Table 4-1 OSI layers and functions

Layer	Function
Application (Layer 7)	Provides the user interface to allow network services. These services may include such things as e-mail and transferring files.
Presentation (Layer 6)	Handles how the data is represented and formatted for the user.
Session (Layer 5)	Permits the devices on the network to hold ongoing communications across the network. Handles session setup, data or message exchanges, and tear-down when the session ends.
Transport (Layer 4)	Ensures that error-free data is given to the user. Handles the setup and tear-down of connections.
Network (Layer 3)	Picks the route packets take and handles addressing of packets for delivery.
Data Link (Layer 2)	Detects and corrects errors. If data is not received properly, requests data to be retransmitted.
Physical (Layer 1)	Sends signals to the network or receives signals from the network.

In this chapter you learn about IEEE 802.11 wireless LAN functions at the lowest layer of the OSI reference model, the Physical layer. Because the Physical layer primarily deals with turning packets into electrical impulses for transmission, you begin by exploring the different wireless modulation schemes that are used. Then you examine each of the IEEE WLAN standards, 802.11b, 802.11a, and 802.11g, and see how they are implemented at the Physical layer.

Wireless Modulation Schemes

The carrier signal sent by radio transmissions is simply a continuous electrical signal that of itself carries no information. The changes to the signal known as modulations enable it to carry information. There are four primary wireless modulation schemes: narrowband transmission, frequency hopping spread spectrum, direct sequence spread spectrum, and orthogonal frequency division multiplexing. Narrowband transmission is used primarily by radio stations, but the other three schemes are used in IEEE 802.11 WLANs.

Narrowband Transmission

Recall that the radio frequency spectrum is the entire range of all radio frequencies. This spectrum is divided into 450 different sections known as bands. Radio signals by nature transmit on only one radio frequency or a very narrow portion of the frequencies. This is known as **narrowband transmission**. Broadcast radio stations, for example, tell their listeners to "tune to 89.5" because this is the frequency on which the radio signal is transmitted. Narrowband transmissions require more power for the signal to be transmitted because the signal must exceed the **noise level**, or the total amount of outside interference (**noise**), by a substantial margin. Narrowband transmissions are illustrated in Figure 4-3.

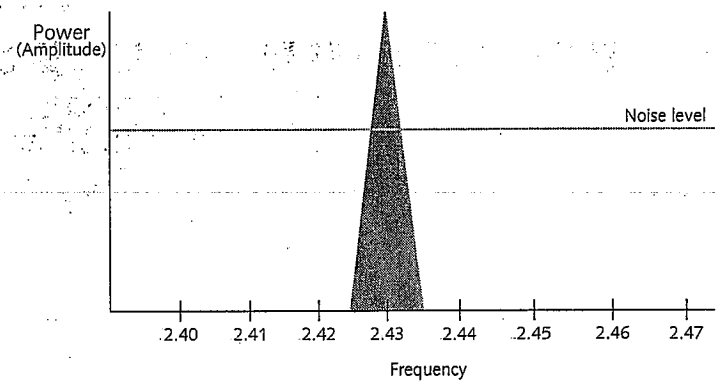

Figure 4-3 Narrowband transmission

A disadvantage of narrowband transmissions is that they are vulnerable to interference from another radio signal being transmitted at or near the same frequency. Much like an accident on a one-lane road can stop all traffic, a single interfering signal at or near the broadcast frequency can render a radio transmission ineffective. This makes narrowband transmissions a poor choice for use in wireless LANs, and the IEEE 802.11 standards do not use narrowband transmissions.

The reason why broadcast radio stations' narrowband transmissions work efficiently is because each station is allowed to transmit on only one frequency in a geographical area. The Federal Communications Commission (FCC) regulates those broadcast radio frequencies.

Spread Spectrum Transmission

An alternative to narrow band transmission is **spread spectrum transmission**. Spread spectrum is a technique that takes a narrow, weaker signal and spreads it over a broader portion of the radio frequency band, as seen in Figure 4-4.

