# CHAPTER 15

## PRACTICE SET

### Questions

**Q15-1.** The modulation technique is GFSK (FSK with Gaussian bandwidth filtering). The carrier frequencies are 2042 + *n* MHz, in which *n* can be 0 to 79 (in most countries).

**Q15-2.** A piconet can have more than eight stations, but only eight of them can be active at one time; the rest should be in a parked state (inactive). If one of the parked stations needs to become active, one of the active stations should move to the parked state.

**Q15-3.** A piconet is the smallest ad hoc network. It is made of one primary (master) station and up to seven secondary (slave) stations. A scatternet is a larger ad hoc network made by gluing two or more piconets using one of the secondary stations in one piconet to act as the primary station in another piconet.

**Q15-4.** We can mention four reasons:

**a.** It is difficult to detect collision in a wireless channel because the received power is low.

**b.** A station, which is normally operating on battery, does not have enough power to both send and receive at the same time, which is necessary for detecting collision.

**c.** Transmission from other wireless LANs may interfere.

**d.** A hidden station may not receive the signal sent by other stations to prevent sending its own.

**Q15-5.** Error rate is much higher in a wireless LAN than in a wired LAN. Fragmentation reduces the frame size and reduces the probability of error in a frame.

**Q15-6.** SNR is the ratio of the signal power to the noise power. If the signal power is decreased or the noise power is increased, SNR will decrease. In a wireless LAN, the signal power is less (using batteries). The noise power is higher in a wireless LAN because the noise is not controlled. The noise from any source can affect the signal exchanged between the sender and the receiver.

**Q15-7.** The medium of a wired LAN is guided (cable or wire); the medium of a wireless LAN is unguided (air).

**Q15-8.** Bluetooth uses the frequency hopping spread spectrum (FHSS), to let stations hop between 79 channels. Hopping is done 1600 times per second, which means the hopping duration is 256 μs.

**Q15-9.** In a wired network, a link-layer switch is connected to the hosts via point-to-point dedicated connections; there is no need for addresses for communication between hosts and the switch. In a wireless network, an AP is connected to the hosts via a multicast network (air); the MAC addresses of the host and the AP make the communication more efficient; when a host sends a frame to the AP, all other hosts drop the received copy of the frame at the MAC sublayer when they find that the frame does not belong to them.

**Q15-10.** The *baseband* layer uses a variation of TDMA called TDD-TDMA (time-division duplex TDMA), in which the stations can send and receive data using time slots (TDMA), but not at the same time (half-duplex).

**Q15-11.** The answer is negative. The addresses are selected from the same address space. For example, if locally there are one wireless and one wired device, they cannot have the same MAC address; addresses should be unique.

**Q15-12.** The radio layer in Bluetooth roughly plays the role of the physical layer in the TCP/IP suite.

**Q15-13.** The allocated band for Bluetooth is the ISM 2.4 GHz band, which actually spans from 2.4 GHz to 2.4835 GHz. This means that the bandwidth is actually 0.0835 GHz or 83.5 MHz.

**Q15-14.** A Bluetooth network is normally a wireless small network that is more suited to communication in a personal environment; a wireless local area can cover a larger geographical areas such as a building or an office.

**Q15-15.** In a wireless environment, a receiving station may receive more than one signal from the same sender related to the same message. One of these signals can be the one received directly; the others are signals reflected back from some barrier. Since the signals have travelled different distances, they can be out of phase. The combination of these signals creates a signal which is the distorted version of the original signal sent by the sender. It is sometimes difficult to detect the original message. We often have difficulty understanding the other party when talking on a cellular phone

**Q15-16.** In the case of wired LANs, we have moved from a shared medium to a dedicated medium (point-to-point communication). In this situation a MAC protocol, such as CSMA/CD, is not needed anymore. In the case of a wireless LAN, the medium (air) is still shared between the users. We need MAC protocols such as CSMA/CA or channelization protocols to control sharing the medium.

**Q15-17.** The 83.5 MHz bandwidth in Bluetooth is divided into 79 channels, each of 1 MHz. The rest of the bandwidth is used for guard bands.

**Q15-18.** In a wired LAN, the medium access process is achieved using the collision detection mechanism. In a wireless LAN, the same task is done using the RTS, CTS, and ACK frames. We need all of these as well as data frames.

