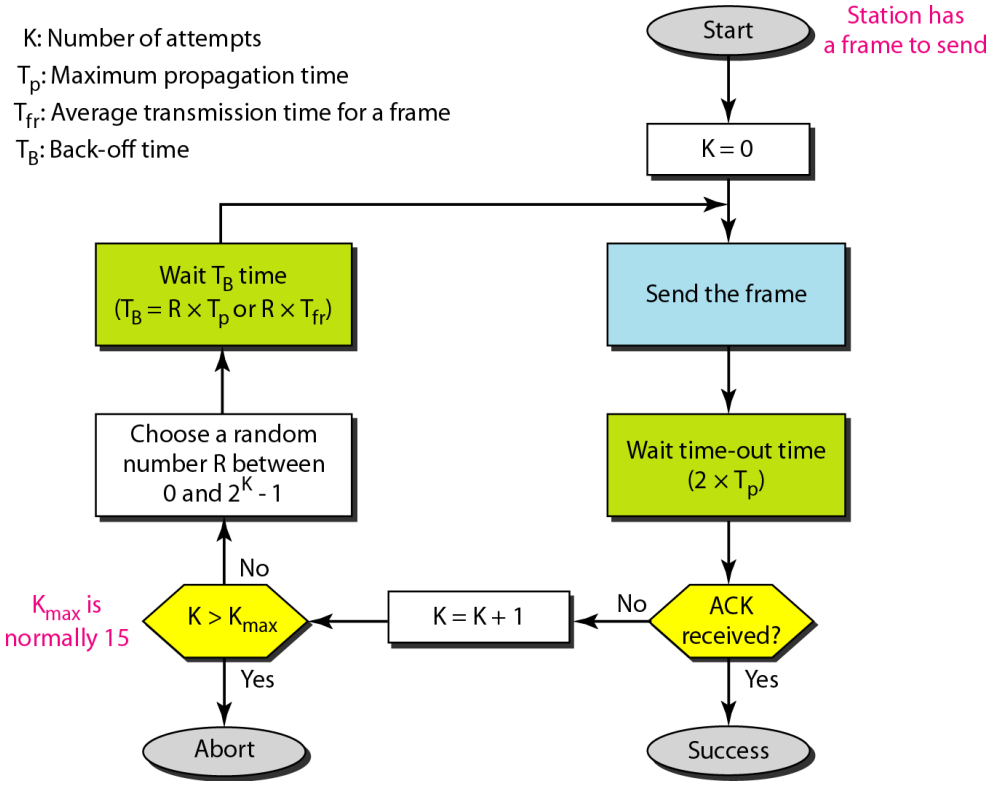
- Even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.

Retransmissions of frames are required for the destroyed frames.

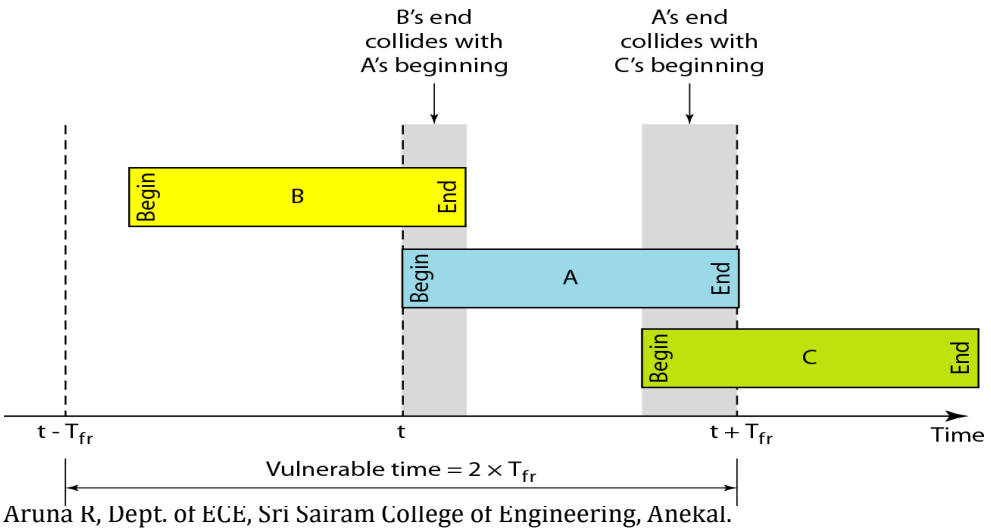
- The pure ALOHA protocol relies on acknowledgements from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgement.
- If the acknowledgement does not arrive after a time-out period, the station assumes that the ACK has been destroyed and resends a frame.

- 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. This time is called back-off time TB. This randomness will help avoid more collisions.
- To prevent congesting the channel with retransmitted frames, pure ALOHA dictates that after a maximum number of retransmission attempts Kmax, a station must give up and try later.

Procedure for pure ALOHA protocol



Vulnerable time for pure ALOHA



Throughput

G = average number of frames generated by the system during one frame transmission time.
Successful transmissions for pure ALOHA is

$$S = G * e^{-2G}$$

The maximum throughput, Smax is for G = ½. i.e., Smax = 0.184 = 18.4%

Problem:

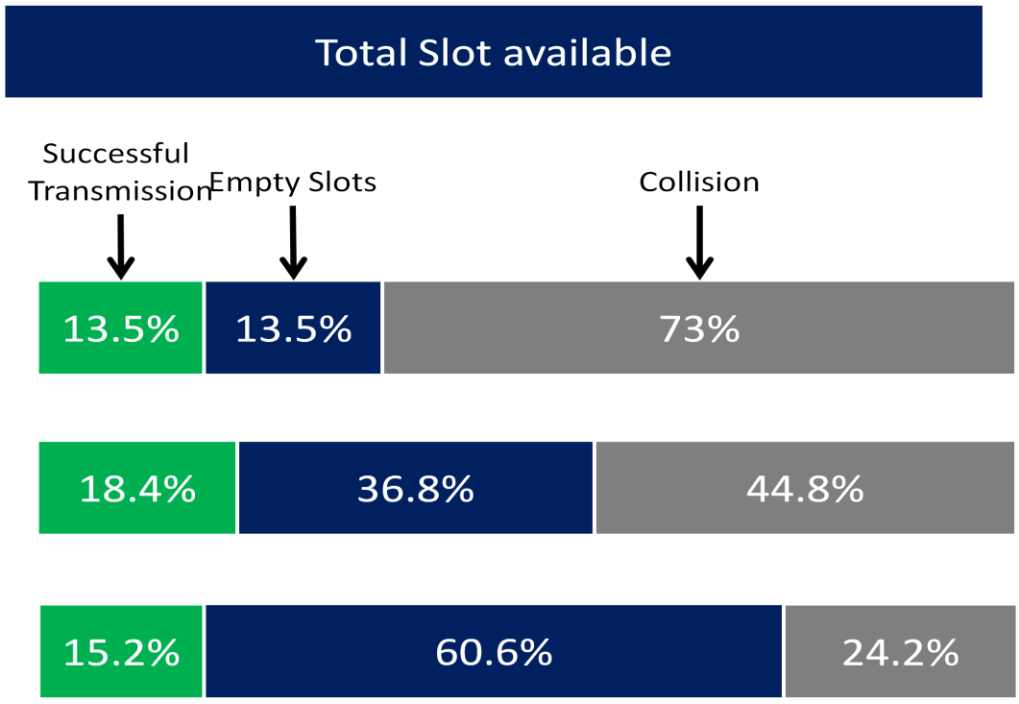
A pure ALOHA network transmits 200-bits frames on a shared channel of 200 kbps. What is the throughput if the system produces?

a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second

Solution:

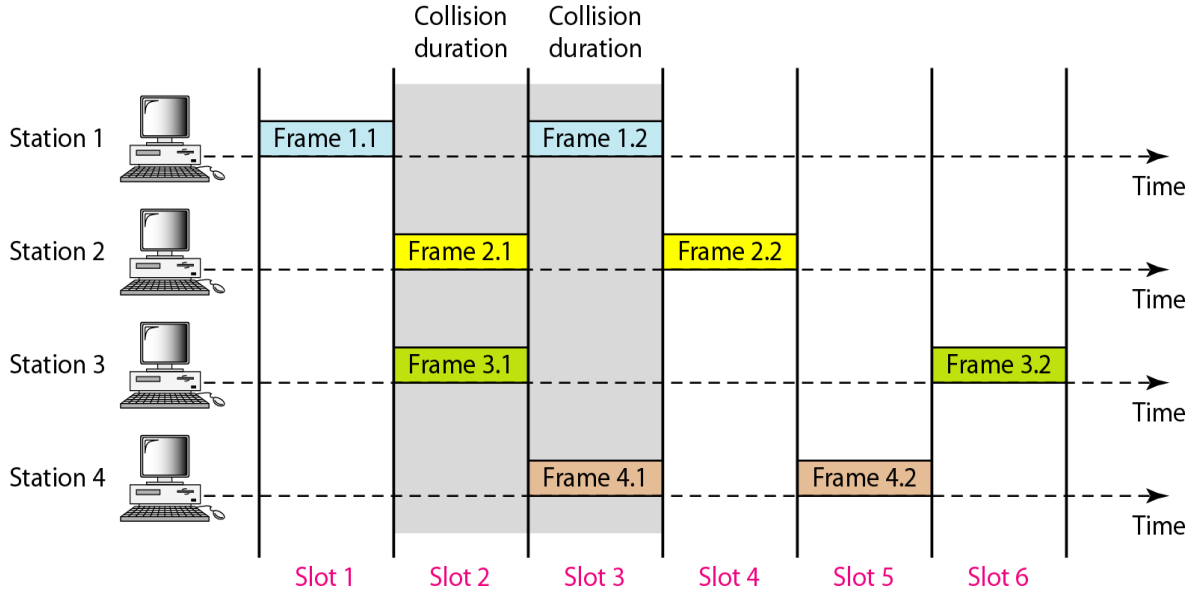
The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or $S = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.
b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or $S = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.
c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.



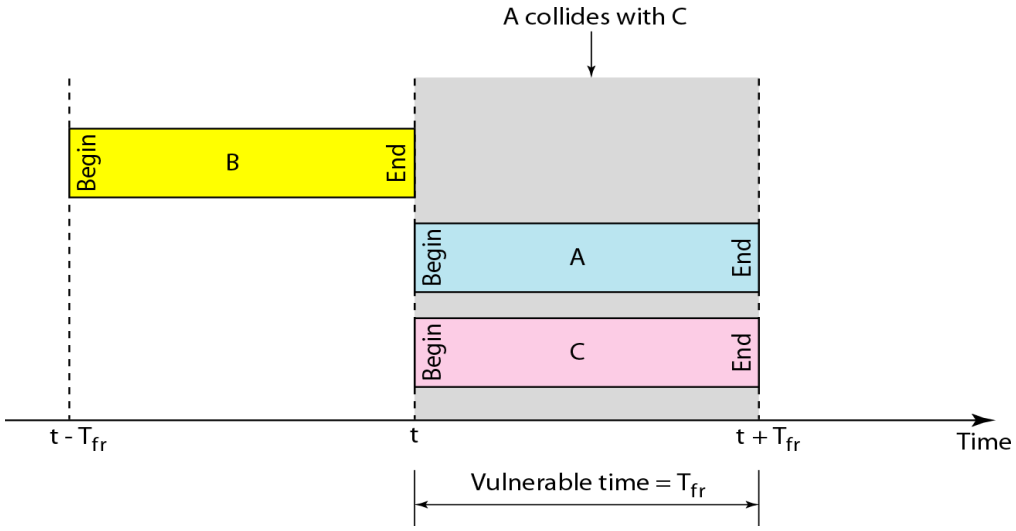
b) SLOTTED ALOHA

Frames in a slotted ALOHA network



Slotted ALOHA Vulnerable time = T_{fr}

Vulnerable time for slotted ALOHA



Throughput

G = average number of frames generated by the system during one frame transmission time.
Successful transmissions for pure ALOHA is
$S = G * e^{-G}$
The maximum throughput, Smax is for G =1 i.e., Smax = 0.368 = 36.8%.

