Module 4

MULTIPLE ACCESS

Introduction

• When nodes use shared-medium, we need multiple-access protocol to coordinate access to medium.

• Analogy:

- This problem is similar to the rules of speaking in an assembly.
- We need to ensure

→ Each people has right to speak.

→ Two people do not speak at the same time

→ Two people do not interrupt each other (i.e. Collision Avoidance)

• Many protocols have been designed to handle access to a shared-link (Figure 12.1).

• These protocols belong to a sublayer in the data-link layer called Media Access Control (MAC).

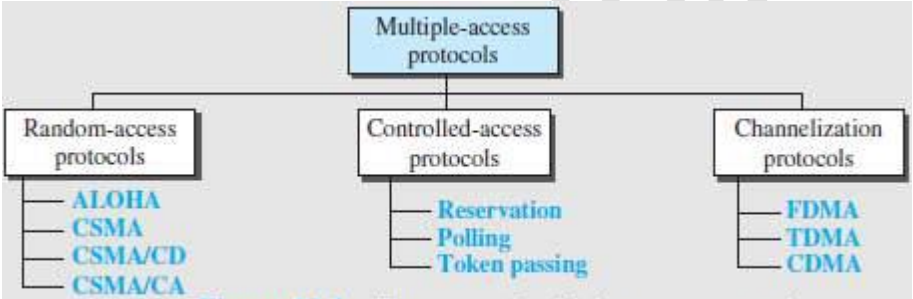


Figure 12.1 *Taxonomy of multiple-access protocols*

Random Access Protocol

• No station is superior to another station.

• No station is assigned control over other station.

• To send the data, a station uses a procedure to make a decision on whether or not to send.

• This decision depends on the state of the medium: idle or busy.

• This is called Random Access because

→ Transmission is random among the stations.

→ There is no scheduled-time for a station to transmit.

• This is called Contention Method because

→ Stations compete with one another to access the medium.

• If more than one station tries to send, there is an access-conflict (i.e. collision) and the frames will be destroyed.

• Each station follows a procedure that answers the following questions:

1) When can the station access the medium?

2) What can the station do if the medium is busy?

3) How can the station determine the success or failure of the transmission?

4) What can the station do if there is a collision?

• Random-access protocols (or Contention methods):

1) ALOHA

2) CSMA (Carrier Sense Multiple Access)

3) CSMA/CD (Carrier Sense Multiple Access with Collision-detection)

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

ALOHA

• ALOHA was designed for a wireless LAN, but it can be used on any shared medium.

• Since the medium is shared between the stations, there is possibility of collisions.

• When 2 or more stations send the data simultaneously, there is possibility of collision & data loss.

Pure ALOHA

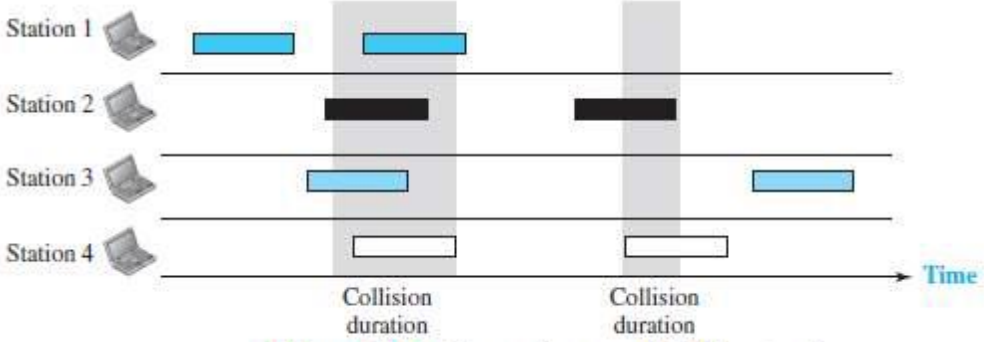


Figure 12.2 *Frames in a pure ALOHA network*

• Here is how it works (Figure 12.2):

1) The sender sends a frame & starts the timer.

2) The receiver receives the frame and responds with an acknowledgment.

3) If the acknowledgment does not arrive after a time-out period, the sender resends the frame. The sender assumes that the frame (or the acknowledgment) has been destroyed.

4) Since the medium is shared between the stations, there is possibility of collisions.

5) If two stations try to resend the frames after the time-out, the frames will collide again.

6) Two methods to deal with collision:

i) Randomness

¤ When the time-out period passes, each station waits a random amount of time before resending the frame. This time is called back-off time TB.

¤ The randomness will help avoid more collisions.

ii) Limit Maximum Retransmission

¤ This method prevents congestion by reducing the number of retransmitted frames.

¤ After a maximum number of retransmission-attempts K_{max}, a station must give up and try later (Figure 12.3).

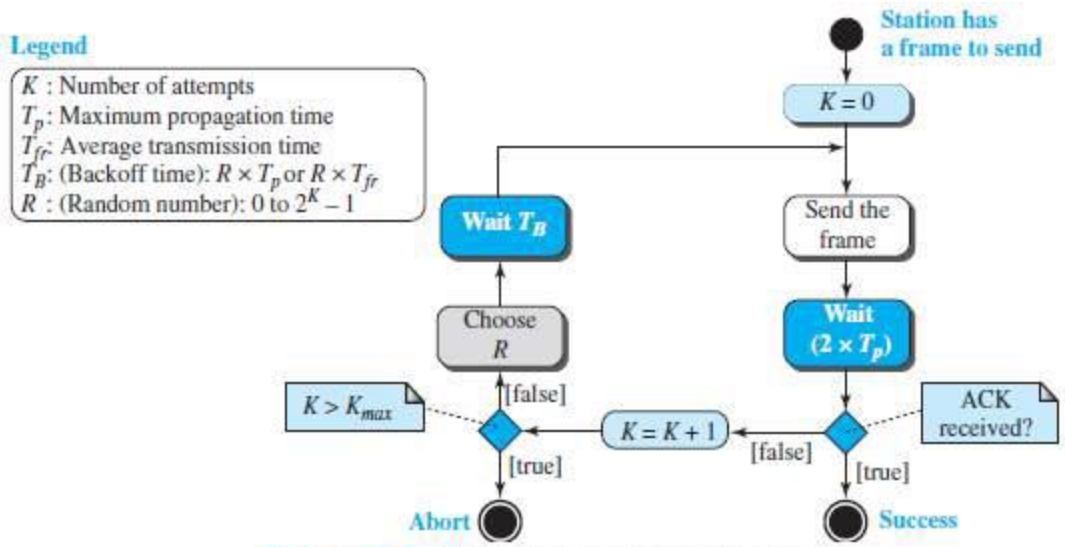


Figure 12.3 *Procedure for pure ALOHA protocol*

Vulnerable time

• The vulnerable-time is defined as a time during which there is a possibility of collision.

Pure ALOHA vulnerable time = $2 \times T_{fr}$

where T_{fr} = Frame transmission time

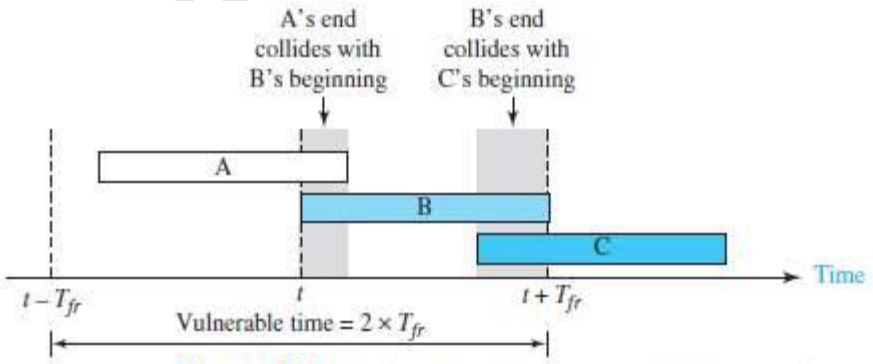


Figure 12.4 *Vulnerable time for pure ALOHA protocol*

• In Figure 12.4,

- If station B sends a frame between t-T_{fr} and t, this leads to a collision between the frames from station A and station B.

- If station C sends a frame between t and t+T_{fr}, this leads to a collision between the frames from station A and station C.

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the period (1 ms) that this station is sending.

Throughput

• The average number of successful transmissions is given by

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

where G = average no. of frames in one frame transmission time (T_{fr})

• For G = 1, the maximum throughput S_{max} = 0.184.

• In other words, out of 100 frames, 18 frames reach their destination successfully.

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is 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

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

a. If the system creates 1000 frames per second, or 1 frame per millisecond, then $G = 1$. In this case $S = G \times e^{-2G} = 0.135$ (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, or 1/2 frames per millisecond, then $G = 1/2$. In this case $S = G \times e^{-2G} = 0.184$ (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, or 1/4 frames per millisecond, then $G = 1/4$. In this case $S = G \times e^{-2G} = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

Slotted ALOHA

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

• The time is divided into time-slots of T_{fr} seconds (Figure 12.5).

• The stations are allowed to send only at the beginning of the time-slot.

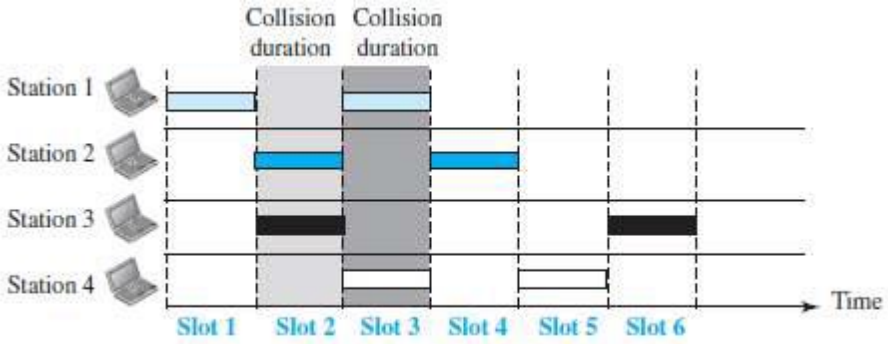


Figure 12.5 *Frames in a slotted ALOHA network*

• If a station misses the time-slot, the station must wait until the beginning of the next time-slot.

• If 2 stations try to resend at beginning of the same time-slot, the frames will collide again (Fig 12.6).

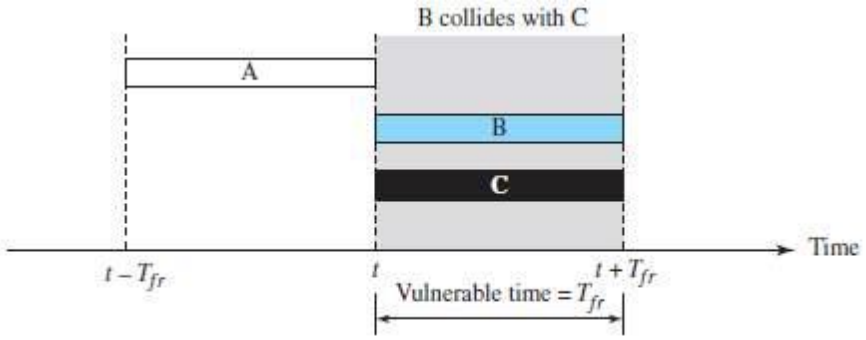


Figure 12.6 *Vulnerable time for slotted ALOHA protocol*

The vulnerable time is given by:

vulnerable time = T_{fr}

Throughput

• The average number of successful transmissions is given by

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

• For G = 1, the maximum throughput S_{max} = 0.368.

• In other words, out of 100 frames, 36 frames reach their destination successfully.

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 $S = G \times e^{-G} = 0.368$ (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 1/2. In this case $S = G \times e^{-G} = 0.303$ (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 1/4. In this case $S = G \times e^{-G} = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

CSMA (Carrier Sense Multiple Access)

• CSMA was developed to minimize the chance of collision and, therefore, increase the performance.

• CSMA is based on the principle "sense before transmit" or "listen before talk."

• Here is how it works:

1) Each station checks the state of the medium: idle or busy.

2) i) If the medium is idle, the station sends the data.

ii) If the medium is busy, the station defers sending.

• CSMA can reduce the possibility of collision, but it cannot eliminate it.

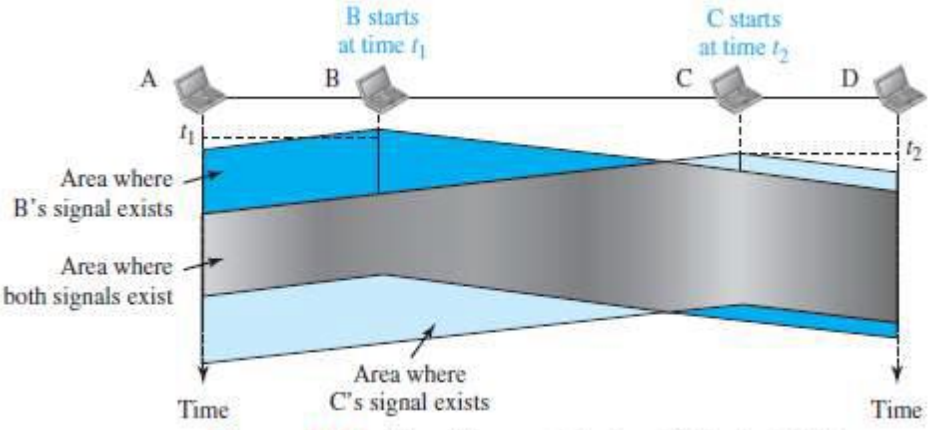


Figure 12.7 *Space/time model of a collision in CSMA*

• The possibility of collision still exists.

For example:

When a station sends a frame, it still takes time

→ for the first bit to reach every station and

→ for every station to sense it.

• For example: In Figure 12.7

- At time t1, station B senses & finds the medium idle, so sends a frame.
- At time t2, station C senses & finds the medium idle, so sends a frame.
- The 2 signals from both stations B & C collide and both frames are destroyed.

Vulnerable Time

• The vulnerable time is the propagation time Tp (Figure 12.8).

• The propagation time is the time needed for a signal to propagate from one end of the medium to the other.

• Collision occurs when

→ a station sends a frame, and

→ other station also sends a frame during propagation time

• If the first bit of the frame reaches the end of the medium, every station will refrain from sending.

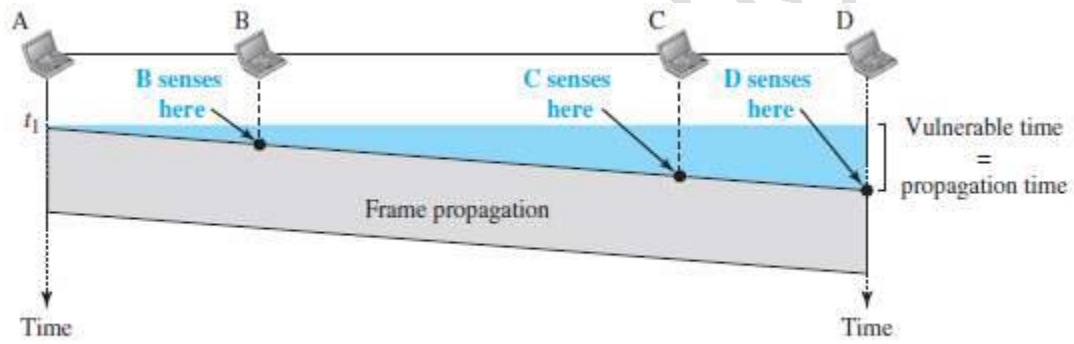


Figure 12.8 *Vulnerable time in CSMA*

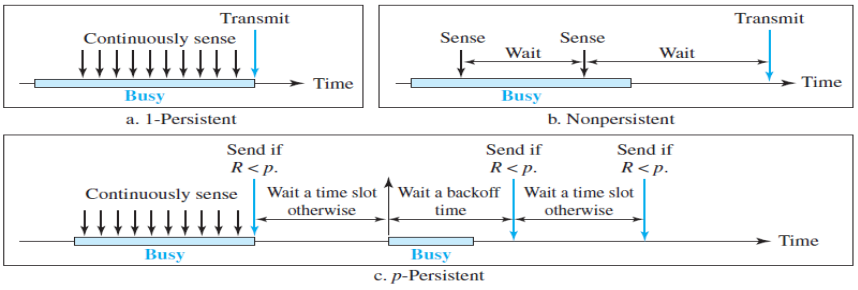
Persistence Methods

• What should a station do if the channel is busy or idle?

Three methods can be used to answer this question:

1) 1-persistent method 2) Non-persistent method and 3) p-persistent method

Figure 12.9 *Behavior of three persistence methods*



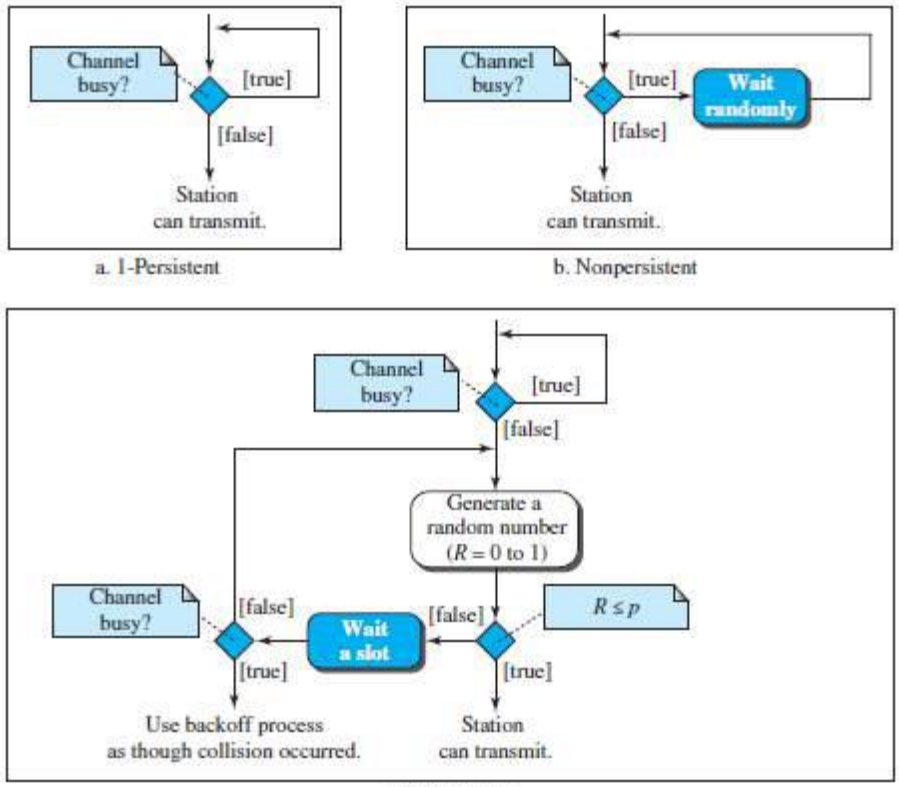


Figure 12.10 *Flow diagram for three persistence methods*

1) 1-Persistent

• Before sending a frame, a station senses the line (Figure 12.10a).

i) If the line is idle, the station sends immediately (with probability = 1).

ii) If the line is busy, the station continues sensing the line.

