Module-5

- **Wired LANs Ethernet**
  Ethernet Protocol
  Standard Ethernet
  Fast Ethernet
  Gigabit Ethernet and 10 Gigabit Ethernet
- **Wireless LANs**
  Introduction
  IEEE 802.11 Project
  Bluetooth.
- **Other wireless Networks**
  Cellular Telephony

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.

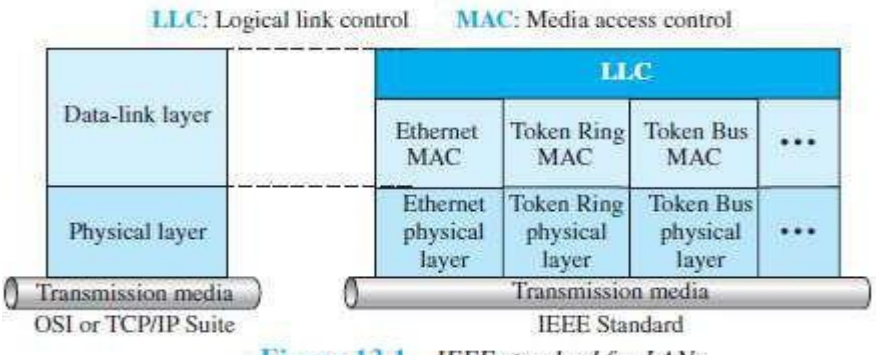


Figure 13.1 *IEEE standard for LANs*

Ethernet Evolution

- Four generations of Ethernet (Figure 13.2):
    3) Standard-Ethernet (10 Mbps)
    4) Fast-Ethernet (100 Mbps)
    5) Gigabit-Ethernet (1 Gbps) and
    6) Ten-Gigabit-Ethernet (10 Gbps)

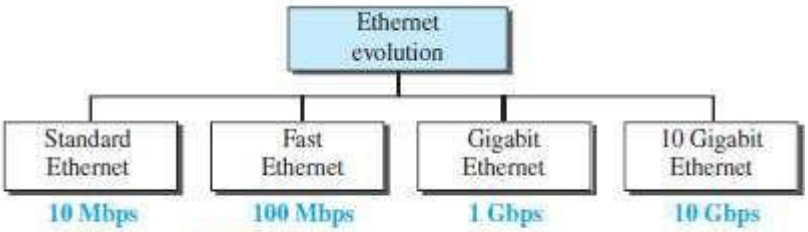


Figure 13.2 *Ethernet evolution through four generations*

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.
  If a frame drops, the sender will not know about it.
  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.
  If the transport layer is UDP (connectionless protocol), the frame is lost.
  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

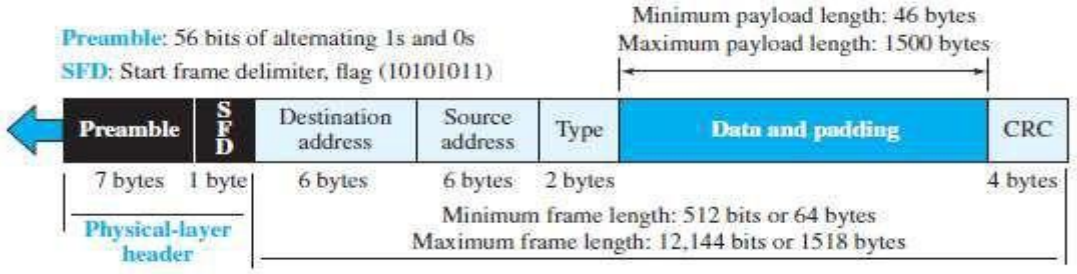


Figure 13.3 *Ethernet frame*

- 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).

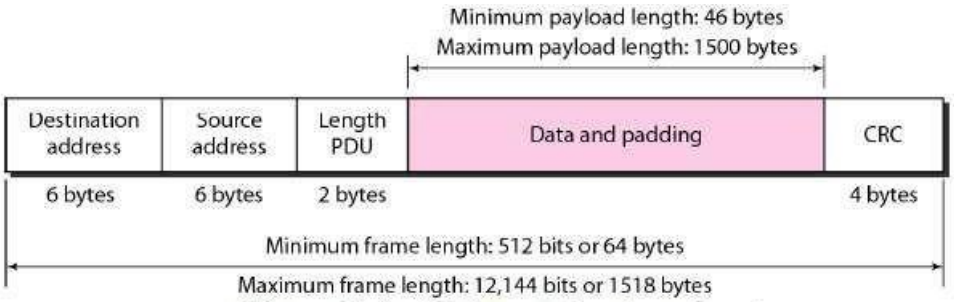


Figure 13.5 *Minimum and maximum lengths*

- The minimum length restriction is required for the correct operation of CSMA/CD.
- Minimum length of frame = 64 bytes.
    8. Minimum data size = 46 bytes.
    9. 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

(NIC □ network interface card)

Example

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.

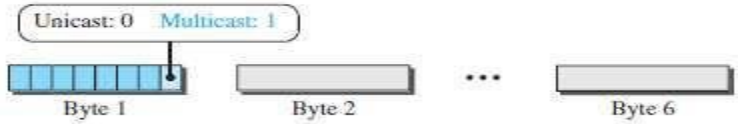


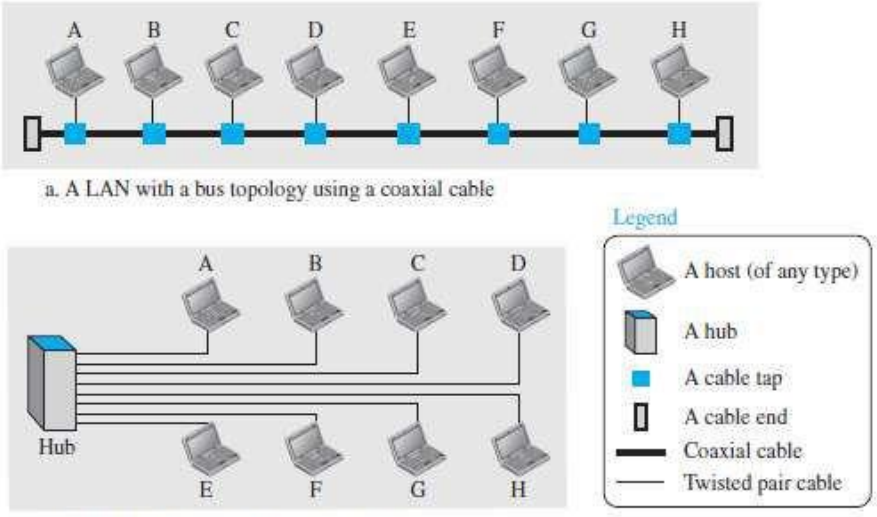
Figure 13.4 *Unicast and multicast addresses*

- 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).



