CHAPTER 6

Evaluating and Selecting Wireless Equipment

The equipment that you select for your broadband wireless wide-area network (WAN) plays a major role in the reliability, scalability, and profitability of your network. This chapter helps you evaluate and select your wireless network equipment.

This chapter does not list feature information vendor by vendor. The quantity of information would be overwhelming and the listing would quickly become outdated. Instead, this chapter aims to help you understand the features and characteristics that are available on wireless equipment. When you understand the features and their significance, you will be in a position to select the equipment that best meets your network needs.

Any New Features This Week?

Wireless equipment is evolving rapidly. Wireless hardware and software features change each week. I have attempted to describe all the significant wireless hardware and software features that were offered (by at least one equipment manufacturer) at the time I wrote this chapter in 2002. Because of rapid equipment evolution, I suggest that you supplement the information presented here with your own feature research.

This chapter contains the following major sections:

- A description of the equipment selection process.
- A brief explanation of the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) seven-layer reference model. An understanding of this model helps you understand how various wireless features fit into your network.
- A list of equipment features, arranged by OSI layer. Following each feature is an explanation of the feature.
- A summary of the features that are the most desirable for wireless backbone equipment, access points (APs), customer premises equipment (CPE), wireless network cards, mesh network nodes, and amplifiers.
- A discussion of compatibility issues that can cause problems when mixing wireless equipment from different vendors.
- Suggestions about evaluating and receiving vendor support.

Overview of the Equipment Selection Process

Your equipment purchase can involve spending only a few hundred dollars, or it can involve spending hundreds of thousands of dollars. The more money that you plan to spend, the more important it is that you include all of the following steps in your selection process.

Reviewing Your Wireless Network Needs

Before you select your wireless equipment, take the time to review your wireless network needs:

- How many wireless end users do you want to serve?
- What network architectural elements do you want your wireless network to include?
- Do you need only point-to-point links or will you deploy point-to-multipoint APs?
- Do you need wireless backbone bandwidth?
- Do you need mesh network nodes or repeaters?
- What features will your wireless network need so that it can connect to your wired network?
- Will you need routing or only bridging?

After you have reviewed both the wireless network features and the wired features that you need, you are ready to begin researching specific wireless equipment features.

Researching Equipment Features

Now that you know your network needs, you can begin listing wireless equipment that matches your needs. The most difficult part of the research process is not learning what features a particular brand of equipment offers. The most difficult part is learning what features are *not* offered or which features do not work the way you expect them to work.

If you have not worked with wireless equipment before, it can be difficult to get an accurate picture by looking only at press releases and advertising flyers. Press releases are typically loaded with attractive buzzwords that promise wireless performance and wireless benefits that are sometimes exaggerated or theoretical. Advertising flyers and spec sheets do not lie about equipment performance, but they sometimes omit information that would reveal performance shortcomings.

Evaluate equipment that offers the specific features that you need, such as distance and bandwidth capabilities, but before you decide to buy, visit a network where that particular vendor's equipment is deployed.

Visiting Deployment Sites

After you have researched equipment features, you will have one or more equipment vendors who can provide equipment that appears (at least on paper) to meet your wireless needs. It is appropriate and proper for you to ask the vendors to recommend one or two existing wireless networks that have deployed their equipment. Visit these sites and talk with the network operators who have deployed the equipment.

Your visit will allow you to learn what features work especially well and what features do not work as expected. You will learn which expectations were exceeded (the good news) and which expectations were not met (the not-so-good news). You will learn if the equipment is easy or difficult to manage. You will also learn if vendor support is poor, good, or outstanding. This is information that you cannot obtain from a spec sheet or an advertising flyer. With the benefit of this information, can make an accurate and informed decision about which equipment to purchase.

Testing Wireless Equipment in the Lab

When you have completed your site visits, there will probably be one or two vendors that you think would be good equipment providers. At this point, consider making a small equipment purchase consisting of either a pair of wireless units or one AP and one CPE unit.

Set up these units indoors and become familiar with them. Configure the units and measure their throughput in both directions. Learn to use the diagnostics.

TIP Practice safety when you are working near wireless equipment. High amounts of microwave energy can cause damage to the human body, so minimize your exposure to this type of energy. Do not point a directional antenna at yourself or at any other nearby person. Turn the wireless equipment off any time you are not testing it. Remember: When you double the distance between yourself and a wireless antenna, you reduce the amount of radiation reaching you to one-fourth the previous level. Whenever possible, maintain as much distance as possible between yourself and a wireless antenna.

When your indoor testing is complete and you are comfortable with the units, proceed to outdoor testing.

Testing Wireless Equipment Outdoors

Testing wireless equipment outdoors allows you to test the range, throughput, and reliability of the equipment in the presence of real-world noise, interference, and weather.

For your outdoor testing, perform the following steps:

Step 1 Pick two locations that are as far apart as the maximum link distance that you expect the equipment to cover. For example, if you plan to build a wireless cell with a 4-mile (6.4 km) radius, pick an AP location that is high enough to have at least two line-of-sight (LOS) paths that are at least 4 miles long.

Step 2 Test using an AP antenna system similar to the one that you expect to use in your actual network deployment.

Step 3 Temporarily set up the CPE at first one and then the other of your two test locations.

Step 4 Test during the busiest part of the day and repeat the throughput tests that you performed indoors. It is important that you test the throughput from the CPE to the AP. This is an important test of the AP's capability to receive in the presence of noise and interference. For more details about throughput testing, see the description in Chapter 7, "Installing Outdoor Wireless Systems."

Step 5 If possible, repeat your performance testing several times over a period of several days or weeks. The equipment performance should remain constant throughout the entire test period.

Your outdoor testing will not tell you how many customers the AP will handle at full load, but it will give you a good preliminary performance indication. If all your test results are good, proceed to the following purchase decision step.

Making Purchase Decisions

Your testing should bring you to the point where you are most comfortable with the performance of one or two brands of wireless equipment. You can now make your purchase decision and be fairly confident that the equipment you buy will meet your performance expectations.

