13. Describe basic GSM EDGE operation.
14. For IS-95A, what is the function of the IWF?
15. Describe the functionality of the three versions of radio link protocol.
16. Describe the basic evolutionary path from GSM to UMTS.
17. What is a "Node B" in the UTRAN system?
18. Describe the basic operations involved in cdma2000 packet data call setup.
19. What happens to the user's PPP session during CDMA handover?
20. What system parameter determines the data rate over the cdma2000 forward supplemental channel during a packet data call?
21. What happens to the user's PPP session if the mobile goes into a dormant state?
22. What is the purpose of the delivery/failure report sent during a mobile originated SMS transfer?
23. What is the basic difference between EMS/MMS and SMS?
24. From a network viewpoint, what is the basic difference between SMS and MMS?
25. Describe the relationship between WAP and MMS.

CHAPTER 8

# Wireless Modulation Techniques and Hardware

Upon completion of this chapter, the student should be able to:

- Discuss the general characteristics of wireline and fiber-optic transmission lines.
- Discuss the propagation conditions peculiar to the air interface for wireless mobile systems and wireless LANs.
- Discuss the coding techniques used by wireless mobile systems to combat transmission errors.
- Explain the basic fundamental concepts of digital modulation techniques and their advantages.
- Explain the basic operation and characteristics of spread spectrum modulation systems.
- Discuss the basic principles behind the operation of ultra-wideband radio technology.
- Explain the theory behind the use of diversity techniques for the improvement of wireless communications.
- Discuss the typical BSC and RBS hardware found at a modern cell site.
- Discuss the technical attributes of a subscriber device.

The first seven chapters of this text have introduced the reader to present-day wireless cellular telecommunications networks that can deliver both voice and rich multimedia messages via high-speed packet data over state-of-the-art, nationwide wireless networks. The focus of these first chapters has been on the network architectures and the various system operations necessary to provide the subscriber with radio link access, security, and mobility. When talking about the air interface for a particular type of technology, such topics as frequency reuse, frequency of operation, modulation techniques, logical channels, timing and synchronization, bit rates, and frame structure have received the most attention. The reasons why these systems were designed in the way they were has not been discussed at any great length.

This chapter is going to delve more deeply into the physical layer (air interface) of wireless mobile systems. It is hoped that some of the natural questions that might arise as the reader has gone through the early chapters of this text will be answered by the coverage provided in this chapter. Starting with a comparison of guided wave transmission and wireless transmission it is felt that the reader will develop an appreciation for the complex coding schemes employed by wireless systems. Emphasis shifts to an explanation of today's modern digital encoding techniques with their inherent spectral efficiencies and their ability to mitigate radio channel impairments. This section also sets the stage for the next several chapters that cover the technologies used to implement wireless LANs, PANs, and MANs. Another section that presents system enhancement techniques such as antenna diversity and rake receivers sheds some light on present and future system developments that are and will be used to improve wireless system quality and data transmission rates.

The chapter ends with an overview of typical GSM and CDMA hardware implementations of the base station subsystems (i.e., the systems that implement the base station controller function and the radio base station function) and subscriber devices. This portion of the chapter will present a snapshot in time of today's cell site hardware that provides the radio link to the mobile user.

## 8.1 TRANSMISSION CHARACTERISTICS OF WIRELINE AND FIBER SYSTEMS

Fixed telecommunication infrastructure takes on many forms and uses many different techniques to transmit information from point to point. Depending upon the distance, form of the information (analog or digital), required data transmission rate, and the environment that needs to be traversed, one might choose from any one of many different technologies to deliver the desired signal or signals from one point to another. For either relatively short or extremely long fixed terrestrial point-to-point networks, one typically finds some form of guided-wave transmission media used. The physical implementations of these media are commonly known as transmission lines. Although today one can point to numerous examples of short-haul, fixed point-to-point radio links that have recently come into their own in terms of popularity, this section will limit its coverage to conductor-based (wireline) and fiber-optic transmission lines. A brief overview of the common types of transmission lines and their characteristics follows. In all cases, these types of transmission media provide a more reliable channel than the typical wireless radio channel.

### Conductor-Based Transmission Lines

The purpose of a **transmission line** (TL) is to guide a signal from point to point as efficiently as possible. At low frequencies (with extremely long wavelengths), current flows within the conductors and is not prone to radiate away from the TL. At higher frequencies, the current flow takes place near the conductor surface (due to the so-called skin effect). At radio frequencies (RF) and higher (microwaves and millimeter waves), the transmission line acts as a structure that guides an electromagnetic wave (EM). Many specialized TLs exist for use at these extremely high frequencies but will not be discussed here.

There are numerous types of TLs available for use in today's telecommunication links. Some of the more commonly encountered **wireline** TLs are unshielded and shielded twisted pair (UTP and STP), LAN Category-n cable, and coaxial cable. These cables are used to provide the local-loop connection to the telephone central office, LAN connectivity, and broadband cable TV service to name just a few applications. In all cases, wireline transmission lines act like low-pass filters, their signal attenuation increases with frequency. The individual characteristics of these wireline cables provide differing levels of bandwidth, maximum transmission rate, and reliability. Therefore, when designing a new telecommunication link or choosing what type of TL to use, one should choose a TL designed for that particular application.

In general, the most important TL characteristics to consider are bandwidth, susceptibility to noise, and frequency response. For the cases of bandwidth and frequency response these characteristics are fairly stable with time and can be designed around or adapted to by intelligent systems (ADSL, HDSL, etc.). These types of systems test the link to determine its initial characteristics and adaptively adjust their operation before attempting to use it. They continue to test the link periodically thereafter and adapt to any changes as necessary. TL susceptibility to noise is another issue. Different twisted pairs within a binder of multiple pairs can have varying amounts of ingress of near- and far-end cross talk (NEXT and FEXT noise) associated with the pair depending upon the various types of traffic being carried on the other pairs within the binder. Also, the existence of other nearby or not-so-nearby electrical noise sources (atmospheric, man-made EMI, etc.) can also impair signal transmission. Coaxial cables offer the advantage of shielding as do various types of shielded twisted pairs. Shielding allows the coaxial cable to be placed in environments that are unfavorable to simple unshielded transmission lines. However, for both coaxial cable and STP, noise ingress can occur at termination points, splices, or connectors. To compensate for these facts, various

coding schemes and transmission protocols have been developed to respond to the ultimate result of too much noise, bit errors, or frame errors in transmitted data. Use of these error detection and correction schemes tends to provide reliable data transport over wireline TLs.

### Fiber-Optic Cables

The ultimate telecommunications transmission media is the fiber-optic cable. Besides having a potential for almost unlimited bandwidth, it is not susceptible to electromagnetic interference (EMI) and its physical construction typically blocks any ingress (or egress for that matter) of stray photons that could cause problems. It is not that fiber-optic cables do not have any noise problems, it is just that the noise is quantum in nature. Therefore, if the optical detector used at the far end of the optical link has a sufficient number of photons reaching it, the bit error rate (BER) will be extremely low and for all practical purposes is nonexistent. In fact, other components in the fiber-optic link (sources, detectors, amplifiers, optical switches, etc.) may contribute more to the generation of noise and bit errors than the cable itself. This fact has led to the popularity of using fiber-optic cables for long-haul, high-capacity (gbps and tbps) backbone telecommunications links and the development of optical transport technologies like SONET that take advantage of these low BERs. In the case of both wireline cables and fiber-optic cables, extremely reliable communications links may be established. Unfortunately, this cannot be said for the radio channel. The next section will examine the characteristics of the air interface.

## 8.2 CHARACTERISTICS OF THE AIR INTERFACE

The last section presented the various characteristics of both wireline and fiber-optic cables. Before discussing the air interface, it is important to note that if more bandwidth or capacity is needed in a fixed system, it is possible to increase the capacity by physically installing additional transmission links (wireline or fiber). This is not necessarily true for the air interface. This being stated, let us turn our attention to the characteristics of the air interface.

If one looks at the evolution of wireless from the days of Marconi to the present, it is fairly obvious that the very early pioneers in the use of wireless knew little about electromagnetic (EM) wave propagation or propagation conditions over the surface of the planet. Although they did realize that EM waves behaved like light waves, they were unable to accurately predict how EM waves would interact with the planet's surface and surrounding atmosphere. To be fair, the early wireless pioneers could not produce EM waves of just any frequency or wavelength that they desired and were therefore forced to experiment with what they could generate. In fact, the very early use of high-frequency alternators (below 100 kHz) was perceived as being so successful that for many years practically all attention and research of the use of other frequency ranges was abandoned. As vacuum tube technology matured further, the understanding of both antenna theory and EM wave propagation increased as higher frequencies were explored. As the maximum frequencies producible by vacuum tubes reached into the medium- and high-frequency ranges, radio broadcasting, using amplitude modulation (AM), and long-distance short-wave broadcasting became commonplace. At the present time, a great deal is known about the propagation of EM waves. It is this knowledge that has guided the assignment of various frequency bands to particular types of radio services by government regulatory agencies like the FCC. Furthermore, to complicate matters, the use of various frequency bands has not been standardized on a worldwide basis. Band use may vary from country to country. Presently, the radio frequency spectrum is considered to extend from the extremely low frequency (ELF) of 30 Hz to the extremely high frequency (EHF) of 300 GHz. Not all of these frequencies are suitable for wireless mobile communications.

## Radio Wave Propagation and Propagation Models

Before looking at any particular EM propagation models, a general overview of terrestrial EM propagation is warranted. EM waves below approximately 2 MHz tend to travel as ground waves. Launched by vertical antennas, these waves tend to follow the curvature of the earth and lose strength fairly rapidly as they travel away from the antenna. They do not penetrate the ionospheric layers that exist in the upper portions of the earth's atmosphere. Frequencies between approximately 2 and 30 MHz propagate as sky waves. Bouncing off of ionospheric layers, these EM waves may propagate completely around the earth through multiple reflections or "hops" between the ground and the ionosphere. Frequencies above approximately 30 MHz tend to travel in straight lines or "rays" and are therefore limited in their propagation by the curvature of the earth. These frequencies pass right through the earth's ionospheric layers. The daily and seasonal variations that occur in the characteristics of the ionospheric layers give rise to the repeated use of the word *approximately* in the previous explanations.

Other propagation considerations include antenna size and the penetration of structures by EM waves. Antenna size is inversely proportional to frequency. The higher the frequency of operation the smaller the antenna structure can be, which is an important consideration for a mobile device. Also, as frequency increases and wavelength decreases, EM waves have a more difficult time penetrating the walls of physical structures in their path. At frequencies above 20 GHz for example, signals generated within a room will usually be confined within the walls of a room. At even higher frequencies, atmospheric water vapor or oxygen will attenuate the signal as it propagates through the atmosphere. These effects, although appearing detrimental at first, can be used to one's advantage for certain applications. More will be said about this topic later on.

When first-generation AMPS cellular radio was first deployed in the United States, it used frequency bands (in the 800-MHz range) refarmed from the upper channels of the UHF television band. These frequencies provided appropriate propagation conditions, antenna size, and building penetration properties. The PCS bands in the 1900-MHz range and the new AWS bands in the 1710- and 2100-MHz range are also suitable for mobile wireless. These services all use licensed spectrum in the ultrahigh-frequency (UHF) band that has been auctioned off (or will be) by the FCC in various-size pieces to different operators and service providers in different basic and major trading areas. New standards for wireless LANs call for operation in either the unlicensed instrumentation, scientific, and medical (ISM) frequency bands or the new unlicensed national information infrastructure (U-NII) bands. The use of either expensive licensed frequencies or free unlicensed frequencies puts a new spin on how the wireless industry will evolve.

### *Wave Propagation Effects at UHF and Above*

Since all of the world's mobile wireless systems use the UHF (300–3000 MHz) band, some additional details about propagation above 300 MHz will be given at this time. Note also that the presently used ISM and U-NII bands are located in both the UHF and superhigh-frequency (SHF) bands (3–30 GHz). For signal propagation both indoors and outdoors, three major effects tend to determine the final signal level that is received at the mobile station from the base station and, the reverse case, the signal level received by the base station from the mobile. In theory, by what is known as the reciprocity theorem, the path loss for these two cases should be almost identical.

These three primary propagation effects are reflection, scattering, and diffraction. Reflection occurs for EM waves incident upon some type of large (compared to a wavelength) surface. For a smooth surface the EM wave undergoes a specular reflection, which means that the angle of incidence equals the angle of reflection. How much of the signal power is reflected from a smooth surface or transmitted into it is a complex function of the type of material, the surface roughness, frequency of the incident EM wave, and other variables. In general, the more electrically conductive the surface or the higher the material's relative dielectric constant, , the greater the amount of signal reflection. And, conversely, the lower the value of , the greater the amount of signal transmission into the medium. Scattering occurs when the signal is incident

upon a rough surface or obstacles smaller than a wavelength. This case produces what is known as a diffuse reflection (i.e., the signal is scattered in many different random directions simultaneously). Finally, diffraction is a subtle effect that causes EM waves to appear to bend around corners. An EM wave incident upon a sharp corner (e.g., the edge of a building rooftop) causes the generation of a weak point source that can illuminate a shadow or non-LOS (NLOS) area behind the object.

See Figure 8–1 for an example of an outdoor propagation case and Figure 8–2 for an example of an indoor propagation case. As shown by Figure 8–1 several signal paths may (and usually do) exist between the base station antenna and the mobile station. The primary signal tends to follow the line-of-sight (LOS) path while several to many other secondary, tertiary, or higher-order reflections also arrive at the mobile. In addition, diffraction of the base station signal can occur from almost any type of object and therefore any number of diffracted signals might also arrive at the mobile. For this case, all the signals arriving at the

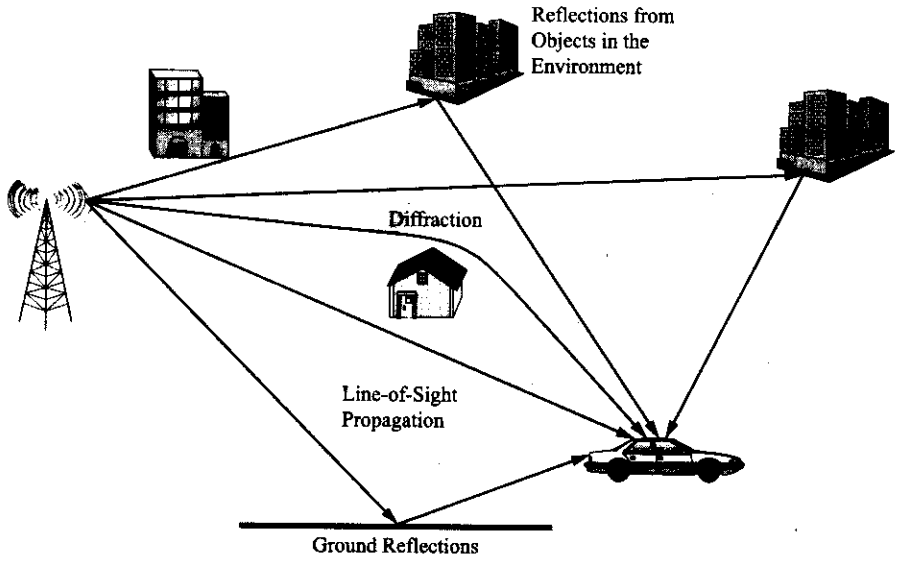



**Figure 8–1** Typical outdoor propagation case.

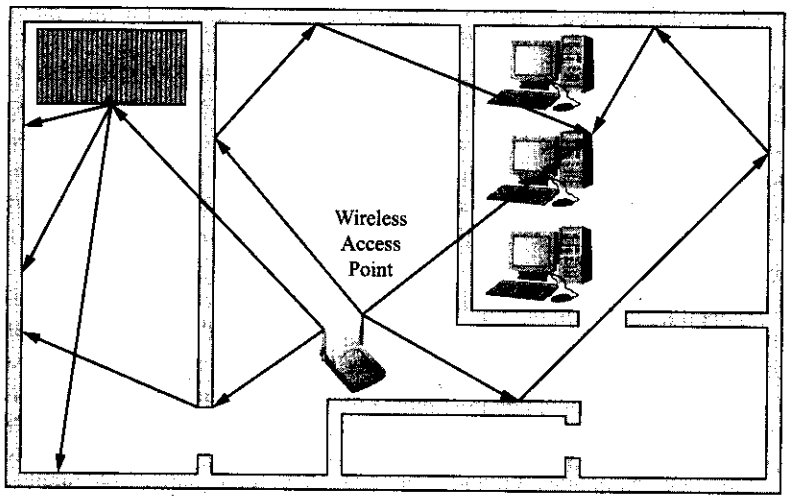



**Figure 8–2** Typical indoor propagation case.

mobile add together vectorially (i.e., both amplitude and phase), with the strongest signals tending to create the composite received signal. **Multipath** is the common term used to describe this type of propagation scenario. Also, note that due to the distances involved, there can be a fairly large spread of delays relative to the LOS signal due to the variety of possible paths that the other secondary signals might travel.

Figure 8–2 shows an example of an indoor propagation situation similar to what might be encountered with a wireless LAN access point and a wirelessly enabled laptop. In this case, the signal from the transmitter propagates through the walls between the rooms, experiences numerous reflections off of walls in a corridor and other interior walls, and undergoes diffraction and scattering due to various other obstacles and sharp corners. Again, all the signals arriving at the receiver will add together vectorially to create the composite received signal. For this case, due to the short propagation distances involved, there will be only a small spread of delays between the arriving signals. This important point will be expanded upon shortly. For the case of a cellular call being received within a structure or a particular wireless LAN situation there may be no direct or unobstructed LOS signal. This being the case, the composite received signal is primarily composed of many weaker secondary signals. As the reader may have already concluded, there are a myriad of possible situations and conditions that might arise for both outdoor and indoor propagation cases. Additionally, the effect on received signals for the case of a mobile moving about within a system's coverage area has not been addressed as of yet.

## Path Loss Models for Various Coverage Areas

The first **path loss** model to consider is that for free space propagation. It may be shown fairly easily that without any outside influences the propagating signal power of an EM wave decreases by the square of the distance traveled as it spreads out. Therefore, the EM wave undergoes an attenuation of –6 dB every time the distance it travels doubles. The power received from an antenna radiating $P_T$ watts in free space is given by the following equation (known as the Friis equation):

$$P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi d}\right)^2 \qquad \textbf{8-1}$$

where $G_T$ and $G_R$ are the transmitting and receiving antenna link gains, respectively, $\lambda$ is the signal wavelength, and $d$ is the distance from the transmitting antenna. A typical technique to simplify the usage of this equation is to rewrite it as:

$$P_R = P_0/d^2 \qquad \textbf{8-2}$$

where $P_0$ is the received signal strength at a distance of one meter. Once $P_0$ has been calculated, it is a simple task to determine the received signal strength at other distances. Also important to note here is that in the free space environment the velocity of propagation for an EM wave translates into an approximately 3.3-ns-per-meter time delay. This means that it takes 3300 ns for a signal to travel a distance of 1000 meters in free space. This fact will be called upon later in our further discussions about multipath propagation. At this point, a free space path loss example is appropriate.

---

*Example 8–1*

What is the received power in dBm for a signal in free space with a transmitting power of 1 W, frequency of 1900 MHz, and distance from the receiver of 1000 meters if the transmitting antenna and receiving antennas both use dipole antennas with gains of approximately 1.6? What is the path loss in dB?

*Solution:* First calculate $P_0$ from Equation 8-1

$$P_0 = (1)(1.6)(1.6)(0.1579)/4\pi(1))^2 = .0004042 \text{ W or } -3.934 \text{ dBm}$$

Then from Equation 8-2,

$$P_R\,(P_0/d^2) = (.4042\text{ mW}/1000^2) = .4042\text{ nW or } -63.934\text{ dBm}$$

The path loss in dB is the difference between the transmitted power, $P_T$, and the received power, $P_R$. Or, in equation form:

$$Path\ Loss = P_T - P_R \qquad \textbf{8-3}$$

For this particular example, the path loss is equal to +30 dBm (–63.934 dBm) or 93.934 dB. Note, 1W = +30 dBm.

---

Unfortunately, the free space model, though instructive, does not give accurate results when applied to mobile radio environments. As already discussed, typically the transmitted signal reaches the receiver over several different paths. At this time several other models will be discussed in the context of relative cell size and environment (i.e., indoor and outdoor).

### *Other Path Loss Models*

A simple first approximation model for a land mobile outdoor environment is known as the **two-ray model.** This model assumes a direct LOS signal between the transmitter and the receiver (similar to free space propagation) and another signal path that consists of a reflected signal off of a flat surface of the earth (also known as a ground reflection). For this scenario the two path lengths will vary depending upon the antenna heights, and the reflected and LOS signal can vary in intensity due to the motion of the mobile and other variations in propagation conditions. Therefore, the composite signal received at the mobile station antenna will consist of EM waves that add either constructively or destructively. An equation that approximates this behavior is:

$$P_R = P_T G_T G_R \left(\frac{h_T^2 h_R^2}{d^4}\right) \qquad \textbf{8-4}$$

where, $h_T$ and $h_R$ are the heights of the transmitting and receiving antennas. Several important details that one can discern from this equation are that the higher the antenna heights are above ground the more the received signal power is and that the power falls off by the distance raised to the fourth power for large values of $d$ (i.e., $d \gg \sqrt{h_T h_R}$ ). This last fact is quite illuminating since it basically doubles the EM wave attenuation rate from –6 dB to –12 dB every time the distance the wave travels doubles. This result is more indicative of the true behavior of a land mobile radio link. Now an approximate equation for path loss using the two-ray model can be written as:

$$Path\ Loss = 40 \log d - (10 \log G_T + 10 \log G_R + 20 \log h_T + 20 \log h_R) \qquad \textbf{8-5}$$

Another popular model for relating the received signal power to the radio link distance is to use the following equation:

$$P_R = P_0 d^{-\alpha} \qquad \textbf{8-6}$$

where $\alpha$ is known as the distance-power gradient. As we have previously discussed, $\alpha = 2$ for free space and $\alpha = 4$ (approximately) for the two-ray model. It is not unreasonable to assume that for both indoor and outdoor urban radio links the value of $\alpha$ will vary depending upon the building types (construction materials, heights, density, etc.), street layouts, and area topography. The value of $\alpha$ may be empirically determined by measurement or through the use of simulation software. In any case, for any particular distance, $d$, one would discover that the true path loss has a random value that is distributed about the value predicted by Equation 8-6 (i.e., the mean value of the distribution). This effect is caused by the random shadowing effects that occur for different locations with the same transmitter receiver separation. As mobile radio

has evolved, several studies have been undertaken to generate more accurate outdoor propagation models. Early studies produced several models that were improvements over the two-ray model. However, the Okumura model, a set of curves covering the cellular bands and higher frequencies, generated from extensive measurements in urban locations over three decades ago, has become popular and widely used for signal prediction in urban areas. Okumura's model was based entirely on measured data but is considered to give reasonable results for cluttered environments. The model gives its best results in urban areas, with less accurate predictions in rural areas. Approximately twenty-five years ago, Hata developed expressions for path loss based on Okumura's curves. These expressions are commonly known as the Okumura-Hata model. Later, the European Co-operative for Scientific and Technical research extended the Hata model to 2 GHz. Others have continued to refine these models (as this area became a hot research topic) to include the effects of rooftops, building heights, terrain, and other pertinent factors.

In case it is not obvious, with these various propagation models, wireless mobile system planners are able to make educated guesses about cell site coverage areas through the use of path loss calculations. At the same time, others have worked to develop accurate models of indoor EM propagation for wireless LANs.

As these propagation models were improved and databases of detailed geographic information became publicly available, these two applications were able to be computerized and linked together. Presently, there are numerous commercial software simulation packages that provide fairly sophisticated and accurate models of signal propagation over a wide range of frequencies and environments. For mobile and fixed radio applications these software packages provide colorized coverage maps, incorporate 2D and 3D imagery, and include topographic data from geographical surveys. For wireless LAN applications, single and multifloor models are incorporated with building layouts to predict coverage areas by data rate, BER, and so on. The reader is urged to perform an Internet search of "propagation prediction software" or a similar topic to be directed to Web sites about these products. Some manufacturers even provide free downloadable demonstration software over the Web.

## Multipath and Doppler Effects

Until this point, the path loss models previously described have been used to estimate the average received signal strength (RSS) for a given point some distance from the transmitter. These models do not address the real-time fluctuations in RSS that the receiver experiences due to the combined consequences of the Doppler effect and the rapidly changing multipath propagation conditions due to the motion (possibly very rapid) of the mobile itself. The rapid changes in signal phase due to the equally rapid changes in signal propagation distance can cause rapid and deep fluctuations in the RSS. Both Doppler effect signal spreading and multipath fading have been studied extensively. Multipath delay spreading leads to both time dispersion of the received signal and frequency selective fading. The Doppler effect leads to frequency dispersion and time selective fading. Typically both fading effects are modeled as Rayleigh distributions or, if there is a dominant LOS propagation path, as Ricean distributions. Commonly, within the wireless industry, any type of rapid fading is referred to as Rayleigh fading. Figure 8–3 shows a typical plot of the random Rayleigh fading of RSS for a typical radio channel. From Figure 8–3 one can see the deep RSS fades that can range up to 40 dB. Interestingly, designers of wireless systems are able to incorporate statistical information about the typical fading characteristics of radio channels into the design of appropriate data coding and interleaving techniques employed at the transmitter that will help to mitigate these fast fading effects. Diversity techniques and frequency hopping are also helpful in this regard.

A typical multipath delay spread is shown in Figure 8–4. A major effect of multipath spread is an increase in intersymbol interference (ISI) if the delay spread is either comparable or larger than the symbol time. Usually, to mitigate this effect, specialized techniques are employed at the receiver. Channel equalization and directional antennas are techniques that are typically used to help in this regard. The next several sections will discuss these mitigation techniques in more detail.

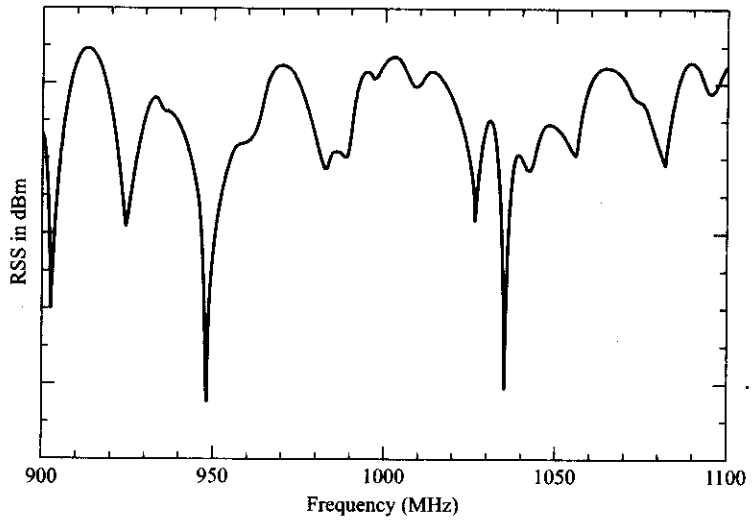



**Figure 8–3** Typical Rayleigh fading for a radio channel in the UHF range.

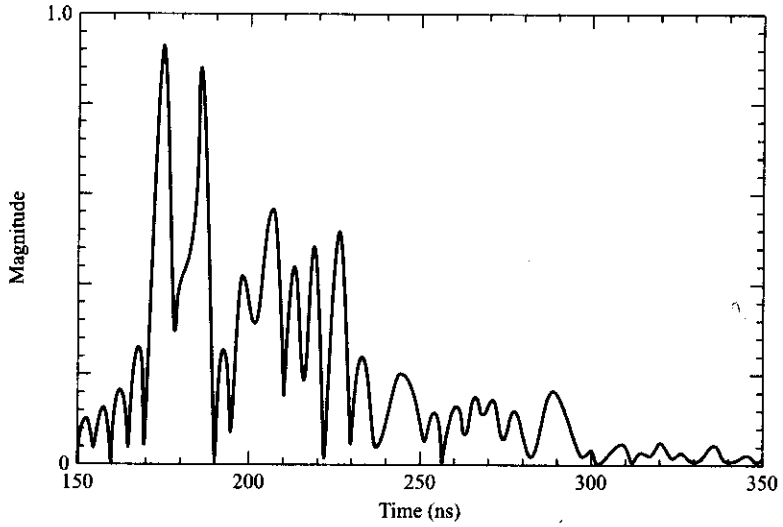



**Figure 8–4** Typical multipath delay spread.

New position location applications for wireless mobile radio (E911, position-sensitive commercial advertisement, etc.) have served to redefine what the important characteristics of a radio channel are in a quest to implement schemes that will provide accurate location determination of a mobile subscriber. In future technology implementations of base and mobile stations, plans exist for multiple input multiple output (MIMO) radio channels links. For this particular technology, the base station has $M$ antenna element and the mobile station has $N$ antenna elements. This gives rise to the possibility of a matrix of $M \times N$ elements that provide information about the radio channel characteristics and provide diversity for signal propagation. Besides the anticipated improvement in location services, technology like this shows promise of increasing wireless mobile system capacity by several times over.

## 8.3 WIRELESS TELECOMMUNICATIONS CODING TECHNIQUES

Now that the properties of the air interface have been discussed in the context of wireless mobile systems, it is time to look at some of the steps taken by the designers of wireless systems to compensate for some of the problems encountered during the use of a mobile radio link. Each of the techniques that will be examined in the next sections are implemented at the transmitter in an attempt to increase the transmitted signal's immunity to radio channel noise and other channel impairments including frequency fading and multipath spread. In a digitally based system, these techniques correspond to an attempt to realize a reduction in bit errors and frame errors. It is also acknowledged that even with the best-designed radio systems there will be random bit errors occurring. Therefore, the best strategy is to employ some form of error detection and correction codes to reduce the required number of requests for retransmission by the system for those instances when errors cannot be corrected.

In addition to the use of coding to reduce and detect errors during transmission, extensive block interleaving schemes are also used at the transmitter to provide enhanced data transmission over the radio link.

### Error Detection and Correction Coding

In contrast to wireline systems where errors tend to occur 1 bit at a time in a purely random fashion, errors in wireless systems tend to occur in bursts. Therefore, error detection and correction codes designed for wireline systems and wireless systems tend to differ in their basic implementation. Error control coding (ECC) is the term used to denote a technique that codes the transmitted bits in a way that attempts to control the overall bit error rate. The type of coding used is also somewhat dependent upon the maximum bit error rate that can be tolerated. Voice data traffic can accept much higher bit error rates than can the transfer of sensitive packet data information. For the latter case, if low enough bit error rates cannot be achieved, a means by which the system can ask for a retransmission of a data packet when necessary must be designed into the system. Such systems are typically known as automatic repeat request (ARQ) schemes. **Block codes** may be used to determine whether an error has occurred during data transmission. Schemes that use block codes to correct errors that might have occurred during transmission are known as forward error correction (FEC) codes. Today, block, convolutional, and turbo codes are used to enhance the transmission of packet data over wireless systems.

#### *Block Codes*

A simple view of block coding is that the system takes a block of data bits and encodes them into another block of bits with some additional bits that are used to detect or combat errors. The simplest form of this technique is through the use of a single parity bit. Using even or odd parity, a single error can be detected. However, it is easy to see that multiple errors may not be detected. Using more sophisticated techniques, additional bits may be generated through a matrix or polynomial generator and added to the original block of bits to form a codeword that will be eventually transmitted by the system. A codeword generated by a polynomial is a form of cyclic code, and codes of this type are known as cyclic redundancy check (CRC) codes. Depending upon the type of coding level employed these schemes can both detect and correct limited numbers of errors. To transmit voice over a GSM traffic channel a limited number of parity bits (3) are added to a block of 50 bits. To transmit a message over the control channel, GSM takes a block of 184 bits and adds 40 parity check bits to generate a 224-bit codeword before it is sent to a convolutional encoder. Since voice traffic can tolerate higher bit error rates and message signaling can be retransmitted, there are more bits used by the system for error detection for GSM control signaling than for GSM voice traffic.