Problem:

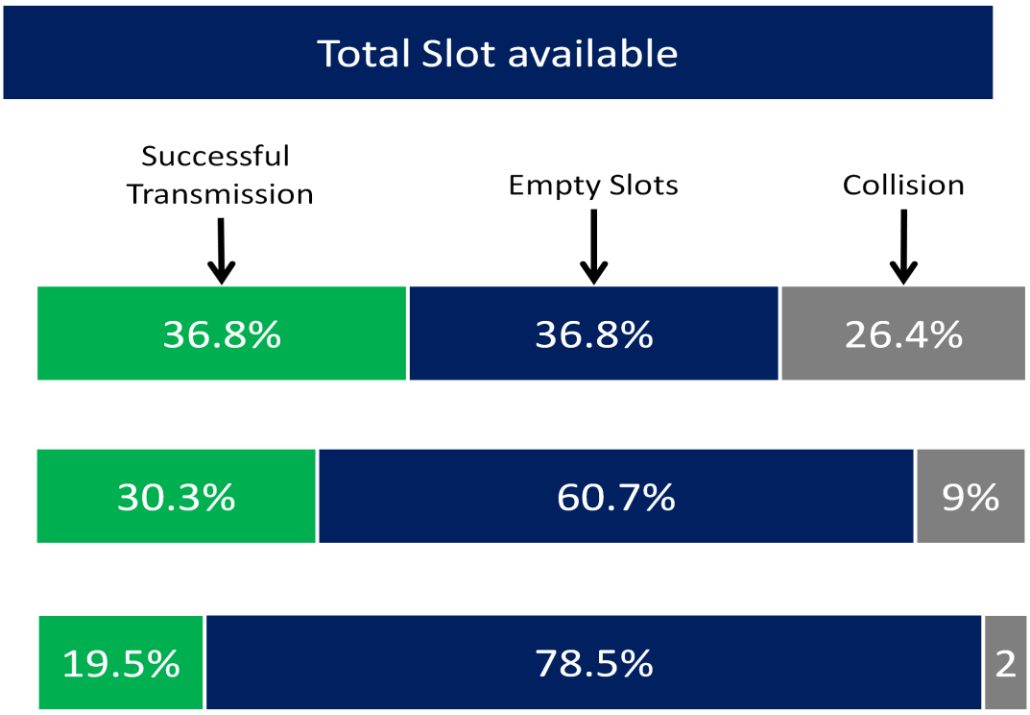
A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces

a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second

Solution

This situation is similar to the previous exercise except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is 200/200 kbps or 1 ms.

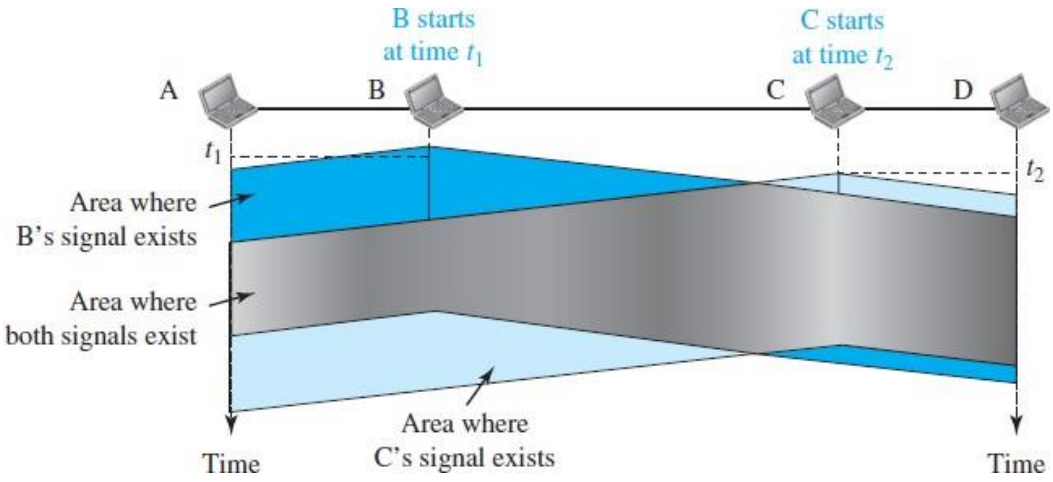
a. In this case G is 1. So $S = G \times e^{-G}$ or $S = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.
b. Here G is $\frac{1}{2}$. In this case $S = G \times e^{-G}$ or $S = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.
c. Now G is $\frac{1}{4}$. In this case $S = G \times e^{-G}$ or $S = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.



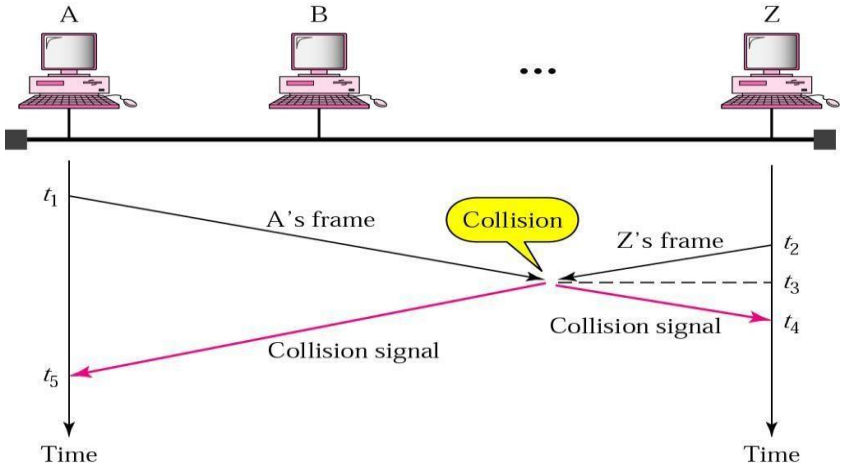
Carrier Sense Multiple Access (CSMA)

The chance of collision can be reduced if a station senses the medium before trying to use it. CSMA requires that each station first listen to the medium before sending. CSMA is based on the principle "sense before transmit" or "listen before talk".

CSMA can reduce the possibility of collision, but it can't eliminate it. The reason for this is shown in the above figure, a space and time model of a CSMA network. Stations are connected to a shared channel. The possibility of collision still exists because of the propagation delay.



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.

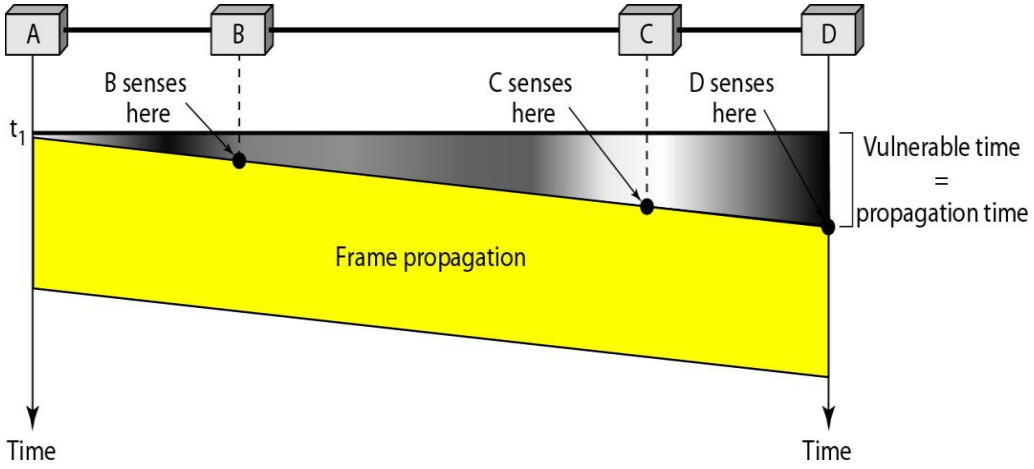


Vulnerable Time

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. But 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.

Figure shows the worst case. The leftmost station, A, sends a frame at time t1, which reaches the rightmost station, D, at time t1 + Tp. The gray area shows the vulnerable area in time and space.



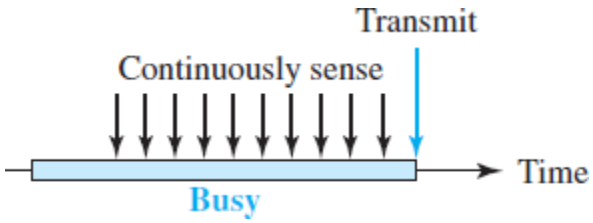
Persistence strategies

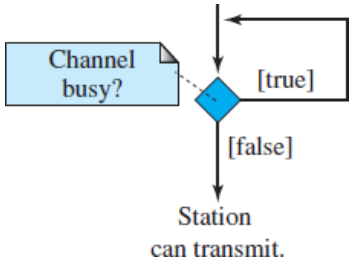
Three persistence methods

1-persistent method, the **non-persistent method,** and the ***p*-persistent method.**

1-Persistent

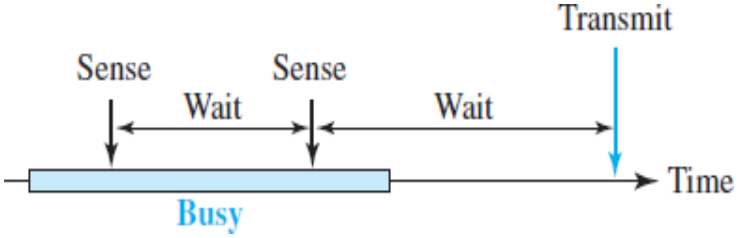
The 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. We will see later that Ethernet uses this method.

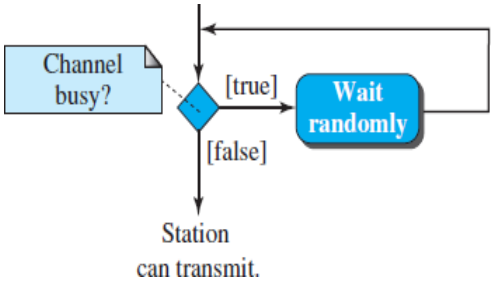




Non-persistent

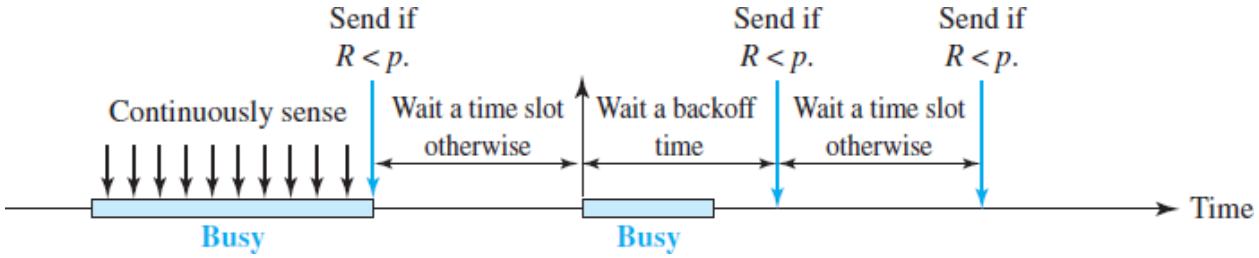
In the non-persistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The non-persistent approach reduces the chance of collision because it is unlikely that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





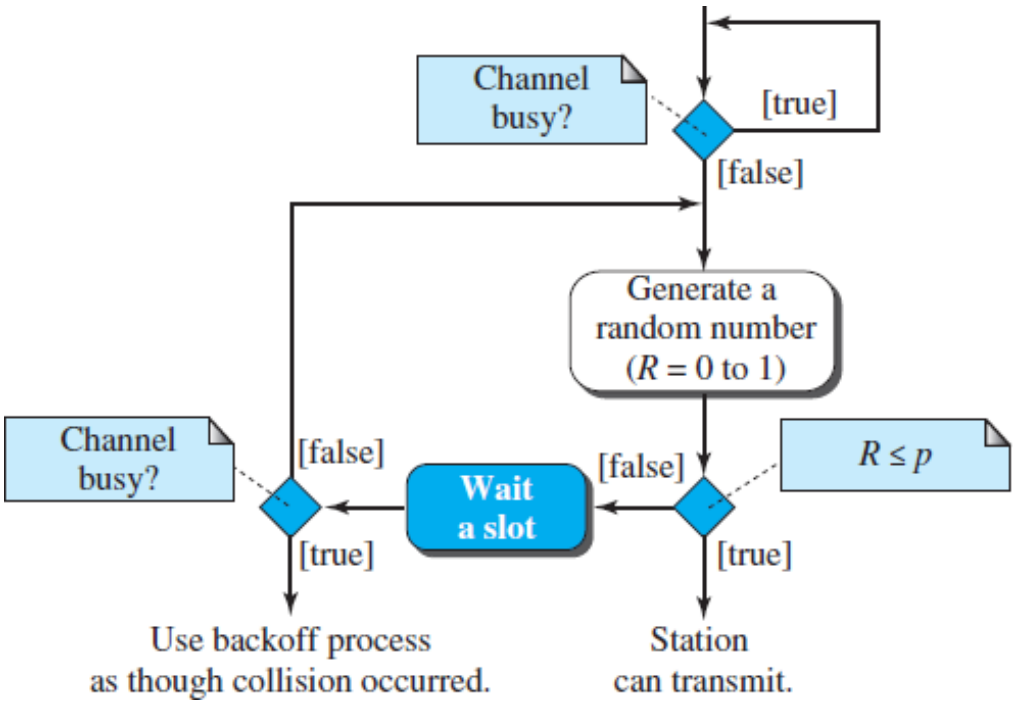
p-P ersistent

The p-persistent method is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time.