Spread spectrum has several advantages over narrowband transmission:

- *Resistance to narrowband interference*—Spread spectrum transmission is more resistant to outside interference. This is because any interference would affect only a small portion of the signal being transmitted instead of impacting the entire signal as with narrowband. In this way spread spectrum transmissions help keep traffic moving, much like multiple lanes of a highway: although an accident in one lane of an eight-lane freeway is inconvenient, there still are seven other lanes by which cars can move around it and keep going.
- *Resistance to spread spectrum interference*—Because each spread spectrum transmitter uses a different set of "procedures" (algorithms) for transmitting its signal, spread spectrum transmissions typically do not interfere with other spread spectrum signals.

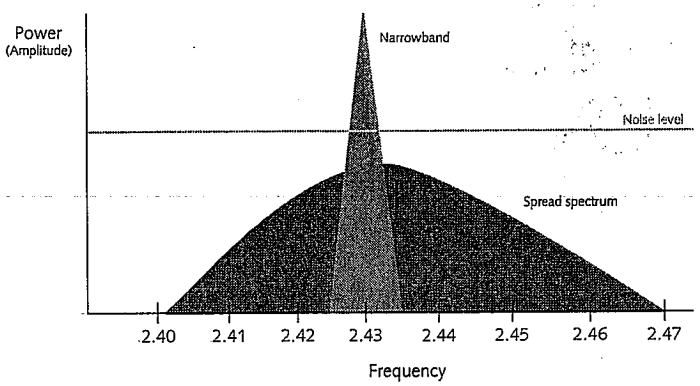

Figure 4-4 Spread spectrum transmission

- *Lower power requirements*—Since spread spectrum requires less power to transmit the signal, the radio sending unit does not require as much energy as does a narrowband unit.
- *Less interference on other systems*—The spread spectrum signal is transmitted beneath the noise level. This means that other radio receivers that pick up the signal would consider it to be "standard" noise and ignore it. The result is that spread spectrum transmissions do not generally interfere with other radio transmissions.
- *More information transmitted*—Spread spectrum transmission can send more bits at one time than a similar narrowband transmission.
- *Increased security*—Other radio receivers see spread spectrum transmissions as noise and ignore it, which provides an additional degree of security for spread spectrum transmissions because other radio receivers cannot easily eavesdrop on the transmission.
- *Resistance to multipath distortion*—Although not entirely eliminated with spread spectrum transmission, the amount of multipath distortion is reduced. This is due to the low power level at which spread spectrum is transmitted.

Spread spectrum transmission uses two methods to spread the signal over a wider area: frequency hopping spread spectrum and direct sequence spread spectrum.

Frequency Hopping Spread Spectrum (FHSS)

The historical background of frequency hopping spread spectrum (FHSS) helps to illustrate this technology. During the early part of World War II Nazi German warships had developed a method for jamming the radios that guided U.S. torpedoes. Film actress Hedy Lamarr, whose first husband manufactured military aircraft control systems, and music composer George Antheil were Hollywood neighbors who struck up a conversation one day regarding how to prevent torpedoes from being jammed. Antheil proposed that rapid changes in radio frequencies could be coordinated in much the same way he had coordinated 16 synchronized player pianos in one of his music pieces. Within a short time they fleshed out their idea and applied for a patent on a "Secret Communication System" in 1941. This invention used slotted paper rolls similar to player-piano rolls to synchronize the frequency changes in a radio transmitter and receiver using 84 frequencies, the number of keys on a piano. They received a U.S. patent for their idea the following year.

Although Lamarr and Antheil's idea was never implemented during the war, once electronics were cheaply available in the late 1950s, the military used the concept as a basic tool for securing military communications. By this time the patent had expired and the duo never received any royalties.

Frequency hopping spread spectrum (FHSS) follows this same concept. Instead of sending on just one frequency (also called a **channel**), frequency hopping uses a range of frequencies that change during the transmission. With FHSS, a short burst is transmitted at one frequency, then a short burst is transmitted at another frequency, and so on, until the entire transmission is completed.

