CHAPTER 11

IEEE 802.11 WLANs

11.1 INTRODUCTION

In this part of the book, we consider broadband local access using WLANs and WPANs. These are successful activities that were evolving outside of the voice-oriented 3G systems as broadband distribution systems for wireless local access. The last chapter provided an overview of the evolution of broadband wireless local access from the LAN industry and then the recent expansion to the home networking market. The following three chapters provide the detailed technical aspects of the important standards in broadband local access.

In the last chapter, we classified broadband local access systems into WLANs and WPANs. There are two camps in the WLAN standardization activities based on the orientation of their MAC layers. The IEEE 802.11 camp is a *connectionless* WLAN camp that evolved from data-oriented computer communications. Its counterpart is the HIPERLAN-2 camp that is more focused on *connection-based* WLANs addressing the needs of voice-oriented cellular telephony. The IEEE 802.11 has settled upon the MAC layer and is working on different physical layers to support higher data rates and today it holds the entire market. There are some activities addressing MAC enhancements in 802.11. The HIPERLAN-2 standard uses the same PHY layer as 802.11a with a MAC that supports the needs of the cellular telephone industry in supporting mechanisms for tariff, integration with existing cellular systems, and providing QoS. We present the IEEE 802.11 standard in this chapter and wireless ATM and HIPERLAN activities in the following chapter. The reader can refer to [CRO97], [STA01], [VAN99], [VAL98] for details on IEEE 802.11.

11.2 WHAT IS IEEE 802.11?

The IEEE 802.11 is the first WLAN standard and so far the only one that has secured a market. The IEEE 802.11 standardization activity originally started in 1987 as a part of the IEEE 802.4 token bus standard under the group number IEEE 802.4L. The IEEE 802.4 is a counterpart of the IEEE 802.3 and 802.5, which pays special attention in supporting factory environments. As we saw in the history of the WLANs in the last chapter, one of the early motives for using WLANs was in factories for control of and communication between equipment. For this reason, car manufacturers such as GM were actively participating in the IEEE 802.4L activities in the early days of this industry. In 1990 the 802.4L WLAN group was renamed as IEEE 802.11, an independent 802 standard, to define the PHY and MAC layers for WLANs. The first IEEE 802.11 standard for 1 and 2 Mbps, completed in 1997, supported DSSS, FHSS, and diffused infrared (DFIR) physical layers. Since completion of this first standard, new PHY layers supporting 11 Mbps using CCK (called IEEE 802.11b) and 54 Mbps using OFDM (called IEEE 802.11a) have been defined. All three versions share the same MAC layer that uses CSMA/CA for contention data, a request-to-send/clear-to-send (RTS/CTS) mechanism to accommodate the hidden terminal problem, and an optional mechanism called point coordination function (PCF) to support time-bounded applications. The IEEE 802.11

standard supports both infrastructure WLANs connecting through an AP and ad hoc operation allowing peer-to-peer communication between terminals.

The IEEE 802.11 standard was the first WLAN standard facing the challenge of organizing a systematic approach for defining a standard for wireless wideband local access. Compared with wired LANs, WLANs operate in a difficult medium for communication, and they need to support mobility and security. The wireless medium has serious bandwidth limitations and frequency regulations. It suffers from time and location dependent multipath fading. It is subject to interference from other WLANs as well as other radio and nonradio devices operating in the vicinity of a WLAN. Wireless standards need to have provisions to *support mobility* that is not shared in the other LAN standards. The IEEE 802.11 body had to examine connection management, link reliability management, and power management—none of which were concerns for other 802 standards. In addition, WLANs have no physical boundaries, and they overlap with each other, and therefore the standardization organization needed to define provisions for the *security* of the links. For all these reasons and because of several competing proposals, it took nearly 10 years for the development of IEEE 802.11 which was far longer than other 802 standards designed for wired mediums. Once the overall picture and the approach became clear, it only took a reasonable time to develop the IEEE 802.11b and IEEE 802.11a enhancements.

11.2.1 Overview of IEEE 802.11

To start a voice-oriented connection-based standard, such as GSM, the first step is to specify the services. Then the reference system architecture and its interfaces are defined, and at last the detailed layered interfaces are specified to accommodate all the services. The situation in connectionless data-oriented networks, such as IEEE 802.11, is quite different. The IEEE 802.11 standard provides for a general PHY and MAC layer specification that can accommodate any connectionless applications whose transport and network layers accommodate the IEEE 802.11 MAC layer. Today, TCP/IP is the dominant transport/network layer protocol hosting all popular connectionless applications such as Web access, e-mail, FTP, or telnet, and it works over all MAC layers of the LANs, including IEEE 802.11. Therefore, the IEEE 802.11 standard does not need to specify the services. However, IEEE 802.11 provides for local and privately owned WLANs with a number of competing solutions. In this situation, the first step in the standardization is to group all the solutions into one set of requirements with a reasonable number of options. The next step, in a manner similar to connection-based standards, is to define a reference system model and its associated detailed interface specifications.

11.2.1.1 Requirements

The number of participants in the IEEE 802.11 standards soon exceeded a hundred suggesting a number of alternative solutions. The finalized set of requirements, which did not came about easily, indicated that the standard should provide:

- Single MAC to support multiple PHY layers
- Mechanisms to allow multiple overlapping networks in the same area

- Provisions to handle the interference from other ISM band radios and microwave ovens
- Mechanism to handle "hidden terminals"
- Options to support time-bounded services
- Provisions to handle privacy and access control

In addition it was decided that the standard would not be concerned with licensed band operations. These requirements set the overall direction of the standard in adopting different alternatives. However, as it often happens in these types of standards, the actual adoptions were based on successful products that were already available in the market.

Example 11.1: Origins of PHY Layer Solutions

The DSSS solution for IEEE 802.11 is based on WaveLAN that was designed at NCR, Netherlands [TUCH91], [WOR91]. The FHSS solution was highly affected by RangeLAN designed by Proxim, CA, and products from Photonics, CA, and Spectrix, IL [SPECweb] affected the DFIR standard.

11.2.2 Reference Architecture

The reference model in connection-based WANs, such as GSM described in Chapter 7, contains a relatively sizable wired infrastructure with a number of hardware and software elements and many interfaces among all these elements. The connectionless IEEE 802.11 local network defines two topologies and several terminologies to start the standardization process. Figure 11.1 illustrates the infrastructure and ad hoc topologies that are the two configurations that the IEEE 802.11 standard considers. In the infrastructure configuration, wireless terminals are connected to a backbone network through APs. In the ad hoc configuration, terminals communicate in a peer-to-peer basis.

In IEEE 802.11 terminology the AP provides access to distribution services through the wireless medium. The *basic service area* (BSA) is the coverage area of one access point. The *basic service set* (BSS) is a set of stations controlled by one access point. The *distribution system* (DS) is the fixed (wired) infrastructure used to connect a set of BSS to create an *extended service set* (ESS). IEEE 802.11 also defines *portal(s)* as the logical point(s) at which non-802.11 packets enter an ESS.

In a typical application a number of laptops are connected through a WLAN to a backbone wired LAN. Each laptop carries a card and the connection point to the backbone is an AP with another card that forms a practical AP consisting of AP and a portal. Figure 11.2 illustrates this practical situation. The cards in the laptop and the AP support the MAC and PHY layers of the IEEE 802.11, the rest of the AP device acts as a bridge to convert the 802.11 protocol to MAC and the PHY layer of the backbone DS, that is typically an IEEE 802.3 Ethernet LAN. Laptops connect to the LAN through the AP to communicate with other devices, such as

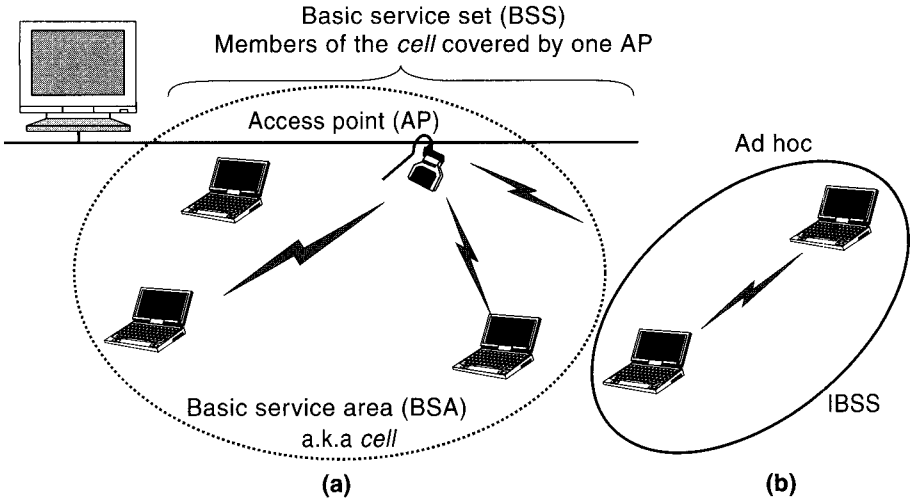


Figure 11.1 Reference model, terminologies, and topologies for the IEEE 802.11: (a) Infrastructure network and (b) ad hoc network.

the server shown in Figure 11.2. Typical ESS is formed by installing APs at different locations to connect to the backbone DS and cover the area.

