

Bonus Web Chapter 3

**RADIO
FREQUENCY**

This Bonus Web Chapter provides the average reader with a crash course in the basics of radio frequency (RF) terminology and hardware. A basic understanding of the fundamental concepts and theories in RF electronics is an invaluable asset to the wireless hacker. At the end of the day, if your hardware isn't working, then no amount of clever software is going to help.

RF Terminology

To start off, let's talk about what is meant by *radio frequency* or *RF*. Technically speaking, RF refers to any signal between the frequencies of 3 Hz and 300 GHz. More practically, however, RF refers to signals from about 3 MHz up to 300 GHz. Signals that fall into this range of frequencies are capable of traveling through space in the form of electromagnetic waves. The distance over which these signals can travel depends on factors such as the signal's frequency and atmospheric conditions.

Communications Systems

The history of wireless communications goes back to the late 1800s when a German physicist by the name of Heinrich Rudolf Hertz first discovered the existence of electromagnetic waves. This discovery marked the creation of the first radio. Although Hertz's radio was very primitive, it established that a signal could be generated at one location and detected at another location without the use of wires. Technology later advanced to the point where Morse code could be transmitted using radio waves rather than relying on telegraph wires. Wireless communication then progressed to the transmission of human voice and audio using radio waves, and today high-speed data communications over wireless links are used every day.

Components of a Communications System

Modern communication systems are generally constructed using the same set of fundamental components. Although the designs have changed over the years, the basic components are very similar to those used for the early radios. Figure 1 shows a block diagram illustrating these basic components as implemented in both a traditional analog (voice) communications system and a typical 802.11 wireless communications system (or radio). Both systems contain largely the same components for the RF front-end and transceiver. The primary differences are in the format of the incoming and outgoing data and the components that interface the data source to the transceiver as designated by the dashed boxes surrounding these components in the figure.

The data source is the component that is generating the information to be transmitted and received by the system. For an analog radio, this could be either a microphone in the case of a communications radio or music in the case of a broadcast radio station. For a digital communications system, the data source is any type of digital bitstream. Of particular interest for readers of this book is the bitstream originating from the bottom level of the TCP/IP stack where the raw data is passed to the physical link layer.

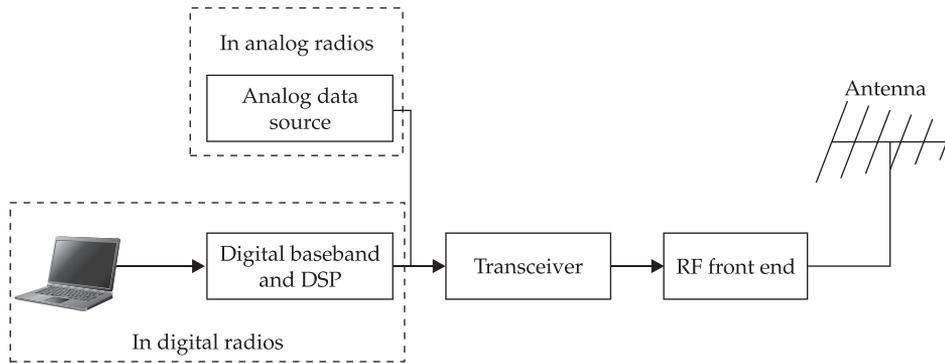


Figure 1 Block diagram of basic communications system

For digital radios, the next component of the radio is the baseband processing. This is where the digital bitstream coming from the data source is converted into an analog *baseband* signal through a process called *modulation*. (The process of modulation is not the same thing as a standard analog to digital conversion. There are various techniques for generating the modulated baseband signal that will be discussed later in the section on modulation.) Now that the data has been converted into an analog signal, the rest of the signal path becomes very similar to that used in more traditional radios. The baseband analog signal is typically the lowest frequency signal in the radio and is at too low a frequency for RF transmission, but this issue is taken care of in the transceiver.

The transceiver handles the process of converting the low-frequency baseband signal into a higher-frequency RF signal through a process called *upconversion*. Within the transceiver, an RF carrier signal is generated at the frequency that will be used for the final RF signal. This RF carrier is then combined with the baseband signal to upconvert the low-frequency baseband to the higher RF carrier frequency. Figure 2A shows both the low-frequency baseband signal and the RF carrier signal that are used in the upconversion process. Figure 2B shows the result of an ideal upconversion where the modulated RF signal is identical to the original baseband signal; except, it is now centered at a much higher frequency. In addition to upconverting outgoing signals, the transceiver also downconverts incoming RF signals to low-frequency baseband signals. The downconversion process is the inverse of the upconversion process.

Although the RF signal exiting the transceiver is now at a suitable frequency for wireless transmission, it is still too weak to travel over any appreciable distance. Likewise, any signal being received by the antenna is too weak to be sent directly to the transceiver. The RF front-end serves two functions: It amplifies signals coming from the transceiver to a power level suitable for transmission, and it amplifies weak signals coming from the antenna to a level that can be detected by the transceiver. The quality and performance of the RF front-end is what determines a radio's overall RF performance. Specifications such

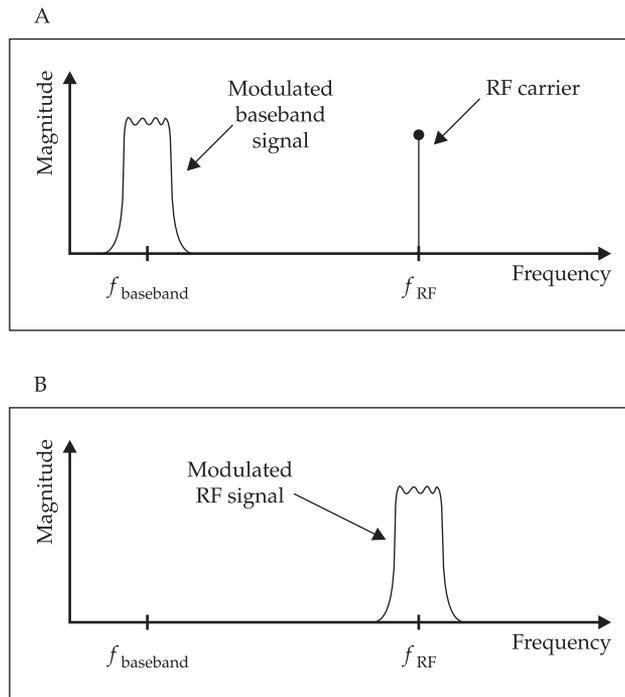


Figure 2 The process of upconverting a modulated baseband signal into a modulated RF signal

as output power and receiver sensitivity are directly determined by the front-end components.

The last component in the radio is the antenna itself, whose purpose is to interface the electric currents flowing in the radio's circuitry to electromagnetic waves in free space. Depending on the radio's intended application, the type of antenna used can vary widely. The quality and performance of the antenna used in a radio has as much impact on its total performance as that of the RF front-end. For this reason, it is important to understand how to properly employ the type of antenna used in any particular application.

Radio Frequency Signals

Before getting into the higher-level aspects of RF communications, let's cover a couple of basic principles and theories. To begin, we'll discuss some of the fundamental properties of analog signals. This is important even for digital wireless communications because the majority of RF components are—and will remain for a long time— analog in nature.

The basic building block for all analog signals is a single sinusoidal tone. A *sinusoidal tone* is a signal whose amplitude variation is defined by the trigonometric sine function (typically, however, the cosine function is used when mathematically expressing a

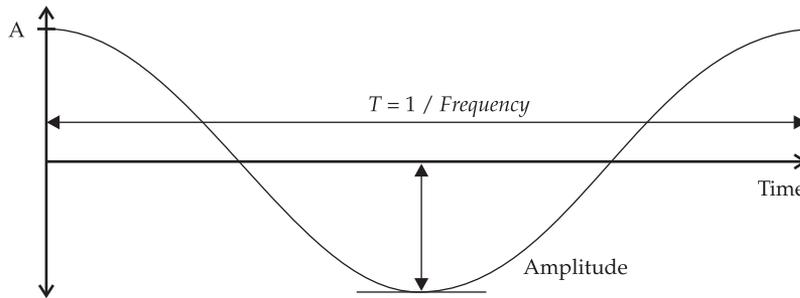


Figure 3 Time-domain waveform of a sinusoidal voltage

sinusoidal function in communications theory). Sinusoids are considered to be functions of time, and an example of a sinusoidal function is shown in Equation 1, where f is the sinusoidal frequency (in Hertz) and ϕ represents the phase shift of the sinusoid. Figure 3 illustrates a sinusoidal voltage in the time domain.

$$V(t) = A \cdot \cos(2\pi ft + \phi) \quad (\text{Eq. 1})$$

Note

Even though this equation is defined in terms of voltage, this doesn't mean sinusoids are restricted to voltages. A sinusoid can be defined in terms of any unit of measure.

Every sinusoid has three basic properties that completely describe its characteristics: amplitude, frequency, and phase. Of these three properties, amplitude and frequency are probably the easiest to understand. *Amplitude* refers to how large of an excursion is generated, or how strong a signal, and is represented by the A coefficient in Equation 1. The *frequency* of a sinusoidal signal refers to how many cycles of the repeating sine function occur per second. For example, a 2.4-GHz signal has 2,400,000,000 cycles of the sine function every second. The *phase* of a sinusoid is a somewhat elusive concept, but is most easily thought of as a shifting of the sinusoid's waveform along the x -axis (usually time). Figure 4 illustrates two sinusoids with a phase shift between them of 90 degrees.

There are two methods for analyzing any analog signal: time-domain analysis and frequency-domain analysis. *Time-domain analysis* is when a signal is plotted as a function of time, as shown in Figures 3 and 4. On the other hand, frequency-domain analysis is made possible through the use of the Fourier Transform, which allows a time-domain signal to be separated into its individual sinusoidal components. Figure 5 shows the RF signal envelope of an 802.11a signal in the time domain, and Figure 6 shows the same signal in the frequency domain. Frequency-domain analysis is a more intuitive method for examining and interpreting analog signals than time-domain analysis because it clearly shows all of the spectral components of a signal. This is advantageous because most modulations encode data in the frequency (spectral) domain.