Figure 4-5 shows how FHSS works. The transmission starts by sending a burst of data at the 2.44 GHz frequency for 1 **millisecond** (**ms** or thousandth of a second). The amount of time that a transmission occurs on a specific frequency is called the **dwell time**. Then the transmission changes to the 2.41 GHz frequency (called the **hop time** and is measured in **microseconds** (μs) or millionths of a second) and transmits for the second millisecond. At the third millisecond the transmission takes place at the 2.42 GHz frequency. This switching of frequencies takes place until the entire transmission is complete. The sequence of changing frequencies is called the **hopping code**, which in Figure 4-5 is 2.44-2.41-2.42-2.40-2.43.

Naturally the receiving station must also know the hopping code in order to correctly receive the transmission.

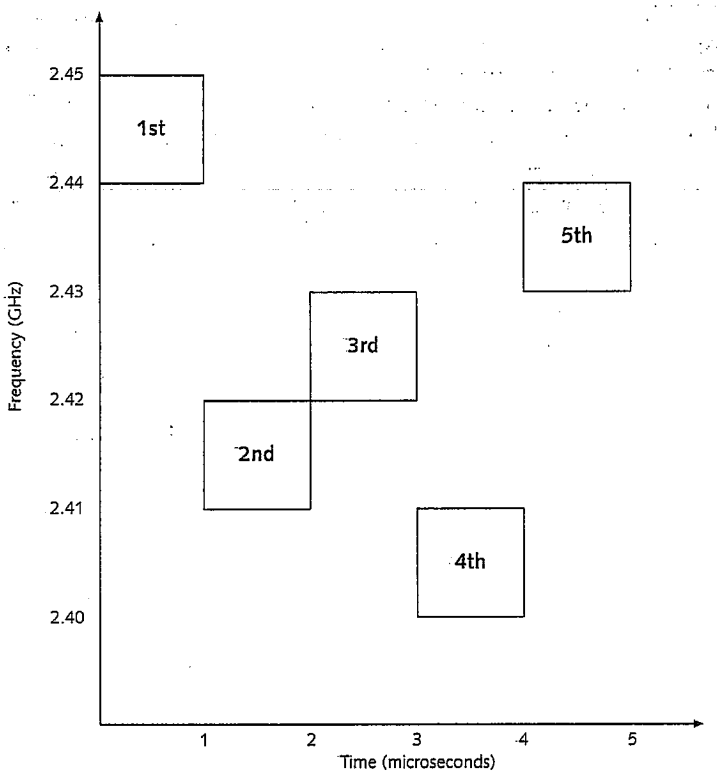

Figure 4-5 Frequency hopping spread spectrum (FHSS) transmission

When transmitting with FHSS, if interference is encountered on a particular frequency then that part of the signal will be retransmitted on the next frequency of the hopping code. Figure 4-6 shows that the second transmission was interfered with, so it was retransmitted on the frequency that would normally carry the third transmission. All subsequent transmissions are then moved to the next frequency of the hopping code. Because FHSS transmits short bursts over a wide range of frequencies, the extent of any interference will be very small and can easily be corrected by error checking. In addition, FHSS signals will have a minimal interference on other signals.

The FCC has established restrictions on FHSS to reduce interference between systems. All FHSS systems in the 900 MHz band must change frequencies ("hop") through 50 channels and cannot spend more than 400 milliseconds (0.4 seconds) on one frequency each 20 seconds. For transmissions in the 2.4 GHz band, the original FCC restrictions required