11.2.3 Layered Protocol Architecture

Figure 11.3 shows the entities in the protocol stack of the IEEE 802.11 standard. The traditional simple MAC and PHY layers definitions in the IEEE 802 substandards are broken into other sublayers to make the specification process easier. The MAC layer is divided into MAC sublayer and MAC management sublayer entities.

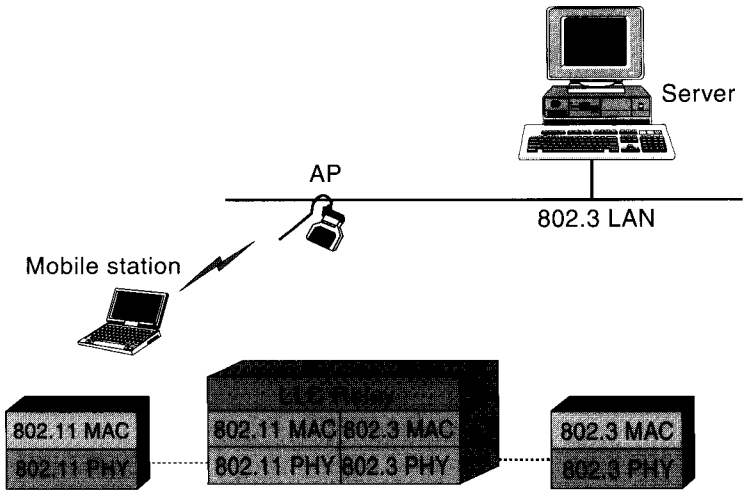


Figure 11.2 Practical implementation of an AP.

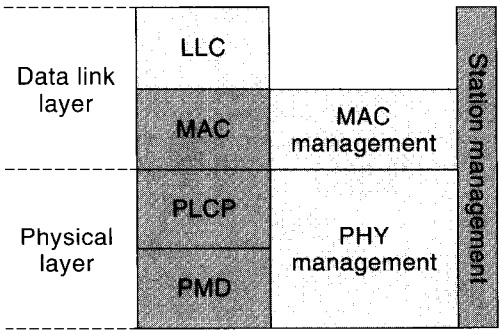


Figure 11.3 Protocol entities for the IEEE 802.11.

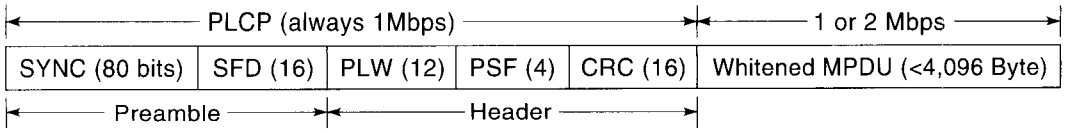
The *MAC* sublayer is responsible for access mechanism and fragmentation and reassembly of the packets. The *MAC layer management* sublayer is responsible for roaming in ESS, power management, and association, dissociation, and reassociation processes for registration connection management. The PHY layer is divided into three sublayers: PHY layer convergence protocol (PLCP), PHY medium dependent (PMD) protocol, and the PHY layer management sublayer. The *PLCP* is responsible for carrier sensing assessment and forming packets for different PHY layers. The *PMD* sublayer specifies the modulation and coding technique for signaling with the medium, and *PHY layer management* decides on channel tuning to different options for each PHY layer. In addition IEEE 802.11 specifies a *station management* sublayer that is responsible for coordination of the interactions between MAC and PHY layers.

11.3 THE PHY LAYER

When the MAC protocol data units (MPDU) arrive to the PLCP layer, a header is attached that is designed specifically for the PMD of the choice for transmission. The PLCP packet is then transmitted by PMD according to the specification of the signaling techniques. In the original IEEE 802.11, there are three choices of FHSS, DSSS, and DFIR for PMD transmission and therefore IEEE 802.11 defines three PLCP packet formats to prepare the MPDU for transmission. The rest of this section provides the details of the PMD, PLCP, and PHY layer management sublayers of all options for the IEEE 802.11 and IEEE 802.11b.

11.3.1 FHSS

Figure 11.4 shows the details of the PLCP header, which is added to the whitened MAC PDU to prepare it for transmission using FHSS physical layer specifications of the IEEE 802.11. There are two data rates for transmission of the information at



SYNC: Alternating 0,1
SFD: 0000110010111101
PLW: Packet length width
PSF: Data rate in 500 kbps steps
CRC: PLCP header coding

Figure 11.4 PLCP frame for the FHSS of the IEEE 802.11.

1 and 2 Mbps using two- and four-level GFSK modulation, respectively. The lower data rate always provides a simpler environment for synchronization between various adaptive parts of the receiver. Besides, with all packets starting with the same format, it is easier for the receiver to start a dialog with the transmitter. As a result, the PLCP header is always transmitted with the lower data rate of 1 Mbps using the simpler two-symbol GFSK modulation. In layman terms this allows a slower warm-up and initial negotiations for the receiver. The MPDU, however, is transmitted either by existing 1 or 2 Mbps transmission rate, or it can be at any other rate that may evolve in the future.

The PLCP additional bits consist of a preamble and a header. The *preamble* is a sequence of alternating 0 and 1 symbol for 80 bits that is used to extract the received clock for carrier and bit synchronization. The start of the frame delimiter (*SFD*) is a specific pattern of 16 bits, shown in the figure, indicating start of the frame. The next part of the PLCP is the header that has three fields. The 12-bit packet length width (PLW) field identifies the length of the packet that could be up to 4 kbytes. The 4 bits of the packet-signaling field (PSF) identifies the data rate in 0.5 Mbps steps starting with 1 Mbps.

Example 11.2: Specification of Data Rate on the Physical Layer

The existing 1 Mbps is represented by 0000 as the first step. The 2 Mbps by 0010 is 2×0.5 Mbps + 1 Mbps = 2 Mbps. The maximum 3-bit number represented by this system is 0111 that is associated with $7 \times 0.5+1 = 4.5$ Mbps. If all four bits are used, we have $15 \times 0.5+1 = 8.5$ Mbps. These limitations impose a need for changes in this field to accommodate next generation systems using data rates higher than 10 Mbps.

The rest of the rates are reserved for the future. The 16-bit CRC code is added to protect the PLCP bits. It can recover from errors of up to 2 bits, and otherwise identify whether the PLCP bits are corrupted. The total overhead of the PCLP is 16 bytes (128 bits) that is less than 0.4 percent of the maximum MPDU load, justifying the low impact of running the PCLP at lower data rates.

The FHSS PMD hops over 78 channels of 1 MHz each in the center of the 2.44 GHz ISM bands. The modulation technique is the GFSK that is described in Chapter 3. For 1 Mbps two levels and for 2 Mbps 4 levels of GFSK are employed.

Each BSS can select one of the three patterns of 26 hops given by (0,3,6,9,...,75), or (1,4,7,10,...,76) or (2,5,8,11,...,77) shown in Figure 11.5. The selection process is the responsibility of the PHY layer management sublayer. The IEEE 802.11 actually specifies specific random hopping patterns for each of these frequency groups that facilitates multivendor interpretability. Multiple BSSs can coexist in the same area by up to three APs using different frequency groups because these sets are nonoverlapping. In practice if three APs are installed next to one another in the same geographic area, we can provide a throughput of up to 6 Mbps. If APs use different frequency hopping patterns using CDMA in the same frequency group, the throughput can be increased substantially. The minimum hop rate of the IEEE 802.11 FHSS system is 2.5 hops per second, which is rather slow. The maximum recommended transmitted power is 100 mW.