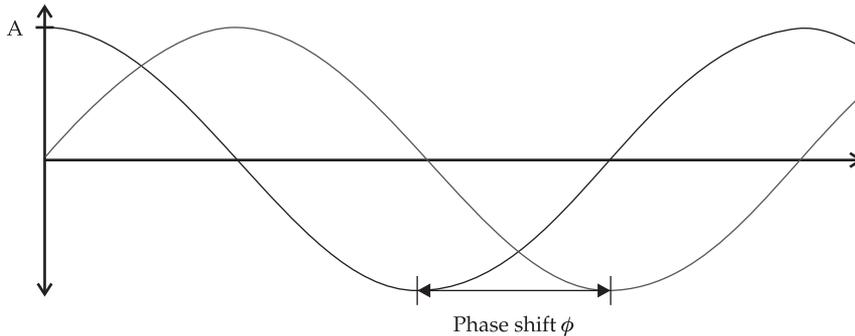


Figure 4 Phase shift between two sinusoids

One of the characteristics of analog signals is how much spectrum they occupy, or in other words, how wide they are when viewed in the frequency domain. This characteristic is referred to as a signal's *bandwidth*. For example, the 802.11a signal shown in Figure 6 has a bandwidth of approximately 16.6 MHz. Note that only the region of the signal with the higher power level is considered when calculating a signal's bandwidth; the remaining spectral content is noise and distortion byproducts of the main signal. Because the graph in Figure 6 is plotted in decibels (dB), the spectral content outside of the 16.6-MHz bandwidth is much weaker than the actual 16.6-MHz signal. Typically, the more data that a signal contains, the more bandwidth it will occupy. For example, a broadcast FM radio signal has a bandwidth of about 150 kHz (or 0.150 MHz), which is considerably smaller than the typical WLAN signal bandwidth of 16.6 MHz.

Electromagnetic Waves

The existence of electromagnetic waves is what makes transmission of RF signals over wireless links possible. *Electromagnetic waves* are time-varying electric and magnetic fields that are able to *propagate*, or travel, through space. The way in which electromagnetic waves propagate depends on several factors, the two most important being the frequency of the signal and the environment through which the wave is traveling.

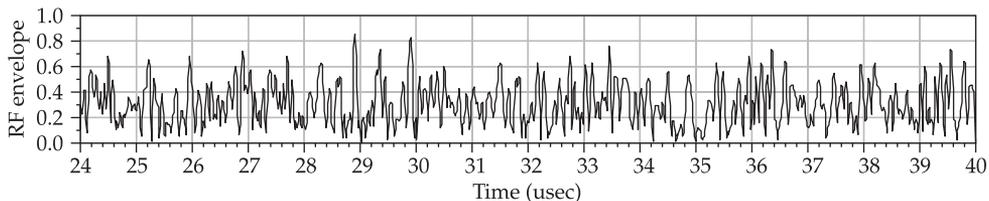


Figure 5 Time-domain plot of RF voltage (envelope)

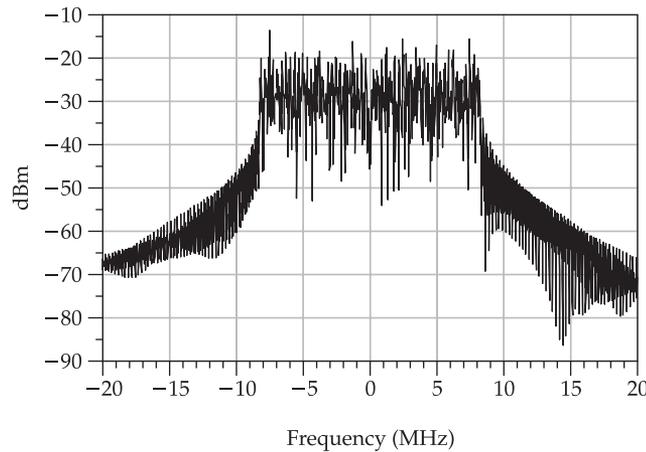


Figure 6 Frequency-domain plot of 802.11a 54-Mbit/sec signal

The frequency of the signal determines the wavelength of the electromagnetic wave. A signal's *wavelength* describes the amount of distance traveled by the signal between adjacent peaks in the signal and can be calculated by dividing the speed of light (for the medium through which the wave is traveling) by the frequency of the signal (as shown in Equation 2). Wavelength dictates many aspects of how a propagating electromagnetic wave will behave. Long wavelengths, on the order of 160–20 meters (corresponding to frequencies between 1.9 to 14 MHz), benefit from atmospheric phenomena that allow them to travel for great distances, oftentimes to opposite sides of the world. Shorter wavelengths (higher frequencies) tend to travel in straight lines and are blocked by obstructions such as walls and buildings. You can visualize this effect by thinking of an electromagnetic wave as a beam of light coming from a flashlight (in fact, light is a type of electromagnetic wave). This is commonly referred to as the *line-of-sight* characteristic of a signal.

$$\lambda = \frac{c}{f} = \frac{300 \cdot 10^6 \text{ meters/sec}}{f} \quad (\text{Eq. 2})$$

Another characteristic of electromagnetic waves is that they will reflect off of conductive surfaces. The ability of a surface to reflect an electromagnetic wave depends on its conductivity as well as its size as compared to a signal's wavelength. Since microwave signals (let's say above 1 GHz) have rather short wavelengths, they are easily reflected by metallic objects. Because of this, microwave signals are commonly affected by a phenomenon called *multipath interference*. Multipath interference occurs when multiple copies of a signal arrive at the same location but have taken different paths to get there. One way this can happen is by a signal being reflected off of multiple surfaces as it travels through space. Multipath interference is more common in indoor and urban environments and is a major problem

that severely affects the performance of wireless communication systems. This degradation in system performance is a result of the blurring together of the multiple signals generated by multipath interference. This blurring is caused by each signal arriving at the receiving antenna at slightly different times since each signal had to travel a slightly longer or shorter path than the others. Imagine trying to listen to a conversation and hearing multiple echoes of the same conversation at the same volume as the conversation itself.

Units of Measure

When working with electronic and RF components, there are several units of measure that always seem to come up. This section provides a brief description of each of these units so no one gets left behind in the following discussions.

Voltage

Voltage is a measure of the difference in electric potential between two conductors and is measured in volts (V). Electric potential can be thought of as the ability of an electric field to cause an electric current to flow through a conductor. Greater differences in electric potential (in other words, higher voltages) are capable of generating larger electric currents. A common analogy is to compare electric potential to the amount of pressure inside a water pipe. The higher the pressure, the more water can be forced through the pipe.

Current

Current is a measure of the number of electrons that flow through a conductor in a finite amount of time and is measured in amperes (or amps). One amp is approximately 6.241×10^{18} electrons per second. To continue with the prior analogy, the flow of electric current is analogous to the amount of water flowing through a pipe.

Power

Power is a measure of how much energy is absorbed or generated in a finite amount of time. Power is typically measured in watts and is equal to 1 Joule of energy transferred per second. In terms of electrical circuits, one watt is equal to the current flowing through a circuit (measured in amps) multiplied by the amount of voltage supplied to the circuit (measured in volts) as shown in Equation 3. In the field of RF electronics, pretty much everything is measured in terms of watts.

$$P = V \cdot I = \frac{V^2}{R} = I^2 \cdot R \quad (\text{Eq. 3})$$

Decibel

The *decibel* is a convenient method for expressing the ratio between two numbers and is indicated by the abbreviation dB. It is important to realize that the decibel is a representation of a ratio rather than of a single number. It is possible to express a specific measurement or value in terms of decibels, but its measurement has to be referenced to a unit. First, we'll look at expressing a regular ratio and then move on to the subject of referenced decibels.

There are two methods for converting a ratio into decibels and which method to use depends on the type of numbers being expressed by the ratio. If the ratio represents voltages or currents, then the correct conversion equation is Equation 4. If the ratio to be converted represents power, then the correct conversion equation is Equation 5. It is important to remember the difference between the methods, as using the wrong conversion will result in an incorrect answer that is always off by a factor of 2.

$$dB = 20 \cdot \log_{10} \left(\frac{value_1}{value_2} \right) \quad (\text{Eq. 4})$$

$$dB = 10 \cdot \log_{10} \left(\frac{value_1}{value_2} \right) \quad (\text{Eq. 5})$$

For someone familiar with electronics, the distinction between Equations 4 and 5 is probably clear. For the layperson, this is a possible point of great consternation. Luckily, it can be safely assumed that for the purposes of this text, Equation 5 is almost always the correct conversion method because RF and communications system engineers almost always think of things in terms of power. Gain is always thought of in terms of power gain. Loss is always thought of in terms of power loss. Signal strength is always thought of in terms of power.

For example, if someone states that a device has a power gain of 20 dB, this means that the power exiting the device is $10^{(20/10)}$ or 100 times greater than the power that entered the device. Or if a device has 3 dB of loss, it means that the power leaving the device is $10^{(3/10)}$ or 2 times smaller than the power entering the device.

One of the benefits of using decibels is that it simplifies many of the calculations necessary when working with RF systems. This is because the addition of two ratios once they have been converted into decibels is the same as multiplying the ratios themselves. An example of this is shown in Equations 6 and 7. Equation 6 shows that the gain (in decibels) of three series amplifiers is the sum of the three gains (in decibels). Equation 7 shows the same calculation, except that the gains are expressed in terms of regular (non-decibel) numbers. Since most quantities in RF are expressed in decibels to begin with, the method used in Equation 6 is typically the most straightforward.

$$Gain_{dB} = G_{1,dB} + G_{2,dB} + G_{3,dB} \quad (\text{Eq. 6})$$

$$Gain = G_1 \cdot G_2 \cdot G_3 \quad (\text{Eq. 7})$$

There are times when it is necessary to express a specific value in decibels. This is accomplished through the use of referenced decibels. The first step is to determine which unit the value is to be referenced to. Typically, this is just the unit scale used to measure the value. For example, if the value to be expressed is 4 volts, then the reference value is 1 volt. This is not always the case though. It is sometimes more convenient to use other values; for example, the reference value commonly used for RF power measurements is 1 milliwatt.