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

b. A LAN with a star topology using a hub

Figure 13.5 *Implementation of standard Ethernet*

Question: 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.

Example

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

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

Max Length= $(2 \times 10^8) \times (51.2 \times 10^{-6})/2 = 5120$m

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.

Example

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

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

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.

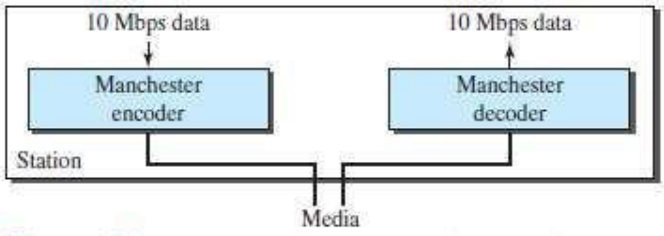


Figure 13.6 *Encoding in a Standard Ethernet implementation*

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.

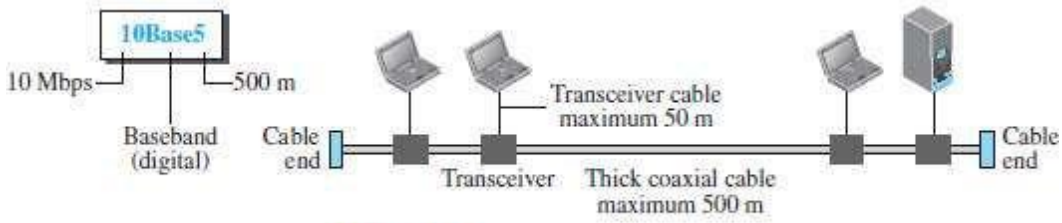


Figure 13.7 *10Base5 implementation*

- 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.

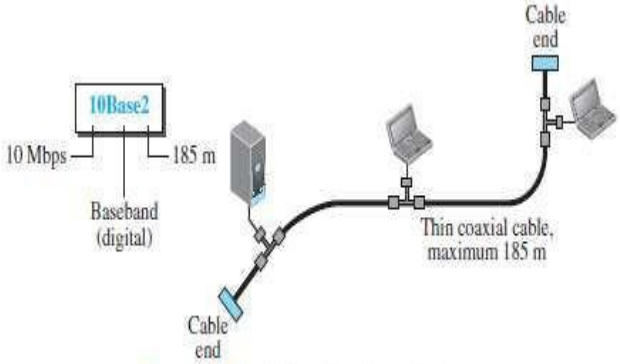


Figure 13.8 *10Base2 implementation*

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.

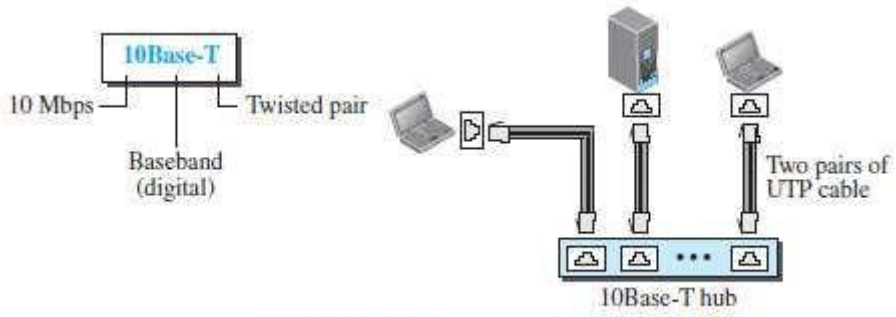


Figure 13.9 *10Base-T implementation*

- 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.

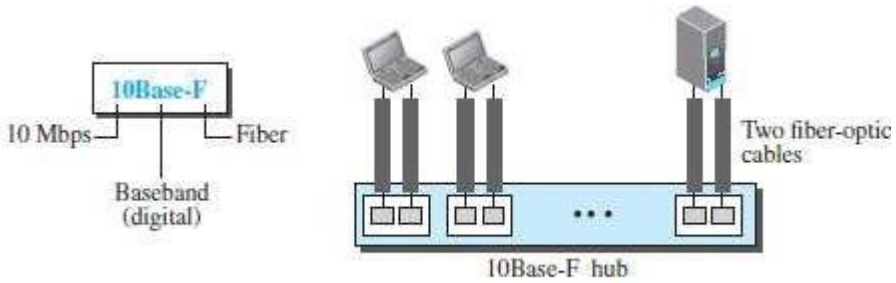


Figure 13.10 *10Base-F implementation*

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.

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

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.

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)
  2) 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

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

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 access).

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.

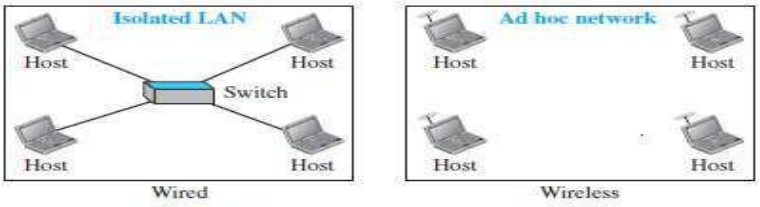


Figure 15.1 *Isolated LANs: wired versus wireless*

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.

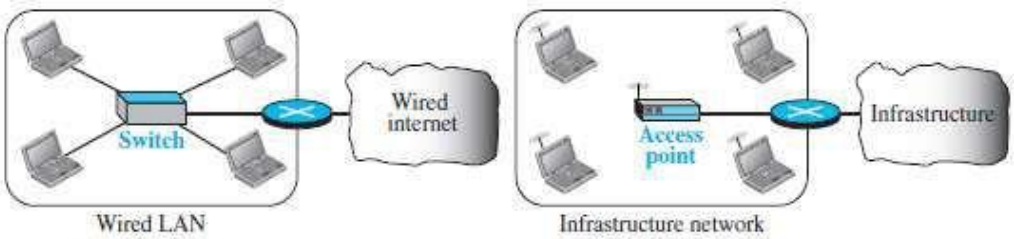


Figure 15.2 *Connection of a wired LAN and a wireless LAN to other networks*

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.