The received MPDU is passed through a scrambler to be randomized. Randomization of the transmitted bits, which is also called whitening because the spectrum of a random signal is flat, eliminated the dc bias of the received signal. A scrambler is a simple shift register finite state machine with special feedback that is used both for scrambling and descrambling of the transmitted bits.

11.3.2 DSSS

The PMD of the DSSS version of the IEEE 802.11 uses a Barker code of length 11 that was described in Example 3.20. The reader should remember that the FHSS receiver is a narrowband receiver (1 MHz bandwidth) whose center frequency hops over 76 MHz, but DSSS communicates using nonoverlapping pulses at the chip rate of 11 Mcps which occupies around 26 MHz of bandwidth. The modulation techniques used for the 1 and 2 Mbps are DBPSK and DQPSK, respectively, which send one or two bits per transmitted symbol. The ISM band at 2.4 GHz is divided into 11 overlapping channels spaced by 5 MHz, shown in Figure 11.6, to provide several choices for coexisting networks in the same area. A PHY layer management sublayer of the AP covering a BSS can select one of the five choices according to the level of interference in different bands. The maximum transmitted power is the same as the FHSS and is recommended at 100mW. The FHSS is easier for implementation because the sampling rate is at the orders of the symbol rate of 1 Msps. The DSSS implementation requires sampling rates at the orders of 11 Mcps. Because of the wider bandwidth, DSSS provides a better coverage and a more stable signal.

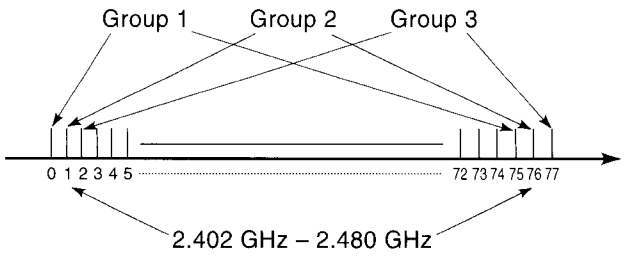


Figure 11.5 Three frequency groups for the FHSS in the IEEE 802.11.

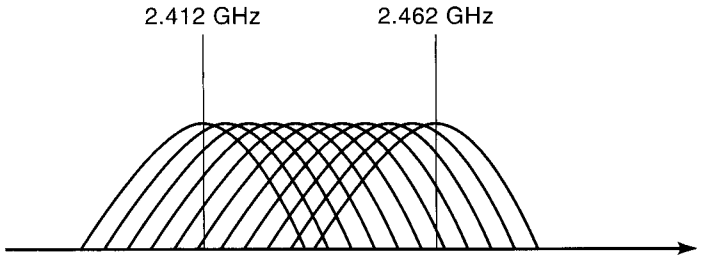
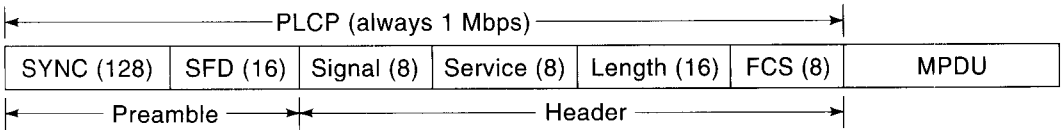


Figure 11.6 Overlapping frequency bands for the DSSS in the IEEE 802.11.

Figure 11.7 shows the details of the PLCP frame for the DSSS version of the IEEE 802.11. The overall format is similar to the FHSS, but the length of the fields is different because transmission techniques are different and different manufacturers designed the model product for development of the FHSS and DSSS standards. The MPDU from the MAC layer is transmitted either at 1 or 2 Mbps, however, analogous to the FHSS version of the standard, the PLCP of the DSSS version also uses the simpler BPSK modulation at 1 Mbps all the time. The MPDU for the DSSS does not need to be scrambled for whitening because each bit is transmitted as a set of random chips that is a whitened transmitted signal. The length of the SYNC in the DSSS is 128 bits that is longer than FHSS because DSSS needs a longer time to synchronize. The format of the SFD of the DSSS is identical to that of the FHSS but the value of the code, shown in Figure 11.7, is different. The PSF field of the FHSS is called *signal* field, and it uses 8 bits to identify data rates in steps of 100 kbps (five times more precision than FHSS).

Example 11.3: Frame Formats for Various Data Rates in IEEE 802.11

Using the above encoding, we represent 1 Mbps for DSSS by 00001010 (10 × 100 kbps), the 2 Mbps by 00010100 (20 × 100 kbps), and the 5.5 Mbps 11 and Mbps (used in IEEE 802.11b) by 001101110 (55 × 100 kbps) and 01101110 (110 × 100 kbps). The maximum number in this system is 11111111, which represents 255 × 100 kbps = 25.5 Mbps.



SYNC: Alternating 0,1
SFD: 1111001110100000
Signal: Data rate in 100 KHz steps
Service: Reserved for future use
Length: Length of MPDU in microsecond
FCS: PLCP header coding

Figure 11.7 PLCP frame for the DSSS of the IEEE 802.11.

The *service* field in the DSSS is reserved for future use, and it does not exist in the FHSS version. The *length* field of the DSSS is analogous to the PLW in the FHSS, however, length field of DSSS specifies the length of the MPDU in microseconds. The frame correction sequence (*FCS*) field of the DSSS is identical to the CRC field of the FHSS.

11.3.3 DFIR

The PMD of DFIR operates based on transmission of 250 ns pulses that are generated by switching the transmitter LEDs on and off for the duration of the pulse. Figure 11.8 illustrates the 16-PPM and 4-PPM modulation techniques recommended by the IEEE 802.11 for 1 and 2 Mbps, respectively. In the 16-PPM, blocks of 4 bits of the information are coded to occupy one of the 16 slots of a 16-bit length sequence according to their value. In this format each 16 × 250 ns = 4,000 ns carries 4 bits of information that supports a 4 bits/4,000 ns = 1 Mbps transmission rate. For the 2 Mbps version, every 2 bits are PPM-modulated into 4 slots of duration 4 × 250 ns = 1,000 ns that generates data at 2 bits/1,000 ns = 2 Mbps. The peak transmitted optical power is specified at 2W with an average of 125 or 250 mW. The wavelength of the light is specified at 850 nm to 950 nm.

The PLCP packet format for the DFIR is shown in Figure 11.9. The PLCP signals are shown in the unit of slots of 250 ns for one basic pulse. The synch and SDF fields are shorter than FHSS and DSSS because noncoherent detection using photosensitive diode detectors do not need carrier recovery or elaborate random code synchronizations. The three-slot data rate indication field starts by 000 for 1 Mbps and 001 for 2 Mbps. The length and FCS are identical to the DSSS. The only new field is the DC level adjustment (DCLA) that sends a sequence of 32 slots, al-

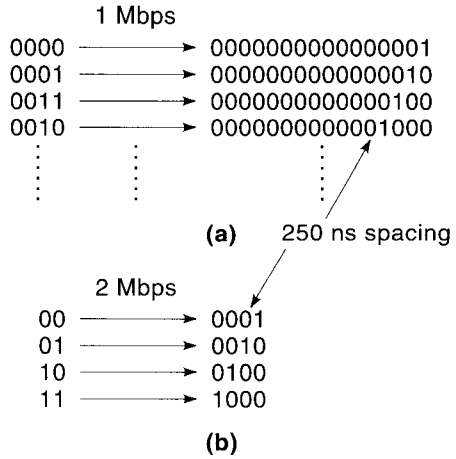
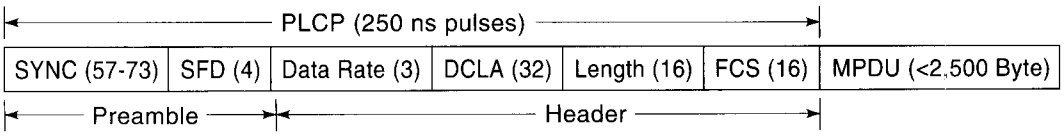


Figure 11.8 PPM using 250 ns pulses in the DFIR version of the IEEE 802.11: (a) 16 PPM for 1 Mbps and (b) 4 PPM for 2 Mbps.



SYNC: Alternating 0,1 pulses
SFD: 1001
Data rate: 000 and 001 for
DCLA: DC level adjustments sequences
Length: Length of MPDU in microsecond
FCS: PLCP header coding

Figure 11.9 PLCP frame for the DFIR of the IEEE 802.11.

lowing the receiver to set its level of the received signal to set threshold for deciding between received zeros and 1s. The MPDU length is restricted to 2,500 bytes.