Unit	Reference Value	Example
dBm	1 milliwatt	100 mW = 100 mW / 1 mW = 100 = 20 dBm 1 uW = 1 uW / 1 mW = 1/1000 = -30 dBm
dBV	1 volt	2 Volts = 2 V / 1 V = 2 = 6 dBV
dBi	Gain of isotropic radiator	3 dB above isotropic gain = 3 dBi

Table 1 Examples of Referenced Decibel Values

The second step is to divide the value to be converted into dB by the reference value chosen. Notice that by dividing the two values, a ratio between the value and the reference unit has been created. This ratio is then converted into decibels just like before, except there is one more important step to take.

The reference value used in the conversion must be indicated in order for the result to be meaningful. This is done by adding a suffix letter to the dB unit designator. Table 1 contains a list of the most common types of referenced decibel units along with their reference values.

Efficiency

Efficiency is a measure of how well a device converts energy from one form into another. In the context of a wireless communications system, there are many components that perform various types of energy conversion. The efficiency with which these components are able to convert energy is an important factor for two main reasons: It determines how long the battery in your mobile wireless device (laptop or PDA) is going to last, as well as how hot the device gets while it is in the process of draining your battery.

In a perfect world, the efficiency of every component would be 100 percent. That is, all of the energy that goes into a device is perfectly converted to the desired energy type. An example of this would be an amplifier that perfectly converts the energy it is taking from your battery into RF energy that is delivered to the antenna. You can be assured, however, that this is not how things work in the real world. That energy being sucked from your battery isn't perfectly converted into the RF energy you want. In fact, RF components typically have efficiencies that are on the order of 10 percent to 30 percent. This means that for every watt of power your battery supplies, only 0.16 to 0.30 watts of RF power are actually produced. The remaining power goes into making things nice and warm.

Efficiency is typically expressed as a percentage and is defined as the amount of energy that leaves a system in the desired form divided by the total amount of energy entering the system. It can be applied to any component that converts one form of energy to another. The two most common RF devices to calculate the efficiencies of are amplifiers and antennas. An example of how to calculate the efficiency of an RF amplifier is shown in Equation 8. Simply divide the amount of RF power generated by the amplifier by the amount of DC power supplied to the amplifier and then multiply by 100.

$$\text{Efficiency}(\%) = 100 \cdot \frac{P_{RF}}{P_{DC}} \quad (\text{Eq. 8})$$

Gain and Loss

Gain and loss are measures of how signal power levels are affected by various components of an RF system. If the signal power exiting an RF component is greater than the signal power entering the component, that component can be said to have *gain*. Conversely, if the signal power exiting a component is lower than the signal power entering the component, it is said to have *loss*. The gain of a device is calculated by dividing the output power (in watts) by the input power (in watts) as shown in Equation 9. This ratio can then be converted into decibels by using Equation 5, shown earlier in the chapter. If the power levels are already expressed in decibels, then gain in decibels is calculated by simply subtracting the input power from the output power as in Equation 10. It is also interesting to note that gain and loss are the complement of each other. When expressed in decibels, a component with gain has a negative loss, and a component with loss has a negative gain.

$$\text{Gain} = \frac{P_{OUT}}{P_{IN}} = \frac{1}{\text{Loss}} \quad (\text{Eq. 9})$$

$$\text{Gain}_{dB} = P_{OUT,dBm} - P_{IN,dBm} = -\text{Loss}_{dB} \quad (\text{Eq. 10})$$

Modulation

Modulation is the process of embedding data that is to be transmitted by a communications system onto an analog carrier that will then be used to transport the data. This is done by converting the data to be transmitted from its native format (either analog or digital) into an analog signal that is suitable for effective RF transmission. The method by which this process is accomplished varies depending on the type of data being modulated as well as the type of medium through which the RF signal will be traveling.

When discussing modulation, there are several terms that describe the various signals used during the modulation process. The term *baseband* is used to refer to the lowest-frequency signal in an RF system. In a digital system, the baseband signal is typically the signal that is being passed back and forth between the Digital Signal Processor (DSP) and the transceiver. In analog modulations, the baseband signal is the actual data itself. The *RF carrier* is a single sinusoidal signal whose frequency is the same as the desired RF output signal. Once the baseband signal has been upconverted to the RF transmission frequency, it is then referred to as the *modulated RF carrier*.

The various types of modulations may be separated into two broad categories: analog and digital. The two predominant types of analog modulation are amplitude modulation and frequency modulation. There are numerous types of digital modulation, but those of interest to readers of this book are PSK, CCK, and QAM. While entire textbooks have been written on the subject of these modulations, it is possible to take a quick look at how they work and the basic characteristics of each.

Analog Modulation Techniques

Analog modulation is the process of converting an analog input signal into a signal that is suitable for RF transmission. It is performed by varying the amplitude and/or phase of an

RF carrier signal based on an analog input signal's time-varying properties. Analog modulation techniques are ideally suited for signals that are inherently analog in nature, such as the human voice and music. Although analog modulation can be used to transmit data, it is inefficient when compared to digital modulation techniques.

Pulse Modulation (PM) Starting with the most basic of all the modulation types is *pulse modulation*. This modulation is the type used by Benjamin Franklin for his telegraphy system. Pulse modulation is only capable of conveying either an “on” or an “off” state by switching the RF carrier signal on or off. While this modulation technique could be used to transmit binary data, it has the drawback of being extraordinarily inefficient for respectable data rates. Pulse modulation is still commonly used for low-data-rate telemetry signals and Morse code.

Amplitude Modulation (AM) This modulation is one of the most common analog modulation techniques. It is accomplished by varying the amplitude of an RF carrier signal based on the amplitude of an analog input signal. As the amplitude of the analog input signal varies in time, the amplitude of the RF signal is made proportional to the time-varying analog input signal amplitude. Figure 7 shows an example analog input signal, and Figure 8 shows the resulting modulated RF signal. The shape of the modulated RF signal is oftentimes referred to as the *signal envelope*, which describes the average power level of the RF signal as a function of time rather than the signal itself. Amplitude modulation is commonly used for long-distance voice communications, broadcast radio, and also in early analog cellular networks.

Frequency Modulation (FM) This is another classic modulation technique. In a frequency modulated signal, it is the frequency of the RF carrier signal that varies as a function of

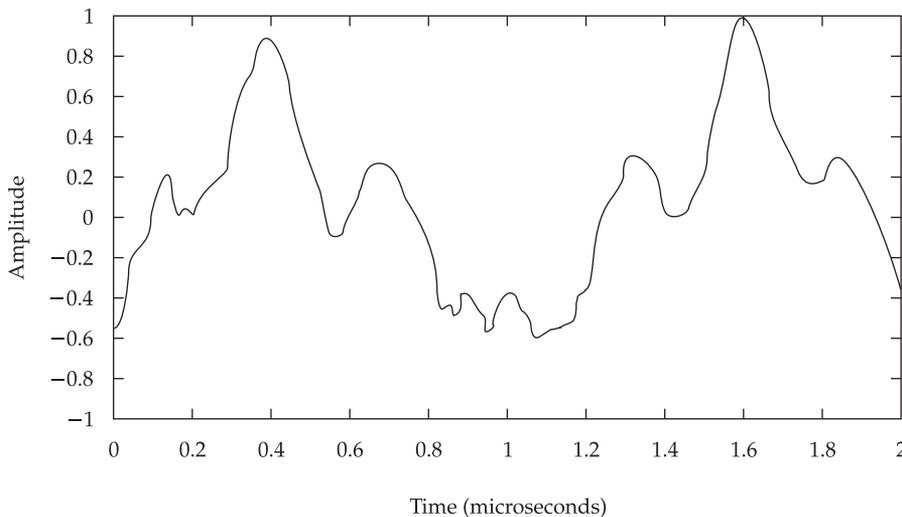


Figure 7 Baseband audio signal

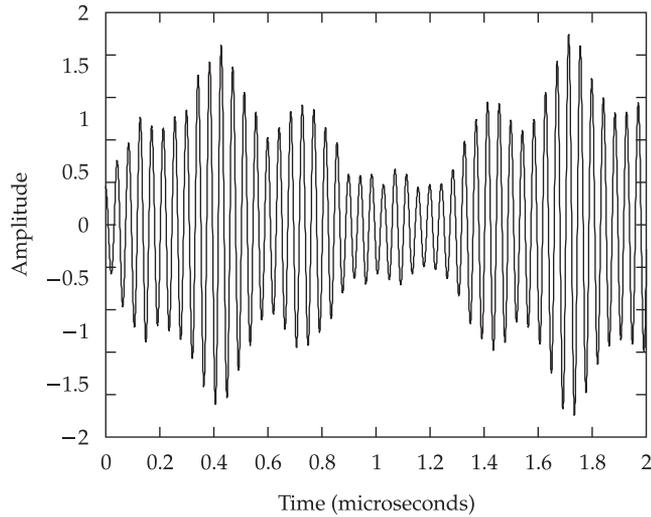


Figure 8 Resulting AM modulated RF signal

time. The amount of variation in the RF carrier’s frequency is determined by the amplitude of the input baseband signal. Figure 9 shows an example of an analog input signal, and Figure 10 shows the resulting frequency modulated RF carrier.