**Q15-19.** Propagation in a wireless LAN is not confined as in a wired LAN. In a wired LAN, propagation is confined to the wires. Most of the original power may reach the destination. In a wireless LAN, the power is distributed in a sphere with the sender at the center and the receiver at one point on the surface. Only a part of the power arrives at the receiver; the rest is lost in the air.

**Q15-20.** The answer is negative. The MAC addresses are coming from the same address space. Only one MAC address can serve in this case.

**Q15-21.** The *L2CAP* layer has a role similar to the LLC sublayer in a LAN. It provides multiplexing, segmentation and reassembly, quality of service, and group management.

# Problems

**P15-1.** We need to remember that the exchanged frames do not leave the BSS. All addresses are addresses of entities inside the BSS. With this in mind, we answer each question:

**a.** Since the exchanged frames do not leave the BSS, the values of both the *To DS* and *From DS* bits in all frames are set to 0s. No frame comes from a distribution system (*From DS* = 0) and no frame goes to a distribution system (*To DS* = 0).

**b.** The RTS frame needs to be sent by the station that wants to send the data frame, station A in this case. There are two addresses in this frame (address 1 and address 2). The value of address 1 is the recipient of the data frame that follows (address 1 = B's address); the value of address 2 is the address of the station that will send the data frame (address 2 = A's station). Note that since the channel is a broadcast channel, every non-hidden station will receive the RTS frame, but address 1 emphasizes that station B needs to respond to the RTS frame.

**c.** The CTS frame needs to be sent by the future recipient of the data frame, which is station B in this case. The value of address 1 in this frame (the only address field) is the address of the intended recipient of the CTS frame, which is station A. All stations that are not hidden from B also receive this frame.

**d.** After receiving the CTS frame, station A can send the data frame. The value of the address 1 field in this frame is the address of the recipient of the frame, which is station B. The value of the address 2 field is the address of the station sending the frame, which is station A. Address 3 in this case is the address of any entity involved in the communication besides the sender and receiver. Since there is no other entity involved, the address chosen is the BSS identification, which has the same format as other MAC addresses. This identification is used here to show that the communication should be confined to this BSS. Stations in other BSSs should drop this frame if it is accidentally received by them. The value of the address 4 field is not used in this case because the frame does not leave the BSS.

**e.** The ACK frame needs to be sent by the recipient of the data frame, station B in this case. The value of the address 1 in this frame is the address of the station that sent the data frame, address A.

**P15-2.** The following shows the steps:

**a.** The router consults its forwarding table and finds that the IP datagram with the destination address 24.12.7.1 needs to be sent out from interface m1.

**b.** The router sends out an ARP request from interface m1 looking for the MAC address of the host with IP address 24.12.7.1. The router sends an ARP packet to the AP1 and get its MAC address. This means that the router now creates an 802.3 (Ethernet) frame with the MAC address of its m1 interface as the source and the MAC address of the host as the destination. The router sends the frame to the AP1.

**c.** The AP1 needs to change the frame format. It extracts information from the 802.3 frame and inserts it into an 802.11 frame. The value of address 1 is the host's MAC address; the value of address 2 is the AP1's MAC address; the value of address 3 is the MAC address of the router, the originator of the communication in this case. Address 4 is not used in this case, because the router that has sent the original message is not wireless. The 802.11 packet is then broadcast in the air and received by the intended destination host.

**P15-3.** DCF is using a version of the Stop-and-Wait protocol. Each frame is considered as one or more fragments. In other words, if a frame is not fragmented, it is considered as the first and only fragment. Each fragment needs to be individually acknowledged by an ACK frame. The sender does not send the fragment until it receives the acknowledgment for the previous frame. The sender sets a timer, and if the acknowledgment for a fragment does not arrive, it resends it. The Stop-and-Wait protocol (used in this case), however, is simpler than the one we discussed before because, in this case, no sequence number and no acknowledgment number is used. Although a data frame has the SC field, the sequence number and fragment number defined there are actually the identification number and offset that define each fragment uniquely for the purpose of reassembly.