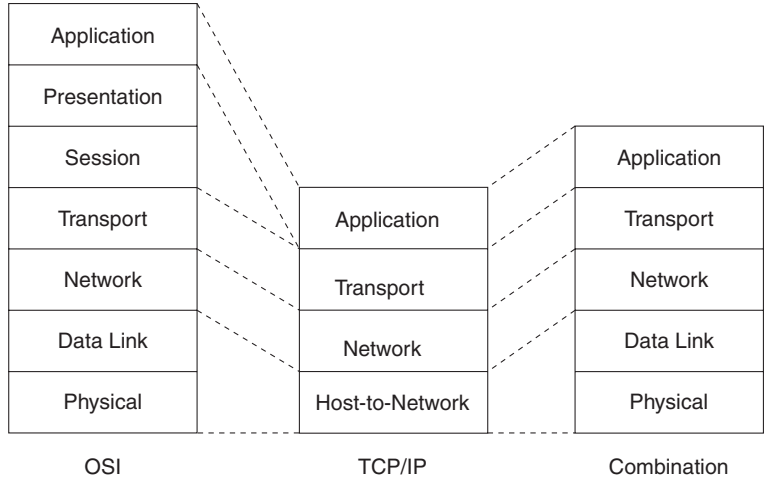
OSI and TCP/IP Reference Models

Several different but similar layered data architectures have been developed to allow reliable data transfer between different computer systems and between different networks. When you understand a little about the service layers and the protocols that these architectures use, you will be in a good position to understand the similarities and the differences between different brands of wireless equipment.

The seven-layer ISO OSI reference model was first proposed around 1983 to allow connectivity (or interworking) between different computer systems. Prior to the OSI reference

model, computer systems made by one manufacturer could not easily communicate with computer systems made by other manufacturers. The intent of the OSI reference model was to allow computer systems to successfully communicate with each other even though different vendors manufactured them. Figure 6-1 shows the OSI reference model alongside the
TCP/IP architecture.

Figure 6-1 *OSI and TCP/IP*



Beginning in the 1970s, the United States Department of Defense began promoting computer networking between university research departments and government installations. One of the primary goals of this internetworking effort was to develop a survivable network—one that would be able to continue communicating even if some of the network nodes or some of the communications links were destroyed. This new networking effort was based on two primary protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP performed transport layer functions equivalent to the transport layer in the OSI model. IP performed network layer functions that were equivalent to the network layer (Layer 3) in the OSI model. When application layer (Layer 7) protocols (Telnet, FTP, SMTP, and so on) and physical (Layer 1) and data link layer (Layer 2) protocols were added, the result was an architecture that effectively contained five layers. Figure 6-1 shows the TCP/IP model alongside the OSI reference model for comparison.

The TCP/IP architecture is functionally equivalent to the OSI reference model. The major similarities and differences are as follows:

- Both models have an application, a transport, and a network/Internet layer.
- The TCP/IP model does not have a session layer (Layer 5 of the OSI reference model) or a presentation layer (Layer 6 of the OSI reference model).

- Both models have a lower layer that connects the upper layers to the actual physical network. In the OSI reference model, the lower layer (Layer 1) is called the physical layer. In the original TCP/IP model, the lower layer was called the host-to-network layer. In present-day use, TCP/IP networks use the combination of a Layer 2 sublayer called the medium access control (MAC) sublayer along with Layer 1 to provide connectivity over the wireless link.

Virtually all the wireless equipment features that you evaluate operate at the physical, data link, and network layers of the OSI and TCP/IP reference models. The wireless features and functionality (modulation type, data rate, and so on) take place at the physical layer. Access to (and sharing of) the wireless medium takes place at the data link layer. Routing takes place at the network layer.

Peer Protocols

Peer protocols run across the Internet but provide communication only between same-layer processes. One example of this same-layer communication process is a Hypertext Transfer Protocol (HTTP) web browser running on the application layer of one network. The HTTP browser retrieves information from its peer web server running on the application layer of another network. Although the HTTP communication is application-layer-to-application layer (peer-to-peer), both networks communicate downward through their lower network layers.

Services

Information is passed from the top (application) layer of one network down through the lower layers. Each layer provides a set of services for the layer just above it and utilizes the services provided by the layer just below it. The set of services between two layers is referred to as the *interface* between the two layers. For example, Layer 6 provides services for Layer 7; Layer 5 provides services for Layer 6; and so on. In this way, Layer 7 (the application layer) can communicate all the way down to Layer 1 (the physical layer).

The following list illustrates how services and protocols operate. When your web browser uses HTTP over a wireless network, the information flow is as follows:

1. The HTTP information request originates at the application layer on the originating network.
2. The HTTP request travels downward from the application layer (using the services provided by all the intermediate layers) to the physical layer on the originating network. The physical layer uses the appropriate wireless *protocol* (for example, the appropriate direct sequence spread spectrum modulation or DSSS) to communicate the request over the air wirelessly to the physical layer on the other network.

3 The physical layer on the other network uses the DSSS protocol to receive the request from the originating network. The physical layer then passes the information up through its interface to the data link layer. Using higher and higher layer services, the request passes upward until it eventually reaches the application layer. There, the HTTP protocol processes the request and replies with a response.

4 Using services of lower and lower layers, the response travels downward to the physical layer. Using the Layer 1 DSSS protocol, the response is transmitted over the air back to the physical layer of the originating network.

5 Using services, the originating network passes the response upward to the application layer where the HTTP protocol receives the response to its original request.