#### *Convolutional and Turbo Encoders*

A **convolutional encoder** does not map blocks of bits into codewords. Instead, a continuous stream of bits is mapped into an output stream that now possesses redundancy. The redundancy introduced to the bit

stream is dependent upon the incoming bits and several of the preceding bits. The number of preceding bits used in the encoding process is known as the constraint length, $K$, and the ratio of input bits to output bits from the encoder is known as the code rate, $R$, of the encoder. For the reverse fundamental channel of a cdma2000 system, a convolutional encoder with $R = 1/3$ and $K = 9$ is used. In practice, the use of convolutional encoders provides better FEC capabilities than available from block codes. Some systems use both block coding techniques and convolutional encoders to generate the final transmitted data packet. Figure 8–5 shows in block diagram form an implementation of a convolutional encoder (with $K = 9$ and $R = 1/2$) specified for use in cdma2000.

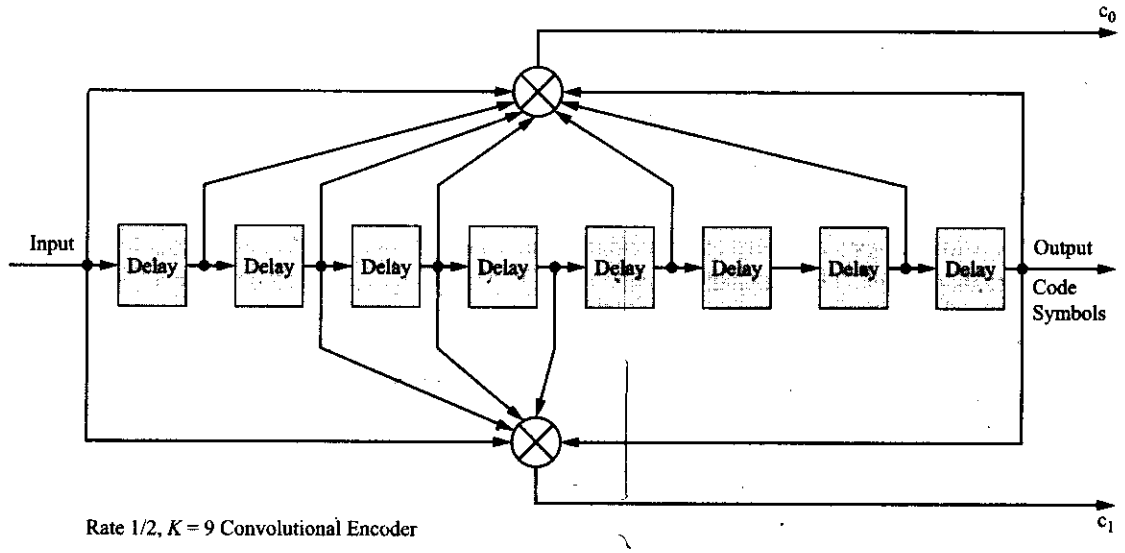



**Figure 8–5** Convolutional encoder with constraint length, $K = 9$ and rate, $R = 1/2$ (Courtesy of 3GPP2).

**Turbo encoders** are a modified form of combined convolutional encoders that can be used to create a new class of enhanced error correction codes. A typical turbo encoder is constructed from two systematic, recursive, convolutional encoders connected in parallel with an interleaver preceding the input to the second convolutional encoder. The output bit streams of the two convolutional encoders are multiplexed together and repeated to form the final code symbols. For cdma2000, Rate 1/2, 1/3, 1/4, and 1/5 turbo encoders are employed instead of convolutional encoders for various higher-bit transfer rates and radio configurations.

## Speech Coding

Speech coding has been addressed in various levels of detail in other chapters but for continuity it is briefly overviewed here. The speech coders used for both GSM and CDMA wireless systems take 20-msec segments of either previously encoded speech or raw speech and process it into lower-bit-rate digitally encoded speech in preparation for its transmission over the air interface. There are many different types of speech coders available today. In general, there are two broad classifications of speech coders: waveform coders and vocoders. Pulse code modulation is an example of a waveform coder whereas the QCELP encoder used in IS-95 CDMA or the RPE-LTP encoder used in GSM are examples of vocoders. Voice traffic from the circuit-switched network is delivered to the base station subsystem in PCM format at a 64 kbps data rate. The vocoders used by the wireless mobile systems perform data rate translation by more efficiently encoding the voice information.

For early GSM wireless systems, speech may be transmitted at full rate, half rate, or enhanced full rate. The full-rate speech coder delivers a block of 260 bits every 20 msec (13 kbps) to the channel encoder. For

the other GSM speech rates the number of bits delivered by the speech coder to the channel encoder varies. However, in all but the half-rate speech case the final transmitted packet (a 20-msec frame) contains 456 bits. For half-rate operation two half packets of 228 bits are combined to make a full frame. A new AMR codec for GSM will be discussed later in this chapter.

In early CDMA systems, the speech coders may operate at either 9.6 or 14.4 kbps and subrates of these values. For operation at 9.6 kbps, 172 bits are provided to the channel encoder every 20 msec. For 14.4 kbps the rate is 268 bits every 20 msec. The final transmitted packet consists of 576 bits in each case. This process will be detailed shortly. The newer enhanced variable rate coder (EVRC) and a new selectable mode vocoder (SMV) for CDMA will be discussed later in this chapter.

## Block Interleaving

**Block interleaving** is a technique used by mobile wireless systems to combat the effects of bit errors introduced during transmission of a frame. The basic idea here is that the error control code used by the system may be able to correct one bit error out of a block of 8 bits. However, it is not able to correct a burst of say six errors within the 8-bit block. If the bits of the block can be interleaved with the bits from other blocks, then, in theory, the burst of six errors can be spread out over six other blocks and the ECC can correct each of the single bit errors in each of the six blocks. Figure 8–6 depicts this process for several noise bursts.

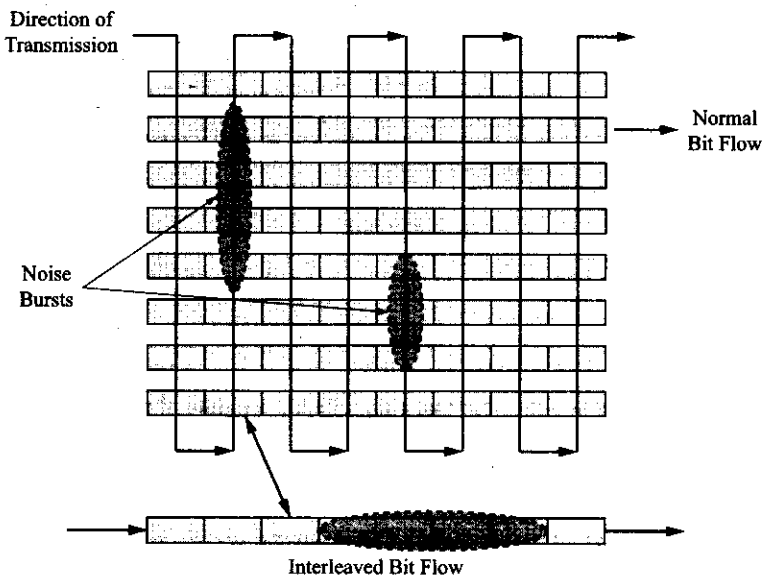



Figure 8–6 Typical block interleaving scheme.

## Examples of Coding and Interleaving

To complete this section's coverage of coding techniques, examples of the creation of transmitted voice packets for both GSM and CDMA operation will be detailed now. A block diagram of the GSM channel encoding system is shown by Figure 8–7.

The process consists of the following steps as indicated by Figure 8–8. The 260 bits delivered by the full-rate coder are divided into 182 bits of Class 1 (protected bits) and 78 bits of Class 2 (unprotected bits). Further, the fifty most important bits of Class 1 (Class 1a bits) are protected by 3 parity bits as shown in the second row of Figure 8–8. The 78 Class 2 bits are separated from the Class 1a, 1b, and CRC bits. These

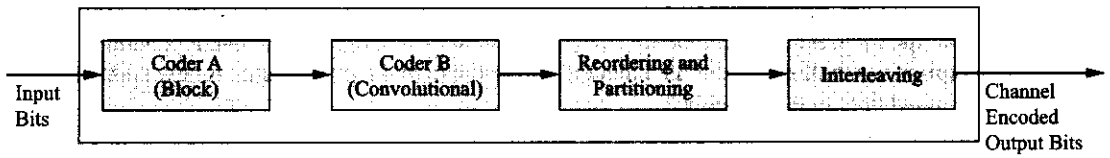



**Figure 8–7** GSM channel encoding block diagram (Courtesy of ETSI).

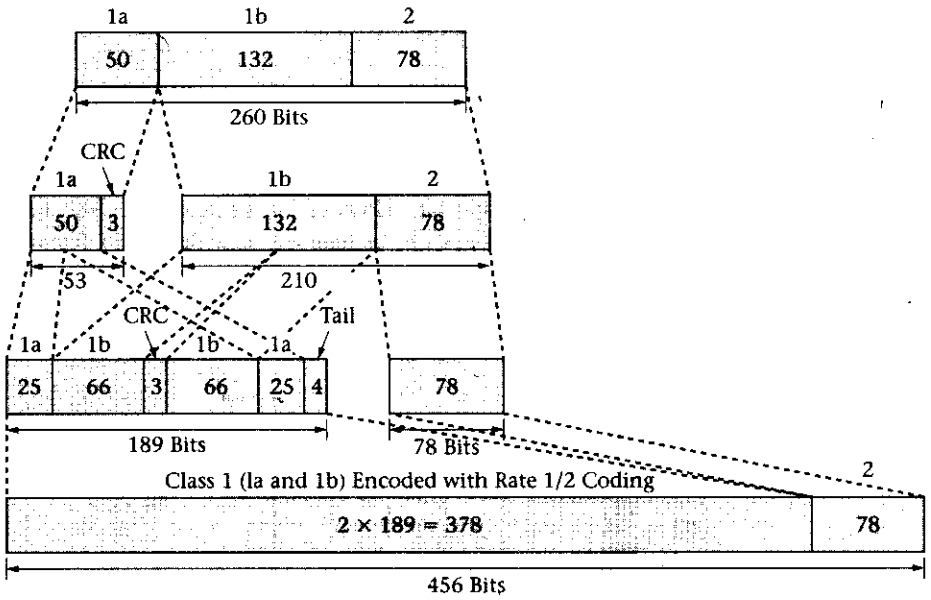



**Figure 8–8** Detailed steps of GSM channel encoding for voice traffic (Courtesy of ETSI).

Class 1 bits are now partitioned and reordered as shown in row three of the figure and applied to an $R = 1/2$ convolutional encoder. The output of the bits from the encoder are combined with the 78 Class 2 bits to yield a 456-bit packet. The reader should note that this scheme provides three different levels of encoding to the different classes of bits that are offered by the vocoder.

The 456 bits are now interleaved over eight half subframes of 57 bits as shown by Figure 8–9. Each group of 57 bits goes into a half subframe (refer back to Figure 5–15) of a normal traffic burst. The interleaving process is not complete yet. Another level of interleaving occurs as the user data is prepared to be transmitted over the air interface. The user's 456-bit, 20-msec frame consisting of eight subframes is interleaved with other user's data over a sequence of normal traffic bursts. Figure 8–10 depicts this process. If a severe fade occurs, its effect will be spread out over the traffic of several users. Naturally, at the receiver, a deinterleaving process must be performed to reorder the incoming bursts of user traffic.

For CDMA2000 wireless systems the channel encoding process is shown by Figure 8–11. As shown in Figure 8–11, for 9.6 kbps voice, 172 bits are offered per 20-msec frame. Twelve frame quality indicator bits and 8 encoder tail bits are added, and the 192 bits are put through an $R = 1/3$ convolutional encoder that outputs 576 bits that are applied to a block interleaver. In a similar fashion, 268 bits per 20-msec frame are offered for the 14.4-kbps rate. The addition of 12 frame quality bits and 8 tail bits yields 288 bits that are applied in this case to an $R = 1/2$ convolutional encoder that outputs 576 bits to be applied to the block interleaver. Again, the interleaving process must be reversed at the receiver.

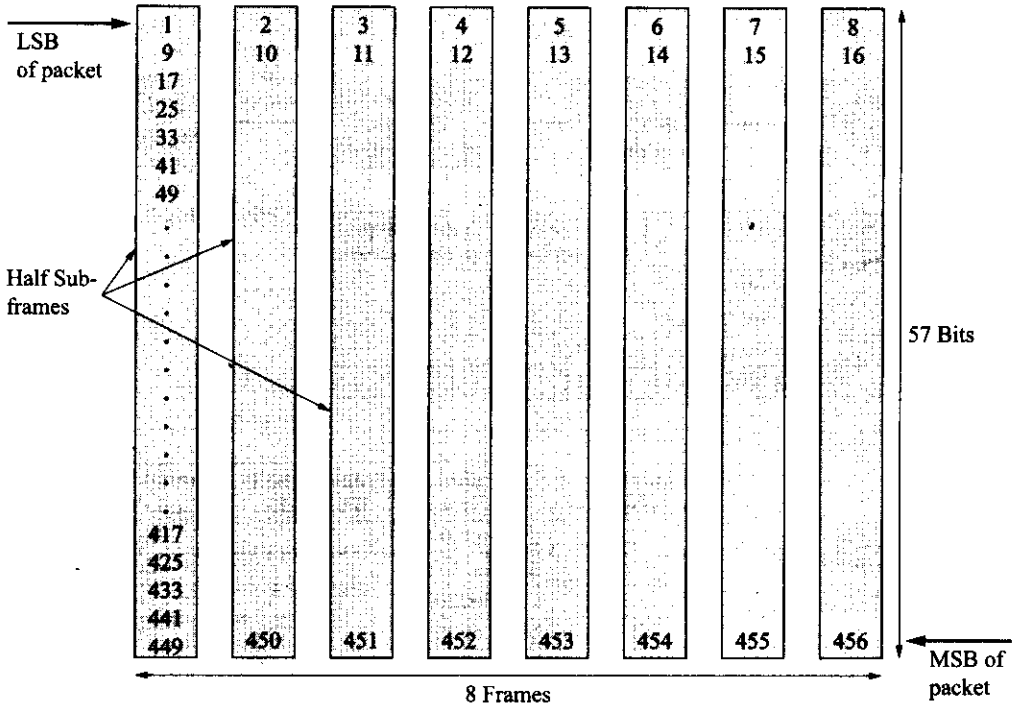



**Figure 8–9** GSM interleaving of encoded voice data.

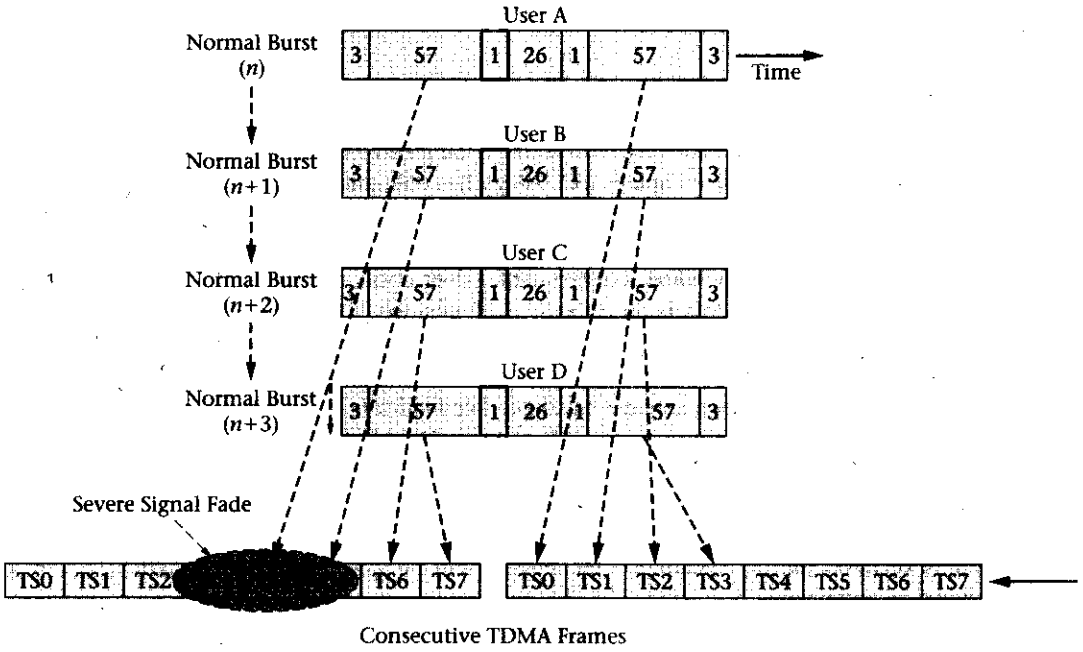
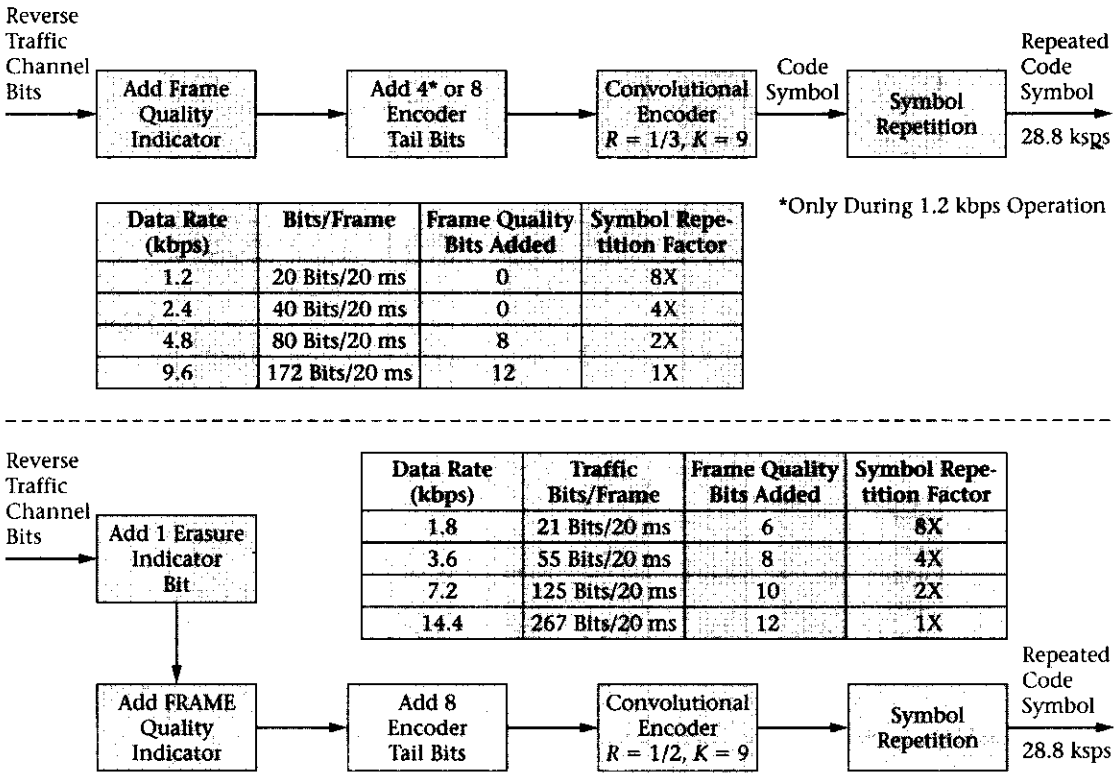



**Figure 8–10** Further data interleaving before transmission.




| Data Rate (kbps) | Bits/Frame | Frame Quality Bits Added | Symbol Repetition Factor |
|---|---|---|---|
| 1.2 | 20 Bits/20 ms | 0 | 8X |
| 2.4 | 40 Bits/20 ms | 0 | 4X |
| 4.8 | 80 Bits/20 ms | 8 | 2X |
| 9.6 | 172 Bits/20 ms | 12 | 1X |

| Data Rate (kbps) | Traffic Bits/Frame | Frame Quality Bits Added | Symbol Repetition Factor |
|---|---|---|---|
| 1.8 | 21 Bits/20 ms | 6 | 8X |
| 3.6 | 55 Bits/20 ms | 8 | 4X |
| 7.2 | 125 Bits/20 ms | 10 | 2X |
| 14.4 | 267 Bits/20 ms | 12 | 1X |

**Figure 8–11** Cdma2000 encoding for 9.6- and 14.4-kbps reverse voice traffic (Courtesy of 3GPP2).

## 8.4 DIGITAL MODULATION TECHNIQUES

As the world of electronic communication has evolved from the transmission of analog signals to the transfer of digital bits and at the same time computer technology has continued to evolve at an astonishing rate, the desire to transmit more bits per second over a telecommunications link has likewise grown. There are several basic steps one can take to increase the number of bits per second transmitted from point A to point B. One such step is to install more wireline, coaxial cable, fiber-optic, or radio links (or combinations of these). However, in most instances, this is an expensive proposition. Therefore, in most cases, new data transmission schemes have been developed to improve transmission rates over each of these media types. These new schemes typically employ some form of bandwidth conservation techniques or some way to make increased use of the transmission media's available bandwidth (e.g., xDSL for copper pairs, spread spectrum for radio links, or wavelength division multiplexing [WDM] for fiber-optic systems). Transmission over wireline media is usually done at baseband frequencies whereas transmission over the other types of transmission media is performed at passband (radio or light) frequencies because of the larger amounts of useable bandwidth afforded by the particular transmission media.

A short review of basic digital modulation techniques will be given here before particular schemes employed by wireless systems are discussed. The first popular use of digital modulation over copper pairs employed frequency shift keying (FSK) for the implementation of phone line modems. A variation on FSK known as minimum shift keying (MSK) became popular because its resulting bandwidth usage is less than that for FSK for the same bit rate. This last fact is important due to the use of the band-limited channel employed by the legacy telephone companies. These digital modulation techniques were also used for the early transmission of data over radio links. At the same time, another form of digital transmission that is

only employed over baseband channels was also used for the transmission of binary bits over copper pairs. This type of digital transmission technique makes use of different line codes to carry the binary bits over the wireline link. One might question the difference between the two digital techniques. The use of line codes produces signal spectral components that extend from 0 Hz to some upper limit. The use of digital modulation produces signal spectral components (typically a primary lobe and secondary sidelobes) that are centered at some higher system carrier frequency and usually do not extend down to 0 Hz (hence the terms *baseband* and *passband*).

These first early forms of digital modulation provided no improved spectral efficiency since only one bit was encoded per symbol or bit time. However, it was not long before more complex second-generation digital modulation techniques were developed. Binary phase shift keying (BPSK) encodes 0s and 1s as transmitter output signals with either 180-degree or 0-degree output phases. However, $n$-PSK (where $n$ is greater than 2 and also a power of 2) systems encode $m$ bits per transmitted symbol, where $m = \log_2 n$. For example, 8-PSK, used by 3G GSM/EDGE wireless systems, encodes 3 bits per transmitted symbol. See Table 8–1 for a 4-PSK truth table, Figure 8–12 for a 4-PSK constellation diagram, and Figure 8–13 for a typical QPSK transmitter. The use of this type of spectrally efficient digital modulation over the radio channel allows for an increase in the packet data transfer rate available from the wireless system in the same bandwidth channel. In general, the value of $m$, also indicates the gain in bandwidth efficiency since the symbol time (which determines the bandwidth) remains constant and only the number of encoded bits per symbol increases.

Table 8–1 4-PSK truth table.

| *Binary Input I and Q Bits* | *QPSK Phase* |
|---|---|
| 10 | $\pi/4$ or +45° |
| 00 | $3\pi/4$ or +135° |
| 01 | $5\pi/4$ or –135° |
| 11 | $7\pi/4$ or –45° |

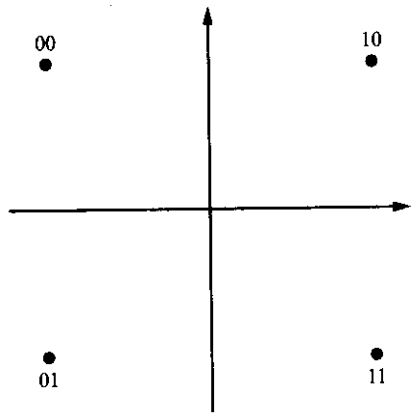



**Figure 8–12** 4-PSK constellation diagram.

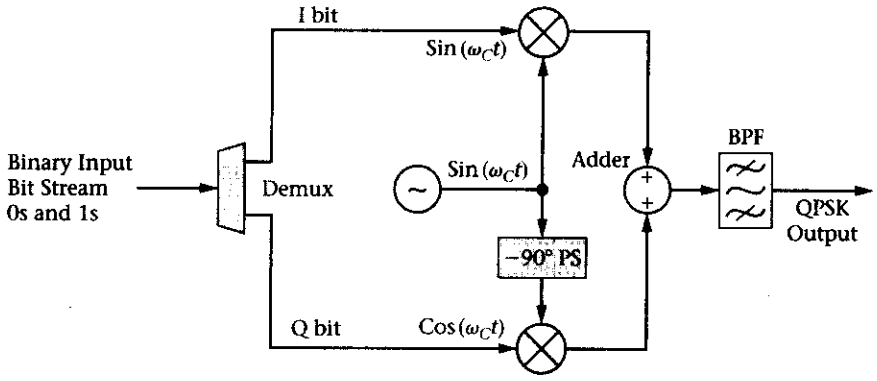



**Figure 8–13** Typical generic QPSK transmitter.

Another form of digital modulation known as quadrature amplitude modulation (n-QAM) encodes information in both the phase and amplitude of the transmitted signal. 64-QAM is capable of encoding 6 bits per transmitted symbol or therefore achieving a bandwidth efficiency of six times. It should be noted that one does not get something for nothing (as the expression goes). For passband digital modulation schemes, as the value of $n$ increases and the C/I ratio for the channel remains constant, the bit error rate will predictably increase. Presently, this form of digital modulation (64-QAM) is not yet used for any commercial mobile wireless systems due to its unacceptable bit error rate. It is however specified for use in the 5-GHz band for wireless LANs (IEEE 802.11a) and also for wireless MANs (IEEE 802.16). Now that suitable background information has been provided, modulation schemes adopted by the most popular wireless systems will be examined.

## Digital Frequency Modulation

The original analog first-generation AMPS system uses conventional FM to provide voice service over a 30-kHz channel. The second-generation digital GSM standard calls for the use of a form of digital frequency modulation known as Gaussian minimum shift keying or GMSK (a form of FSK). Since GSM is a FDMA-based wireless system with 200-kHz-wide channels, it is important that the sidelobe power of the transmitted RF signals is reduced as much as possible to prevent adjacent channel interference. GSM GMSK is a fairly simple modulation scheme that encodes 0s and 1s as two different frequencies—both shifted from the carrier frequency by 67.708 kHz. If the system uses coherent detection at the receiver, a minimal frequency difference of $1/2T$ where $T$ is the bit time may be maintained between the two frequencies used by the system as is the case for GSM. Furthermore, by passing the baseband binary information stream through a baseband filter with a Gaussian frequency response curve before modulation, a further reduction in the amplitude of the sidelobes of the transmitted signal can be achieved. Depending upon the type of digital traffic sent over the radio link, Gaussian filters with different bandwidth characteristics perform better than others. Also, since the output amplitude of a GMSK signal does not vary in amplitude, the nonlinearity inherent in RF power amplifiers will not affect the GMSK signal to any great extent with the additional generation of sidelobes. GMSK is a popular form of air interface modulation scheme for second-generation wireless radio systems.

## Digital Phase Modulation

In digital phase modulation, the baseband information signal is encoded in the phase of the transmitted RF signal. Quadrature PSK or QPSK ($n = 4$) encodes 2 bits per transmitted symbol (refer back to Table 8–1 and Figure 8–12). As was done with GMSK, pulse shaping filters can be used to control the sidelobe amplitude of the resultant QPSK signal. However, a key difference between QPSK and GMSK is that the QPSK

signal is not a constant amplitude signal nor is it a constant phase signal. This fact, combined with the nonlinearity associated with RF power amplifiers used in base and mobile station transmitter sections, gives rise to less-than-optimal performance for this type of digital modulation. In actuality, due to the fact that the QPSK signal amplitude can go to zero at times (as it transitions between symbols), sidelobe regeneration is both possible and probable.

Further enhancements to basic QPSK modulation are possible yielding several QPSK variants. Offset QPSK or OQPSK applies the I and Q bit streams to the balanced modulators of the QPSK transmitter (refer back to Figure 8–13) with a time delay of a half of a symbol time, $T/2$, between them. The net result of this modification is to reduce the fluctuations in the signal amplitude and the amount of possible phase shift between different symbols. Note that QPSK is used by IS-95 CDMA for the modulation of the forward channels and OQPSK is used for the modulation of the CDMA reverse channels. Cdma2000 also uses these same basic modulation schemes but adds 8-PSK and 16-QAM.

Another variation of QPSK used by mobile wireless systems is $\pi/4$ – QPSK. This form of QPSK restricts the phase shift between different symbols to either $\pm\pi/4$ or $\pm 3\pi/4$. Figure 8–14 shows the constellation diagram of the possible symbols of $\pi/4$ – QPSK. Actually, the diagram consists of two QPSK constellations overlaid on one another with a phase shift. As can be seen from the diagram, the transition from one symbol to another (indicated by the dotted lines) never goes through zero amplitude. For this scheme, the phase shift from the previous symbol indicates the binary bit pair of the new symbol. Therefore, $\pi/4$ – QPSK, like OQPSK, also reduces signal amplitude fluctuations significantly and thus reduces the magnitude of possible sidelobe regeneration. Interestingly, studies have shown that $\pi/4$ – QPSK performs better than OQPSK in the presence of multipath spreading and fading. NA-TDMA uses $\pi/4$ – QPSK digital modulation in a 30-kHz channel.

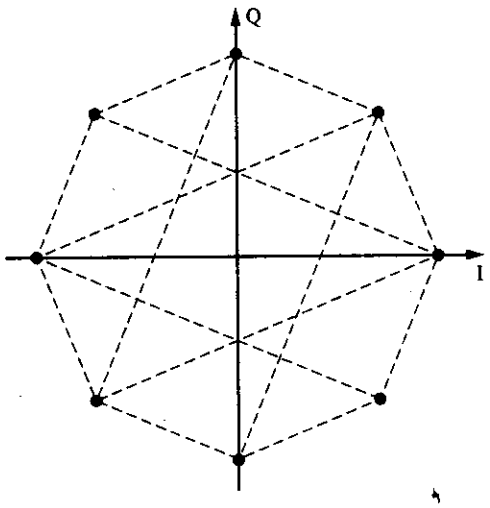



**Figure 8–14** Constellation diagram for $\pi/4$ – QPSK.

## OFDM

The modulation schemes just discussed were chosen to support wireless mobility in digital cellular networks. For wireless LANs and other last-mile fixed broadband wireless networks, where mobility is not the prime design factor, other modulation techniques have been examined and put into operation to support high-speed packet data transfer rates in these more benign, well-behaved wireless networks. During the late 1990s, orthogonal frequency division multiplexing or **OFDM,** a modulation technique gaining in popularity, was chosen as the modulation scheme for the IEEE 802.11a wireless LAN standard. OFDM is really a form of multicarrier, multisymbol, multirate FDM in which the user gets to use all the FDM channels

together. The term *OFDM* comes from the fact that the carriers of the FDM channels possess the property of orthogonality. Without going into the theoretical underpinnings of this concept, the simple definition of orthogonality implies that orthogonal signals will not interfere with each other at a receiver. This simple but extremely important concept can be used to enhance packet data transfer rates over fixed FDM transmission systems.

The implementation of an OFDM system is fairly straightforward. Instead of attempting to transmit $N$ symbols per second over a single forward carrier link, $M$ carriers (the multicarriers) are used to transmit $N/M$ symbols per second, which ends up yielding the same data transfer rate, $N$. Additionally, the frequency spacing between each carrier is chosen to satisfy the orthogonality criteria. For each carrier, a multisymbol digital modulation scheme is used to transmit more than 1 bit per symbol time. Typically, some form of n-PSK or n-QAM would be used for this purpose. Another feature of an OFDM system would be the ability for the system to sense the radio channel quality and be able to fall back to lower data rates as needed. This can be done with multirate modems that only transmit as many bits per symbol as the C/I rate allows. Most wireless LANs possess this built-in fall-back ability. As the user moves away from an access point, the C/I ratio usually decreases and the multisymbol, multirate modem used by the system changes to a lower but useable data rate. More practical implementation details of OFDM will be discussed in Chapter 9—Wireless LANs/IEEE 802.11x.