**P15-4.** Each 802.11 frame has 34 bytes of overhead to be added to the payload (frame body) which arrives from the upper layer (we ignore the preamble and other bytes that are added at the physical layer). In other words, the size of the frame is:

$$\text{frame size} = \text{payload size} + 34$$

Now we can answer the questions:

**a.** Without fragmentation, the size of the frame would be $1200 + 34 = 1234$ bytes.

**b.** The size of each fragment is $400 + 34 = 434$ bytes.

**c.** The total bytes sent is then $3 \times 434 = 1302$ bytes.

**d.** The extra bytes sent is $1302 - 1234 = 68$ bytes.

**P15-5.** We describe each IFS below:

**a.** The short interframe space (SIFS) is used to allow the two parties in a single session to continue their transmission. This includes the time that a party needs to send a CTS after receiving an RTS, sending an ACK after receiving a data fragment, or sending the next fragment after receiving the ACK for the previous fragment. It cannot be used to start a new session.

**b.** The base station that needs to send a beacon or poll frame (in PCF mode) needs to wait for a PIFS period of time to do so. PIFS is longer than SIFS to allow other stations to finish their sessions. However, if a time period of SIFS elapses and the entitled station did not use its opportunity, the base station can send its beacon or poll frame (after waiting PIFS) if it has one.

**c.** If a base station does not use its opportunity after PIFS time and a time equal to DIFS elapses, a station using DCF can start a new dialog. You may have noticed that PIFS is smaller than DIFS to give priority to the PCF sublayer.

**d.** An EIFS is normally used when there is an error in transmission and the station needs to wait this period of time to report the situation. This period is larger than the other ones to force the station to wait to see if the error is corrected before an action. For example, if a station has received a wrong frame, it needs to wait for a while to see if the correct frame will eventually arrive.

**P15-6.** We show the value of addresses in each communication phase:

**a.** Communication from station A to the AP1 occurs in a wireless environment (802.11). However, since the frame needs to go to the distribution system ultimately, the value of the *To DS* bit is set to 1, but the value of the *From DS* bit is zero. We need to consider four addresses. The first two addresses are the immediate destination and source addresses in BSS1. The third address is the final destination in BSS2. The fourth address is not used in this case. Address 1 needs to be the AP1 to allow the AP1 to send an ACK to A. Address 2 needs to be A to define the original source of the packet for the next two sections of communication. Address 3 needs to be C to allow the frame to reach its final destination.

Address 1: AP1 Address 2: A Address 3: C Address 4: —

**b.** Communication from the AP1 to the AP2 occurs in a wired environment (802.3); we need to consider two addresses: destination address and source address. The destination address is host C, taken from the address 3 in the packet received at the AP1. The source address is host A, taken from address 2 in the packet received at the AP1.

Destination address: C Source address: A

**c.** Communication from the AP2 to station C occurs in a wireless environment (802.11) again. However, since the frame comes from a distribution system, the value of the *To DS* bit is set to 0, but the value of the *From DS* bit is 1. We need to consider four addresses. The first two addresses are the immediate destination and source addresses in BSS2. The third address is the original source in BSS1. The fourth address is not used in this case.

| | | | |
|---|---|---|---|
| Address 1: C | Address 2: AP2 | Address 3: A | Address 4: — |

**P15-7.** We show the value of addresses in each communication phase:

**a.** Communication from station A to the AP1 occurs in a wireless environment (802.11). However, since the frame needs to go to the distribution system ultimately, the value of the *To DS* bit is set to 1, but the value of the *From DS* bit is zero.The situation is the same as the previous problem. The addresses are as follows:

| | | | |
|---|---|---|---|
| Address 1: AP1 | Address 2: A | Address 3: C | Address 4: — |

**b.** Communication from the AP1 to the AP2 now occurs in a wireless environment; we need to consider four addresses. However, since the frame needs to go to the distribution system and comes from the distribution system, the value of both *To DS* bit and *From DS* are set to 1s. Address 1 is the address of the immediate receiver, which is the address of the AP2. Address 2 is the address of the immediate sender, which is the AP1. Address 3 is the address of the final destination which is station C. Address 4 is the address of the original source, which is station A. The addresses are shown below:

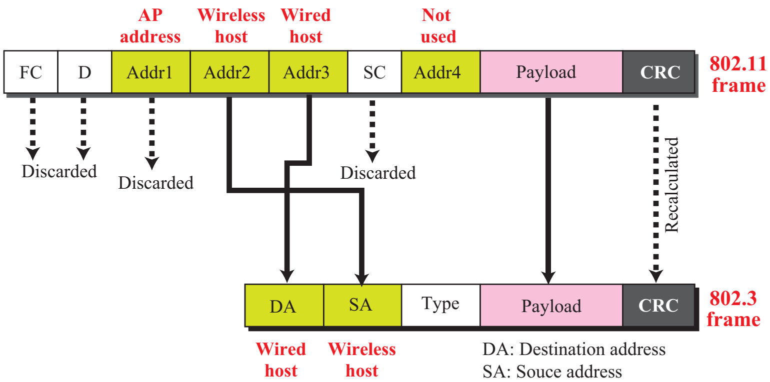
| | | | |
|---|---|---|---|
| Address 1: AP2 | Address 2: AP1 | Address 3: C | Address 4: A |

**c.** Communication from the AP2 to station C occurs in a wireless environment (802.11) again. However, since the frame comes from a distribution system, the value of the *To DS* bit is set to 0, but the value of the *From DS* bit is 1. We need to consider four addresses. This is the same as the previous problem. Addresses are shown below:

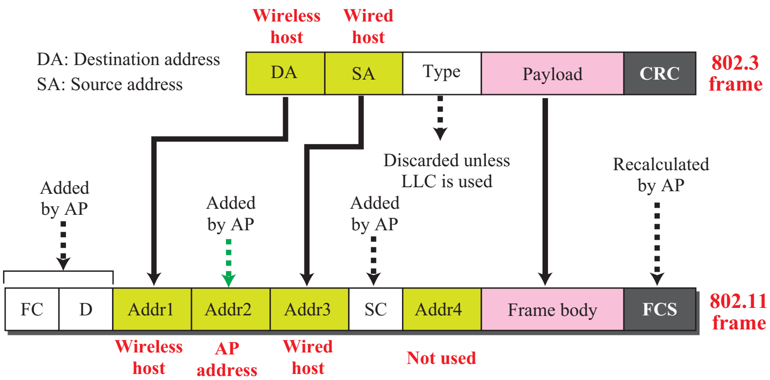
| | | | |
|---|---|---|---|
| Address 1: C | Address 2: AP2 | Address 3: A | Address 4: — |

**P15-8.** This is needed because a data frame or a fragment may be lost and need to be resent, which means the duration of the session becomes longer. The requirement ensures that other stations refrain from accessing the channel until the session is over.

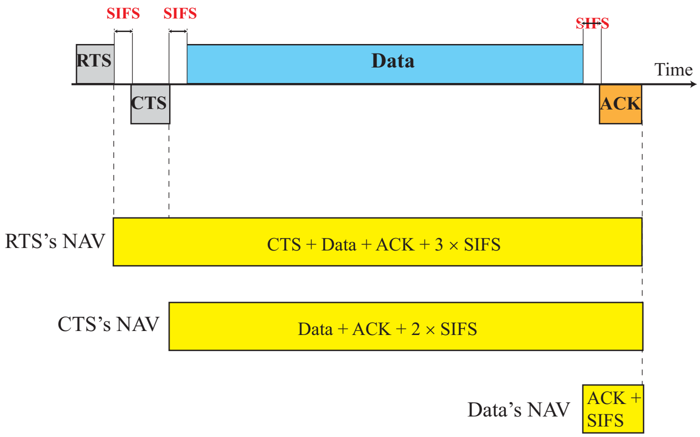
**P15-9.** The following shows how the fields in the 802.3 frame are filled, by the AP, from the fields of the 802.3 frame. The values of some fields are discarded.




**P15-10.** The following shows how the fields in the 802.11 frame are filled, by the AP, from the fields of the 802.3 frame. Some new pieces of information are also added that were not required in the 802.3 frame.



**P15-11.** To better understand the value of the NAV that needs to be set for each frame, we first show the time line for the transactions and the NAV (ignoring the propagation delay) in the following figure.