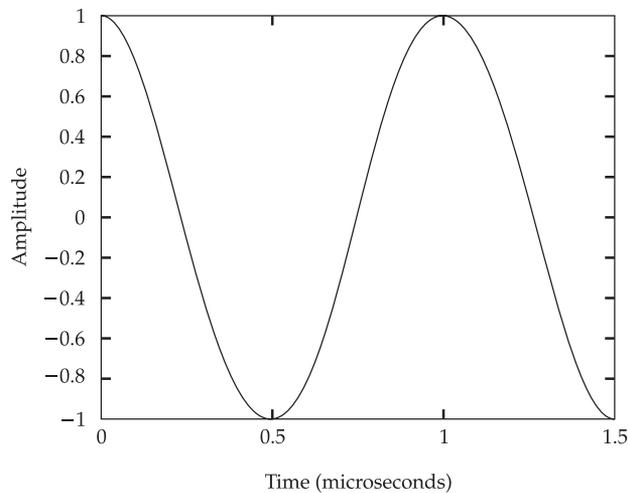


Figure 9 Baseband input signal

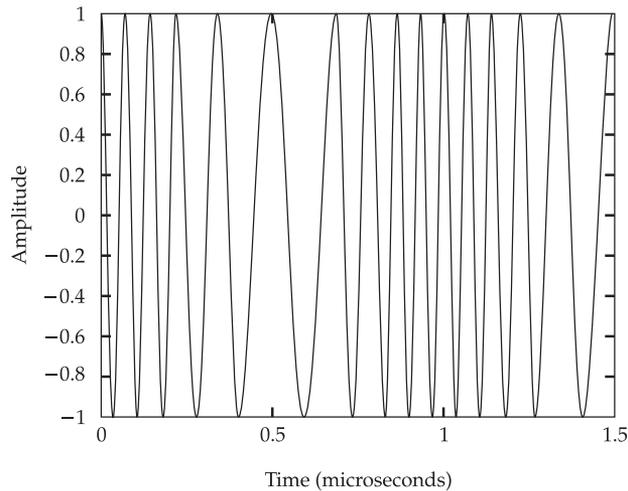


Figure 10 Resulting FM modulated RF signal

Digital Modulation Techniques

Digital modulation is the process of converting a digital bitstream into an analog signal suitable for RF transmission. This process is usually accomplished using digital signal processing due to the levels of complexity involved with modern modulations. A digital bitstream is input into the digital signal processor (DSP) and the analog output signal is generated using a digital-to-analog converter (DAC). It is worth noting that the digital data is not being converted directly to an analog signal. The DSP is analyzing the digital data and synthesizing an appropriate analog signal to represent the digital data based upon the type of modulation being implemented.

The first step performed by the DSP is to divide the digital bitstream into small equally sized groups of bits called *symbols*. The number of bits contained in, or represented by, a symbol depends on the type of modulation being used, but most modern modulation techniques can represent anywhere from 1 to 6 bits per symbol. These groups of bits are then used to form a sequence of symbols. Each of these symbols represents a unique analog output from the DAC. This process of separating the bitstream into symbols using a 16-QAM modulation is shown in the top portion of Figure 11.

In order to conveniently represent the analog output of the DAC in a graphical manner, a type of graph called a *constellation diagram* is often used. A constellation diagram graphically depicts the various magnitudes and phases of the generated analog signal. The points on a constellation diagram represent unique combinations of magnitude and phase that, in turn, represent the various symbols used in a particular modulation.

The DSP steps through the sequence of symbols one at a time and for each symbol synthesizes the corresponding analog signal. This is shown in Figure 11 by the

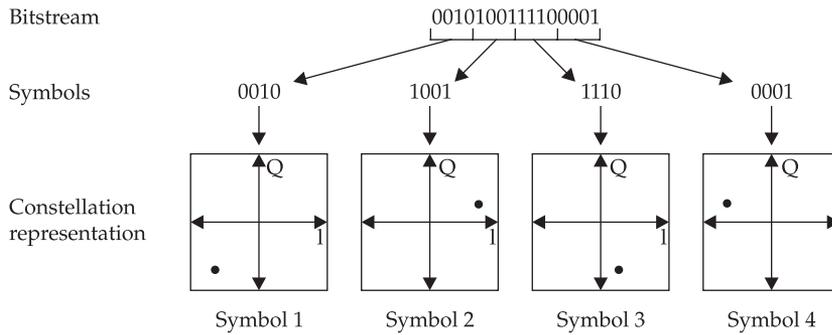


Figure 11 Process of dividing a digital bitstream into individual symbols using 16-QAM modulation

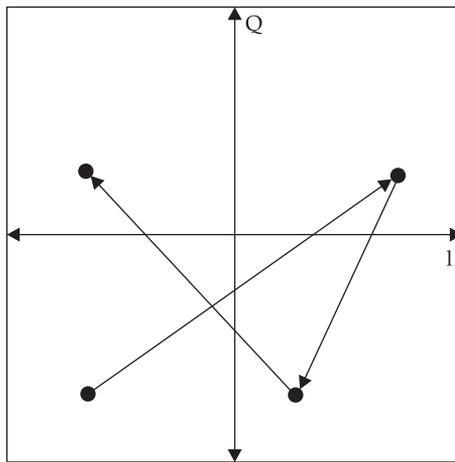


Figure 12 Constellation diagram showing the transition between symbols

constellation diagrams for each symbol. The transition between each symbol is shown in Figure 12. The rate at which the DSP steps through the sequence of symbols is called the *symbol rate*. This rate is typically governed by the wireless standard being implemented. Since the number of bits represented by each symbol is known, the raw throughput can be calculated by multiplying the number of bits represented by each symbol by the symbol rate.

Now that we've covered the fundamental aspects of digital modulations, let's take a look at the various types of digital modulation.

Phase Shift Keying We'll start our discussion of digital modulations with *phase shift keying (PSK)*. PSK is one of the simplest digital modulation techniques and is also one of the most

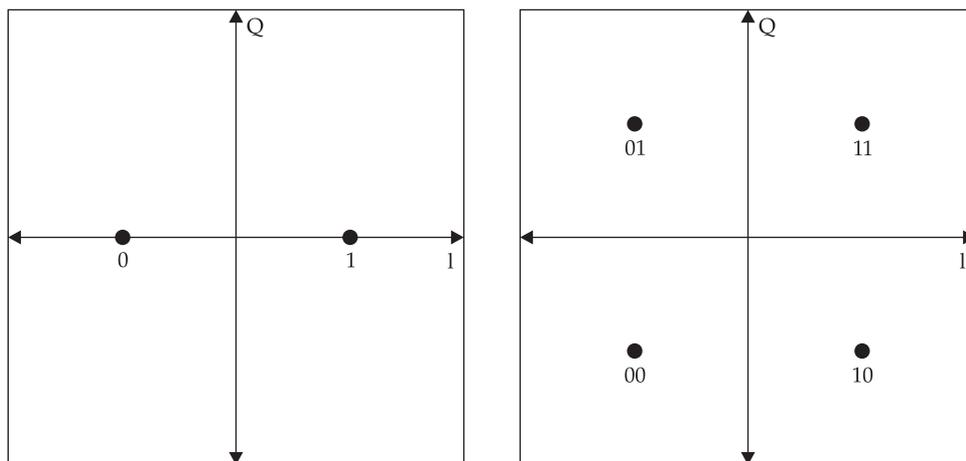


Figure 13 Constellation diagrams for BPSK (left) and QPSK (right)

robust. Simplicity and robustness do come at a price, however, as the data rate achievable by a PSK signal is rather low compared to other modulation techniques.

In a PSK-modulated signal, the phase of an RF carrier is varied among specific phases depending on the symbol being represented. Two common types of PSK modulation are binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK). BPSK utilizes two discrete phase states, and QPSK utilizes four discrete phase states. Since QPSK can represent twice as many symbols (as it has twice as many phase states) as BPSK, QPSK is capable of twice the data rate of BPSK. Constellation diagrams are shown in Figure 13.

There is a variation of PSK called differential PSK that is often implemented in wireless communications. The basic concept of DPSK is the same as in PSK except that rather than having each phase state represent a particular symbol, the transition between phases is used to represent each symbol. This reduces the amount of complexity required in the receiver's DSP to demodulate a signal. Table 2 shows a list of the absolute phases used in QPSK to represent each symbol, as compared to the amount of relative phase shift used in DQPSK to represent the same symbol.

Symbol	QPSK (Absolute Phase)	DQPSK (Phase Change)
00	-135	0
01	+135	+90
11	+45	+180
10	-45	-90

Table 2 Different Symbol Representations of QPSK and DQPSK

Complementary Code Keying (CCK) This is a modulation technique that utilizes spread-spectrum techniques coupled with the unique mathematical properties of complementary sequences to achieve higher data rates than ordinarily possible with plain spread-spectrum communications. The complementary sequences used in CCK modulation change the manner in which the symbols used in the modulation represent the data as compared to a regular spread-spectrum system. The mathematical properties associated with this process allow a CCK signal to be transmitted at the same symbol rate as a conventional spread-spectrum signal but with a much higher actual data rate. However, CCK is of less interest these days since it is largely being phased out in favor of OFDM-based systems.

The primary application of CCK modulation was in the 802.11b standard for the 5.5 and 11 Mbit/sec data rates. It was chosen because it allows for higher data rates while still using spread-spectrum DQPSK modulation of the lower speed 1 and 2 Mbit/sec 802.11 legacy standard. This allowed 802.11b networks to achieve faster data rates while still being compatible with older 802.11 legacy networks.

Quadrature Amplitude Modulation (QAM) This technique is a complex digital modulation capable of extremely high data rates. These high data rates are possible because of the large number of possible symbols that can be created using this modulation technique. There are various types of QAM, but the two most common are 16-QAM and 64-QAM, each of which is named after the number of symbols used in the modulation. Each symbol in a 16-QAM modulation represents 4 bits, and each symbol in a 64-QAM modulation represents 6 bits.

Symbols are constructed by varying both the magnitude and phase of the baseband signal. Each unique amplitude and phase combination represents a symbol. In most QAM signals, when these symbols are plotted on a constellation diagram, they are visible as a rectangular grid. Figure 14 shows the constellation diagrams for both a 16-QAM signal and a 64-QAM signal.