## 8.5 SPREAD SPECTRUM MODULATION TECHNIQUES

Another type of modulation technique used for wireless systems is known as **spread spectrum modulation.** Although this technique was first used by the U.S. military and is over fifty years old, it was not used in commercial wireless systems until the 1980s. Amazingly enough, at this time, spread spectrum modulation, implemented as some variation of CDMA technology, is expected to be the basic modulation scheme of choice for all future 3G system implementations including the upgrade of GSM/NA-TDMA wireless. Additionally, the IEEE 802.11 wireless LAN standards have also adopted it. One would have to believe that spread spectrum technology was adopted for wireless LAN use primarily due to the fact that the FCC first released spectrum allocations for wireless LANs in the unlicensed ISM bands and now in the unlicensed U-NII bands under the proviso that devices operating in these bands use spread spectrum modulation. Spread spectrum modulation has many qualities that have led to its embrace as the modulation scheme of the future. Some of these advantages are the ability to overlay a spread spectrum system over a frequency band with already deployed radio services, extremely good anti-interference characteristics, high wireless mobile system capacity, and robust and reliable transmission over radio links in urban and indoor environments that are susceptible to intense selective multipath conditions. There are two basic ways of implementing spread spectrum transmission: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). The next sections will provide additional details about these techniques.

### Frequency Hopping Spread Spectrum

Frequency hopping spread spectrum is a relatively simple technique, the invention of which is credited to a movie star named Hedy Lamarr. FHSS consists of a system that changes the center frequency of transmission on a periodic basis in a pseudorandom sequence. There are usually a limited number of different carrier frequencies to hop to and the hopping sequence is designed in such a fashion as to keep the occurrence of the various hopping frequencies statistically independent from one another. For the system to work both the transmitter and receiver must have prior knowledge of the hopping sequence. Figure 8–15 shows an example of a FHSS system.

As the transmitter implements the hopping sequence the effective signal bandwidth increases to include all of the utilized carrier frequencies. However, the instantaneous bandwidth is just that of a single modulated carrier. The use of FHSS does not provide any improvement in a noise-free environment. However,

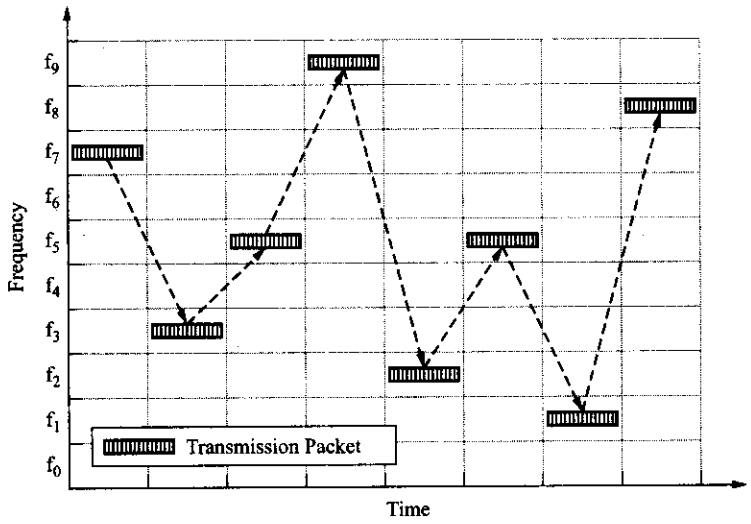



**Figure 8–15** Frequency hopping spread spectrum example.

for the situation where narrowband noise exists or deep-frequency selective fading is prevalent, the FHSS scheme will allow only a small fraction of the transmitted data to be corrupted while the rest of the transmitted information remains error free. The IEEE 802.11 standard specifies that the system may use FHSS techniques during operation. In an effort to improve GSM transmission reliability and system capacity, frequency hopping is sometimes implemented within a cell. In one typical GSM implementation of this technique, each transmitter will always transmit on the same frequency. However, the physical channel data will be sent from different transmitters with every burst. A variation on this is to have the physical channel data sent from the same transmitter all the time but the transmitter will use a new frequency with every burst.

## Direct Sequence Spread Spectrum

The second form of spread spectrum is direct sequence spread spectrum. DSSS has been previously discussed in reference to CDMA technology in Chapter 6. In this case, a spreading code is applied to the baseband data stream at the transmitter and the same spreading code is applied to the received signal to perform demodulation. As with FHSS, both the transmitter and the receiver must have knowledge of the "key" spreading code in use for the DSSS system to work properly. Since the spreading chips are themselves many times shorter in duration than the baseband bits that they are encoding and spreading, the final transmitted signal now consists of many more bits or symbols per second than the original data stream. The number of chips per second now determines the basic bandwidth of the transmitted signal. For IS-95 CDMA, the chip rate is 1.2288 mcps and the approximate real-time signal bandwidth is 1.25 MHz. Higher additional chip rates are specified for used in the cdma2000 standard. DSSS systems enjoy the improved noise immunity provided by the increased signal bandwidth.

To improve the noise immunity characteristics of wireless mobile DSSS systems and to allow more than one signal to be transmitted on the same carrier frequency simultaneously, special orthogonal Walsh codes are used as part of the spreading process. At the transmitter, in this scheme, many signals of the same carrier frequency, each carrying different payloads, may be spread by different Walsh codes. Then, at the receiver each carrier (of the same frequency) spread with a Walsh code other than the "key" Walsh code appears to the receiver as a noise signal. This property is exploited as has been discussed before to increase the capacity of a limited amount of frequency spectrum.

### Other Coding Forms

There are numerous other techniques that have been researched and developed to modulate signals for the effective transmission of data over the radio channel. Each of these techniques usually provides some improved transmission enhancement or some type of benefit to the user at the cost of another transmission characteristic. Some of these techniques have been employed in commercial systems whereas others have not yet left the laboratory. Two techniques that should be mentioned are pulse position modulation (PPM) and complementary code keying (CCK). PPM is an older technique that embeds information in the position of a pulse or codeword relative to a fixed periodic time signal. This technique has been explored in conjunction with relatively new ultra-wideband radio technology, the subject of the next section of this chapter. CCK is a form of modulation where a stream of data bits to be transmitted is subdivided into groups of bits and then each group is encoded by a special orthogonal code (a polyphase complementary code in the CCK case). IS-95 CDMA uses a similar technique on the reverse radio link channels by encoding every 6-data-bit combination as one of sixty-four, 64-bit Walsh codes. The IEEE 802.11b standard adopted a form of CCK to increase the maximum data transmission rate from 2 mbps to 11 mbps for 802.11 wireless LANs. For this new standard, with CCK, the chip rate and the signal bandwidth remained constant but the data rate was increased to 11 mbps.

## 8.6 ULTRA-WIDEBAND RADIO TECHNOLOGY

Recently, a great deal of interest has been generated by the emerging use of **ultra-wideband** (UWB) radio technology. Using this technology allows for the overlay of novel radio services into preexisting frequency bands. This technology is extremely well suited for the short-range application space (i.e., IEEE 802.15) and has recently received regulatory approval from the FCC in the United States. Its use is predicated on the innovative approach of effectively sharing radio frequency spectrum instead of looking for new frequency bands for new services. At this time, a number of potential uses of UWB technology have been identified. A brief list includes imaging systems (ground-penetrating radar), vehicular radar, measurement and positioning systems, and data communications. Practical data communications uses include high-data-rate wireless personal area networks, future advanced intelligent wireless area networks, and measurement and sensor applications linked to a support network.

Using extremely narrow pulses (subnanosecond to nanosecond) UWB radio systems are able to provide high-data-rate (100 to 500 mbps) transfers over short distances (1–10 meters). At the same time, the bandwidth of such a high-data-rate UWB system may extend over several to many GHz within the FCC-allocated 3.1- to 10.6-GHz range. Many modulation schemes have been proposed for UWB including PPM. However, the technologic challenge comes when attempting to adapt UWB technology to multiple user scenarios. Presently, numerous researchers are busy finding ways to implement UWB radio technology solutions for wireless applications. More details about UWB will be given in Chapter 10—Wireless PANs/IEEE 802.15x.

## 8.7 DIVERSITY TECHNIQUES

As has been explained earlier, the biggest problem encountered in the use of the urban mobile radio channel is the large and rapid fluctuations that can occur in RSS due to multipath fading. It is impractical to try and counteract the diminished RSS by raising the system transmitting power since typical fades can cover several orders of magnitude with deep fades covering over three or four orders of magnitude, well beyond the limits of transmitter power control systems. The most effective technique that can be used to mitigate the effects of fading is to employ some form of time, space, or frequency diversity for either or both the transmission and reception of the desired signal. The basic idea behind these solutions is that fading will

not remain the same as time passes nor will it be the same over different signal paths or for different frequencies over the same paths. There are several methods that can be used to provide diversity to a wireless mobile system. In each case, several different received signals are usually combined to improve the system's performance. Some of the more popular ways to obtain two or more signals for this purpose are to make use of specialized receivers, physically provide additional antennas, operate over more than one frequency, and use smart antenna technology. The operation of a system over more than one frequency has been previously addressed during the discussions of FHSS, GSM frequency hopping, and multicarrier systems. Therefore, this topic will not be pursued any further here. The next several sections will address the other techniques that have been mentioned and some newly emerging technologies.

## Specialized Receiver Technology

In an effort to combat multipath effects, several innovative receiver implementations have been created. Recognizing that multiple signals will arrive at a receiver over the mobile radio channel, these receivers exploit that fact by isolating the signal paths at the receiver. Furthermore, if one recognizes that the fading of each multipath signal is different, then it can be seen that this isolation process will in fact yield the diverse signals needed to improve receiver performance. An early embodiment of this concept is the **RAKE receiver** originally designed in the 1950s for the equalization of multipath. See Figure 8–16 for a block diagram of the structure of a typical RAKE receiver used for CDMA.

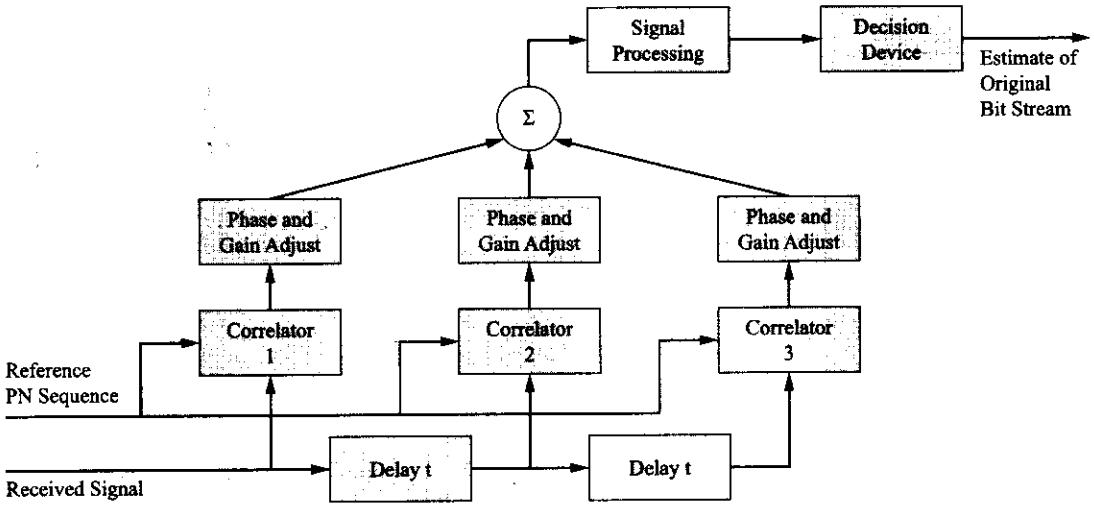



**Figure 8–16** RAKE receiver block diagram.

Modern, digitally implemented RAKE receivers used in today's CDMA wireless mobile systems may only have a few RAKE taps but possess the ability to dynamically adjust the taps (move the rake fingers) in response to a search algorithm used to locate multipath components. These smart receivers can generate several signals that can be further combined by several standard diversity combining techniques to provide a more reliable receiver output and therefore improve system performance.

There are potential problems with this type of receiver that are tied to the multipath delay and spread introduced to the radio link. The multipath components that can be resolved have a time dependence that is proportional to the inverse of the system chip rate and the system-tolerated multipath spread is proportional to the inverse of the symbol time. For the IS-95 CDMA system, using a chip rate of 1.2288 mcps allows the resolution of multipath components of the order of approximately 1/1.2288 mcps or 800 ns by the RAKE receiver. For a symbol rate of 14.4 kbps (encoded with QPSK) a multipath spread of up to approximately

1/7200 or 140 s may be tolerated without ISI. Since the typical multipath spread for an outdoor environment is in the order of tens of microseconds and for indoor environments nanoseconds, CDMA systems do not suffer from ISI and these types of receiver can be implemented. However, in an indoor environment the CDMA RAKE receiver would not be able to resolve multipath components.

The GSM system employs an equalization technique at the receiver to improve system performance. As outlined in Chapter 5, a training sequence of 0s and 1s is transmitted during the middle of a normal burst of user data (refer back to Figure 5–15). The receiver uses this training sequence to train the complex adaptive equalizer incorporated into the GSM mobile receiver to improve system performance. Due to the complexity of these systems no further details will be presented here.

## Space Diversity

A typical technique used to improve mobile wireless system performance is to employ **space diversity** in the form of additional receiving antennas located at the base station. At this time it is still problematic to achieve antenna diversity for a mobile station due to its typically small size in relation to a wavelength of the radio frequency employed. This fact may change in the near future with the adoption of advanced antenna technology schemes (MINO, smart antennas, etc.). In theory, the paths taken by the reverse signal to arrive at each antenna will not be affected equally by multipath fading or spread. There are many ways to achieve the needed space diversity at the base station site. Figures 8–17 shows several practical implementations.

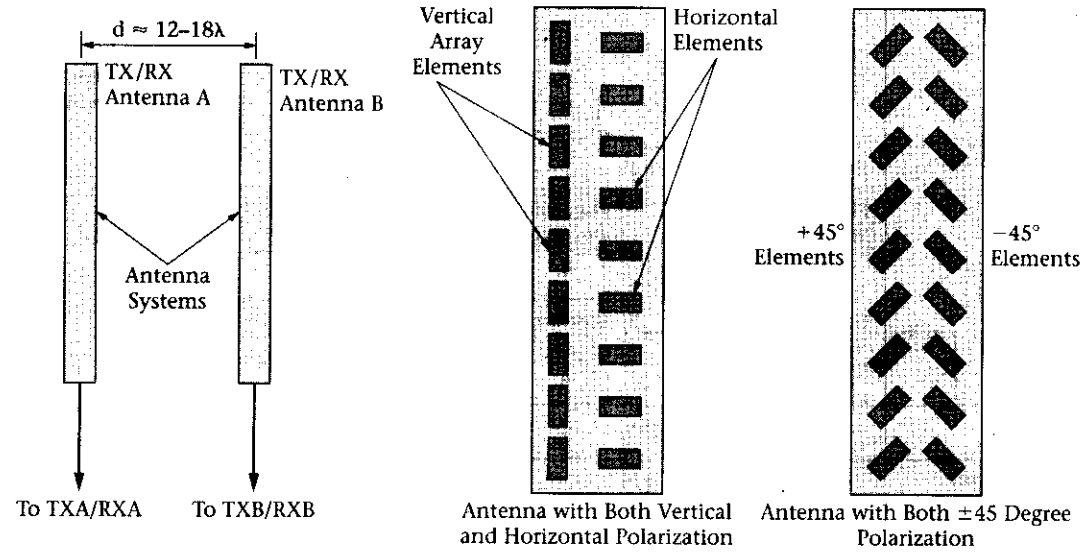



**Figure 8–17** Space and polarization diversity antenna schemes.

As can be seen in the figures, both space and polarization diversity can be used by the appropriate positioning of the antenna units. The antennas feed multiple receivers, with the strongest received signal being used by the system. This technique is universally implemented by wireless mobile service providers in the design of their systems. Polarization diversity is used to counter the change in EM signal polarization that can be induced by the environment during reflection, scattering, and so on.

## Smart Antennas

In the 3G specifications, the support of smart antenna technology is included. This technique to improve system performance makes use of phased array or "beam steering" antenna systems. These types of antennas can

use narrow pencil-beam patterns to communicate with a subset of the active users within a cell. Once a mobile subscriber has been located by the system, a narrow radio beam may be pointed in the user's direction through the use of sophisticated antenna technology. The use of a radio link that approaches point-to-point type link characteristics is extremely useful in a mobile environment. Besides the elimination of most multipath signals, a fact that will certainly improve system performance, the amount of interference received will be reduced and system capacity can be increased. As the mobile user moves about the coverage area, the smart antenna will track the mobile's motion. See Figure 8–18 for a depiction of a smart antenna system.

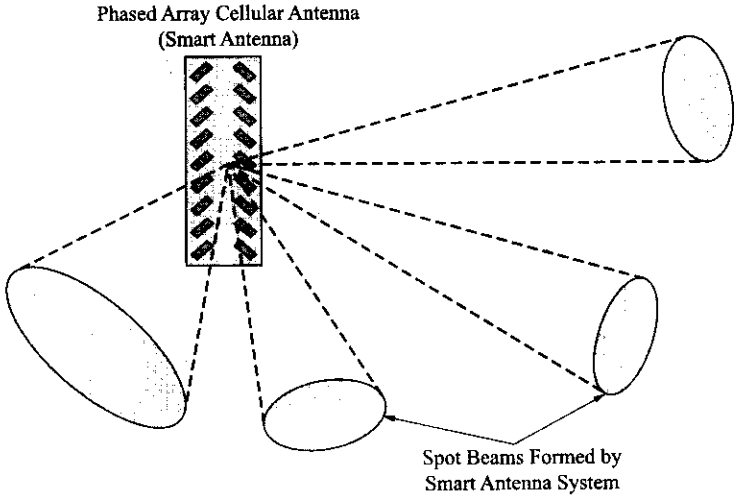


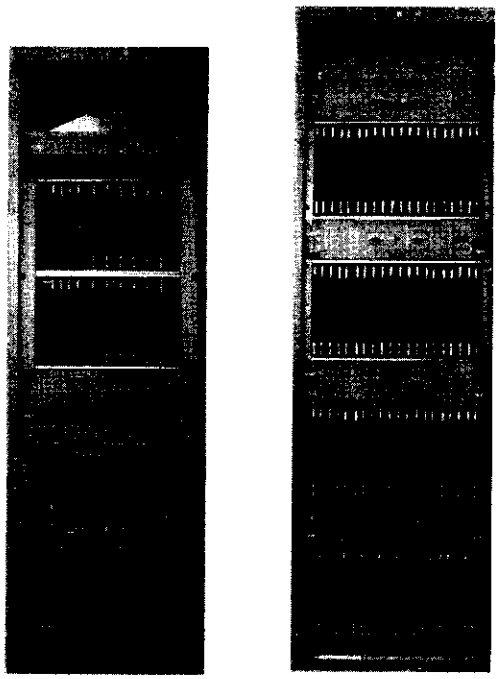

**Figure 8–18** Depiction of a 3G smart antenna system.

### Single Antenna Interference Cancellation

Single antenna interference cancellation (SAIC) is a newly developed technique that can be used to improve the downlink performance of a GSM system. To fully benefit from this technology the GSM system should be synchronous (i.e., tied to the timing of the GPS system). Interestingly, for synchronous GSM systems, the benefit of applying frequency hopping to such systems also improves. SAIC uses either of two sophisticated algorithms to cancel interference from the dominate interferer. The two types of techniques that can be used are known as joint detection (JD) and blind interference cancellation (BIC). In both cases, the systems tend to suppress interference that would normally increase the bit error rate of the system. Hence, the overall system BER characteristics are improved. SAIC can in theory increase the capacity of present GSM systems if changes to the system (timing) and the mobile receivers (more complex detection algorithms) are put in place.

## 8.8 TYPICAL GSM SYSTEM HARDWARE

In this and the next section, a more detailed look will be taken at the actual hardware implementation of the base station subsystem (i.e., base station controller and radio base station). The primary focus of this section will be on the system-level details of typical 2.5G+GSM hardware. The GSM BSC/TRC (and the newer 3G RNC) will usually be centrally located within the system coverage area. Housed in standard radio relay-rack frame configurations (several cabinets may be needed), the typical BSC/TRC or RNC can manage a number of radio base stations (base transceiver stations) in a serving area of a GSM or 3G UMTS network. See Figure 8–19 for pictures of a typical BSC and a standalone TRC system.



BSC TRC

**Figure 8–19** Typical GSM cellular BSC and TRC (Courtesy of Siemens).

The typical RBS is located at the cell site (antenna site) and consist of either a self-contained, environmentally conditioned, stand-alone unit that can be located outdoors on a concrete pad (see Figure 8–20) or a unit housed in a standard radio relay rack for placement in a controlled environment structure with other equipment (refer back to Figure 8–19).

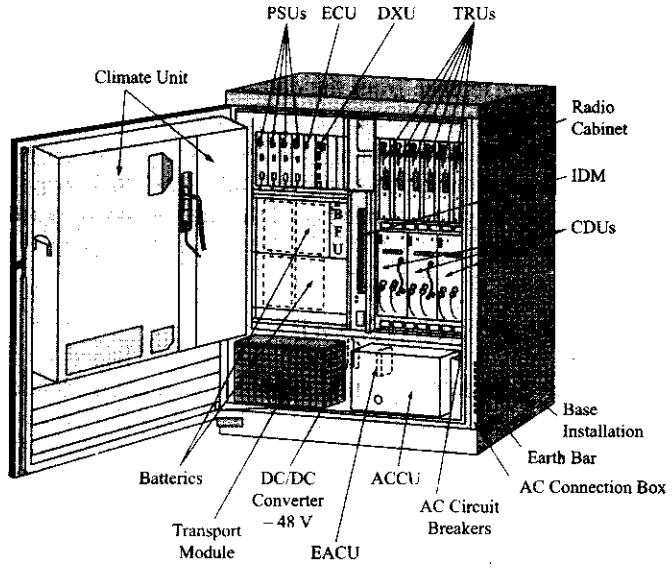



**Figure 8–20** Typical outdoor radio base station (Courtesy of Ericsson).

The next several sections will provide details about these air interface-related network elements and the subsystems that they consist of. It is always risky to provide a snapshot in time of any type of telecommunications hardware (since it is always in a constant state of transition). However, an attempt will be made here to provide an accurate picture of the state of the art in wireless mobile systems hardware.

## Base Station Controller

Figure 8–21 shows a block diagram of a typical BSC with the major subsystems designated. These subsections are input and output exchange/interface circuits, a group switch, a subrate switch, a transcoder and rate adaptation unit, an SS7 signal terminal, a packet control unit, and numerous embedded microcontrollers to provide control functions. Also shown are the communication links that connect the BSC to the MSC and the RBS. It is possible to separate the transcoder function from the BSC but this is not shown here. The next sections will describe the function of these major BSC subsections.

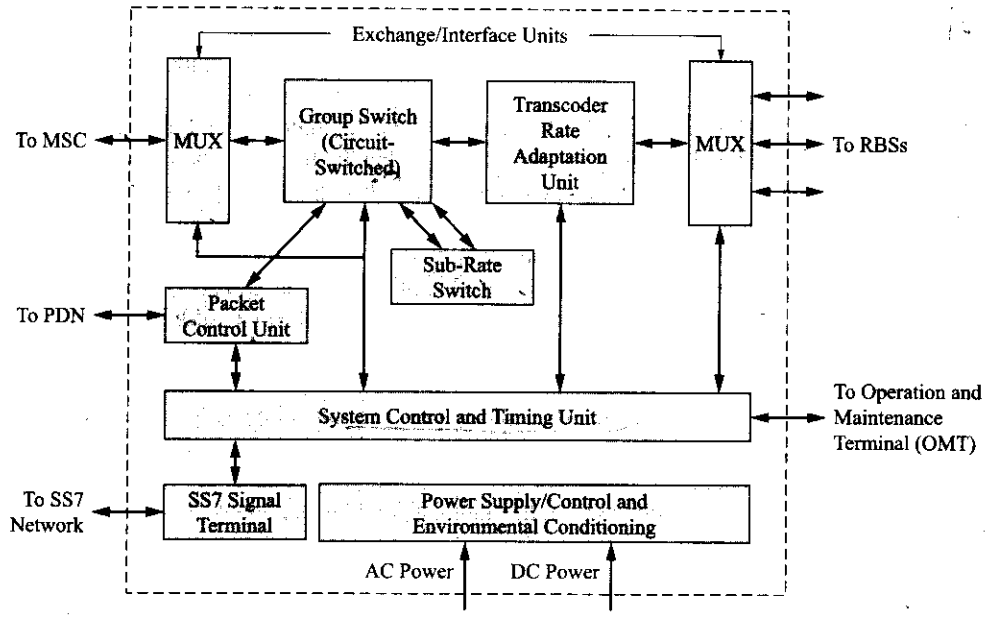



Figure 8–21 Typical GSM BSC block diagram.

### *Specific BSC Parts*

The BSC consists of several subsections that perform the functions of interfacing the RBS to the MSC and the PDN, allocating radio resources to the mobile subscriber, and managing aspects of power control and mobility. These subsections and their functions will be described here.

The exchange/interface circuits are basically multiplexer/demultiplexer units that can provide interconnections to the MSC, PDN, or RBSs. Traditionally, the connection from the MSC to the BSC and from the BSC to the RBS is provided by leased T1/E1/J1-carrier circuits. The connection from the MSC (PSTN) to the BSC provides 64 kbps PCM voice signals and also call control (LAPD) information messages. The T1 signal carrying twenty-four DS0, 64 kbps voice signals must be demultiplexed at the BSC to provide individual signals to the group switch. Once the voice signals from the PSTN have been transcoded, they are multiplexed together and forwarded to the proper RBS over T1/E1/J1 facilities at a much lower bit rate. Conversely, vocoded speech from the RBS must be converted (transcoded) to PCM and multiplexed before being sent to the PSTN via the MSC. A high-speed 155 mbps fiber-optic link from the PDN is typically

connected to another exchange/interface circuit that provides multiplex/demultiplex functions and buffers the high-speed packet data. The packet data is also applied to a group switch to be directed to the correct RBS.

The group switch is used to cross-connect 64-kbps timeslots, in essence, placing a call onto the correct timeslot on the correct communications link to the correct RBS. The subrate switch is able to switch traffic at submultiples of 64 kbps (i.e., $n \times 8$ kbps). Refer back to Chapter 3 for a more detailed discussion of the operation of a group switch.

The transcoder performs the translation of 64 kbps PCM into digitally encoded (vocoded) speech at rates of 13 kbps (full rate) toward the RBS and reverses the process toward the MSC. With full-rate speech, a 64 kbps PCM signal is converted to 13 kbps to which 3 kbps of overhead is added to bring the total to 16 kbps. Enhanced full-rate speech transcoding is similar. Half-rate transcoders decode and encode between 64 kbps and 6.5 kbps, with 1.5 kbps added to yield a rate of 8 kbps. Full-rate and half-rate data calls are rate adapted so that 14.4 kbps becomes 16 kbps and 4.8 kbps becomes 8 kbps. The new GSM adaptive multirate codec (AMR) defines multiple voice encoding rates (from 4.75 to 12.2 kbps), each with a different level of error control that brings the final data rate to the same total value for each. Depending upon the channel conditions the AMR codec can be directed to provide more or less error protection with the same basic data transfer rate over the traffic channels.

The packet control unit (PCU) resides in the BSC and provides the interface between the serving GPRS support node (SGSN) of the GPRS PLM network and the RBSs for the transmission of data over the GSM air interface. The connection from the packet control unit to the RBSs is able to provide data transfer rates of 16 kbps. Therefore, both circuit-switched calls and packet data transfers look identical to the GSM RBS. The upgrade to GSM GPRS service for a RBS can be performed by a software upgrade.

The typical relay rack cabinet housing a BSC consists of various subracks (shelves) (refer back to Figure 8–19) that usually contain one or more subfunctions of the entire system. In addition to the necessary power supply components and the cooling fans, there will typically be device subracks and a hub subrack (BSC system control). The device subracks (magazines) will house the low-speed exchange/interface circuit boards, transcoder and rate adaptation boards, and the packet control unit subsystem. In addition, the hub subrack will typically house the group switch, subrate switch, central processor boards, and device subrack connectivity board. An operation maintenance terminal (OMT) interface is provided by the BSC that allows for control/maintenance of the BSC system through OMT software. Alternatively, this function can be done from the MSC.

### *BSC Radio Network Operations*

The BSC is actively involved with performing certain network functions that are necessary to provide optimal radio resource management, connection management, and mobility management among other things. The RBS and the mobile station are constantly performing RSS measurements of the serving cell and handover candidate cells that are passed on to the BSC. The base station controller monitors the use of radio resources and the RSS measurements to make decisions about handover operations and power level control. The service operator can program the BSC to configure its serving area (consisting of from one to many RBSs) by assigning cell names, frequency channels, location area identifiers, RBS and mobile station power control levels and adjustment procedures, frequency hopping algorithms, signal strength thresholds, intracell handover locating data, neighbor relations, channel groups, cell load sharing, cell state, and other cell parameters. Furthermore, the configuration of control channel data, broadcast control channel data, and subcells is done through the BSC.

Additionally, the BSC can perform many system supervision functions on an hourly, daily, weekly, monthly, or some other (time period) basis. These functions can be written to a log and accessed by supervisory software that can perform statistical analysis of the data. Self-maintenance functions are also implemented by the BSC operating system. BSC alarms and abnormal conditions are logged and, if serious enough, escalated to a network level. The BSC monitors the RBSs that it serves and handles fault and alarm

conditions that might exist at an RBS. If necessary the BSC escalates the RBS alarms to a higher level (network). More detail about RBS maintenance will be provided shortly.

## Radio Base Station

The other necessary component of the base station subsystem is the radio base station (refer back to Figure 8–20). Located at the cell site close to the antenna, the RBS typically is a self-contained unit that contains several subsystems that perform the necessary operations to provide a radio link for the mobile subscriber. A communications link (Abis) exists between the RBS and the BSC to provide transfer of user data and network (LAPD) signaling messages. A block diagram of a typical RBS is shown in Figure 8–22. The primary subsystems of a GSM RBS are a distribution switch unit, several radio transceiver units, RF combining and distribution units, power supply units (PSUs), cooling system (fans), and a power distribution control unit. Additionally, for a stand-alone outdoor unit an environmental control unit (ECU) for heating and cooling is included. The base station also contains a memory unit that stores the most recent installation database (IDB) (the RBS configuration), various alarm indicators, and a communications interface that allows an operator to configure various operational parameters and perform maintenance functions through OMT software. Typical RBS units will utilize subracks to mount hardware within a relay rack. However, many new smaller, low-power RBSs are taking on nontradition form factors for use in micro- or picocell environments where they are mounted to interior walls of malls, on poles, or on the sides of buildings.