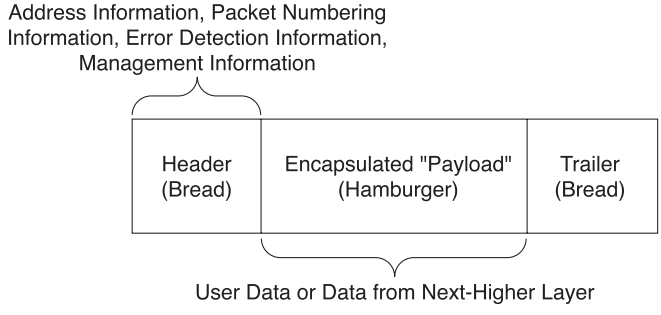
Basic Packet Structure and Frame Types

Packet switching store-and-forward techniques underlie the operation of layered architectures. Packet switching uses an underlying data structure, called a *packet*. A packet is like a hamburger on a bun. Although the exact packet structure varies from layer to layer and protocol to protocol, most packets contain a data payload section. The data payload is the hamburger in the middle of the bun. Other fields encapsulate (surround) the data payload and make up the bun. The bun typically provides the following:

- Source and destination address information
- Packet numbering information
- Packet acknowledgment information
- Error detection and correction information

Figure 6-2 shows this general packet structure.

Figure 6-2 *General Packet Structure*



Packets prepared by Layer 2 (the data link layer) are called *frames*. Not all frames contain payload data. Wireless APs and wireless stations exchange three types of frames, each with the following functions:

- Data frames carry user payload data (the hamburger) between different wireless network nodes.
- Control frames carry information such as request-to-send (RTS) and clear-to-send (CTS) messages as well as frame acknowledgments (ACK).
- Management frames carry association and authentication requests and responses in addition to beacon information.

Application Layer Functions and Protocols

The application layer is where the end user programs run. Telnet, Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and HTTP are examples of application layer protocols. Wireless equipment that you evaluate will likely have network management software that operates at the application layer level.

Transport Layer Functions and Protocols

The transport layer's job is to provide reliable communications from application to application regardless of the lower-layer protocols and communications links. The transport layer encapsulates data from the application layer (and the session layer, if used) and passes it down to the network layer.

Typical transport layer protocols are TCP and User Datagram Protocol (UDP). Wireless equipment that you evaluate does not usually have features that operate at the transport layer level.

Network Layer Functions and Protocols

The essential network layer protocol is IP. In addition to IP, the network layer often utilizes other routing protocols such as Routing Information Protocol (RIP) and Border Gateway Protocol (BGP).

The network layer encapsulates data (the hamburger) from the transport layer between IP source, IP destination, and IP routing information. Packet routing typically goes from intermediate network to intermediate network before the packets finally arrive at their destination network.

Data Link Layer Functions and Protocols

The data link layer includes the logical link control (LLC) sublayer and the MAC sublayer. The data link layer normally performs a wide variety of functions, including segmenting the bit stream into frames, error handling, flow control, and access control.

Examples of data link layer protocols include Point-to-Point Protocol (PPP) and Spanning Tree Protocol.

LLC Sublayer Functions and Protocols

The LLC sublayer makes up the top half of the data link layer and interfaces to the network layer (above) and the MAC sublayer (below). The LLC Sublayer encapsulates the Layer 3 data by adding sequence and acknowledgment numbers. The LLC Sublayer might provide different service options, depending on the network software.

MAC Sublayer Functions and Protocols

The MAC sublayer makes up the bottom half of the data link layer. The MAC sublayer interfaces to the physical (wireless) layer and provides the following functions:

- **Reliable delivery**—The MAC sublayer provides a reliable delivery mechanism that looks for an acknowledgment for every frame that is sent. If an acknowledgment is not received, the MAC sublayer retransmits the frame.
- **Access control**—The MAC sublayer controls access to the wireless channel. The two basic types of access control are carrier sense multiple access with collision avoidance (CSMA/CA) and polling. CSMA/CA is a distributed coordination function (DCF) because the decision about when to transmit is distributed to all wireless stations. Each wireless station listens before transmitting. If a station hears that the frequency is busy, it backs off (waits) a random amount of time and tries again. When the frequency is clear, the station proceeds to transmit. In addition, a request-to-send/clear-to-send (RTS/CTS) mechanism can be enabled. Large packets are more likely to collide; therefore, stations that have packets larger than the RTS/CTS threshold must request and receive clearance from the AP MAC before they can transmit their packets. Finally, in networks that have heavy traffic and many end users, a point coordination function (PCF) can be used. One single point (the MAC in the AP) coordinates transmissions from all stations. The PCF polls each wireless station and then tells each end user when it can transmit.

NOTE You might have heard of wireless networks with a hidden node problem. This problem can occur in a network that uses DCF. In most wireless networks, certain wireless stations cannot hear all the other wireless stations. Under heavy traffic loads, several stations might try to transmit at the same time. This can happen even when the stations are using RTS/CTS. When stations transmit at the same time, collisions occur and network throughput drops drastically. The solution to hidden-node problems is to use wireless equipment that can support PCF.

- **Encryption**—The MAC also provides encryption. The most frequently used encryption method is wired equivalent privacy (WEP).

MAC control frame subtypes include RTS, CTS, and ACK. Examples of management frame subtypes include Beacon, Probe Request, Authentication, and Association Request.

Physical Layer Functions and Protocols

The physical layer transports encapsulated data from the data link layer and transmits it wirelessly to the distant network. There are several physical layer wireless standards. There are also many proprietary physical layer wireless protocols. In addition to your wireless feature evaluation, you will evaluate physical layer wired-interface features such as Ethernet and serial port features.

Physical Layer Wired-Interface Features

This section describes the wired-interface feature options that you will encounter when you begin to research and select your wireless equipment.

NOTE No wireless equipment vendor offers all the listed features in any model of their wireless equipment—nor should they. Each wireless network is built to serve a specific set of end user needs. These end user needs dictate the best set of wired and wireless features for that particular network. Each feature listed in the following sections is offered on at least one brand and model of wireless equipment. It is important that, as you consider the available features, you keep your wireless network needs in mind. Your equipment research involves finding the best match between your network needs and the wireless equipment feature set offered on a particular model of wireless equipment.