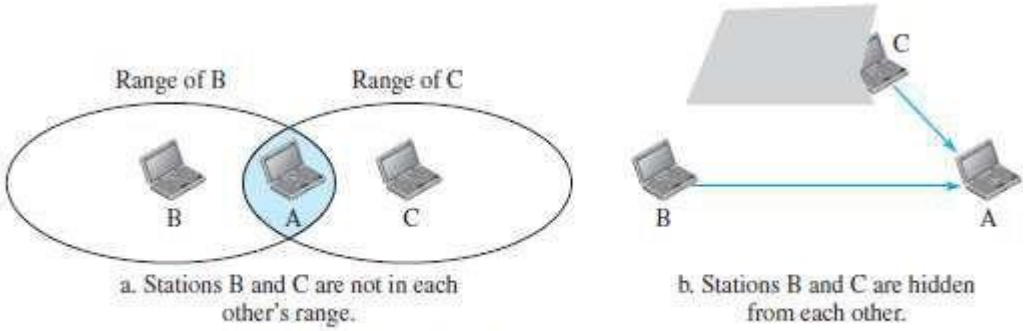


Figure 15.3 *Hidden station problem*

IEEE 802.11
Architecture

- The standard defines 2 kinds of services: 1) Basic service set (BSS) and
  2) Extended service set (ESS).

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.

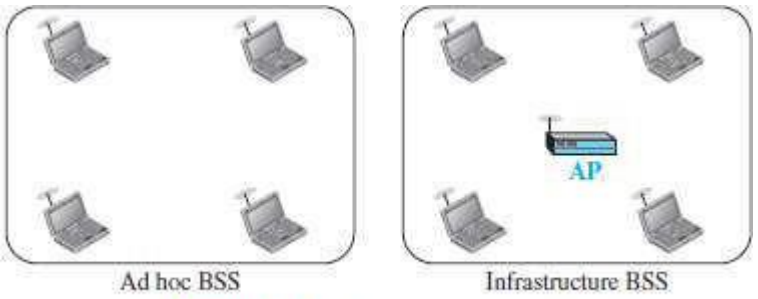


Figure 15.4 *Basic service sets (BSSs)*

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.

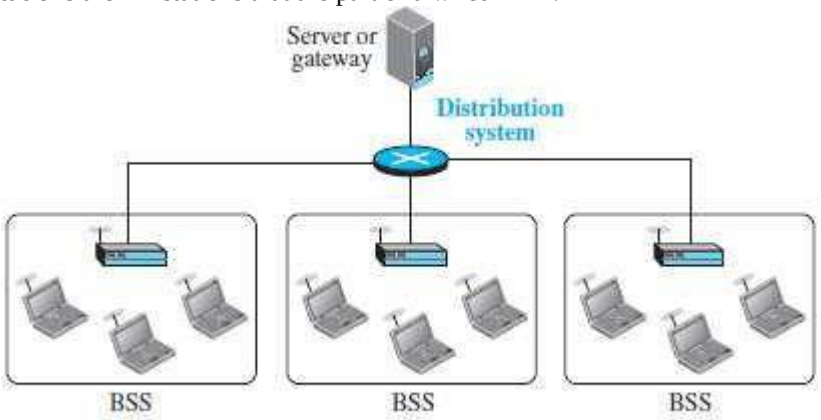


Figure 15.5 *Extended service set (ESS)*

- 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:

3) 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.

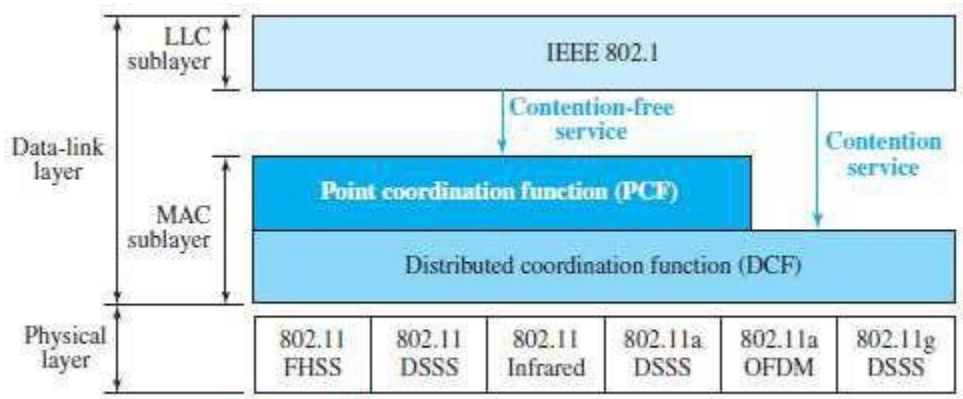


Figure 15.6 *MAC layers in IEEE 802.11 standard*

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.

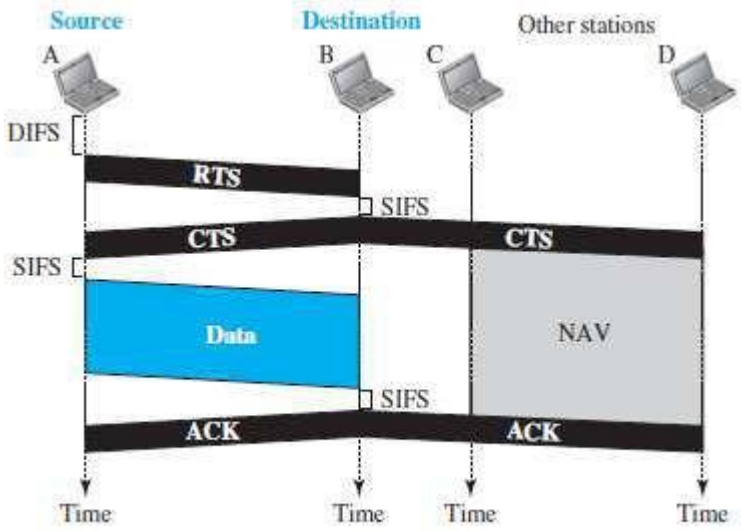


Figure 15.7 *CSMA/CA and NAV*

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 interframe space SIFS □ short inter frame space) (RTS □ requestto 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.