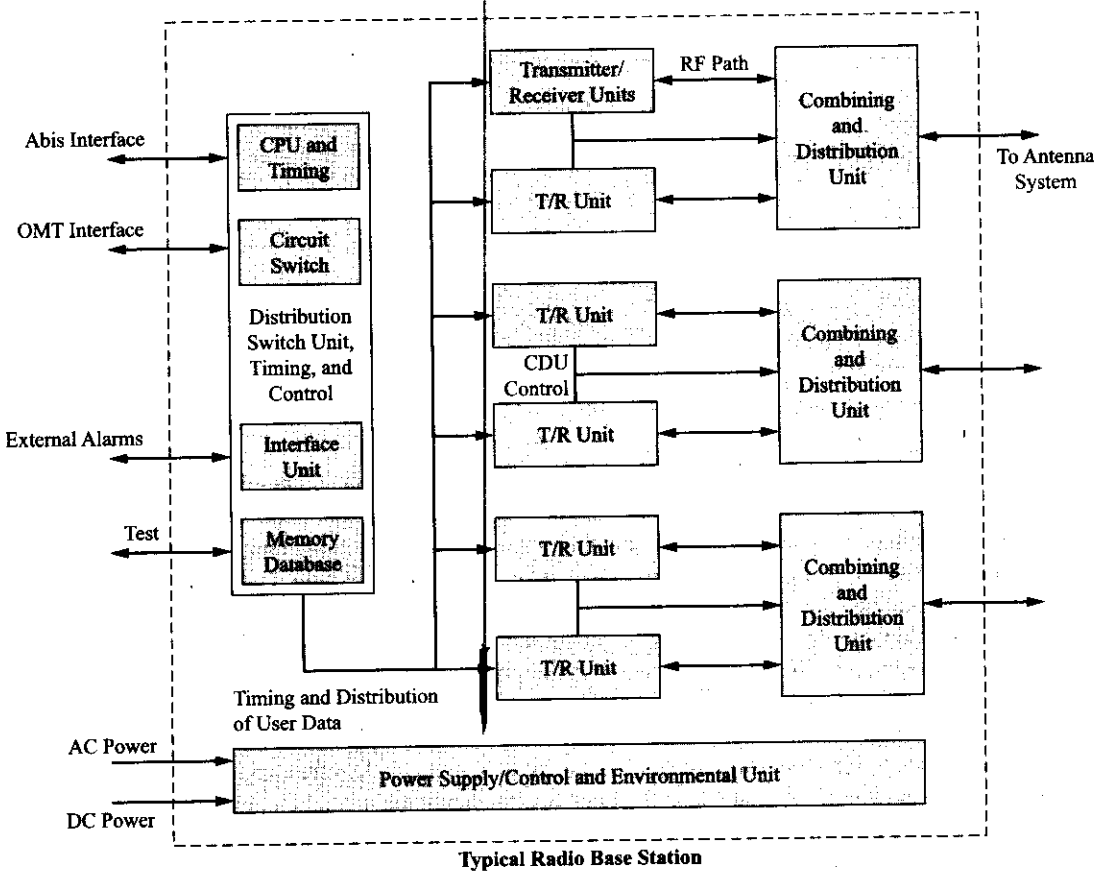



**Figure 8–22** Typical GSM RBS block diagram.

### *Radio Base Station Subsystems*

The distribution switch unit (DXU) serves as the radio base station master control unit. Its basic function is to provide RBS timing and to cross-connect user data being carried on a T1/E1/J1-carrier data link from the BSC with the correct RBS transceiver and timeslot. The distribution switch unit has several subsections that include a timing unit, an interface unit, a central processor unit (CPU), and an interface switch unit. The CPU carries out the resource management function within the RBS. Some of the functionality it enables is providing an interface to the OMT, providing internal and external alarm indications, decoding of LAPD signaling information, and loading and storage of software for the replaceable units within the RBS system. Furthermore, for ease of maintenance there is a stored database of information regarding the cabinet configuration (installed hardware) and each replaceable unit's configuration parameters. The main timing unit acquires its timing from the incoming bit stream and distributes it throughout the RBS system.

Some further details of the communication link between the BSC and the RBS are appropriate here. Figure 8–23 shows the Abis interface between the BSC and the RBS. It is a T1 facility carrying twenty-four DS0s. Each DS0 carries 64 kbps of data. As shown, three DS0s support one RBS transceiver unit by providing up to 64 kbps of LAPD protocol signaling and 128 kbps of user data (16 kbps per timeslot × 8 timeslots per transceiver carrier = 128 kbps). With this configuration eight RBS transceivers could be supported over one T1-carrier. Other more efficient configurations are possible by combining four LAPD signaling signals onto a single DS0. Also, if less than eight transceivers are used in a single RBS the T1-carrier could be used to drop feed other RBSs.

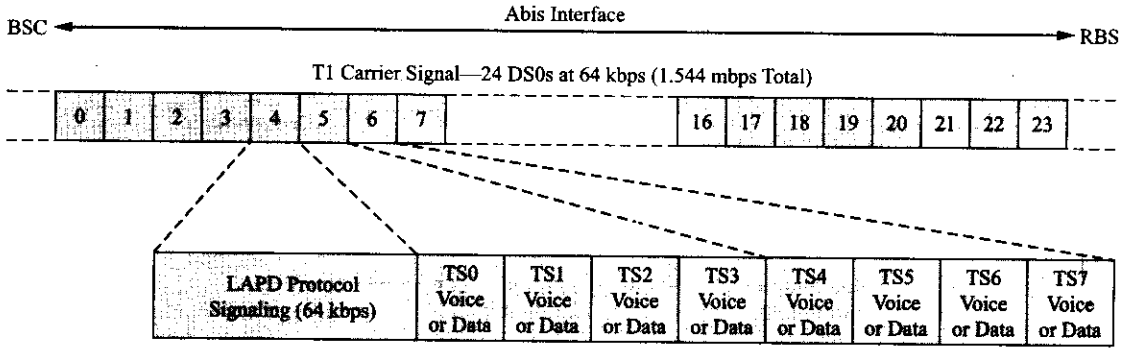



**Figure 8–23** Abis interface between the BSC and RBS.

The RBS transceiver units (TRUs) are transmitter/receiver and signal processing units that are used to broadcast and receive radio frequency signals that are sent over the radio link between the RBS and the mobile station. A transceiver unit typically contains three major subsections (see Figure 8–24): the transmitter section, receiver section, and the signal processing and control section. Each transceiver can handle eight air timeslots and has one transmit output and two receiver inputs for antenna diversity. There is also a test loop function that can be used to test the transmitter/receiver combination. The processing subsection acts as the transceiver controller. It interfaces with the other components of the RBS system over several different signal busses and performs downlink and uplink digital signal processing functions such as channel coding, interleaving, encryption, burst formatting, and the reverse functions for reception. Also, Viterbi equalization operations for receiving are performed by this section. The transmitter section performs the digital modulation, power amplification, and power control functions with typical maximum outputs in the 20-watt (+43 dBm) range. The dual receivers in the receiver section perform the demodulation function and pass the two signals on to the processing section.

RF combining and distribution units (CDUs) are used to connect several transceivers to the same antenna. The ability to share antennas is extremely important and several methods have been put into

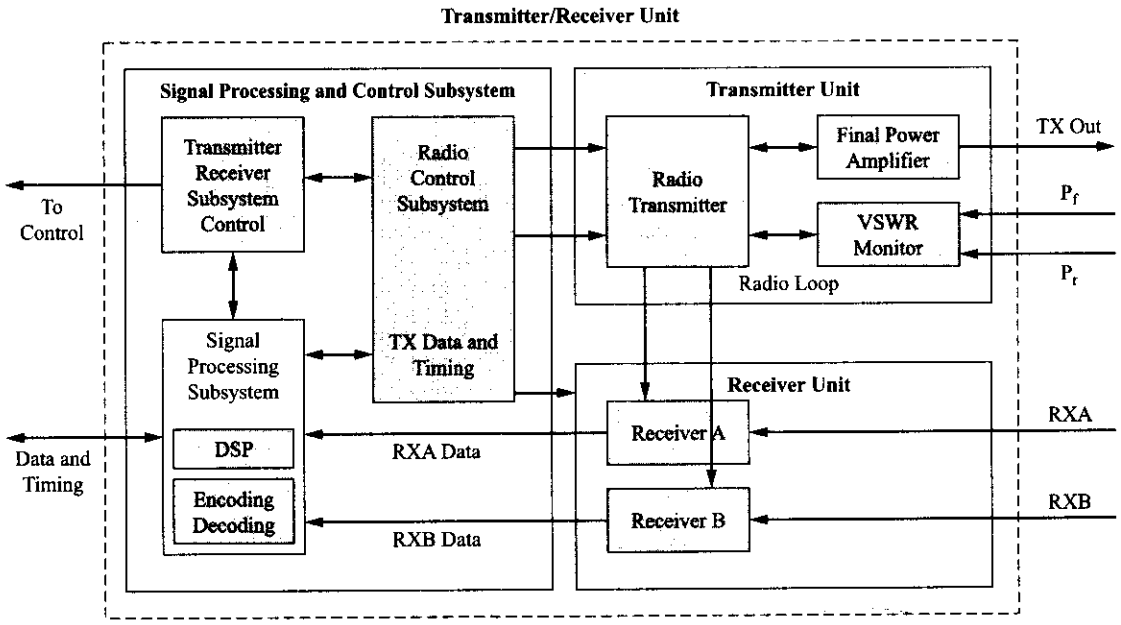



**Figure 8–24** Typical RBS transceiver unit.

practice to implement this. The two most popular methods either use a device known as a hybrid to construct a hybrid combiner or employ RF filters to perform the same function. A **hybrid combiner** is a broadband device that allows two incoming transmitter signals to be applied to it without the two original signal sources interacting with one another. The hybrid output consists of both input signals but their signal levels have been reduced by at least 3 dB. Older filter combiners use several bandpass filters (BPFs) constructed from mechanically tuneable resonant cavities. These high-Q BPFs allow the signal from each transmitter through but block the reverse transmission of any other transmitter signals. Today, hybrid combiners are gaining in popularity. A combining and distribution unit is a complex device that uses one of the methods discussed earlier to combine two signals but also includes additional functionality in the form of signal dividers and amplifiers to provide signals to more than one receiver, RF circulators or isolators to protect the transceiver from reflected RF power if a fault develops somewhere in the combining unit or at the antenna, and a measurement coupler that can provide accurate information about forward and reverse power for both power control and VSWR measurements.

If one desires to use the same antenna for both transmission and reception a **duplex filter** is needed. Figure 8–25 shows a typical duplex filter. Note that the unit consists of two BPFs that only allow the desired signals to pass. Duplex filters are also used with tower-mounted, low-noise amplifiers that are used to improve receiver sensitivity at the cell site. See Figure 8–26.

Before leaving this topic a typical RBS/antenna configuration will be illustrated (see Figure 8–27). For this case, a cell site houses a single RBS with two transceivers, and only two antennas are to be used. This would typically be a large, high-power omnicell. As shown by Figure 8–27, tower-mounted, low-noise amplifiers are used and each transceiver unit receives signals off of both antennas hence providing diversity. Antenna units will typically have gain factors associated with them that will increase the effective radiated power (ERP) of the system. Additionally, antennas will often be mounted in a down-tilted fashion to improve system operation. See Figure 8–28 for typical antenna configurations.

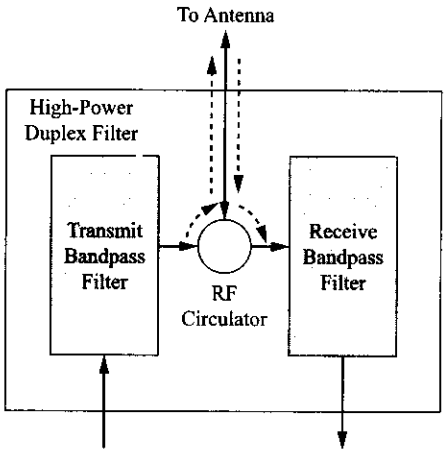



**Figure 8–25** Cellular duplex-filter block diagram.

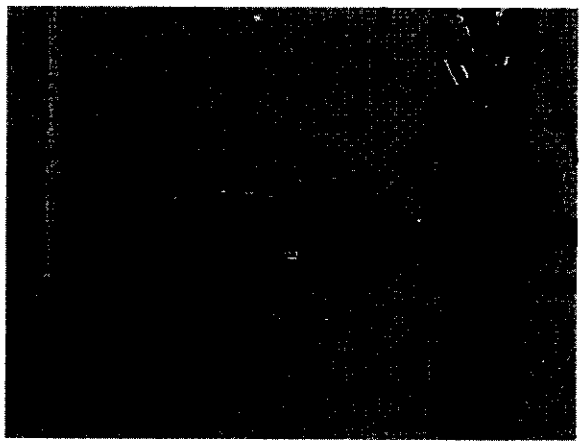


**Figure 8–26** Tower-mounted antenna amplifiers.

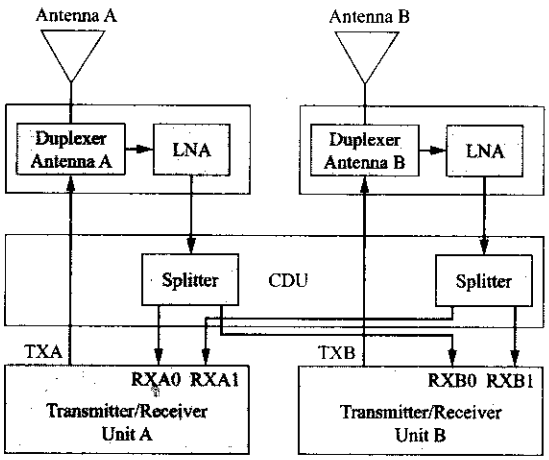



**Figure 8–27** Typical RBS/antenna configuration.

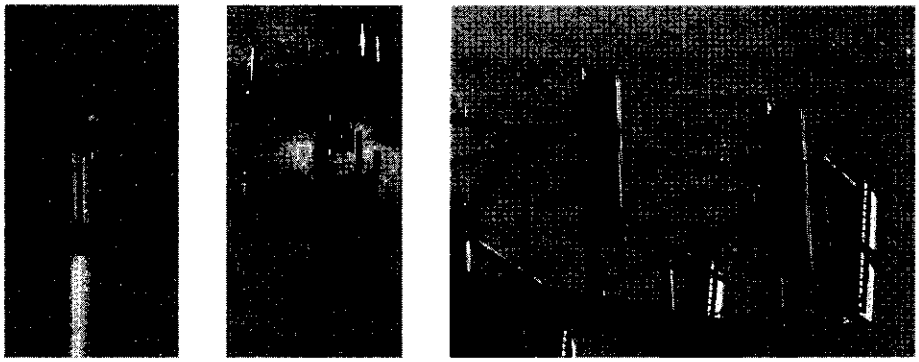


Figure 8–28 Cellular antenna systems (monopole and platform configurations).

### *Software Handling/Maintenance*

Today's RBSs are highly sophisticated, computer-controlled, complex transceivers. Through the use of an RS-232 "craft interface" port a service technician may gain access to a wealth of information about the RBS system's configuration and the present functionality of its subsystems through OMT software run on a laptop while on site or off-site through the BSC. OMT software allows one to examine the present system configuration as stored in the installation database of the central RBS control (distribution switch unit) or modify the system configuration and reload the new configuration into the system memory. Various RBS system parameters may be entered, modified, or recalibrated as needed. If a malfunction occurs, the Windows-based OMT software can be used to troubleshoot the system. Typically, OMT will allow the service technician to identify the faulty field replaceable unit (FRU) and it can be replaced. The OMT software deals with the hardware and software components of the RBS as managed objects (MOs). Furthermore, the MOs consist of either both hardware and software or software only. The managed objects are organized into a hierarchical structure for easier display and understanding of their function within the system. The RBS replaceable units are also organized in a hierarchical structure and are addressable by the OMT software using a GUI (point and click) type interface.

Summarizing, the OMT software tool is used during the RBS testing and installation process. It is also used for updating and maintaining the RBS internal database, for defining RBS external alarms, and during the performance of both preventive and corrective maintenance functions on the RBS.

## 8.9 TYPICAL CDMA SYSTEM HARDWARE

As was the case with our discussions of GSM and CDMA systems in earlier chapters, after a thorough coverage of one system, it is not necessary to repeat details of similar aspects of the other system unless there are significant differences between the two. In this section, only differences pertinent to CDMA hardware will be presented. The two basic components of the cdma2000 base station subsystem are still the BSC and RBSs. Recall that in cdma2000, the C-RAN consists of one or multiple base station subsystems and a radio network manager. The BSC provides access to the PSTN through the MSC and the PDN through the packet core network (refer back to Chapter 7). Typically, traditional T1/E1/J1 spans connect the MSC to the BSC. However, the system may use a fiber-optic connection from the MSC to the BSC and a multiplexer can be used at the BSC to convert the fiber-optic signals back over to the required electrical signals. The RBS can have several physical implementations including main and remote units. The next sections will take a closer look at these systems.

## Base Station Controller

The typical cdma2000 BSC or UMTS W-CDMA RNC is very similar to a GSM BSC and provides much of the same functionality to the system although there are some differences that should be pointed out. See Figure 8–29 for pictures of a typical W-CDMA RNC and RBS. The main cabinet of the BSC/RNC typically contains a connection backplane, power supply and cooling system, device subracks, and a hub subrack. The hub subrack contains the BSC/RNC system control, timing, and switching modules: central processing, GPS timing, interface to other BSS systems, RNM and OMT interfaces, packet core network interface, and device subrack connectivity all interconnected through an ATM switch.

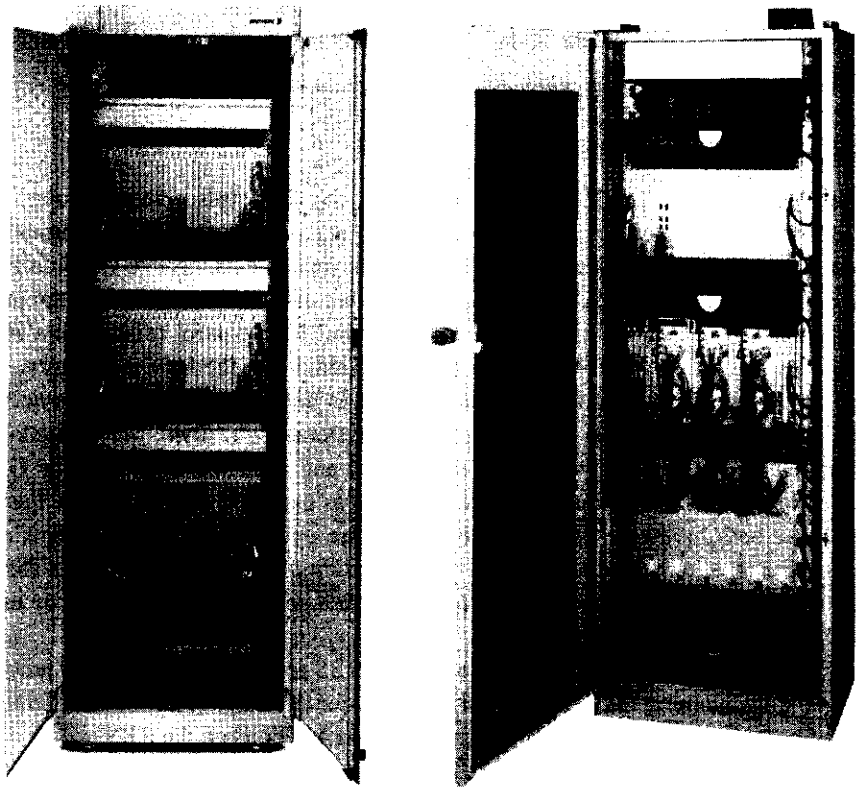


**Figure 8–29** Typical W-CDMA BSC and RBS (Courtesy of Ericsson).

The hub subrack contains exchange/interface boards that support ATM fiber-optic links to the PCN, a global positioning board (in conjunction with an external antenna) provides accurate timing signals to the BSC/RNC and in turn to the RBS, and additional exchange/interface boards provide T1/E1/J1 connectivity. The device subracks provide general processing, payload processing, ATM switching, service option processing (includes vocoding functions), an SS7 interface, an interface to the hub subrack, and an interface to the RBSs (T1/E1/J1 spans).

## Radio Base Station

The typical cdma2000 RBS looks very similar to a GSM or W-CDMA base station as can be seen in Figure 8–30. The RBS provides a radio link for the subscriber, CDMA encoding and decoding of the uplink/downlink signals, and supports subscriber mobility operations. The main control subsystem of the

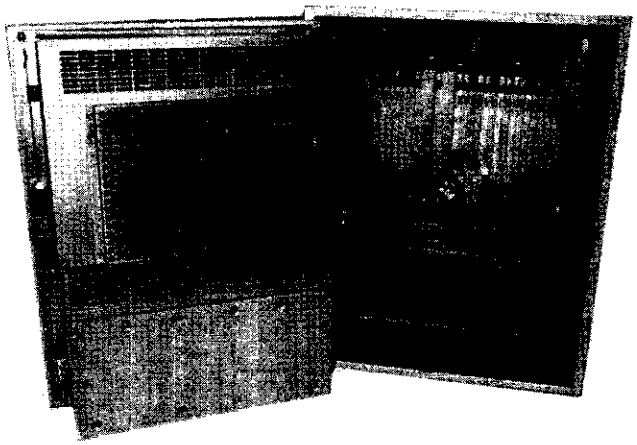


**Figure 8–30** Typical cdma2000 RBS (Courtesy of Ericsson).

RBS monitors and manages the RBS, provides the necessary system timing (synchronized to the GPS system), and provides alarm functions for the RNM or the local OMT connection. If the RBS consists of a main and remote unit, the main unit also provides timing, frequency references, and control messages to each remote unit over a communications link (typically, fiber optic). The transceiver portion of the CDMA RBS consists of channel cards that provide the main baseband signal processing functions for the CDMA code channels and an RF electronics processing module. These channel cards are capable of providing 128 uplink and 256 downlink channel elements. On the downlink they provide CDMA encoding and on the uplink they provide CDMA decoding using the techniques set forth in Chapter 6. Each card supports one carrier and three sectors. The RF electronics and power amplifier portion of the RBS may be colocated with the main unit or remotely located close to the system antenna elements. Over another optical link, baseband signals from the channel card consisting of pilot, sync, paging, and traffic channel elements are fed to the RF processing electronics and high-power RF amplifier. Similarly, received signals are amplified and down converted to baseband signals and then sent to the main unit for further processing over the fiber link.

The reader is reminded that the total RF output power of the CDMA transmitter is shared among all the individual channel elements that are being transmitted concurrently. Typically, an RBS can output approximately 20 watts per carrier. In this case, the pilot channel would have a power of 3 watts (15% of the total output power), the sync channel a power of .3 watts (10% of the pilot power), and the paging channel approximately 1 watt (35% of the pilot power). This leaves approximately 16 watts to be shared equally among system users. Therefore, if thirty- two users shared the system, and each user was approximately the same distance from the RBS, each traffic channel element would have approximately 0.5 watts of power associated with it. Recall that the CDMA antenna will typically have a fairly high gain associated with it (10–20 dB) that will raise the final ERP greatly. Also recall that the sophisticated CDMA forward link power control process will adjust the RBS traffic channel output power accordingly.

## 8.10 SUBSCRIBER DEVICES

Today, subscriber devices are like personal computers (PCs) were a decade ago when the reduced cost and increased capabilities of ICs made it possible to introduce new functionality and features into the desktop PC model that up until that point were prohibitively expensive. Each manufacturer of mobile devices has numerous products that provide from basic cell phone functionality up to the newest and highest-resolution color displays and color cameras that can be used for wireless multimedia applications. For twenty years the PC industry drove the semiconductor industry. Recently, we have entered into an era when the mobile device is driving the semiconductor industry.

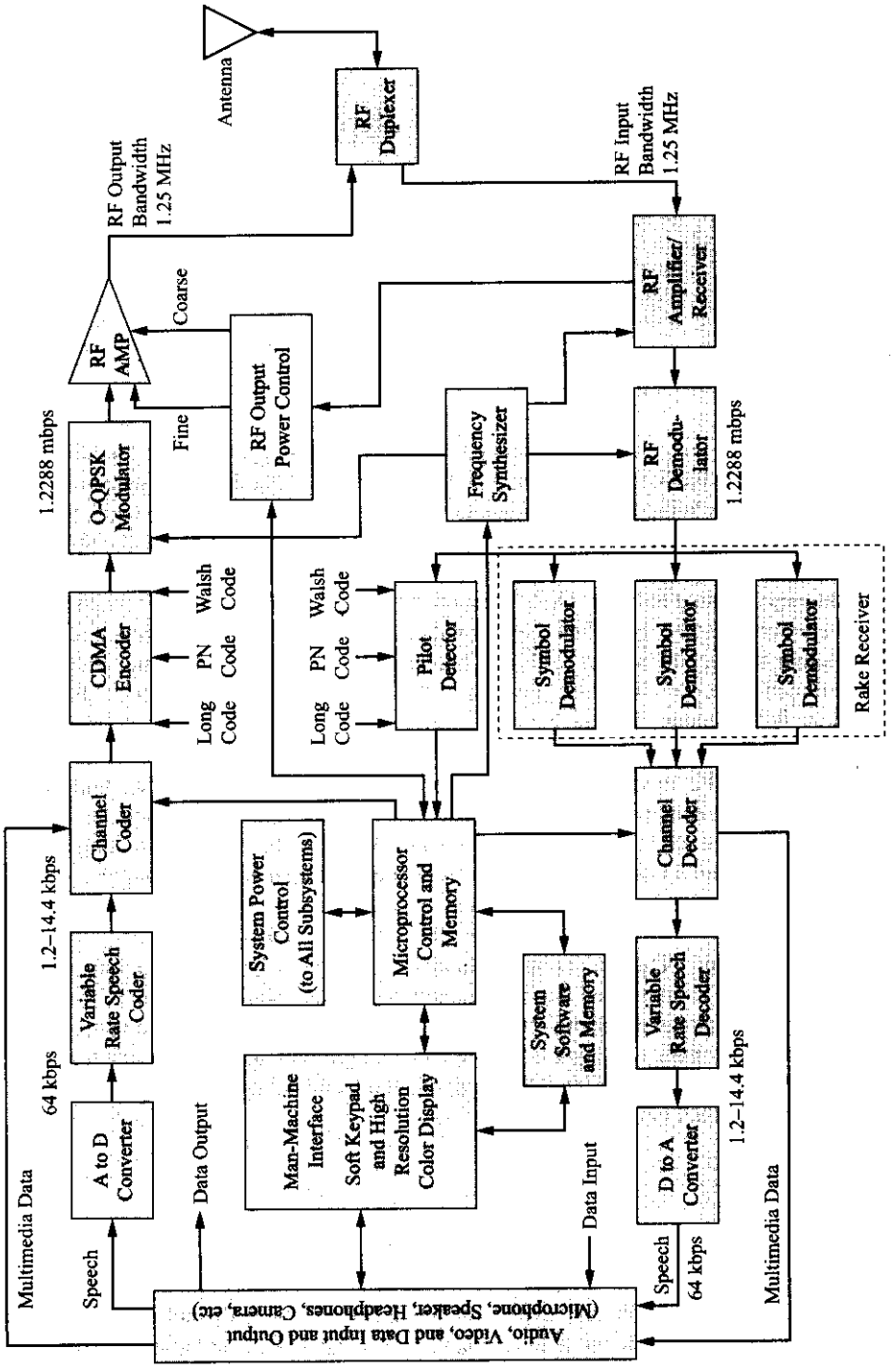



**Figure 8–31** Typical cdma mobile phone block diagram.

This section will not attempt to provide a detailed description of today's enhanced mobile devices for they are not devices that are foreign to the general public. Quite the contrary, with over one billion cell phone users in the world these devices are part of our everyday experience. Most subscribers to wireless mobile service have several old mobiles sitting around somewhere in their home or apartment that were abandoned after their previous service contract (or contracts) expired. Presently, the average life span of a mobile device is less than two years. With the rapid changes in microelectronics technology that have and continue to occur, that two- to three-year-old cell phone or PDA begins to look like quite a relic! Besides, today's mobile devices are "throw-away" or warranty replacement products for which repairs are typically not even attempted. It is truly amazing that we have evolved electronics to the point that the typical mobile device has more processing power than the million-dollar mainframe computers of a bygone era that occurred only twenty-five years ago.

## CDMA Mobile Radios

The basic block diagram of an early dual-mode phone has been introduced earlier in this text (Chapter 3) and received some discussion at that time. For the sake of continuity, a short description of a CDMA mobile phone will be included here. See Figure 8–31 for a typical block diagram. For any mobile device there needs to be a man-machine interface. This is where most of the action is today as high-resolution displays, high-quality sound, and color cameras allow for the display and transmission of multimedia signals provided in real time. To provide the radio link to the wireless network an RF section that provides digital transmission and reception functions is necessary. In many cases, dual- and tri-mode radios (different frequency bands and modulation schemes) are becoming commonplace. To deal with the ever increasing receiver complexity a high-speed digital signal processing (DSP) section is also required for the processing of various codes and complex noise reduction schemes. In time, the reprogrammable or reconfigurable software radio will provide the radio functionality for the mobile device. Lastly, there must be a power supply section that powers the unit. As more processing power, memory storage, video, and display technology is integrated into the mobile device this part of the device takes on a more important role. Sophisticated power control intelligence is being built into newer devices to achieve higher efficiencies of operation. The reader is urged to go to the Web site of a mobile device manufacturer to see what the newest and best device has for features and functionality.

# QUESTIONS AND PROBLEMS

1. Describe the function/purpose of a transmission line.
2. What technique is used to compensate for noise problems (i.e., bit errors) encountered when transmitting digital information over conductor-based transmission lines?
3. What advantages do fiber-optic cables have over conductor-based transmission lines?
4. Convert the range of frequencies from ELF to EHF (3 kHz to 300 GHz) to a corresponding range of wavelengths.
5. What three basic EM wave propagation effects are most likely to affect cellular wireless operation?
6. What EM wave propagation effect can illuminate a shadow area behind an object?
7. Define the term *multipath* in the context of EM wave propagation.
8. Why is the free space path loss model inappropriate to apply to wireless cellular operation?
9. If the transmitted power is 600 mW at a frequency of 850 MHz, determine the path loss at a distance of 5000 meters and the received signal power in dBm. Use the free space path loss model.
10. What is the basic difference between the two-ray path loss model and the free space path loss model?
11. Repeat Problem #9 using the distance-power gradient model (Equation 8-6) using $\alpha = 4$.
12. Repeat Problem #9 using the distance-power gradient model (Equation 8-6) using $\alpha = 3$.
13. Describe the basic operation of an ARQ scheme.
14. What is the basic purpose of a block code?

15. How many output bits are produced when a 256-bit digital word is applied to a convolutional encoder with $R = 1/3$?
16. Describe the basic process involved in the block interleaving of data bits before transmission.
17. What is the basic advantage that digital modulation offers?
18. Describe 8-PSK modulation.
19. Describe an OFDM modulation system.
20. If an OFDM system transmits 32 kbps over each carrier and uses 16 carriers, what is the overall data rate?
21. Describe FHSS operation.
22. Describe DSSS operation.
23. Define ultra-wideband radio technology.
24. What type of radio pulses are used by UWB?
25. Describe the basic theory behind the use of diversity in a wireless system.
26. Describe the basic theory behind the operation of a RAKE receiver.
27. Describe the usual implementation of space diversity for a wireless system.
28. Describe how polarization diversity is implemented for a cellular wireless system.
29. Describe the operation of an RF combining unit.
30. What function does the distribution switch unit serve in a GSM radio base station?
31. Describe the function of a cellular duplex filter.
32. How is maintenance usually performed on a modern cellular radio base station?
33. What is OMT software?
34. What timing standard does the typical CDMA system use?
35. How is CDMA system timing achieved?
36. If a certain CDMA radio base station can output a 50 watt carrier signal, how much power is in the pilot channel? How much power in the sync channel?
37. What is the ERP for a CDMA radio base station that can output 10 watts and has a 17-dB antenna gain?
38. Describe the man-machine interface of a cellular wireless mobile radio.
39. Visit the Web site of a mobile phone manufacturer and list the features of the newest models.
40. What is meant by a multimode mobile phone?

CHAPTER 9

# Wireless LANs/IEEE 802.11x

Upon completion of this chapter, the student should be able to:

- Discuss the basic differences between wireless LANs and wireless mobile systems.
- Discuss the evolution of the IEEE 802.11 standard and its extensions—IEEE 802.11x.
- Discuss the fundamental differences between wired and wireless LANs.
- Explain the basic architecture of IEEE 802.11 wireless LANs.
- Discuss the services offered by the wireless LAN MAC sublayer.
- Discuss the MAC layer operations used to access and join a wireless network.
- Explain the basic details of WLAN FHSS and DSSS physical layers.
- Discuss the adoption of the higher-rate IEEE 802.11x standards and the technical details of IEEE 802.11b/a/g.
- Discuss the present status of wireless LAN security as embodied by IEEE 802.11i.
- Discuss the status of competing wireless LAN technologies.
- Discuss typical wireless LAN hardware and system deployment strategies.