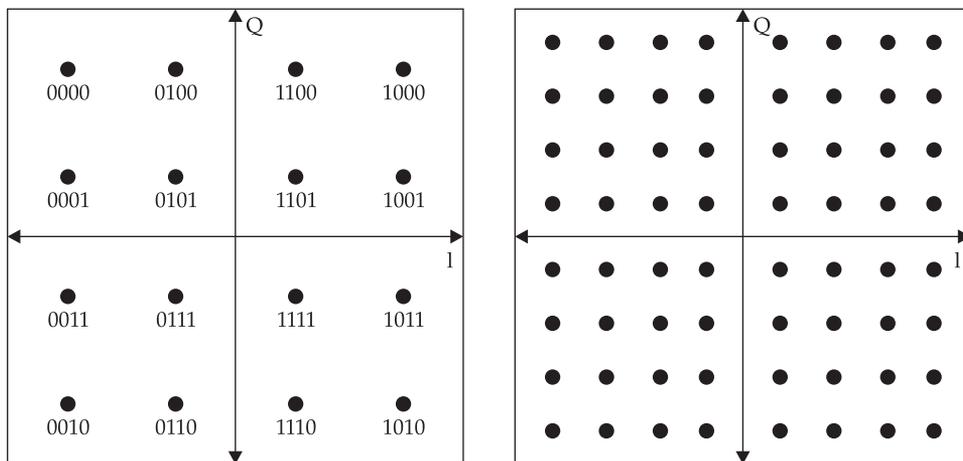


Figure 14 Constellation diagrams for 16-QAM and 64-QAM signals

Spread Spectrum and Multiplexing

Spread spectrum and multiplexing are two methods for sharing a fixed amount of bandwidth between multiple users. These techniques are utilized because there is only a certain amount of available RF spectrum. In fact, the commercial communications bands are quite small compared to the number of users competing for the spectrum. The techniques used to help alleviate this problem have undergone continuous development and revision. This section will cover the most prevalent of these techniques today.

Spread Spectrum

The concept of spread-spectrum communications was originally developed as a means for the obfuscation (or hiding) and scrambling of a communications signal. Early development was predominately related to the application of this technique toward military communications.

Spread spectrum operates by taking an ordinary communication signal and then spreading it across a much wider bandwidth than that occupied by the original signal. It is from this spreading process that the technique derives its name. There are two unique characteristics of a signal once it has been spread.

First, the spreading process spreads the power level of the signal over a wider range of frequencies than it initially occupied. This reduces the amount of signal power present at any one particular frequency, but it does not change the total amount of power present in the entire signal. If the spreading is wide enough, the signal can actually seem to “disappear” into the noise, which has merit in military communications because once a signal falls below the noise floor, it is very difficult to even detect its presence.

Second, it is virtually impossible to recover the original signal without knowing exactly how it was spread to begin with. This means that even if someone is able to detect the communications signal, they won't be able to extract any data from it. However, if the original spreading technique is known, then a spread-spectrum signal is very easy to detect and unspread.

Even though they are beneficial for other reasons, these same properties are what make spread-spectrum techniques appealing for wireless communications. Now that you know the basic ideas behind spread spectrum, let's take a look at two of the prevalent spread-spectrum techniques.

Frequency Hopping Spread Spectrum (FHSS) This technique operates by rapidly changing the frequency at which a communications signal is being transmitted. Because the transmission frequency is changing at a rapid rate, the signal is effectively spread over a greater bandwidth. In order to successfully receive a signal that has been transmitted using FHSS, the frequency that a receiver is listening to has to move in tandem with the transmitter. In order for the receiver to successfully track the transmitter, it has to know the sequence of frequencies that the transmitter will be using, the amount of time that the transmitter will use each frequency, and the current location of the transmitter in the sequence of frequencies. The most common commercial application of Frequency Hopping Spread Spectrum is the Bluetooth wireless standard.

Direct Sequence Spread Spectrum (DSSS) This is the most commonly used spread-spectrum technique. DSSS works by combining an ordinary communications signal with pseudorandom noise in the spreading process. The resulting signal appears to be random noise, but when the same pseudorandom noise is used to despread the signal, the original signal is extracted.

The core of DSSS is the pseudorandom noise used in the spreading and despreading process. This noise is generated from a sequence of pseudorandom bits called a *PN sequence*. The key characteristic of the PN sequence is that it is not a truly random sequence and is, in fact, completely deterministic. A pseudorandom algorithm is used to generate the PN sequence, and due to the nature of any algorithm, if the same starting condition is employed, the algorithm will always generate the same output. This means that a receiver can generate the exact same noise signal used by the transmitter if it knows the algorithm and initial condition used. Without this knowledge, however, the pseudorandom noise generated by the PN sequence will appear to be random.

One of the useful characteristics of DSSS is that without the correct despreading PN sequence, the signal appears as random noise. Taking this one step further, if multiple DSSS signals are transmitted in the same communications channel but each of them uses different PN sequences, then the resulting signal will still appear to be random noise. Now, this is where the magic begins to happen. Let's say there are four different DSSS signals that are all transmitted at the same frequency but with different PN sequences. Before despreading, the combined signal still appears like random noise, but if a PN sequence matching the one used to spread one of the original four signals is applied to the combined received signal, then the signal originally spread with that PN sequence will "pop" out of the noise. This is true for each of the original four signals. If the corresponding PN sequence is used, that signal will be extracted from the received signal. This property of DSSS effectively allows multiple users to share the same communications channel simultaneously.

DSSS is, in fact, a highly sophisticated technique with an elaborate mathematical foundation. To effectively exploit the properties just described, the PN sequences employed by each of the users must be generated in a manner that satisfies numerous mathematical requirements. The method by which these sequences are generated varies depending on the wireless standard being implemented. Code Division Multiple Access is probably one of the most famous applications of DSSS. Other systems that incorporate DSSS are 802.11 and the Global Positioning System (GPS). The exploitation of the unique properties of DSSS signals is at the core of these systems and this is what makes their operation possible.

Multiplexing

Multiplexing is the process of dividing a single communication channel into subcomponents so that the channel can be shared among numerous users and/or sources. The manner in which the channels are divided depends on the type of multiplexing being utilized. In the following sections, the most relevant multiplexing schemes are discussed.

Frequency Division Multiplexing (FDM) This is the simplest form of multiplexing. In this form of multiplexing, a separate frequency is used for every signal. Because any modulated

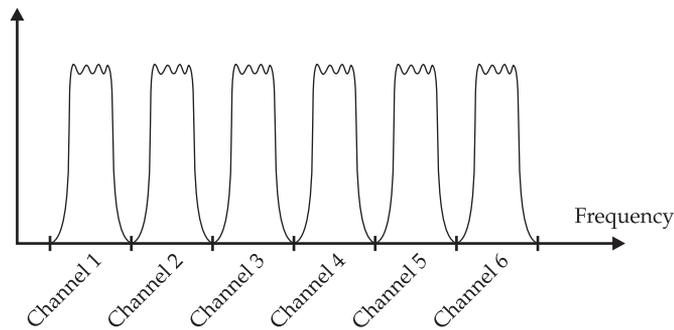


Figure 15 Using different channels for different signals

signal has a bandwidth associated with it, the available spectrum is often divided into channels with each channel having slightly more bandwidth than the bandwidth of the signal that is to fit inside the channel. Figure 15 illustrates the centering of RF signals inside different channels. These channels are then individually assigned to each user. One of the major problems with FDM is its inefficient usage of the frequency spectrum. Each user has their own dedicated channel, which means users can't share the same channel. Once the system runs out of available channels, additional users must wait until another user disconnects.

Time Division Multiple Access (TDMA) This technique multiplexes each channel in the temporal dimension by dividing the channel into a finite number of timeslots. Each timeslot is a short segment of time that is allocated to an individual user during which that user is allowed to transmit and receive data. Once every user has been given a chance to communicate with the system, the system starts cycling through the timeslots again. TDMA is depicted graphically in Figure 16. By multiplexing a single channel in the temporal dimension, multiple users are able to share the same amount of bandwidth. TDMA was the multiplexing approach used by the old 2G digital cellular networks.

Code Division Multiple Access (CDMA) This technique is a direct implementation of Direct Sequence Spread Spectrum. Each user on a CDMA system has their own unique PN sequence that they employ during the spreading process. All of the PN sequences being used on a particular channel are chosen such that they are statistically uncorrelated. The implications of being statistically uncorrelated are that when many users are transmitting on the same frequency, the sum of all these signals generates uncorrelated random noise. The basestation will separately despread each of the individual signals using the PN sequence associated with each user. CDMA also exploits the phenomena of process gain to elevate each user's signal out of wideband noise when the correct PN sequence is applied, allowing many users to share the same frequency channel without having to synchronize with each other.

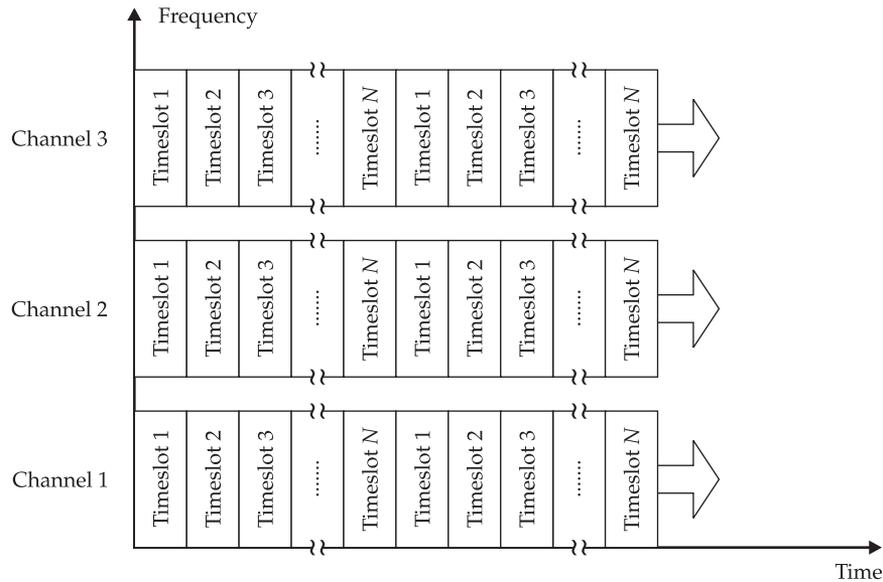


Figure 16 The temporal multiplexing scheme used in TDMA

Orthogonal Frequency Division Multiplexing (OFDM) This is, in its purest form, a technique for achieving higher throughput wireless communications than normally achievable by traditional modulation techniques. This is done by dividing the high-speed digital bitstream being transmitted into several lower-speed bitstreams operating in parallel. Each of these bitstreams is then modulated onto separate subcarriers using standard modulation techniques. The frequencies of the subcarriers are carefully chosen such that they are orthogonal with each other. As a result of the subcarriers being at orthogonal frequencies, crosstalk and interference amongst the various subcarriers is prevented.