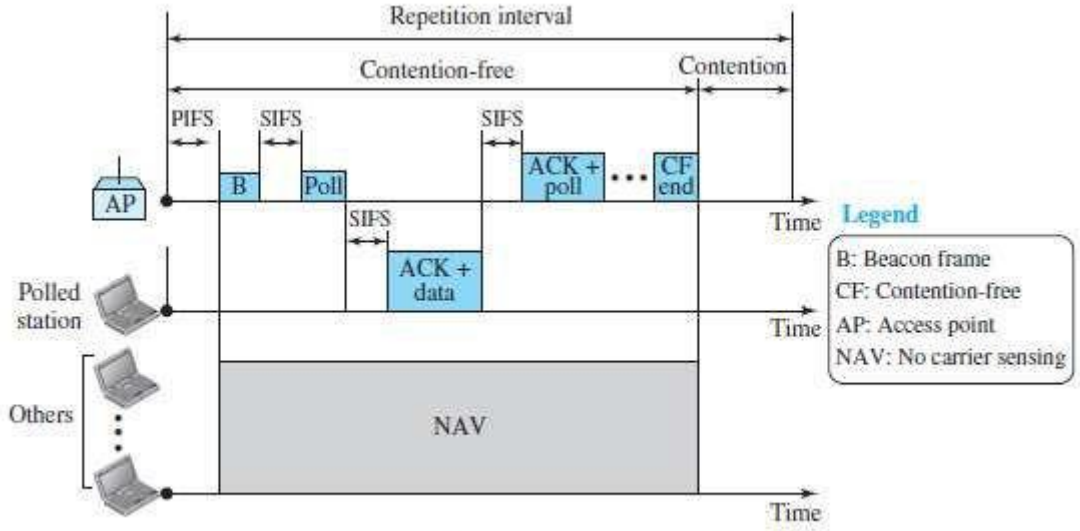


Figure 15.8 *Example of repetition interval*

- 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

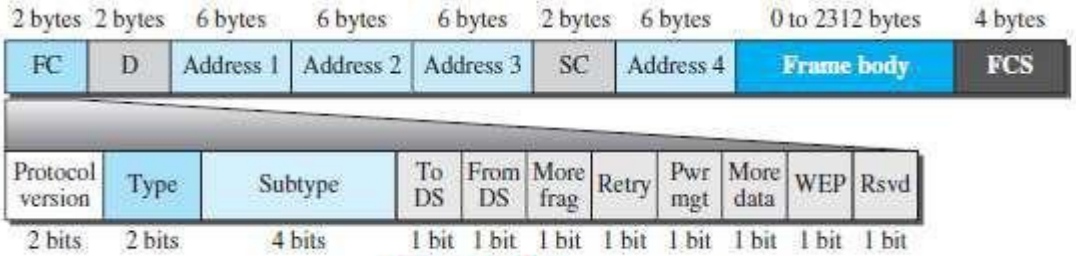


Figure 15.9 *Frame format*

- 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.

7) Management Frames

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

8) 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)

9) 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.

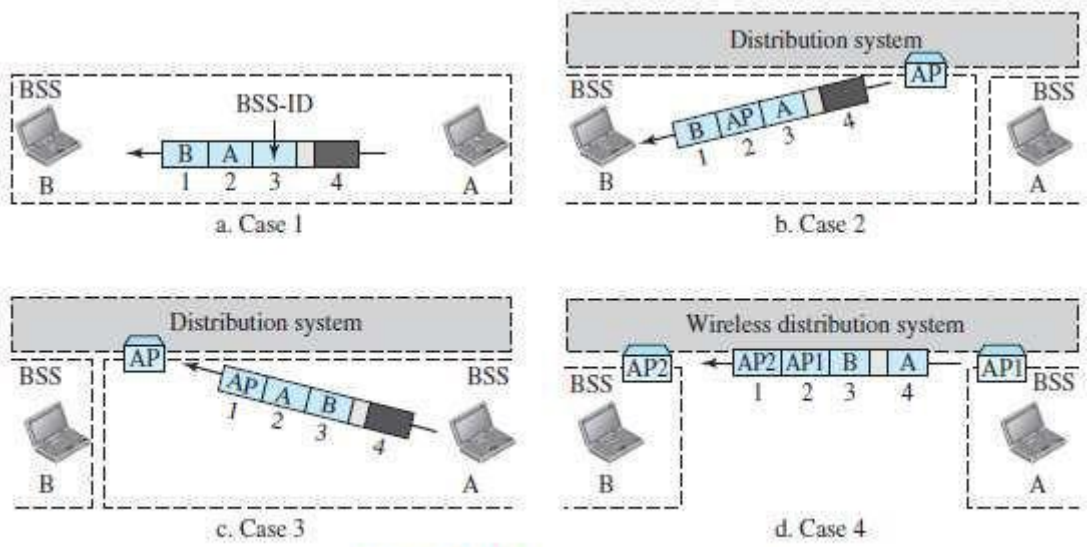


Figure 15.11 *Addressing mechanisms*

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.

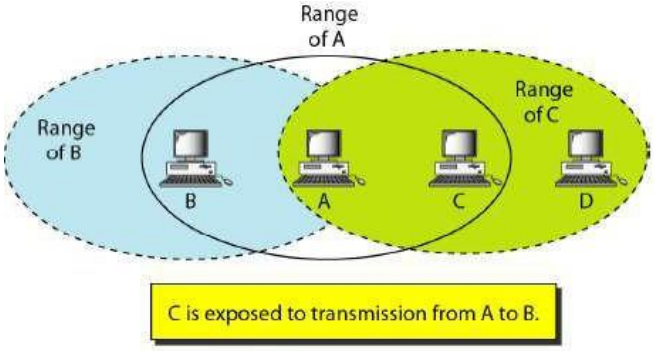


Figure 14.12 *Exposed station problem*

- 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.

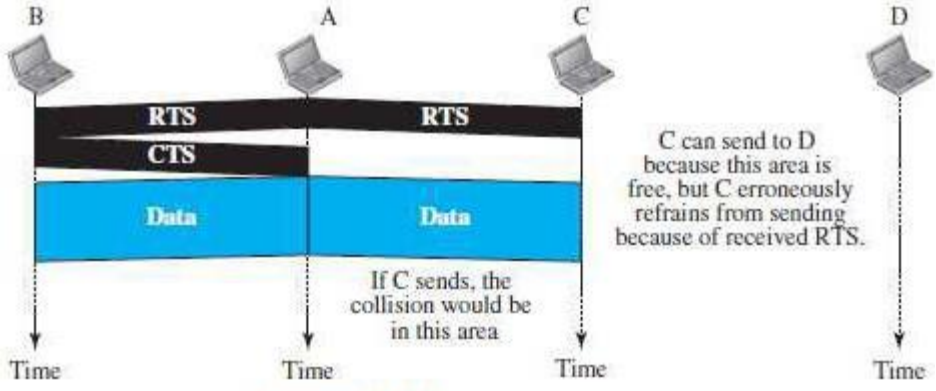


Figure 15.12 *Exposed station problem*

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, andmedical)

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.
- 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 secondary.
- 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.