Your physical layer wired-interface feature evaluation includes some or all of the following:

- Low-speed data ports
- Ethernet ports
- High-speed data ports
- Voice interfaces

Low-Speed Data Ports

Most wireless equipment contains at least one low-speed port, such as the following:

- **Low-speed serial data ports**—On some equipment, a low-speed serial data port is used for initial system configuration. The serial port speed generally ranges between 4800 bits per second (bps) and 19.2 kilobits per second (kbps).
- **Low-speed user data ports**—Early wireless modems were frequently designed to transport only low-speed serial data over the wireless link. Port speeds range from 4800 bps to 128 kbps.
- **Dialup telco interfaces**—Dialup telco interfaces provide low-speed dial backup connectivity for times when a higher-speed primary link, such as a T1 or digital subscriber line (DSL) link, is unavailable.

Ethernet Ports

Ethernet interfaces allow network data to access the wireless network. Wireless equipment can include one or more of the following Ethernet interfaces:

- **10Base-T**—This is the most common Ethernet interface.
- **100Base-TX**—This interface is found on higher-speed wireless equipment.
- **Ethernet hubs or switches**—This interface is found on some wireless APs.

High-Speed Data Ports

In addition to Ethernet interfaces, it is often desirable to use wireless bridges or routers to transport other high-speed non-Ethernet data streams. To transport these streams, wireless equipment can include the following interfaces:

- **Digital subscriber line (DSL) interfaces**—DSL interfaces enable a wireless bridge or router to extend or share a DSL connection.
- **Cable interfaces**—Cable interfaces enable wireless equipment to extend or share a cable Internet connection.

- **Asynchronous Transfer Mode (ATM) interfaces**—ATM interfaces enable wireless equipment to connect to and from an ATM network.
- **T1/E1 interfaces**—T1/E1 interfaces enable wireless equipment to extend a 1.544 megabit per second (Mbps) T1 line or a 2.048 Mbps E1 line from point A to point B, for example, between two private automatic branch exchanges (PABXs). Some models of wireless equipment provide T1/E1 connectivity only. Other wireless equipment models provide simultaneous wireless Ethernet and T1/E1 connectivity.

TIP Telecommunications managers who want to provide both Ethernet and voice-PABX connectivity between buildings find wireless equipment that simultaneously provides both Ethernet and T1 connectivity to be especially useful.

- **T3/E3 interfaces**—45-Mbps T3 interfaces enable full-duplex wireless equipment to provide T3 connectivity between two points.
- **Optical Carrier 3 (OC-3) interfaces**—155-Mbps OC-3 interfaces enable full-duplex wireless equipment to provide OC-3 connectivity between two points. Wireless OC-3 equipment usually has the capability to carry several T1 or E1 circuits in addition to the OC-3 circuit.
- **Optical Carrier 12 (OC-12) interfaces**—622-Mbps OC-12 interfaces allow full-duplex wireless equipment to provide OC-12 connectivity between two points.

TIP Remember that, in general, there is an inverse relationship between wireless bandwidth and wireless distance; as bandwidth goes up, distance goes down. OC-12 wireless equipment typically operates only over distances up to approximately 1312 ft. (400 m).

Voice Interfaces

Voice interfaces enable wireless equipment to carry voice in addition to data. The following types of voice interfaces are possible:

- **Voice over Internet Protocol (VoIP) interfaces**—VoIP interfaces allow IP telephones to connect directly to the wireless equipment and to make on-network voice calls. Making calls to the public switched telephone network (PSTN) requires the use of an external telephone gateway.
- **Talkback/orderwire interfaces**—A talkback interface (sometimes called an *order wire*) provides a two-way voice circuit. Maintenance personnel normally use this circuit for end-to-end voice communication over the wireless link while servicing the wireless equipment.

Wired-Interface Security Features

Physical layer wired-interface security features limit user access to the system administration console via a serial port or an Ethernet port. Successful entry of a password is required before gaining access to system administration functions. Additionally, some equipment allows a management station IP address to be configured. Attempts to access the system administration console from other IP addresses are refused.

Physical Layer Wireless-Interface Features

Wireless features operate at the physical layer; therefore, your wireless-interface feature evaluation covers a broad range of features. The following sections cover these feature categories:

- **NLOS**—Non line-of-sight and near line-of-sight equipment capabilities
- **Wireless frequency bands**—Propagation characteristics and equipment availability for each of the license-free bands
- **Modulation types**—Various types of modulation used by license-free equipment
- **Bandwidth and throughput**—Tradeoffs between data rate, data throughput, and link distance
- **Noise and interference-reduction features**—Receiver and antenna features that improve signal reception abilities
- **Security**—Physical layer wireless security features
- **Miscellaneous wireless features**—Transmit and receive features that can play a significant role in the performance of your wireless network operation

Non Line-of-Sight Features

In the broadband wireless industry, there is no agreement about the exact meaning of the term *NLOS*. Here are two common ways that NLOS is used:

- **Near line-of-sight**—When equipment vendors state that their equipment has *near*-LOS capabilities, they are claiming that it operates satisfactorily even when there is a partially obstructed line-of-sight path, as long as there are not too many obstacles to the line-of-sight path. For example, perhaps a few trees are intruding into the Fresnel zone.
- **Non line-of sight**—When equipment vendors state that their equipment has *non*-LOS capabilities, they are claiming that it operates satisfactorily even when there is an obstructed line-of-sight path. For example, perhaps buildings, trees, and hills are completely blocking the path.

Because there is no standard definition of NLOS, the process of evaluating NLOS performance claims is a challenging one. Almost all vendors of NLOS equipment (either accidentally or intentionally) exclude information about the range of their NLOS equipment. The impression is left with the customer (you) that the NLOS equipment has the same communications range as LOS wireless equipment. This is never the case; the range of NLOS equipment is always substantially less than the range of equipment that is operating over a true, unobstructed LOS path.