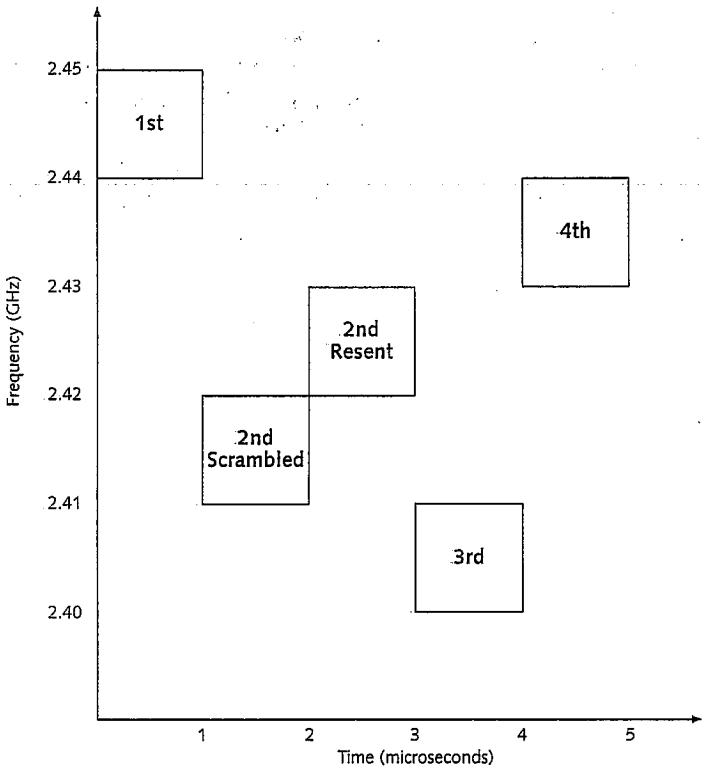

Figure 4-6 FHSS error correction

transmissions to hop through at least 75 channels (before repeating) with each channel 1 MHz in frequency. The dwell time could not be more than 400 milliseconds on one frequency each 30 seconds at a maximum output of 1 watt. In mid-2000 the FCC amended some of the 2.4 GHz restrictions. The number of required hops was reduced to 15 and the power output was decreased to 125 milliwatts (mW) while the channel size or bandwidth was increased to 5 MHz.

Due to speed limitations FHSS is not widely implemented in today's WLAN systems. Bluetooth technology does use FHSS. Bluetooth divides the 2.4 GHz frequency into 79 different frequencies spaced 1 GHz apart. In one second of Bluetooth transmission the frequency will change 1,600 times, or once every 625 μs.

Direct Sequence Spread Spectrum (DSSS)

The other type of spread spectrum technology is **direct sequence spread spectrum (DSSS)**. DSSS uses an expanded redundant code to transmit each data bit. Figure 4-7 shows three original data bits to be transmitted: 1, 0, and 1 (top of figure). However, instead of transmitting these three bits, a different sequence of bits is substituted as seen in the middle line of the figure. This bit pattern is called the **chipping code** (sometimes also called the

Barker code). In this figure the chipping code is 1001. That means instead of sending a 1 bit, the chipping code of a 1 (1001) is substituted instead. The inverse of that binary code (0110) is substituted for the 0 data bit to be transmitted. Instead of sending a 0 bit, the chipping code of a 0 (0110) is sent instead.

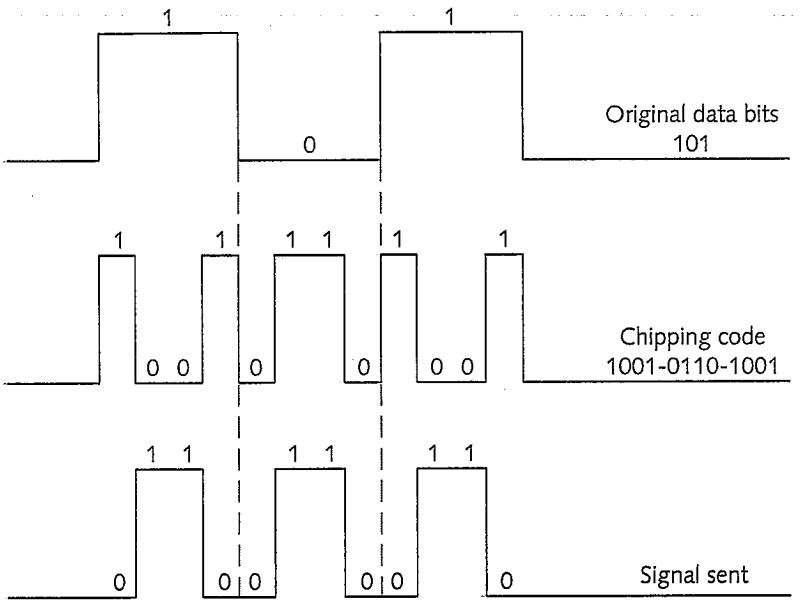

Figure 4-7 Direct sequence spread spectrum (DSSS) transmission

The term "chipping code" is used because a single radio bit is commonly referred to as a "chip."