This chapter is the first of several chapters that introduces another class of wireless network technologies. Until this time the focus of this text has been on wireless mobile networks that provide mobile subscribers with voice and data service via connections to the PSTN and the PDN. In addition, these wireless networks also provide the mobile user with near seamless mobility on a national and soon-to-be-global scale. Starting with this chapter, attention shifts to the IEEE standardized specifications for wireless LANs, PANs, and MANs. These standards form the basis for the implementation of high-performance wireless computer networks that are used in a variety of different operating spaces (i.e., short, medium, and long range) with a wide range of data throughput speeds.

This chapter will discuss basic wireless LAN (IEEE 802.11) technology. Beginning with a short introduction to the history of wireless LANs (WLANs), the reader will be quickly brought up to speed on the present state of the standards and the corresponding technology implementations. Wireless LAN architectural structure will be discussed in the context of the services provided by the WLAN. Details of Layer 2 MAC operations will be presented before the details of the physical layer are discussed. Once the details of the operation of the initial standard have been introduced, focus shifts to the extensions to the standard that have since been adopted. Details of the physical layers of IEEE 802.11b/a/g are presented with emphasis upon the changes and modifications needed to implement higher-data-rate transfer speeds and new complex modulation schemes. Next, details of the newly adopted 802.11i standard that adds an advanced security

protocol to the 802.11 standard are introduced. The chapter ends with a short discussion about other competing wireless LAN technologies (if any still exist) and typical WLAN hardware and its deployment.

## 9.1 INTRODUCTION TO IEEE 802.11X TECHNOLOGIES

The IEEE 802.11x standards form the basis for the implementation of high-performance wireless computer networks. The vast majority of the wired LANs in the world use network interface cards based on the IEEE 802 standards (e.g., Ethernet is based on 802.3 and token ring is based on 802.5). The IEEE 802.11x standards define the over-the-air protocols necessary to support networking in a LAN environment. In essence, the wireless LAN standards were written to provide a wireless extension to the existing wired standards. Furthermore, the WLAN standards would be developed with the following goals: seamless roaming, message forwarding, the greatest range of operation, and support for a large number of users. The IEEE finalized the initial standard for wireless LANs (802.11) in June of 1997.

This initial standard specified an operating frequency of 2.4 GHz (an ISM band) with data rates of 1 and 2 mbps and the use of either of two spread spectrum modulation techniques, FHSS or DSSS. Additionally, the standard also addressed the use of infrared (IR) light within the physical layer specifications. Since the release of the initial specification, the IEEE 802.11x working groups have continued to meet and refine the technology. The results of these efforts have led to enhancements and extensions to the original specifications that have raised the maximum data rates, added new frequencies of operation, and attempted to deal with other issues like interference from other services, security concerns, quality of service (QoS), and interoperability between different vendor access points (APs).

In the last several years, the uptake rate and deployment of WLANs has proven to be an unqualified success story with a strong embracement of the technology by several different sectors of the economy. Many Enterprise organizations have added WLANs to their computer networks in an attempt to increase their employee productivity. Various collaborations of business partners have begun to provide networks of so-called WLAN hot spots in airports, hotels, coffee shops, McDonald's restaurants, and other popular metro areas. And finally, the general public, led by the consumers of high-speed Internet access, have begun to construct their own wireless home and small-office networks to share their connection to high-speed Internet access among several computers and to also enjoy the untethered aspects of WLANs. The general public has even adopted the term **Wi-Fi** (for wireless fidelity) to describe this new technology. There are many predictions of the worldwide deployment of tens of thousands of new hot spots in this present year (2005) and increased consumer usage of wireless LANs in the home.

Recent industry predictions have called for continuous double-digit growth in the WLAN industry until the last few years of this decade as it quickly becomes a business generating several billons of dollars a year. However, as the WLAN industry matures, changes in technology and revenue growth are also predicted to occur. For one thing, manufacturers are integrating Wi-Fi chips into portable laptop and tablet PCs. Prices of the Wi-Fi-enabling chips and access points will continue to fall, the market for PCMIA Wi-Fi cards will disappear, and, most importantly, through more widespread Wi-Fi availability and competition, revenue to service providers and operators of aggregated Wi-Fi hot-spot networks will drop. Furthermore, as uncertain as the WLAN business model is today, unforeseen and planned innovations like local government/town-provided community WLAN coverage muddies the waters even more. As always, the path that a particular telecommunications technology takes is difficult to predict. However, the force that shapes the path is always the same—economics. An informative Web site about wireless LAN technology and news pertaining to the Wi-Fi industry can be found on the Web at www.wi-fiplanet.com.

## 9.2 EVOLUTION OF WIRELESS LANS

The evolution of wireless LANs has been closely tied to the development of wired computer networks, the expansion and increased use of the Internet, and the subsequent proliferation of networked computers tied

to the Internet. At the same time, the evolution of microelectronics has continued to follow Moore's law with increased reductions in size and price and increased chip functionality and speed. These factors have contributed to the development of low-cost hardware with which one can implement a wireless LAN. As mentioned before, the major chip manufacturers have already designed low-cost Wi-Fi chip sets for use in laptops and tablet PCs, and the largest manufacturer of microprocessors has outlined its vision (see the technology section of www.intel.com) to add wireless connectivity to each microprocessor chip before the end of the decade. Manufacturers of consumer electronics gaming devices (e.g., Sony PlayStation 2, Microsoft Xbox) have included Ethernet ports on their products. It is only a matter of time before WLAN connectivity will come as a standard feature on higher-end consumer electronics products. Since WLANs cost so much less to install than wired LANs, it will be interesting to see how it all plays out over the next few years. Also, the development and possible widespread deployment of wireless personal area networks (WPANs) in the near future may well serve as another driver of WLAN technology. WPANs will be discussed in Chapter 10.

The next few sections will give a brief overview of the early history of wireless LANs and then bring the reader up to speed on today's present technology.

## The Beginnings—ALOHA-Net

In 1971, network and radio technologies were brought together for the first time during the implementation of a research project called ALOHA-Net at the University of Hawaii. The ALOHA-Net system allowed computers at seven campuses spread out over four islands to communicate with a central computer on Oahu without using expensive and sometimes unreliable telephone lines. The ALOHA-Net used a "star topology" between the central computer and the remote stations.

In the 1980s, "ham" radio operators kept radio networking alive by designing and building what were known as terminal node controllers. These devices allowed the amateur radio operators the ability to interface their PCs to their radio equipment and form packet radio networks with other ham operators. The commercial development of radio-based LANs began in the United States in 1985 when the FCC opened up the industrial, scientific, and medical (ISM) bands located between 920 MHz and 5.85 GHz to the public (see Figure 9–1).

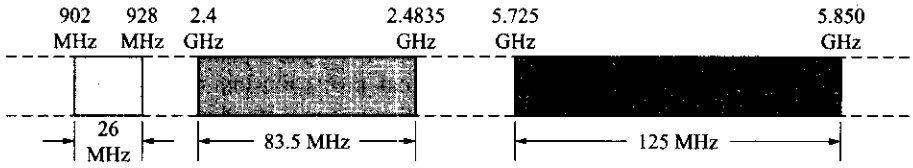



**Figure 9–1** The original ISM bands.

At the time, microelectronics technology being what it was, the first radio-based LANs operating at 920 MHz were expensive proprietary systems that did not assume a form factor conducive to their quick acceptance. It was not until 1990, when the microelectronics group at Lucent Technologies (later to become Agere Systems) launched one of the first commercially successful WLAN products lines. The WaveLAN suite of access points, radio cards, and radio card adapters (meant to interface the radio cards to desktop computers) operated in the 920-MHz range. A new suite of WaveLAN products for use at 2.4 GHz started shipping in 1994. The design specifications of these early products were very influential in shaping the final IEEE 802.11 standard.

On the standards side of things, in May of 1991, Victor Hayes submitted a project authorization request (PAR) to the IEEE to initiate the 802.11 "working group." As mentioned previously, this group, consisting mostly of interested parties from the WLAN industry, completed their work and the initial 802.11 standard was finalized in the summer of 1997. There are several important aspects of the 802.11 standard that should

be emphasized. It called for the use of the 2.4-GHz unlicensed ISM band and the use of spread spectrum forms of modulation to reduce interference between other applications using this band (at the time, microwave ovens, cordless phones, etc.).

## Extensions to 802.11

The IEEE 802.11 standard provided for a maximum transfer rate of 2 mbps. At the time, most wired LANs operated at either 10 or 100 mbps and it is felt that this fact led to the slow acceptance rate of WLANs during the late 1990s. In 1999, the IEEE undated the current standard to correct errors found in the initial standard and in late 1999 published two supplements to the updated 802.11 standard. IEEE 802.11b specified a data rate extension of the initial 802.11 DSSS specification to provide 11 mbps in the 2.4-GHz band. Also, the IEEE 802.11a extension specified operation at rates up to 54 mbps in the newer 5-GHz frequency band. For 802.11a, a new modulation technique known as orthogonal frequency division multiplexing (OFDM) was specified. The standard also provides for a number of set "fall-back rates" when the radio channel conditions cannot support the highest possible data rate. With these two rate extensions, available low-cost WLAN technology offered performance comparable to what computer network users were accustomed to over wired LANs. With a concerted marketing push, the moniker of Wi-Fi was adopted and the popularity of wireless LANs was on the upswing. Agere Systems sold its ten millionth 802.11b radio card by 2001.

In 2001, an extension to 802.11, 802.11d, added requirements and definitions that were necessary to permit 802.11 WLAN equipment to operate in other countries not covered by the current standard. Then, on June 12, 2003, the IEEE adopted another extension to the 802.11b standard. IEEE 802.11g specifies a data rate extension of the initial 802.11b DSSS specification to provide data rates up to 54 mbps (still in the 2.4-GHz band). Additionally, the 802.11 working group (WG) has been busy with the following projects:

- 802.11e—The project's purpose is to enhance the current 802.11 media access control (MAC) specification to expand support for LAN applications that have quality of service requirements. Example applications include transport of voice, audio, and video over 802.11x networks; video conferencing; and media stream distribution. The enhancement of the MAC layer in conjunction with the enhanced physical (PHY) layer provided by 802.11a/b/g will provide the necessary system performance improvements for new higher-level applications. The idea of Voice over WLANs (VoWLAN) has started to receive a larger share of attention lately as a proposed WLAN application (implemented through an integration of WLAN technology with wireless mobile phones).
- 802.11f—The project's purpose is to develop an interaccess point protocol (IAPP) to allow for multiple vendor access point (AP) interoperability across a distribution system (DS) supporting IEEE 802.11 wireless LAN links. For these purposes a DS supports a standard IETF Internet protocol environment. This work has recently (2003) been accepted and published.
- 802.11h—The project's purpose is to enhance the current 802.11 MAC and 802.11a PHY specifications with network management and control extensions to provide spectrum and transmit power control management in the unlicensed 5-GHz band. These enhancements would provide improvements in channel energy management, through measurement and reporting functions, and also provide dynamic channel selection and transmit power control functions. This project would also provide for easier acceptance of the IEEE 802.11 standard in European countries.
- 802.11i—The project's purpose is to enhance the 802.11 MAC to enhance security and authentication mechanisms. This work has recently been accepted (2004) and published and is presented in more detail in a succeeding section of this chapter.
- 802.11j—The project's purpose is to enhance the standard to add newly available 4.9- and 5.0-GHz channels for operation in Japan. This work has recently been accepted (2004) and published.
- 802.11k—The project's purpose is to enhance the scope of radio resource measurements from only internal use, to allow access to these measurements to external entities. This will allow for the introduction of WLAN mobility management functions and improve coexistence algorithms by allowing external entities to manage these processes.

- 802.11ma—The project's purpose is to update the standard by providing editorial and technical corrections.
- 802.11n—The project's purpose is to enhance the WLAN user's experience by providing data throughput rates in excess of 100 mbps.
- 802.11p—The project's purpose is to enhance WLAN technology to provide the ability to communicate to and between vehicles at speeds up to 200 km/h at distances up to 1000 meters using the 5.850–5.925 GHz band within North America. This project has the aim of enhancing the mobility and safety of all surface transportation.
- 802.11r—The project's purpose is to improve basic service set (BSS) transitions (i.e., WLAN handoffs) within 802.11 extended service sets (ESSs) to prevent the disruption of data flow during these events. This will enhance the operation of applications like VoIP.
- 802.11s—The project's purpose is to support WLAN mesh operation by providing the protocol for auto configuring and multihop topologies in an ESS mesh network.
- 802.11u—The project's purpose is to enhance the IEEE 802.11 MAC and PHY layers to provide the ability to internetwork with other external networks.
- 802.11v—The project's purpose is to provide wireless network management enhancements to the IEEE 802.11 MAC and PHY layers that will extend the work performed by the IEEE 802.11k project. Although IEEE 802.11k provides the means to retrieve data about station operation, this extension will provide the ability to configure the station.

The reader might note that certain letters that might be misinterpreted as numbers are avoided when labeling the extensions to the standard. The reader is also urged to visit the IEEE standards Web site at http://standards.ieee.org to learn more about the status of the IEEE 802.11x standards and any new initiatives that might grow out of the continuing efforts of the IEEE 802.11x working group.

### Layer 1: Overview

To implement the simplest form of a wireless LAN, one needs two or more radio card-equipped or WLAN-enabled PCs. What is known as an ad-hoc or peer-to-peer wireless network can be configured with a peer-to-peer operating system. This configuration will be discussed in more depth in the next section. The next-simplest type of wireless LAN uses one or more radio card-equipped or WLAN-enabled PCs or notebooks and an IEEE 802.11x access point. Both the radio cards and the access points contain radio transceiver hardware that provides the radio link for the transmission of data back and forth between the two units. One might consider the radio card or embedded Wi-Fi chip set to be analogous to the mobile station of the wireless mobile network whereas the access point plays the role of the cellular radio base station. The major differences between the two wireless systems at the physical layer level are the form of modulation used, the frequency bands employed, and the limited range of operation available from the WLAN. Another, important distinction is that presently there is no interconnection to the circuit-switched network (PSTN) via the wireless LAN. Interestingly, one's connectivity to the Internet or the PDN via the WLAN may be provided by a wireless Internet service provider (WISP), an Enterprise's connection to an ISP, or through a high-speed service provider's connection (typically, cable modem or xDSL service) to an ISP. A more in-depth discussion of the physical layer will be provided in a later section of this chapter.

## 9.3 IEEE 802.11 DESIGN ISSUES

A wireless network has a fundamental uniqueness that sets it apart from a wired LAN. In a wired LAN, an IP address is equivalent to a physical location or a hardwired connection. This fact is implicitly assumed in the design of a wired LAN where a length of CAT-n LAN cable connects the PC's network interface card (NIC) or RJ-45 jack to the LAN. In a WLAN, the addressable unit is known as a **station** (STA). The wirelessly enabled station serves as a message destination but in general does not indicate a fixed location. A

further differentiator of wireless versus wired LANs lies in the fundamental difference in the modes of signal propagation encountered in the two systems. Wired (point-to-point) connections yield highly predictable and reliable transmission of signals whereas wireless radio links are highly unreliable. These facts aside, there are some just as important but subtle effects to be considered when designing a wireless LAN, such as: a wireless LAN can have actively changing topologies, WLAN radio link signals are not protected from outside EM interference, WLAN radio links experience time-varying multipath effects and therefore the useable range of the system varies, WLANs have neither absolute nor observable boundaries, and the possibility exists that the WLAN lacks full connectivity, that is, where every station can hear every other station. This last consequence of the use of wireless is sometimes referred to as the hidden station effect. Two final factors to consider are that IEEE 802.11 is required to handle both mobile and portable stations and deal with battery-powered equipment. Mobile stations by definition are actually in motion and moving about the WLAN whereas portable stations may be moved about to different locations within the WLAN but are only used while at a fixed location. The fact that a station may be battery powered gives rise to power management schemes that might require a WLAN station to go into the sleep mode. If this is the case, this also must be considered in the design of the system. The next few sections will address the components and the basic topologies (known as service sets) supported by the IEEE 802.11 architecture. These so-called service sets provide WLAN functionality that supports station mobility that is transparent to higher-protocol layers.

## Independent Basic Service Set Networks

The **basic service set** (BSS) is the simplest and most fundamental structure of an IEEE 802.11x WLAN. See Figure 9–2 for a diagram of an **independent BSS** (IBSS). There is no backbone infrastructure and the network consists of at least two (there can be more) wireless stations. As mentioned before this structure is sometimes referred to as a peer-to-peer or **ad hoc wireless network.** As the figure shows, a propagation boundary will exist but its exact extent and shape are subject to many variables. As discussed in Chapter 8, simulation software exists that can provide some reasonable estimates of RSS for typical multifloor architectural layouts and various building materials. However, the colorized signal-strength contours provided by these software tools are only as good as the models used to create them. At the present time, the deviation of the predicted values to the actual values can be quite substantial. It is also possible to have two or more of these IBSSs in existence and operational within the same general area but not in communication with one another.

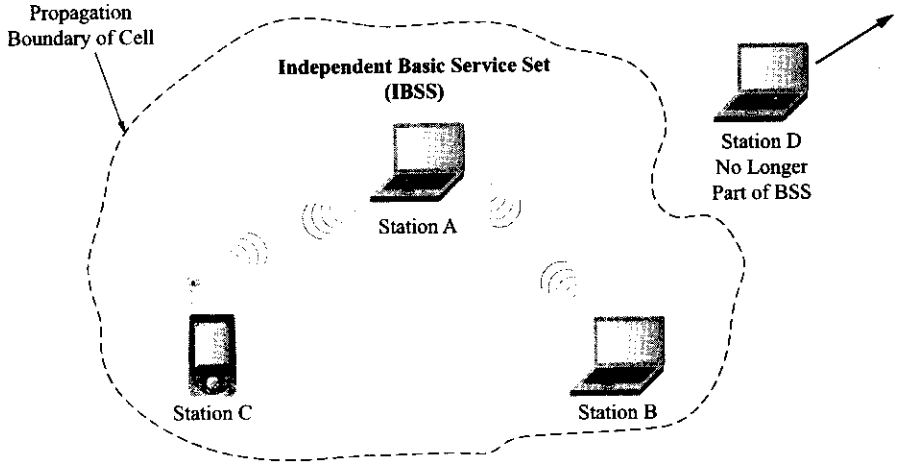



**Figure 9–2** A typical independent basic service set.

Within the IBSS structure, it is important to note that the association between an STA and a BSS is a dynamic relationship. An STA may be turned on or off or come into or go out of range of the BSS an unlimited number of times. The STA becomes a member of the BSS structure when it becomes associated with the BSS. The association process is dynamic and will be discussed at some length shortly.

## Distribution System Concepts

For any wireless LAN the maximum station–to-station distance that may be supported is determined by many factors including RF output power and the propagation conditions of the local environment. To provide for an extended wireless network consisting of multiple BSSs, the standard allows for an architectural component known as the distribution system (DS) to provide this functionality. To provide flexibility to the WLAN architecture, IEEE 802.11 logically separates the wireless medium (WM) from the distribution system medium (DSM). Figure 9–3 shows a diagram of a distribution system and several access points serving different BSSs.

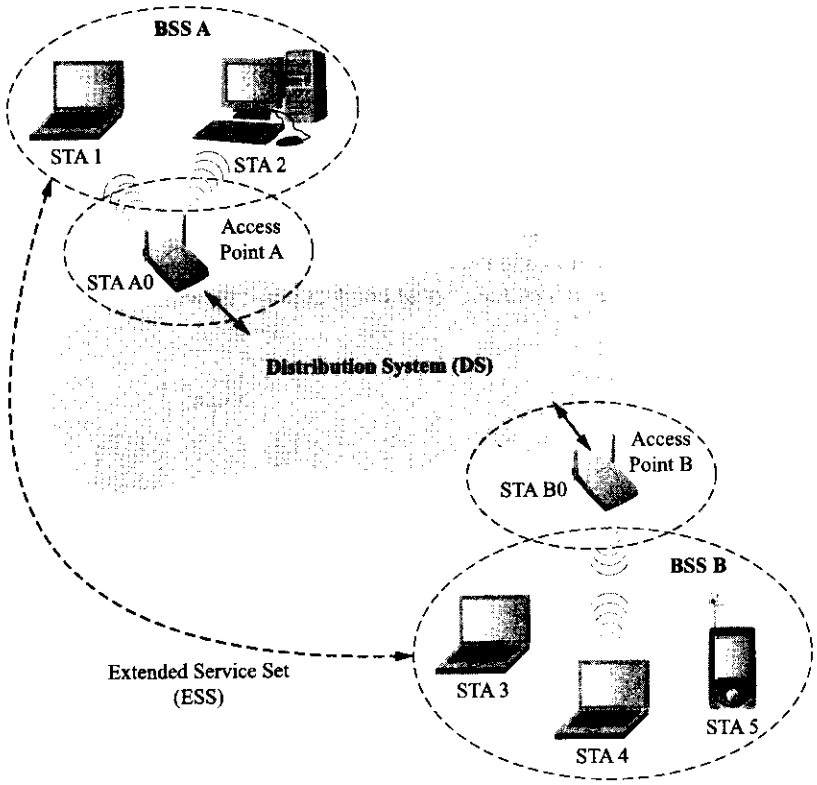



**Figure 9–3** A typical distribution system and several access points.

The function of the DS is to enable mobile device support. It does this by providing the logical services necessary to perform address-to-destination mapping and the seamless integration of multiple BSSs. This last function is physically performed by a device known as an **access point** (AP). The AP provides access to the DS by providing DS services and at the same time performing the STA function within the BSS. In Figure 9–3, data transfers occur between stations within a BSS and the DS via an AP. One should note that all the APs are also stations and as such have addresses. However, the address used by an AP for data communications on the WM side and the one used on the DSM side are not necessarily one and the same. This network structure gives rise to the use of APs as bridges to extend the reach of a network.

## Extended Service Set Networks

As noted already, depending upon the desired WLAN coverage area, the wireless BSS network may or may not provide sufficient coverage to satisfy the user's needs. Therefore, the IEEE 802.11 standard provides for the use of multiple BSSs and a DS to create a wireless network of arbitrary size and complexity. These networks are known as **extended service set** (ESS) networks. ESS networks provide advantages since they appear to be the same as an IBBS network to an upper layer logical link control (LLC) protocol. As a consequence of this, stations within an ESS network may communicate with one another and mobile stations may move transparently from one BSS to another as long as they are all part of the same ESS network. Furthermore, through the use of an ESS network all of the following situations may occur: BSSs may overlap to provide continuous coverage areas or BSSs can be physically separate entities, BSSs may be physically collocated for redundancy reasons, and one or more IBSS or ESS networks may be physically located in the same area. This last situation can commonly occur when separate organizations set up their own WLANs in close proximity to one another.

## Integration of Wired and Wireless LANs

The last piece of the wireless LAN architecture puzzle is supplied by a device known as a portal. To integrate the 802.11 wireless LAN with a traditional 802.x wired LAN (see Figure 9–4) a portal or logical point must exist where medium access control (MAC) service data units or MSDUs can enter the wireless LAN distribution system. The portal's function is to provide logical integration between the wireless LAN architecture and the existing wired LAN. In most hardware implementations, the portal function is also provided by the AP. For this case, the DS can be an already existing wired LAN. To summarize, the ESS network architecture provides traffic segmentation and range extension through the use of APs and the DS. The portal (typically, provided by the AP) provides the logical connect point between the wireless LAN and other wired LANs.

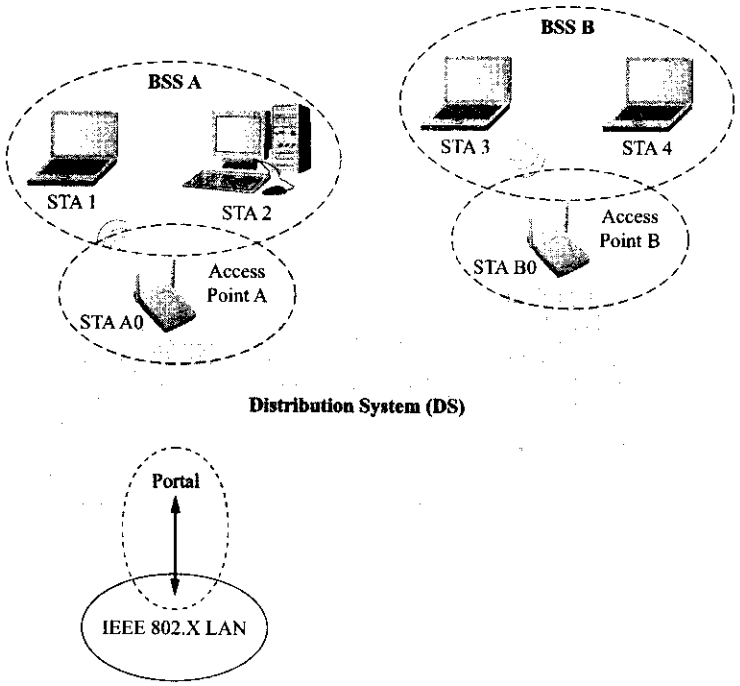



**Figure 9–4** A wireless LAN with a connection to an IEEE 802.x wired LAN.

## 9.4 IEEE 802.11 SERVICES—LAYER 2: OVERVIEW

The IEEE 802.2 standard specifies the logical link control (Layer 2) services that are provided to the network layer protocol. In the OSI model, the LLC is the highest layer of the data link layer (see Figure 9–5). The MAC (part of Layer 2) and physical layers (Layer 1) of the IEEE 802 standard are organized into separate standards apart from the LLC since there is a tight coupling between the medium access control, the medium used, and the network topology. The LLC will not be discussed at any great length in this section except to point out that the services it supplies are designed to provide the exchange of data between end users across a LAN using an IEEE 802-based MAC control link. LLC protocol data units (PDUs) are handed down through the MAC service access point (SAP) to the MAC sublayer. The LLC PDU is encapsulated with control information at the start and end of the packet, forming the MAC frame. The MAC frame is passed over the physical layer from the source to the destination. This section does not present details of the LLC but instead will focus on the operational aspects of IEEE 802.11 and in particular the services specified within the standard.

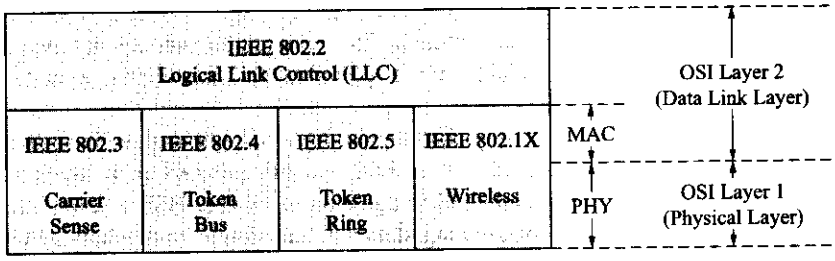



**Figure 9–5** Relationship of IEEE 802.xx standards to the OSI layers (Courtesy of IEEE).

The IEEE 802.11 architecture purposely does not specify details of the DS implementation. This was done to provide a high level of flexibility in the possible implementations of this portion of the network. Instead, the standard specifies architectural services. The services are in turn associated with particular components of the wireless LAN structure. These services are classified as either station services (SS) or distribution system services (DSS). In each case, the services provide the functions that the logical link control (LLC) layer requires for sending MSDUs between two devices on the network. The station services provide the necessary functionality for the network operations of authentication, deauthentication, privacy, and MSDU delivery. The associated distribution services operations are services typically provided by the access point, such as association, disassociation, distribution, integration, and reassociation. At this point, it is hoped that the reader has some vague (or better yet, informed) ideas as to the meaning of some of these terms from the coverage provided about wireless mobile systems by the first seven chapters of this book. There are many analogies one may draw between the operations of the two systems. However, not all of these terms are readily recognizable so explanations will be provided shortly. In any case. each wireless LAN service is specified for use by MAC sublayer entities. See Figure 9–6 for a depiction of the logical architecture of the 802.11 standard.

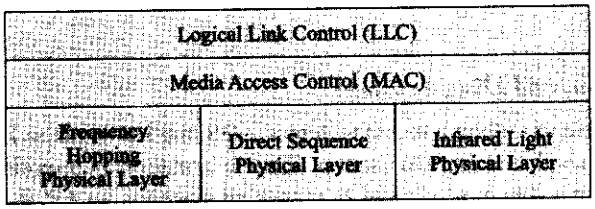



**Figure 9–6** Logical architecture of the IEEE 802.11 standard (Courtesy of IEEE).

One more aspect of IEEE 802.11 architecture that should be noted is that different portions of the network (i.e., WM, DSM, and wired LAN) are allowed to operate with different address spaces. The standard has designated the IEEE 802 48-bit (MAC) address space for the WM and therefore it is compatible with wired LAN addressing. For many cases, the possibility exists that the three logical address spaces used within a system might all be the same. However, this is not always the case, as in the situation when the DS implementation uses network layer addressing to provide enhanced mobility functions.

## Overview of Services—Distribution

IEEE 802.11 specifies nine different services. Six of the nine are used to support MSDU delivery between WLAN stations. The other three services are used to control WLAN access and provide confidentiality. Each of the various services is supported by one or more MAC frame types. The MAC sublayer uses three types of messages: control, data, and management. The control messages support the delivery of both data and management messages. The data and management messages are used to support the services. The details of this will be discussed in an upcoming section. At this time, the following section will describe how the particular service is used, how it relates to the other services, and its relationship to the overall network architecture. It should be pointed out that within an ESS network all services are available; however, within an IBSS only station services are available. While going through the following material, the reader should refer back to Figure 9–4 as necessary.

The distribution service is the most commonly used service by a WLAN station. Every time a data message is sent either to or from a station that is part of an ESS network this service is invoked. Consider the transfer of a data message from a station in one BSS to a station in another BSS where both BSSs are part of an ESS network. The message from the originating station is transferred to the station/AP that connects to the DS. The AP hands off the message to the DS. The DS delivers the message to the AP/station of the destination BSS and the data message is finally transferred to the destination station. A variation on this network operation is when the destination station resides in the same BSS as the originating station. In this case, the input and output AP (station) for the message would be the same. It is of no consequence that the message did not have to travel through the physical DSM in this last example. In both cases cited, the distribution service was invoked by the operation.

The integration service is invoked whenever the message to be delivered is intended for an IEEE 802 LAN. As explained previously, this operation would involve the use of a portal that connects the DS to the IEEE 802 LAN. The integration function would perform the steps necessary (address translations, etc.) to deliver the message. In many cases, where the DS is a wired LAN, the AP would provide this functionality.

The following discussion involves the services that support the distribution service. Since the primary purpose of a MAC sublayer is to transfer MSDUs between MAC sublayer entities, there are certain associated operations that must first be performed to provide the correct context for the data message transfer (e.g., a station must first be associated with the network before the distribution service can be invoked.) Before proceeding further, definitions of WLAN station mobility will be set forth. The first case is the noncase, as there is no transition by the wireless station to another state of connection; however, the station may physically move about the BSS. The second case, BSS transition, is when a WLAN station moves between BSSs of the same ESS network. The third case involves the movement of the WLAN station from one BSS in a particular ESS to a BSS in another ESS. The association services support different types of mobility.

### *Association, Reassociation, and Disassociation*

For a wireless LAN to be able to deliver a message across a DS, the DS needs to know which AP to deliver the message to in order to reach a particular station. This information is provided to the DS through the association operation. Before a station is allowed to send a message via an AP, it must first become associated with the particular AP. The process of becoming associated with an AP invokes the association service

that is always initiated by the station. This service provides a many-to-one mapping of stations to APs for use by the DS. At any given time, a wireless station can only be associated with one AP and at the same time an AP can be associated with many stations. When first powered up, a station scans the radio link to learn what APs are present and then requests to establish an association by invoking the association service. Once an association has occurred, it is sufficient to support the case of no-transition mobility but not the case of BSS-transition mobility.

The reassociation service is invoked to support BSS-transition mobility within an ESS network. Reassociation is also always initiated by a WLAN station. If the station moves within the ESS network to another BSS, the reassociation process will provide the DS with a correct up-to-date mapping of the station/AP relationship. The disassociation service is invoked whenever a preexisting association needs to be terminated. Disassociation may be initiated by either party to an association and since it is a notification as opposed to a request, it cannot be refused by either party. Stations attempt to disassociate whenever they leave a network, and APs may need to disassociate stations to enable the removal of an AP from a network if that becomes necessary.