A signal that has been generated using OFDM techniques has a higher spectral efficiency than a signal containing the same data but generated with traditional modulation. The primary benefit of OFDM is that it eliminates many of the problems associated with the high symbol rates required in order to achieve high data rates with traditional modulations. OFDM also operates at a much slower symbol rate than non-OFDM systems at comparable data rates. Because of the slower symbol rate, the *guard interval* (amount of blank or whitespace time) required between symbols is much less than the *symbol time* (how long each symbol is transmitted). This means that a greater percentage of the time is spent transmitting data rather than waiting as compared to non-OFDM systems. Since the data rate of each subcarrier is slower than the combined data rate, the symbol rates required are lower, which reduces the effects of multipath interference. This characteristic of OFDM allows for the high throughputs offered by 802.11a and 802.11g.

RF Hardware

The performance of the RF electronics used in modern communication radios largely determines the level of achievable performance. Fortunately, most RF electronics are integrated into commercially available wireless cards, which means that by selecting a quality high-performance wireless card, you can safely assume the components in the RF signal path have been carefully selected to deliver excellent performance. There are a few RF components, external to the wireless card, that are also of great importance in ensuring superior performance. This section discusses these components and provides the relevant information to allow the reader to better understand their operation.

Antennas

Quite simply stated, the antenna is what puts the signal into the air and gets it back out again. It does this by converting the electrical energy being delivered to the antenna into electromagnetic waves that are then able capable of traveling over long distances. Antennas are reciprocal in nature, which means that they are capable of both transmitting and receiving a signal equally well. This allows the same antenna to be used for both transmission and reception of RF signals.

When discussing different types of antennas, there are several characteristics that are used to describe an antenna's top-level behavior and performance. These characteristics are gain, radiation pattern, resonant frequency, polarization, and efficiency. The combination of these characteristics determines the types of applications in which an antenna can be effectively used. Conversely, if the desired application for an antenna is already known, these characteristics can be used to help select an appropriate antenna.

Antenna Gain and Radiation Pattern

Antenna gain is used to describe how well an antenna is able to focus RF energy in a particular direction and varies depending on the direction at which the antenna is being viewed. Antenna gain is expressed as a ratio (usually in decibels) that compares the antenna's performance to that of a known reference antenna. The most common reference antenna is an isotropic radiator, which is a purely theoretical antenna that radiates energy equally well in all directions. If an isotropic radiator is used as the reference antenna, the antenna gain is expressed in decibels using the dBi unit (the *i* stands for *isotropic*). Another very common reference antenna is a half-wave dipole antenna. If a half-wave dipole is used as the reference, the gain is expressed in decibels using the dBd unit (in this case, the *d* stands for *dipole*). These two methods for expressing antenna gain are related to each other and 0 dBd is equal to 2.15 dBi. As an example, consider an antenna that radiates four times as much power in a given direction than an isotropic radiator. The gain of this antenna would be equal to 6 dBi in that direction.

It is important to note that the total amount of RF energy radiated by the antenna cannot be greater than the amount of RF energy being delivered to the antenna. This means that if an antenna is able to focus more RF energy in one direction, then it must radiate less energy in other directions.

The manner in which a practical antenna's gain varies as a function of direction defines its *radiation pattern*. The radiation pattern of an antenna is commonly depicted graphically by plotting the antenna's gain as a function of angle on a polar plot. In order to accurately describe the radiation pattern of an antenna, two plots are required: *azimuth* and *elevation*. The azimuth radiation pattern describes how the gain of an antenna varies when it is viewed from different points on the horizon. An example of an azimuth radiation pattern is shown in Figure 17 for a simple directional antenna. From the plot, you can see that there is more gain (roughly 10 dBi in this case) in the boresight direction than in all other directions. Figure 18 shows the elevation radiation pattern for the same antenna as in Figure 17. The elevation radiation pattern describes the variation in gain when viewed from different angles (or elevations) above the antenna.

The *directivity* of an antenna refers to how well it is able to focus energy in one specific direction while preventing energy from being radiated in other directions. The greater an antenna's directivity, the higher its gain will be in its primary direction.

A term that is commonly used when working with antennas is *Effective Isotropic Radiated Power (EIRP)*. EIRP is used to describe how much power would have to be radiated by an isotropic radiator (a source that emits energy equally well in all directions) in order to achieve the same amount of power radiated in a particular direction by a transmitting antenna. As convoluted as that may sound, it is an easy quantity to calculate. Just take the amount of RF power being delivered to the antenna (in dBm) and add the gain (in dB) of the antenna, as shown in Equation 11:

$$EIRP_{dBm} = P_{RF(dBm)} + G_{Antenna(dB)} \quad (\text{Eq. 11})$$

Resonant Frequency

As with most RF components, the range of frequencies over which any one particular antenna will exhibit acceptable performance characteristics is limited. In the case of antennas, this is because the electrical size of the antenna components is critical to their performance. Electrical size refers to how large a physical dimension is as compared to a signal's wavelength. If you remember from Equation 2, a signal's wavelength is calculated based on a signal's frequency. This means that the electrical size of an object also changes as a function of frequency. As it turns out, an electrical size (or length) of $\lambda/4$ (one-fourth the wavelength) has a tendency to crop up repeatedly in the world of RF. In the case of antennas, it is common for many of the elements in an antenna to have an electrical size that is mathematically related to this $\lambda/4$ value (either directly or by some multiplicative factor). Since the wavelength of a signal changes as a function of frequency, while the physical size of an antenna remains constant, the elements of an antenna can only be properly sized at certain frequencies. When the elements are properly sized as compared to a signal's wavelength, the antenna is said to *resonate*, and the frequency at which this happens is referred to as the *resonant frequency*.

Typically, the resonant frequency of an antenna is where it is going to exhibit the best performance characteristics. As the frequency increases or decreases, antenna performance begins to change, usually for the worse. The frequencies at which antenna

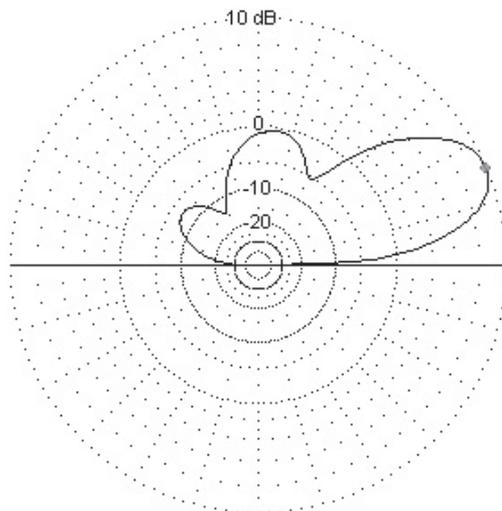


Figure 17 Azimuth radiation plot

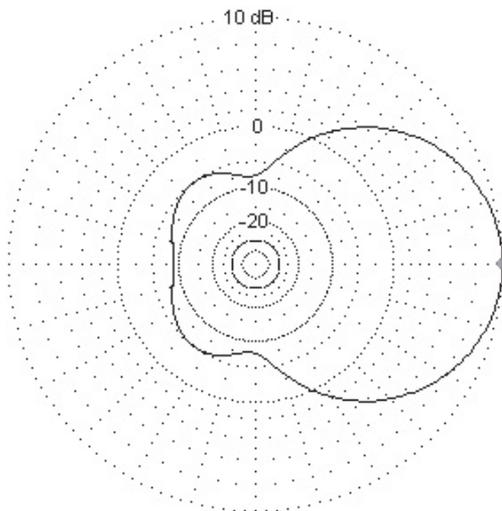


Figure 18 Elevation radiation plot

performance drops below acceptable limits define its bandwidth. The amount of bandwidth associated with an antenna depends on its design and construction.

Antenna Polarization

When an antenna is excited with an electric current, it generates electric and magnetic fields in a specific pattern around its radiating elements. The pattern in which these fields are generated depends on the design of the antenna and the environment in which the antenna is located. The orientation of these fields is what determines the polarization of the antenna.

In order for an antenna to be able to convert electromagnetic waves back into electric currents, the polarization of the electromagnetic waves must match the polarization of the antenna. If there is a partial mismatch between the polarizations, then only some of the electromagnetic energy will be converted into electric current. If the polarizations are perpendicular to each other, then theoretically speaking, none of the electromagnetic energy will be converted to electric currents. This means that in order for an antenna to effectively receive the signal transmitted by another antenna, the polarizations of both antennas must be the same.

Antenna polarizations are typically defined by the orientation of the electric (or E) field. If the electric field is oriented vertically, then the antenna is said to have *vertical polarization*. Conversely, if the electric field is oriented horizontally, the antenna is said to have *horizontal polarization*. There is another type of polarization called *elliptical polarization*, where the electric field rotates as the signal propagates through space. For any given type of wireless communication, typically only one type of polarization is used, so that all the antennas in the system have the same orientation and can effectively communicate with each other. Most commercial wireless applications utilize *vertical polarization*. This is why most WLAN devices always have their antennas pointed upward.

One last comment about polarization is that simply because a signal was transmitted with vertical polarization doesn't mean it will arrive at the receiver with that same polarization. As microwave signals reflect off of surfaces and travel through and/or around obstacles, the electric and magnetic fields can rotate. It is hard to predict when this sort of thing will occur, but it is important to keep in mind that it is possible. Because of this, adjusting the orientation of an antenna can sometimes improve signal strength. But as a general rule, it's a good idea to keep it oriented either vertically or horizontally.