The p-persistent approach 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:

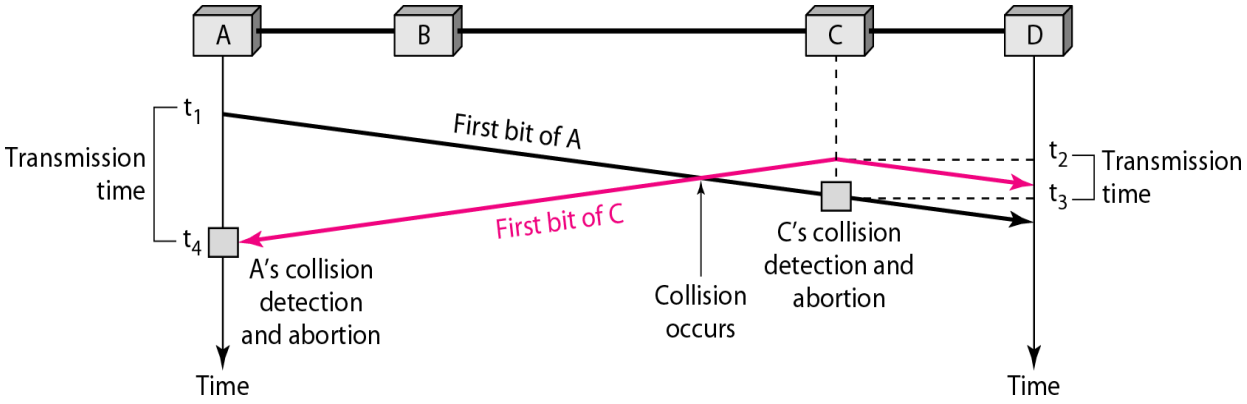
1. With probability p, the station sends its frame.
2. With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.
   - If the line is idle, it goes to step 1.
   - If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.



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

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision. 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. One of the LAN protocols that used CSMA/CD is the traditional Ethernet with the data rate of 10 Mbps.

To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. In Figure, stations A and C are involved in the collision.



- At time *t*1, station A has executed its persistence procedure and starts sending the bits of its frame.
- At time *t*2, 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 *t*2.
- Station C detects a collision at time *t*3 when it receives the first bit of A's frame.
- Station C immediately (or after a short time) aborts transmission.
- Station A detects collision at time *t*4 when it receives the first bit of C's frame; it also immediately aborts transmission.
- Looking at the figure, we see that A transmits for the duration *t*4 − *t*1; C transmits for the duration *t*3 − *t*2.

Minimum Frame Size

If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time T_P to reach the second and the effect of the collision takes another time T_P to reach the first. So the requirement is that the first station must still be transmitting after $2T_p$.

Procedure

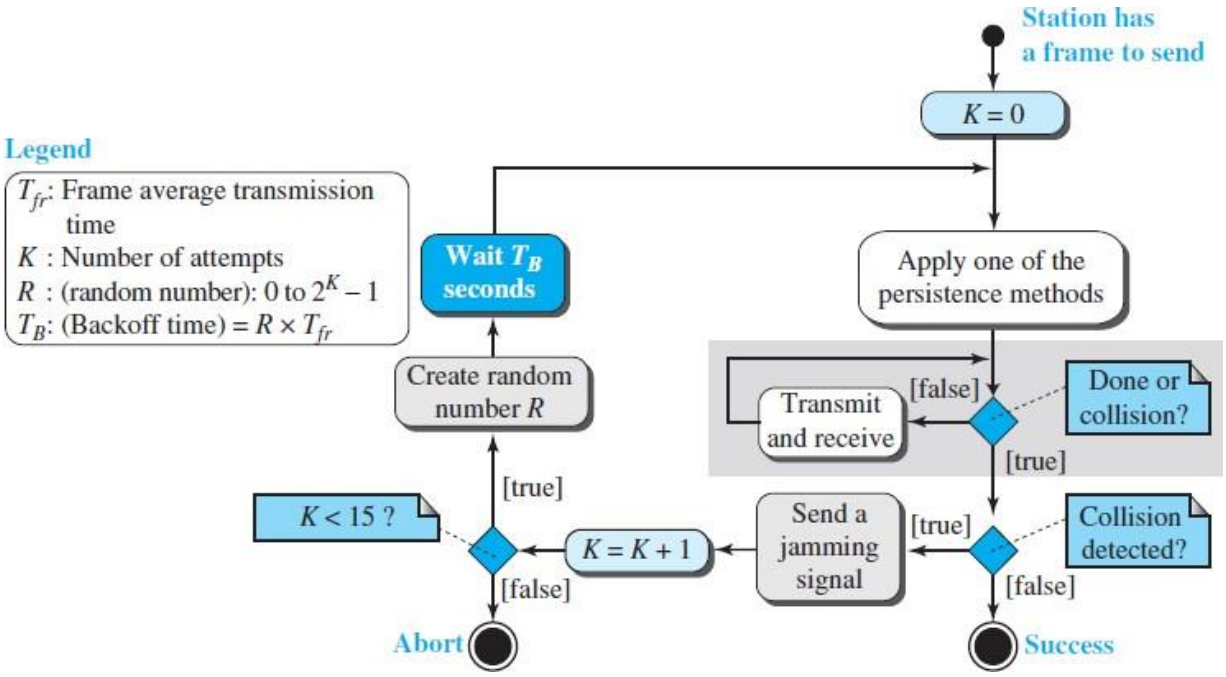
Now let us look at the flow diagram for CSMA/CD in below Figure. It is similar to the one for the ALOHA protocol, but there are differences.

- The first difference is the addition of the persistence process.
- The second difference is the frame transmission. In CSMA/CD, transmission and collision detection are continuous processes. The station transmits and receives

continuously and simultaneously (using two different ports or a bidirectional port),

constantly monitor in order to detect one of two conditions: either transmission is finished or a collision is detected.

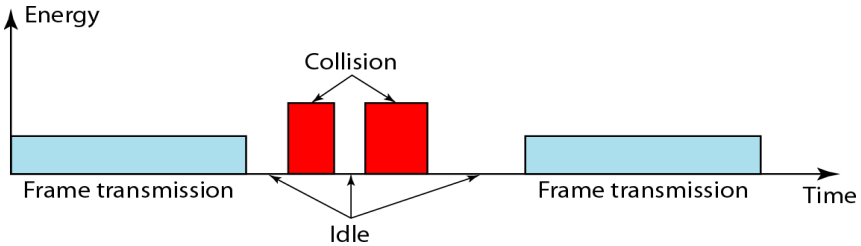
- The third difference is the sending of a short **jamming signal** to make sure that all other stations become aware of the collision.



CSMA/CD: Energy Level & Throughput

Energy Level

A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.
The level of energy in a channel can have three values: zero, normal, and abnormal.
At the zero level, the channel is idle.
At the normal level, a station has successfully captured the channel and is sending its frame.
At the abnormal level, there is a collision and the level of the energy is twice the normal level.
Figure shows the situation.



Throughput

The throughput of CSMA/CD is greater than that of pure or slotted ALOHA. The maximum throughput occurs at a different value of G and is based on the persistence method.

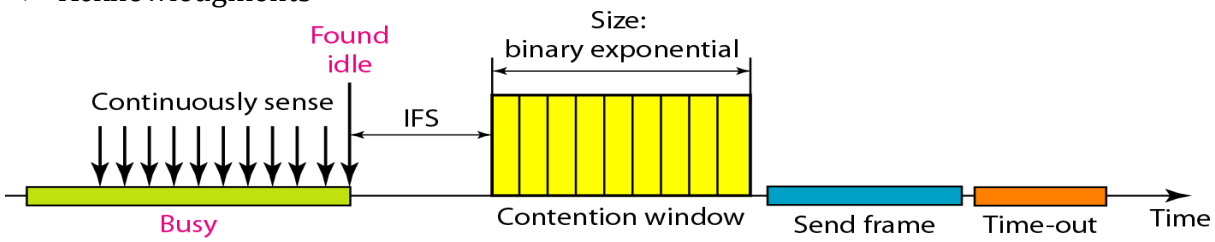
- For the p-persistent method, the maximum throughput is depends on the value of p.
- For the 1-persistent method, the maximum throughput is around 50 percent when G = 1.
- For the non-persistent method, the maximum throughput can go up to 90 percent

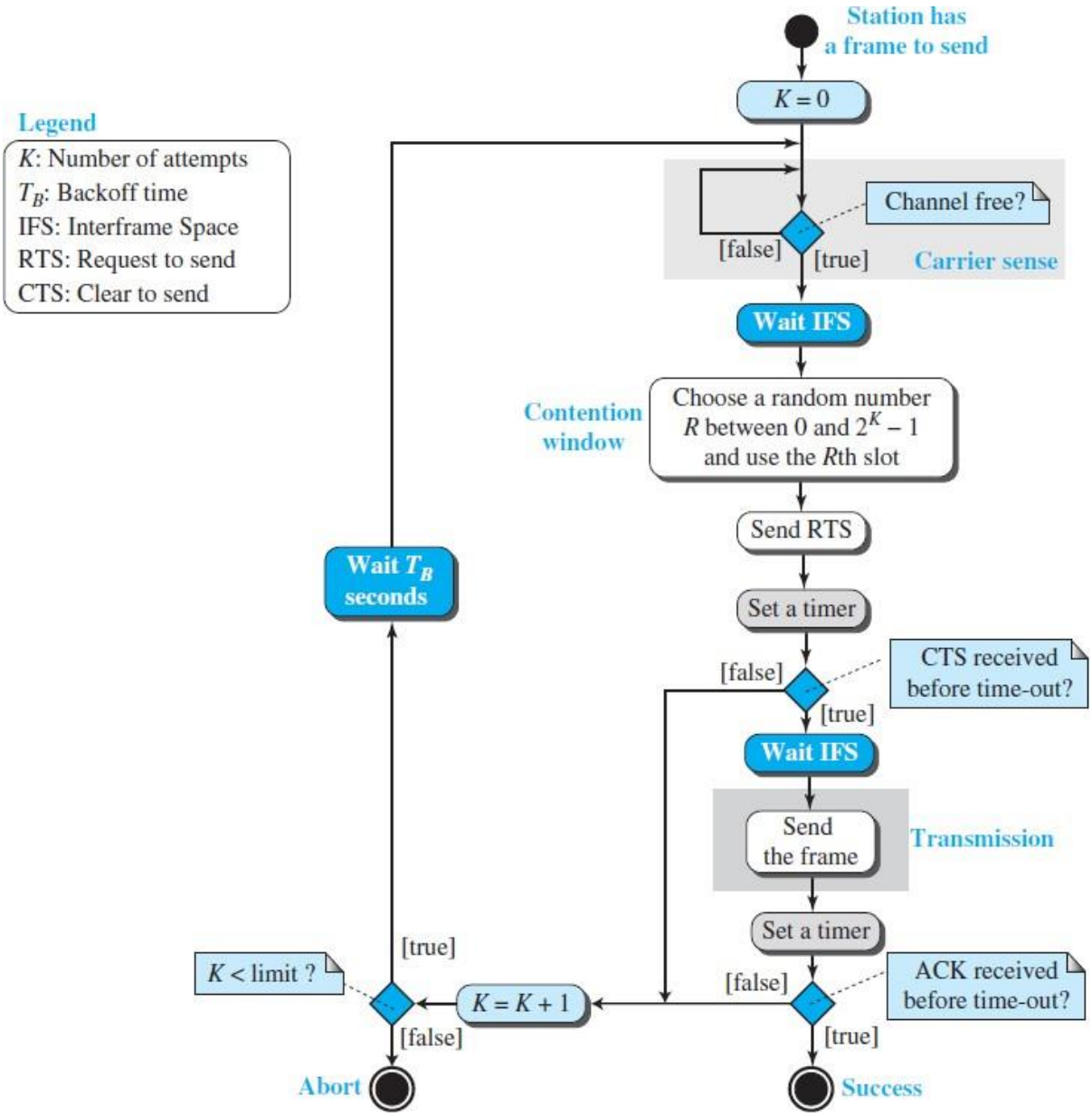
when G is between 3 and 8.