### *Access and Security Control Services*

As mentioned previously, the inherent differences between wired and wireless LANs (physically closed versus open systems) give rise to the need for several additional services that attempt to bring the wireless LAN up to the functional equivalent of a wired LAN. Authentication and privacy services are used to provide the wireless LAN with characteristics that mimic the traits of a wired LAN. Wireless LAN access is controlled via the authentication service. This service is used to allow all wireless stations to establish their identity with all the other stations that they will potentially communicate with. If a mutually agreed-upon level of authentication cannot be established between two stations, then an association will not be established. The IEEE 802.11 standard supports several authentication processes including open system and shared key. In both cases, the authentication provided between stations is at link level. This station service allows a single station to be authenticated with many other stations at any given time. A complementary service is deauthentication. Whenever an existing authentication is to be terminated, the deauthentication service is invoked. Deauthentication is similar to disassociation in that when it is invoked it also performs the disassociation function. Again, deauthentication is a notification not a request and falls into the category of a station service.

IEEE 802.11 includes the ability to provide basic encryption to the contents of messages. This ability is provided by the privacy service. All wireless LAN stations start their operation in an unencrypted state to set up the authentication and privacy services. This station service allows for the use of an optional privacy algorithm known as **wired equivalent privacy** (WEP). WEP may be invoked for data frames and some authentication messages. WEP was never meant to provide an ultimate form of wireless LAN security. Already, several enhancements have been introduced to the original standard and the newly accepted IEEE 802.11i standard is expected to provide the needed security protocols necessary for widespread adoption of WLANs in the Enterprise environment. More details about WLAN security will be presented in a later section of this chapter.

### *Relationships between Services*

When a station is going to communicate with another station over the WM, the type of messages (MAC frames) that can be sent from the source to the destination depends upon the current state existing between the two stations. Figure 9–7 shows the connection between the allowable architectural services and the current relationship of the sending station and the destination station. As shown by the figure, different levels or states of station authentication and association correspond to different types of transferable frame classes. Class 1 frames are various control (request to send, clear to send, acknowledgement, etc.), management, and restricted data frames; Class 2 frames are only management frames (e.g., association, reassociation, and disassociation); and Class 3 includes all three types of frames including unrestricted data frames. If incorrect or

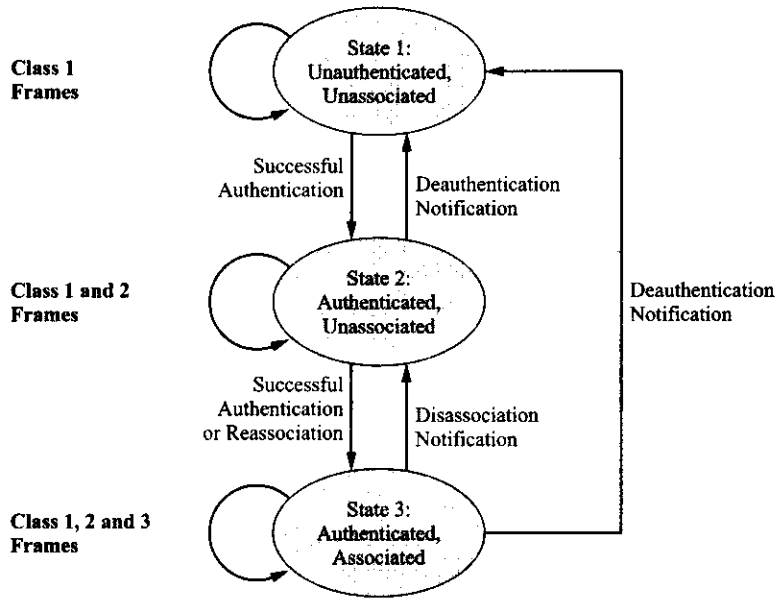



**Figure 9–7** Relationship between sending and receiving stations (Courtesy of IEEE).

unallowed classes of frames are sent and received, deauthentication or disassociation frames (as appropriate) will be sent back to the sending station.

Each one of the services introduced previously in this section is supported by one or more IEEE 802.11 messages. To give the reader a feel for the general makeup of the message and type of information contained in the messages, several examples of different message types will be given here.

---

### *Example 9–1*

For a wireless station to send data to another wireless station it sends a data message of the following form:

Service Type: *Data Message*

— *Message Type: Data*

— *Message subtype: Data*

— *Information items:*

- *IEEE source address of message*
- *IEEE destination address of message*
- *BSS ID*

— *Direction of message: From STA to STA*

---

### *Example 9–2*

For a station to associate, the association service causes the following messages to occur:

Service Type: *Association Request*

— *Message type: Management*

— *Message subtype: Association request*

— *Information items:*

- *IEEE address of the STA initiating the request*
- *IEEE address of the AP with which the initiating station will associate*
- *ESS ID*

— *Direction of message: From STA to AP*

*Association Response*

— *Message type: Management*

— *Message subtype: Association response*

— *Information items:*

- *Results of the requested association; either successful or unsuccessful*
- *For a successful association, the response will include the association identifier, AID*

— *Direction of the message: From AP to STA*

---

The messages for reassociation, disassociation, privacy, authentication, and deauthentication are all similar to the examples shown. Note that for an IBSS, there is by definition only one BSS, and therefore since there is no DS there can be no DS services. In this case, only Class 1 and Class 2 frames can be sent. The reader should reflect upon the similarities and differences of wireless LAN network attachment (initialization) procedures and those of the wireless mobile networks previously discussed.

## 9.5 IEEE 802.11 MAC LAYER OPERATIONS

Each station and access point on an 802.11 network implements the MAC sublayer service. The MAC sublayer provides these primary wireless network operations to wireless stations: accessing the wireless medium, joining a network, and authentication and privacy. Once these operations have been successfully performed, the devices on the network may communicate through the transmission of MAC frames. There are three types of MAC frames: control, management, and data. Control frames are used to assist in the delivery of data frames. Management frames are used to establish initial communications between stations and access points. Data frames carry information. Additionally, the MAC sublayer provides for several different types of MAC services. The primary MAC services are asynchronous data service, security service, and MSDU ordering service. The next several sections will provide a discussion of MAC services, the LCC/MAC layer service primitives, MAC frames, and techniques used in accessing and joining a wireless network in greater depth.

### MAC Services

In the IEEE 802.11 standard all wireless stations support asynchronous data service. This asynchronous transport of MSDUs is performed on a "best-effort" connectionless basis (i.e., no guarantees of successful MSDU delivery) using unicast, multicast, and broadcast transport. This MAC service provides peer LLC entities with the ability to exchange MSDUs. This act is accomplished through the local MAC (sending) entity using the physical layer to transport a MSDU to a peer MAC (receiving) entity at which point it is

delivered to the peer LLC entity. There are two classes of operation possible within asynchronous data service. These different classes are used to deal with the potential necessity of reordering the received MSDUs. Each LLC entity that initiates the transfer of MSDUs is able to select the class of operation desired to either provide for this function by the peer MAC entity or not.

The security services in IEEE 802.11 are provided by the authentication service and the WEP encryption mechanism. The security services offered are limited to the exchange of data between stations. The privacy service offered by WEP is the encryption of the MSDU. WEP is considered a logical service located within the MAC sublayer and its implementation is transparent to the LLC and other higher layers. Again, more will be said about this topic later in the chapter.

The services provided by the MAC sublayer permit either StrictlyOrdered or ReorderableMulticast service. Various MAC power management modes may require the reordering of MSDUs before their transmission to a designated station to improve the probability of successful delivery. If the StrictlyOrdered service class is used, it precludes the use of power management at the destination station.

## LLC/MAC Layer Service Primitives

The LLC/MAC layer service primitives allow for communication between the two layers. These service primitives take on the following basic forms: request, confirm, indication, and response. Through the use of these primitives, a layer may request another layer to perform a specific service, a layer may confirm the results of a previous service primitive request, a layer may indicate the occurrence of a significant event, or a layer may provide a response primitive to complete an action that was initiated by an indication primitive. In the 802.11 standard, the LLC layer communicates with its associated MAC layer through the use of the following three service primitives:

- MA-UNITDATA.request This primitive is used to request the transfer of a MSDU from a local LLC sublayer entity to a single peer LLC sublayer entity or a group of peer entities through the use of a group address. The primitive is sent to the associated MAC sublayer entity that in turn creates the proper MAC frame and then passes it on to the physical layer for transfer to a peer MAC sublayer entity or entities as the case may be. The data frame may be an information frame that contains data or a control frame that the local LLC is communicating to the peer LLC.
- MA-UNITDATA.indication This primitive is used by the MAC sublayer entity to define the transfer of a data frame (MSDU) from the MAC sublayer to the peer LLC sublayer entity or entities in the case of a group address. This operation only occurs if the MSDU has been received without errors, is a validly formatted frame, has valid WEP encryption (if employed), and the destination address indicates the correct MAC address of the station.
- MA-UNITDATA-STATUS.indication This primitive has only local significance. It is passed from the MAC sublayer entity to the LLC sublayer entity and used to indicate status information about the service provided for the corresponding preceding MA-UNITDATA. request primitive.

## MAC Basic Frame Structures

The IEEE 802.11 standard specifies the format of the MAC frames. Any equipment that is compatible with this standard is able to properly construct frames for transmission and decode frames upon reception. Each MAC frame consists of the following basic components: a MAC header, a variable length frame body, and a frame check sequence (FCS). The MAC header consists of several fields including frame control, duration, address, and sequence control information. The frame body contains information that is specific to the frame type. The FCS contains an IEEE 32-bit cyclic redundancy code (CRC). Figure 9–8 shows the general structure of a MAC frame format and a management MAC frame example. The fields labeled address 2, address 3, sequence control, address 4, and frame body are only present in certain types of frames. Within an individual frame field, there typically exist subfields that are used to provide additional information.

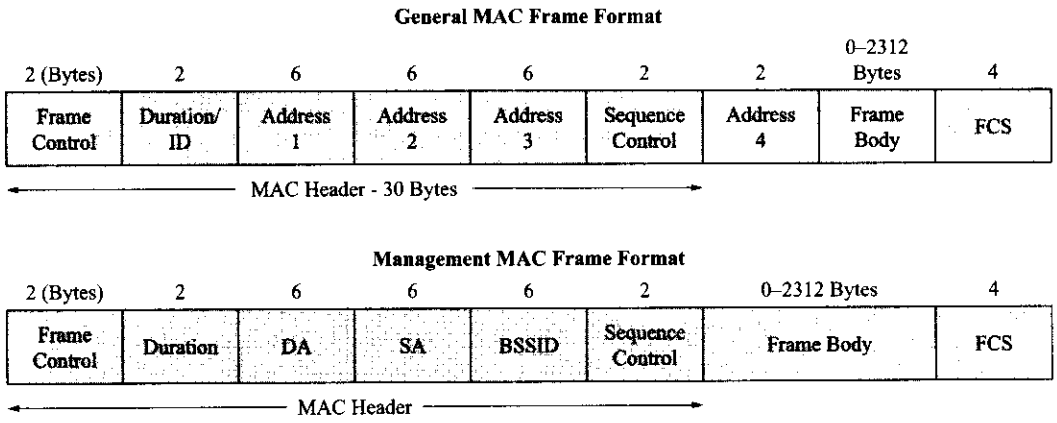



**Figure 9–8** Examples of IEEE 802.11 MAC frame formats (Courtesy of IEEE).

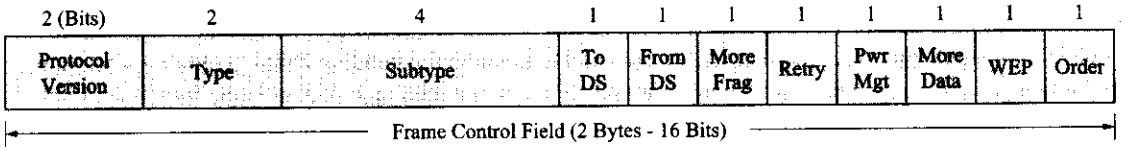



**Figure 9–9** Further details of the frame control field of the MAC frame (Courtesy of IEEE).

Figure 9–9 shows the structure of the frame control field (i.e., the first 2 bytes of the MAC frame). As one can see, further information can be encoded into the control frame subfields that can even consist of 1-bit fields. For further details of the meanings and possible encodings for these fields one should look at the most recent version of the IEEE 802.11 standard. This work will not go into that fine amount of detail.

Returning to the general MAC frame format shown by Figure 9–8, a few comments about the address, sequence, and frame body fields are appropriate here. The four address fields in the MAC frame format are used to indicate the basic service set identifier (BSSID), destination address (DA), source address (SA), receiver address (RA), and transmitter address (TA) (although not all at the same time). Furthermore, some types of MAC frames may not contain some of the address fields just mentioned. Each address field is 48 bits in length and can therefore use 48-bit IEEE 802 MAC addresses to indicate an individual station on the network or a group address. The group address can be one of two types, either a multicast group or a broadcast group (i.e., all of the stations presently active in the wireless LAN). The BSSID field is used to uniquely identify each BSS. For a typical wireless LAN, the value of this field is the MAC address currently in use by the station portion of the AP or APs of the WLAN. The sequence field consists of 16 bits that are composed of two subfields of 4 bits and 12 bits. The 12 bit field provides a sequence number for each MSDU and the 4-bit field provides a MSDU fragment number, if needed. The frame body field has a minimum length of 0 bytes and as shown in the figure can be as long as 2312 bytes.

### *Frame Types*

As mentioned before, there are three different types of MAC frames. There are also numerous variations of each MAC frame type. To provide some continuity to this topic, examples will be given here for several of the different categories of MAC frames but the reader will have to consult the IEEE 802.11 standard for more detail. Typical control frames are request to send, clear to send, acknowledgement, and power-save poll. Figure 9–10 shows the format of the frame control field for a control frame.

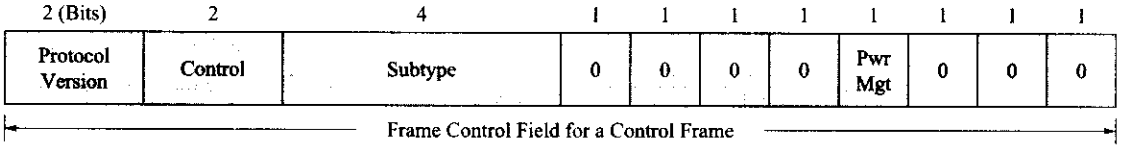



**Figure 9–10** Format of a frame control field for a control frame (Courtesy of IEEE).

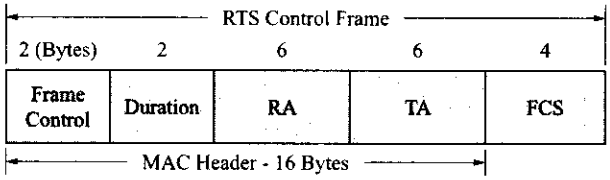



**Figure 9–11** IEEE 802.11 RTS frame (Courtesy of IEEE).

In the figure, the RA of the RTS frame is the address of the station on the WM that is the intended destination of the pending data or management frame. The TA is the address of the sending station and the duration value is the time in microseconds that will be required to transmit the pending frame, a clear to send frame, an acknowledgement frame, and to add three short interframe space intervals. A data frame format is identical to the frame shown in Figure 9–8. For the data frame the content of the various address fields is determined by the values of the To and From DS bits in the frame control subfields of the data frame. Figure 9–11 shows the format of a Request to Send (RTS) control frame. Unfortunately, this chapter will not be able to delineate all the details outlined in the IEEE 802.11 standard.

## 802.11 MAC layer Operations—Accessing and Joining a Wireless Network

Before any transfer of data can occur over an IEEE 802.11 wireless network, access must be gained to the network. In the present standard there are two methods outlined to perform this function. The primary access method makes use of a distributed control function (DCF) that is known as carrier sense multiple access with collision avoidance (CSMA/CA). This DCF is implemented in all wireless LAN stations and is used within both IBSSs and ESS networks. Essentially, the operation of this wireless version of the DCF is very similar to how it functions for a wired Ethernet LAN. The station desiring to transmit must physically sense the medium to determine if another station is transmitting. If no transmission is detected and the medium is determined not to be in a busy state, the station transmission may proceed. The CSMA/CA algorithm also includes provisions for a minimum time gap (interframe space) between the transmissions of frames. A transmitting station will defer transmitting until this time period has elapsed. If the wireless medium is determined to be busy through the use of some other nonphysical methods, the station desiring to transmit will wait until the end of the current transmission.

After just completing a successful transmission or after deferring transmission, the waiting station will select a random backoff time interval before attempting to transmit again. This random backoff procedure is very helpful in resolving contention conflicts caused by the possibly of many stations waiting to transmit. Figure 9–12 shows how the collision window (CW) backoff time increases exponentially for each retransmission try. The backoff time is equal to a random number (integer) times the value of CW. For a network with low utilization a station usually does not have to wait long before being allowed to broadcast a waiting frame. However, for a network with high utilization there can be extensive time delays before frame transmission is permitted even with this backoff procedure.

An additional enhancement used to further minimize collisions is for the wireless stations involved in the data transfer to send short control frames (i.e., request to send [RTS] and clear to send [CTS] frames). This is done after a determination that the wireless medium is idle, and after any deferrals or backoffs and before

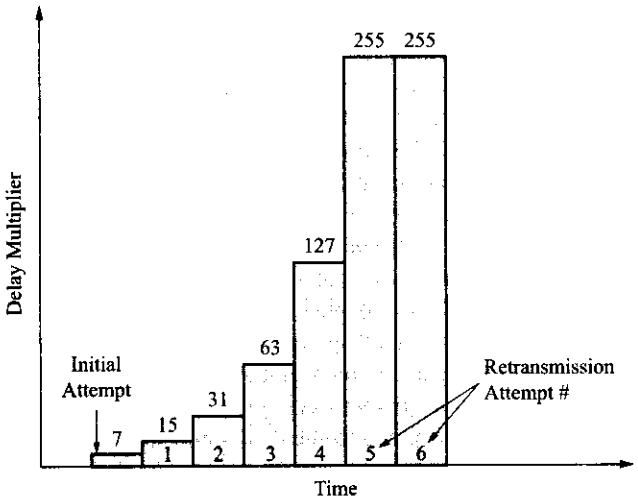



**Figure 9–12** Collision window backoff time (Courtesy of IEEE).

any data transfer occurs. The CTS and RTS frames contain a duration/ID field (refer back to Figure 9–10 for the structure of an RTS frame) that sets the length of time that the medium is to be reserved to accomplish the actual data transfer and the return of an acknowledgement frame due to the directed traffic. This information is used to set an internal timer within the other wireless stations active in the network and provides what is known as a virtual carrier-sense mechanism. Note also that this process helps to solve the hidden-station problem since if a station within a BSS does not hear the sending station's RTS frame (it might be out of range), it might hear the CTS message returned by the receiving station. The use of RTS/CTS frames is not always justifiable since they add considerable overhead for short data frames. With multirate operation possible, RTS/CTS frames are always sent at one of the basic rates sets.

Another optional wireless network access method is known as the **point coordination function** (PCF). This method (used only in an ESS network) uses a point coordinator (PC) that operates at the access point of a BSS. In this scheme, the PCF determines which station has the right to transmit. The PCF basically performs a polling function of the active stations in the BSS and acts as the polling master deciding which station gets to transmit next. This operation can be complicated by the colocation of another BSS. The PCF uses a virtual carrier-sense procedure aided by an access priority algorithm. The PCF distributes a form of timing information within a beacon management frame that is used to set a network allocation vector (NAV) timer within any active station. This act provides the PCF with control of the WM since it inhibits any active transmission by the stations attached to the PC/AP until the NAV timer decrements to zero. Another aspect of the PCF is that it employs a shorter interframe space (IFS) than used by the DFC system. This fact allows point-coordinated traffic to have priority over DCF traffic in areas where overlapping operation is occurring and one of the BSSs is DCF based. This last fact is very important because it provides the ability for a PCF-based system to create a contention-free (CF) access method.

It is possible for the DCF and the PCF methods of wireless network access to coexist and operate concurrently within the same BSS. When this is the case, the two access methods alternate back and forth providing a contention-free period that can be used for high-priority data transfers followed by a contention period and so forth. In all cases, both virtual carrier-sense and physical carrier-sense methods are used by the station to determine the busy-idle state of the medium. Naturally, whenever the station is transmitting the medium is also considered busy. There are many more details to the operation of DCF and PCF network access that will not be considered here because they are beyond the scope of what this author is attempting to accomplish—provide an overview of basic wireless LAN operation. Instead, a listing of other details that fall under DCF and PCF operation will be provided here to give the reader an appreciation for

the intricacies of these topics. Some of the DCF details are MAC-level acknowledgements; different types of interframe spaces; backoff time calculation; DCF access operation rules (i.e., basic access, backoff procedures, recovery procedures, setting and resetting the NAV, control of the channel, RTS/CTS use with fragmentation, and CTS procedure); directed, broadcast, and multicast MPDU transfer procedure; ACK procedures; duplication detection; and DCF timing relations. Some of the PCF details are contention-free period (CFP) structure and timing, PCF access procedures (i.e. fundamental access, NAV operation during the CFP, PCF transfer procedures, contention-free polling list), fragmentation, defragmentation, multirate support, and frame exchange sequences. Since the system is not perfect, some of these details outline the procedures necessary to recover from errors in data transfer or inadvertent data collisions.

The act of joining a wireless network occurs shortly after a wireless station is first turned on. When first powered up, the station will enter a passive or active scanning mode under software control. In the passive scanning mode the station listens to each channel for a predetermined period. In this mode, the station basically waits for the transmission of a **beacon frame** having the correct service set identifier (SSID) that the station wants to join. Once the station has detected the beacon, a connection will be negotiated by proceeding with the standard authentication and association process. In active scanning, a probe frame is transmitted by the station. The frame indicates the SSID of the network that the station desires to join. The station awaits a probe response frame that will indicate the presence of the desired network. Once the probe response frame is received the connection is negotiated by proceeding with the standard authentication and association process. If a probe is sent using a default broadcast SSID (a typical situation), any network within range will respond. Furthermore, an access point will respond to all probe requests and for the case of an IBSS, the station that last generated a beacon frame will respond to a probe request. After the station has joined with an IBSS or a BSS belonging to an ESS network, it becomes synchronized to a common master clock and implements the physical layer setup parameters offered by the network.

At this time it is appropriate to discuss the synchronization process in more detail to tie up the loose ends just generated in the prior discussion about joining a network. A timing synchronization function (TSF) is used to keep the internal timers for all stations in a BSS synchronized. For an ESS network the AP provides the master clock that is used for the TSF. The AP randomly starts its timer to avoid synchronization with the clocks of other APs. The AP periodically transmits special beacon frames that contain a copy of its TSF timer. The stations in the BSS use the information contained in the beacon frame to set their internal TSF timers. A station in a BSS that has a timestamp that does not match the received beacon will adjust its timestamp to that of the beacon. Figure 9–13 shows the process of periodically broadcasting a beacon and the effect of a busy medium on that process.

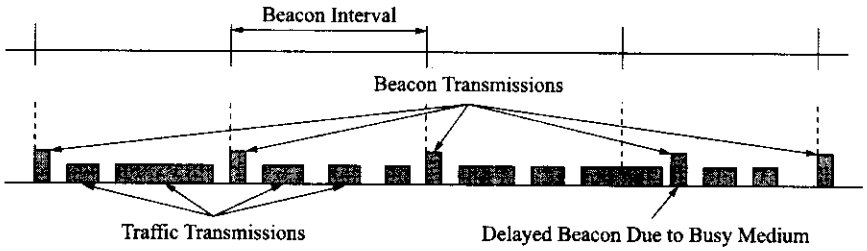



**Figure 9–13** Periodic broadcast of a beacon (Courtesy of IEEE).

For an IBSS an algorithm is used that distributes the generation of the beacon over the members of the IBSS. See Figure 9–14 for a depiction of this process. Each station within the IBSS adopts the timing from any beacon or probe response that has a TSF value that is later than its own value. The internal station TSF timer is a 64-bit binary clock that increments every microsecond. The accuracy of a TSF timer synchronized to a beacon is designed to be within ± 0.01%. The TSF also supports other important wireless network functions. Within the beacon frame is information about the particular physical layer that is being

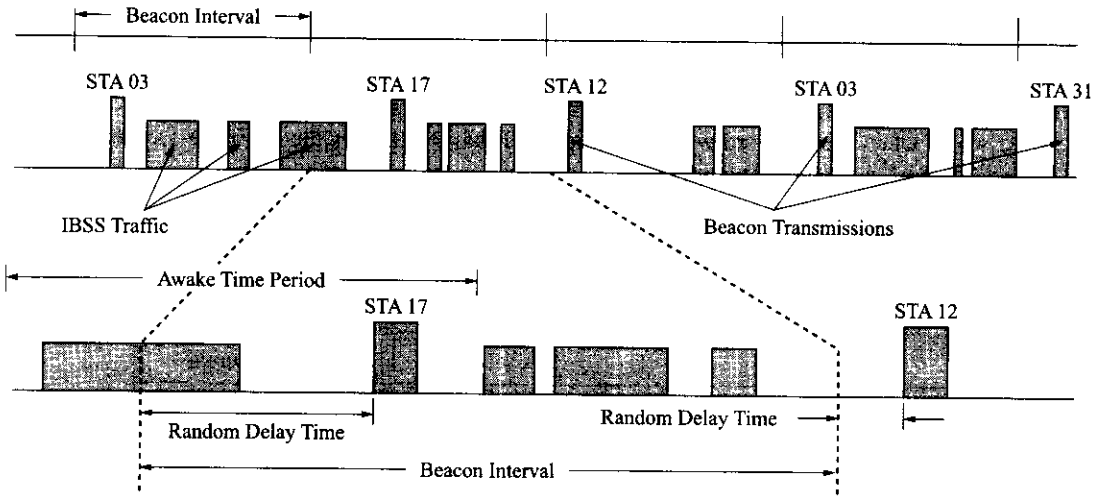



**Figure 9–14** Beacon transmissions for an IBSS (Courtesy of IEEE).

used (e.g., frequency hopping sequence or DSSS code) and the AP's clock value. This value is used to enable power saving functions for the station. If the station is in the sleep mode, the clock value will be used to provide the correct wake-up time for the station to listen for a transmitted beacon.

## 9.6 IEEE 802.11 LAYER 1: DETAILS

In general, the physical layer for a wireless LAN consists of three functional entities. The physical medium dependent (PMD) system, the physical layer convergence function (PLCF), and the layer management function. The PMD system defines the specific transmitting and receiving characteristics (frequency of operation, timing, modulation techniques, etc.) used to transfer data over the wireless medium between two or more wireless stations. The PLCF adapts the PMD system to the physical layer service and is supported by a physical layer convergence procedure (PLCP). The PLCP defines a mapping of MAC sublayer protocol data units (MPDUs) into a suitable framing format. Once formatted, user data and management information can be sent and received between two or more wireless stations over the associated PMD system. Since there can be more than one type of PMD (as is the case for IEEE 802.11), there may be a need for more than one PLCP. The physical layer management entity (PLME) performs the management functions for the physical layer in conjunction with the MAC layer management entity (MLME). These two entities provide the layer management interfaces through which layer management operations may be invoked.

The physical layer service is provided to the MAC entity at the wireless station through the PHY-SAP (physical layer service access point). In conjunction with the interface between the physical layer convergence protocol sublayer and the PDM sublayer, known as the PMD-SAP, a set of service primitives has been specified. This section is going to emphasize the physical aspects of the wireless network implementations specified by IEEE 802.11 and will therefore not provide a great deal of detail about the various service primitives pertaining to either the physical layer or its management. If the reader has a great interest in these topics, he or she is urged to refer to Sections 10 and 12 of the IEEE 802.11 standard.

The updated (1999) wireless network standard called for the use of three different physical layer modes of operation (see Sections 14–16 of the standard). They are frequency hopping spread spectrum, direct sequence spread spectrum, and infrared. The basic concepts of the first two modes have been discussed previously in Chapter 8 and the last mode is yet to be discussed. As most of the enhancements to the standard have been associated with the spread spectrum techniques, our emphasis will be on these modes of operation.

## Frequency Hopping Spread Spectrum Overview

The IEEE 802.11 specifications call for the use of frequency hopping spread spectrum (FHSS) using the 2.4-GHz ISM band (2.400 to 2.500 GHz). However, these frequencies were not universally available in all parts of the world when the standard was first adopted. Table 9–1 shows the available frequencies in this range for a number of geographic locations.

**Table 9–1** Available IEEE 802.11 frequencies at 2.4 GHz (Courtesy of IEEE).

| *Minimum* | *Hopping Set* | *Region* |
|---|---|---|
| 75 | 79 | North America |
| 20 | 79 | Europe[1] |
| Not Applicable | 23 | Japan |
| 20 | 27 | Spain |
| 20 | 35 | France |

[1]Except Spain and France

Shortly thereafter, a supplement to the standard (IEEE 802.11d) that was adopted in 2001 provided a mechanism to extend the operation of WLANs beyond the original regulatory domains specified by Table 9–1. This supplement provides the means by which an access point can provide the required radio transmitter parameters to an IEEE 802.11-compatible mobile station. With these parameters the wireless station is able to configure itself to operate within the applicable regulations of the geographic or political subdivision that it is located in. Furthermore, the supplement provides the ability for the mobile station to roam between various regulatory domains. To accomplish this enhancement, additional beacon, probe request, and probe response frame formats were added to the standard that include appropriate country information elements and hopping pattern information. Other additions and modifications were made to the MAC sublayer functional descriptions, the MAC sublayer management entity, and the frequency hopping physical layer specifications to facilitate these different operational modes and the ability to roam across regulatory domains.

### *FHSS Physical Layer*

As mentioned before, the ability to provide the MAC entity with the physical layer service is dependent upon the use of various protocols that adapt the physical medium to the physical services and further provide the ability to transfer MAC protocol data units (MPDUs) over the wireless medium. The use of FHSS for the physical layer service calls for the use of an FHSS PLCP sublayer, an FHSS physical layer management entity (PLME), and an FHSS PMD sublayer.

The FHSS PLCP protocol data unit (PPDU) frame format supports the asynchronous transport of MPDUs between stations within a wireless LAN. The PPDU consists of a PLCP preamble, a PLCP header, and a PSDU. The preamble facilitates the correct operation of the receiver circuitry. The header field provides information about length of the PSDU data word, the transfer data rate in mbps, and an error check field. The payload, PSDU, is sent after undergoing a scrambling process. To facilitate the operation of the physical layer, the FHSS PLCP consists of three inter- coupled state machines. They are known as the transmit, receive, and carrier sense/clear channel assessment (CS/CCA) state machines.

The FHSS PLME supplies services to upper-layer management entities (MLME). The PLME/PMD services are defined in terms of service primitives. The MLME of an IEEE 802.11 wireless station performs

the synchronization process to provide for the synchronized frequency hopping for all stations within a BSS or IBSS network. The FHSS PLME accepts service primitives from the MLME to change the tune frequency at a time set by the MLME. A FHSS PLME state machine helps facilitate these operations.

The FHSS PMD sublayer services are provided to the convergence layer through the acceptance of services primitives. The PMD provides the actual signal modulation, timing, frequency hopping, and so forth to generate the transmitted wireless signal. At the receiver the PDM sublayer reverses the process. The net effect is the transfer of a data stream and the delivery of timing and receiver parameter information to the receiving convergence sublayer. Again, a great deal of detail has been skipped over in this short presentation but the basic concepts have been outlined.

### *FHSS PMD Sublayers, 1.0 and 2.0 Mbps*

In general, the first IEEE 802.11 standard only addressed a limited but technically advanced market (i.e., Europe, Japan, and North America). However, as discussed earlier that situation has changed as extensions to the standard have been introduced. The initial standard called for data rates of either 1 or 2 mbps over the FHSS physical layer. The standard called for a conformant system to be able to operate within the frequency ranges listed in Table 9–1. Furthermore, the number of hopping frequencies to be used was also delineated (see Table 9–2) within the standard.