The last step is to add the original data bit to the chipping code, as seen in the bottom line of Figure 4-7, to create the signal that is actually sent. The adding of the chipping code and the value to add to the chipping code is accomplished by the Boolean operation of exclusive or (XOR). For example, if a 1 bit is to be transmitted, then a 1 is added to each bit of the chipping code.

Bit to be transmitted is 1				
Chipping code for 1:	1	0	0	1
Value to add to chipping code:	1	1	1	1
Signal sent	0	1	1	0

If a 0 data bit is to be transmitted, then a 0 is added to each bit of the chipping code:

Bit to be transmitted is 0				
Chipping code for 0:	0	1	1	0
Value to add to chipping code:	0	0	0	0
Signal sent	0	1	1	0

Although it may appear that 0-1-1-0 would be sent for all 0 and 1 bits to be transmitted, that is not the case. When the bits to be transmitted are consecutive 1 bits, an extra 0 is placed between them in the chipping code so that it becomes [1001][0][1001], which would result in a transmitted code of [0-1-1-0]-[1]-[0-1-1-0].

There are several advantages to using DSSS with a chipping code:

- *Error correction*—If there is interference in the transmission when sending a single bit, it would have to be resent, which takes time (albeit very little time unless there is a large amount of interference). However, if there is interference when sending the chipping code, advanced statistical techniques embedded in the receiving device can recover the original data without the need for retransmission.
- *Less interference on other systems*—If the DSSS signal is picked up by an unintended device, the signal will appear as low-powered noise and will be ignored.
- *Shared frequency bandwidth*—Use of the chipping code makes it possible to share the frequency band with similar devices. Known as **co-location**, this is achieved by assigning each device a unique chipping code in order that all the transmissions can use the same frequency yet remain separate. The transmission of one network would only appear as noise to another network and be filtered out.
- *Security*—If an eavesdropper picked up the signal of the original data bit it would be a simple task to read the message. If a chipping code were used that would make reading the message more difficult if not impossible.

As with FHSS, the FCC has also placed restrictions on DSSS. The maximum output level of power is 1 watt. Also, the length of the chipping code must be at least 10 bits (in the example above the chipping code is only 4 bits long).

Orthogonal Frequency Division Multiplexing (OFDM)

In Chapter 3 you learned that ground-level objects in the path of radio transmissions do not necessarily completely block a radio signal but can cause refraction or diffraction, which results in some signals arriving later than other signals that can move in a straight line without obstructions. This is known as multipath distortion. The result is that the receiving device gets the signal from several different directions and at different times. Even though the receiving device may have already received the straight line signal, it must still wait until all reflections are received before it can do anything. Consider for a moment the analogy of a school crossing guard at a local elementary school. The crossing guard stops all automobile

traffic while children cross the street. Even though one student may sprint across the street and arrive well ahead of all other children, nevertheless all traffic is held up by the crossing guard until the slowest child drags across the street.

This is similar to the problem that WLANs face. With multipath distortion, the RF signals bounce off walls and furniture and are delayed reaching the receiver. The receiving device must wait until all reflections are received before it can transmit. If it does not, then some of the delayed signal may spread into its next transmission. Increasing the speed of the WLAN only causes longer delays in waiting for reflections. Because a device must wait to transmit until it receives the last reflected signal, this in effect puts a ceiling limit on the overall speed of the WLAN. With current technology this ceiling would be between 10 and 20 Mbps.

One solution to this problem is a **multiplexing** technique, or sending multiple signals at the same time, known as **orthogonal frequency division multiplexing (OFDM)**. Although OFDM was modified specifically for indoor wireless use, its history dates back to the mid-1960s and is used today in European digital TV and audio transmission. Its primary role is to split a high-speed digital signal into several slower signals running in parallel.

OFDM is also the technology behind consumer-based Digital Subscriber Line (DSL) service, which provides home Internet access over standard telephone lines.