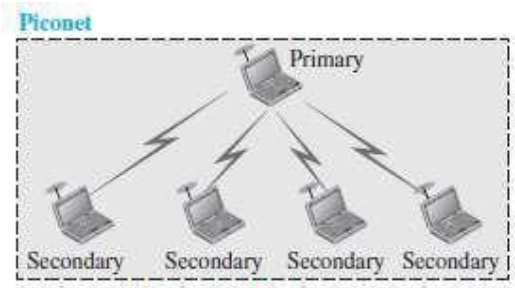


Figure 15.17 *Piconet*

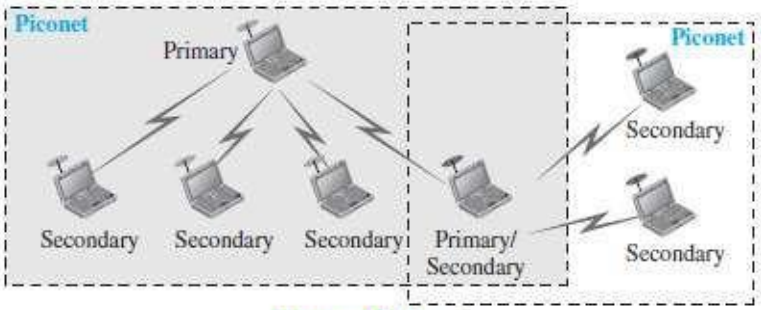


Figure 15.18 *Scatternet*

- 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 secondary's 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).

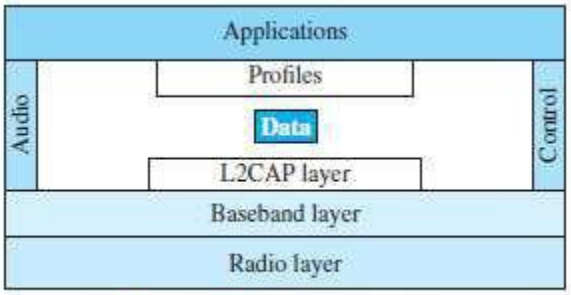


Figure 15.19 *Bluetooth layers*

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 „a" is represented by a frequency deviation below the carrier.

➢ The frequencies, in megahertz, are defined according to the following formula for each channel:

➢ For example,

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

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; secondary cannot communicate directly with one another.

TDMA

- Bluetooth uses a form of TDMA that is called TDD-TDMA (time division 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 (half duplex);

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).

SCA

- This link is used when avoiding latency is more important than data-integrity. (Latency □ delay in data delivery
  Integrity □ error-freedelivery)

ACL

- This link is used when data-integrity is more important than avoiding latency.

Frame Types

- A frame in the baseband layer can be one of 3 types: 1) one-slot 2) three-slot or 3) five-slot.

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.

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.

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

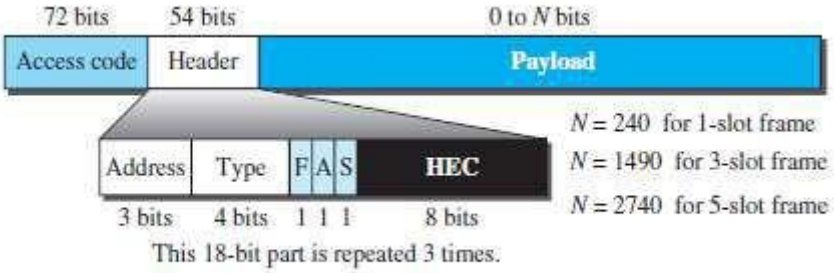


Figure 15.23 *Frame format types*

- The following describes each field (Figure 15.23):

Access Code

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

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.

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 AdaptationProtocol)
- 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.

CELLULAR TELEPHONY

- Cellular telephony is designed to provide communications
  - → between two moving units called mobile-stations (MSs) or
  - → between one mobile-station and one stationary unit called a land unit (Figure 16.6).
- A service-provider is responsible for
  - → locating & tracking a caller
  - → assigning a channel to the call and
  - → transferring the channel from base-station to base-station as the caller moves out-of-range.
- Each cellular service-area is divided into small regions called cells.
- Each cell contains an antenna.
- Each cell is controlled by AC powered network-station called the base-station (BS).
- Each base-station is controlled by a switching office called a mobile-switching-center (MSC).
- MSC coordinates communication between all the base-stations and the telephone central office.
- MSC is a computerized center that is responsible for
  - → connecting calls
  - → recording call information and
  - → billing.
- Cell-size is not fixed; Cell-size can be increased or decreased depending on population of the area.
- Cell-radius = 1 to 12 mi.
- Compared to low-density areas, high-density areas require many smaller cells to meet traffic demands.
- Cell-size is optimized to prevent the interference of adjacent cell-signals.

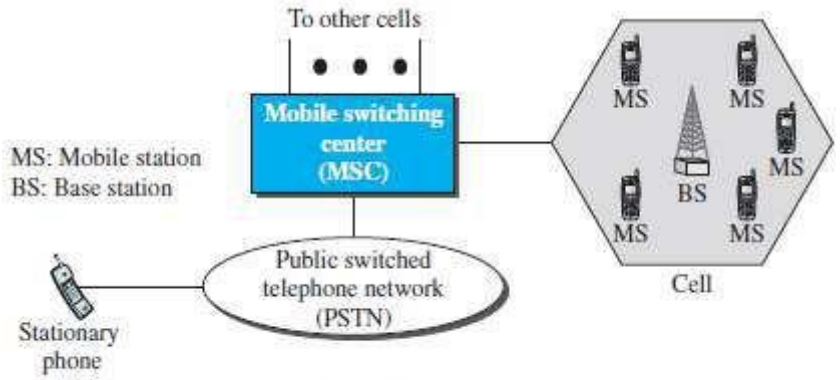


Figure 16.6 *Cellular system*

Operation
Frequency Reuse Principle

- In general, neighboring-cells cannot use the same set of frequencies for communication.
- Using same set of frequencies may create interference for the users located near the cell-boundaries.
- However,
  → set of frequencies available is limited and
  → frequencies need to be reused.
- A frequency reuse pattern is a configuration of N cells. Where N = reuse factor
- Each cell uses a unique set of frequencies.
- When the pattern is repeated, the frequencies can be reused.
- There are several different patterns (Figure 16.7).
- The numbers in the cells define the pattern.
- The cells with the same number in a pattern can use the same set of frequencies. These cells are called the reusing cells.