Now, you will learn about features that actually improve performance in NLOS environments. Two significant challenges that an NLOS environment presents for wireless equipment are as follows:

- **Multipath**—Any equipment feature that improves performance in a multipath environment also improves performance in an NLOS environment. These features are as follows:
  - Diversity antennas
  - Circularly polarized antennas
  - Smart antennas that constantly adjust their beamwidth to receive and transmit energy directly to and from each individual end user antenna
  - Adaptive equalization
  - Multicarrier modulation, such as OFDM

  Whenever possible, always try to design your wireless WANs to use LOS paths. You will achieve more reliable coverage at longer distances.
- **Attenuation**—Attenuation losses in a non-LOS environment are the reason that the communications range in an NLOS environment is less than in a LOS environment. The following equipment and network features reduce attention and improve NLOS performance:
  - Receiver sensitivity
  - 900 MHz frequency band
  - Mesh networks

Wireless Frequency Bands

The following sections describe the license-free frequency bands, including the propagation characteristics and the power levels of each band.

900 MHz

900 MHz is the lowest-frequency industrial, scientific, and medical (ISM) band. The total width of the band is 26 MHz. Signals in this band have a wavelength of approximately 12 inches (30 cm). These signals have the capability to pass through some obstructions without being completely lost. For example, they can pass through light trees and diffract

over one low hill and still be strong enough to be received several miles away. 900 MHz is the best band to use when there are just a few obstacles to the LOS path. Table 6-1 shows 900-MHz power levels.

Table 6-1 *Power Levels for the 900-MHz Band*

Band	Maximum Transmitter Power	Maximum Antenna Gain	EIRP (Equivalent Isotropic Radiated Power)
902 to 928 MHz	+30 dBm (1 Watt)	+6 dBi	+36 dBi (4 Watts, relative to an isotropic antenna)

2.4 GHz

2.4 GHz is the middle ISM band. The total width of the band is 83 MHz. Signals in this band have a wavelength of approximately 4.8 inches (12 cm). These signals have little capability to pass through obstructions without being lost. Passing through one wall can result in 10 to 12 dB of attenuation. Attenuation from trees varies depending on the presence of leaves and whether the leaves are wet or dry but, on average, the attenuation from trees is approximately .5 dB per meter. One 30-ft (10-meter) diameter tree (the tree canopy/leaves are 30 feet across, not the tree trunk) results in about 5 dB of attenuation; 6 dB of attenuation reduces the length of a wireless link to 1/2 of its previous length. You can see that passing a 2.4-GHz signal through a few trees can easily reduce the usable length of the wireless path to a few hundred feet. Table 6-2 shows 2.4-GHz power levels.

Table 6-2 *Power Levels for the 2.4 GHz Band*

Band	Maximum Transmitter Power	Maximum Antenna Gain	Maximum EIRP
2403 to 2483 MHz (Point-to-Multipoint)	+30 dBm (1 Watt)	+6 dBi	+36 dBi (4 Watts).
2403 to 2483 MHz (Point-to-Point only)	+30 dBm (1 Watt)	(3-to-1 Rule) For every 3 dBi (above +6 dBi) of antenna gain, reduce the transmitter power by 1 dB. (For example, for a +9 dBi antenna, reduce transmitter power to +29 dBm.)	Depends on antenna size. With a +24 dBi antenna and +24 dBm of transmitter power, +48 dBi (64 Watts) is possible in a Point-to-Point (only) link.
2403 to 2483 MHz Wideband frequency hopping spread spectrum using from 15 to 74 hopping frequencies	+21 dBm (125 mW)	+6 dBi	+27 dBi (500 mW).

3.5 GHz

The 3.5-GHz band is not available for use in the United States; however, some frequency subbands between 3.3 and 4.0 GHz are available for use (usually on a licensed basis) in a number of other countries. This band is mentioned here because equipment for this band is, in many cases, similar to equipment for the 2.4-GHz band. Signals in this band have a wavelength of approximately 9 cm (3.4 in). The propagation characteristics are somewhat similar to the 2.4-GHz band, although attenuation from trees and other obstructions is higher.

5 GHz

There are four license-free subbands at 5 GHz, although two of these bands overlap each other. There is one ISM band from 5725 to 5850 MHz (5.725 to 5.850 GHz), and there are three Unlicensed National Information Infrastructure (U-NII) bands: 5150 to 5250 MHz, 5250 to 5350 MHz, and 5725 to 5825 MHz. The ISM band is 125 MHz wide, and each U-NII band is 100 MHz wide. Signals in the 5-GHz subbands have a wavelength of approximately 2 inches (5 cm). Each 5 GHz subband is wider than the entire 2.4-GHz band; therefore, it is possible to build 5-GHz wireless equipment that provides more bandwidth and more throughput than equipment for any other license-free band. The attenuation from trees at 5 GHz is about 1.2 dB per meter; therefore, each 30-ft (10-meter) diameter tree (crown) that blocks an LOS path reduces the length of a wireless link by approximately 75 percent. Table 6-3 shows 5-GHz power levels.

Table 6-3 *Power Levels for the 5-GHz Band*

Band	Maximum Transmitter Power	Maximum Antenna Gain	EIRP
ISM 5725 to 5850 MHz	+30 dBm (1 Watt)	+6 dBi	+36 dBi (4 Watts). Note that point-to-point systems can use an antenna with more than +6 dBi gain with no transmitter power reduction.
U-NII 5150 to 5250 MHz	+17 dBm (50 mW)	+6 dBi	+23 dBi (500 mW; indoor use only per FCC regulations.)
U-NII 5250 to 5350 MHz	+24 dBm (250 mW)	+6 dBi	+30 dBi. (1 Watt).
U-NII 5725 to 5825 MHz	+30 dBm (1 Watt)	+6 dBi	+36 dBi (4 Watts) Note that point-to-point systems can use an antenna with up to +23 dBi gain with no transmitter power reduction.

60 GHz

The 59 to 64-GHz ISM band was approved for use in the United States in 1999. The total width of this band is almost 5 GHz. Signals in this band have a wavelength of about 2/10 of an inch (1/2 cm). Signals at this frequency are attenuated by the presence of oxygen in the air; therefore, the maximum wireless link distance is approximately half a mile (800 m), assuming that a LOS path is available. Obstructions completely block the signal. The advantage of this band is that equipment is available that provides point-to-point raw data rates up to 622 Mbps. In addition, the oxygen absorption means that the likelihood of interference from other networks is low.