**Table 9–2** Number of IEEE 802.11 hopping frequencies (Courtesy of IEEE).

| *Lower Limit* | *Upper Limit* | *Regulatory Range* | *Region* |
|---|---|---|---|
| 2.402 GHz | 2.480 GHz | 2.400–2.4835 GHz | North America |
| 2.402 GHz | 2.480 GHz | 2.400–2.4835 GHz | Europe[1] |
| 2.473 GHz | 2.495 GHz | 2.471–2.497 GHz | Japan |
| 2.447 GHz | 2.473 GHz | 2.445–2.475 GHz | Spain |
| 2.448 GHz | 2.482 GHz | 2.4465–2.4835 GHz | France |

[1]Except Spain and France

For North America and Europe the channel center frequency is defined in sequential 1-MHz steps. The band starts with Channel #2 at 2.402 GHz and ends with Channel #80 at 2.480 GHz (excluding Spain and France). In Japan, the band starts with Channel #73 at 2.473 MHz and ends with Channel #95 at 2.495 GHz. The channels allowed in France and Spain will be left as an exercise for the reader to determine. The occupied channel bandwidth and the hop rate are governed by the local geographic regulations.

*FHSS Hopping Details* The hopping sequence that is used by a BSS should conform to a pseudorandom pattern that is given by the following equation.

$$F_x = \{ f_x(1),\ f_x(2),\ \ldots f_x(p) \} \qquad \textbf{9-1}$$

where $f_x(i)$ is the channel number for the $i^{th}$ frequency in the $x^{th}$ hopping pattern and $p$ is the number of different possible frequency channels in the hopping pattern. Refer back to Figure 8-15 for an example of a simple hopping pattern. Without going into further detail, the sequences are designed to maintain a minimum distance between hops (i.e., 6 MHz in North America and Europe and 5 MHz in Japan) and are further broken up into sets. For North America and Europe the net result is three sets of hopping sequences of twenty-six patterns each (a total of seventy-eight sequences). The other geographic areas addressed in the standard have fewer hopping sequence patterns available.

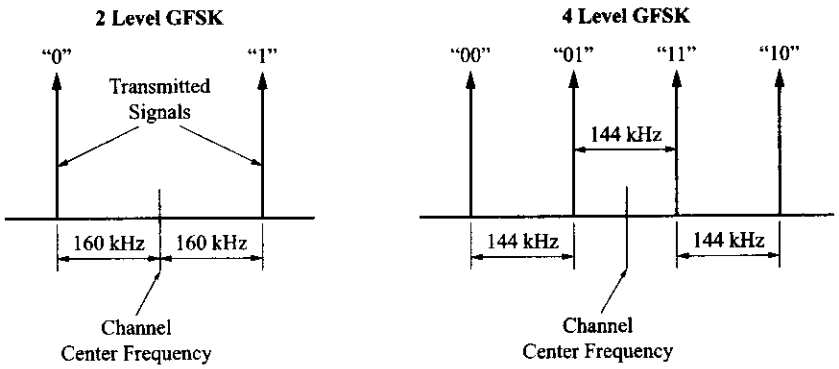



**Figure 9–15** IEEE 802.11 GFSK modulation process: 2 and 4 level.

*FHSS Modulation Details* FHSS uses either two- or four-level Gaussian frequency shift keying (GFSK) depending upon the data rate. For a data rate of 1 mbps the input to the 2-GFSK modulator is either a 0 or a 1. The modulator will transmit a frequency that is either slightly higher or lower than the channel center frequency to encode the data. The nominal frequency shift from the channel center frequency is ±160kHz. For a data rate of 2 mbps, the input to the 4-GFSK modulator is one of four possible 2-bit binary combinations. Four different frequencies are used to encode the four different combinations. However, during each symbol time, two binary bits are transmitted. Interestingly, the four-level digital modulation technique doubles the data rate while maintaining the same bandwidth signals (this technique provides the system with bandwidth efficiency). Figure 9–15 illustrates the modulation process for both 2- and 4-level GFSK.

The nominal transmitter output power level from an IEEE 802.11 station shall be at least 10 mW (+10 dBm) of equivalent isotropically radiated power (EIRP). Furthermore, if the station output power can exceed 100 mW (+20 dBm) EIRP there must be provisions built into the station for power control that will lower the power to 100 mW or lower. The receiver should have a sensitivity of at least –80 dBm for a data rate of 1 mbps and a sensitivity of –75 dBm for a data rate of 2 mbps. This specification corresponds to a maximum frame error rate (FER) of 3% for PSDUs of 400 bytes in length. The standard also supports antenna diversity for both transmitter and receiver sections. As one might surmise, the standard gives many more technical details (spectrum shape, intermodulation sensitivity, frequency tolerance, etc.) for operation of the transmitter and receiver sections of the wireless station that will not be addressed here because of their minimal relevance to the basic system operational concepts.

## Direct Sequence Spread Spectrum Overview

The IEEE 802.11 specifications call for the use of direct sequence spread spectrum (DSSS) over the 2.4-GHz ISM band as provided for in the United States according to FCC 15.247 and in Europe by ETS 300-328. The DSSS system also provides a wireless LAN with both 1- and 2-mbps data rates. To comply with FCC regulations that call for a processing gain of at least 10 dB, the baseband digital stream will be chipped at a rate of 11 mcps with an 11-chip PN code. To provide the required data rates the DSSS system uses modulation schemes of either differential binary phase shift keying (DBPSK) or differential quadrature phase shift keying (DQPSK). Similar to the FHSS scheme already presented, the DSSS physical layer will have a DSSS PLCP sublayer, a DSSS physical layer management entity (DSSS PLME), and its own DSSS PDM sublayer to transport the data wirelessly between stations.

### *DSSS PLCP Sublayer*

The DSSS PLCP sublayer is somewhat different than the FHSS implementation and therefore will be discussed here. Figure 9–16 shows the DSSS PLCP frame format that composes the PPDU. It consists of a

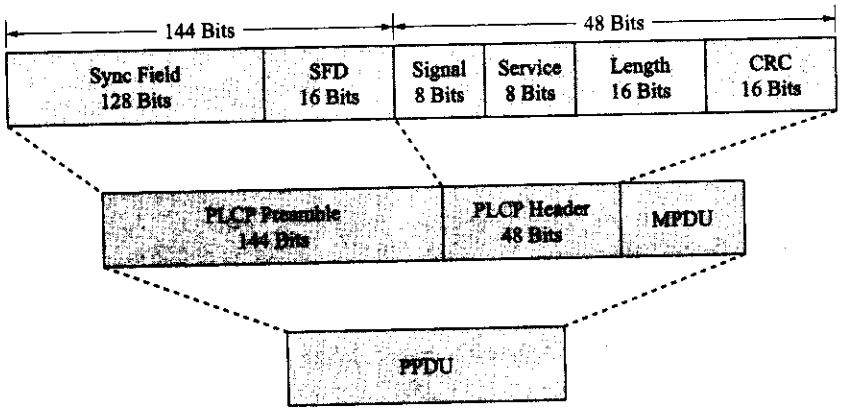



**Figure 9–16** IEEE 802.11 DSSS PLCP frame format (Courtesy of IEEE).

PLCP preamble, PLCP header, and an MPDU. The PLCP preamble consists of a synchronization subfield and a start frame delimiter (SFD). The synchronization field consists of 128 bits of scrambled 1s. This field is provided to facilitate the synchronization of the receiver. The 16-bit SFD is used to indicate the start of the PLCP header field. The 48-bit PLCP header field consists of four subfields, an 8-bit signal field, an 8-bit service field, a 16-bit length field, and a 16-bit CRC field. The signal field indicates the modulation type and data rate, the service field is reserved for future use, the length field indicates the number of microseconds needed to transmit the MPDU (from 16 to $2^{16} - 1$ $\mu$ sec), and the CRC field is used for error detection. All bits to be transmitted over the DSSS physical layer are scrambled before transmission and unscrambled upon reception.

The reader should recall that CDMA technology, used for wireless mobile systems, uses a form of DSSS. For that system, more than one user can transmit over the same frequency allocation at the same time. The reason that this is possible is because special Walsh codes are used to spread the signals and create individual channel elements. The use of DSSS for an IEEE 802.11 wireless LAN does not allow for this type of operation since the same Barker code is used for all transmitters in the network. Therefore, for DSSS WLAN operation the transmission of a PPDU cannot occur until a clear channel assessment is given. We have already discussed the techniques employed to perform the determination of a busy-idle condition and will not repeat the details here. Once the clear channel primitive has been sent to the MAC, the MAC will initiate a transmit request primitive back to the PLCP. The necessary steps will be taken to construct the PPDU and transmission will start. As before, with the FHSS PLCP, the DSSS PLCP transmit and receive procedures can be modeled by state machines.

### *DSSS PMD Layer*

As shown in Figure 9–17, the transmitting DSSS PMD sublayer accepts PLCP sublayer service primitives and provides the physical means by which data transfers can occur over the wireless medium. At the receiver end of the link the DSSS PDM sublayer primitives and parameters for the receiving function provide a data stream transfer, timing information, and associated received signal parameters to the PLCP sublayer.

### *DSSS Physical Layer Details*

The DSSS frequency channel plan is shown in Table 9–3. All channels marked by an "X" must be supported for use in the various countries indicated.

The spreading sequence used by DSSS, known as an 11-bit **Barker sequence,** is given here:

$$+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1,$$

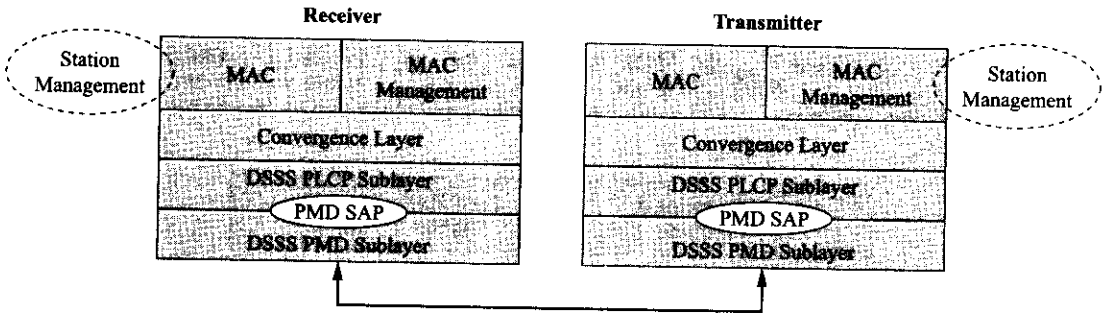



**Figure 9–17** Operation of the DSSS PMD sublayer (Courtesy of IEEE).

**Table 9–3** IEEE 802.11 DSSS frequency channel plan (Courtesy of IEEE).

| *CHNL_ID* | *Frequency* | *Regulatory domains* | | | | | |
|---|---|---|---|---|---|---|---|
| | | *X'10' FCC* | *X'20' IC* | *X'30' ETSI* | *X'31' Spain* | *X'32' France* | *X'40' MKK* |
| 1 | 2412 MHz | X | X | X | — | — | — |
| 2 | 2417 MHz | X | X | X | — | — | — |
| 3 | 2422 MHz | X | X | X | — | — | — |
| 4 | 2427 MHz | X | X | X | — | — | — |
| 5 | 2432 MHz | X | X | X | — | — | — |
| 6 | 2437 MHz | X | X | X | — | — | — |
| 7 | 2442 MHz | X | X | X | — | — | — |
| 8 | 2447 MHz | X | X | X | — | — | — |
| 9 | 2452 MHz | X | X | X | — | — | — |
| 10 | 2457 MHz | X | X | X | X | X | — |
| 11 | 2462 MHz | X | X | X | X | X | — |
| 12 | 2467 MHz | — | — | X | — | X | — |
| 13 | 2472 MHz | — | — | X | — | X | — |
| 14 | 2484 MHz | — | — | — | — | — | X |

This 11-bit sequence is used as the PN spreading code for wireless LAN DSSS operation. The baseband digital symbol duration should be exactly 11 chips long for proper synchronization. Figure 9–18 shows an example of the spreading procedure using the 11-bit code.

The final data transfer rate depends upon whether DBPSK (encodes 1 bit per transmitted symbol time) or DQPSK (encodes 2 bits per symbol time) is used. For DSSS the minimum output power level to be used is 1 mW or 0 dBm and the maximum is 1000 mW (+30 dBm) as shown by Table 9–4. Power control that

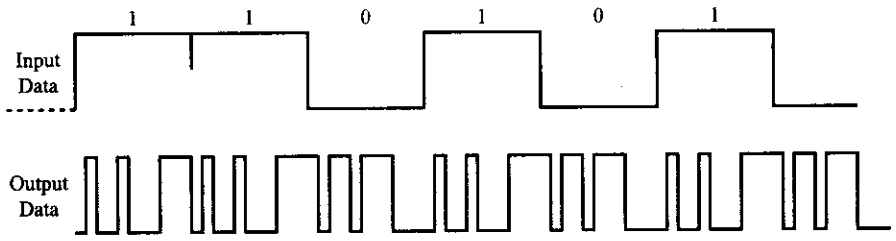



**Figure 9–18** Spreading process using the Barker sequence.

**Table 9–4** IEEE 802.11 DSSS power levels (Courtesy of IEEE).

| *Maximum Output Power* | *Region* | *Compliance Document* |
|---|---|---|
| 1000 mW | United States | FCC 15.247 |
| 100 mW (EIRP) | Europe | ETS 300-328 |
| 10 mW/MHz | Japan | MPT ordinance for Regulating Radio Equipment, Article 49-20 |

provides four power output levels including 100 mW shall be provided for stations capable of outputs higher than 100 mW. The standards specify a transmit spectrum mask, and certain frequency tolerances and modulation accuracy. The DSSS receiver must be able to provide a maximum FER of $8 \times 10^{-2}$ for an MPDU length of 1024 bytes for input signal levels between –4 dBm and –80 dBm. Furthermore, the adjacent channel rejection for channels ≥30 MHz apart must be greater than 35 dB for the same maximum FER. Additional power level specifications are given for the clear channel assessment (CCA) operation that is used to determine when the radio channel is busy or idle.

### Infrared Overview

Only a few comments will be offered here about the infrared mode of wireless LAN operation. At the time of the initial standard, an IR physical layer made perfect sense and in theory could provide the same level of service as the radio channel physical layers albeit over a much shorter range. The standard called for the use of near-visible light in the 850- to 950-nm range for signaling (similar to a TV remote control). For this WLAN implementation, the IR signal is not directed. Instead, the standard called for the use of diffuse infrared transmission. In theory this provides for non-line-of-sight transmission, but this is not a sure thing 100% of the time. As just mentioned, the maximum range afforded by the IR physical layer is low (i.e., in the tens of meters); also, IR signals do not penetrate walls and do not work outside in sunlight. One might question whether there are any significant advantages to IR systems, and the answer is an unqualified yes. Worldwide, there is presently no regulatory restriction on the use of IR. Because of a lack of popularity of IR-based wireless LANs and the increased data transfer rates provided in newer IEEE 802.11x standards using the radio channel, this type of technology (IR) has been passed by for the moment and will receive no more attention at this time by this author. If the reader has some interest in pursuing the details of the IR physical layer, they are available in Section 16 of the standard.

## 9.7 IEEE 802.11A/B/G—HIGHER RATE STANDARDS

Shortly after the adoption of IEEE 802.11, several higher-data-rate extensions were added to the standard. These extensions added new, more complex digital modulation schemes and the use of a new band of

frequencies in the 5-GHz range. These enhancements to the wireless LAN standard came at a very opportune time for the fledgling WLAN industry. As mentioned earlier, data transfer speeds of 1 and 2 mbps, as specified in the initial standard, were way below what wired LAN users had become accustomed to. The new extensions provided data transfer rates that were compatible with wired LAN rates and in the process brought wireless LANs into the mainstream of computer networking. For the first time, the IT departments of both large and small enterprises, school systems, and other computer network users had another choice when it came to computer network infrastructure. The details of these three extensions will be described next in the order of their adoption.

## IEEE 802.11b

IEEE 802.11b was the first rate extension to be adopted. It provides a higher-speed physical layer extension in the 2.4-GHz band by employing more complex modulation schemes. The rate extension adds data rates of 5.5 mbps and 11 mbps in addition to the legacy 1- and 2-mbps rates. To provide the higher rates, 8-chip complementary code keying (CCK) is employed for the modulation scheme. Since the same chipping rate of 11 mbps is used for the new higher data rates, the final signal bandwidth is the same as the original standard. The new high-rate capability offered by 802.11b is known as high-rate DSSS or HR/DSSS. HR/DSSS uses the same PLCP frame format as the initial DSSS physical layer and therefore both rate sets can be used in the same BSS, with rate switching occurring during the transfer of the PSDU. Figure 9–19 shows the long PLCP format that is similar to Figure 9–16 except for the different rate sets used for the transmission of the PSDU. Besides the higher-speed extensions to the DSSS system, several optional features provide enhancements to the standard improving the system radio transmission performance.

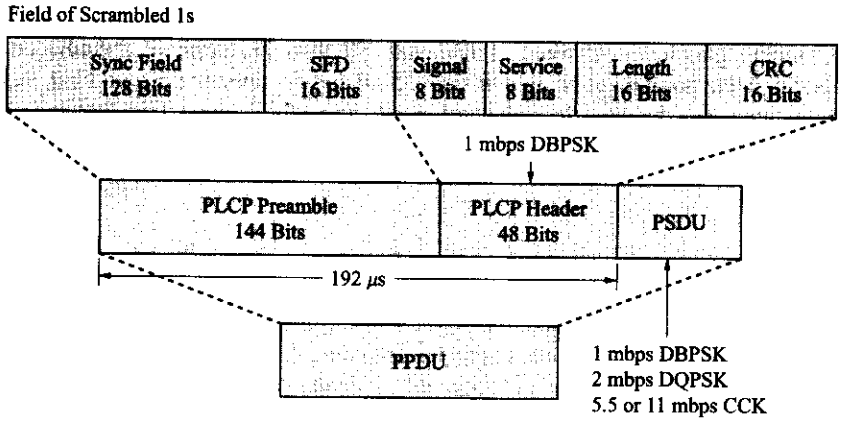



**Figure 9–19** IEEE 802.11b long PLCP format (Courtesy of IEEE).

An optional encoding mode replaces the CCK modulation with packet binary convolutional coding (HR/DSSS/PBCC). This option was added with an eye toward the future as the use of PBCC will most likely facilitate additional rate increases. Another possible optional mode replaces the long PLCP preamble with a shorter PLCP preamble (see Figure 9–20). This option provides higher data throughput rates for the 2-, 5.5-, and 11-mbps rate sets by reducing the overhead involved in the transmission of the preamble. This mode of operation is known as HR/DSSS/short. Furthermore, HR/DSSS/short can coexist with the other DSSS physical layers under certain circumstances. A final optional capability included in 802.11b is that of channel agility. The use of frequency hopping even on a limited basis provides improved radio link performance in the face of certain types of EMI. Figure 9–21 depicts the two basic frequency hopping schemes available for use in North America with IEEE 802.11b.

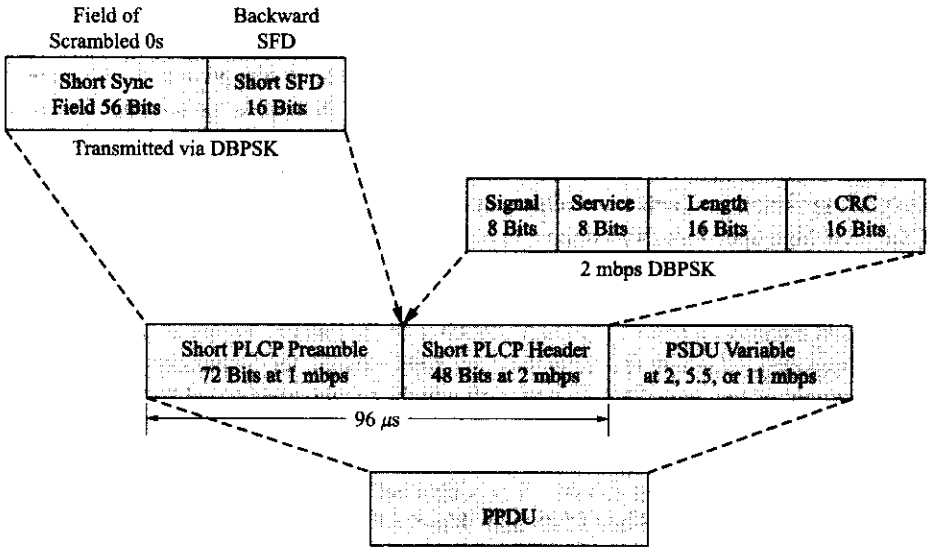



**Figure 9–20** IEEE 802.11b short PLCP format (Courtesy of IEEE).

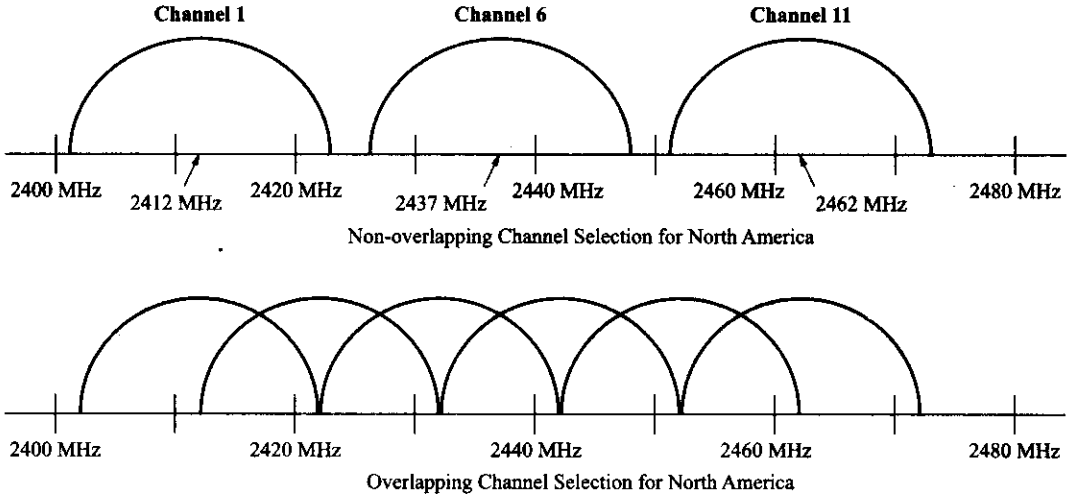



**Figure 9–21** The two basic hopping schemes available for use in North America (Courtesy of IEEE).

### *802.11b Modulation Schemes*

Four data rates, each with a different modulation format, are specified by the 802.11b standard for the high-rate physical layer. The technology employed for the basic and enhanced access rates remains the same; however, the high-speed 5.5- and 11-mbps data rates use CCK or an optional PBCC mode. For the complex CCK modulation modes, the spreading code, C, has a length of 8 and the individual code values are based on complex complementary codes. Through the use of the CCK modulation scheme, 4 data bits are able to be transmitted per symbol (at a rate of 1.375 msps) to achieve a data rate of 5.5 mbps. To achieve the 11-mbps data rate, 8 data bits are transmitted per symbol, again at the 1.375-msps rate.

## IEEE 802.11a

IEEE 802.11a was the next rate extension to be adopted. This extension provided for a new high-speed physical layer to be operational in the 5-GHz band. Through the use of an orthogonal frequency division multiplexing (OFDM) system and complex digital modulation techniques, high-speed data rates of 6, 9, 12, 18, 24, 36, 48, and 54 mbps may be supported within the new standard. However, data rates of 6, 12, and 24 mbps must be supported for both transmitting and receiving by IEEE 802.11a conformant equipment. This use of this new high-speed transmission technology combined with the additional bandwidth available in the 5-GHz band again provided a boost to the wireless LAN industry.

A few comments about the new frequency band are appropriate here. The original ISM band already contained unlicensed bandwidth from 5.725 to 5.850 GHz (refer back to Figure 9–1) that was available for WLAN use. Unfortunately, although the frequency spectrum existed, the technology of the early 1990s precluded the development of inexpensive chip sets with which the spectrum could be used. This obstacle was overcome by the end of the 1990s. However, in the interim, the unlicensed national information infrastructure (U-NII) bands in the 5-GHz range became available in the United States according to the Code of Federal Regulations, Title 47, Section 15.407. This additional bandwidth provided a substantial increase to the previously available unlicensed bandwidth and therefore provided some promise to the future of the wireless LAN industry.

Even though the OFDM physical layer has major differences in its physical implementation, its interaction with the wireless MAC layer is very similar to FHSS and DSSS physical layer schemes. The major differences reside in the convergence procedure that provides for the PSDUs to be converted to PPDUs. Figure 9–22 shows the OFDM PLCP frame format for the PPDU.

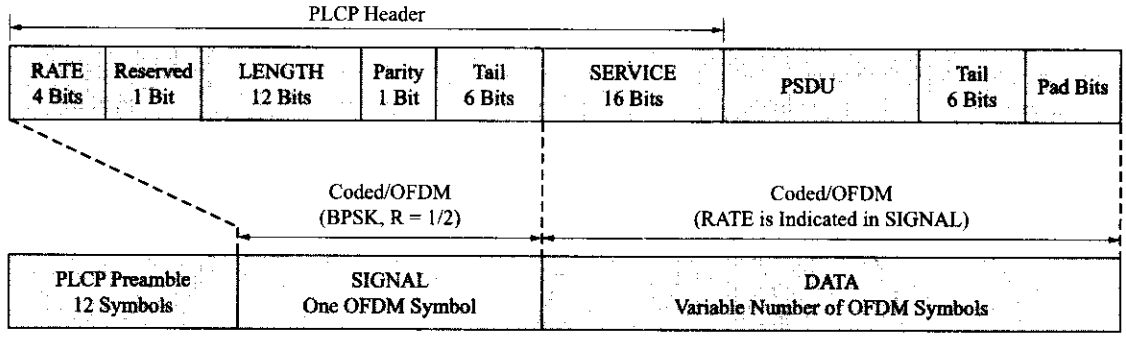



**Figure 9–22** IEEE 802.11a OFDM PLCP frame format (Courtesy of IEEE).

As can be seen in the figure, the frame consists of a twelve-symbol PLCP preamble and a 5-byte PLCP header. The first 3 bytes of the PLCP header constitute a single OFDM symbol. The remaining PLCP service field and the PSDU (labeled as DATA) are transmitted at the data rate specified within the rate subfield of the PLCP header. The rate and length fields may also be used by the CCA mechanism to predict the duration of the packet even though the station may not physically support the data rate indicated. The details of the PLCP preamble are shown in Figure 9–23. It consists of ten short training symbols and two long training symbols. As indicated by the figure, this "short symbol" time is used by the receiver to adjust the system automatic gain control (AGC), for diversity selection, timing acquisition, and coarse frequency adjustment. The long symbol time is used for channel estimation and fine frequency acquisition within the receiver.

### *802.11a Modulation Scheme*

The OFDM scheme employed by IEEE 802.11a uses fifty-two subcarriers (four of which are used as pilots) that are modulated using the following types of modulation schemes: binary or quadrature phase shift keying (BPSK/QPSK), 16-quadrature amplitude modulation (16-QAM), or 64-QAM. To provide forward

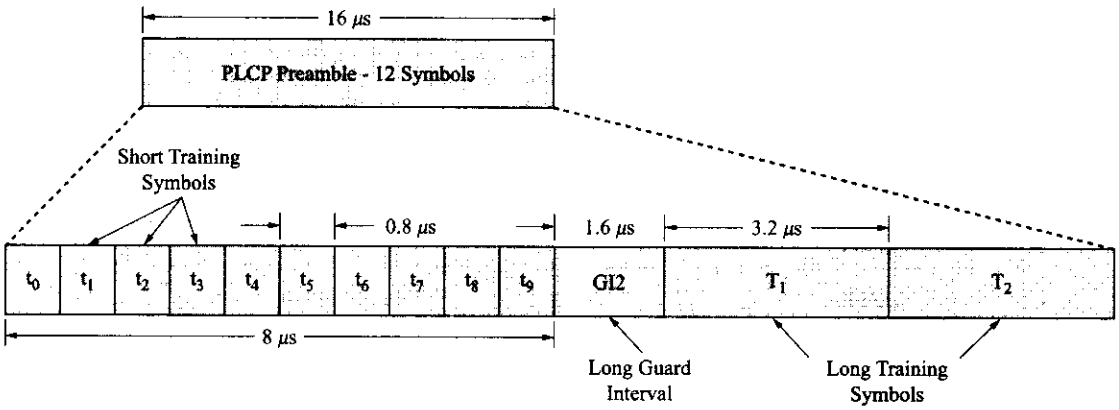



**Figure 9–23** PLCP preamble format details (Courtesy of IEEE).

error correction coding, convolutional coding with coding rates of $R$ = 1/2, 2/3, or 3/4 is employed by the system, as well as block interleaving of the encoded bits. To achieve these high data rates, the system divides a high-speed serial bit stream into multiple lower-speed subsignals that the system transmits simultaneously at different frequencies (subcarriers) in parallel. See Figure 9–24. Table 9–5 provides a matrix of the required modulation type, convolutional coding rate, $R$, coded bits per subcarrier, coded bits per OFDM symbol, and data bits per symbol.

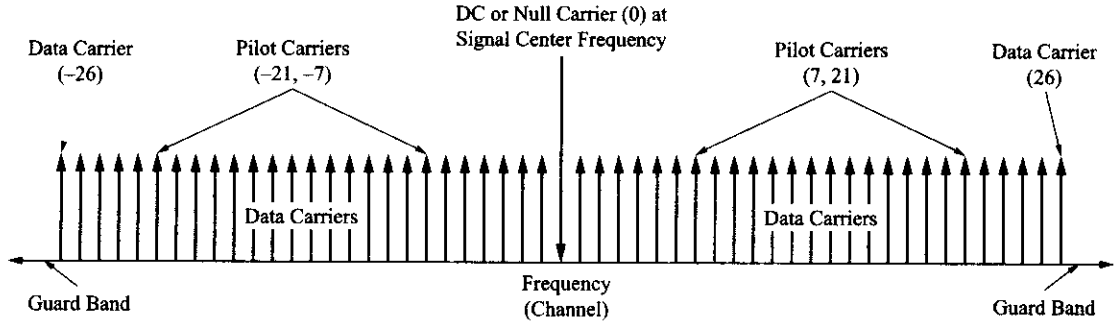



**Figure 9–24** IEEE 802.11a OFDM modulation scheme.

An example of this technique should help to illustrate the process. To transfer data at a rate of 24 mbps, the bit stream is divided up into groups of 96 bits and further subdivided into 48 groups of 2 binary bits per group. Each group of 2 bits undergoes convolutional coding at an $R$ = 1/2 rate producing 48 groups of 4 binary bits per group. Each 4-bit group is encoded into a single 16-QAM symbol for transmission by one of the 48 subcarriers in a 4 $\mu$ sec time interval. The simultaneous transmission of the 48 subcarriers results in a total transfer of 192 coded bits (known as an OFDM symbol) every symbol time of which half of the symbol bits (96 bits) are actual data bits. In this case, the data rate is 96/4 $\mu$ sec = 24 mbps. Therefore, for each OFDM symbol, each subcarrier represents $n$ bits of the entire 48 × $n$-bit OFDM symbol. A subcarrier spacing of 312.5 kHz results in a total signal bandwidth of approximately 16.6 MHz. The reader might notice the similarity of this technique to the digital multitone (DMT) modulation technique employed by ADSL for high-speed data transmission over wireline media (local-loop copper pairs).

The four pilot subcarriers are BPSK modulated by a pseudobinary sequence and used by the receiver's electronics to increase the system's resistance to frequency offsets and phase noise (i.e., used to lower the FER). The fifty-two subcarrier frequencies may be labeled as –26 to +26 with 0 omitted. The four pilots are then located at subcarrier frequencies –21, –7, +7, and +21 (refer back to Figure 9–24).