Carrier Sense Multiple Access with collision avoidance (CSMA/CA)

CSMA/CA was invented for wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies:

- The interframe space
- The contention window and
- Acknowledgments





Interframe Space (IFS).

Collisions are avoided by deferring transmissions even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS. Even though the channel may appear idle when it is sensed, a distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station.

After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window. The IFS variable can also be used to prioritize stations or frame types. For example, a station that is assigned 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 backoff strategy. One interesting point about the contention window is it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

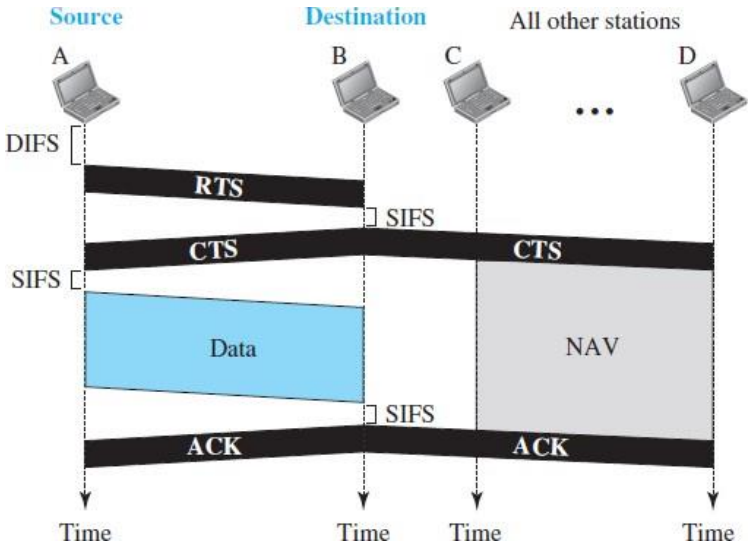
Acknowledgment

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

CSMA/CA and NAV : Frame Exchange Time Line

Figure shows the exchange of data and control frames in time.

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
   - ❖ The channel uses a persistence strategy with backoff until the channel is idle.
   - ❖ After the station is found to be idle, the station waits for a period of time called the DCF 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.



Network Allocation Vector

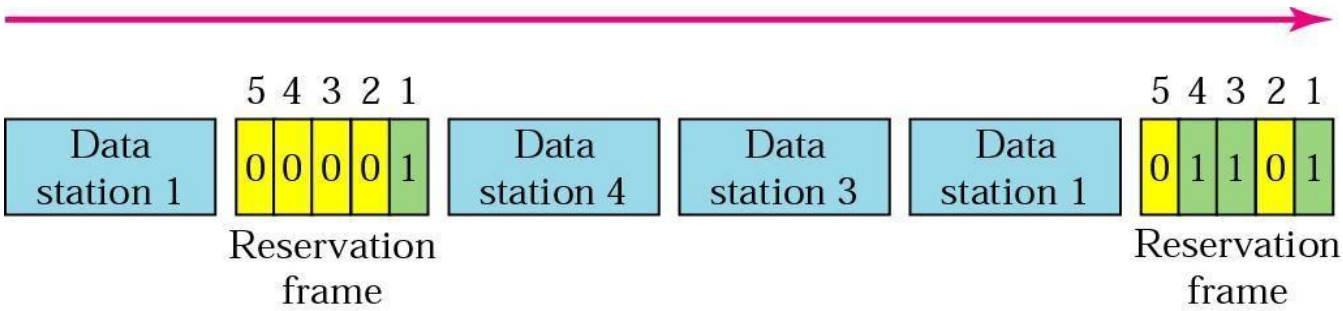
NAV is a key feature for collision avoidance. A stations defer sending their data if one station acquires access with NAV.

When a station sends an RTS (request to send) 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.

CONTROLLED ACCESS

In controlled access, the stations consult one another to find which station has the right to send. A station can't send unless it has been authorized by other stations.

a) Reservation:



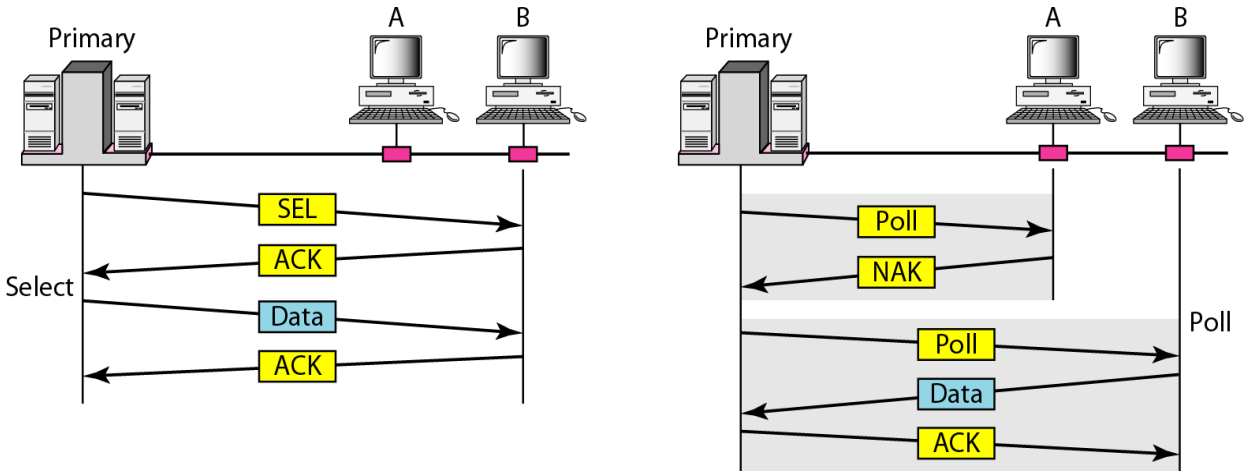
In the reservation method, a station needs to make a reservation before sending the data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in the interval.

b) Polling:

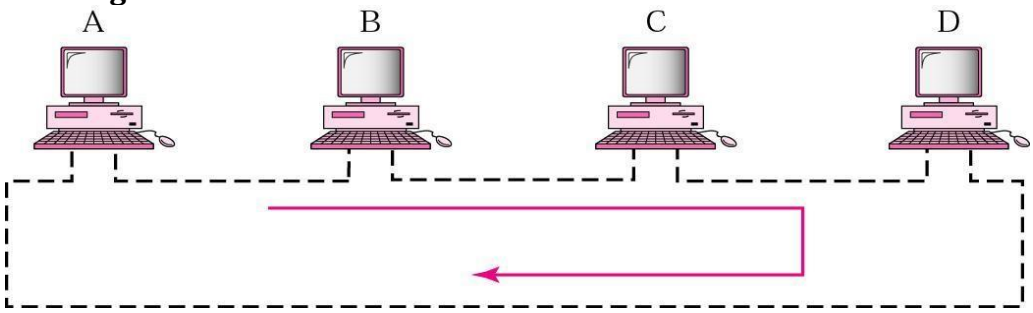
Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary

device even when the ultimate destination is a secondary device.

The select function is used whenever the primary device has something to send. The poll function is used by the primary device to solicit transmissions from the secondary device.

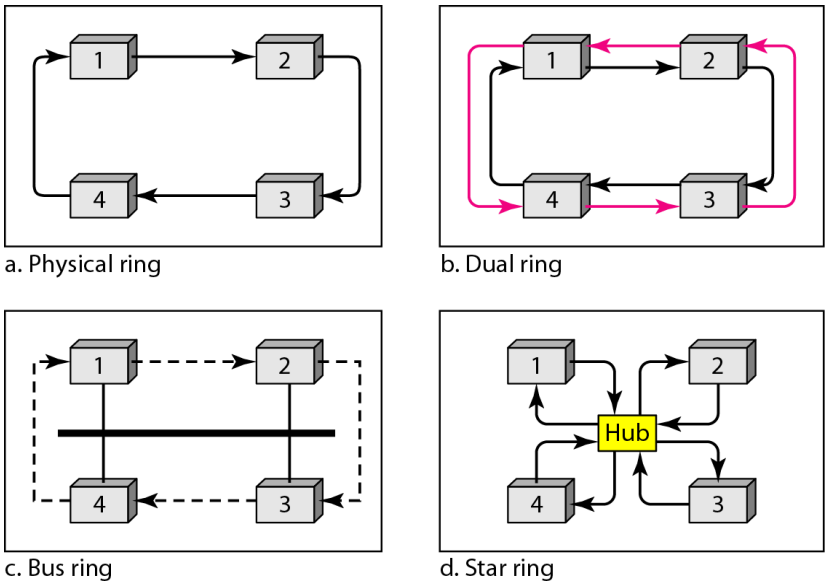


c) Token Passing:



In the token-passing method, the stations in a network are organized in a logical ring. Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed.

Token-passing method:



Wired LANs: Ethernet

IEEE STANDARDS

- In 1985, the Computer Society of the IEEE started a project to set standards to enable intercommunication among equipment from a variety of manufacturers is called **Project 802**.
- It is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.
- The standard was adopted by the American National Standards Institute (ANSI).
- In 1987, the International Organization for Standardization (ISO) also approved under the designation ISO 8802.

Data Link Layer

The data link control handles framing, flow control, and error control.
Framing is handled in both the LLC sublayer and the MAC sublayer.
The IEEE has subdivided the data link layer into two sublayers:

- **Logical link control (LLC)** and
- **Media access control** (**MAC**).

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

Logical Link Control (LLC)

- In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control.
- The LLC provides one single data link control protocol for all IEEE LANs.
- LLC is different from the media access control sublayer, which provides different protocols for different LANs.
- A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

Framing:

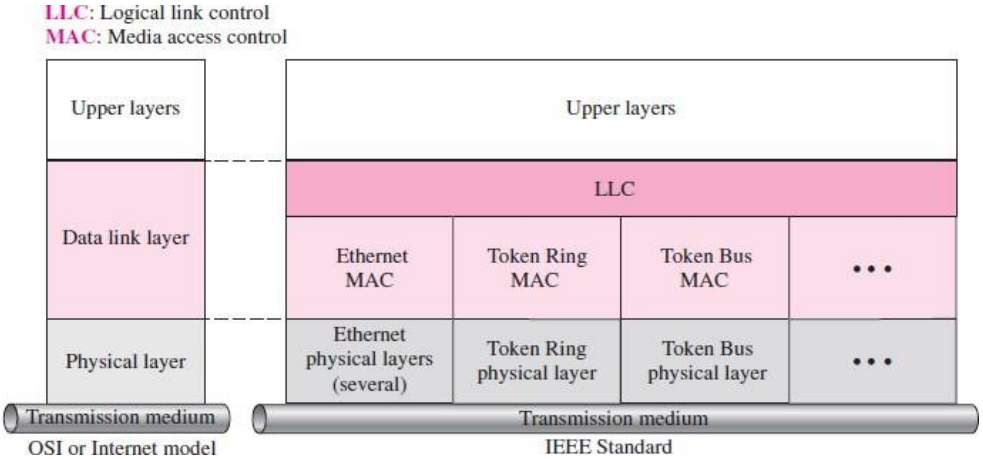
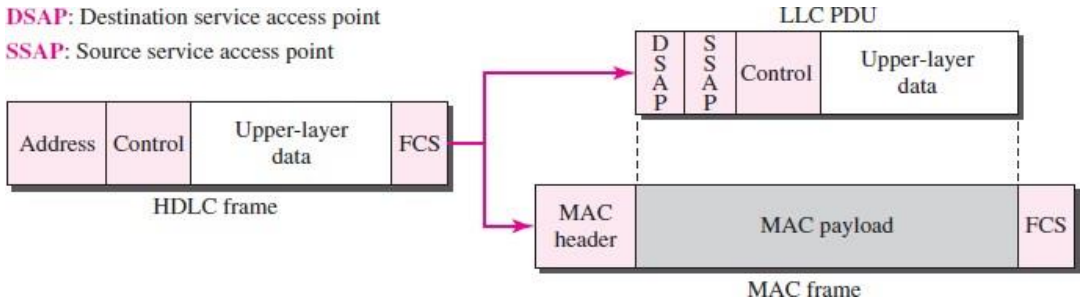


Figure shows one single LLC protocol serving several MAC protocols.