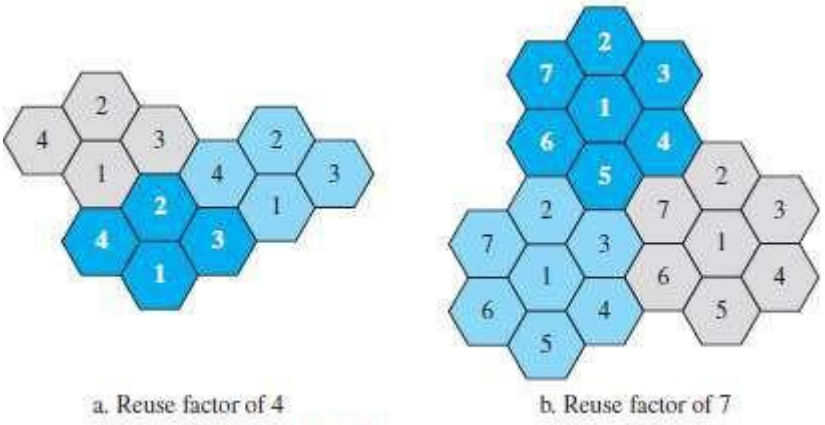


Figure 16.7 *Frequency reuse patterns*

Transmitting

- Procedure to place a call from a mobile-station:
  1) The caller
  → enters a phone number and
  → presses the send button.
  2) The mobile-station
  → scans the band to determine setup channel with a strong signal and
  → sends the data (phone number) to the closest base-station.
  3) The base-station sends the data to the MSC.
  4) The MSC sends the data on to the telephone central office.
  5) If called party is available, a connection is made and the result is relayed back to the MSC.
  6) The MSC assigns an unused voice channel to the call, and a connection is established.
  7) The mobile-station automatically adjusts its tuning to the new channel.
  8) Finally, voice communication can begin.

Receiving

- Procedure to receive a call from a mobile-station:
  9) When a mobile phone is called, the telephone central office sends phone number to the MSC.
  10) MSC searches for the location of the mobile-station by sending query-signals to each cell in a process. This is called paging.
  11) When the mobile-station is found, the MSC transmits a ringing signal.
  12) When the mobile-station answers, the MSC assigns a voice channel to the call.
  13) Finally, voice communication can begin.

Handoff

- During a conversation, the mobile-station may move from one cell to another.
- Problem: When the mobile-station goes to cell-boundary, the signal becomes weak.
- To solve this problem, the MSC monitors the level of the signal every few seconds.
- If signal-strength decreases, MSC determines a new cell to accommodate the communication.
- Then, MSC changes the channel carrying the call (hands signal off from old channel to a new one).
- Two types of Handoff: 1) Hard Handoff 2) Soft Handoff

14) Hard Handoff

- Early systems used a hard handoff.
- A mobile-station only communicates with one base-station.
- When the MS moves from one cell to another cell,
  - i) Firstly, communication must be broken with the old base-station.
  - ii) Then, communication can be established with the new base-station.
- This may create a rough transition.

15) Soft Handoff

- New systems use a soft handoff.
- A mobile-station can communicate with two base-stations at the same time.
- When the MS moves from one cell to another cell,
  - i) Firstly, communication must be broken with the old base-station.
  - ii) Then, the same communication may continue with the new base-station.

Roaming

- Roaming means that the user
  - → can have access to communication or
  - → can be reached where there is coverage.
- Usually, a service-provider has limited coverage.
- Neighboring service-providers can provide extended coverage through a roaming contract.

First Generation (1G)

- The first generation was designed for voice communication using analog signals.
- The main system evolved in the first generation: AMPS (Advanced Mobile Phone System).

AMPS

- This system is a 1G analog cellular system.
- The system uses FDMA to separate channels in a link.
- Here we discuss, two issues: 1) Bands 2) Transmission

1) Bands

- The system operates in the ISM 800-MHz band.
- The system uses 2 separate channels (Figure 16.8):
  - i) First channel is used for forward communication (base-station to mobile-station) Band range: 869 to 894 MHz
  - ii) Second channel is used for reverse communication (mobile-station to base-station). Band range: 824 to 849 MHz

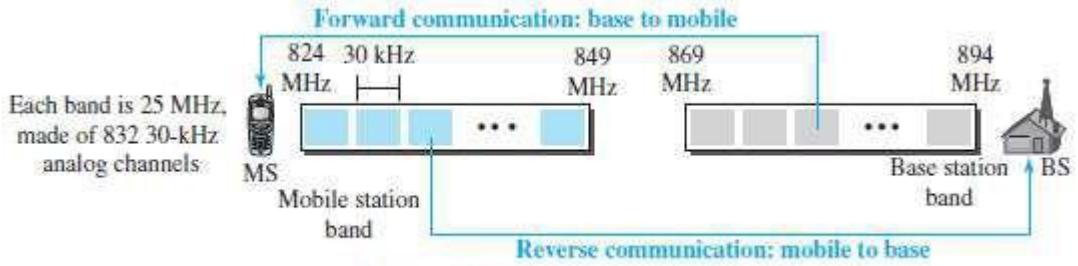


Figure 16.8 *Cellular bands for AMPS*

2) Transmission

- The system uses FM and FSK for modulation (Figure 16.9).
  - i) Voice channels are modulated using FM.
  - ii) Control channels are modulated using FSK to create 30-kHz analog signals.
- The system uses FDMA to divide each 25-MHz band into 30-kHz channels.