11.3.4 IEEE 802.11a, b

The PHY layer of the IEEE 802.11a is based on an OFDM transmission that operates in the 5 GHz U-NII bands. The principle of operation of OFDM was discussed in Chapter 3. The specifics of the IEEE 802.11a OFDM system are shared with the HIPERLAN-2 standard, and we provide it in the next chapter. The IEEE 802.11a and b MAC layer remains the same as that of the other IEEE 802.11 standards.

At 2.4 GHz, the IEEE 802.11b standard specifies a new PHY layer, called CCK, to support data rates of 5.5 and 11 Mbps. The IEEE 802.11b uses the same PLCP as the IEEE 802.11 DSSS standard. The principles of operation of the CCK were provided in Chapter 3. There are several unique features for the IEEE 802.11b that are worth mentioning. The IEEE 802.11b uses Walsh codes with complementary codes for M-ary orthogonal data transmission. This scheme interoperates with existing 1 and 2 Mbps networks using the same preamble and header. Therefore, it can be easily integrated in the existing IEEE 802.11 DSSS modems.

In the CCK method described in Example 3.17, we explained that the CCK maps blocks of eight bits of the incoming data into blocks of eight-QPSK complex symbols to derive an 11 Mbps data transmission system with the same chip transmission rate of the 11 Mcps. This mapping was explained to be performed by a CCK encoder that uses the 8-bit input block as the address of one of the 256 orthogonal eight-QPSK symbol sequence to be transmitted. The transformation that makes this mapping possible was given by

$$c = \{e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, -e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j(\varphi_1)}\} \tag{11.1}$$

where $(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ are four phases associated with the eight-bit arriving block with each two bits combined in a four-phase complex number. After finding four complex phases associated to an eight-bit arriving block, we replace them in the earlier

equation to obtain one of the 256 complex orthogonal CCK codes. All the terms of the earlier equation share the first phase; if we factor that out we have

$$c = \{e^{j(\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_3+\varphi_4)}, e^{j(\varphi_2+\varphi_4)}, -e^{j(\varphi_4)}, e^{j(\varphi_2+\varphi_3)}, e^{j(\varphi_3)}, -e^{j(\varphi_2)}, 1\}e^{j(\varphi_1)} \quad (11.2)$$

This change suggests that our 256 transformation matrix can be decomposed into two transformations, one a unity transformation that maps two bits (one complex phase) directly and the other one that maps six bits (three phases) into an 8-element complex vector with 64 possibilities determined by the inner function of the above equation. The above decomposition leads to a simplified implementation of the CCK system that is shown in the Figure 11.10. At the transmitter the serial data in multiplied into 8-bit addresses. Six of the eight bits are used to select one of the 64 orthogonal codes produced as one of the 8-complex code, and two bits are directly modulated over all elements of the code that are transmitted sequentially. The receiver is actually comprised of two parts: one the standard IEEE 802.11 DSSS decoder using Barker codes and one a decoder with 64 correlators for the orthogonal codes and an ordinary demodulator for IEEE 802.11b. By checking the PLCP data rate, the field receiver knows which decoder should be employed for the received packets. This scheme provides an environment for implementation of a WLAN that accommodates both 802.11 and 802.11b devices.

The IEEE 802.11b also supports 5.5 Mbps as a backup for the 11Mbps operation. Figure 11.11 shows the format of the bits for both data rates. In the 5.5 Mbps mode, blocks of four bits, rather than eight bits, are used for multiplexing, and two of the four bits are used to select one of the four possible complex orthogonal vectors.

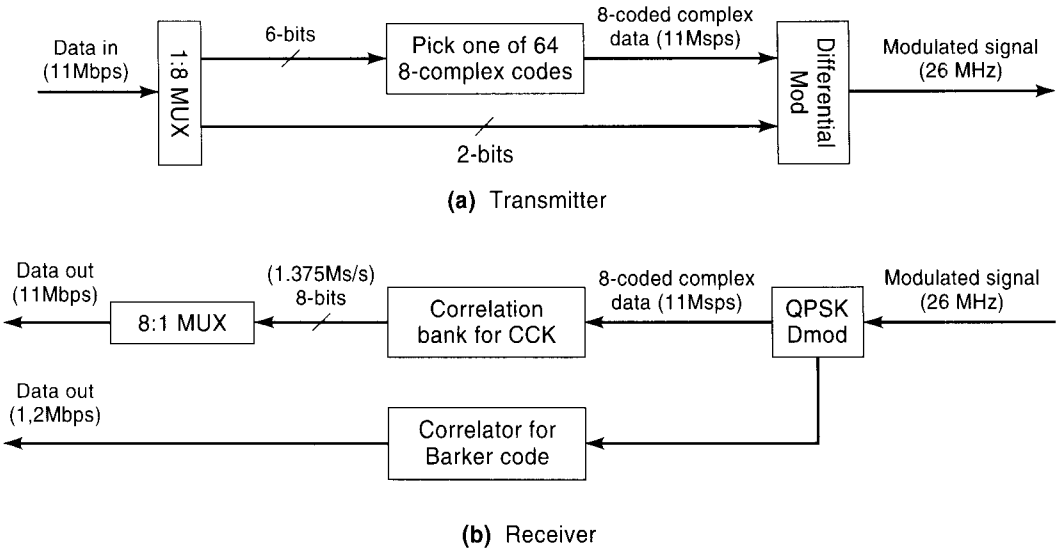


Figure 11.10 Simplified implementation of the CCK for IEEE 802.11b.

$$c = \{e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}\, e^{j(\varphi_1+\varphi_3+\varphi_4)},\ e^{j(\varphi_1+\varphi_2+\varphi_4)},\ -e^{j(\varphi_1+\varphi_4)},\ e^{j(\varphi_1+\varphi_2+\varphi_3)}\, e^{j(\varphi_1\varphi_3)},\ -e^{j(\varphi_1+\varphi_2)},\ e^{j\varphi_1}\}$$

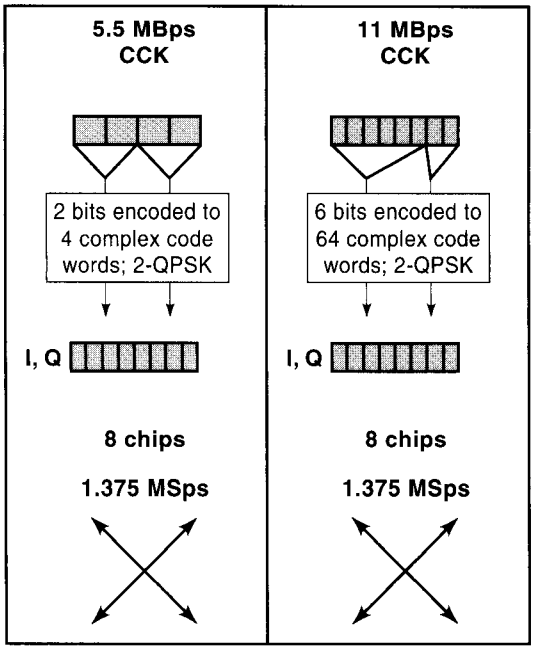


Figure 11.11 Multiplexing of the input data for 5.5 and 11 Mbps IEEE 802.11b systems.

11.3.5 Carrier Sensing

In IEEE 802.3 sensing the channel is very simple. The receiver reads the peak voltage on the wire of cable and compares it against a threshold. In the IEEE 802.11, the sensing mechanism is more complicated, and it is performed either physically or virtually. The PHY sensing is through the clear channel assessment (CCA) signal produced by PLCP in the PHY layer of the IEEE 802.11. The CCA is generated based on "real" sensing of the air-interface either by sensing the detected bits in the air or by checking the RSS of the carrier against a threshold. Decisions based on the detected bits are made slightly slower, but they are more reliable. Decisions based on the RSS may create a false alarm caused by measuring the level of the interference. The best designs take advantage of both carrier sensing and detected data sensing. In addition to PHY sensing, the IEEE 802.11 also provides for the virtual carrier sensing. Virtual carrier sensing is based on a network allocation vector (NAV) signal supported by the RTS/CTS and PCF mechanisms in the MAC layer. In either of these MAC operations, the system allows generation of a NAV signal that acts like a sensed channel to prevent transmission of contention data for a preset duration of time. A "length" field in the MAC layer is used to specify the amount of time that must elapse before the medium can be freed.