Radiation Efficiency

Radiation efficiency is a metric for describing how "well" an antenna works. You could also refer to this as an antenna's "suck factor." All antennas are not created equal. Even if two antennas have similar radiation patterns, one will more than likely perform better than the other. There are many factors that contribute to an antenna's performance but common ones include the type of metal used for construction, dimensional accuracy in antenna components, and the antenna design itself. Technically speaking though, an antenna's efficiency is defined as the amount of electromagnetic energy generated by the antenna divided by the amount of RF energy delivered to the antenna.

It should not come as a surprise that most home-brew antennas have lower radiation efficiency than commercially available antennas of similar design. Determining an antenna's radiation efficiency is often a difficult task, even for the pros. For the average

person it is probably better to think of this in terms of a general “suck factor” than a mathematical quantity. If one antenna works better than the other, it probably sucks less.

Antenna Designs

Let’s now talk about some of the most common antenna designs that you are likely to encounter when working with wireless communications.

Omnidirectional Designs The *dipole* is probably the most widely used stock antenna in wireless hardware. The basic dipole design consists of a metal element one-half wavelength long that is symmetrically fed from the center. There are many methods for constructing this antenna depending on its application. The flexible rubber antennas found on wireless access points are dipole antennas. Also, the integrated antennas used in some USB 802.11 adapters are dipole antennas fabricated using planar PCB technology. As another example, the driven element on a Yagi antenna is, in fact, a dipole antenna.

Dipole antennas have a relatively omnidirectional azimuthal radiation pattern when the dipole element is oriented vertically (hence giving it vertical polarization); this means that the amount of signal radiated by the antenna is constant as you look at it from different points on the ground. The dipole antenna does not radiate much power in the upward or downward directions, which is why it is able to exhibit gain in the azimuth. The gain of an ideal dipole antenna is on the order of 2.15 dBi.

Monopole antennas are another type of omnidirectional antenna. They are constructed out of a vertically oriented element that is typically $1/4^{\text{th}}$ or $5/8^{\text{th}}$ s of a wavelength long. For a monopole antenna to be effective, the surface underneath the radiating element should be a flat conductive surface that is parallel to the ground. Monopole antennas have a constant gain when viewed from the azimuth that is higher than a dipole antenna. This is because a monopole antenna does not radiate any energy toward the ground. Because of this characteristic, a monopole antenna’s radiation pattern is generally considered to be desirable as compared to that of a dipole. Unfortunately, practical monopole antennas are difficult to realize because of the ground plane required.

Directional Antennas The *Yagi-Uda* antenna is named after the engineers who first developed it, although it is commonly referred to only as a “Yagi.” The Yagi antenna is an extremely prevalent directional antenna due to its relatively simple design and high gain. Yagi antennas are an array of metal rods (or elements) that are all oriented parallel to each other and lie in the same plane. The length and spacing of these elements determines the frequency band at which the antenna will operate, and the number of elements used determines the amount of gain it will have. The orientation of the individual antenna elements is what determines the polarization of a Yagi antenna. If the elements are oriented vertically, then the antenna will have vertical polarization.

The most ubiquitous example of a *parabolic* antenna is that of a satellite dish. Parabolic antennas make use of a parabolic reflecting surface (hence the name) to “catch” electromagnetic energy and direct (or focus) it toward a smaller antenna (typically called the *feed*). The benefit of a parabolic antenna is the extraordinarily large amount of gain achievable. But, of course, there is no such thing as a free lunch! In exchange for the high gain, parabolic antennas are highly directive and in turn must be precisely pointed toward

the antenna at the other end of the link. The positioning of parabolic reflectors can be tricky as they tend to be large, and in addition to catching radio waves, they also do a really good job at catching wind as well. Even with these drawbacks, parabolic antennas find extensive use in microwave and millimeter wave applications where high antenna gain is necessary to compensate for increased path loss over long link distances.

Antenna *arrays* are a method for increasing the effective gain of an antenna. Arrays are constructed by taking several antennas and mounting them near each other in a specific pattern and spacing. Although antenna arrays are more complex than stand-alone antennas, there are applications where the increased amount of gain makes an antenna array a viable solution.

Amplifiers

Amplification is the process of taking a weak signal and increasing its *amplitude* (or power). As a signal progresses through a communications system, the signal must be continuously amplified in order for the data contained within the signal to remain intact. Amplifiers are the components within communications systems whose sole purpose is to amplify a signal. While this may sound like a relatively simple task, the physical limitations of practical amplifiers often make it more of a challenge than you might guess. Because of these performance limitations, there are several different types of amplifiers used, depending on their location in the system.

Low Noise Amplifiers

Low noise amplifiers (LNA) could be described as hearing aids for a radio. The LNA is typically the very first amplifier that a signal will encounter once it is received by the antenna. Just as the human brain can't decipher what someone is saying if the background noise is too high, a receiver can't demodulate an RF signal if the amount of received noise is too high. Noise is everywhere in nature, and electronics are no exception to this.

The RF signal coming from an antenna has two major components: the desired RF signal and noise. The strength of the received RF signal varies depending on many factors including transmitted power level, distance from transmitter, type of antenna being used, and the type of environment between the transmitter and receiver. The amount of noise present in a microwave signal is dominated by thermal noise and is typically at a constant level. The amount noise that is present at the input of a receiver is referred to as the *noise floor* of the receiver.

A problem quickly arises as the amount of power contained within a received RF signal decreases: At some point, the RF signal power will fall below the noise floor of the receiver, and once this happens, the receiver can no longer detect the signal. In fact, the data contained within a signal is typically lost well before the signal disappears into the noise. The *signal to noise ratio (SNR)* of a signal describes how much stronger a signal is than the accompanying noise and is calculated as shown in Equations 12a and 12b:

$$SNR = \frac{P_{RF}}{P_{NOISE}} \quad (\text{Eq. 12a})$$

$$SNR_{dB} = P_{RF,dBm} - P_{NOISE,dBm} \quad (\text{Eq. 12b})$$

It is impossible for an amplifier to differentiate between an RF signal and a noise signal. For this reason, whenever the RF signal is amplified in the receiver, the noise signal is also amplified by the same amount. Every active component in an amplifier will also contribute an additional noise component to the signal. The end result of all this is a reduction in the signal to noise ratio of the received signal. The first components that a signal has to pass through once it comes from the antenna tend to dominate the degradation in SNR.

Low noise amplifiers are designed to contribute a very small amount of additional noise to the signal which they are amplifying. They are typically one of the very first components in the receive signal path. By providing a healthy amount of gain coupled with a minimal amount of noise, they are able to reduce the negative impact on SNR caused by the subsequent components in the receiver. The standard measurement of the quality of a LNA (and entire receivers) is called *noise figure*. The noise figure of an amplifier or receiver is expressed in dB and the smaller the number, the better.

Power Amplifiers

Power amplifiers (PA) are the last type of amplifier that a signal passes through on its way to the antenna during transmission. Once an RF signal reaches a certain power level, typically -10 dBm (100 μ W) to 0 dBm (1 mW), it becomes increasingly difficult to amplify it any further using regular amplifiers. Power amplifiers are specifically designed to amplify signals to the high power levels required before the signal reaches the antenna. The power amplifiers used in wireless LAN applications are capable of generating +18 dBm (63 mW) of clean (nondistorted) output power. Newer wireless standards, such as WiMax, require clean power levels of up to +24 dBm (250 mW). Power amplifiers used in very high power applications are capable of generating over +50 dBm (100 Watts) in a single chip that is smaller than your fingernail!

Just as the LNA determines most of the receive characteristics of a radio, the PA is the component that determines the transmit capabilities of a radio. A radio's transmit power is directly determined by the power amplifier inside it. Unlike LNAs, the characteristics of PAs that make them difficult to design and implement are not easily explained at a basic level. PAs have the characteristic of sounding deceptively simple, but are often tricky to design and implement.

Government Regulations

All wireless telecommunications make use of some portion of the electromagnetic spectrum. The electromagnetic spectrum consists of any signal whose frequency is between 3 kHz and 300 GHz. While the extreme low and high ends of this range are only used for highly specialized applications, the frequencies between 3 MHz and 40 GHz are used extensively for wireless communications. Even with such a vast range of frequencies available, there is fierce competition for access to this spectrum. Figure 19 contains a largely unreadable chart of all U.S. frequency allocations that illustrates just how much has been crammed into the RF spectrum. (A PDF version of this chart can be found at the NTIA Office of Spectrum Management website, www.ntia.doc.gov/osmhome/allochrt.pdf) Due to

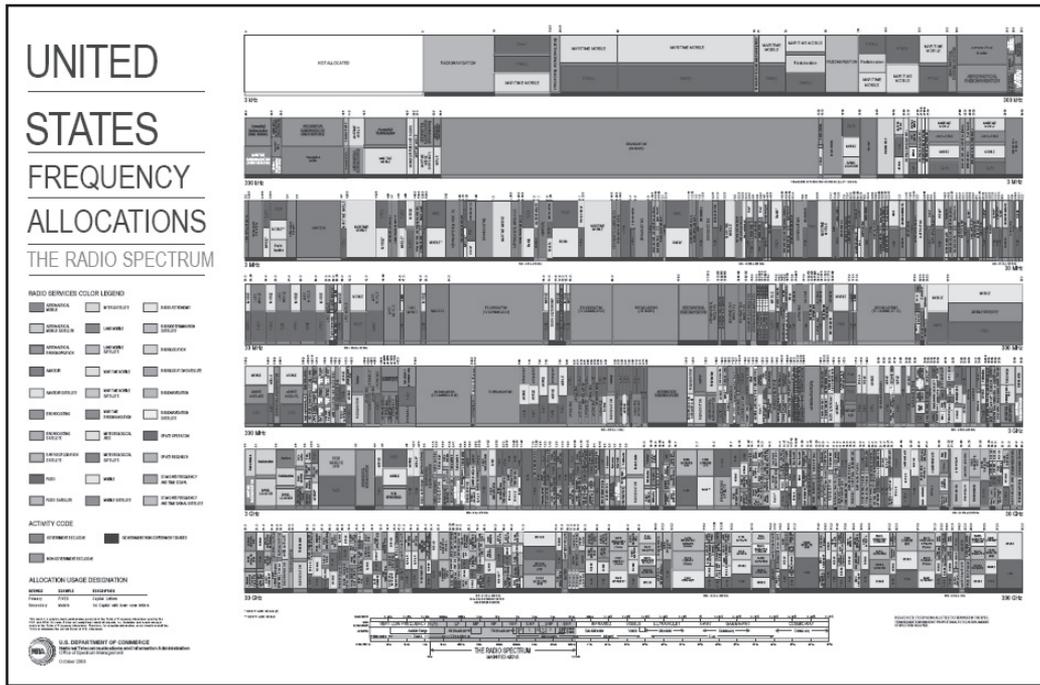


Figure 19 Graphical depiction of every frequency allocation in the United States (www.ntia.doc.gov/osmhome/allochrt.pdf)

the large amount of demand, governmental regulatory agencies have been commissioned to regulate the usage of the electromagnetic spectrum. Probably the most well known of these agencies is the Federal Communications Commission (FCC).