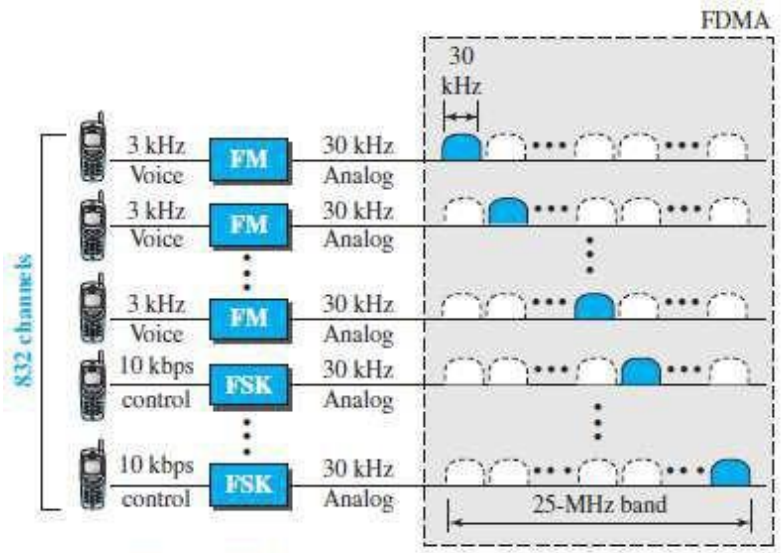


Figure 16.9 *AMPS reverse communication band*

Second Generation (2G)

- The second generation was designed for higher-quality voice communication using digital signals.
- 1G vs. 2G:
    1) The first generation was designed for analog voice communication.
    2) The second generation was mainly designed for digital voice communication.
- Three major systems evolved in the second generation:
    1) D-AMPS (digital AMPS)
    2) GSM (Global System for Mobile communication) and
    3) IS-95 (Interim Standard).

D-AMPS

- D-AMPS (Digital AMPS) was improved version of analog AMPS.
- D-AMPS was backward-compatible with AMPS.
- Thus, in a cell,
    1) First telephone may use AMPS and
    2) Second telephone may use D-AMPS.
- Here we discuss, two issues: 1) Bands 2) Transmission
    1) Band
    - The system uses the same bands and channels as AMPS (Figure 16.10).

    2) Transmission
    - Each voice channel is digitized using a very complex PCM and compression technique.

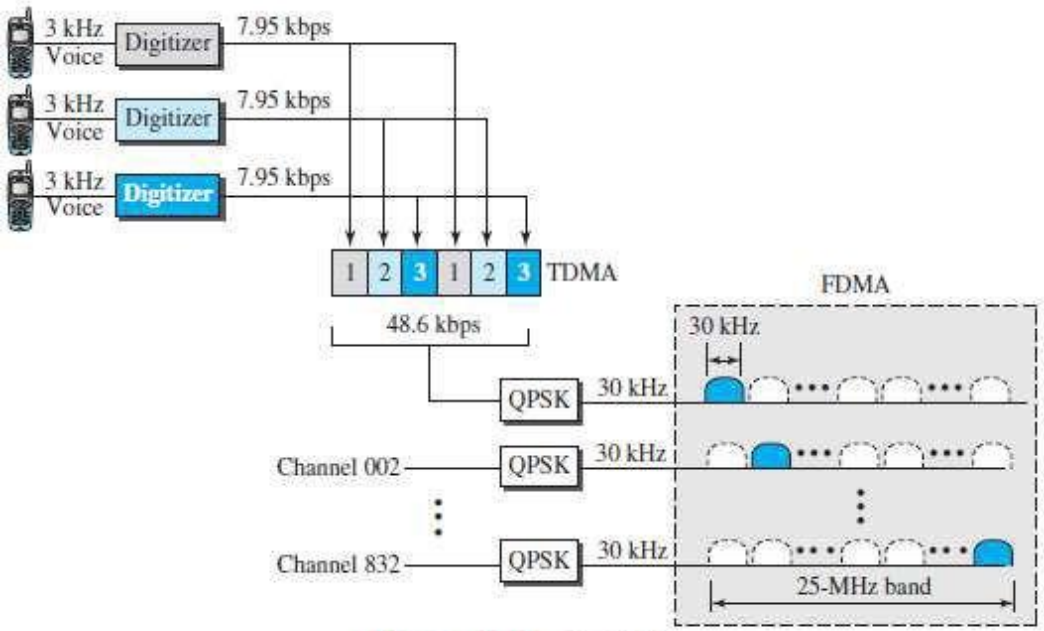


Figure 16.10 *D-AMPS*

GSM

- Aim of GSM: to replace a number of incompatible 1G technologies.
- Here we discuss, two issues: 1) Bands 2) Transmission

Bands

- The system uses two bands for duplex communication (Figure 16.11).
- Each band is 25 MHz in width.
- Each band is divided into 124 channels of 200 kHz.

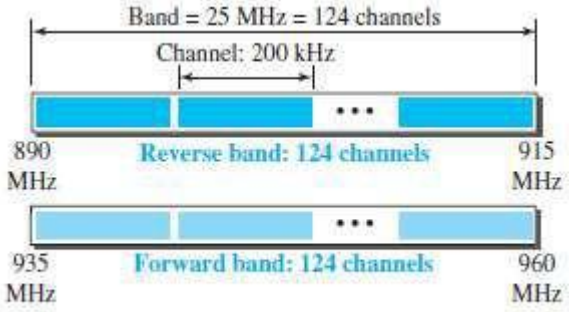


Figure 16.11 *GSM bands*

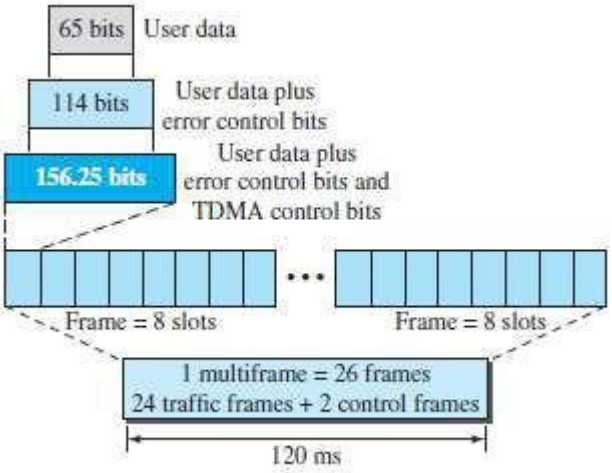


Figure 16.13 *Multiframe components*

Transmission

- Each voice channel is digitized and compressed to a 13-kbps digital signal (Figure 16.12).
- Each slot carries 156.25 bits.
- Eight slots share a frame (TDMA).
- 26 frames also share a multiframe (TDMA).
- We can calculate the bit rate of each channel as follows.

$$\text{Channel data rate} = (1/120\text{ ms}) \times 26 \times 8 \times 156.25 = 270.8\text{ kbps}$$

- Each 270.8-kbps digital channel modulates a carrier using GMSK (a form of FSK); the result is a 200-kHz analog signal.
- Finally, 124 analog channels of 200 kHz are combined using FDMA. The result is a 25-MHz band (Figure 16.13).