11.4 MAC SUBLAYER

The overall MAC layer responsibilities are divided between MAC sublayer and MAC layer management sublayer. The major responsibilities of the MAC sublayer are to define the access mechanisms and packet formats. The MAC management sublayer defines roaming support in the ESS, power management, and security.

The IEEE 802.11 specifies three access mechanisms that support both contention and contention-free access. The contention mechanism is supported by CSMA/CA protocol that was explained in the Example 4.18. There are two cases for contention-free transmission. The first case is the RTS/CTS, discussed in Section 4.3, which is used to solve the hidden terminal problem. The second case is the implementation of the PCF for time-bounded information.

To allow coordination of a number of options for the MAC operations, IEEE 802.11 recommends three inter-frame spacings (IFSs) between the transmissions of the packets. These IFS periods provide a mechanism for assigning priority that is then used for implementation of QoS support for time-bounded or other applications. After completion of each transmission, all terminals having information packets wait for one of the three IFS periods according to the level of priority of their information packet. These interframing intervals are DCF-IFS (DIFS) used for contention data spacing that has the lowest priority and longest duration. Short IFS (SIFS), used for highest priority packets such as ACK and CTS (clear to send), has the lowest duration of time. The PCF IFS (PIFS), designed for PCF operation, has the second priority rate with a duration between DIFS and SIFS.

In CSMA/CA, as soon as the MAC has a packet to transmit, it senses the channel to see if the channel is available both physically and virtually. If the channel is virtually busy because a NAV signal is turned on, the operation is delayed until the NAV signal has disappeared. When the channel is virtually available, the MAC layer senses the PHY condition of the channel. If the channel is idle, as shown in Figure 11.12, the terminal waits for a DIFS period and transmits the data. If the channel is sensed busy, MAC runs a random number generator to set a *backoff* clock. During the transmission of the packet and its associated DIFS, contention is differed but sensing continues. When the channel becomes available, as shown in Figure 11.12, a contention window start in which all terminals having packets for transmission run down their *backoff* clocks. The first terminal that expires its clock starts transmission. Other terminals sense the new transmission and freeze their clock to be restarted after the completion of the current transmission in the next contention period. This mechanism reduces the collisions, but it cannot

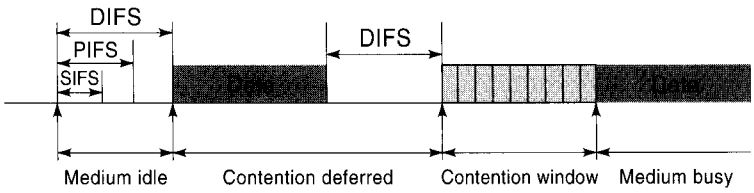


Figure 11.12 Primary operation of the CSMA/CA in the IEEE 802.11.

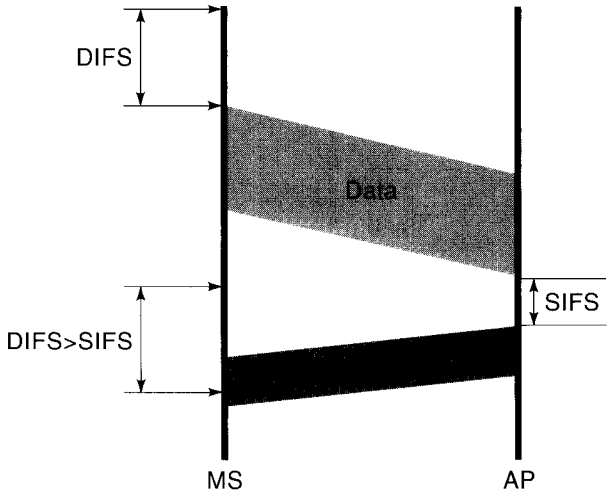


Figure 11.13 Implementation of the CSMA/CA with ACK in an infrastructure network.

eliminate it. To reduce the probability of repeated collisions, in a manner similar to IEEE 802.3 described in Example 4.17, the length of backoff time is exponentially increased as the terminal goes through successive retransmissions.

The IEEE 802.11 recommends both CSMA/CA based on the clear channel assignment signal from the PHY layer and CSMA/CA with ACK for MAC recovery. Note that Ethernet does not provide for MAC recovery, and this feature is unique to the IEEE 802.11. Figure 11.13 illustrated a sample operation of the CSMA/CA with ACK in a communication between a terminal and an AP. When the AP receives a packet of data, it waits for a SIFS and sends the ACK. Because SIFS is smaller than DIFS, all the other terminals must wait until transmission of the ACK to the MS is completed. The CSMA with ACK is not implemented on most of the IEEE 802.11 products, and ACK is left for other layers of the protocol that are implemented on software.

In the RTS/CTS mechanism in the IEEE 802.11 MAC sublayer, shown in Figure 11.14, a terminal ready for transmission sends a short RTS packet (20 bytes) identifying the source address, destination address, and the length of the data to be transmitted. The destination station will respond with a CTS packet (16 bytes) after a SIFS period. The source terminal receives the CTS and sends the data after another SIFS. The destination terminal sends an ACK after another SIFS period. Other terminals hearing RTS/CTS that is not addressed to them will go to the virtual carrier-sensing mode for the entire period identified in the RTS/CTS communication, by setting their NAV signal on. Therefore, the source terminal sends its packet with no contention. After completion of the transmission, the destination terminal sends an acknowledgment packet, and the NAV signal is terminated, opening the contention for other users. This method provides a unique access right to a terminal to transmit without any contention. It helps in the situations when a terminal with low received power at the AP is shadowed with terminals with much higher received power.

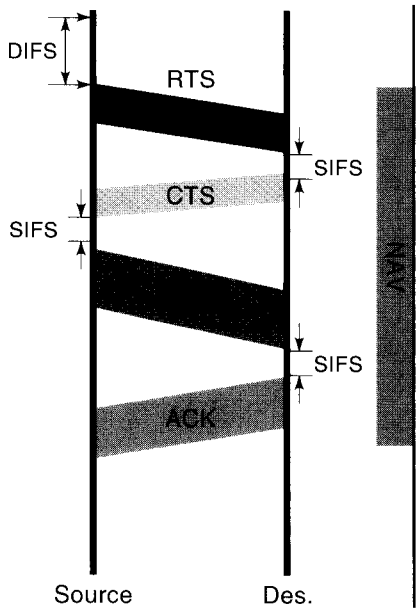


Figure 11.14 Implementation of the RTS/CTS mechanisms in the IEEE 802.11.

The PCF mechanism in the IEEE 802.11 MAC sublayer, shown in Figure 11.15, is built on top of the DCF using CSMA to support contention-free time bounded and asynchronous transmission operations. This is another optional MAC service that has complicated the MAC layer, and all manufacturers have not chosen to implement it in their products. In the PCF operation, only available for

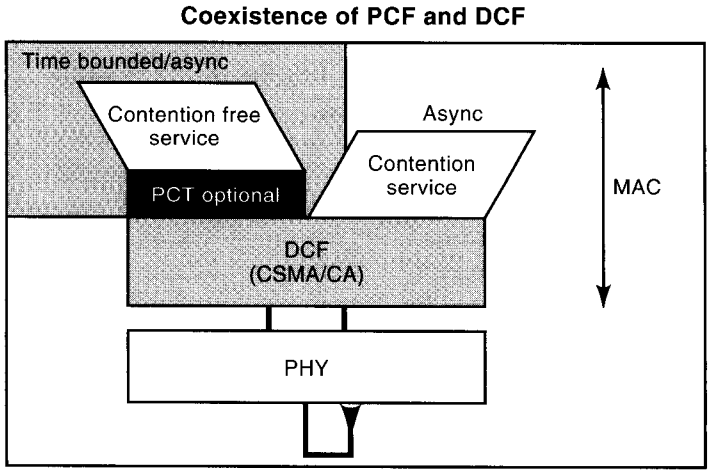


Figure 11.15 Implementation PCF on top of the DCF in the IEEE 802.11.