Based on the figure, we have the following NAV durations:

**a.** RST $= 4 + 40 + 4 + 3 \times 1 = 51$ μs.

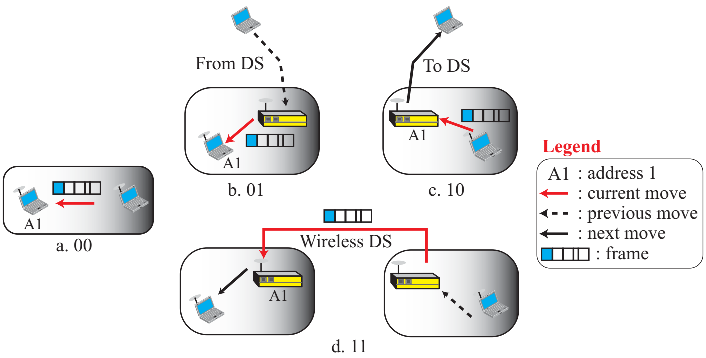
**b.** CST $= 40 + 4 + 2 \times 1 = 46$ μs.

**c.** Data $= 4 + 1 = 5$ μs.

**d.** ACK $= 0$ μs. After the ACK is transmitted, there is no need for channel reservation.

**P15-12.** Although station C cannot get the RTS frame, it can get the CTS frame that is sent by B. Since the RTS frame also sets the NAV duration in its D field, station C gets the news and refrains from accessing the channel.

**P15-13.** Address 1 in 802.11 always defines the destination address in the current movement of the frame in the wireless environment. The following figure shows address 1 in all four situations:



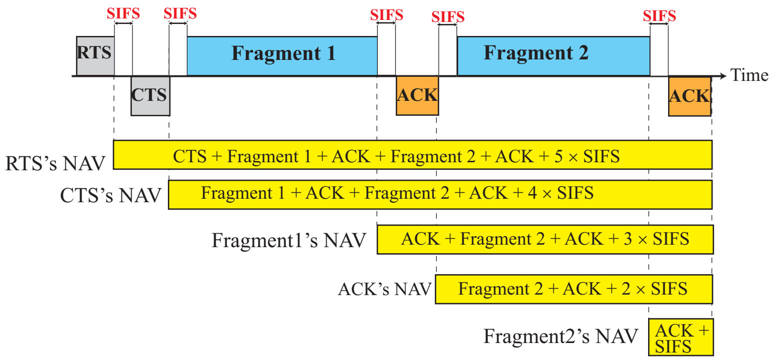

**a.** When both *To DS* and *From DS* bits are 0s, the communication is confined to the BSS. The frame has not entered the BSS before the current movement and will not leave the BSS after the current movement. We have an ad hoc network; the communication is between two stations, which means address 1 is the address of the destination host.

**b.** When *To DS* is 0 but *From DS* is 1, the frame is coming from a distribution system (DS). The frame has entered the BSS and is travelling from the AP to the destination station. Address1 is the address of the destination host.

**c.** When *To DS* is 1 but *From DS* is 0, the frame is going to a distribution system (DS). The frame is travelling inside the BSS, but is supposed to leave the AP and go to the DS. Address 1 is the address destination in the current move, which is the AP.

**d.** When both *To DS* and *From DS* bits are 1s, the frame is travelling in the DS itself, which is wireless. A frame is going from one AP in the source BSS to another AP in the destination BSS, but we are interested in the address field when the frame is travelling in the wireless DS. Address 1 is the address of the AP in the destination BSS.

**P15-14.** To better understand the value of the NAV that needs to be set for each frame, we first show the time line for the transactions and the NAV (ignoring the propagation delay) in the following figure.