• This method has the highest chance of collision because 2 or more stations:

→ may find the line idle and

→ send the frames immediately.

2) Non-persistent

• Before sending a frame, a station senses the line (Figure 12.10b).

i) If the line is idle, the station sends immediately.

ii) If the line is busy, the station waits a random amount of time and then senses the line again.

• This method reduces the chance of collision because 2 or more stations:

→ will not wait for the same amount of time and

→ will not retry to send simultaneously.

3) P-Persistent

• This method is used if the channel has time-slots with a slot-duration equal to or greater than the maximum propagation time (Figure 12.10c).

• Advantages:

i) It combines the advantages of the other 2 methods.

ii) It reduces the chance of collision and improves efficiency.

• After the station finds the line idle, it follows these steps:

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

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

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

ii) If line is busy, it assumes that collision has occurred and uses the back off procedure.

CSMA/CD (Carrier Sense Multiple Access with Collision-detection)

• Disadvantage of CSMA: CSMA does not specify the procedure after a collision has occurred.

Solution: CSMA/CD enhances the CSMA to handle the collision.

• Here is how it works (Figure 12.12):

1) A station
   → sends the frame &
   → then monitors the medium to see if the transmission was successful or not.
2) If the transmission was unsuccessful (i.e. there is a collision), the frame is sent again.

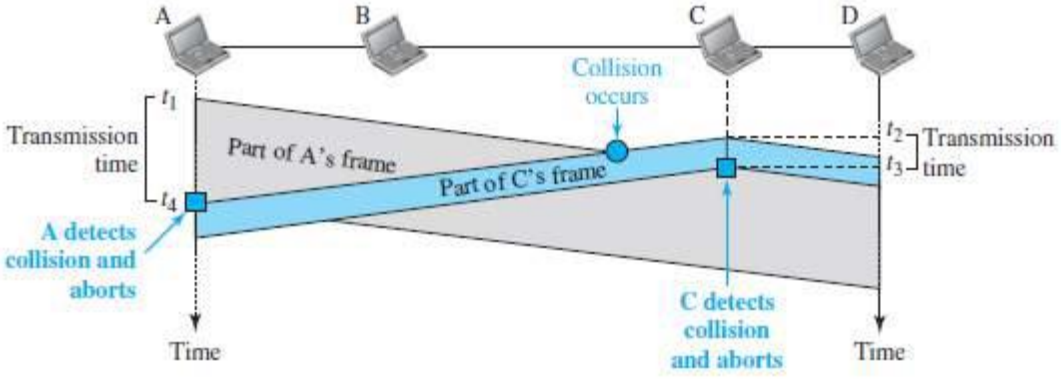


Figure 12.12 *Collision and abortion in CSMA/CD*

• In the Figure 12.11,

- At time t1, station A has executed its procedure and starts sending the bits of its frame.
- At time t2, station C has executed its procedure and starts sending the bits of its frame.
- The collision occurs sometime after time t2.
- Station C detects a collision at time t3 when it receives the first bit of A's frame. Station C immediately aborts transmission.

- Station A detects collision at time t4 when it receives the first bit of C's frame. Station A also immediately aborts transmission.
- Station A transmits for the duration t4–t1. Station C transmits for the duration t3-t2.
- For the protocol to work:
    - The length of any frame divided by the bit rate must be more than either of these durations.

Minimum Frame Size

• For CSMA/CD to work, we need to restrict the frame-size.

• Before sending the last bit of the frame, the sender must

→ detect a collision and

→ abort the transmission.

• This is so because the sender

→ does not keep a copy of the frame and

→ does not monitor the line for collision-detection.

• Frame transmission time T_{fr} is given by

$$\mathbf{T_{fr}=2T_p}$$

where T_p=maximum propagation time

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs, what is the minimum size of the frame?

Solution

The minimum frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet, as we will see later in the chapter.

Procedure

• CSMA/CD is similar to ALOHA with 2 differences (Figure 12.13):

1) Addition of the persistence process.

¤ We need to sense the channel before sending the frame by using non-persistent, 1- persistent or p-persistent.

2) Frame transmission.

i) In ALOHA, first the entire frame is transmitted and then acknowledgment is waited for.

ii) In CSMA/CD, transmission and collision-detection is a continuous process.

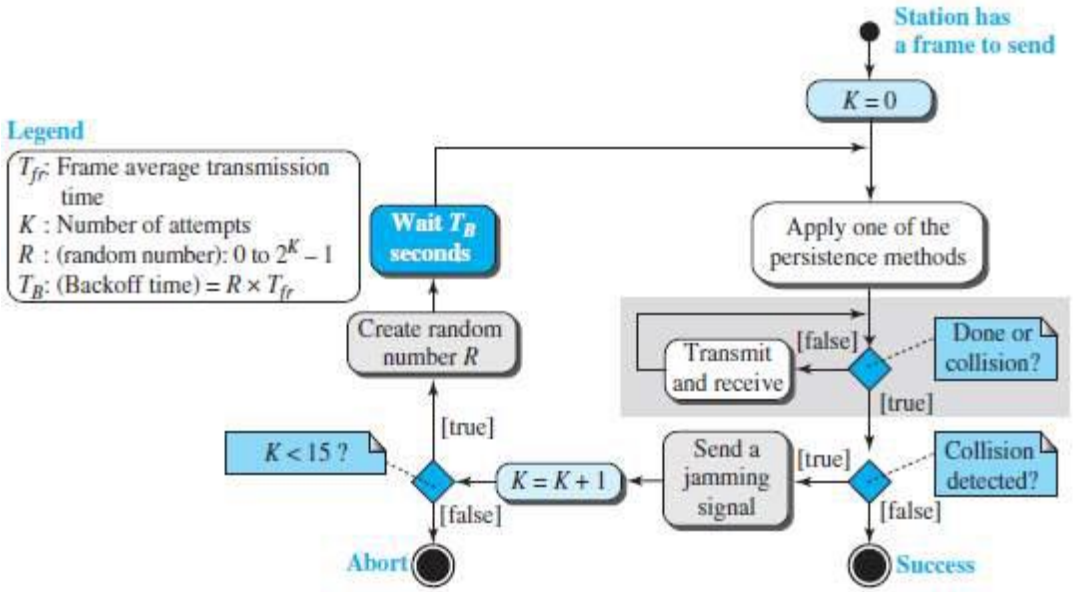


Figure 12.13 *Flow diagram for the CSMA/CD*

Energy Level

• In a channel, the energy-level can have 3 values: 1) Zero 2) Normal and 3) Abnormal.

1) At zero level, the channel is idle (Figure 12.14).

2) At normal level, a station has successfully captured the channel and is sending its frame.

3) At abnormal level, there is a collision and the level of the energy is twice the normal level.

• A sender needs to monitor the energy-level to determine if the channel is

→ Idle

→ Busy or

→ Collision mode

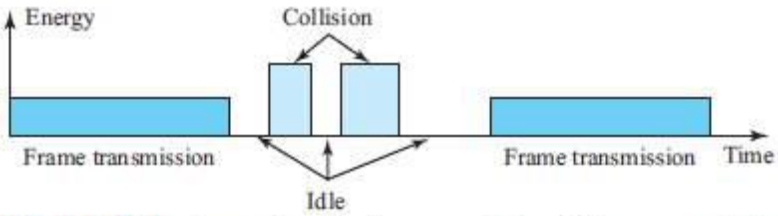


Figure 12.14 *Energy level during transmission, idleness, or collision*

Throughput

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

• The maximum throughput is based on

→ Different value of G

→ Persistent method used (non-persistent, 1-persistent, or p-persistent) and

→ 'p' value in the p-persistent method.

• For 1-persistent method, the maximum throughput is 50% when G =1.

• For non-persistent method, the maximum throughput is 90% when G is between 3 and 8.

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

• Here is how it works (Figure 12.15):

1) A station needs to be able to receive while transmitting to detect a collision.

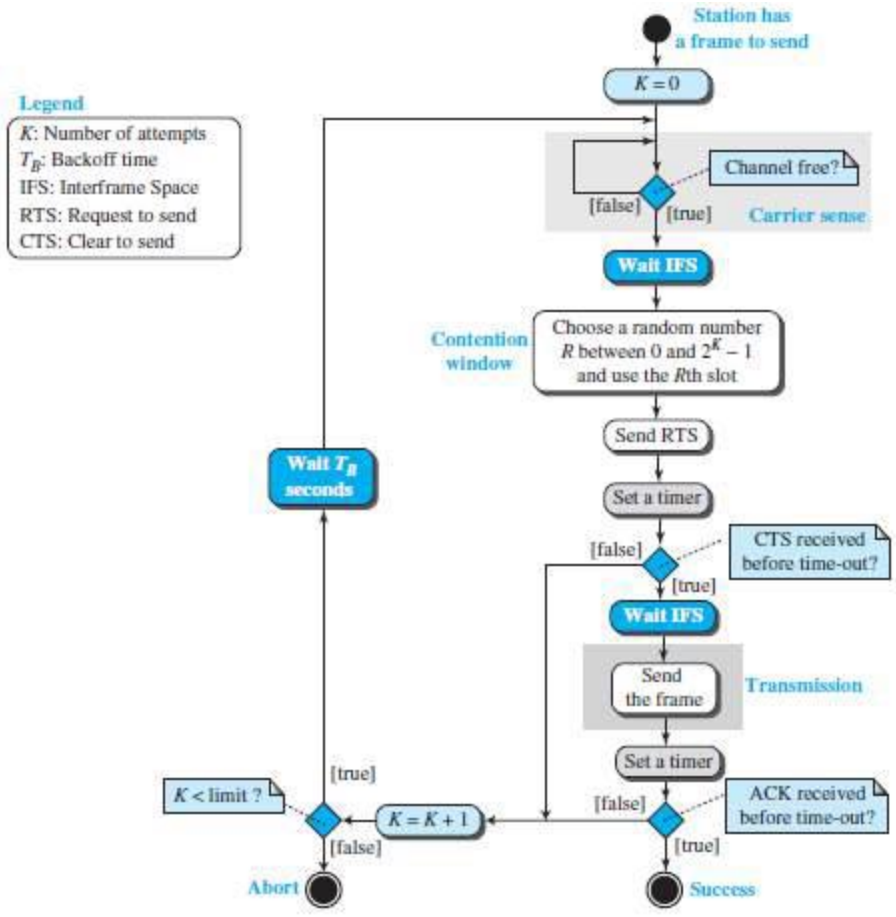
i) When there is no collision, the station receives one signal: its own signal.

ii) When there is a collision, the station receives 2 signals:

a) Its own signal and

b) Signal transmitted by a second station.

2) To distinguish b/w these 2 cases, the received signals in these 2 cases must be different.



• CSMA/CA was invented to avoid collisions on wireless networks.

• **Three methods to avoid collisions** (Figure 12.16):

1) Interframe space(IFS) 2) Contention window and 3) Acknowledgments

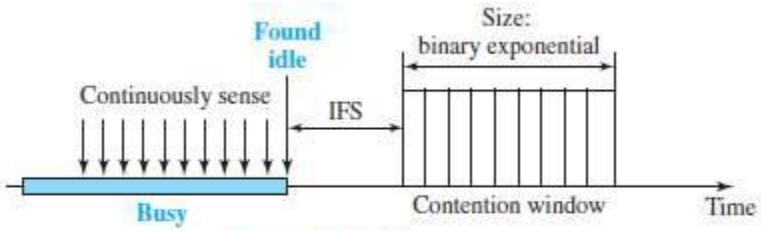


Figure 12.16 *Contention window*

1) Interframe Space (IFS)

• Collisions are avoided by deferring transmission even if the channel is found idle.

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

• After the IFS time, if the channel is still idle, then, the station waits for the contention-time & finally, the station sends the frame.

• 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.

2) Contention Window

• The contention-window is an amount of time divided into time-slots.

• A ready-station chooses a random-number of slots as its wait time.

• In the window, the number of slots changes according to the binary exponential back-off strategy.

• For example:

At first time, number of slots is set to one slot and

Then, number of slots is doubled each time if the station cannot detect an idle channel.

3) Acknowledgment

• There may be a collision resulting in destroyed-data.

• In addition, the data may be corrupted during the transmission.

• To help guarantee that the receiver has received the frame, we can use

i) Positive acknowledgment and

ii) Time-out timer

Frame Exchange Time Line

• Two control frames are used:

1) Request to send (RTS)

2) Clear to send (CTS)

• The procedure for exchange of data and control frames in time (Figure 12.17):

1) The source senses the medium by checking the energy level at the carrier frequency.

ii) If the medium is idle, then the source waits for a period of time called the DCF Interframe Space (DIFS); finally, the source sends a RTS.

2) The destination

→ receives the RTS

→ waits a period of time called the short interframe space (SIFS)

→ sends a control frame CTS to the source.

CTS indicate that the destination station is ready to receive data.

3) The source

→ receives the CTS

→ waits a period of time SIFS

→ sends a data to the destination

4) The destination

→ receives the data

→ waits a period of time SIFS

→ sends a acknowledgment ACK to the source.

ACK indicates that the destination has been received the frame.

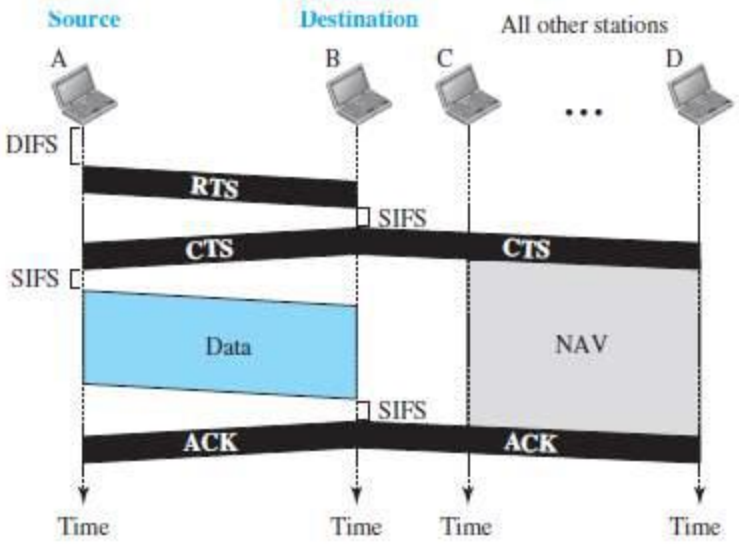


Figure 12.17 *CSMA/CA and NAV*

Network Allocation Vector (NAV)

• When a source-station sends an RTS, it includes the duration of time that it needs to occupy the channel.

• The remaining stations create a timer called a network allocation vector (NAV).

• NAV indicates waiting time to check the channel for idleness.

• Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

Collision during Handshaking

• Two or more stations may try to send RTS at the same time.

• These RTS may collide.

• The source assumes there has been a collision if it has not received CTS from the destination.

• The backoff strategy is employed, and the source tries again.

Hidden-Station Problem

• Figure 12.17 also shows that the RTS from B reaches A, but not C.

• However, because both B and C are within the range of A, the CTS reaches C.

• Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

CSMA/CA and Wireless Networks

• CSMA/CA was mostly intended for use in wireless networks.

• However, it is not sophisticated enough to handle some particular issues related to wireless networks, such as hidden terminals or exposed terminals.

CONTROLLED ACCESS PROTOCOLS

• Here, the stations consult one another to find which station has the right to send.

• A station cannot send unless it has been authorized by other stations.

• Three popular controlled-access methods are:

1) Reservation

2) Polling

3) Token Passing

Reservation

• Before sending data, each station needs to make a reservation of the medium.

• Time is divided into intervals.

• In each interval, a reservation-frame precedes the data-frames.

• If no. of stations = N, then there are N reservation mini-slots in the reservation-frame.

• Each mini-slot belongs to a station.

• When a station wants to send a data-frame, it makes a reservation in its own minislot.

• The stations that have made reservations can send their data-frames.

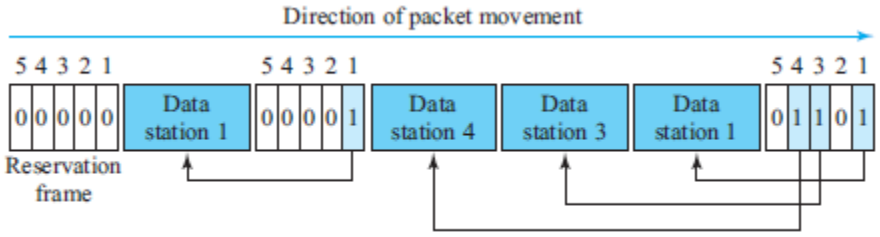


Figure 12.18 *Reservation access method*

For example (Figure 12.18):

- 5 stations have a 5-minislot reservation-frame.
- In the first interval, only stations 1, 3, and 4 have made reservations.
- In the second interval, only station-1 has made a reservation.