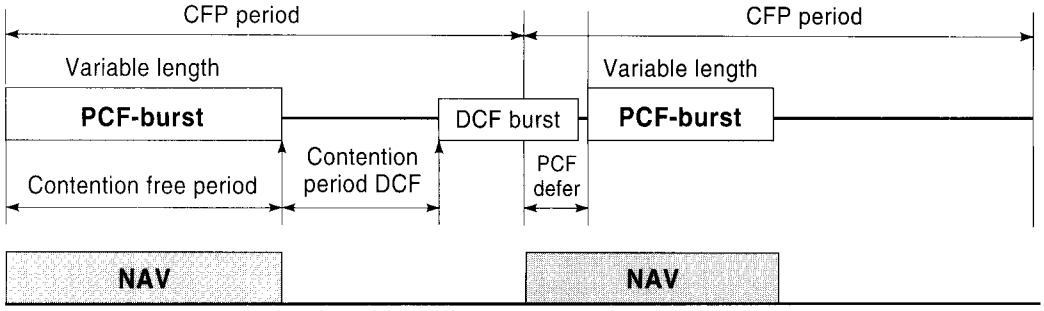


Figure 11.16 Alternation of contention-free and contention periods under PCF control from AP.

infrastructure networks, the AP takes charge of the operation to provide the service to all terminals involved. The AP, playing the point coordinator, stops all other terminals and polls other stations in a semiperiodic manner. Figure 11.16 illustrates the operation of the PCF. The AP organizes a periodical contention-free period (CFP) for the time-bounded information. It coordinates time-bounded data to be transmitted at the beginning of each CFP, and during those periods it arranges an NAV signal for all other terminals. The length of the PCF period is variable, and it only occupies a portion of the CFP. The rest of the CFP is released for contention and DCF packets. If a DCF packet occupies the channel and does not complete before the start of the next CFP, the starting time of the CFP will defer (see Fig. 11.16). However, the NAV signal for all other terminals goes to operation at the beginning of the CFP.

11.4.1 General MAC Frame Format

To discuss the packet format, it is instructional to start with the IEEE 802.3 Ethernet packet format. The original Ethernet standard defines only one frame format shown in Figure 11.17. The control and management in the network are so simple that one frame format accommodates the entire operation of the network. Each packet starts with a preamble, alternating 1 and 0 values that are used for synchronization. An SFD sequence of eight bits having the bit configuration 10101011 indicates the start of the frame. The destination address (DA) and source address (SA) for the MAC are either two bytes or six bytes but are practically always implemented in six bytes. A length-field indicates the number of bytes in the subsequent MAC client data field. The MAC client data field and a pad field contain the data transferred from the source station to bring the frame size up to the minimum length for carrier sensing. The last field is the frame check sequence, which contains a 4-byte CRC for error checking. As we saw earlier in this section, in the IEEE 802.11 the preamble, SFD, and the length of the packet fields were defined

Preamble (7)	Start delimiter (1)	DA (2 or 6)	SA (2 or 6)	Length of data (2)	Data (0–1500)	Pad (0–46)	Checksum (4)

Figure 11.17 Frame format of the IEEE 802.3 Ethernet.

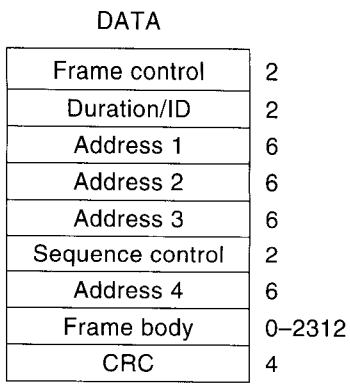
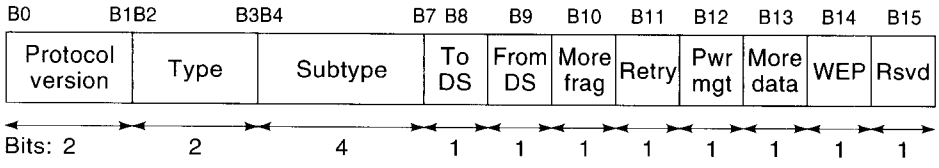


Figure 11.18 General MAC frame format of the IEEE 802.11.

in the PLCP of the PHY layer packet format. Therefore the MAC frame format of the 802.11 is equivalent to the remaining five fields of the 802.3 handling addressing, MAC client data, and MAC error correcting bits. The 802.11 frame format is much more complicated than 802.3 because it should also accommodate a number of management and control packets.

Figure 11.18 shows the general MAC frame format of the IEEE 802.11. It starts with the *frame control* field. This field carries instructions on the nature of the packet. It distinguishes data from control and management frame and specifies the type of control or management signaling that the packet is meant to do. The details of frame control and its format are shown in Figure 11.19. The *duration/ID* field is used to identify the length of the fragmented packets to follow. The four *address fields* in the 802.11 frame format, rather than two in the 802.3, identify the source, destination, and APs that they are connected to which are identified by a six-byte (48-bit) Ethernet-like address. The *sequence control* is used for fragmenta-



Protocol version: currently 00, other options reserved for future
To DS/from DS; "1" for communication between two APs
More fragmentation: "1" if another section of a fragment follows
Retry: "1" if packet is retransmitted
Power management: "1" if station is in sleep mode
Wave data: "1" more packets to the terminal in power-save mode
Wired equivalent privacy: "1" data bits are encrypted

Figure 11.19 Details of the frame control field in the MAC header of the IEEE 802.11.

tion numbering to control the sequencing. The sequence control and duration/ID are only available in the 802.11 to support fragmentation and the reassembly feature of the MAC protocol. The *frame body* of the 802.11 contains 0–2,312 bytes as compared with 802.3 that have 46–1,500 bytes. Similar to the IEEE 802.3, the IEEE 802.11 uses a four-byte CRC for protection of the MAC client information. Note that we had shorter CRC codes in PLCP that were used to protect the PLCL header.

Example 11.4: Packet Formats

Figure 11.20 shows three examples of the short packets RTS, CTS, and ACK. Not all the fields are included in all packets. But the general format follows the same pattern.

11.4.2 Control Field in MAC Frames

Compared with Ethernet, IEEE 802.11 is a wireless network that needs to have control and management signaling to handle registration process, mobility management, power management, and security. To implement these features, the frame format of the 802.11 should accommodate a number of instructing packets, similar to those we described in WANs. The capability of implementing these instructions is embedded in the control field of the MAC frames. Figure 11.20 shows the overall format of the control field in the 802.11 MAC frame with description of all fields except type and subtype. These two fields are very important because they specify

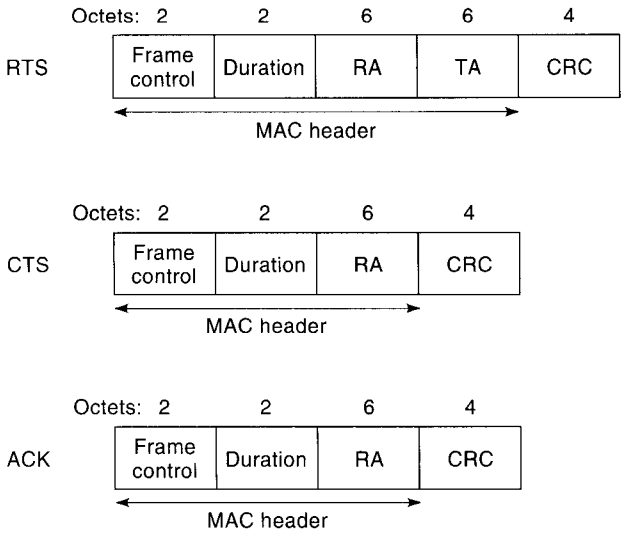


Figure 11.20 Details of the frame control field in the MAC header of the IEEE 802.11.

Table 11.1. Type and Subtype Fields and Their Associated Instructions

- Management Type (00)
  - Association Request/Response (0000/0001)
  - Reassociation Request/Response (0010/0011)
  - Probe-Request/Response (0100/0101)
  - Beacon (1000)
  - ATIM: Announcement Traffic Indication Map (1001)
  - Dissociation (1010)
  - Authentication/Deauthentication (1011/1100)
- Control Type (01)
  - Power Save Poll (1010)
  - RTS/CTS (1011/1100)
  - ACK (1101)
  - CF End/CF End with ACK (1110/1111)
- Data Type (10)
  - Data/Data with CF ACK/No Data (0000/0001)
  - Data Poll with CF/Data Poll with CF and ACK (0010/0011)
  - No Data/CF ACK (0100/0101)
  - CF Poll/CF Poll ACK (0101/0110)

various instructions for using the packet. The 2-bit *type* field specifies four options for the frame type:

- Management Frame (00)
- Control Frame (01)
- Data Frame (10)
- Unspecified (11)

The four-bit *subtype* provides an opportunity to define up to 16 instructions for each type of frame. Table 11.1 shows all used six bits for the type and subtypes in the frame control field. Combinations that are not used provide an opportunity to incorporate new features in the future.