- Framing is handled in both the LLC sublayer and the MAC sublayer.
- LLC defines a protocol data unit (PDU), similar to that of High-level Data Link Control (HDLC). The header contains a control field like the one in HDLC; this field is used for flow and error control.
- The two other header fields define the upper-layer protocol at the source and destination that uses LLC.

- These fields are called the **destination service access point (DSAP)** and the **source service access point (SSAP).** The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer.
- A frame defined in HDLC is divided into a Protocol Data Unit (PDU) at the LLC sublayer and a frame at the MAC sublayer, as shown in Figure.



HDLC frame compared with LLC and MAC frames

Need for LLC:

LLC is needed to provide flow and error control for the upper-layer protocols.

For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols.

Media Access Control (MAC)

- IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.
  - It defines CSMA/CD as the media access method for Ethernet LANs and the token passing method for Token Ring and Token Bus LANs.
- Part of the framing function is also handled by the MAC layer.
- MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

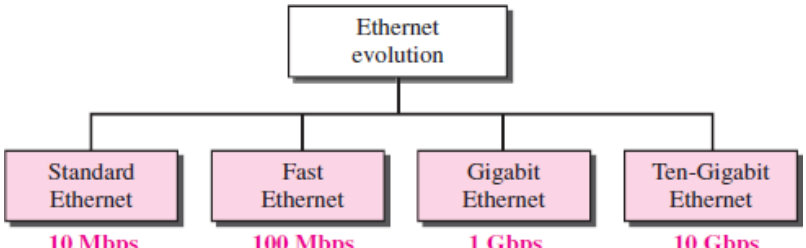
Physical Layer

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

STANDARD ETHERNET

It has gone through four generations:

- Standard Ethernet (10† Mbps),
- Fast Ethernet (100 Mbps),
- Gigabit Ethernet (1 Gbps), and
- Ten-Gigabit Ethernet (10 Gbps).



Ethernet evolution through four generations

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.

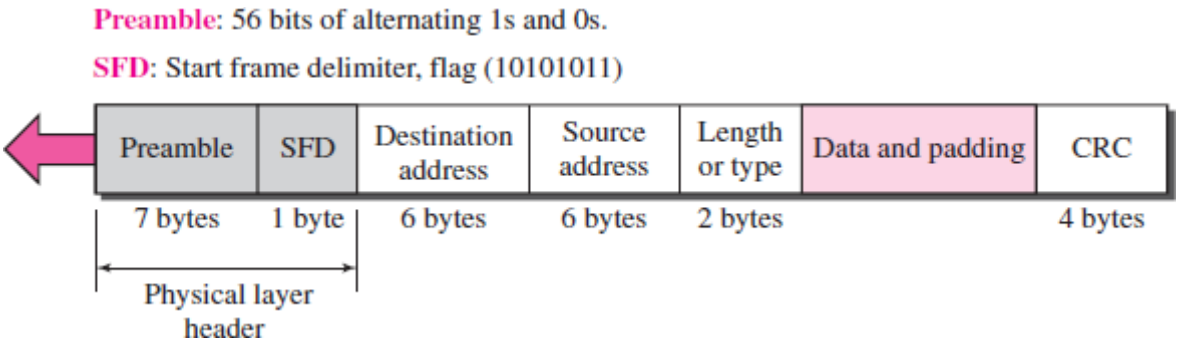
Characteristic: Connectionless and Unreliable Service

- Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame.

- Ethernet is also unreliable like IP and UDP. If a frame is corrupted during transmission and the receiver finds out about the corruption, which has a high level of probability of happening because of the CRC-32, the receiver drops the frame silently. It is the duty of high-level protocols to find out about it.

Frame Format

- The Ethernet frame contains seven fields: Preamble, SFD, DA, SA, length or type of protocol data unit (PDU), Upper-layer data and padding and the CRC.
- Ethernet does not provide any mechanism for acknowledging received frames



Frame of MAC layer

Preamble:

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

Start frame delimiter (SFD):

- The second field (1 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.

CRC: The last field contains error detection information, in this case a CRC-32

Frame Length

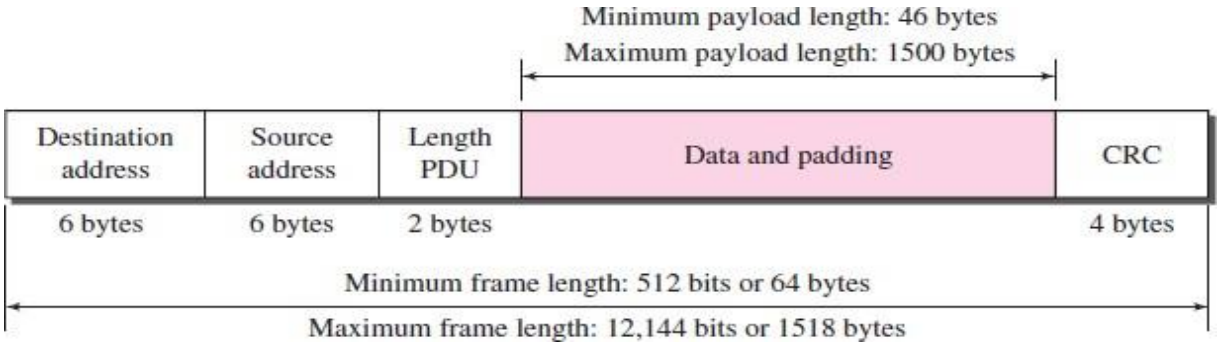
- Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame.
- The minimum length restriction is required for the correct operation of CSMA/CD.
- An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes.
- Part of this length is the header and the trailer.

If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 − 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

The standard defines the maximum length of a frame (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.



Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC).

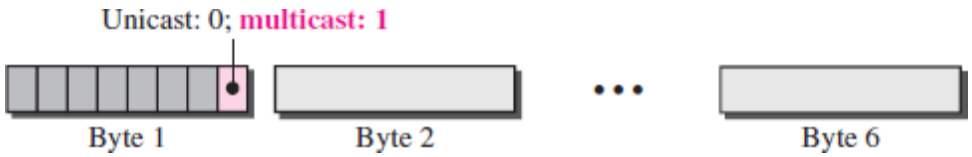
The NIC fits inside the station and provides the station with a 6-byte physical address.

As shown in Figure, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

Example of an Ethernet address in hexadecimal notation

Unicast, Multicast, and Broadcast Addresses

- A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one.
- A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many.
- The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight 1s.



Unicast address from a Multicast address

- A source address is always a unicast address—the frame comes from only one station.
- The destination address, however, can be unicast, multicast, or broadcast.
- If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

Example 1:

Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

Solution:

To find the type of the address, we need to look at the second hexadecimal digit from the left.

- If it is even, the address is unicast.
- If it is odd, the address is multicast.
- If all digits are F's, the address is broadcast.

Therefore, we have the following:

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.

- The way the addresses are sent out on line is different from the way they are written in hexadecimal notation.
- The transmission is left-to-right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last.

- This means that the bit that defines an address as unicast or multicast arrives first at the receiver.

Example 2:
Show how the address 47:20:1B:2E:08:EE is sent out on line.

Solution:
The address is sent left-to-right, byte by byte; for each byte, it is sent right-to-left, bit by bit, as shown below:

11100010 00000100 11011000 01110100 00010000 01110111

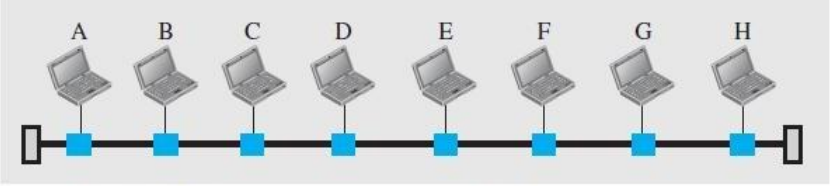
Distinguish Between Unicast, Multicast, and Broadcast Transmission
Standard Ethernet is always broadcast, no matter if the intention is unicast, multicast, or broadcast.
The actual unicast, multicast, and broadcast transmissions are distinguished from each other as,

- In a unicast transmission, all stations will receive the frame, the intended recipient keeps and handles the frame; the rest discard it.
- In a multicast transmission, all stations will receive the frame, the stations that are members of the group keep and handle it; the rest discard it.
- In a broadcast transmission, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

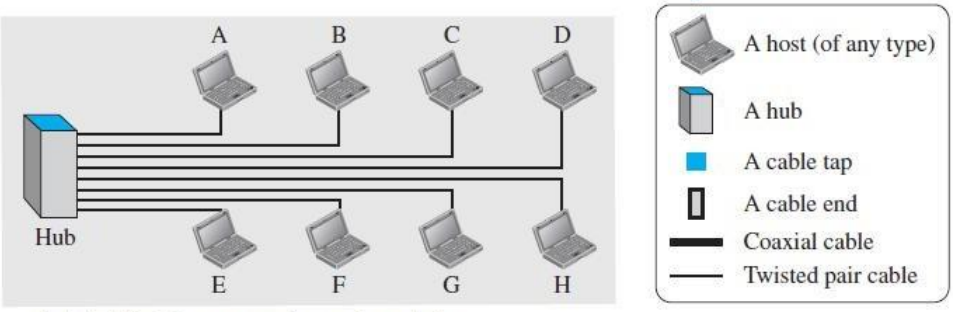
Example:
Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star topology) as shown in Figure.

In the bus topology, when station A sends a frame to station B, all stations will receive it.

In the star topology, when station A sends a frame to station B, the hub will receive it. Since the hub is a passive element, it does not check the destination address of the frame; it regenerates the bits (if they have been weakened) and sends them to all stations except station A. In fact, it floods the network with the frame. The answer is in the way the frames are kept or dropped.



a. A LAN with a bus topology using a coaxial cable



b. A LAN with a star topology using a hub

Access Method

Since the network that uses the standard Ethernet protocol is a broadcast network, we need to use an access method to control access to the sharing medium. The standard Ethernet chose CSMA/CD with 1-persistent method; Let us use a scenario to see how this method works for the Ethernet protocol.

Assume station A has a frame to send to station D.

i. Station A first should check whether any other station is sending (carrier sense).
ii. Station A measures the level of energy on the medium (for a short period of time, normally less than 100 μs).
iii. If there is no signal energy on the medium, it starts sending its frame.
iv. Station A continuously monitors the medium until it becomes idle for 100 μs. It then starts sending the frame.
v. However, station A needs to keep a copy of the frame in its buffer until it is sure that there is no collision.

The medium sensing does not stop after station A has started sending the frame. Station A needs to send and receive continuously.