Polling

• In a network, one device is designated as a primary station and other devices are designated as secondary stations.

• Functions of primary-device:

1) The primary-device controls the link.

2) The primary-device is always the initiator of a session.

3) The primary-device is determines which device is allowed to use the channel at a given time.

4) All data exchanges must be made through the primary-device.

• The secondary devices follow instructions of primary-device.

• Disadvantage: If the primary station fails, the system goes down.

• Poll and select functions are used to prevent collisions (Figure 12.19).

1) Select

- If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.
- The primary

→ alerts the secondary about upcoming transmission by sending select frame (SEL)

→ then waits for an acknowledgment (ACK) from secondary

→ then sends the data frame and

→ finally waits for an acknowledgment (ACK) from the secondary.

2) Poll

- If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function.
- When the first secondary is approached, it responds either

  → with a NAK frame if it has no data to send or

  → with data-frame if it has data to send.

  i) If the response is negative (NAK frame), then the primary polls the next secondary in the same manner.

  ii) When the response is positive (a data-frame), the primary

  → reads the frame and

  → returns an acknowledgment (ACK frame).

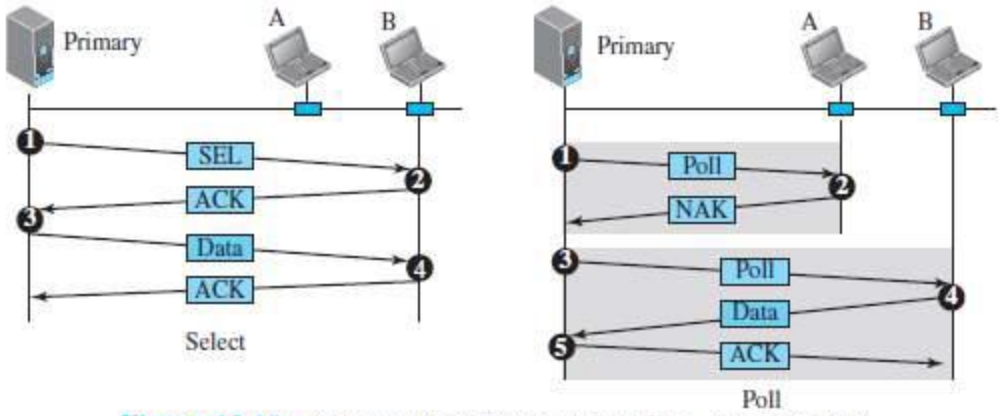


Figure 12.19 *Select and poll functions in polling-access method*

Token Passing

• In a network, the stations are organized in a ring fashion i.e. for each station; there is a predecessor and a successor.

1) The predecessor is the station which is logically before the station in the ring.

2) The successor is the station which is after the station in the ring.

• The current station is the one that is accessing the channel now.

• A token is a special packet that circulates through the ring.

• Here is how it works:

- A station can send the data only if it has the token.
- When a station wants to send the data, it waits until it receives the token from its predecessor.
- Then, the station holds the token and sends its data.
- When the station finishes sending the data, the station

→ releases the token

→ passes the token to the successor.

• Main functions of token management:

1) Stations must be limited in the time they can hold the token.

2) The token must be monitored to ensure it has not been lost or destroyed.

For ex: if a station that is holding the token fails, the token will disappear from the network

3) Assign priorities

→ to the stations and

→ to the types of data being transmitted.

4) Make low-priority stations release the token to high priority stations.

Logical Ring

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

• Four physical topologies to create a logical ring (Figure 12.20):

1) Physical ring

2) Dual ring

3) Bus ring

4) Star ring

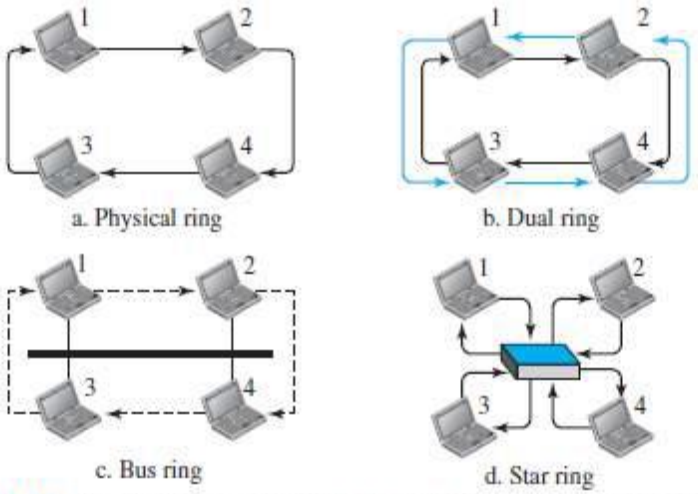


Figure 12.20 *Logical ring and physical topology in token-passing access method*

1) Physical Ring Topology

• When a station sends token to its successor, token cannot be seen by other stations. (Figure 12.20a)

• This means that the token does not have the address of the next successor.

• Disadvantage: If one of the links fails, the whole system fails.

2) Dual Ring Topology

• A second (auxiliary) ring

→ is used along with the main ring (Figure 12.20b).

→ operates in the reverse direction compared with the main ring.

→ is used for emergencies only (such as a spare tire for a car).

• If the main ring fails, the system automatically combines the 2 rings to form a temporary ring.

• After the failed link is restored, the second ring becomes idle again.

• Each station needs to have 2 transmitter-ports and 2 receiver-ports.

• This topology is used in

i) FDDI (Fiber Distributed Data Interface) and

ii) CDDI (Copper Distributed Data Interface).

3) Bus Ring Topology

• The stations are connected to a single cable called a bus (Figure 12.20c).

• This makes a logical ring, because each station knows the address of its successor and predecessor.

• When a station has finished sending its data, the station

→ releases the token and

→ inserts the address of its successor in the token.

• Only the station gets the token to access the shared media.

• This topology is used in the Token Bus LAN.

4) Star Ring Topology

• The physical topology is a star (Figure 12.20d).

• There is a hub that acts as the connector.

• The wiring inside the hub makes the ring i.e. the stations are connected to the ring through the 2 wire connections.

• Disadvantages:

1) This topology is less prone to failure because

If a link goes down, then the link will be bypassed by the hub and the rest of the stations can operate.

2) Also adding and removing stations from the ring is easier.

• This topology is used in the Token Ring LAN.

CHANNELIZATION PROTOCOLS

• Channelization is a multiple-access method.

• The available bandwidth of a link is shared b/w different stations in time, frequency, or through code.

• Three channelization protocols:

1) FDMA (Frequency Division Multiple Access)

2) TDMA (Time Division Multiple Access) and

3) CDMA (Code Division Multiple Access)

FDMA (Frequency Division Multiple Access)

• The available bandwidth is divided into frequency-bands (Figure 12.21).

• Each band is reserved for a specific station.

• Each station can send the data in the allocated band.

• Each station also uses a bandpass filter to confine the transmitter frequencies.

• To prevent interferences, small guard bands are used to separate the allocated bands from one another.

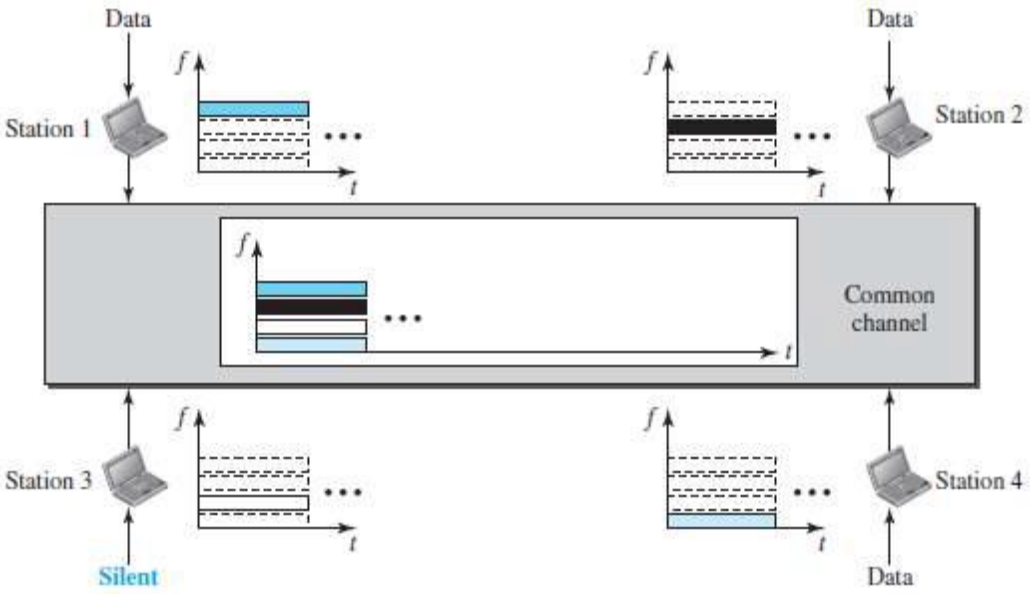


Figure 12.21 *Frequency-division multiple access (FDMA)*

• FDM vs. FDMA

1) FDM

- FDM is a multiplexing method in the physical layer.
- FDM

  → combines individual-loads from low-bandwidth channels and

  → transmits aggregated-load by using a high-bandwidth channel.
- The channels that are combined are low-pass.

- The multiplexer
  → modulates & combines the signals and
  → creates a bandpass signal.
- The bandwidth of each channel is shifted by the multiplexer.

2) FDMA

- FDMA is an access method in the data link layer.
- In each station, the data link layer tells the physical layer to make a bandpass signal from the data passed to it.
- The signal must be created in the allocated band.
- There is no physical multiplexer at the physical layer.
- The signals created at each station are automatically bandpass-filtered.
- They are mixed when they are sent to the common channel.

TDMA (Time Division Multiple Access)

• The stations share the bandwidth of the channel in time (Figure 12.22).

• Each time-slot is reserved for a specific station.

• Each station can send the data in the allocated time-slot.

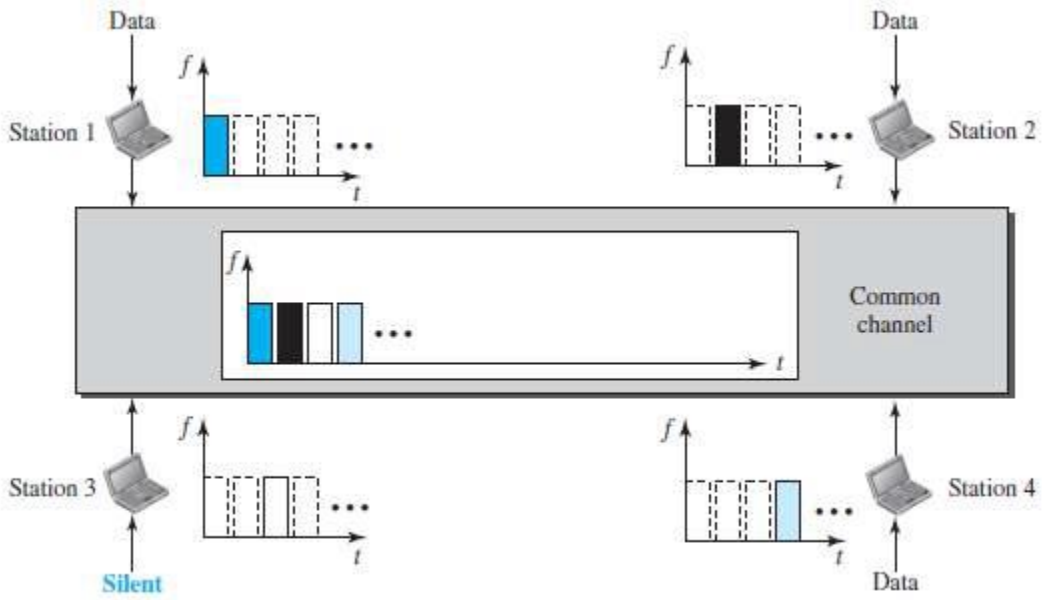


Figure 12.22 *Time-division multiple access (TDMA)*

• Main problem: Achieving synchronization between the different stations. i.e. each station needs to know the beginning of its slot and the location of its slot.

This may be difficult because of propagation delays introduced in the system.

• To compensate for the delays, we can insert guard-times.

• Normally, synchronization is accomplished by having some synchronization bits at the beginning of each slot.

• TDMA vs. TDM

1) TDM

- TDM is a multiplexing method in the physical layer.
- TDM:

  → combines the individual-data from slower channels and

  → transmits the aggregated- data by using a faster channel.
- The multiplexer interleaves data units from each channel.

2) TDMA

- TDMA is an access method in the data link layer.
- In each station, the data link layer tells the physical layer to use the allocated time-slot.
- There is no physical multiplexer at the physical layer.

CDMA (Code Division Multiple Access)

• CDMA simply means communication with different codes.

• CDMA differs from FDMA because

→ only one channel occupies the entire bandwidth of the link.

• CDMA differs from TDMA because

→ all stations can send data simultaneously; there is no timesharing.

(Analogy: CDMA simply means communication with different codes.

For example, in a large room with many people, 2 people can talk privately in English if nobody else understands English. Another 2 people can talk in Chinese if they are the only ones who understand Chinese, and so on).

Implementation

• Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel.

• The data from station-1 are d1, from station-2 are d2, and so on.

• The code assigned to the first station is c1, to the second is c2, and so on.

• We assume that the assigned codes have 2 properties.

1) If we multiply each code by another, we get 0.

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

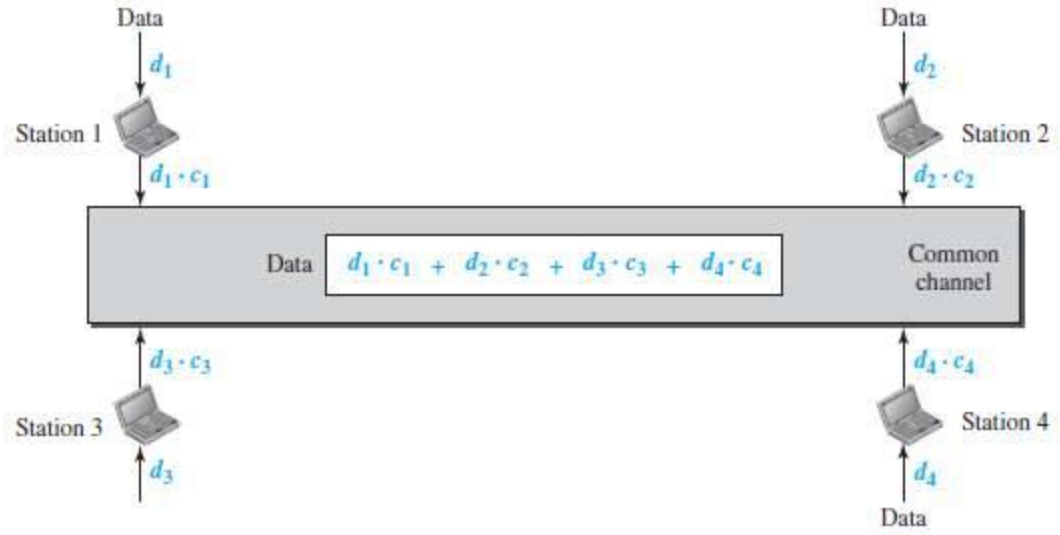


Figure 12.23 *Simple idea of communication with code*

Here is how it works (Figure 12.23):

- Station-1 multiplies the data by the code to get d1.c1.
- Station-2 multiplies the data by the code to get d2.c2. And so on.
- The data that go on the channel are the sum of all these terms.

$$d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4$$

- The receiver multiplies the data on the channel by the code of the sender.
- For example, suppose stations 1 and 2 are talking to each other.
- Station-2 wants to hear what station-1 is saying.
- Station-2 multiplies the data on the channel by c1 the code of station-1.

(c1.c1)=4, (c2.c1)=0, (c3.c1)=0, and (c4.c1)=0,

Therefore, station-2 divides the result by 4 to get the data from station-1.

$$\begin{aligned} \text{data} &= (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1 \\ &= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 = 4 \times d_1 \end{aligned}$$

Chips

• CDMA is based on coding theory.

• Each station is assigned a code, which is a sequence of numbers called chips (Figure 12.24).

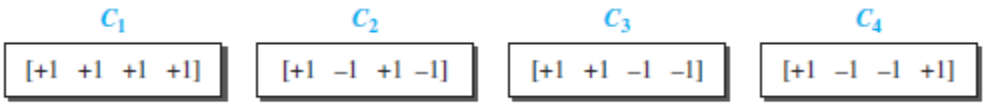


Figure 12.24 *Chip sequences*

These sequences were carefully selected & are called orthogonal sequences

• These sequences have the following properties:

1) Each sequence is made of N elements, where N is the number of stations.

2) Multiplication of a sequence by a scalar:

If we multiply a sequence by a number i.e. every element in the sequence is multiplied by that element.

For example,

$$2 \cdot [+1 +1 -1 -1] = [+2 +2 -2 -2]$$

3) Inner product of 2 equal sequences:

If we multiply 2 equal sequences, element by element, and add the results, we get N, where N is the number of elements in the each sequence.

For example,

$$[+1 +1 -1 -1] \cdot [+1 +1 -1 -1] = 1 + 1 + 1 + 1 = 4$$

4) Inner product of 2 different sequences:

If we multiply 2 different sequences, element by element, and add the results, we get 0.

For example,

$$[+1 +1 -1 -1] \cdot [+1 +1 +1 +1] = 1 + 1 - 1 - 1 = 0$$

5) Adding 2 sequences means adding the corresponding elements. The result is another sequence.

For example,

$$[+1 +1 -1 -1] + [+1 +1 +1 +1] = [+2 +2 \ 0 \ 0]$$

Data Representation

• We follow the following rules for encoding:

1) To send a 0 bit, a station encodes the bit as -1

2) To send a 1 bit, a station encodes the bit as +1

3) When a station is idle, it sends no signal, which is interpreted as a 0.