11.5 MAC MANAGEMENT SUBLAYER

The MAC management sublayer handles establishment of communications between stations and APs. This layer handles the mechanisms required for a mobile environment. The same issues that exist in other wireless systems exist here to a large extent. In general, a MAC management frame has the format shown in Figure 11.21. A variety of MAC management frames are used for different purposes.

11.5.1 Registration

The *beacon* is a management frame that is transmitted quasi-periodically by the AP to establish the timing synchronization function (TSF). It contains information such as the BSS-ID, timestamp (for synchronization), traffic indication map (for sleep mode), power management, and roaming. RSS measurements are made on the beacon message. The beacon is used to identify the AP, the network, and so on.

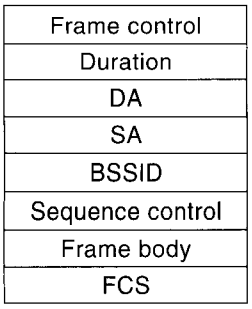


Figure 11.21 MAC management frame format.

In order to deliver a frame to an MS, the distribution system must know which AP is serving the MS. *Association* is a procedure by which an MS "registers" with an AP. Only after association can an MS send or receive packets through an AP. How the association information is maintained in the distribution system is *not* specified by the standard. An MS sends the *association request* frame to the AP if it wants to associate with the AP. The AP grants permission to the MS via an *association response* frame. MAC management frames similar to these two frames are made use of in handoff.

11.5.2 Handoff

There are three mobility types in IEEE 802.11. The "no transition" type implies that the MS is static or moving within a BSA. A "BSS transition" indicates that the MS moves from one BSS to another within the same ESS. The most general form of mobility is "ESS transition" when the MS moves from one BSS to another BSS that is part of a new ESS. In this case upper layer connections may break (it will need a mobile IP for continuous connection).

The *reassociation* service is used when an MS moves from one BSS to another within the same ESS. The MS always initiates it, and it enables the distribution system to recognize the fact that the MS has moved its association from one AP to another. The *dissociation* service is used to terminate an association. It may be invoked by either party of an association (the AP or the MS), and it is a notification and not a request. It cannot be refused. MSs leaving a BSS will send a dissociation message to the AP that need not be always received.

The handoff procedures in a WLAN are as shown in Figure 11.22. The AP broadcasts a beacon signal periodically (typically the period is around 100 ms). An MS that powers on scans the beacon signal and *associates* itself with the AP with the strongest beacon. The beacon contains information corresponding to the AP such as a timestamp, beacon interval, capabilities, ESS ID, and traffic indication map (TIM). The MS uses the information in the beacon to distinguish between different APs.

The MS keeps track of the RSS of the beacon of the AP with which it is associated, and when the RSS becomes weak, it starts to scan for stronger beacons from neighboring APs. The scanning process can be either active or passive. In passive scanning, the MS simply listens to available beacons. In active scanning, the MS

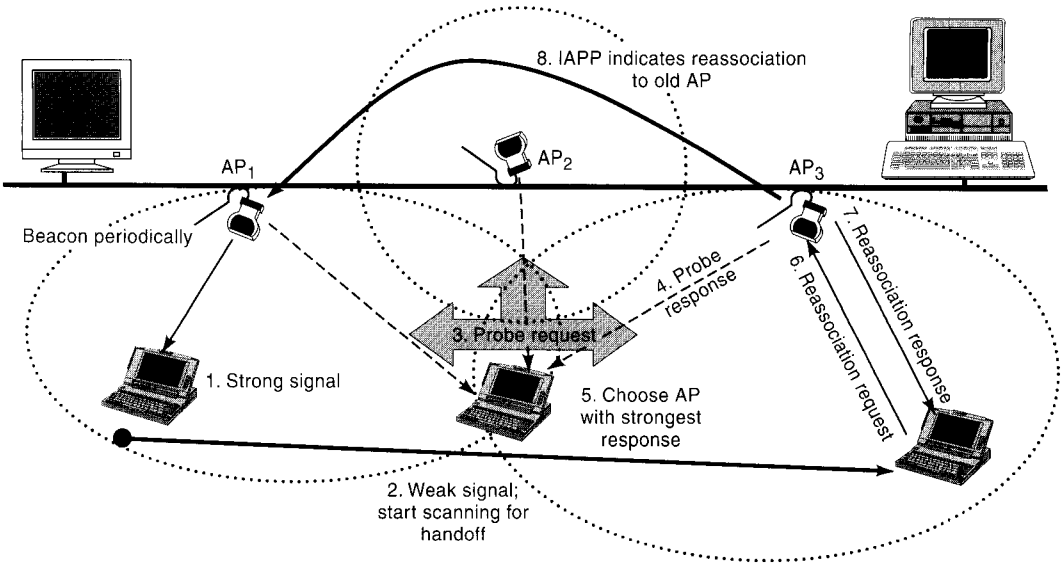


Figure 11.22 Handoff procedure in IEEE 802.11.

sends a probe request to a targeted set of APs that are capable of receiving its probe. Each AP that receives the probe responds with a probe response that contains the same information that is available in a regular beacon with the exception of the TIM. The probe response thus serves as a "solicited beacon." The mobile chooses the AP with the strongest beacon or probe response and sends a *reassociation request* to the new AP. The reassociation requests contains information about the MS as well as the old AP. In response, the new AP sends a *reassociation response* that has information about the supported bit rates, station ID, and so on needed to resume communication. The old AP is not informed by the MS about the change of location. So far, each WLAN vendor had some form of proprietary implementation of the emerging IAPP (inter-access point protocol) standard for completing the last stage of the handoff procedure (intimating the old AP about the mobile host's change of location). The IAPP protocol employs two PDUs to indicate that a handoff has taken place. These PDUs are transferred over the wired network from the new AP to the old AP using UDP-IP (Figure 11.23). If the AP does not have an IP address, an 802.11 subnetwork access protocol (SNAP) is employed for transferring the PDUs. IAPP is also used to announce the existence of APs and to create a database of APs within each AP.

11.5.3 Power Management

The power conservation problem in WLANs is that stations receive data in bursts but remain in an idle receive state constantly, which dominates the LAN adaptor power consumption. The challenge is how we can power off during the idle periods and maintain the session. The IEEE 802.11 solution is to put the MS in sleeping

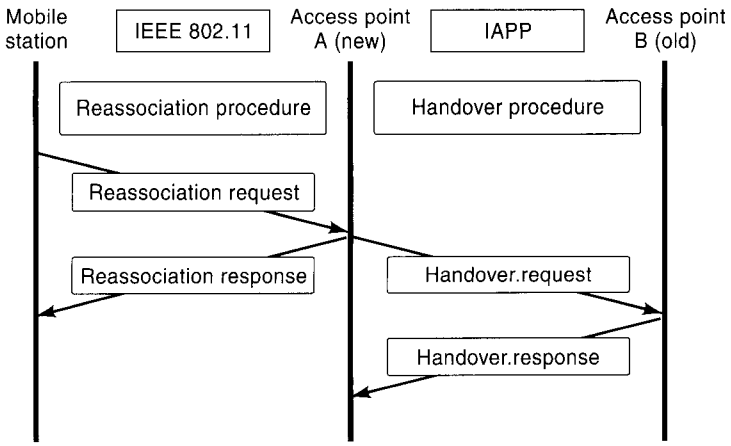


Figure 11.23 Role of IAPP in handoff.

mode, buffer the data at AP, and send the data when the MS is awakened. Compared with the continuous power control in cellular telephones, this is a solution tailored for bursty data applications.

Since using TSF, all MSs are synchronized, and they will wake up at the same time to listen to the beacon (see Fig. 11.24). MS uses the power-management bit in the frame control field to announce its sleep/awake mode. With every beacon a TIM is sent that has the list of stations having buffered data. The MS learns that it has a buffered data by checking beacon and TIM. The MS with buffered data sends a power-save poll to AP. The AP sends the buffered data when the station is in active mode.

11.5.4 Security

There are provisions for authentication and privacy in IEEE 802.11. There are two types of *authentication* schemes in IEEE 802.11. The open system authentication is the default. Here the request frame sends the authentication algorithm ID for "open system." The response frame sends the results of request. The shared key authentication provides a greater amount of security. The request frame sends the authentication frame ID for the "shared key" using a 40-bit secret code that is shared between itself and the AP. The second station sends a challenge text (128 bytes). The first station sends the encrypted challenged text as the response. The

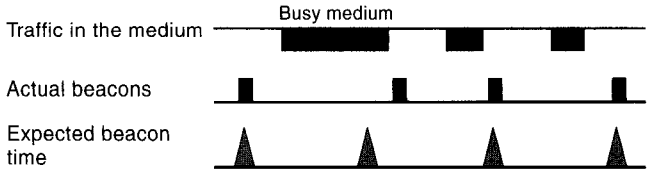


Figure 11.24 Listening to the beacon for power management.