Two cases may occur:

a. Station A has sent 512 bits and no collision is sensed, the station then is sure that the frame will go through and stops sensing the medium. If we consider the transmission rate of the Ethernet as 10 Mbps, this means that it takes the station 512/(10 Mbps) = 51.2 μs to send out 512 bits. With the speed of propagation in a cable (2×10^8 meters), the first bit could have gone 10,240 meters (one way) or only 5120 meters (round trip), have collided with a bit from the last station on the cable, and have gone back. In other words, if a collision were to occur, it should occur by the time the sender has sent out 512 bits (worst case) and the first bit has made a round trip of 5120 meters. We should know that if the collision happens in the middle of the cable, not at the end, station A hears the collision earlier and aborts the transmission. We also need to mention another issue. The above assumption is that the length of the cable is 5120 meters. The designer of the standard Ethernet actually put a restriction of 2500 meters because we need to consider the delays encountered throughout the journey. It means that they considered the worst case. The whole idea is that if station A does not sense the collision before sending 512 bits, there must have been no collision, because during this time, the first bit has reached the end of the line and all other stations know that a station is sending and refrain from sending. In other words, the problem occurs when another station (for example, the last station) starts sending before the first bit of station A has reached it. The other station mistakenly thinks that the line is free because the first bit has not yet reached it. The reader should notice that the restriction of 512 bits actually helps the sending station: The sending station is certain that no collision will occur if it is not heard during the first 512 bits, so it can discard the copy of the frame in its buffer.

b. Station A has sensed a collision before sending 512 bits. This means that one of the previous bits has collided with a bit sent by another station. In this case both stations should refrain from sending and keep the frame in their buffer for resending when the line becomes available. However, to inform other stations that there is a collision in the network, the station sends a 48-bit jam signal. The jam signal is to create enough signal (even if the collision

happens after a fewbits) to alert other stations about the collision. After sending the jam signal, the stations need to increment the value of *K* (number of attempts). If after increment *K*

= 15, the experience has shown that the network is too busy, the station needs to abort its effort and try again. If $K < 15$, the station can wait a backoff time (TB in Figure 12.13) and restart the process. As Figure 12.13 shows, the station creates a random number between 0 and $2K - 1$, which means each time the collision occurs, the range of the random number increases exponentially. After the first collision ($K = 1$) the random number is in the range (0, 1). After the second collision ($K = 2$) it is in the range (0, 1, 2, 3). After the third collision ($K = 3$) it is in the range (0, 1, 2, 3, 4, 5, 6, 7). So after each collision, the probability increases that the backoff time becomes longer. This is due to the fact that if the collision happens even after the third or fourth attempt, it means that the network is really busy; a longer backoff time is needed.

Efficiency of Standard Ethernet

The efficiency of the Ethernet is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station.

$$\textbf{Efficiency} = 1 / (1 + 6.4 * a)$$

Where "***a" is the number of frames that can fit on the medium.***

It can be calculated as; ***a = (propagation delay)/(transmission delay)***

Example

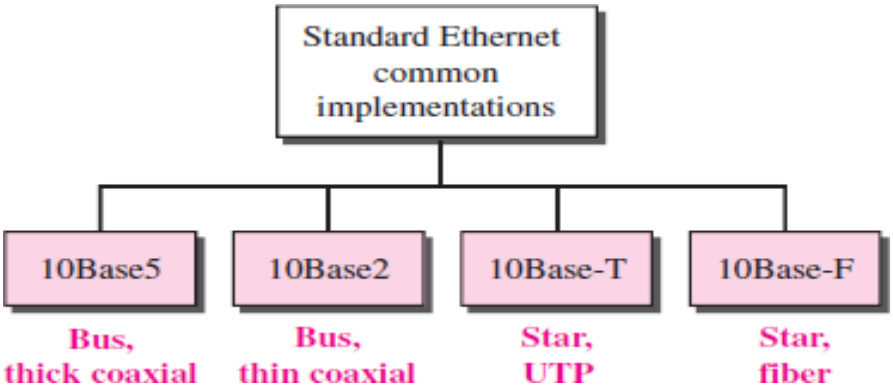
In the Standard Ethernet with the transmission rate of 10 Mbps, we assume that the length of the medium is 2500 m and the size of the frame is 512 bits. The propagation speed of a signal in a cable is normally 2×10^8 m/s.

Propagation delay = $2500/(2 \times 10^8) = 12.5$ µs	Transmission delay = $512/(10^7) = 51.2$ µs
$a = 12.5/51.2 = 0.24$	Efficiency = 39%

The example shows that *a = 0.24, which means only 0.24 of a frame occupies the whole* medium in this case. The efficiency is 39 percent, which is considered moderate; it means that only 61 percent of the time the medium is occupied but not used by a station.

Physical Layer: Implementation

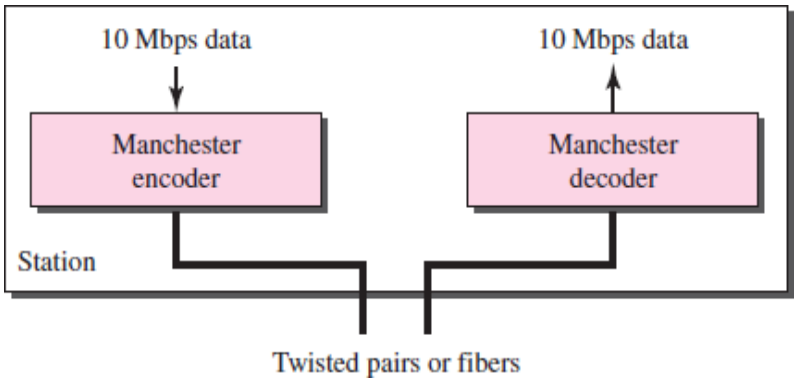
The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in Figure.



Categories of Standard Ethernet

Encoding and Decoding

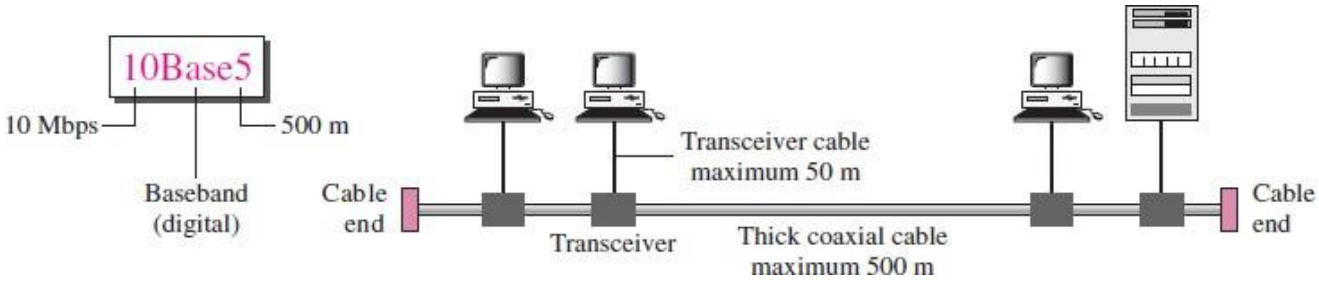
- All standard implementations use digital signaling (baseband) at 10 Mbps.
- At the sender, data are converted to a digital signal using the Manchester scheme.
- At the receiver, the received signal is interpreted as Manchester and decoded into data.
- Manchester encoding is self-synchronous, providing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



Encoding in a Standard Ethernet implementation

10Base5: Thick Ethernet

- The first implementation is called 10Base5, thick Ethernet, or Thicknet.
- 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.



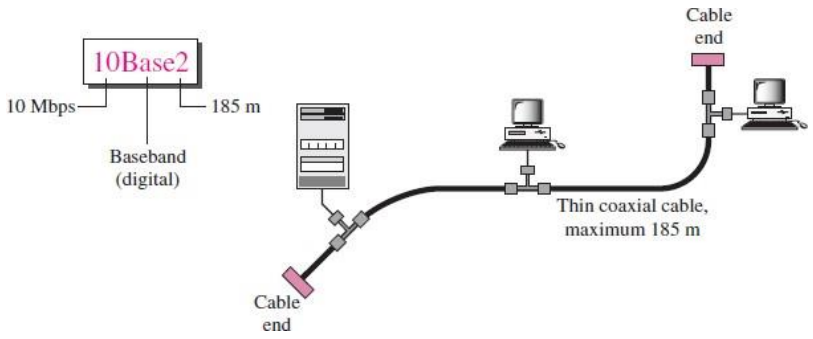
10Base5 implementation

- 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.
- 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.
- 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

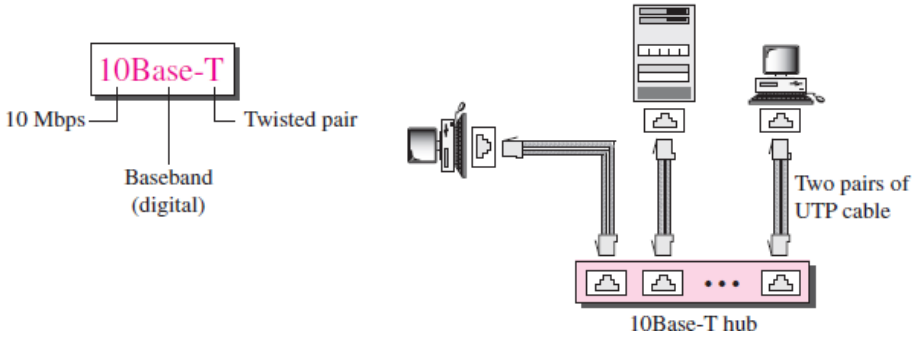
high level of attenuation in thin coaxial cable.



10Base2 implementation

10Base-T: Twisted-Pair Ethernet

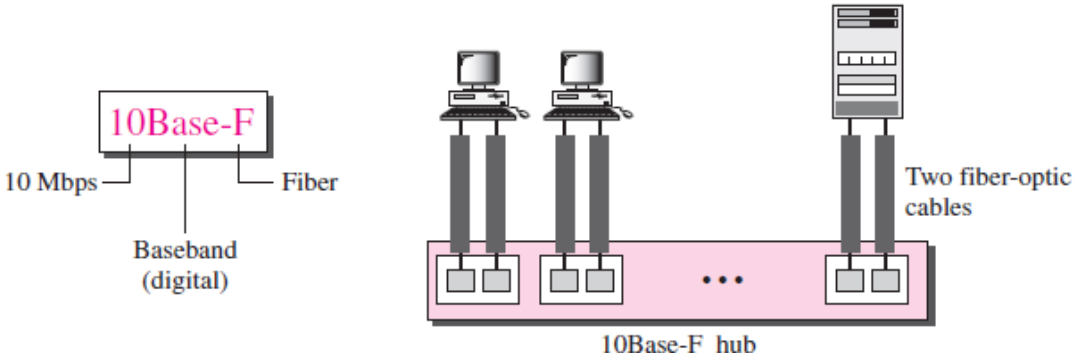
- The third implementation is called **10Base-T** or **twisted-pair Ethernet.**
- 10Base-T uses a physical star topology.
- The stations are connected to a hub via two pairs of twisted cable,
- Two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and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



10Base-T implementation

10Base-F: Fiber Ethernet

- 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.



10Base-F implementation

Summary of Standard Ethernet implementations:

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000 m	Manchester

CHANGES IN THE STANDARD

The 10-Mbps Standard Ethernet has gone through several changes before moving to the higher data rates. These changes actually opened the road to the evolution of the Ethernet to become compatible with other high-data-rate LANs.

BRIDGED ETHERNET

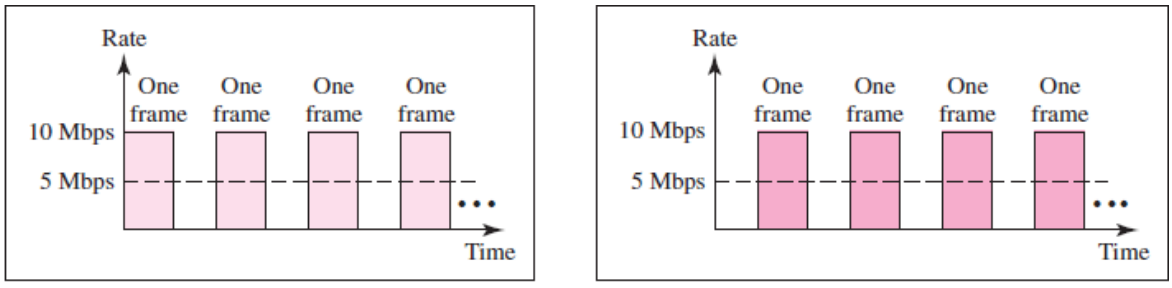
- The first step in the Ethernet evolution was the division of a LAN by **bridges.**
- Bridges have two effects on an Ethernet LAN: They raise the bandwidth and they separate collision domains.

Raising the Bandwidth

- In an unbridged Ethernet network, the total capacity (10 Mbps) is shared among all stations with a frame to send; the stations share the bandwidth of the network.
- If only one station has frames to send, it benefits from the total capacity (10 Mbps).
- But if more than one station needs to use the network, the capacity is shared.