Encoding and Decoding

We assume that

- Stations 1 and 2 are sending a 0 bit.
- Station-4 is sending a 1 bit.
- Station-3 is silent.

Here is how it works (Figure 12.26):

- At the sender-site, the data are translated to -1, -1, 0, and +1.
- Each station multiplies the corresponding number by its chip (its orthogonal sequence).
- The result is a new sequence which is sent to the channel.

- The sequence on the channel is the sum of all 4 sequences.
- Now imagine station-3, which is silent, is listening to station-2.
- Station-3 multiplies the total data on the channel by the code for station-2, which is [+1 -1 +1-1], to get $[-1\ -1\ -3\ +1] \bullet [+1\ -1\ +1\ -1] = -4/4 = -1 \rightarrow$ bit 1

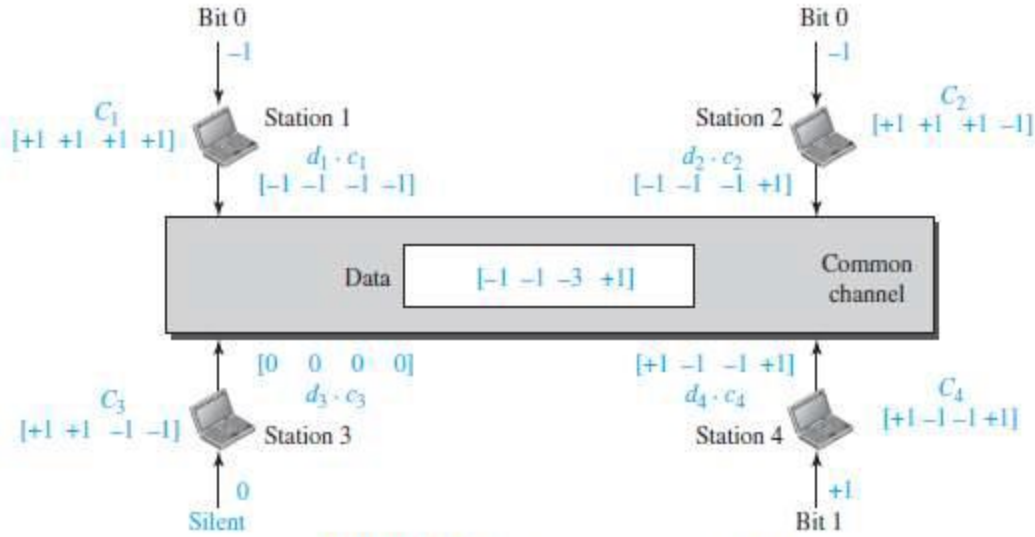


Figure 12.26 *Sharing channel in CDMA*

Sequence Generation

• To generate chip sequences, we use a Walsh table (Figure 12.29).

• Walsh table is a 2-dimensional table with an equal number of rows and columns.

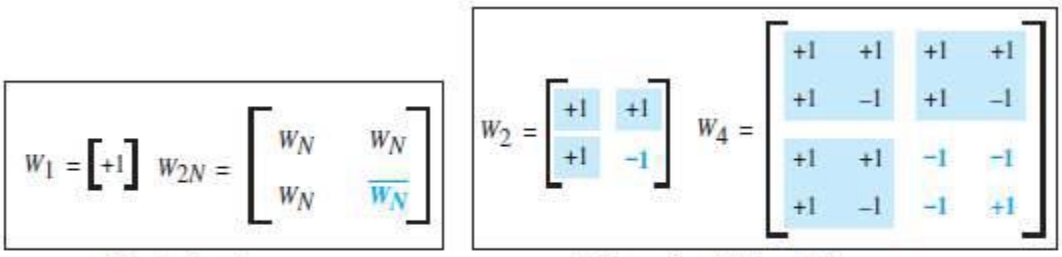


Figure 12.29 *General rule and examples of creating Walsh tables*

• In the Walsh table, each row is a sequence of chips.

• W1 for a one-chip sequence has one row and one column. We can choose –1 or +1 for the chip for this trivial table (we chose +1).

• According to Walsh, if we know the table for N sequences W_N, we can create the table for 2N sequences W_{2N} (Figure 12.29).

• The W_N with the overbar W_N stands for the complement of W_N where each +1 is changed to -1 and vice versa.

• After we select W_1, W_2 can be made from four W_1's, with the last one the complement of W_1

• After W_2 is generated, W_4 can be made of four W_2's, with the last one the complement of W_2.

• The number of sequences in a Walsh table needs to be $N = 2^m$.

Find the chips for a network with

a. Two stations
b. Four stations

Solution

We can use the rows of W_2 and W_4 in Figure 12.29:

a. For a two-station network, we have [+1 +1] and [+1 −1].
b. For a four-station network we have [+1 +1 +1 +1], [+1 −1 +1 −1], [+1 +1 −1 −1], and [+1 −1 −1 +1].

What is the number of sequences if we have 90 stations in our network?

Solution

The number of sequences needs to be 2^m. We need to choose $m = 7$ and $N = 2^7$ or 128. We can then use 90 of the sequences as the chips.

Prove that a receiving station can get the data sent by a specific sender if it multiplies the entire data on the channel by the sender's chip code and then divides it by the number of stations.

Solution

Let us prove this for the first station, using our previous four-station example. We can say that the data on the channel $D = (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4)$. The receiver that wants to get the data sent by station 1 multiplies these data by c_1.

$$
\begin{aligned}
D \cdot c_1 &= (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \quad c_1 \\
&= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 \\
&= d_1 \times N + d_2 \times 0 + d_3 \times 0 + d_4 \times 0 \\
&= d_1 \times N
\end{aligned}
$$

When we divide the result by N, we get d_1.

WIRED LANs – ETHERNET

ETHERNET PROTOCOL

IEEE Project 802

• The data-link-layer is divided into 2 sublayers (Figure 13.1):

1) LLC

- Flow-control, error-control, and framing duties are grouped into one sublayer called LLC.
- Framing is handled in both the LLC and the MAC.
- LLC vs. MAC

  i) LLC provides one single data-link-control protocol for all IEEE LANs.

  ii) MAC provides different protocols for different LANs.
- A single LLC protocol can provide interconnectivity between different LANs because

  → it makes the MAC sublayer transparent.

2) MAC

- This defines the specific access-method for each LAN.
- For example:

  i) CSMA/CD is used for Ethernet LANs.

  ii) Token-passing method is used for Token Ring and Token Bus LANs.
- The framing function is also handled by the MAC layer.
- The MAC contains a number of distinct modules.
- Each module defines the access-method and the framing-format specific to the corresponding LAN protocol.

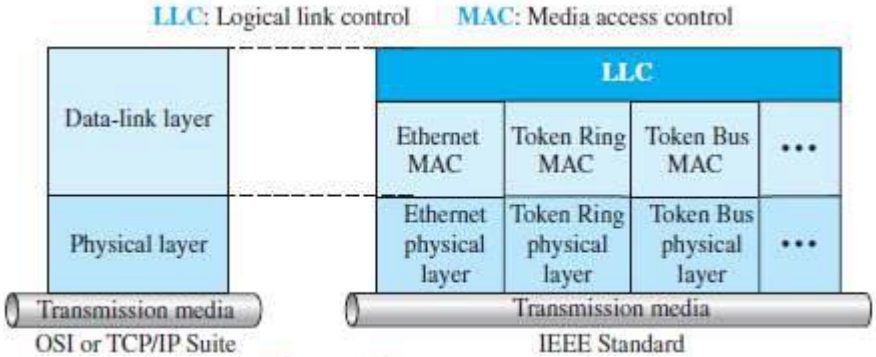


Figure 13.1 *IEEE standard for LANs*

Ethernet Evolution

• Four generations of Ethernet (Figure 13.2):

1) Standard-Ethernet (10 Mbps)

2) Fast-Ethernet (100 Mbps)

3) Gigabit-Ethernet (1 Gbps) and

4) Ten-Gigabit-Ethernet (10 Gbps)

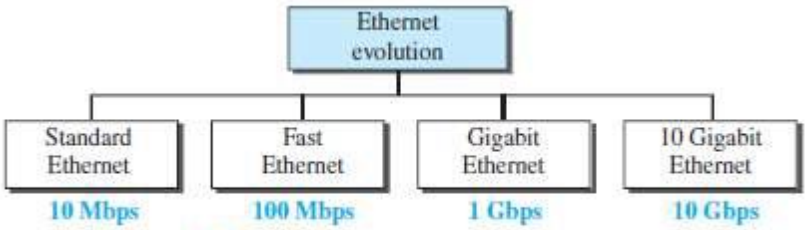


Figure 13.2 *Ethernet evolution through four generations*

STANDARD-ETHERNET

• The original Ethernet technology with data-rate of 10 Mbps are referred to as the Standard Ethernet.

Characteristics

Connectionless and Unreliable Service

• Ethernet provides a connectionless service. Thus, each frame sent is independent of another frame.

• Ethernet has no connection establishment or connection termination phases.

• The sender sends a frame whenever it has it.

The receiver may or may not be ready for receiving the frame.

• The sender may overload the receiver with frames, which may result in dropping frames.

1) If a frame drops, the sender will not know about it.

2) If a frame is corrupted during transmission, the receiver drops the frame.

• Since IP is also connectionless, it will also not know about frame drops.

1) If the transport layer is UDP (connectionless protocol), the frame is lost.

2) If the transport layer is TCP, the sender-TCP does not receive acknowledgment for its segment and sends it again.

• Ethernet is also unreliable like IP and UDP.

Frame Format

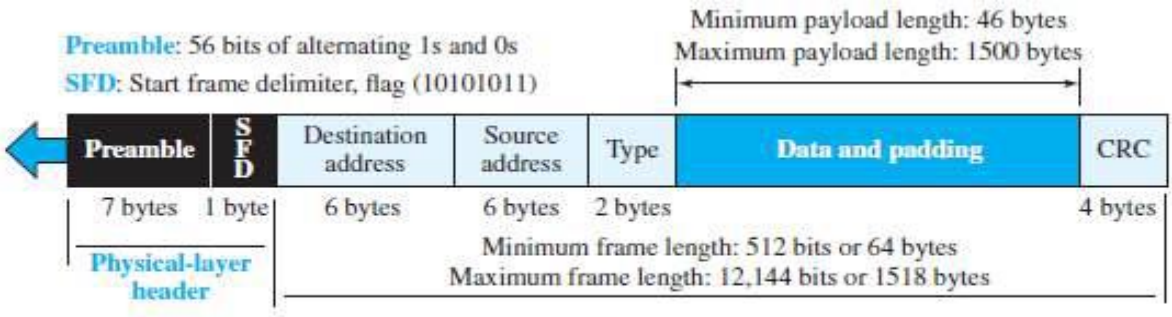


Figure 13.3 *Ethernet frame*

• The Ethernet frame contains 7 fields (Figure 13.3):

1) Preamble

- This field contains 7 bytes (56 bits) of alternating 0s and 1s.
- This field

  → alerts the receiving-system to the coming frame and

  → enables the receiving-system to synchronize its input timing.
- The preamble is actually added at the physical-layer and is not (formally) part of the frame.

2) Start frame delimiter (SFD)

- This field signals the beginning of the frame.
- The SFD warns the stations that this is the last chance for synchronization.
- This field contains the value: 10101011.
- The last 2 bits (11) alerts the receiver that the next field is the destination-address.

3) Destination-address (DA)

- This field contains the physical-address of the destination-station.

4) Source-address (SA)

- This field contains the physical-address of the sender-station.

5) Length or type

- This field is defined as a i) type field or ii) length field.

  i) In original Ethernet, this field is used as the type field.

  ¤ Type field defines the upper-layer protocol using the MAC frame.

  ii) In IEEE standard, this field is used as the length field.

  ¤ Length field defines the number of bytes in the data-field.

6) Data

- This field carries data encapsulated from the upper-layer protocols.
- Minimum data size = 46 bytes. Maximum data size = 1500 bytes.

7) CRC

- This field contains error detection information such as a CRC-32.

Frame Length

• Ethernet has imposed restrictions on both minimum & maximum lengths of a frame (Figure 13.5).

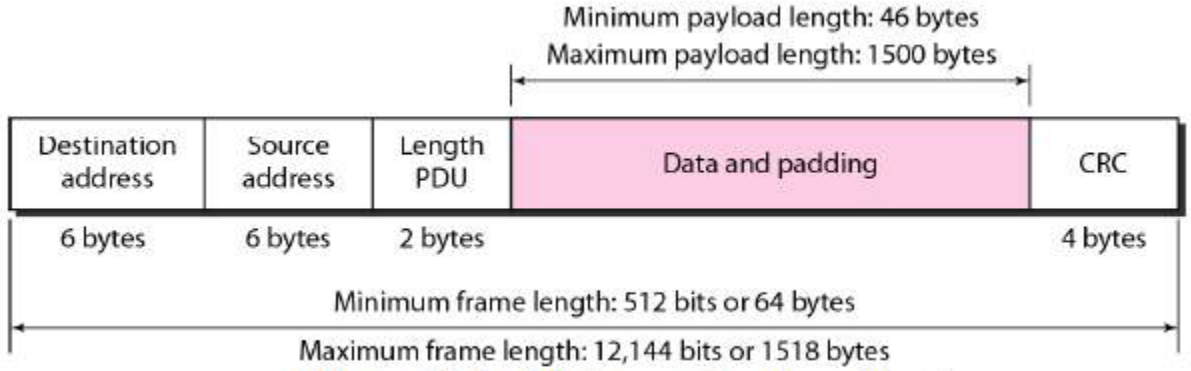


Figure 13.5 *Minimum and maximum lengths*

The minimum length restriction is required for the correct operation of CSMA/CD.

• Minimum length of frame = 64 bytes.

1) Minimum data size = 46 bytes.

2) Header size + Trailer size = 14 + 4 = 18 bytes. (i.e. 18 bytes = 6 bytes source-address + 6 bytes dest-address + 2 bytes length + 4 bytes CRC).

• The minimum length of data from the upper layer = 46 bytes.

• If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

• Maximum length of frame =1518 bytes.

1) Maximum data size = 1500 bytes.

2) Header size + trailer size = 14 + 4 = 18 bytes.

• The maximum length restriction has 2 reasons:

1) Memory was very expensive when Ethernet was designed. A maximum length restriction helped to reduce the size of the buffer.

2) This restriction prevents one station from

→ monopolizing the shared medium

→ blocking other stations that have data to send.

Addressing

• In an Ethernet-network, each station has its own NIC (6-byte =48 bits).

• The NIC provides the station with a 6-byte physical-address (or Ethernet-address).

• For example, the following shows an Ethernet MAC address:

06:01 :02:01:2C:4B

6 bytes = 12 hex digits = 48 bits

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

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

Hexadecimal	47	20	1B	2E	08	EE
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Unicast, Multicast, and Broadcast Addresses

A source-address is always a unicast address i.e. the frame comes from only one station.

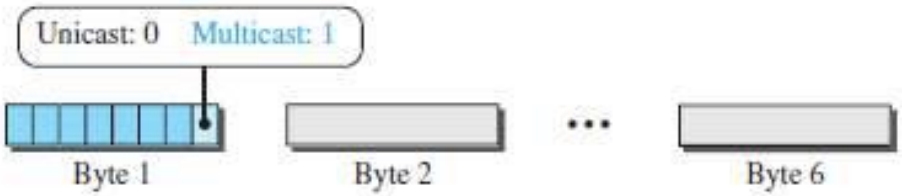


Figure 13.4 *Unicast and multicast addresses*

However, the destination-address can be 1) Unicast 2) Multicast or 3) Broadcast.

• As shown in Figure 13.4,

If LSB of first byte in a destination-address is 0,

Then, the address is unicast;

Otherwise, the address is multicast.

1) A unicast destination-address defines only one recipient.

¤ The relationship between the sender and the receiver is one-to-one.

2) A multicast destination-address defines a group of addresses.

¤ The relationship between the sender and the receivers is one-to-many.

3) 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 48 1s (6-byte =48 bits).

• Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star

topology) (Figure 13.5).

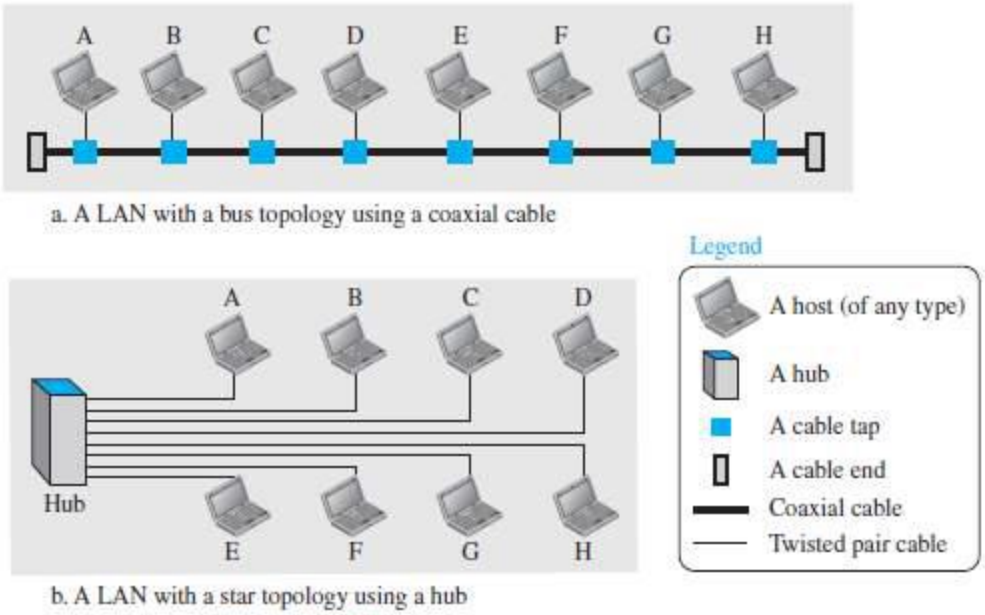


Figure 13.5 *Implementation of standard Ethernet*

How actual unicast, multicast & broadcast transmissions are distinguished from each other?