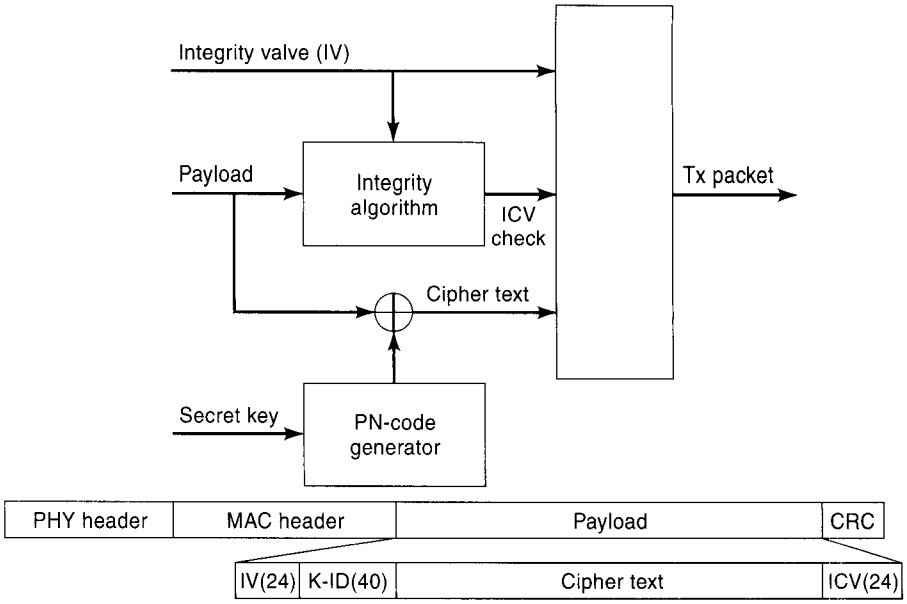


Figure 11.25 Privacy in IEEE 802.11.

second station sends the authentication results. This is exactly like the challenge response identification protocols discussed in Chapter 6. Note that the 40-bit key provides very little security. The secret key algorithm usually employed in all systems is RC-4, although some products employ DES. *Privacy* can also be maintained in IEEE 802.11 via the wired-equivalent privacy (WEP) specification. A pseudorandom generator is used (see Fig. 11.25) along with the 40-bit secret key to create a key sequence that is simply XOR-ed with the plaintext message. This offers very little security and is quite susceptible to planned attacks.

QUESTIONS

11.1 Name four major transmission techniques considered for WLAN standards and give the standard activity associated with each of them.

11.2 Compare OFDM and spread spectrum technology for the WLAN application.

11.3 Give the physical specification summary of the DSSS and FHSS used by the IEEE 802.11.

11.4 What are the MAC services of IEEE 802.11 that are not provided in the traditional LANs such as 802.3?

11.5 Why does the MAC layer of the 802.11 have four address fields, compared with 802.3, which has two?

11.6 What is the PCF in 802.11, what services does it provide, and how is it implemented?

11.7 What is the RTS/CTS in 802.11, what services does it provide, and how is it implemented?

11.8 What is the difference between an ESS and a BSS in the IEEE 802.11?

11.9 Explain why an AP in the 802.11 also acts as a bridge.

11.10 What are the differences between carrier sensing in the 802.11 and 802.3?

11.11 What are the responsibilities of the MAC management sublayer in 802.11?

11.12 What is the difference between the backoff algorithms in the 802.11 and 802.3?

11.13 What is the purpose of PIF, DIF, and SIF time intervals and how are they used in the IEEE 802.11?

11.14 Why do we have four addressing slots in the 802.11 MAC and only two in the 802.3?

11.15 What is the 802.11 MAC frame that has the type/subtype frame control code of 001000? What are its responsibilities?

11.16 What is the difference between a probe and a beacon signal in 802.11?

11.17 Explain how the timing of the beacon signal in 802.11 operates.

11.18 What is the difference between power control in 802.11 and power control in cellular systems?

11.19 What was the mission of the IAPP group?

PROBLEMS

11.1 The original WaveLAN, the basis for the IEEE 802.11, uses an 11-bit Barker code of $[1,-1,1,1,-1,1,1,1,-1,-1,-1]$ for DSSS.

a. Sketch the ACF of the code.

b. If we use the system using random codes with the same chip length in a CDMA environment, how many simultaneous data users can we support with an omni-directional antenna and one access point?

11.2 **a.** If in the PPM-IR PHY layer used for the IEEE 802.11 instead of PPM we were using baseband Manchester coding, what would be the transmission data rate? Your reasoning must be given.

b. What is the symbol transmission rate in the IEEE 802.11b? How many complex QPSK symbols are used in one coded symbol? How many bits are mapped into one transmitted symbol? What is the redundancy of the coded symbols (the ratio of the coded symbols to total number of choices)?

11.3 **a.** Use the equation for generation of CCK to generate the complex transmitted codes associated with the data sequence {0,1,0,0,1,0,1,1}.

b. Repeat (a) for the sequence {1,1,0,0,1,1,0,0}.

c. Show that the two generated codes are orthogonal.

11.4 Redraw the timing diagram of Example 4.18, shown in Figure 4.15, assuming that Terminal B uses the RTS/CTS mechanism to send its packet.

11.5 A voice-over IP application layer software generates a 64 kbps coded voice packet every 50 ms. This software is installed in two laptops with WLAN PCMCIA cards communicating with an AP connected to a Fast Ethernet (100 Mbps).

a. Use Figure 4.37 to give the buffer length at the receivers.

b. What is the length of the voice packets in ms, if the PCMCIA cards were DSSS IEEE 802.11?

c. If the two terminals start to send voice packets almost at the same time, give the timing diagram to show how the first packets are delivered though the wireless medium to the AP using the CSMA/CA mechanism.

d. Repeat (b) and (c) if 802.11b was used instead of DSSS 802.11.

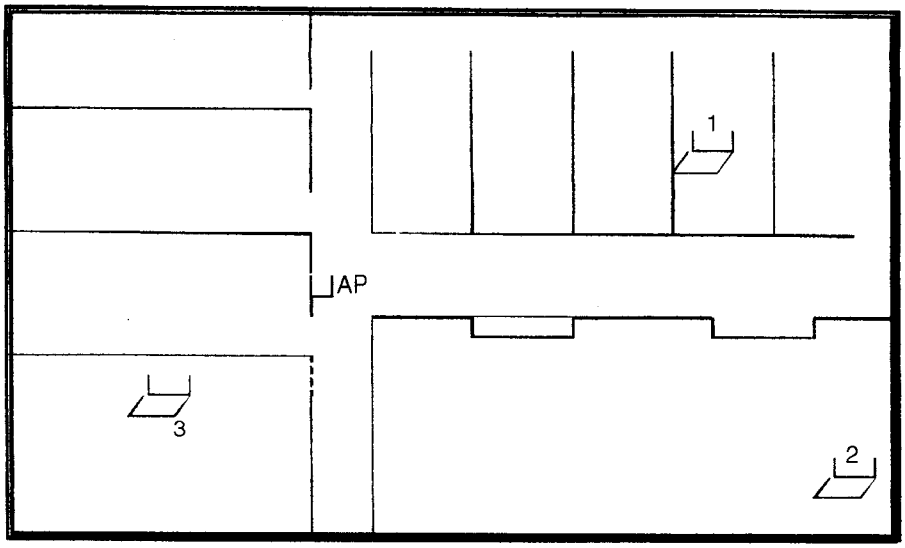


Figure 11.26 Layout of an office building with a WLAN.

11.6 Figure 11.26 shows the layout of an office building. If the distance between the AP and the MSs 1, 2, and 3 are 50, 65, and 25 meters, respectively, determine the path loss for between the AP and MSs:

- **a.** Using a loss of 3dB per wall.
- **b.** Using the JTC model.
- **c.** Using the 802.11 transmitted and received power specifications to determine whether a single AP can cover the entire building.
- **d.** If the minimum SNR requirement for proper operation of the IEEE 802.11 modems is 10 dB, find out which of the three MSs in the previous problem may be hidden with another terminal (use the JTC model for propagation).