The FCC determines how the electromagnetic spectrum is to be used in the United States and is also in charge of enforcing these regulations. While many people gripe about the FCC in terms of broadcasting regulations, the FCC is needed to prevent complete chaos in RF communications. Many regions in the world have their own regulatory agency that serves the same function as the FCC in the U.S. In fact, there is even an international committee called the International Telecommunications Union (ITU) that is made up of numerous member countries.

The manner in which each of these regulatory agencies has decided to divide up the RF spectrum sometimes varies. This means that a radio may be perfectly legal to operate in one region but violates government regulations in other countries. This presents a challenge for creating wireless telecommunication standards that are intended for international adoption. Compromises are often required in order to assure that the same wireless device can operate in all regions of the world. This can be seen in the 802.11 standards where only certain of the frequency channels defined by the standard can be used depending on the region in which a device is operating.

Wireless Standards

Now that you know all about RF signals, hardware, and modulations, you can examine how they are used in various wireless standards. Since most of the heavy lifting has already been done, this section may seem somewhat light. Additional coverage of the various wireless standards is covered in Bonus Web Chapter 1.

Wireless LAN (802.11 a/b/g/n)

Wireless LAN standards are referred to by their corresponding IEEE standard number. All the Wireless LAN specifications are contained within these various IEEE 802.11 standards. Most of the 802.11 standards are, in fact, ratifications or additions to the original 802.11 standard. The suffix letter attached to the 802.11 designation is used to refer to each specific standard. There are numerous 802.11 standards in existence today, and the most prevalent of these are the 802.11a, 802.11b, 802.11g, and 802.11n ratifications. Each of these standards has particular characteristics that make it unique. Table 3 provides a summary of these four standards.

In each of the 802.11 standard ratifications, a great deal of consideration is made toward ensuring interoperability of the various standards. For example, the 802.11g standard took a long time to become an official standard, and most of the time was spent ensuring that it would be backward compatible with the earlier 802.11b standard.

802.11a

The 802.11a ratification made two important additions to the wireless LAN standards. The first of these is the addition of the 5 GHz frequency band, which opened up numerous badly needed frequency channels. Second, a new type of modulation was implemented in 802.11a that provided an increased maximum theoretical data throughput of 54 Mbit/sec.

The new 5 GHz channels utilized in the 802.11a standard do not suffer from the same interference problems as those in the 2.4 GHz ISM band. Table 4 lists the channels and frequencies available in the 802.11a standard. Once again, the “no free lunch” rule applies here since 5 GHz has a shorter range than the 2.4 GHz standards. The reduced range is due to two factors. First, the path loss at 5 GHz is greater than it is for 2.4 GHz. The second attribute of the 5 GHz reduced range comes from the increased line-of-sight behavior as compared to that of 2.4 GHz. Table 4 provides a list of all the 802.11a channels and their corresponding frequencies.

Protocol	Frequency Band	Typical Data Rate	Maximum Data Rate
Legacy	2.4 GHz	1 Mbit/s	2 Mbit/s
802.11a	5 GHz	25 Mbit/s	54 Mbit/s
802.11b	2.4 GHz	6.5 Mbit/s	11 Mbit/s
802.11g	2.4 GHz	11 Mbit/s	54 Mbit/s
802.11n	2.4 and 5 GHz	200 Mbit/s	540 Mbit/s

Table 3 The Common 802.11X Standards

Channel	Frequency (MHz)	A	E	J	W
34	5170			Y	
36	5180	Y	Y		Y
38	5190			Y	
40	5200	Y	Y		Y
42	5210			Y	
44	5220	Y	Y		Y
46	5230			Y	
48	5240	Y	Y		Y
52	5260	Y	Y		Y
56	5280	Y	Y		Y
60	5300	Y	Y		Y
64	5320	Y	Y		Y
100	5500		Y		Y
104	5520		Y		Y
108	5540		Y		Y
112	5560		Y		Y
116	5580		Y		Y
120	5600		Y		Y
124	5620		Y		Y
128	5640		Y		Y
132	5660		Y		Y
136	5680		Y		Y
140	5700		Y		Y
149	5745	Y			Y
153	5765	Y			Y
157	5785	Y			Y
161	5805	Y			Y

A: Americas

E: EMEA (Europe, Middle East, Africa)

J: Japan

W: Rest of the world

Table 4 Channel Numbers and Frequencies for 802.11a

Data Rate (Mbit/s)	Modulation
54	64-QAM (3/4)
48	64-QAM (2/3)
36	16-QAM (3/4)
24	16-QAM (1/2)
18	QPSK (3/4)
12	QPSK (1/2)
9	BPSK (3/4)
6	BPSK (1/2)

Table 5 802.11a Data Rates and Modulations

The modulation utilized in the 802.11a standard is a combination of Orthogonal Frequency Division Multiplexing (OFDM) coupled with advanced modulation techniques such as 16-QAM and 64-QAM. An 802.11a signal consists of 52 individually modulated subcarriers that are combined to construct the complete signal. The combination of these two techniques solved the inherent problems with the high data rate spread-spectrum signals encountered with the prior standards. As a result of this improved modulation technique, 802.11a is capable of achieving a theoretical maximum data rate of 54 Mbit/sec. Table 5 shows a list of all the available data rates in 802.11a along with the specific modulations used for each.

802.11b

The 802.11b standard operates in the 2.4 GHz ISM band and supports increased data rates as compared to the original 802.11 standard. The addition of the higher data rates in 802.11b was accomplished through the use of complementary code keying (CCK) modulation. A great deal of time was spent by the standards committee to find a modulation technique that allowed higher data rates while still maintaining interoperability with the lower data rate. Table 6 provides a list of the 802.11b channels and their corresponding frequencies. Table 7 shows the available data rates in 802.11b along with the associated modulation technique for each.

802.11g

The 802.11g standard is somewhat of a hybrid combination of both the 802.11a and the 802.11b standards. It operates in the 2.4 GHz ISM band and shares the same channels as 802.11b, but it implements the same type of modulation technique as 802.11a. This allows the addition of the 802.11a data rates to the 2.4 GHz band. 802.11g is fully interoperable with 802.11b networks. In fact, much of the time spent on the 802.11g ratification was spent on ensuring interoperability with the 802.11b standard. Although the standard committee went to great lengths to achieve this, operating 802.11b and 802.11g networks in close proximity negatively impacts the performance of the 802.11g network. The frequency channels used by 802.11g are identical to 802.11b and the modulations used in 802.11g are listed in Table 8.

Channel	Frequency (MHz)	A	E	J	W
1	2412	Y	Y	Y	Y
2	2417	Y	Y	Y	Y
3	2422	Y	Y	Y	Y
4	2427	Y	Y	Y	Y
5	2432	Y	Y	Y	Y
6	2437	Y	Y	Y	Y
7	2442	Y	Y	Y	Y
8	2447	Y	Y	Y	Y
9	2452	Y	Y	Y	Y
10	2457	Y	Y	Y	Y
11	2462	Y	Y	Y	Y
12	2467		Y	Y	Y
13	2472		Y	Y	Y
14	2484			Y	

- A: Americas**
- E: EMEA (Europe, Middle East, Africa)**
- J: Japan**
- W: Rest of the world**

Table 6 Channel Numbers and Frequencies for 802.11b

Data Rate (Mbit/s)	Modulation
11 Mb/s	CCK
5.5 Mb/s	CCK
2 Mb/s	DBPSK / DQPSK+DSSS
1 Mb/s	DBPSK / DQPSK+DSSS

Table 7 802.11b Data Rates and Modulations

802.11n

802.11n is the latest and greatest addition to the suite of wireless LAN standards. When the 802.11n standard was commissioned by the IEEE, the primary goal was to develop a wireless standard that could achieve a raw data rate at the MAC level of over 100 Mbit/sec.

Data Rate (Mbit/s)	Modulation
54	64-QAM (3/4)
48	64-QAM (2/3)
36	16-QAM (3/4)
24	16-QAM (1/2)
18	QPSK (3/4)
12	QPSK (1/2)
11	CCK
9	BPSK (3/4)
6	BPSK (1/2)
5.5	CCK
2	DBPSK / DQPSK+DSSS
1	DBPSK / DQPSK+DSSS

Table 8 Data Rates and Modulations Used by 802.11g

Ratified in 2009 (on paper), the 802.11n standard can achieve 300 Mbit/sec. This standard makes use of both the 2.4- and 5-GHz frequency bands.

An interesting aspect of 802.11n is that it exploits the phenomena of multipath interference, which typically causes a severe reduction in data throughput, to actually increase data throughput with a technology called Multiple Input Multiple Output (MIMO). MIMO devices have multiple antennas that are capable of transmitting and receiving different copies of the same signal. By analyzing the signals transmitted and received from each of the antennas using digital signal processing, the effects of multipath propagation are used to increase the amount of data that can be communicated by the signal.

Summary

This Bonus Web Chapter has covered some of the under-the-hood components of wireless communications and has also provided a little more technical detail than typically covered. Many of the topics covered are just interesting to know about, but others have hopefully provided a useful insight into how wireless hardware works and will enable the reader to more effectively use their tools. If the reader is interested in learning more about the material covered in this chapter, they should be able to find plenty of resources on the Internet by searching for the keywords used in the chapter.