Answer: The way the frames are kept or dropped.

1) In a unicast transmission, all stations will receive the frame, the intended recipient keeps and handles the frame; the rest discard it.

2) 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.

3) In a broadcast transmission, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

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 Fs, 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 Fs in hexadecimal.

Access-method

• Standard-Ethernet uses 1-persistent CSMA/CD.

1) Slot Time

Slot time = round-trip time + time required to send the jam sequence.

• The RTT means time required for a frame to travel from one end of a maximum-length network to the other end (RTT →Round-Trip Time).

• The slot time is defined in bits.

• The slot time is the time required for a station to send 512 bits.

• The actual slot time depends on the data-rate.

For example: 10-Mbps Ethernet has slot time of 51.2 μs.

2) Slot Time and Collision

• The choice of a 512-bit slot time was not accidental.

• It was chosen to allow the proper functioning of CSMA/CD.

3) Slot Time and Maximum Network Length

• There is a relationship between

→ slot time and

→ maximum length of the network (collision domain).

• This relationship is dependent on the propagation-speed of the signal in the particular medium.

i) In most transmission media, the signal propagates at $2x10^8$ m/s (two-thirds of the rate for propagation in air).

ii) For traditional Ethernet, we calculate

$$\text{MaxLength} = \text{PropagationSpeed} \times \frac{\text{SlotTime}}{2}$$

MaxLength= (2 x 108) x $(51.2 \text{ X } 10^{-6})/2$= 5120m

Efficiency of Standard Ethernet

• The efficiency 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.

• The practical efficiency of standard Ethernet has been measured to be

$$\text{Efficiency} = 1 / (1 + 6.4 \times a)$$

where a = number of frames that can fit on the medium.

a = (propagation delay)/(transmission delay)

• As the value of parameter a decreases, the efficiency increases.

• If the length of the media is shorter or the frame size longer, the efficiency increases.

• In the ideal case, a = 0 and the efficiency is 1.

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%**

Implementation

• The Standard-Ethernet defines several physical-layer implementations (Table 13.1).

Table 13.1 *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

Encoding and Decoding

• All standard implementations use digital-signaling (baseband) at 10 Mbps (Figure 13.6).

1) At the sender, data are converted to a digital-signal using the Manchester scheme.

2) At the receiver, the received-signal is

→ interpreted as Manchester and

→ decoded into data.

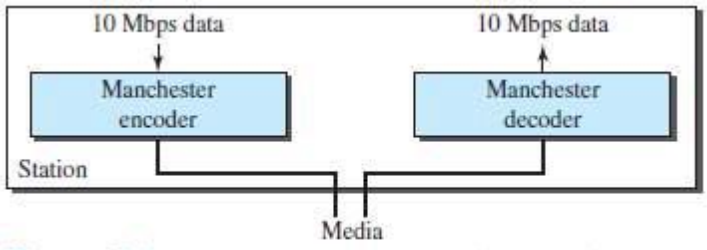


Figure 13.6 *Encoding in a Standard Ethernet implementation*

1) 10Base5: Thick Ethernet

- 10Base5 uses a bus topology (Figure 13.7).
- A external transceiver is connected to a thick coaxial-cable.(transceiver = transmitter/receiver)
- The transceiver is responsible for

  → transmitting

→ receiving and

→ detecting collisions.

- The transceiver is connected to the station via a coaxial-cable.

The cable provides separate paths for sending and receiving.

The collision can only happen in the coaxial cable.

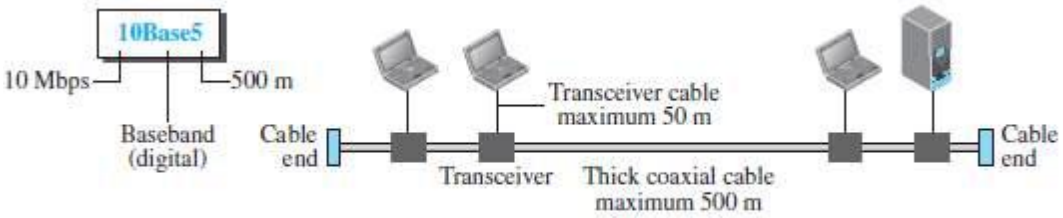


Figure 13.7 *10Base5 implementation*

- The maximum-length of the cable must not exceed 500m. If maximum-length is exceeded, then there will be excessive degradation of the signal.
- If a cable-length of more than 500 m is needed, the total cable-length can be divided into up to 5 segments.
- Each segment of maximum length 500-meter, can be connected using repeaters.

2) 10Base2: Thin Ethernet

- 10Base2 uses a bus topology (Figure 13.8).
- The cable is much thinner and more flexible than 10Base5.
- Flexible means the cable can be bent to pass very close to the stations.
- The transceiver is part of the NIC, which is installed inside the station.
- The collision can only happen in the coaxial cable.

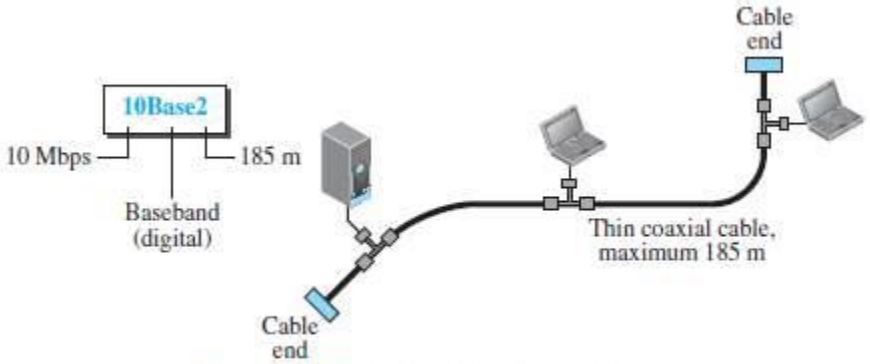


Figure 13.8 *10Base2 implementation*

Advantages:

1) Thin coaxial-cable is less expensive than thick coaxial-cable.

2) Tee connections are much cheaper than taps.

3) Installation is simpler because the thin coaxial cable is very flexible.

Disadvantage:

1) Length of each segment cannot exceed 185m due to the high attenuation in the cable.

3)10Base- T: Twisted-Pair Ethernet

- 10Base-T uses a star topology to connect stations to a hub (Figure 13.9).
- The stations are connected to a hub using two pairs of twisted-cable.

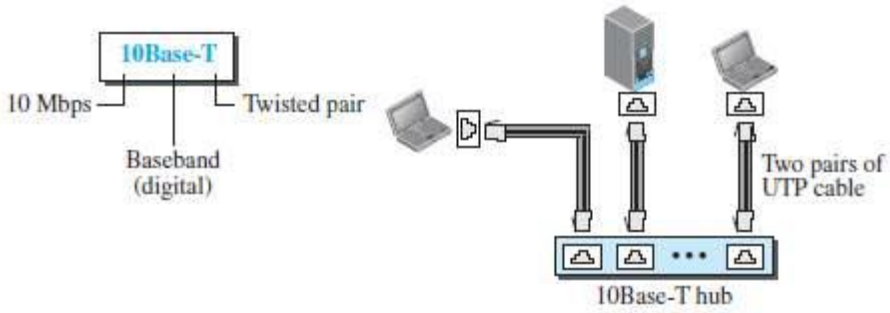


Figure 13.9 *10Base-T implementation*

- Two pairs of twisted cable create two paths between the station and the hub.
  1) First path for sending.
  2) Second path for receiving.
- The collision can happen in the hub.
- The maximum length of the cable is 100 m. This minimizes the effect of attenuation in the cable.

4) 10Base-F: Fiber Ethernet

- 10Base-F uses a star topology to connect stations to a hub (Figure 13.10).
- The stations are connected to the hub using two fiber-optic cables.

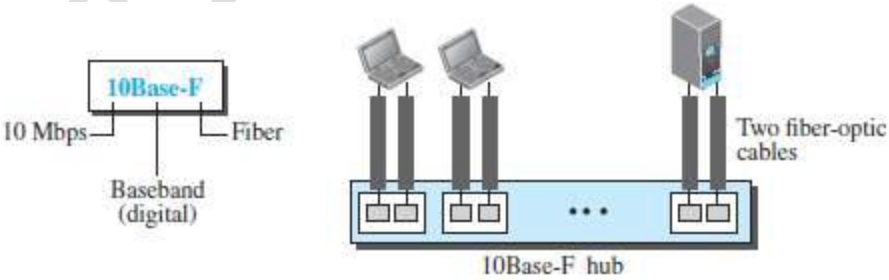


Figure 13.10 *10Base-F implementation*

Changes in the Standard

Bridged Ethernet

• Bridges have two effects on an Ethernet LAN:

i) They raise the bandwidth &

ii) They separate collision domains.

1) Raising the Bandwidth

• A bridge divides the network into two or more networks.

• Bandwidth-wise, each network is independent.

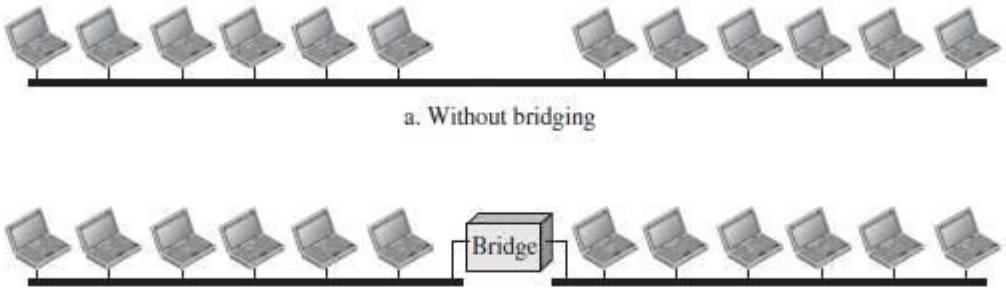


Figure 13.12 *A network with and without a bridge*

For example (Figure 13.12):

- 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 (actually 7 because the bridge acts as a station in each segment), not 12 stations.
- In a network with a heavy load, each station theoretically is offered 10/7 Mbps instead of 10/12 Mbps.

2) Separating Collision Domains

• Another advantage of a bridge is the separation of the collision domain.

• Figure 13.13 shows the collision domains for an un-bridged and a bridged network.

• You can see that the collision domain becomes much smaller and the probability of collision is reduced tremendously.

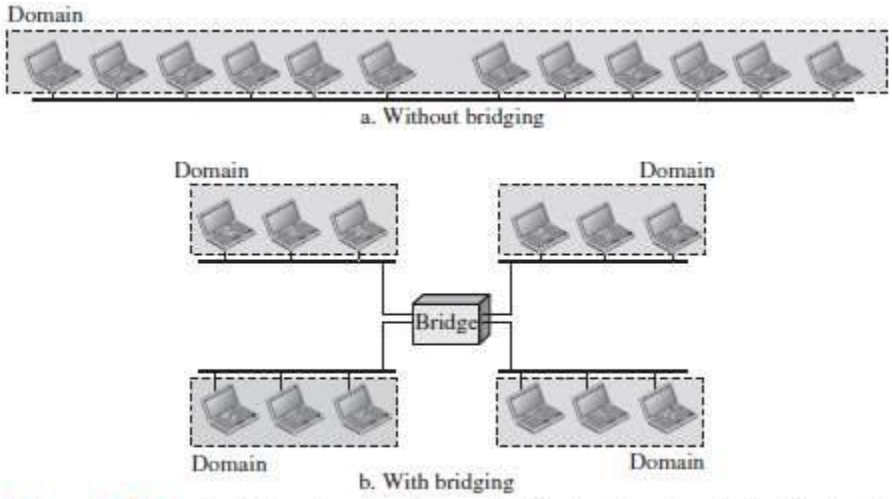


Figure 13.13 *Collision domains in an unbridged network and a bridged network*

Switched Ethernet

• The idea of a bridged LAN can be extended to a switched LAN (Figure 13.14).

• If we can have a multiple-port bridge, we can have an N-port switch.

• In this way, the bandwidth is shared only between the station and the switch.

• A layer-2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.

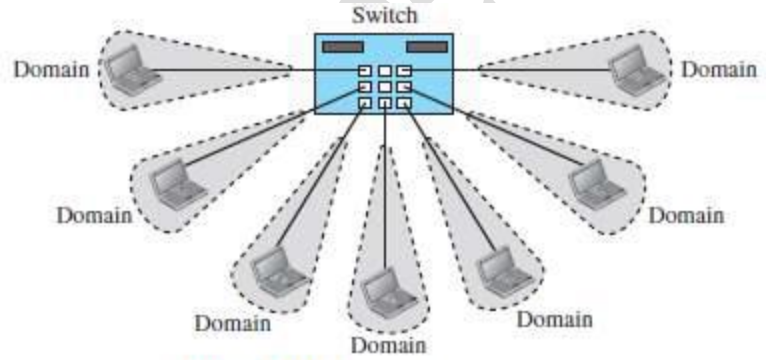


Figure 13.14 *Switched Ethernet*

Full-Duplex Ethernet

• The full-duplex mode increases the capacity of each domain from 10 to 20 Mbps.

• Instead of using one link between the station and the switch, the configuration uses two links: one to transmit and one to receive.

1) No Need for CSMA/CD

- In full-duplex switched Ethernet, There is no need for the CSMA/CD method.
- 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.
- Carrier sensing and collision-detection functionalities of the MAC sublayer can be turned off.

2) MAC Control Layer

- 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 (100 MBPS)

• IEEE created Fast-Ethernet under the name 802.3u.

• Fast-Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.

• Goals of Fast-Ethernet:

1) Upgrade the data-rate to 100 Mbps.

2) Make it compatible with Standard-Ethernet.

3) Keep the same 48-bit address.

4) Keep the same frame format.

5) Keep the same minimum and maximum frame-lengths.

Access Method

• Access method is same in Standard-Ethernet.

• Only the star topology is used.

• For the star topology, there are 2 choices:

1) In the half-duplex approach, the stations are connected via a hub. CSMA/CD was used as access-method.

2) In the full-duplex approach, the connection is made via a switch with buffers at each port.

There is no need for CSMA/CD.

Autonegotiation

- A new feature added to Fast-Ethernet is called autonegotiation.
- It provides a station/hub with a range of capabilities.
- It was used for the following purposes:

1) To allow 2 devices to negotiate the mode or data-rate of operation.

2) To allow incompatible devices to connect to one another.

For example: a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity.

3) To allow one device to have multiple capabilities.

4) 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 of the features of this layer are as follows. 1) Topology 2) Implementation and 3) Encoding.

Topology

• Fast-Ethernet is used to connect two or more stations together (Figure 13.19).

1) If there are only 2 stations, they can be connected in point-to-point.

2) If there are 3 or more stations, they can be connected in star topology with a hub at the center.

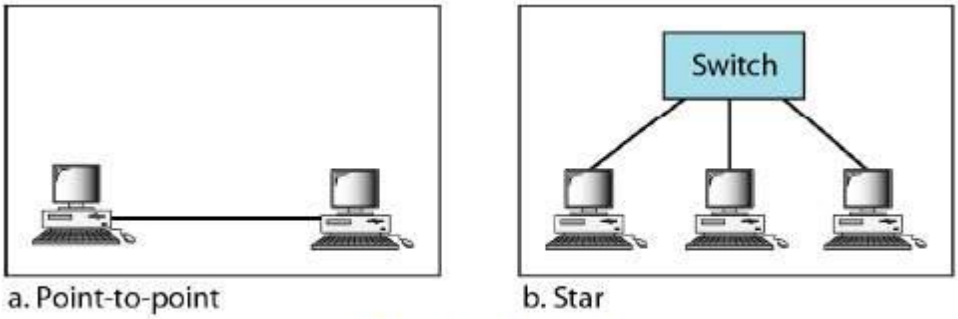


Figure 13.19 *Fast Ethernet topology*

Implementation

• Fast-Ethernet can be classified as either a two-wire or a four-wire implementation (Table 13.2).

1) The 2-wire implementations use
   → Category 5 UTP (100Base-TX) or
   → Fiber-optic cable (100Base-FX)
2) The 4-wire implementations use category 3 UTP (100Base-T4).

Table 13.2 *Summary of Fast Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	UTP or STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

Encoding

• There are 3 different encoding schemes.

1) 100Base-TX

- This uses 2 pairs of twisted-pair cable (either category 5 UTP or STP) (Figure 13.16a).

- The MLT-3 encoding scheme is used for implementation. This is because MLT-3 has good bandwidth performance.
- However, 4B/5B block-coding is used to provide bit synchronization. This is because MLT-3 is not a self-synchronous line coding scheme.
- 4B/5B coding creates a data-rate of 125 Mbps, which is fed into MLT-3 for encoding.

2) 100Base-FX

- This uses 2 pairs of fiber-optic cables (Figure 13.16b).
- Optical fiber can easily handle high bandwidth requirements.
- The NRZ-I encoding scheme is used for implementation.
- However, 4B/5B block-coding is used to provide bit synchronization. This is because NRZ-I is not a self-synchronous line coding scheme.
- 4B/5B encoding increases the bit rate from 100 to 125 Mbps, which can easily be handled by fiber-optic cable.

3) 100Base-T4

- This uses 4 pairs of UTP for transmitting 100 Mbps (Figure 13.16c).
- Each UTP cannot easily handle more than 25 Mbaud.
- One pair switches between sending and receiving.
- Three pairs of UTP can handle only 75 Mbaud (25 Mbaud) each.
- Encoding/decoding is more complicated.
- We need an encoding scheme that converts 100 Mbps to a 75 Mbaud signal. This requirement is satisfied by 8B/6T.
- The 8B/6T encoding scheme is used for implementation.

i) 8 data elements are encoded as 6 signal elements.

ii) This means that 100 Mbps uses only (6/8) x 100 Mbps, or 75 Mbaud.