Example:

If two stations have a lot of frames to send, they probably alternate in usage. When one station is sending, the other one refrains from sending. In this case, each station on average sends at a rate of 5 Mbps.



a. First station b. Second station

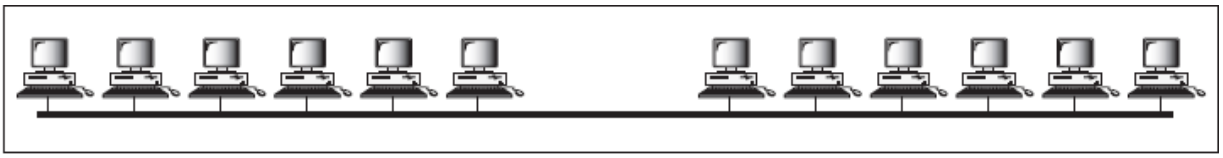
Sharing bandwidth

A bridge divides the network into two or more networks. Bandwidth-wise, each network is independent.

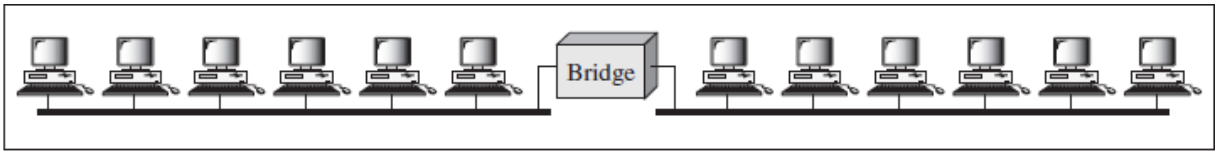
Example:

- A network with 12 stations is divided into two networks, each with 6 stations.
- Now each network has a capacity of 10 Mbps.
- The 10-Mbps capacity in each segment is now shared between 6 stations not 12 stations.
- In a network with a heavy load, each station theoretically is offered 10/6 Mbps instead of 10/12 Mbps, assuming that the traffic is not going through the bridge.

- Further divide the network, can gain more bandwidth for each segment.



a. Without bridging

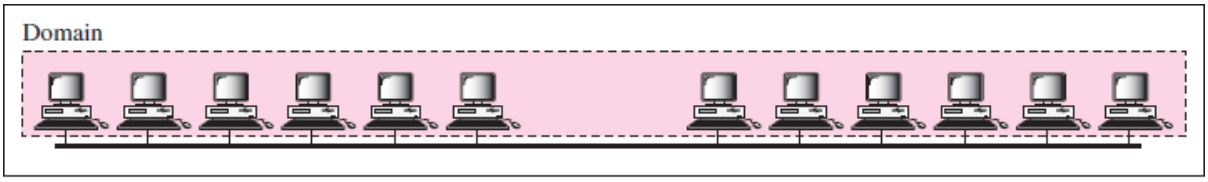


b. With bridging

Separating Collision Domains

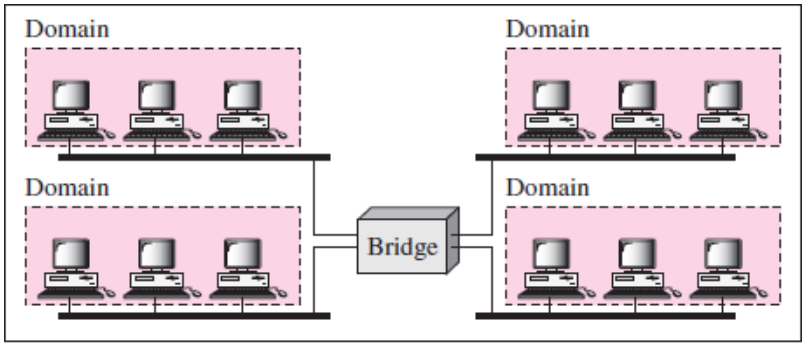
- Another advantage of a bridge is the separation of the **collision domain.**
- Below figure shows the collision domains for an unbridged and a bridged network.
- The collision domain becomes much smaller and the probability of collision is reduced tremendously.

Without bridging, 12 stations contend for access to the medium;



a. Without bridging

With bridging only 3 stations contend for access to the medium.

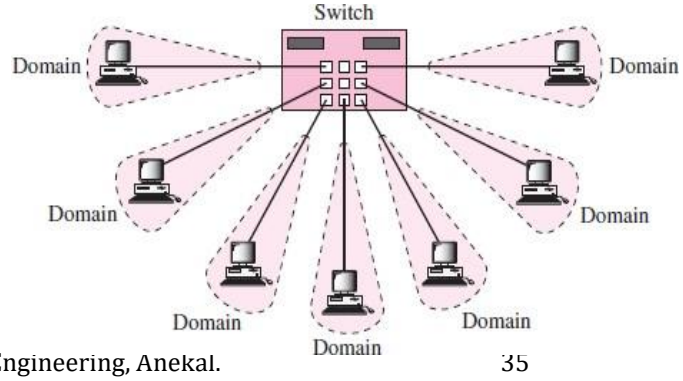


b. With bridging

Collision domains in an unbridged network and a bridged network

SWITCHED ETHERNET

- The idea of a bridged LAN can be extended to a switched LAN. For multiple-port bridge, have an *N*-port switch.
- The bandwidth is shared only between the station and the switch (5 Mbps each), the collision domain is divided into *N* domains.
- A layer 2 **switch** is an *N*-port bridge with additional sophistication that allows faster handling of the packets.



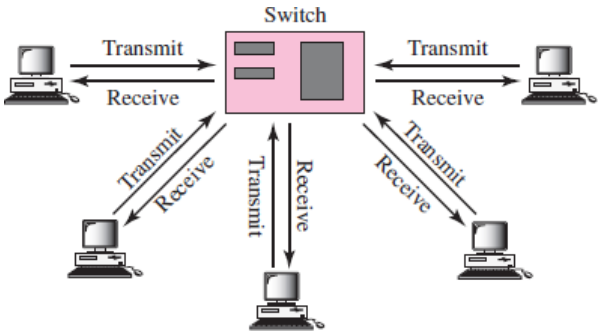
Evolution from a bridged Ethernet to a

switched Ethernet was a big step that opened the way to an even faster Ethernet.

Switched Ethernet

Full-Duplex Ethernet: (10Base-T is always full-duplex)

- The evolution was to move from switched Ethernet to full-duplex switched Ethernet mode is to increases the capacity of each domain from 10 to 20 Mbps as well dual communication.



Full-duplex switched Ethernet

Figure shows a switched Ethernet in full-duplex mode, the configuration uses two links: one to transmit and one to receive.

No Need for CSMA/CD

- In full-duplex switched Ethernet, there is no need for the CSMA/CD method.
- In a full-duplex switched Ethernet, each station is connected to the switch via two separate links. Each station or switch can send and receive independently without worrying about collision.
- Each link is a point-to-point dedicated path between the station and the switch.
- There is no longer a need for carrier sensing; there is no longer a need for collision detection.
- The job of the MAC layer becomes much easier.
- The carrier sensing and collision detection functionalities of the MAC sublayer can be turned off.

MAC Control Layer

- Standard Ethernet was designed as a connectionless protocol at the MAC sublayer.
- There is no explicit flow control or error control to inform the sender that the frame has arrived at the destination without error.
- When the receiver receives the frame, it does not send any positive or negative acknowledgment.
- To provide for flow and error control in full-duplex switched Ethernet, a new sublayer, called the MAC control, is added between the LLC sublayer and the MAC sublayer.

FAST ETHERNET

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

The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.

4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

MAC Sublayer

The evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched.
For the star topology, there are two choices, as half duplex and full duplex.

- In the half-duplex approach, the stations are connected via a hub.
- In the full-duplex approach, the connection is made via a switch with buffers at each port.
- The access method is the same (CSMA/CD) for the half-duplex approach; for fullduplex Fast Ethernet, there is no need for CSMA/CD.
- Implementations keep CSMA/CD for backward compatibility with Standard Ethernet.

AUTONEGOTIATION: A new feature added to Fast Ethernet is called auto negotiation.
It allows a station or a hub a range of capabilities.
Auto negotiation allows two devices to negotiate the mode or data rate of operation.
It was designed particularly for the following purposes:

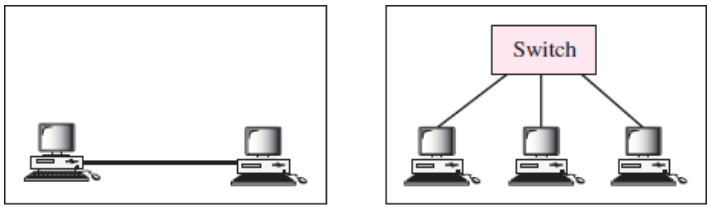
- To allow incompatible devices to connect to one another.
- To allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.

Physical Layer

The physical layer in Fast Ethernet is more complicated than the one in Standard Ethernet.
Some features of this layer are:

Topology

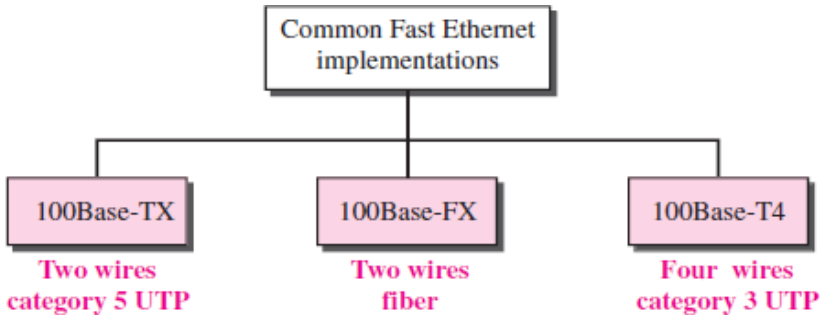
Fast Ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center, as shown in Figure.



Fast Ethernet topology

Implementation

Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire. The two-wire implementation can be either category 5 UTP (100Base-TX) or fiber-optic cable (100Base-FX). The four-wire implementation is designed only for category 3 UTP (100Base-T4) as shown in Figure.



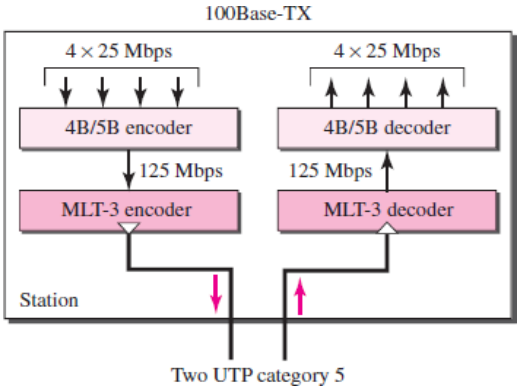
Fast Ethernet implementations

Encoding

Manchester encoding needs a 200-Mbaud bandwidth for a data rate of 100 Mbps, which makes it unsuitable for a medium such as twisted-pair cable. Therefore, three different encoding schemes were chosen as shown in Figure.

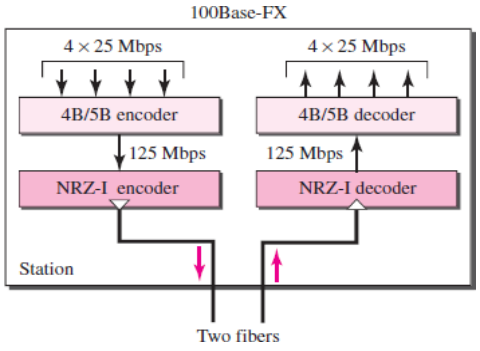
100Base-TX:

- 100Base-TX uses two pairs of twisted-pair cable (either category 5 UTP or STP).
- MLT-3 scheme was selected for its good bandwidth performance.
- MLT-3 is not a self-synchronous line coding scheme, 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.



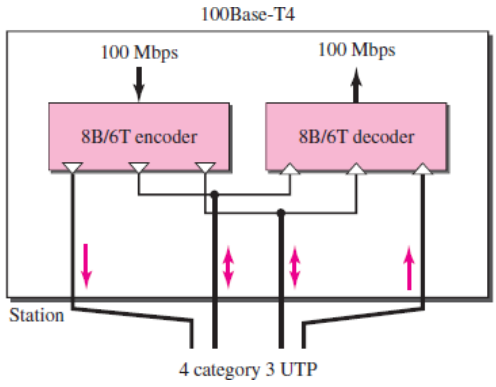
100Base-FX:

- 100Base-FX uses two pairs of fiber-optic cables.
- Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes. The designers of 100Base-FX selected the NRZ-I encoding scheme for this implementation.
- The block encoding increases the bit rate from 100 to 125 Mbps, which can easily be handled by fiber-optic cable.