Instead of sending one long stream of data across a single channel, OFDM sends the transmission in parallel across several lower-speed channels. The sending device breaks the transmission down into pieces and then sends it over the channels in parallel. The receiving device combines the signals received from the individual channels to recreate the transmission. By using parallel transmission channels, OFDM can combine several lower-speed channels to send data at a higher speed. This is illustrated in Figure 4-8.

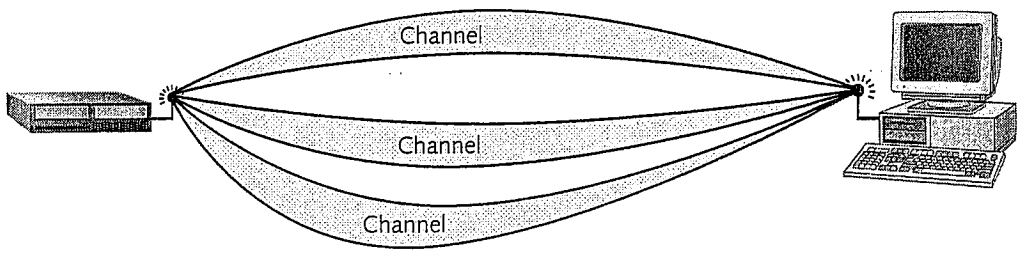

Figure 4-8 Multiple channels

Although it may seem contradictory, OFDM *increases* throughput by sending the data more *slowly*. Consider for a moment a single-lane toll road that handles automobile traffic and has one toll booth. This road backs up every morning and afternoon during rush hour. The best solution to this bottleneck is not to raise the speed limit of cars going through the toll booth. Although that would slightly increase the number of cars getting through, the traffic flow is

still limited by all of the cars waiting at a single toll booth. Rather, the best solution is to add multiple toll booths on parallel lanes. And, if flashing signs direct cars to empty toll booths, that would speed the process even more. This in effect is OFDM: multiple transmission paths with traffic directed to the appropriate lanes.

OFDM avoids problems caused by multipath distortion by sending the message slowly enough that any delayed copies (refracted or diffracted signals) are late by a much smaller amount of time than a standard transmission. This means that the network does not have to wait long for the reflections. And because the transmissions are sent in parallel, the total throughput is actually increased. That is, in a given unit of time the total amount of data sent in parallel is greater and time spent waiting for reflections is less with OFDM than with a single channel transmission. This amounts to a higher throughput and a faster WLAN. OFDM is illustrated in Figure 4-9. OFDM is used in IEEE 802.11a networks.

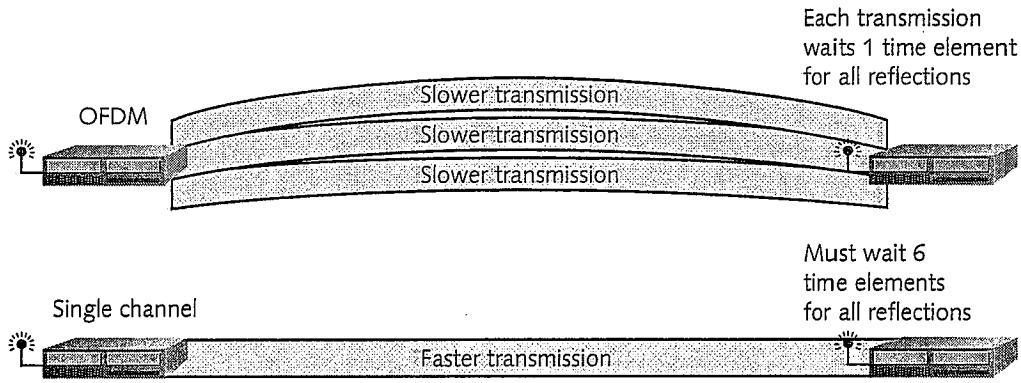

Figure 4-9 Orthogonal frequency division multiplexing (OFDM) vs. single-channel transmissions

Comparison of Wireless Modulation Schemes

Each modulation scheme—FHSS, DSSS, and OFDM—has strengths and weaknesses. However, when compared side-by-side, the schemes that offer the highest throughput are preferred for WLANs.