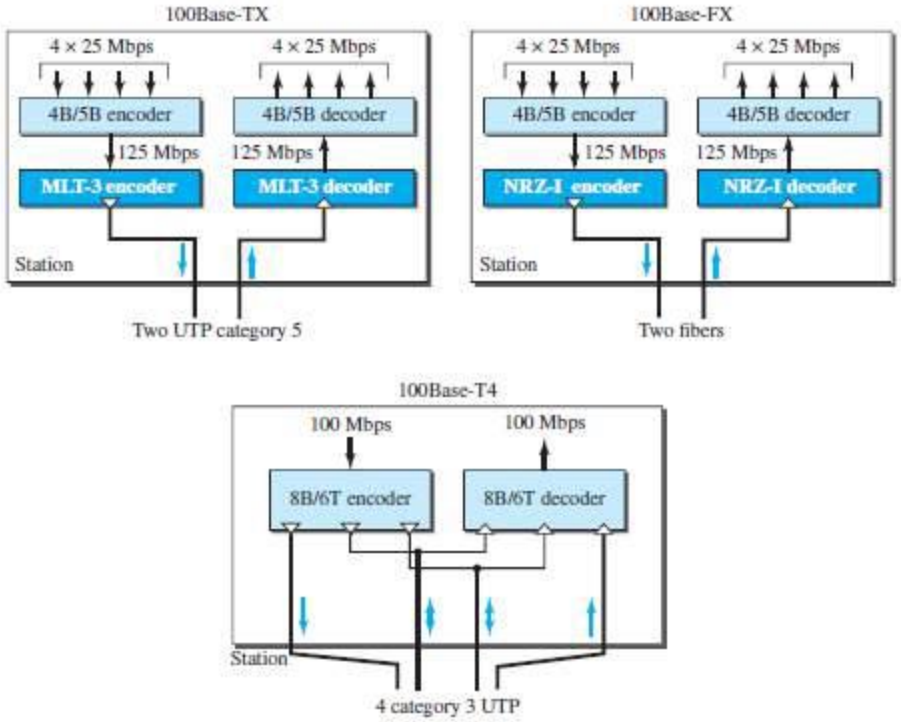


Figure 13.16 *Encoding for Fast Ethernet implementation*

GIGABIT ETHERNET

• IEEE created Gigabit-Ethernet under the name 802.3z.

• Goals of Gigabit-Ethernet:

1) Upgrade the data-rate to 1 Gbps.

2) Make it compatible with Standard or Fast-Ethernet.

3) Use the same 48-bit address.

4) Use the same frame format.

5) Keep the same minimum and maximum frame-lengths.

6) To support auto-negotiation as defined in Fast-Ethernet.

MAC Sublayer

• Gigabit-Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex.

• Almost all implementations of Gigabit-Ethernet follow the full-duplex approach.

1) Full-Duplex Mode

• There is a central switch connected to all computers or other switches.

• Each switch has buffers for each input-port in which data are stored until they are transmitted.

• There is no collision. This means that CSMA/CD is not used.

• Lack of collision implies that the maximum length of the cable is determined

→ by the signal attenuation in the cable &

→ not by the collision-detection process.

2) Half-Duplex Mode

• A switch is replaced by a hub, which acts as the common cable in which a collision might occur.

• CSMA/CD is used.

• The maximum length of the network is totally dependent on the minimum frame size.

• Three methods have been defined: traditional, carder extension, and frame bursting.

i) Traditional

Like traditional Ethernet, the minimum length of a frame is 512 bits.

However, because the length of a bit is 1/100 shorter,

Slot time is 512 bits x 1/1000 gs which is equal to 0.512 gs.

- 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.

ii) Carrier Extension

- To allow for a longer network, we increase the minimum frame-length.
- Minimum length of frame is 512 bytes (4096 bits). Thus, minimum length is 8 times longer.
- A station adds extension bits (padding) to any frame that is less than 4096 bits.
- The maximum length of the network is 200 m.
- A length from the hub to the station is 100 m.

iii) Frame Bursting

- Carrier extension is very inefficient if

  → we have a series of short frames to send

  → each frame carries redundant data.
- To improve efficiency, frame bursting was proposed.
- Instead of adding an extension to each frame, multiple frames are sent.
- However, to make these multiple frames look like one frame, padding is added between the frames. Thus, the channel is not idle.

Physical-layer

• The physical-layer in Gigabit-Ethernet is more complicated than that in Standard or Fast-Ethernet.

• Some of the features of this layer are as follows. 1) Topology 2) Implementation and 3) Encoding.

Topology

• Gigabit-Ethernet is used to connect two or more stations together.

1) If there are only 2 stations, they can be connected in point-to-point.

2) If there are 3 or more stations, they can be connected in star topology with a hub at center.

Implementation

• Gigabit-Ethernet can be classified as either a two-wire or a four-wire implementation (Table 13.3).

1) The 2-wire implementations use

→ Fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave) or

→ STP (1000Base-CX)

The 4-wire implementations use category 5 twisted-pair cable (1000Base-T).

Table 13.3 *Summary of Gigabit Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

Encoding

1) Two-wire Implementation

• The NRZ encoding scheme is used for two-wire implementation (Figure 13.17a).

• However, 8B/10B block-coding is used to provide bit synchronization. This is because NRZ is not a self-synchronous line coding scheme.

• 8B/10B coding creates a data-rate of 1.25 Gbps.

• One wire (fiber or STP) is used for sending. Another wire is used for receiving.

2) Four-wire Implementation

• In this, it is not possible to have 2 wires for input and 2 for output (Figure 13.17b).

• This is „.“ each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP.

• As a solution, 4D-PAM5 encoding is used to reduce the bandwidth.

• Thus, 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.

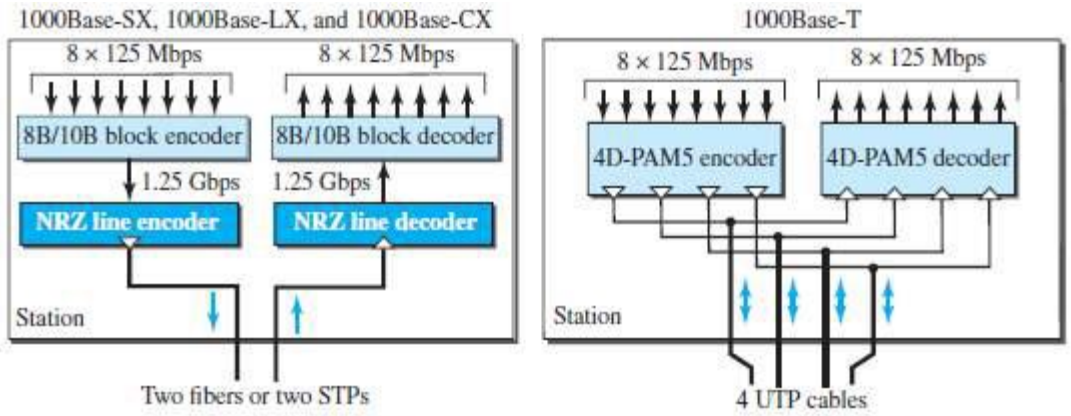


Figure 13.17 *Encoding in Gigabit Ethernet implementations*

TEN GIGABIT ETHERNET

• IEEE created Ten-Gigabit-Ethernet under the name 802.3ae.

• Goals of the Gigabit-Ethernet:

1) Upgrade the data-rate to 10 Gbps.

2) Make it compatible with Standard, Fast, and Gigabit-Ethernet.

3) Use the same 48-bit address.

4) Use the same frame format.

5) Keep the same minimum and maximum frame-lengths.

6) Allow the interconnection of existing LANs into a MAN or a WAN .

7) Make Ethernet compatible with technologies such as Frame Relay and ATM.

Implementation

• Ten-Gigabit-Ethernet operates only in full duplex mode.

• This means there is no need for contention; CSMA/CD is not used.

• Four implementations are the most common (Table 13.4):

1) 10GBase-SR

2) 10GBase-LR

3) 10GBase-EW and

4) 10GBase-X4

Table 13.4 *Summary of 10 Gigabit Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

WIRELESS LANs

Introduction of Wireless-LANs

Architectural Comparison

1) Medium

• In a wired LAN, we use wires to connect hosts.

• In a switched LAN, with a link-layer switch, the communication between the hosts is point-to-point and full-duplex (bidirectional).

• In a wireless LAN, the medium is air, the signal is generally broadcast.

• When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple accesses).

2) Hosts

• In a wired LAN, a host is always connected to its network at a point with a fixed link layer address related to its network interface card (NIC).

• Of course, a host can move from one point in the Internet to another point.

• In this case, its link-layer address remains the same, but its network-layer address will change.

• In a wireless LAN, a host is not physically connected to the network; it can move freely and can use the services provided by the network.

• Therefore, mobility in a wired network and wireless network are totally different issues.

3) Isolated LANs

• A wired isolated LAN is a set of hosts connected via a link-layer switch (Figure 15.1).

• A wireless isolated LAN, called an ad hoc network in wireless LAN terminology, is a set of hosts that communicate freely with each other.

• The concept of a link-layer switch does not exist in wireless LANs.

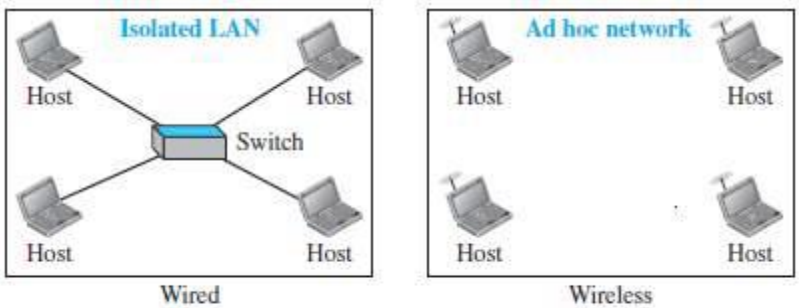


Figure 15.1 *Isolated LANs: wired versus wireless*

4) Connection to Other Networks

• A wired LAN can be connected to another network or the Internet using a router.

• A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN (Figure 15.2).

• In this case, the wireless LAN is referred to as an infrastructure network, and the connection to the wired infrastructure, such as the Internet, is done via a device called an access point (AP).

• An access point is gluing two different environments together: one wired and one wireless.

1) Communication between the AP and the wireless host occurs in a wireless environment.

2) Communication between the AP and the infrastructure occurs in a wired environment.

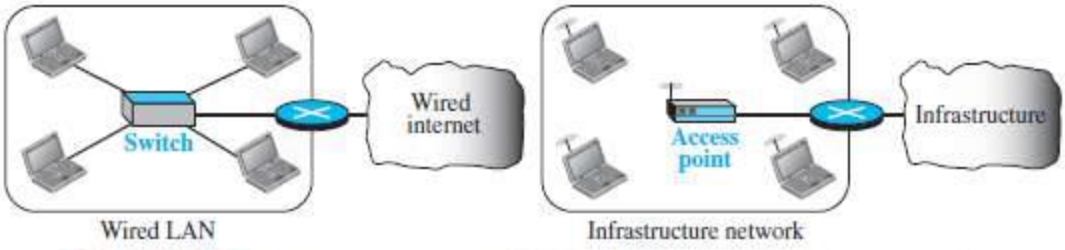


Figure 15.2 *Connection of a wired LAN and a wireless LAN to other networks*

Characteristics

1) Attenuation

• The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver.

• The situation becomes worse with mobile senders that operate on batteries and normally have small power supplies.

2) Interference

• Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.

3) Multipath Propagation

• A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects.

• The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.

4) Error

• Error detection is more serious issues in a wireless network than in a wired network.

i) If SNR is high, it means that the signal is stronger than the noise (unwanted signal), so we may be able to convert the signal to actual data.

ii) When SNR is low, it means that the signal is corrupted by the noise and the data cannot be recovered.

Access Control

• The CSMA/CD algorithm does not work in wireless LANs for three reasons:

1) To detect a collision, a host needs to send and receive at the same time which means the host needs to work in a duplex mode. Wireless hosts do not have enough power to do so (the power is supplied by batteries).

¤ They can only send or receive at one time.

2) The distance between stations can be great.

¤ Signal fading could prevent a station at one end from hearing a collision at other end.

3) Because of the hidden station problem, in which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected.

Hidden station problem

¤ Figure 15.3 shows an example of the hidden station problem.

¤ Every station in transmission range of Station B can hear any signal transmitted by station B.

¤ Every station in transmission range of Station C can hear any signal transmitted by station C.

¤ Station C is outside the transmission range of B;

Likewise, station B is outside the transmission range of C.

¤ However, Station A is in the area covered by both B and C;

Therefore, Station A can hear any signal transmitted by B or C.

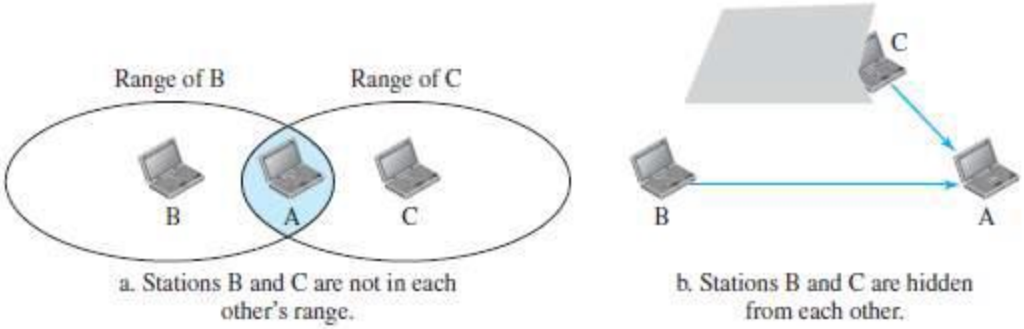


Figure 15.3 *Hidden station problem*

IEEE 802.11

Architecture

• The standard defines 2 kinds of services:

1) Basic service set (BSS) and

2) Extended service set (ESS).

Basic service set (BSS)

• IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless-LAN.

• A basic service set is made of (Figure 15.4):

→ stationary or mobile wireless stations and

→ optional central base station, known as the access point (AP).

• There are 2 types of architecture:

1) Ad hoc Architecture

- The BSS without an AP is a stand-alone network and cannot send data to other BSSs.
- Stations can form a network without the need of an AP.
- Stations can locate one another and agree to be part of a BSS.

2) Infrastructure Network

- A BSS with an AP is referred to as an infrastructure network.

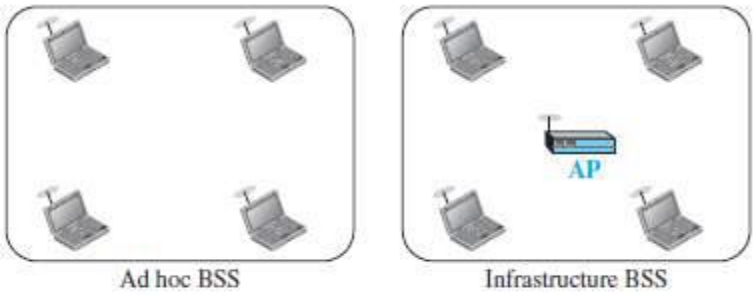


Figure 15.4 *Basic service sets (BSSs)*

Extended service set (ESS)

• The ESS is made up of 2 or more BSSs with APs (Figure 15.5).

• The BSSs are connected through a distribution-system, which is usually a wired LAN.

• The distribution-system connects the APs in the BSSs.

• IEEE 802.11 does not restrict the distribution-system;

The distribution-system can be any IEEE LAN such as an Ethernet.

• The ESS uses 2 types of stations:

1) Mobile stations are normal stations inside a BSS.

2) Stationary stations are AP stations that are part of a wired LAN.

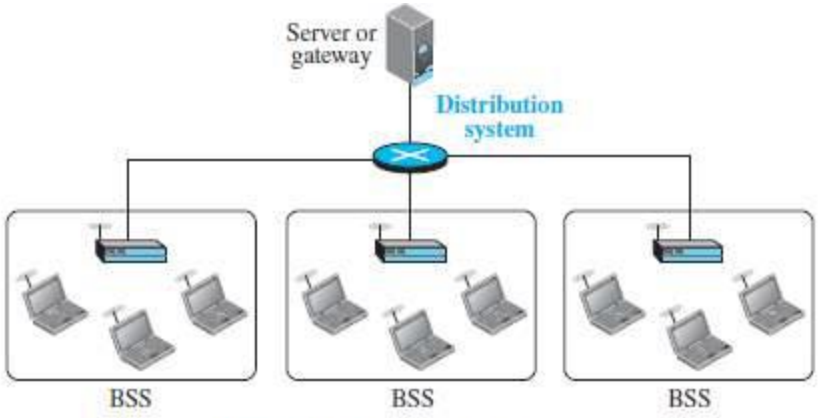


Figure 15.5 *Extended service set (ESS)*

• When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.

• However, communication between two stations in two different BSSs usually occurs via two APs.

Station Types

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

1) No-transition

2) BSS-transition

3) ESS-transition mobility

1) A station with no-transition mobility is either

→ stationary (not moving) or

→ moving only inside a BSS.

2) A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.

3) A station with ESS-transition mobility can move from one ESS to another.

However, IEEE 802.11 does not guarantee that communication is continuous during the move.

MAC Sublayer

• IEEE 802.11 defines 2 MAC sublayers:

1) Distributed coordination function (DCF) &

2) Point coordination function (PCF).

• The figure 15.6 shows the relationship between

1) Two MAC sublayers

2) LLC sublayer &

3) Physical layer.