Modulation Types

This section covers the following information:

- A quick review of the modulation process
- A direct sequence spread spectrum (DSSS) description
- A frequency hopping spread spectrum (FHSS) description
- An orthogonal frequency division multiplexing (OFDM) description
- A brief mention of other spread spectrum and non-spread types of modulation

Understanding the Modulation Process

Chapter 1, "An Introduction to Broadband License-Free Wireless Wide-Area Networking," defined *modulation* as the process of adding intelligence to the signal. The modulation process creates a change in some combination of the amplitude, the frequency, or the phase of a signal. Many types of modulation exist, including amplitude modulation used by commercial AM broadcast stations and frequency modulation (FM) used by police departments and fire departments, for example.

Spread spectrum modulation was originally designed for use by the military to camouflage the existence of and the content of military communications. Descriptions of the two types of spread spectrum modulation follow.

Direct Sequence Spread Spectrum (DSSS) Modulation

DSSS modulation simultaneously widens (spreads) a data signal out and reduces the amplitude (technically, it reduces the power density) of the signal. The resulting modulated signal resembles a low-level noise signal that is widely dispersed around a single frequency. The modulated DSSS signal is wider than the bandwidth of the original data. For example, an 11-Mbps raw data rate signal becomes a 22-MHz-wide DSSS signal. In the 2.4-GHz frequency band, there is enough room for three nonoverlapping 11 Mbps-wide signal

channels. Each time a DSSS signal is transmitted, the wireless energy is centered around only one frequency; therefore, DSSS modulation is a *single-carrier* modulation scheme.

Frequency Hopping Spread Spectrum Modulation

Frequency Hopping Spread Spectrum (FHSS) modulation does not spread its signal energy out, but it rapidly shifts the energy from frequency to frequency. A narrowband FHSS signal is transmitted first on one narrow (1-MHz) channel and then quickly shifted to another channel, then another, and another, and so on. The rapid frequency hopping gives this type of modulation its name. The two following types of FHSS are now allowed in the 2.4-GHz band:

- **Narrowband frequency hopping**—Narrowband FHSS signals are 1 MHz wide. They hop using a total of 79 different frequencies. The signal can hop between these frequencies in 78 unique hopping patterns or hopping sequences. 802.11 standards define narrowband frequency hopping.

NOTE Hopping sequences are sometimes different in different countries. Check with your national telecommunications authority for the regulations in your country.

- **Wideband frequency hopping**—Wideband FHSS signals can be up to 5 MHz wide and can hop using a total of less than 75 different frequencies. Typical wideband FHSS systems use far less than 75 frequencies; one such system uses 43 frequencies with a signal that is 1.7 MHz wide. Wideband frequency hopping systems are relatively new and are just beginning to be deployed in outdoor wireless WANs.

FHSS equipment changes its center frequency each time it hops; however, each time it transmits, the wireless energy is still centered on only one frequency. FHSS is, therefore, a single-carrier modulation scheme.

Orthogonal Frequency Division Multiplexing Modulation

Orthogonal Frequency Division Multiplexing (OFDM) modulation transmits bursts that use more than one carrier frequency simultaneously. Compared to a DSSS signal, an OFDM signal has the following characteristics:

- Occupies the same amount of bandwidth
- Uses 52 carriers instead of one carrier
- Carries more information with each transmitted burst
- Is more resistant to multipath fading

802.11a equipment uses OFDM modulation and operates on the 5-GHz band; 802.11g uses OFDM on the 2.4-GHz band. OFDM is a *multicarrier* modulation scheme because it transmits using more than one carrier simultaneously.

Other Spread Spectrum Modulation Types

Other types of spread spectrum modulation are now legal to use. These versions are proprietary to particular manufacturers and do not interoperate with 802.11b, 802.11a, or 802.11g systems.

One example of a proprietary spread spectrum modulation type is multicarrier DSSS. Rather than using just one DSSS carrier, multicarrier DSSS uses several simultaneous carrier frequencies to transport data. This multicarrier approach is a hybrid combination of single-carrier and multicarrier modulation.

Other Nonspread Spectrum Modulation Types

In the ISM bands, the FCC originally required that spread spectrum modulation be used. Recent rule changes now allow additional modulation types. In the U-NII bands, nonspread spectrum modulation types are permitted, and equipment manufacturers use proprietary digital modulation schemes to offer a variety of high-bandwidth point-to-point and point-to-multipoint systems.

Bandwidth and Throughput

It is important for you to understand wireless throughput so that you can meet (or exceed) the expectations of your wireless end users. This section describes the following:

- The difference between the wireless data rate and the wireless throughput
- The tradeoff between throughput and distance
- Examples of low, medium, and high throughput equipment

Comparison Between Data Rate and Throughput (Including Simplex Versus Duplex Throughput)

There is a common misunderstanding regarding the bandwidth, the data rate, and the throughput of a wireless device:

- Bandwidth refers to the raw data rate of the device.
- Throughput refers to the actual amount of end user data that the device can transfer in a given time interval.

The result of this misunderstanding is that wireless network users are frequently disappointed in the wireless throughput (data transfer speeds) that they experience.

Understandably, wireless equipment manufacturers want their equipment to look as attractive as possible to potential buyers. For this reason, they usually use the raw data rate in their sales and advertising material. An 802.11b AP, for example, provides a raw data rate of 11 Mbps.

Wireless users have a different expectation; they are interested in how fast a web page or a file downloads. They are interested in the capability of the wireless device to deliver their data. When the wireless users' 802.11b AP delivers just 5.5 Mbps of data throughput, they feel that there must be a problem with the equipment.