**Table 9–5** IEEE 802.11a data rates (Courtesy of IEEE).

| *Data Rate (mbps)* | *Modulation Scheme* | *Coding Rate* | *Coded Bits per Subcarrier ($N_{BPSC}$)* | *Code Bits per OFDM Symbol ($N_{CBPS}$)* | *Data Bits per OFDM Symbol ($N_{DBPS}$)* |
|---|---|---|---|---|---|
| 6 | BPSK | 1/2 | 1 | 48 | 24 |
| 9 | BPSK | 3/4 | 1 | 48 | 36 |
| 12 | QPSK | 1/2 | 2 | 96 | 48 |
| 18 | QPSK | 3/4 | 2 | 96 | 72 |
| 24 | 16-QAM | 1/2 | 4 | 192 | 96 |
| 36 | 16-QAM | 3/4 | 4 | 192 | 144 |
| 48 | 32-QAM | 2/3 | 6 | 288 | 192 |
| 54 | 32-QAM | 3/4 | 6 | 288 | 216 |

### *OFDM Operating Frequency Range*

The IEEE 802.11a standard calls for the use of the OFDM physical layer in the 5-GHz band as allocated by the appropriate regulatory body in its operational region. In the United States, the FCC is responsible for the allocation of the 5-GHz unlicensed U-NII bands. The channel numbering system for frequencies above 5 GHz is fairly straightforward and given by the following relationship:

$$\textit{Channel center frequency in MHz} = 5000 + 5 \times n_{ch} \qquad \textbf{9-2}$$

where $n_{ch} = 0, 1, 2, \ldots, 200$

Table 9–6 shows the present valid operating channel numbers for use in the United States, and Table 9–7 indicates the power limits imposed on these subbands. The FCC issued a "Report and Order" on

**Table 9–6** Valid IEEE 802.11 operating channels (Courtesy of IEEE).

| *Regulatory Domain* | *Frequency Band (GHz)* | *Operating Channel Numbers* | *Channel Center Frequency (MHz)* |
|---|---|---|---|
| United States | U-NII lower band (5.15–5.25) | 36<br>40<br>44<br>48 | 5180<br>5200<br>5220<br>5240 |
| United States | U-NII middle band (5.25–5.35) | 52<br>56<br>60<br>64 | 5260<br>5280<br>5300<br>5320 |
| United States | U-NII upper band (5.725–5.825) | 149<br>153<br>157<br>161 | 5745<br>5765<br>5785<br>5805 |

**Table 9–7** IEEE 802.11 power limits (Courtesy of IEEE).

| *Frequency Band (GHz)* | *Maximum Output Power with up to 6 dBi antenna gain (mW)* |
|---|---|
| 5.15–5.25 | 40 (2.5 mW/MHz) |
| 5.25–5.35 | 200 (12.5 mW/MHz) |
| 5.725–5.825 | 800 (50 mW/MHz) |

November 13, 2003, that adds an additional 255 MHz of bandwidth from 5.470 to 5.725 GHz to be used by U-NII devices and radio LANs (RLANs). Devices using this new band and the 5.250- to 5.350-GHz band will have the same set of technical requirements. They will also need to employ some form of dynamic frequency selection (DFS) and transmitter power control (TPC) mechanisms due to the shared nature of the band. Presently, these bands are used for radio location devices, radar, research space satellites, and so on.

Presently, as shown in Table 9–6, there are twenty-four valid, 20-MHz channels available for OFDM operation in the United States. As was the case for the IEEE 802.11b rate extension, the IEEE 802.11a standard provides many additional details about both the transmitter and receiver technical specifications. Table 9–8 details the receiver performance specifications for a packet error rate (PER) of less than 10% for a PDSU of 1000 bytes. The reader should note the change in receiver sensitivity required for the lowest data rate (–82 dBm) versus the highest data rate (–65 dBm). These values translate into high data transfer rates close to the access point and lower rates as the wireless station moves farther away from the AP.

**Table 9–8** Receiver performance requirements for IEEE 802.11 (Courtesy of IEEE).

| *Data Rate (mbps)* | *Minimum Sensitivity (dBm)* | *Adjacent Channel Rejection (dB)* | *Alternate Adjacent Channel Rejection (dB)* |
|---|---|---|---|
| 6 | –82 | 16 | 32 |
| 9 | –81 | 15 | 31 |
| 12 | –79 | 13 | 29 |
| 18 | –77 | 11 | 27 |
| 24 | –74 | 8 | 24 |
| 36 | –70 | 4 | 20 |
| 48 | –66 | 0 | 16 |
| 54 | –65 | –1 | 15 |

## IEEE 802.11g

The last rate extension to the IEEE 802.11 standard to be adopted was IEEE 802.11g in June of 2003. This amendment is a further higherdata-rate extension in the 2.4-GHz band. The extended rate physical (ERP) layer specification builds upon the prior specifications of the IEEE 802.11x standards that use DSSS, CCK, and optional PBCC modulation to provide data rates of 1, 2, 5.5, and 11 mbps. The ERP layer builds on both PBCC modulation modes and the OFDM techniques introduced in IEEE 802.11a to provide support

for data rates of 6, 9, 12, 18, 24, 36, 48, and 54 mbps. It is mandatory in IEEE 802.11g that compliant equipment provides transmission and reception at 1, 2, 5.5, 6, 11, 12, and 24 mbps.

IEEE 802.11g defines two additional ERP-PBCC optional modulation modes that use 8-PSK with resulting payload data rates of 22 and 33 mbps. Also, another optional modulation form known as DSSS-OFDM is defined with payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 mbps.

### *ERP Layer Operation*

The ERP layer has the ability to operate in several mixed and combined modes. Depending upon what options are enabled, the ERP layer can deal with any of the specified data rate extensions for the 2.4-GHz band or non-ERP modes. As an example, a BSS could operate in an ERP-DSSS/CCK-only mode, a mixed mode of ERP-DSSS/CCK and non-ERP, or a mixed mode of ERP-DSSS-OFDM and ERP-DSSS/CCK. The IEEE 802.11g standard outlines the necessary modifications and additions to provide this functionality.

### *DSSS-OFDM Operation*

A few comments about DSSS-OFDM operation are appropriate here. For this combined form of operation, the PPDU format specified by the IEEE 802.11b extension (shown previously as Figure 9–19) is relatively unchanged. A Barker symbol-modulated preamble (DSSS) is still used. However, the single-carrier PSDU is replaced by a PSDU that is transmitted using OFDM techniques. The IEEE 802.11g specification outlines the needed radio and physical layer behavior needed to transition from the DSSS preamble to the OFDM-encoded PSDU data. The OFDM system employed is identical to that described previously (i.e., fifty-two subcarriers in a 20-MHz band) except for the fact that it is now specified for operation within the 2.4-GHz band.

## 9.8 IEEE 802.11I—WIRELESS LAN SECURITY

Although it is difficult to understand the motivation behind their actions, it is a fact of life that there is a small but quite persistent and, if you will, equally malicious group of so-called computer hackers. These individuals are continually inventing new computer viruses and launching attacks on the world's computers and computer networks with these rouge programs. Although the Internet is typically used as the initial delivery mechanism, these computer virus programs often use infected machines to pass the viruses on to other machines on the same computer network or other computer networks (again, via the Internet). The usual intent of these virus programs is to cause harm to the operating system of the infected machine and the data that is contained on the system's hard drive. In some cases, these hackers are content to take control of "hacked" machines to help carry out denial-of-service attacks on a particular computer network or network target.

Still another group of computer users has seen the advent of wireless LANs as an opportunity (they would call it a challenge!) to hack into these wireless networks to gain free high-speed Internet access or access to someone else's Intranet. Additionally, many of these individuals have seen fit to set up wireless LANs without security and offer Internet access for free to anyone in the coverage area of the open network. Although this group often professes its nonmalicious intents, some in this group have gone as far as to survey various geographic locations as a form of a wireless LAN scavenger hunt or game. These wireless LAN scavengers or **wardrivers** as they have been named oftentimes will go as far as to publicize open or unsecured wireless LANs on Internet Web sites or to mark the sidewalks of major metropolitan cities with cryptic symbols (known to other wardrivers) indicating the presence of such an open wireless network. Presently, there are various free software programs available that, in conjunction with a wireless network card (operated in RF monitor mode), allow one to detect the presence of wireless LAN networks and to determine the level or lack of security employed by the particular network. In fact, recent surveys (2004) of existing wireless LANs indicate that the vast majority use either no security or minimal levels of

security! Furthermore, even if the wireless network is employing basic security, AirSnort and WEPcrack are two programs that are able to recover encryption keys through passive monitoring of wireless LAN traffic. For both programs, advantage is taken of flaws in the original WEP protocol to crack the system security. The wide acceptance of the IEEE 802.11 extensions by the home computer user with the resulting proliferation of wireless home networks has brought wireless LANs into the mainstream as a means to provide mobility to the user. At the same time, the wireless hacking predicament and the lack of a robust wireless LAN security protocol has brought this problem to the attention of Enterprise IT managers who are under pressure to provide the same wireless mobility to Enterprise workers. This situation has resulted in a concerted effort to increase the level of security available for IEEE 802.11x wireless LANs. Recently, in 2004, IEEE 802.11i was adopted to provide this increased level of security.

## Types of Wireless LAN Security Problems

Before discussing the details of wireless LAN security, a quick review of some of the popular types of attacks on these networks will be instructive:

- Eavesdropping: the attacker listens to private communications or steals sensitive information by listening to wireless data traffic.
- MAC spoofing: the attacker is able to identify a valid MAC address of a legitimate network user and makes a copy of it to gain access to the wireless network.
- Dictionary attack: the attacker systematically tries all possible passwords in an attempt to determine the correct one and gain access to the network.
- Man-in-the-middle attack: the attacker impersonates a legitimate access point in order to gain sensitive user information (i.e., passwords and user names) from a legitimate user that has inadvertently attempted to associate with the rouge access point.
- Theft of service: the attacker gains Internet access through the Enterprise or home wireless LAN infrastructure resulting in ISP charges for unauthorized use or the unauthorized sending of e-mail (spam) from the compromised network.
- Session hijacking: the attacker waits until a client has successfully authenticated to the network, sends a disassociation message to the client using the MAC address of the access point, and then starts sending traffic to the access point by spoofing the MAC address of the client.

## Initial IEEE 802.11 Security

The original IEEE 802.11 standard included limited authentication protocols and, as it turned out, a weak form of data encryption. A casual overview of these procedures was presented earlier in this chapter during a discussion of the services offered by a wireless network. Simply put, the initial IEEE 802.11 authentication process supported MAC authentication of wireless clients and the standard allowed for what was known as wired equivalent privacy (WEP) encryption.

### *Authentication Details*

IEEE 802.11 performs user authentication in the following fashion: only traffic from authorized MAC addresses will be allowed through the access point. This is accomplished by checking the MAC address of the station requesting association against the access point's own database of valid users or through a RADIUS (remote authentication dial-in user service) server external to the access point that is used for overall network authentication. However, this type of authentication is considered inadequate due to the fact that it may be circumvented and because it is unilateral in nature. For this case, the process of authentication may be thwarted by changing the MAC address of a wireless network card from an invalid one to a legitimate one. Also, since authentication is performed on the hardware that is being used and not tied to the user's identity, it is possible that equipment stolen from a legitimate user could be used to join the network. Lastly, the unilateral aspect of this form of authentication is troublesome from the following

standpoint: a user could unknowingly associate with a rouge access point since the user does not authenticate the access point. This man-in-the-middle attack could yield restricted information that could be used to gain access to the actual wireless network.

### *WEP Encryption Details*

The WEP algorithm is symmetric in nature. The same key is used for both encryption and decryption. The WEP key used to encrypt wireless LAN traffic consists of two parts: a 24-bit initialization vector (IV) and a 40-bit user-defined key. The IV and the user key are combined to create a 64-bit composite key that is used to encrypt the user data during the transmission process as shown by Figure 9–25. As shown by the diagram, the 64-bit key is applied to a pseudorandom number generator (PRNG) at the same time the data stream is used to calculate an integrity check value (ICV) to prevent unauthorized modification of the data. The ICV is appended to the data and the resulting data stream is mathematically combined with the correct-length key sequence. Finally, the IV is broadcast in the clear together with the encrypted data as the composite message.

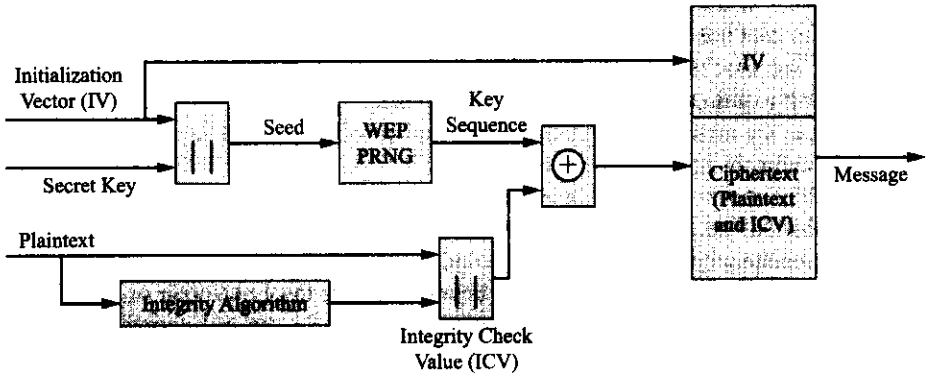



**Figure 9–25** WEP encryption block diagram (Courtesy of IEEE).

Figure 9–26 shows the decryption process that occurs after reception of the transmitted data. The incoming IV is used to generate the required key sequence to decipher the incoming message. The integrity check algorithm is performed on the recovered data and the result is compared to the transmitted ICV. If the two values of ICV are not equal an error message is sent to MAC management.

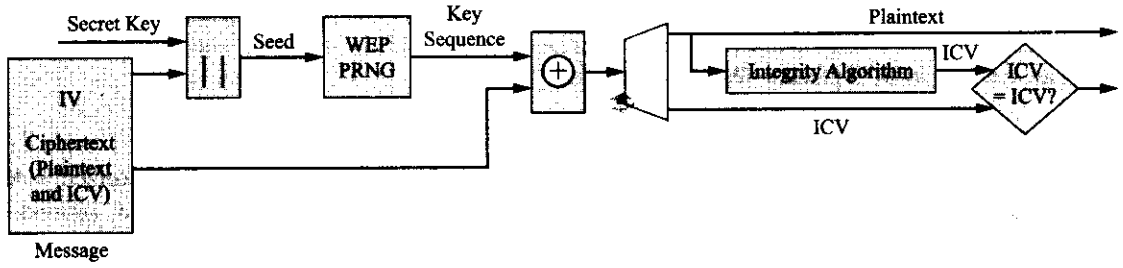



**Figure 9–26** WEP decryption block diagram (Courtesy of IEEE).

It did not take long for several academic researchers to discover and subsequently point out the vulnerabilities of the WEP IV keys (e.g., see "Weakness in the Key Scheduling Algorithm of RC4," by Fluhrer, Mantin, and Shamir). As discussed earlier, the RC4 algorithm developed by RSA Security could be broken fairly easily by free software programs posted on the Internet.

## IEEE 802.11 Temporary Security Enhancements

As soon as it became well known that the original version of WEP could be hacked fairly easily, several vendors began to offer enhanced proprietary forms of WEP that would allow equipment the capability of not using the weak IVs during transmit cycles. This was most effective in wireless LANs that used the vendor's equipment for both the stations and the access points. Later, multilevel WEP was introduced with 64-, 128-, and 152-bit user keys, and a more robust intermediate solution or fix that could be applied to existing wireless LAN hardware was derived from the draft version of IEEE 802.11i. This fix is known as **Wi-Fi protected access** or WPA. WPA is a specification of standards-based interoperable security enhancements that improve wireless LAN security. WPA was designed to run on existing hardware through a software upgrade and provides better data protection and access control to a wireless LAN. Data encryption is improved by using the temporal key integrity protocol (TKIP). TKIP enhances WEP by using a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector with sequencing rules, and a rekeying mechanism. Additionally, WPA supplies Enterprise-level user authentication via IEEE 802.1x (the standard for port-based network access control, adopted in 2001) and the extensible authorization protocol (EAP). Together these technologies provide for a much stronger user authentication process. The key to this authentication structure is the use of a centralized authentication (RADIUS) server and mutual authentication to prevent man-in-the-middle attacks.

### *Further Details of EAP and IEEE 802.1x*

The IEEE 802.1x framework is based on the Internet Engineering Task Force (IETF) extensible authorization protocol over LAN (EAPoL) messages. Due to conflicting interests among the wireless LAN vendors, the finalization of IEEE 802.11i was delayed repeatedly. In the meantime, several industry groups and vendors promoted their own short-term solutions to the security problem before the final adoption of the IEEE 802.11i standard. The net result of these actions was that various forms of EAP were developed and adopted for use. Therefore, at this time there are a number of EAPoL authentication protocols that the wireless LAN user may choose from. The most common types of EAP are listed here:

- EAP-MD5 (message digest 5) is a weak form of authentication. Since it only offers client-side authentication it will not be used when the highest level of security is needed.
- EAP-TLS (transport layer security) has no known security weaknesses and has strong support from Microsoft. It requires the use of a RADIUS server and digital certificates at both the station and the RADIUS server. It is supported in Windows XP and there are updates to support it in earlier Windows operating system versions.
- LEAP (EAP Cisco Wireless version) provides a fairly effective way to secure wireless networks while still using WEP-based devices. It is vulnerable to dictionary attacks and therefore is not recommended for use with IEEE 802.11i.
- EAP-TTLS (tunneled TLS) and PEAP (protected EAP) are similar EAP authentication protocols that are supported by a large number of wireless LAN vendors. These protocols also use digital certificates but only at the RADIUS server. The station authenticates the RADIUS server using the server's digital certificate, and a secure tunnel is then set up between the station and the server through which the server can then authenticate the station.

In each case, when a station attempts to connect to a wireless LAN under IEEE 802.1x, the access point will enable the station to connect but then forces it into an unauthorized state in which only EAP traffic is passed along to the RADIUS server. Using EAP messages and either passwords or public/private key encryption technology the RADIUS server will authenticate the station. Next, the RADIUS server will provide the access point with an initial encryption key that was derived from the station through the authentication process. The access point then generates a second key for use in communicating with the station. It encrypts the second key with the initial key from the RADIUS server and sends it to the station. The access point then sends fresh keys to the station periodically to ensure that security is not broken. Figure 9–27

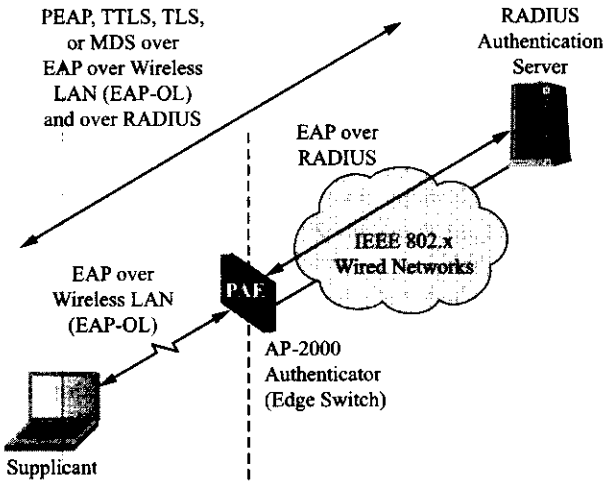



**Figure 9–27** WPA operation with EAP-TLS.

shows this process in more detail for the EAP-TLS protocol. For the EAP protocols, new terms have been introduced: the station is known as the supplicant, the access point is the authenticator, and the RADIUS server is the authentication server.

## IEEE 802.11i—WPA Version 2

IEEE 802.11i was finally ratified during 2004. It is also known as WPA version 2 or WPA2. Also, networks employing the IEEE 802.11i standard are known as **robust security networks** (RSNs). WPA2 uses an advanced form of encryption known as AES (**advanced encryption standard**) that allows for compatibility with FIPS PUB 140-2, a U.S. government security standard. In an effort to prevent a reoccurrence of the WEP security problems, the international cryptographic community played an active role in the development of the IEEE 802.11i standard. AES is a block cipher that was chosen for its robustness. Presently, it resists all known techniques of cryptanalysis.

As of this writing, RSN-certified wireless LAN equipment is available in the marketplace. This fact should provide many reluctant IT departments with the push needed to add wireless LANs to their network infrastructure. Additionally, vendors have already implemented proactive security measures by adding rouge access point detection and notification schemes to IEEE 802.11i-compliant wireless access points. One might question what can be done with legacy wireless LANs that consist of original IEEE 802.11/b equipment that is either not compatible with the new standard or is not upgradeable to it. In these cases, it is possible to run both simultaneously if certain additional measures are put into place. For mixed-mode enterprise networks, running virtual private network (VPN) software on legacy stations and moving legacy access points outside a firewall is one possible solution. One final note, this short treatment of the status of wireless LAN security is not meant to be exhaustively comprehensive in its scope, and it is hoped that the readers with an interest in this topic will avail themselves of the many references available.

# 9.9 COMPETING WIRELESS TECHNOLOGIES

As was the case with cellular wireless, the rest of world has also been working on regional or national wireless LAN standards. The most noteworthy projects will be mentioned here. HiperLAN1 and HiperLAN2 are the European equivalents of the IEEE 802.11x standards. The reader is directed to the HiperLAN2 global forum at www.hiperlan2.com for the most up-to-date news about this technology.

### HiperLAN1 and HiperLAN2

The **HiperLAN** project began in Europe and was ratified by the European Telecommunications Standards Institute (ETSI) in 1996 under the banner of the Broadband Radio Access Network (BRAN) organization. The second iteration of the standard (HiperLAN1) calls for operation in the 5.2-GHz radio band, using GMSK modulation, with support for data rates up to 24 mbps. In 1998, the ETSI established a new project for BRAN based on wireless ATM. The ESTI started work on three main set of standards: HiperLAN Type 2 (HiperLAN2) with 25-mbps data rates and indoor, local mobility, HiperAccess with 25-mbps data rates and outdoor, fixed operation, and HiperLink with 155 mbps over a fixed backbone.

HiperLAN2 is a high-performance, next-generation radio LAN technology with its roots in the Wireless ATM Forum. It uses the 5-GHz band, supporting up to 54 mbps using a connection-oriented protocol for sharing access among end user devices; supporting QoS it can carry Ethernet frames, ATM cells, and IP packets. It provides increased security, dynamic frequency selection, and is moving toward compatibility with 3G wireless. It employs a physical layer similar to 802.11a with OFDM modulation, using fifty-two subcarriers, over a 20-MHz channel. However, as of this writing (2005), if one searches the Web, there are still no HiperLAN2 products for sale and the Web site of the HiperLAN2 Forum has gone stale. It is this author's opinion that HiperLAN2 will not compete with IEEE 802.11 technology in the near future. Also, recall the purpose of the 802.11h project—to work on revisions to 802.11 that will make it easier to be deployed in Europe.

### HomeRF and MMAC

A HomeRF working group was formed in 1998 with a goal of providing an open industry specification to be known as SWAP for the purpose of wireless home networking between PCs and consumer electronic devices. SWAP (shared wireless access protocol) was to operate at 2.4 GHz, use FHSS, and provide data rates of 1 and 2 mbps. The early versions of HomeRF were incompatible with IEEE 802.11b. In 2002 the group moved toward the endorsement of IEEE 802.11a as the next generation of wireless LANs. The HomeRF working group disbanded in January of 2003.

MMAC stands for multimedia mobile access communication. This is a fairly recent Japanese initiative that appears to have just as quickly faded away. Recall that IEEE 802.11j that has recently been adopted addresses the Japanese market. The IEEE 802.11x standard has proven to be an impressive market leader and may soon prove to be the de facto worldwide standard for wireless LANs if that is not already the case.

## 9.10 TYPICAL WLAN HARDWARE

Presently, the consumer may purchase home (consumer electronics) wireless LAN equipment (radio cards and APs) through numerous retail outlets, or more robust "industrial quality" hardware implementations of the IEEE 802.11x standard through the sales distributors of these products. Typical versions of these products are shown in Figures 9–28 through 9–30.

As mentioned earlier, PC manufacturers are starting to integrate the wireless LAN station function into the legacy PC, laptop PC, tablet PC, and PDA. It will not be long before this functionality is also provided in a 3G-enabled subscriber device.

### Hardware Setup

The typical setup procedures for a **radio card** (a transceiver that plugs into a PC or laptop computer) or an AP are quite straightforward. Software drivers provided with the products or supplied with the PC operating system are usually easily installed by users. The radio card software driver typically offers a configuration utility that simplifies the management and configuration of the card. The typical functions that can be managed are the network association and basic configuration parameters. A typical association

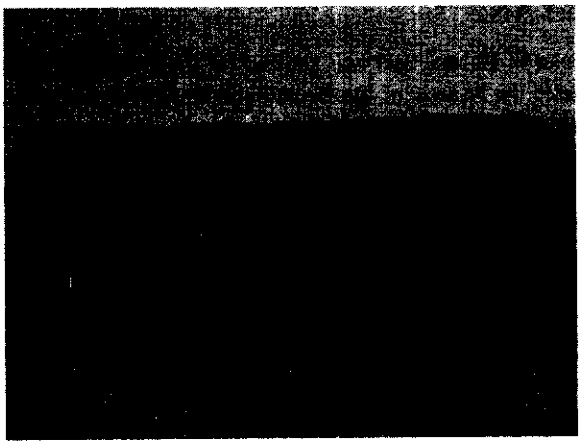


**Figure 9–28** Wireless LAN notebook radio card.

**Figure 9–29** Consumer quality wireless LAN access point.

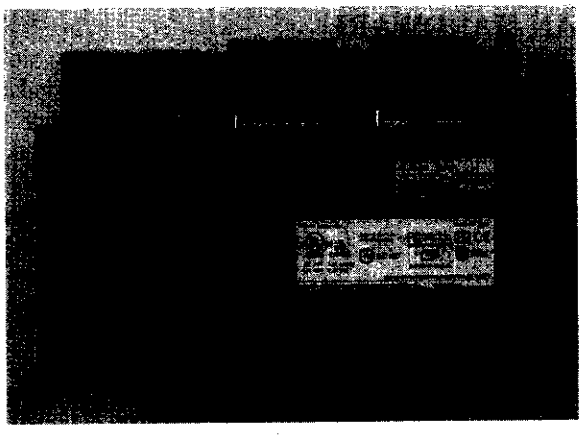


**Figure 9–30** Commercial quality wireless LAN access point.

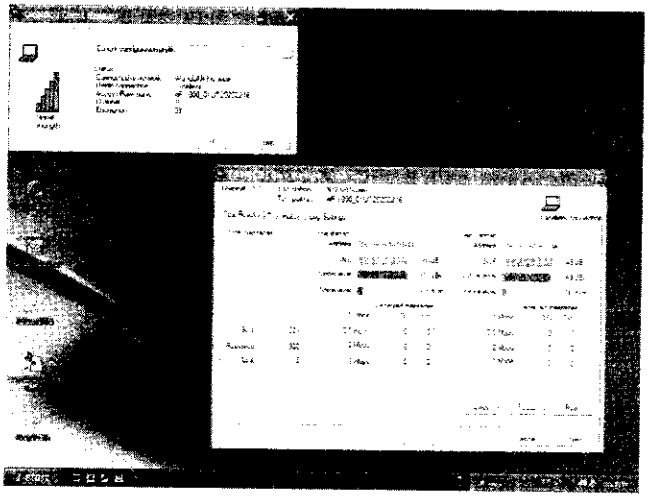


**Figure 9–31** Typical WLAN association information screen.

screen will report various statistics such as operational mode (802.11a, 802.11b, etc.), association state, network name, channel, security parameters, signal strength, send/receive packet transfer rates, history of packets sent and received, and other miscellaneous system statistics. See Figure 9–31 for a screen shot of a typical association information screen.

The configuration utility typically allows the user to configure basic network associations, wireless security, and advanced system parameters. The basic configuration usually deals with the type of network (either ad hoc or access point). If set to ad hoc or peer-to-peer, several more parameters must be defined to facilitate this type of operation (mode, network name, channel, encryption keys, etc.). For AP operation many of the operations performed are automatic. Other options to set are mode, auto mode preference, power savings, and roaming. The security configuration usually lets the user set the level of security desired from none to some highest available level. Depending upon the date of manufacture, today's wireless LAN security has been enhanced to provide 64-, 128-, or 152-bit WEP encryption; other forms of proprietary encryption schemes; and ultimately RSN (IEEE 802.11i) security. Advanced system settings might deal with the use of RTS/CTS, fragmentation options, channel assignment, and transmit rates. Additional features of the configuration utility are the presentation of network statistics. These statistics are usually available in several graphical forms (including real-time bar graphs) about the number of packets sent and received and finer details about the type of packets, transmission retries, last ACK RSS indication (RSSI), errors, and so forth. Also typically available within the configuration utility is a site RF monitor function that can provide radio link parameters and display information about all the wireless networks that are operational within the station's receiving range. Some products also provide a "snoop" tool that allows the system to scan the entire 2.4- and 5-GHz bands. With this tool one may determine if there is any wireless network activity currently taking place.

The setup of an access point is usually performed through the same general method as the radio card. Usually a Windows-type AP management program will be supplied with the AP. In this case, the access point will usually be addressed over the wired network it is connected to through a default IP address. The default address will be entered into the access point manager software and the user/manager will be able to invoke management and configuration utilities to set up the AP. Most of the details presented about the functionality of the radio card configuration utility may also be applied to the AP management software. Presently, most major manufacturers of wireless LAN APs also offer a software management tool that provides control of a network of APs. Another system solution that is being used for large wireless LANs with many APs is to employ an AP controller (APC) to provide management of the other APs and thus off-loading most of the management function from the other APs.

A typical implementation of the access point for a home network consists of a wireless access point router combined with a small four-port switch as shown in Figure 9–28. This device provides an Ethernet interface to a high-speed cable modem or xDSL connection and allows a shared access to the high-speed connection through wired Ethernet LAN connections via the four-port switch or wireless access through the wireless AP section of the device.

Most wireless LAN products come with quality documentation that leads the buyer through the setup procedures in easy-to-follow "plug-and-play" type steps. This is one more reason why the take-up rate of wireless IEEE 802.11x LANs has been accelerating at an exponential rate and moving into the consumer market-place.

## QUESTIONS AND PROBLEMS

1. What are the basic goals of the IEEE 802.11 wireless LAN standards?
2. What data rates are supported by the initial IEEE 802.11 wireless LAN standards?
3. What are the IEEE 802.11 extensions?
4. What is the simplest wireless LAN configuration possible?
5. What function/purpose does the wireless LAN access point have?
6. What is a fundamental difference between a wireless LAN and a wired LAN?
7. Describe the basic structure of a wireless LAN independent basic service set.
8. Describe the basic structure of a wireless LAN extended service set network.
9. What basic functions do the station services provide for the operation of a wireless LAN?
10. What basic functions do the distribution services provide for the operation of a wireless LAN?
11. Describe the wireless LAN association function.
12. Describe the wireless LAN disassociation function.
13. Describe wireless LAN mobility.
14. Describe the difference between Class 1 and Class 2 wireless LAN frames.
15. Name the three types of wireless LAN MAC frames.
16. How is a wireless LAN basic service set identified?
17. Describe the basic procedure employed to gain access to and to subsequently join a wireless LAN system.
18. What is the purpose of the wireless LAN beacon frame?
19. What component of a wireless LAN provides timing to the wireless LAN network?
20. Describe the basic operation of Gaussian FSK modulation used to encode data for transmission over the air during WLAN operation.
21. Both CDMA cellular and wireless LANs use forms of direct sequence spread spectrum modulation; describe the basic difference between the two systems.
22. When is power control used during wireless LAN operation?
23. Comment on the use of IR transmission technology for the implementation of a wireless LAN.
24. What advantages does the use of IR transmission technology have?
25. How do the IEEE 802.11 extensions achieve higher data transfer rates?
26. Describe how the data rate of 18 mbps is achieved under the IEEE 802.11a standard.
27. Describe how the data rate of 48 mbps is achieved under the IEEE 802.11a standard.
28. Do a Web search of "HiperLAN." Discuss the status of this wireless LAN technology.
29. How does one normally set up a wireless LAN access point?
30. What is the function/purpose of a wireless LAN "snoop" tool?