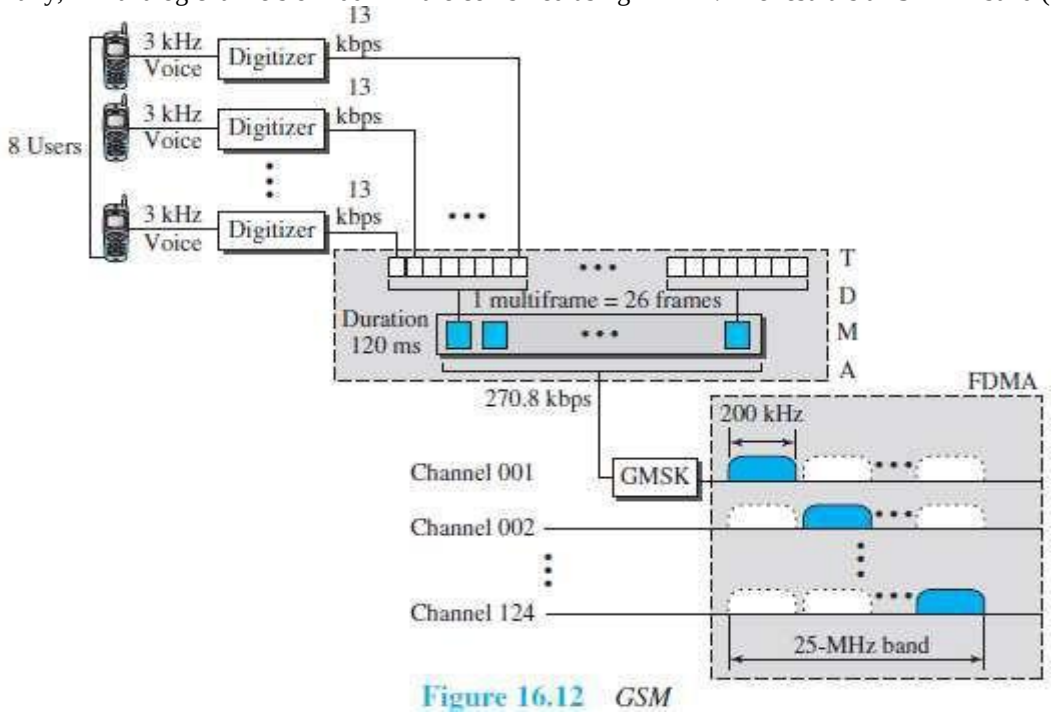


Figure 16.12 *GSM*

IS-95

- The system is based on CDMA and DSSS.

Third Generation (3G)

- 3G cellular telephony provides both digital data and voice communication.
- For example: Using a Smartphone,
  A person can talk to anyone else in the world.
  A person can download a movie, surf the Internet or play games.
- Interesting characteristics: the Smartphone is always connected; we do not need to dial a number to connect to the Internet.

(IMT □ Internet Mobile Communication)

- Some objectives defined by the blueprint IMT-2000 (3G working group):
  1) Voice quality comparable to that of the existing public telephone network.
  2) Data-rate of
     → 144 kbps for access in a moving vehicle (car)
     → 384 kbps for access as the user walks (pedestrians) and
     → 2 Mbps for the stationary user (office or home).
  3) Support for packet-switched and circuit-switched data services.
  4) A band of 2 GHz.
  5) Bandwidths of 2 MHz.
  6) Interface to the Internet

IMT-2000 Radio Interfaces

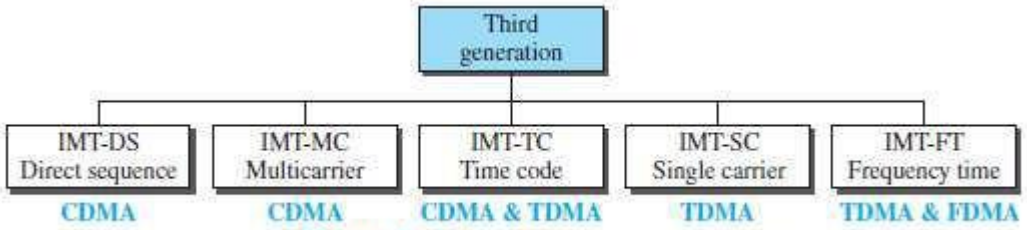


Figure 16.16 *IMT-2000 radio interfaces*

Fourth Generation (4G)

- 4G cellular telephony is expected to be a complete evolution in wireless communications.
- Some objectives defined by the 4G working group:
  1) A spectrally efficient system.
  2) High network capacity.
  3) Data-rate of
     → 100 Mbps for access in a moving vehicle
     → 1 Gbps for stationary users and
     → 100 Mbps between any two points in the world.
  4) Smooth handoff across heterogeneous networks.
  5) Seamless connectivity and global roaming across multiple networks.
  6) High quality of service for next generation multimedia support.
  7) Interoperability with existing wireless standards.
  8) All IP, packet-switched, networks.
- 4G is only packet-based networks.
- 4G supports IPv6.
- 4G provides better multicast, security, and route optimization capabilities.
- Here we discuss, following issues:
  1) Access Scheme
  2) Modulation
  3) Radio System
  4) Antenna
  5) Applications

1) Access Scheme

- To increase efficiency,
  i) capacity, ii) scalability & iii) new access techniques are being considered for 4G.
- For example:
  i) OFDMA and IFDMA are being considered for the downlink & uplink of the next generation UMTS.
  ii) MC-CDMA is proposed for the IEEE 802.20 standard.

2) Modulation

- More efficient 64-QAM is being proposed for use with the LTE standards.

3) Radio System

- The 4G uses a SDR system.
- The components of an SDR are pieces of software and thus flexible.
- The SDR can change its program to shift its frequencies to mitigate frequency interference.

4) Antenna

- The MIMO and MU-MIMO antenna system is proposed for 4G.
- Using this antenna, 4G allows independent streams to be transmitted simultaneously from all the antennas to increase the data-rate.
- MIMO also allows the transmitter and receiver coordinates to move to an open frequency when interference occurs.

5) Applications

- At the present rates of 15-30 Mbps, 4G is capable of providing users with streaming high-definition television.
- At 100 Mbps, the content of a DVD-5 can be downloaded within about 5 minutes for offline access.

OFDMA: Orthogonal FDMA IFDMA: interleaved FDMA
LTE LongTerm Evolution SDR: Software Defined Radio
MIMO: multiple-input multiple-output MU-MIMO: multiuser MIMO
UMTS Universal Mobile Telecommunications System
MC-CDMA multicarrier code division multiple access