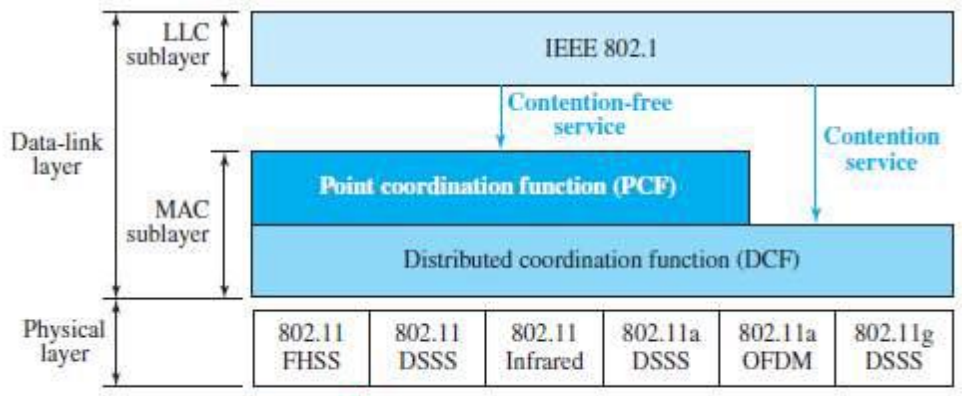


Figure 15.6 *MAC layers in IEEE 802.11 standard*

DCF

• One of the 2 protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF).

• DCF uses CSMA/CA as the access method.

• Wireless-LANs cannot implement CSMA/CD for 3 reasons:

1) For collision-detection, a station must be able to send data & receive collision-signals at the same time. This can mean costly stations and increased bandwidth requirements.

2) Collision may not be detected because of the hidden station problem.

3) The distance between stations can be great.

Signal fading could prevent a station at one end from hearing a collision at the other end.

• Process Flowchart: Figure 15.7 shows the process flowchart for CSMA/CA as used in wireless-LANs.

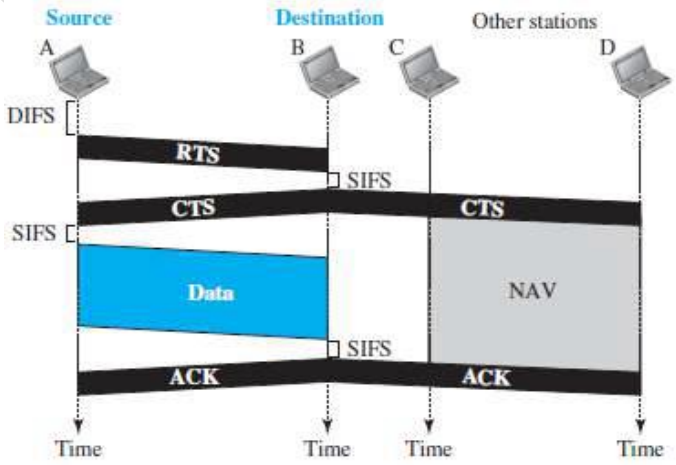


Figure 15.7 *CSMA/CA and NAV*

1) Before sending a frame, the source-station senses the medium by checking the energy-level at the carrier-frequency.

i) The channel uses a persistence strategy with back-off until the channel is idle.

ii) After the station is found to be idle,

→ the station waits for a period of time called the DIFS.

→ then the station sends a control frame called the RTS.

2) After receiving the RTS and waiting a period of time called the SIFS, the destination-station sends a control frame, called the CTS, to the source-station.

CTS frame indicate 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.

(DIFS → Distributed Inter Frame Space, SIFS→ Short Inter Frame Space)

(RTS → Request To Send, CTS → Clear To Send)

Network Allocation Vector

• When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel (NAV→ Network Allocation Vector).

• The stations that are affected by this transmission create a timer called a NAV.

• NAV shows how much time must pass before these stations are allowed to check the channel for idleness.

• Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

• In other words, each station, before sensing the medium to see if it is idle, first checks its NAV to see if it has expired.

Collision During Handshaking

• Two or more stations may try to send RTS frames at the same time.

• These control frames may collide.

• However, because there is no mechanism for collision-detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver.

• The back-off strategy is employed, and the sender tries again.

PCF

• The PCF is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network) (PCF → Point Coordination Function).

• The PCF is implemented on top of the DCF.

• The PCF is used mostly for time-sensitive transmission.

• PCF has a centralized, contention-free polling access method.

• The AP performs polling for stations that are capable of being polled.

• The stations are polled one after another, sending any data they have to the AP.

• To give priority to PCF over DCF, another set of inter-frame spaces has been defined: PIFS and SIFS.

1) The SIFS is the same as that in DCF &

2) PIFS (PCF IFS) is shorter than the DIFS.

• This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.

• Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium.

• To prevent this, a repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic.

• The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame.

• When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval.

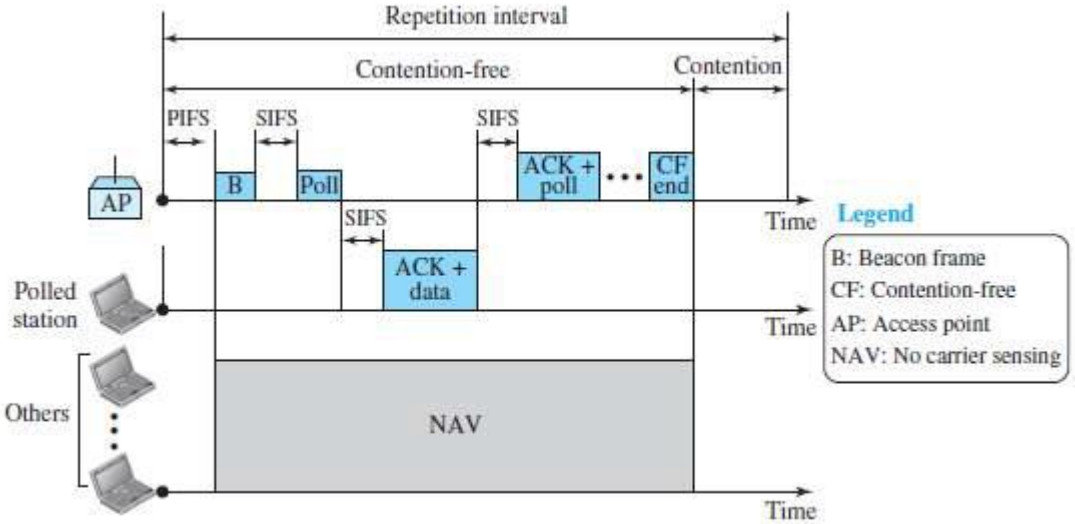


Figure 15.8 *Example of repetition interval*

• During the repetition interval, the PC (point controller) can send a poll frame, receive data, send an ACK, receive an ACK, or do any combination of these (802.11 uses piggybacking).

• At the end of the contention-free period, the PC sends a CF end (contention-free end) frame to allow the contention-based stations to use the medium.

Fragmentation

• The wireless environment is very noisy; a corrupt frame has to be retransmitted.

• The protocol, therefore, recommends fragmentation--the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.

Frame Format

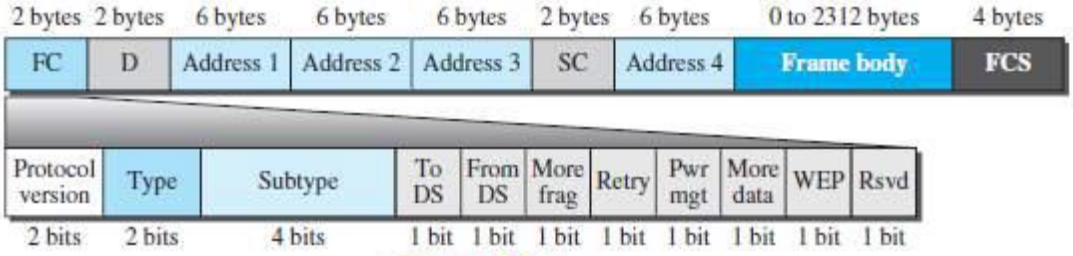


Figure 15.9 *Frame format*

The MAC layer frame consists of nine fields (Figure 15.9):

1) Frame control (FC)

- The FC field is 2 bytes long and defines the type of frame and some control information. The table describes the subfields.

Table 15.1 *Subfields in FC field*

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 15.2)
To DS	Defined later
From DS	Defined later
More frag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

2) D

- In all frame types except one, this field defines the duration of the transmission that is used to set the value of NAV.
- In one control frame, this field defines the ID of the frame.

3) Addresses

- There are four address fields, each 6 bytes long.
- The meaning of each address field depends on the value of the ToDS and FromDS subfields.

4) Sequence control

- This field defines the sequence number of the frame to be used in flow control.

5) Frame body

- This field contains information based on the type and the subtype defined in the FC field.
- This field can be between 0 and 2312 bytes,

6) FCS

- The FCS contains a CRC-32 error detection sequence.

Frame Types

• A wireless-LAN defined by IEEE 802.11 has three categories of frames:

1. Management Frames,
2. Control Frames, and
3. Data-frames.

1) Management Frames

- Management frames are used for the initial communication between stations and access points.

2) Control Frames

- Control frames are used for accessing the channel and acknowledging frames (Figure 15.10).

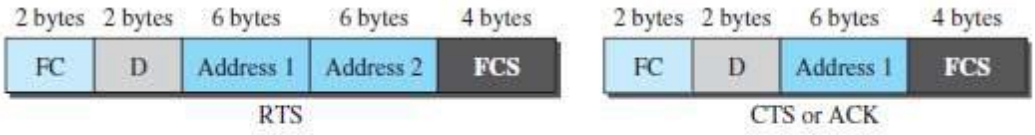


Figure 15.10 *Control frames*

For control frames the value of the type field is 01; the values of the subtype fields for frames are shown in the table 14.2.

Table 15.2 *Values of subtype fields in control frames*

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

3) Data-frames

- Data-frames are used for carrying data and control information.

Addressing Mechanism

• The IEEE 802.11 addressing mechanism specifies 4 cases, defined by the value of the 2 flags in the FC field, To DS and From DS.

• Each flag can be either 0 or 1, resulting in 4 different situations.

• The interpretation of the 4 addresses (address 1 to address 4) in the MAC frame depends on the value of these flags, as shown in the Table 15.3.

Table 15.3 *Addresses*

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

• Address 1 is always the address of the next device.

• Address 2 is always the address of the previous device.

• Address 3 is the address of the final destination-station if it is not defined by address 1.

• Address 4 is the address of the original source-station if it is not the same as address 2.

Case-1:00

- In this case, To DS = 0 and From DS = 0 (Figure 15.11a).
- This means that the frame is

→ not going to a distribution-system (To DS = 0) and i

→ not coming from a distribution-system (From DS = 0).

- The frame is going from one station in a BSS to another without passing through the distribution-system.
- The ACK frame should be sent to the original sender.

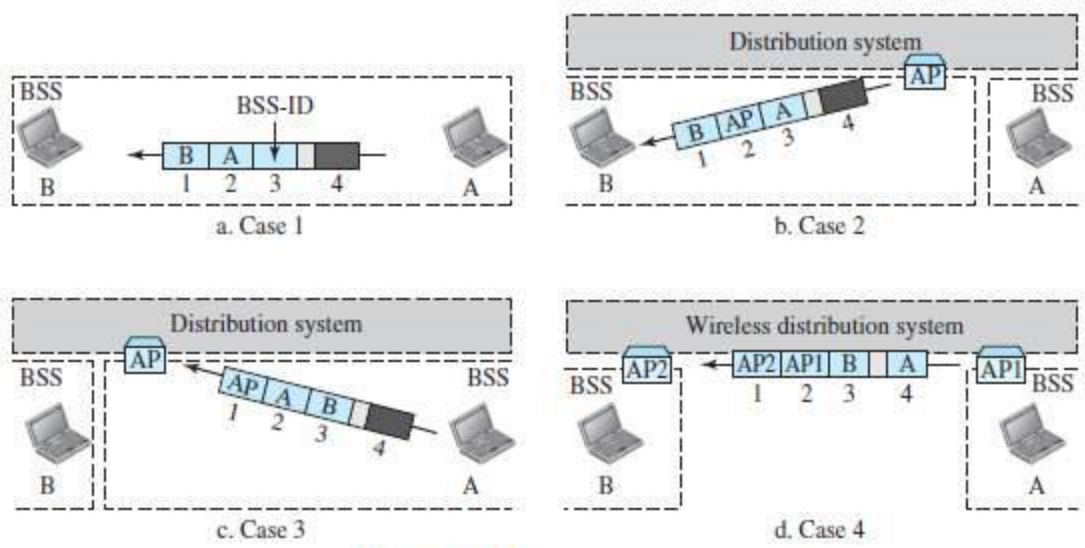


Figure 15.11 *Addressing mechanisms*

Case-2:01

- In this case, To DS = 0 and From DS = 1 (Figure 15.11b).
- This means that the frame is coming from a distribution-system (From DS = 1).
- The frame is coming from an AP and going to a station.
- The ACK should be sent to the AP.
- The address 3 contains the original sender of the frame (in another BSS).

Case-3:10

- In this case, To DS = 1 and From DS = 0 (Figure 15.11c).
- This means that the frame is going to a distribution-system (To DS = 1).
- The frame is going from a station to an AP. The ACK is sent to the original station.
- The address 3 contains the final destination of the frame (in another BSS).

Case-4:11

- In this case, To DS = 1 and From DS = 1 (Figure 15.11d).
- This is the case in which the distribution-system is also wireless.
- The frame is going from one AP to another AP in a wireless distribution-system.
- We do not need to define addresses if the distribution-system is a wired LAN because the frame in these cases has the format of a wired LAN frame (for example: Ethernet,).
- Here, we need four addresses to define

  → original sender

  → final destination, and

  → two intermediate APs.

Exposed Station Problem

• In this problem, a station refrains from using a channel even when the channel is available for use.

• In the figure 14.12, station A is transmitting to station B.

• Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.

• However, station C is exposed to transmission from A i.e. station C hears what A is sending and thus refrains from sending.

• In other words, C is too conservative and wastes the capacity of the channel.

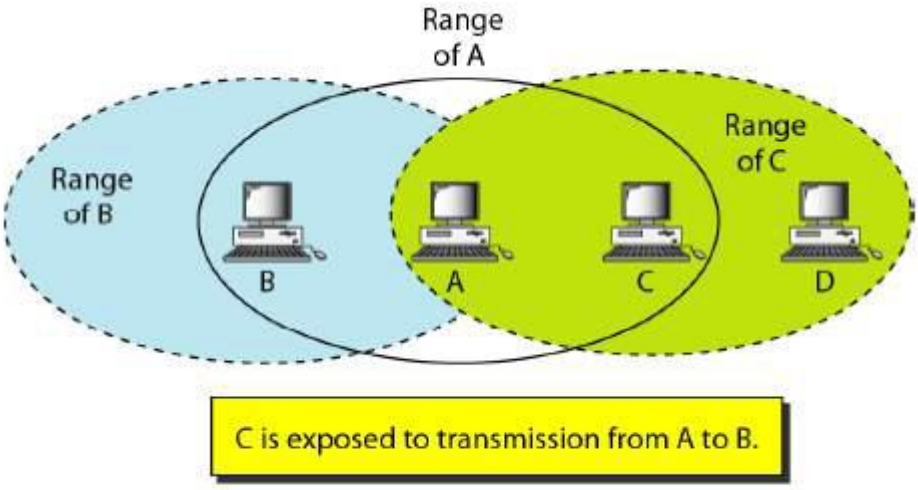


Figure 14.12 *Exposed station problem*

The handshaking messages RTS and CTS cannot help in this case.

• Station C hears the RTS from A, but does not hear the CTS from B.

• Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D.

• Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state.

• However, Station B responds with a CTS.

• The problem is here (Figure 15.12). If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D. It remains exposed until A finishes sending its data as the figure shows.

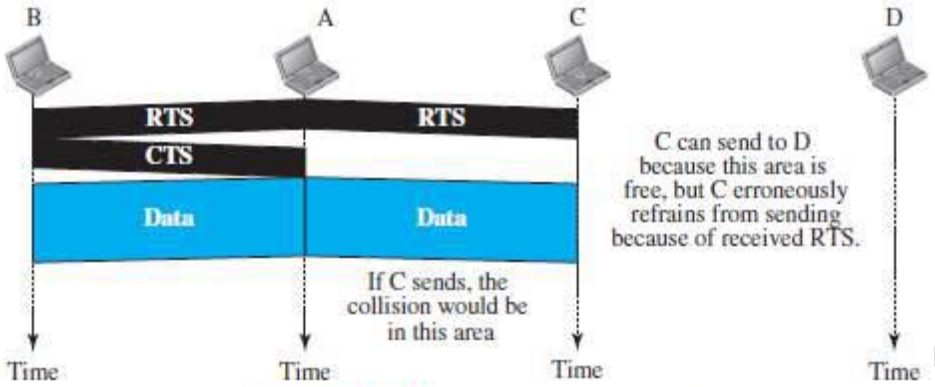


Figure 15.12 *Exposed station problem*

Physical Layer

Table 15.4 *Specifications*

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

• All implementations, except the infrared, operate in the ISM band.

• ISM band defines 3 unlicensed bands in the 3 ranges.

i) 902-928 MHz,

ii) 2.400--4.835 GHz, and

iii) 5.725-5.850 GHz. (ISM → Industrial, Scientific, And Medical)

IEEE 802.11 FHSS

• IEEE 802.11 FHSS uses the FHSS method (Figure 15.13).

• FHSS uses the 2.4-GHz ISM band.

• The band is divided into 79 subbands of 1 MHz (and some guard bands).

• A pseudorandom number generator selects the hopping sequence.

• The modulation technique is either two-level FSK or four-level FSK with 1 or 2 bits/baud.

• This results in a data-rate of 1 or 2 Mbps

(FHSS→ Frequency-Hopping Spread Spectrum DSSS → Direct Sequence Spread Spectrum)

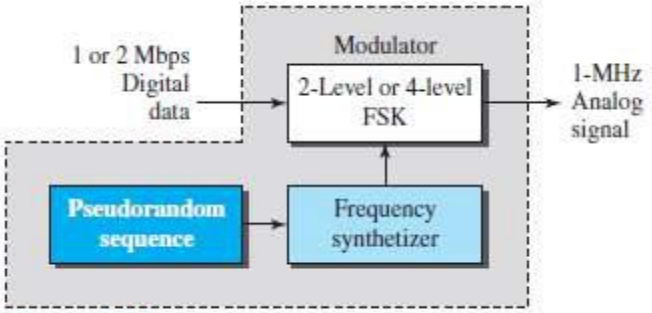


Figure 15.13 *Physical layer of IEEE 802.11 FHSS*

IEEE 802.11 DSSS

• IEEE 802.11 DSSS uses the DSSS method (Figure 15.14).