Most frequently, the real data throughput potential of a half-duplex wireless network is approximately 50 percent of the raw data rate. An 802.11b AP operating at the maximum 11-Mbps raw data rate has a maximum throughput potential of about 5.5 Mbps. This difference between raw data rate and actual throughput has several causes, including these:

- The framing and signaling overhead
- The half-duplex turnaround time between transmit and receive
- The lower efficiency inherent in the transmission of small packets

Collisions between wireless users and interference from other networks can reduce the throughput below 50 percent. Chapter 8, "Solving Noise and Interference Problems," discusses this issue in more detail.

Remember that your end users rely on you to set their throughput expectations realistically. When they measure their throughput and discover that it meets or slightly exceeds the throughput that you told them to expect, they will judge your wireless network performance to be good.

Tradeoff Between Data Rate and Distance

As you evaluate wireless equipment, you will invariably compare different equipment brands based on how long of a link they can support. Link distance is important; however, during your comparison, it is important that you compare apples to apples. When you compare two brands of wireless equipment side by side, you must compare their link distances at the same data rate. Other factors being equal, the higher the throughput (or the higher the raw data rate), the shorter the communications range. Table 6-4 lists the typical outdoor link distances from an 802.11b AP (using a standard low-gain omnidirectional antenna).

Table 6-4 *Examples of 802.11b Data Rates Versus Distances*

Data Rate	Distance in Ft. (m)
11 Mbps	500 (152)
5.5 Mbps	885 (270)
2 Mbps	1300 (396)
1 Mbps	1500 (457)

As the data rate increases, the maximum AP link distance decreases. AP data rates automatically fall back to the next lower level when the AP detects the signal quality decreasing as the link distance increases.

Sub-1 Mbps Data Rates

Two types of wireless systems operate at sub-1 Mbps data rates:

- Low-speed (such as 4800 bps to 128 kbps) wireless modems that provide a point-to-point wireless extension for an RS-232 serial data system.
- 128 kbps to 1 Mbps point-to-point or point-to-multipoint wireless Ethernet bridges or AP systems. These systems are useful for Internet access.

1-Mbps to 11-Mbps Data Rates

Most point-to-multipoint wireless WAN systems are in this category. This category also includes both 802.11 (2 Mbps) and 802.11b (11 Mbps) systems.

12-Mbps to 60-Mbps Data Rates

This category includes both high-bandwidth point-to-point backbone equipment and point-to-multipoint equipment. Here are some examples:

- Point-to-point equipment is available with bandwidths of 12 Mbps, 20 Mbps, 24 Mbps, and 45 Mbps.
- Point-to-multipoint equipment is available with shared, aggregate bandwidths of 20 Mbps, 40 Mbps, 54 Mbps, and 60 Mbps.
- 802.11a WLAN equipment is becoming available. However, as this book was being written, this equipment was not yet appropriate for use in outdoor wireless networks. The power level was too low, and there is no connector to attach an outdoor antenna.

Over 60-Mbps Data Rates

The higher in frequency wireless equipment operates, the more bandwidth that is available. Products that provide more than 60 Mbps of bandwidth operate almost exclusively in the 5.3- and 5.8-GHz U-NII bands, although a few short-range products operate in the 60-GHz band. Products that operate in these bands have aggregate bandwidths of 90 Mbps, 100 Mbps, 155 Mbps (OC-3), 200 Mbps, 480 Mbps, 622 Mbps (OC-12), and 872 Mbps. All these are full-duplex products.

Noise and Interference Reduction Features

Noise is defined as anything and everything other than the desired signal. Interference reduces the throughput of a wireless network. Interference has many sources, so it is important that you consider and utilize all possible noise-reduction features.

NOTE Chapter 8 is devoted completely to the topic of understanding and minimizing the effects of noise and interference. Refer to Chapter 8 for additional information as you read about the following interference-reduction features.

In the outdoor wireless environment, many potential interference sources exist. You can use a few equipment characteristics to provide some help in minimizing the effects of interference.

The following interference-reduction features operate at the physical layer to help reduce the effects that interference can have on both AP and CPE throughput.

Receiver Selectivity

Selectivity is the capability of a receiver to reject signals that are not exactly on the desired receiving frequency. No receiver is perfectly selective; no receiver has the capability to completely reject all off-frequency signals; therefore, all receivers are susceptible to being overloaded by nearby, strong off-frequency signals. These off-frequency signals can be within the license-free band (in-band interference), or they can be outside the band (out-of-band interference).

Overloading causes a receiver to become desensitized (to experience a reduced sensitivity) to the desired signals. The symptom of a desensitized receiver is a reduction in the receiving distance. Some receivers allow you to configure a higher receive threshold level. This feature enables you to intentionally reduce the sensitivity and therefore reduce the intensity of the overloading. This feature is similar to a “squelch” control on an FM two-way radio.

It can be difficult for you to compare receiver selectivity and to predict overload resistance because most manufacturers do not publish overload specifications. Keep the following general guidelines in mind as you evaluate wireless equipment:

- Wireless equipment that is designed for outdoor WAN use should be less susceptible to being overloaded when compared to indoor wireless LAN equipment.
- Wireless equipment that is designed for indoor LAN use is likely to be more susceptible to being overloaded when used outdoors.
- All wireless equipment might need to have an external bandpass filter added when there are one or more strong, nearby transmitters such as FM, AM, or television broadcast transmitters.

Multipath Resistance

Multipath fading is a fact of life at microwave frequencies. *Multipath* is caused when signal reflections cause several signals (echoes) to be received almost simultaneously. Equipment features that minimize the effects of multipath include the following:

- **Antenna diversity**—Antenna diversity helps minimize multipath by using two separate antennas. The antennas are separated from each other, and when the signal fades, one antenna receives a stronger signal than the other antenna. The receiver automatically selects the strongest antenna signal on each incoming packet, so fading is reduced.
- **Circular antenna polarization**—Circularly polarized antennas discriminate against multipath interference. Equipment that offers the option of using a circularly polarized antenna provides more protection against multipath compared to equipment without a circularly polarized antenna.
- **OFDM**—Equipment that uses orthogonal frequency division multiplexing modulation provides more immunity to multipath interference compared to non-OFDM equipment.