100Base-T4:

- A new standard, called 100Base-T4, was designed to use category 3 or higher UTP.
- The implementation uses four pairs of UTP for transmitting 100 Mbps.
- Encoding/decoding in 100Base-T4 is more complicated.
- As this implementation uses category 3 UTP, each twisted-pair cannot easily handle more than 25 Mbaud.
- In this design, one pair switches between sending and receiving.
- Three pairs of UTP category 3, however, can handle only 75 Mbaud (25 Mbaud) each.
- An encoding scheme that converts 100 Mbps to a 75 Mbaud signal.
- In 8B/6T, eight data elements are encoded as six signal elements.
- This means that 100 Mbps uses only (6/8) × 100 Mbps, or 75 Mbaud.



Summary of Fast Ethernet implementations

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.

The goals of the Gigabit Ethernet design can be summarized as follows:

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

MAC Sublayer

A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. To achieve a data rate 1 Gbps, Gigabit Ethernet has two distinctive approaches for medium access:

- Half-duplex and
- Full-duplex.

All implementations of Gigabit Ethernet follow the full-duplex approach.

Full-Duplex Mode

- In full-duplex mode, there is a central switch connected to all computers or other switches.
- In this mode, each switch has buffers for each input port in which data are stored until they are transmitted.
- There is no collision.
- The maximum length of the cable is determined by the signal attenuation in the cable, not by the collision detection process.

Half-Duplex Mode

- Gigabit Ethernet can also be used in half-duplex mode, but it is rare.
- In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur.
- The half-duplex approach uses CSMA/CD.
- The maximum length of the network is totally dependent on the minimum frame size.
- Three methods have been defined:
  - Traditional
  - Carrier extension and
  - Frame bursting

Traditional:

- The minimum length of the frame as in traditional Ethernet is 512 bits.
- 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.
- 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, it increases 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.
- Carrier extension is very inefficient if we have a series of short frames to send; each frame carries redundant data.

Frame Bursting:

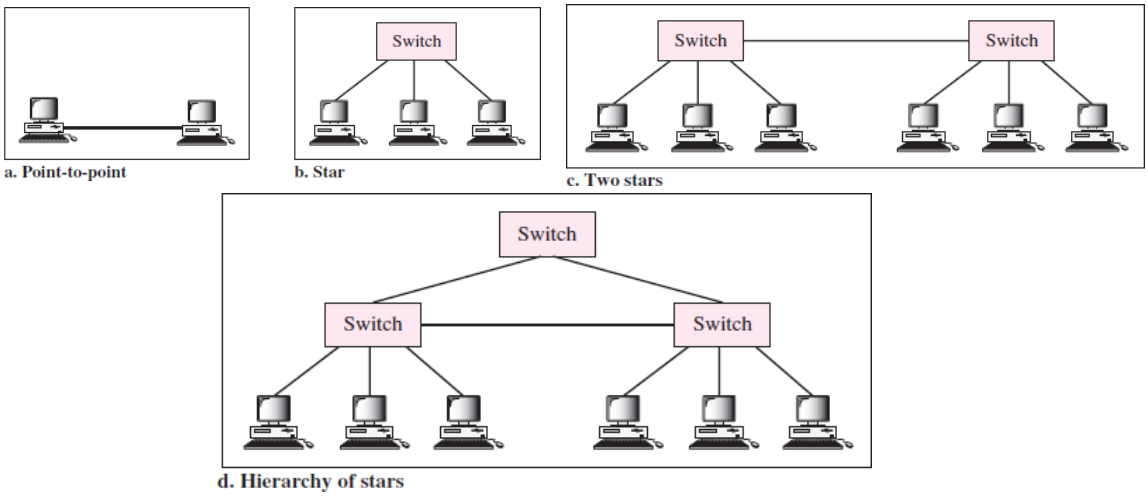
- To improve efficiency, frame bursting was proposed.
- Instead of adding an extension to each frame, multiple frames are sent.
- Padding is added between the frames to make these multiple frames look like one frame.

Physical Layer

The physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet. Some features of this layer are:

Topology

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



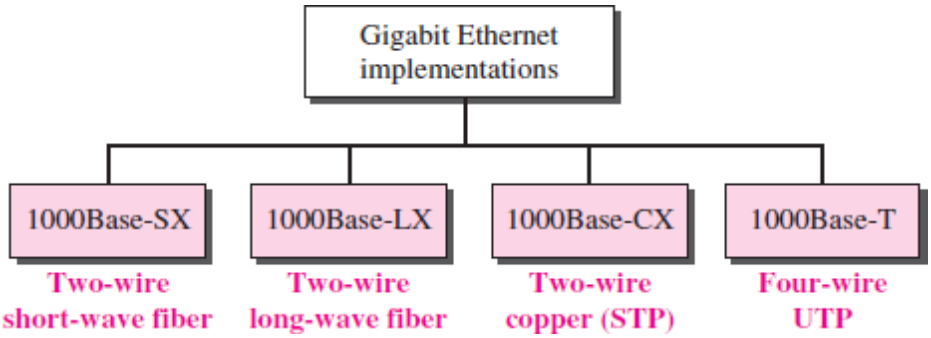
Topologies of Gigabit Ethernet

Implementation

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

It has four implementations, as shown in Figure.

1000Base-T was designed in response to those users, installed this wiring for other purposes such as Fast Ethernet or telephone services.

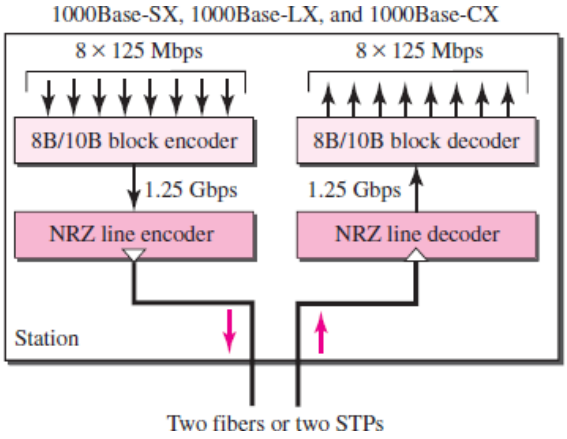


Encoding

Gigabit Ethernet cannot use the Manchester encoding scheme because it involves a very high bandwidth (2 GBaud). Figure shows the encoding/decoding schemes for the four implementations.

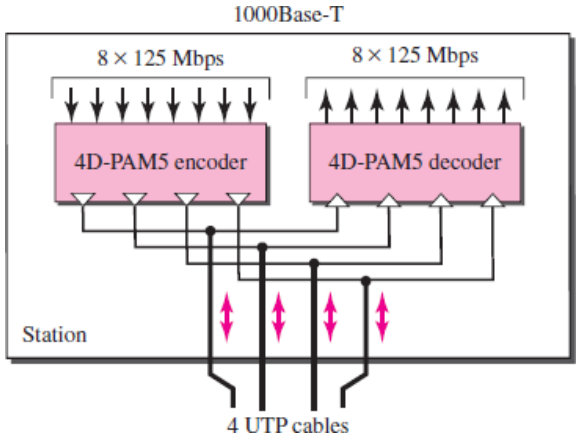
Two-wire implementation:

- The two-wire implementations use an NRZ scheme, but NRZ does not self-synchronize properly. To synchronize bits, particularly at this high data rate, 8B/10B block encoding is used.
- This block encoding prevents long sequences of 0s or 1s in the stream, but the resulting stream is 1.25 Gbps.
- In this implementation, one wire (fiber or STP) is used for sending and one for receiving.



Four-wire implementation:

- In the four-wire implementation it is not possible to have 2 wires for input and 2 for output, because each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP.
- 4D-PAM5 encoding is used to reduce the bandwidth.
- All four wires are involved in both input and output; each wire carries 250 Mbps, which is in the range for category 5 UTP cable.



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

Ten-Gigabit Ethernet

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae.
The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

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.

MAC Sublayer

Ten-Gigabit Ethernet operates only in full duplex mode.

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 10GBase-E.

Summary of Ten-Gigabit Ethernet implementations

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

Questions and Answers

1. **How is the preamble field different from the SFD field?**
   Preamble: The pattern of alternating 0s and 1s provides only an alert and a timing pulse for synchronize
   Start frame delimiter (SFD): The pattern of 6 bits alternating 0s and 1s and last 2 bits is 11 alerts the receiver about destination address and warns the station for synchronize

2. **What is the purpose of an NIC?**
   The Network Interface Card (NIC) fits inside the station and provides the station with a 6-byte physical address.

3. **What is the difference between a unicast, multicast, and broadcast address?**

Type of Address	Destination Address	Recipients Relationship
Unicast	Only one recipient	One-to-one
Multicast	Group of addresses	One-to-many
Broadcast	Special case of the multicast address	Recipients are all the stations on the LAN

4. **What are the advantages of dividing an Ethernet LAN with a bridge?**
   - Gains more bandwidth
   - Collision domain becomes much smaller.
   - Probability of collision is reduced.

5. **What is the relationship between a switch and a bridge?**
   - For multiple-port Bridge, have an *N*-port switch.
   - Bridged Ethernet to a Switched Ethernet was a big step that opened the way to an even faster Ethernet.
   - Also allows faster handling of the packets.

6. **Why is there no need for CSMA/CD on a full-duplex Ethernet LAN?**
   - In full-duplex switched Ethernet, there is no need for the CSMA/CD method.
   - In a full-duplex switched Ethernet, each station is connected to the switch via two separate links. Each station or switch can send and receive independently without worrying about collision.
   - Each link is a point-to-point dedicated path between the station and the switch.
   - There is no longer a need for carrier sensing; there is no longer a need for collision detection.
   - The job of the MAC layer becomes much easier.
   - The carrier sensing and collision detection functionalities of the MAC sublayer can be turned off.

7. **Compare the data rates for Standard Ethernet, Fast Ethernet, Gigabit Ethernet, and Ten-Gigabit Ethernet.**

   Standard Ethernet:

Specification	10BASE5	10BASE2	10BASE-F	10BASE-T

Maximum segment length	500 m	185 m	varies from 400 m to 2000 m	100m
topology	Bus	Bus	Star	Star
medium	50-"omega" thick coax.	50-"omega" thin coax.	multimode fiber	100-"omega" UTP
connector	NICDB15	BNC	ST	RJ-45
Medium attachment	MAU bolted to coax	ethernal or on NIC	External or on NIC	External or on NIC
stations/cable segment	100	30	N/A	2(NIC, repeater)
Maximum	5	5	5	5 segments

Fast Ethernet:

Specification	**100BASE-Tx**	**100BASE-Fx**	**100BASE-T4**
IEEE standard	802.3u-1995	802.3u-1995	802.3u-1995
Encoding	4B/5B	4B/5B	8B/6T
cabling	UTP cat.5 or STP	Multimode or single mode fiber	UTP cat.3/4/5
signal frequency	125 MHz	125 MHz	25 MHz
No. of pairs needed	2	2	4
No. of transmit pairs	1	1	3
distance	100m	150/412/2000 m	100m
Full duplex capabilities	Yes	Yes	No

Gigabit Ethernet:

Standard	Physical Medium
1000Base-SX	Fiber optics- maximum segment length 550m, Short wavelength
1000Base-LX	Fiber optics- maximum segment length 5000m, Long wavelength
1000Base-CX	2 pair of STP- maximum segment length 25m
1000Base-T	4 pairs of UTP – maximum segment length 100m

8. Difference between Fast Ethernet and Gigabit Ethernet.

- Speed of the Fast Ethernet is 100Mbps, whereas it is 1000Mbps in Gigabit Ethernet.

- ❖ Better performance and reduced bottlenecks are expected due to higher bandwidth in Gigabit Ethernet than Fast Ethernet.
- ❖ Upgrade from Ethernet to Fast Ethernet is easy and cheaper than upgrading Fast Ethernet to Gigabit Ethernet.
- ❖ Needs specific network devices, which can support 1000Mbps data rate, in Gigabit Ethernet.
- ❖ Devices connected to Gigabit Ethernet needs manual configuration up to some extent, whereas most of the devices connected to Fast Ethernet configure automatically themselves – negotiate the optimum speed and duplexity.

9. What are the common Standard Ethernet implementations?
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

10. What are the common Fast Ethernet implementations?
Fast Ethernet implementations

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

11. What are the common Gigabit Ethernet implementations?
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

12. What are the common Ten-Gigabit Ethernet implementations?
Ten-Gigabit Ethernet implementations

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