• DSSS uses the 2.4-GHz ISM band.

• The modulation technique in this specification is PSK at 1 Mbaud/s.

• The system allows 1 or 2 bits/baud (BPSK or QPSK).

  • This results in a data-rate of 1 or 2 Mbps.

Figure 15.14 *Physical layer of IEEE 802.11 DSSS*

(HRDSSS→ High-Rate Direct Sequence Spread Spectrum, CCK → Complementary Code Keying)

(OFDM → Orthogonal Frequency-Division Multiplexing)

802.11 Infrared

• IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm (Figure 15.15).

• The modulation technique is called pulse position modulation (PPM).

• For a 1-Mbps data-rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and the rest are set to 0.

• For a 2-Mbps data-rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bit is set to 1 and the rest are set to 0.

• The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

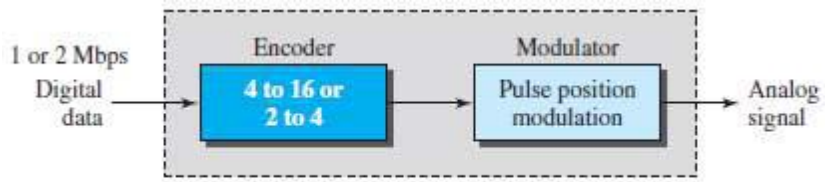


Figure 15.15 *Physical layer of IEEE 802.11 infrared*

IEEE 802.11a OFDM

• IEEE 802.11a OFDM describes the OFDM method for signal generation in a 5-GHz ISM band.

• OFDM is similar to FDM, with 2 major difference:

1) All the subbands are used by one source at a given time.

2) Sources contend with one another at the data-link-layer for access.

• The band is divided into 52 subbands. Out of which,

1) 48 subbands are used for sending 48 groups of bits at a time.

2) 4 subbands are used for sending control information.

• The scheme is similar to ADSL.

• Dividing the band into subbands diminishes the effects of interference.

• If the subbands are used randomly, security can also be increased.

• OFDM uses PSK and QAM for modulation.

• The common data-rates are

i) 18 Mbps (PSK) and ii) 54 Mbps (QAM).

IEEE 802.11b DSSS

• IEEE 802.11 b DSSS describes the HRDSSS method for signal generation in the 2.4-GHz ISM band.

• HR-DSSS is similar to DSSS, with 1 major difference: HR-DSSS uses encoding method called CCK.

• CCK encodes 4 or 8 bits to one CCK symbol (Figure 15.16).

• To be backward compatible with DSSS, HR-DSSS defines 4 data-rates: 1, 2, 5.5, and 11 Mbps.

1) The first two versions (1- & 2-Mbps) use the same modulation techniques as DSSS.

2) The 5.5-Mbps version

→ uses BPSK and

→ transmits at 1.375 Mbaud/s with 4-bit CCK encoding.

3) The 11-Mbps version

→ uses QPSK and

→ transmits at 1.375 Mbps with 8-bit CCK encoding.

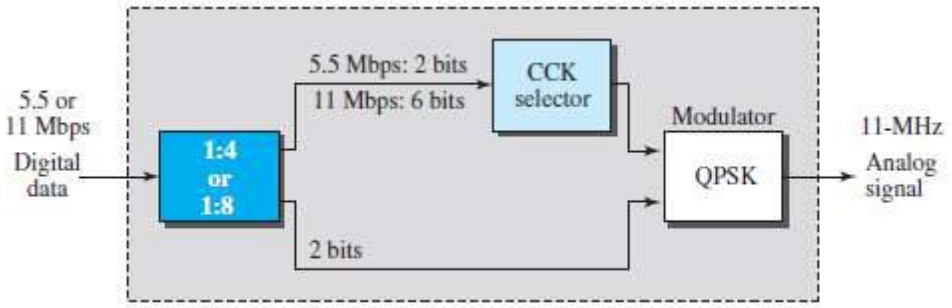


Figure 15.16 *Physical layer of IEEE 802.11b*

IEEE 802.11g

• This new specification defines forward error correction and OFDM using the 2.4-GHz ISM band.

• The modulation technique achieves a 22- or 54-Mbps data-rate.

• It is backward compatible with 802.11b, but the modulation technique is OFDM.

BLUETOOTH

• Bluetooth is a wireless-LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.

• A Bluetooth LAN is an ad hoc network. This means the network is formed spontaneously.

• The devices

→ find each other and

→ make a network called a piconet (Usually, devices are called gadgets)

• A Bluetooth LAN can even be connected to the Internet if one of the devices has this capability.

• By nature, a Bluetooth LAN cannot be large.

• If there are many devices that try to connect, there is confusion.

• Bluetooth technology has several applications.

1) Peripheral devices such as a wireless mouse/keyboard can communicate with the computer.

2) In a small health care center, monitoring-devices can communicate with sensor-devices.

3) Home security devices can connect different sensors to the main security controller.

4) Conference attendees can synchronize their laptop computers at a conference.

• Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.

• The standard defines a wireless PAN operable in an area the size of a room or a hall.

(PAN →Personal-Area Network)

Architecture

• Bluetooth defines 2 types of networks: 1) Piconet and 2) Scatternet.

Piconets

- A Bluetooth network is called a piconet, or a small net. (Figure 15.17).
- A piconet can have up to 8 stations. Out of which

  i) One of station is called the primary.

  ii) The remaining stations are called secondaries.
- All the secondary-stations synchronize their clocks and hopping sequence with the primary station.
- A piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many.

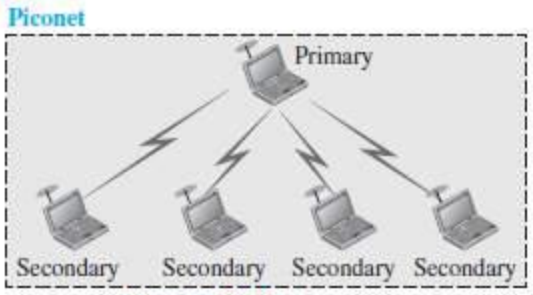


Figure 15.17 *Piconet*

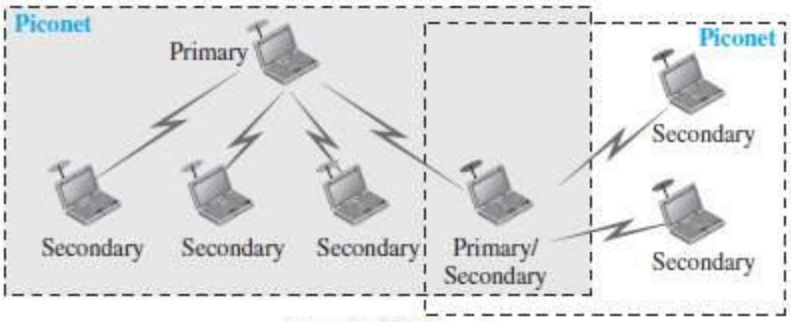


Figure 15.18 *Scatternet*

- Although a piconet can have a maximum of 7 secondaries, an additional 8 secondaries can be in the parked state.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.
- Because only 8 stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Scatternet

- Piconets can be combined to form a scatternet (Figure 15.18).
- A station can be a member of 2 piconets.

- A secondary station in one piconet can be the primary in another piconet. This is called mediator station.

  1) Acting as a secondary, mediator station can receive messages from the primary in the first piconet.

  2) Acting as a primary, mediator station can deliver the message to secondaries in the second piconet.

Bluetooth Devices

• A Bluetooth device has a built-in short-range radio transmitter.

• The current data-rate is 1 Mbps with a 2.4-GHz bandwidth.

• This means that there is a possibility of interference between the IEEE 802.11b wireless-LANs and Bluetooth LANs.

Bluetooth Layers

• Bluetooth uses several layers that do not exactly match those of the Internet model (Figure 15.19).

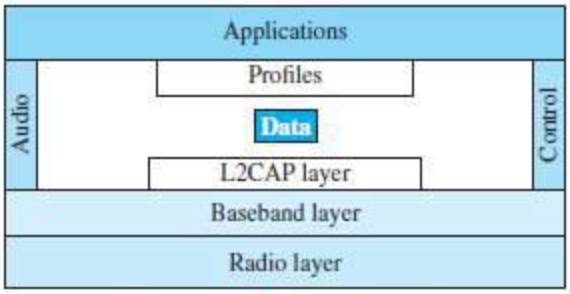


Figure 15.19 *Bluetooth layers*

Radio Layer

• The radio layer is roughly equivalent to the physical layer of the Internet model.

• Bluetooth devices are low-power and have a range of 10 m.

1) Band

- Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

2) FHSS

- Bluetooth uses the Frequency-Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.
- Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second.
- A device uses a frequency for only 625 μs (1/1600 s) before it hops to another frequency; the dwell time is 625 μs.

3) Modulation

- To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering).
- GFSK has a carrier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit 0 is represented by a frequency deviation below the carrier.
- The frequencies, in megahertz, are defined according to the following formula for each channel:

$$f_c = 2402 + n \text{ MHz} \qquad n = 0, 1, 2, 3, \ldots, 78$$

For example,

- The first channel uses carrier frequency 2402 MHz (2.402 GHz).
- The second channel uses carrier frequency 2403 MHz (2.403 GHz).

Baseband Layer

• The baseband layer is roughly equivalent to the MAC sublayer in LANs.

• The access method is TDMA.

• The primary and secondary communicate with each other using time slots.

• The length of a time slot is exactly the same as the dwell time, 625 μs.

• This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary.

• The communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

TDMA

• Bluetooth uses a form of TDMA that is called TDD-TDMA (timedivision duplex TDMA).

• TDD-TDMA is a kind of half-duplex communication in which the secondary and receiver send and receive data, but not at the same time (Halfduplex);

• However, the communication for each direction uses different hops.

• This is similar to walkie-talkies using different carrier frequencies.

Single-Secondary Communication

- If the piconet has only one secondary, the TDMA operation is very simple (Fig 15.21).
- The time is divided into slots of 625 μs.
- The primary uses even numbered slots (0, 2, 4, ...); the secondary uses odd-numbered slots (1, 3, 5,...).
- TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode.
- In slot 0, the primary sends, and the secondary receives; in slot 1, the secondary sends, and the primary receives. The cycle is repeated.

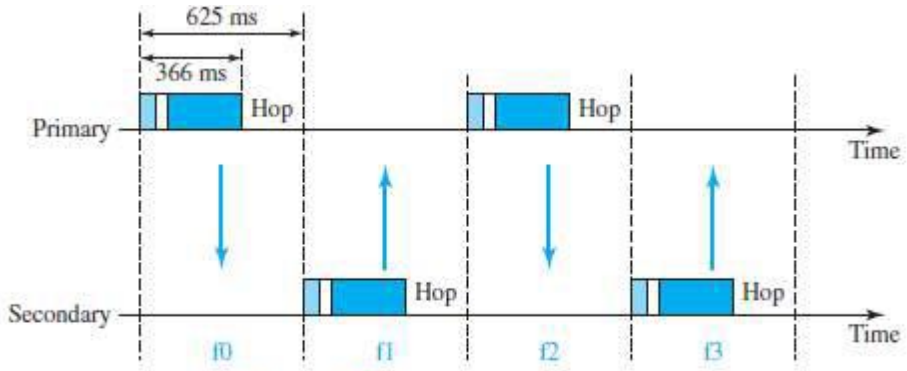


Figure 15.21 *Single-secondary communication*

Links

• Two types of links can be created between a primary and a secondary:

1) SCQ link (Synchronous Connection-oriented Link) and

2) ACL links (Asynchronous Connectionless Link).

1) SCA

- This link is used when avoiding latency is more important than data-integrity.
  (Latency → delay in data delivery, Integrity→error-free delivery)
- A physical-link is created between the primary and a secondary by reserving specific slots at regular intervals.
- The basic unit of connection is 2 slots. One slot is used for each direction.
- If a packet is damaged, it is never retransmitted.
- Application: Used for real-time audio where avoiding delay is all-important.
- A secondary
  → can create up to 3 SCQ links with the primary
  → can send digitized audio (PCM) at 64 kbps in each link.

2) ACL

- This link is used when data-integrity is more important than avoiding latency.
- If a payload encapsulated in the frame is corrupted, it is retransmitted.
- A secondary returns an ACL frame in the available odd-numbered slot if and only if the previous slot has been addressed to it.
- ACL can use one, three, or more slots and can achieve a maximum data-rate of 721 kbps.

Frame Types

• A frame in the baseband layer can be one of 3 types:

1) one-slot

2) three-slot or

3) five-slot.

1) One-slot frame

- A slot is 625 μs.
- However, in a one-slot frame exchange, 259 μs is needed for hopping & control mechanisms.
- This means that a one-slot frame can last only 625 - 259, or 366 μs.
- With a 1-MHz bandwidth and 1 bit/Hz, the size of a one-slot frame is 366 bits.

2) Three-slot frame

- A three-slot frame occupies 3 slots.
- However, since 259 μs is used for hopping, the length of the frame is 3 x 625 - 259 = 1616 μs or 1616 bits.
- A device that uses a three-slot frame remains at the same hop (at the same carrier frequency) for 3 slots.
- Even though only once hop number is used, 3 hop numbers are consumed.
- That means the hop number for each frame is equal to the first slot of the frame.

3) Five-slot frame

- A five-slot frame also uses 259 bits for hopping, which means that the length of the frame is 5 x 625 - 259 =2866 bits.

Frame Format

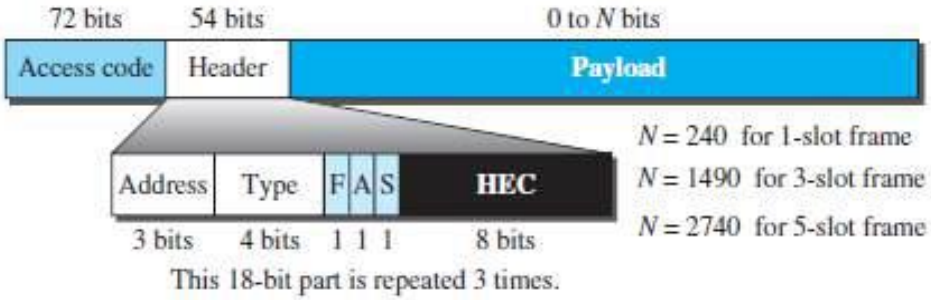


Figure 15.23 *Frame format types*

The following describes each field (Figure 15.23):

1) Access code

- This field contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from anothe

2) Header

- This field is a repeated I8-bit pattern. Each pattern has the following subfields:

i) Address

¤ This subfield can define up to 7 secondaries (1 to 7).

¤ If the address is zero, it is used for broadcast communication from the primary to all secondaries.

ii) Type

¤ This subfield defines the type of data coming from the upper layers.

iii) F

¤ This subfield is for flow control.

¤ When set (1), it indicates that the device is unable to receive more frames (buffer is full).

iv) A

¤ This subfield is for acknowledgment.

¤ Bluetooth uses Stop-and-Wait ARQ.

1 bit is sufficient for acknowledgment.

v) S

¤ This subfield holds a sequence number.

¤ Bluetooth uses Stop-and-Wait ARQ

¤ 1 bit is sufficient for sequence numbering.

vi) HEC (header error correction)

¤ This subfield is a checksum to detect errors in each 18-bit header section.

- The header has three identical 18-bit sections.
- The receiver compares these three sections, bit by bit.
- If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules.
- This is a form of forward error correction (for the header only).
- This double error control is needed because the nature of the communication, via air, is very noisy.
- There is no retransmission in this sublayer.

3) Payload

- This subfield can be 0 to 2740 bits long.
- It contains data or control information coming from the upper layers.

L2CAP

• The L2CAP is roughly equivalent to the LLC sublayer in LANs (Figure 15.20).

• It is used for data exchange on an ACL link. (L2CAP Logical Link Control and Adaptation Protocol)

• SCQ channels do not use L2CAP(Figure 14.25)

Figure 15.20 *L2CAP data packet format*

The following describes each field:

1) Length

- This field defines the size of the data, in bytes, coming from the upper layers.
- Data can be up to 65,535 bytes.

2) CID (Channel ID)

- This field defines a unique identifier for the virtual channel created at this level.

• The L2CAP has specific duties:

1) Multiplexing
2) Segmentation and reassembly
3) QoS (Quality of Service) and
4) Group management.

1) Multiplexing

- The L2CAP can do multiplexing.
- At the sender site, L2CAP
  → accepts data from one of the upper-layer protocols
  → frames the data and
  → delivers the data to the baseband layer.
- At the receiver site, L2CAP
  → accepts a frame from the baseband layer
  → extracts the data, and
  → delivers the data to the appropriate protocol layer.
- It creates a kind of virtual channel.

2) Segmentation and Reassembly

- In the baseband layer, the maximum size of the payload field is 2774 bits, or 343 bytes.
- This includes 4 bytes to define the packet and packet-length.
- Therefore, the size of the packet that can arrive from an upper layer can only be 339 bytes.
- However, application layers sometimes need to send a data packet that can be up to 65,535 bytes (for example: an Internet packet).
- The L2CAP

→ divides the large packets into segments and

→ adds extra information to define the location of the segments in the original packet.

- The L2CAP segments the packet at the source and reassembles them at the destination.

3) QoS

- Bluetooth allows the stations to define a QoS level.
- If no QoS level is defined, Bluetooth defaults to best-effort service; it will do its best under the circumstances.

4) Group Management

- Another functionality of L2CAP is to allow devices to create a type of logical addressing between themselves.
- This is similar to multicasting.
- For example: 2 or 3 secondary devices can be part of a multicast group to receive data from the primary.