Even though FHSS transmissions are less prone to interference from outside signals than DSSS, and WLAN systems that use FHSS have the potential for a higher number of co-location units than DSSS (as many as 12 to 15 co-located FHSS can share frequency in a given area as opposed to only three DSSS systems), the determining factor in which type radio transmission is preferred comes down to speed. DSSS has the potential for greater transmission speeds over FHSS. FHSS transmits a short burst on one frequency that is typically only 1 MHz. On the other hand, DSSS transmits on a frequency that is 22 MHz wide. The amount of data that a channel can send and receive, known as **throughput**, is much greater in DSSS than in FHSS. DSSS has a potential bandwidth of up to 11 Mbps

whereas FHSS can only transmit at a maximum of 3 Mbps. Because of its higher throughput, DSSS systems are preferred over FHSS for 802.11b WLANs.

However, the dramatically increased throughput that can be achieved by OFDM has placed it as the leader today among the modulation schemes. Because it can support speeds of over 100 Mbps for 802.11a WLANs and over 54 Mbps for 802.11g WLANs, OFDM is the preferred modulation technique for WLANs at this writing.

IEEE 802.11 Physical Layer Standards

IEEE wireless standards follow the OSI model, with some modifications. IEEE has divided the Data Link layer into two sublayers, as shown in Figure 4-10. The sublayers are the Logical Link Control (LLC) sublayer, which provides a common interface, reliability, and flow control, and the Media Access Control (MAC) sublayer, which appends physical addresses to the frame. The reason for this change was to allow higher-level protocols, such as those operating in the Network layer, to interact with Data Link layer protocols without regard for Physical layer specifications.

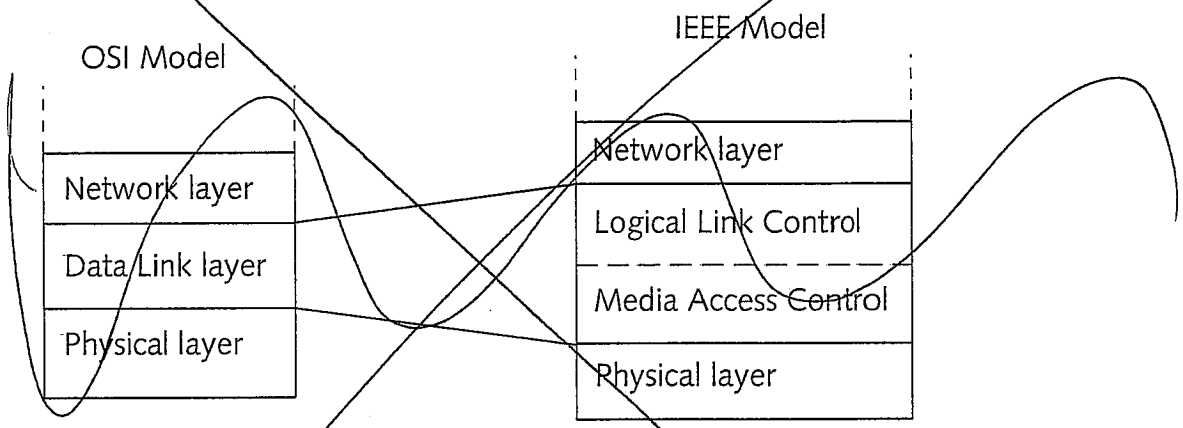

Figure 4-10 Data Link sublayers

Likewise, the IEEE has subdivided the Physical layer (sometimes abbreviated PHY) for WLANs into two sublayers, as seen in Figure 4-11. The **Physical Medium Dependent (PMD)** sublayer makes up the standards for both the characteristics of the wireless medium (such as DSSS or FHSS) and defines the method for transmitting and receiving data through that medium. The second sublayer of the PHY layer is the **Physical Layer Convergence Procedure (PLCP)** sublayer. The PLCP sublayer performs two basic functions: it reformats the data received from the MAC layer (when transmitting) into a frame that the PMD sublayer can transmit, as seen in Figure 4-12, and it "listens" to the medium to determine when the data can be sent.