Based on the figure, we have the following NAV durations

**a.** RST $= 4 + 20 + 4 + 20 + 4 + 5 \times 1 = 57$ µs.

**b.** CST $= 20 + 4 + 20 + 4 + 4 \times 1 = 52$ µs.

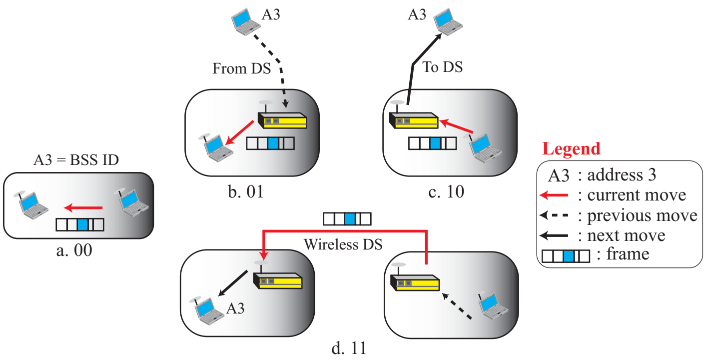
**c.** Fragment 1 $= 4 + 20 + 4 + 3 \times 1 = 31$ µs.

**d.** ACK $= 20 + 4 + 2 \times 1 = 26$ µs.

**e.** Fragment 2 $= 4 + 1 = 5$ µs.

**f.** ACK $= 0$ µs. After the second ACK is transmitted, there is no need for channel reservation.

**P15-15.** In 802.11, what address 3 defines depends on the type of the network. In an ad hoc, address 3 defines the BSS identification. In an infrastructure network, it either defines the address of the source in the previous move or the address of the destination in the next move, whichever is appropriate. The following figure shows address 3 in all four situations:



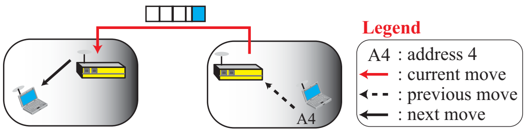

**a.** When both the *To DS* and *From DS* bits are 0s, the communication is confined to the BSS. The frame has not entered the BSS before the current movement and will not leave the BSS after the current movement. We have an ad hoc network; the communication is between two stations. Address 3 will set to the BSS ID to emphasize that the frame belongs to this BSS. Other BSSs that may accidentally receive the frame will discard it.

**b.** When *To DS* is 0 but *From DS* is 1, the frame is coming from a distribution system (DS). The frame has entered the BSS and is travelling from the AP to the destination station. Address 3 is the address of the device (station or router) that originally sent the 802.3 frame. This address is needed for the final destination in case a response is needed.

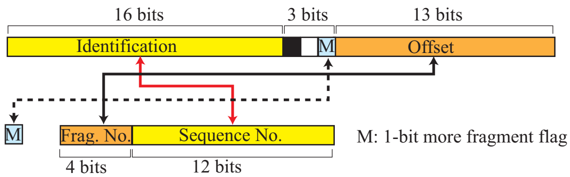
**c.** When *To DS* is 1 but *From DS* is 0, the frame is going to a distribution system (DS). The frame is travelling inside the BSS, but is supposed to leave the AP and go to the DS. Address 3 is the address of the device (host or router) in the DS. This address helps the AP to create an 802.3 frame to send to the DS.

**d.** When both the *To DS* and *From DS* bits are 1s, the frame is travelling in the DS itself, which is wireless. A frame is going from one AP in the source BSS to another AP in the destination BSS, but we are interested in the address field when the frame is travelling in the wireless DS. Address 3 is the address of the final destination host in the destination BSS. This address helps the AP to know the destination of the frame that will travel in the second BSS.

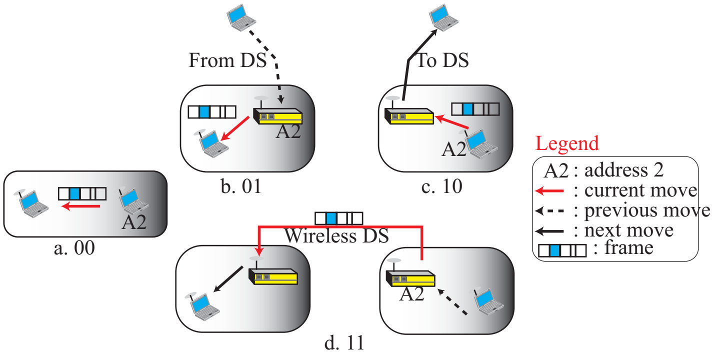
**P15-16.** Address 4 in an 802.11 network is used only in the last situation: when both the *To DS* and *From DS* bits are 1s. In this situation the frame is travelling in the DS itself, which is wireless. The value of address 4 defines the address of the original source in the original BSS that started the communication. This address is needed by the AP2 to be copied to the address 3 field when sending the frame in the next move (inside the destination BSS). The following figure shows the situation:




**P15-17.** IP uses three fields in the header for fragmentation: *identification* (16 bits), *flags* (3 bits), and *offset* (13 bits). The 802.11 protocol uses three subfields in the header for this purpose: *fragment number* (4 bits), *sequence number* (12 bits), and *more fragment* (1 bit). The *fragment number* and *sequence number* subfields are part of the *sequence control* (SC) field; the *more fragment* subfield is part of the *frame control* (FC) field. The following shows the relationship between the fields in the two protocols:



**P15-18.** Address 2 in 802.11 always defines the source address in the current movement of the frame in the wireless environment. The following figure shows address 2 in all four situations:




**a.** When both *To DS* and *From DS* bits are 0s, the communication is confined to the BSS. The frame has not entered the BSS before the current movement and will not leave the BSS after the current movement. We have an ad hoc network; the communication is between two stations, which means address 2 is the address of the source host.

**b.** When *To DS* is 0 but *From DS* is 1, the frame is coming from a distribution system (DS). The frame has entered the BSS and is travelling from the AP to the destination station. Address 2 is the address of the AP.

**c.** When *To DS* is 1 but *From DS* is 0, the frame is going to a distribution system (DS). The frame is travelling inside the BSS, but is supposed to leave the AP and go to the DS. Address 2 is the source address in the current move, which is the host.

**d.** When both *To DS* and *From DS* bits are 1s, the frame is travelling in the DS itself, which is wireless. A frame is going from one AP in the source BSS to another AP in the destination BSS, but we are interested in the address field when the frame is travelling in the wireless DS. Address 2 is the address of the AP in the source BSS.

**P15-19.** We describe the procedure for each station:

**a.** Station A wins the contention and can start using the channel.

**b.** Station B needs to wait four slots and test the channel again. If the channel is idle, it can use the channel; otherwise, it should start the procedure again.

**c.** Station C needs to wait 20 slots and test the channel again. If the channel is idle, it can use the channel; otherwise, it should start the procedure again.

**P15-20.** A BSSID identifies a BSS and distinguishes it from other BSSs. Its major benefit is to filter and distinguish frames sent through the air. Several BSSs may geographically overlap, which means a frame from one BSS may reach a station in another BSS. A station that receives a frame with a BSSID different from its own BSS should drop the frame. When a station joins the network, it gets the BSSID from the software and stores it.

**a.** In an ad hoc network, BSSID defines the BSS (it is used as address 3 in communication between stations).

**b.** In an infrastructure network, the BSSID is actually the MAC address of the AP. Since stations send frames (which are destined for DS) only to an AP and receive frames (which are coming from DS) only from an AP, the address of the AP is always included in message exchange as one of the addresses.

**P15-21.** The following shows the steps:

**a.** The host knows the IP address of its default router (address of interface m2). It may also know the MAC address of this interface (in its cache). Otherwise, the AP2 needs to send an ARP frame to discover. The host encapsulates its IP datagram in an 802.11 frame in which address 1 is the MAC address of the AP2 and address 2 is its own MAC address. Address 3 in this case is the MAC address of the router (interface m2). The frame is sent to the AP2.

**b.** The AP2 receives the frame and changes the frame format. It now creates an 802.3 frame in which the destination address is a copy of address 3 and the source address is a copy of address 2 (the original host).

**P15-22.** The sequence number in each fragment is the number used to glue the fragments together (it is the same in all fragments). The fragment numbers start from 0 and go to 3. The fragment flag is set in the first three fragments and is unset in the last. The following shows the field values (in binary as they appear in the frame):

| M | Fragment Number | Sequence Number |
|---|---|---|
| 1 | 0000 | 1100 1100 1001 |
| 1 | 0001 | 1100 1100 1001 |
| 1 | 0010 | 1100 1100 1001 |
| 0 | 0011 | 1100 1100 1001 |

**P15-23.** The address subfield in the header field is only 3 bits:

**a.** With a 3-bit address field, the address domain is in the range of 0 to 7.

**b.** Since the size of the address domain is only 8, we can have only 8 active stations in a Bluetooth network.