Multipath interference is worse in a physical environment where you find many obstacles that reflect wireless signals. The center of a city with many tall, flat, reflective metal building surfaces is a high multipath environment. If you plan to deploy wireless service in a high-multipath environment, use as many multipath-reduction features and techniques as possible.

Miscellaneous Interference Reduction Techniques

There are many sources of noise and interference besides multipath. The following miscellaneous features help reduce the distance-robbing effects of noise and interference:

- **Selectable antenna polarization**—Interference from other wireless systems is usually either vertically polarized or horizontally polarized. Equipment that allows you to select either vertical or horizontal polarization allows you to minimize interference from other systems by selecting polarization opposite to other, interfering networks.
- **Smart antenna technology**—Smart antennas enable the antenna pattern beamwidth to be automatically adjusted under software control. In this way, the antenna pattern can be automatically steered to minimize or avoid interference. Smart antenna technology is a relatively new technology that is just beginning to appear in license-free wireless WAN equipment.
- **Smart radio features**—Smart radio features include the radio's capability to automatically scan the available frequencies and to choose the frequency with the least amount of interference. Automatic power adjustment is another smart radio feature. The wireless equipment measures the strength and the quality of the received signal and adjusts the transmit power level up or down to maintain the desired link quality. Using only the amount of power needed minimizes the interference to other wireless systems.

Physical Layer Wireless Security Features

There are a number of physical layer wireless security features as well as many higher-layer security features. The following sections describe the main physical layer security features.

Antenna Pattern/Signal Strength

Although not immediately obvious, antenna directivity provides a certain measure of security. Unauthorized wireless users must physically position themselves in an area where a usable signal exists. This is another reason to carefully consider where you radiate your signal. Rather than broadcasting it everywhere, use directional antennas to radiate only into the areas where your end users are located.

Modulation Type

Like antenna directivity, modulation type is a not-so-obvious security feature. If a wireless network uses DSSS, a hacker must use the same DSSS modulation type. Likewise, if a network uses FHSS, a hacker must use FHSS. If a network uses another proprietary modulation type, an unauthorized user must use the same proprietary modulation type. Therefore, proprietary modulation types provide a higher level of physical layer security than 802.11b, for example.

Network ID (SSID, ESSID)

Several different logical networks can exist in the same physical space. Wireless packets contain a service set identifier (SSID), extended service set identifier (ESSID), or network ID to specify the logical network that a wireless station belongs to. The ESSID is a basic network security feature. If a wireless station does not possess the correct ESSID (or network ID), it cannot connect to a wireless network.

Miscellaneous Wireless Features

This section describes miscellaneous transmit and receive features. Although these features cannot be neatly classified into a specific section, their presence or absence can play a significant role in the performance of your wireless network operation; evaluate them carefully.

Miscellaneous Transmit Features

The following miscellaneous transmitter features can affect the design and performance of your wireless WAN:

- **Transmitter output power**—Most license-free wireless equipment is limited by Federal Communications Commission (FCC) regulations to one watt (+30 dBm) of transmitter output power. Available transmitter output power levels typically vary from 1 watt (1W) down to 200 mW, 100mW, 50 mW, and 30 mW.

TIP The role of transmitter power in the successful operation of a wireless network is often misunderstood. Many people believe that more power is always better; however, this is not true in many cases. Your best approach is to transmit with only the amount of power that you need to cover your desired service area. Transmitting with too much power results in a transmitting range that is larger than your receiving range. This causes unnecessary interference to other networks. The owner of the other networks might then feel the need to retaliate with excessive transmitter power, which can lead to a cycle of escalation in which everyone loses.

- **Configurable transmitter power control**—A few models of wireless equipment allow you to configure the transmitter output power; however, for most wireless equipment, the power output is not configurable. Only one or two equipment models exist where the AP automatically configures the transmitter power of the end user nodes. The purpose of automatic power control is to use only the power needed for a reliable link. Avoiding the use of excessive power minimizes interference between the end user nodes.

Miscellaneous Receive Features

The following receive features affect the performance of your wireless WAN in many ways:

- **Receiver threshold**—A receiver starts working (receiving and decoding an incoming signal) when the signal reaches the receiver threshold level. Signals below the threshold are either not received or are received with numerous errors. Signals above the threshold are received with a low error rate. The low error rate allows the wireless link to deliver maximum throughput. If you are comparing two different receiver thresholds, the receiver with the lower threshold receives over a longer distance. For example, a receiver with a –85 dBm threshold is better than a receiver with a –80 dBm threshold.

NOTE When comparing receiver thresholds, compare the threshold values at the same data rate. Comparisons at different data rates are invalid because as the data rate goes up, a receiver's threshold goes up. Stated another way, as the data rate goes up, the receiver becomes less sensitive.

- **Noise figure**—Receivers create noise in their circuitry. *Noise figure* refers to internal noise or the relative lack of internal noise created by the receiver. The lower the internal noise, the better a weak signal is received. A 3-dB noise figure is better than a 6-dB noise figure, for example.

Miscellaneous Transmit/Receive Features

The following features, when present, apply on both transmit and receive:

- **AP and bridge**—Some wireless APs can be used either as an AP (connecting to many end users) or as a bridge. An AP with bridging capability provides you with more network flexibility than an AP without the capability to work as a bridge.
- **AP and repeater**—Most APs can serve both as an AP and as a repeater at the same time.
- **Number of wireless ports**—Most wireless equipment has one wireless port. Some equipment has more than one wireless port. Multiport equipment can operate simultaneously on more than one frequency or more than one band. One example is an AP that has one 2.4-GHz and one 5-GHz wireless port.
- **External antenna connector**—Wireless WAN equipment must always be connected to an antenna that has LOS paths to the end users. Except in the case of CPE that has the radio integrated with the antenna, this means that the wireless equipment must have a connector for an external antenna. Equipment that is designed to be used indoors often lacks a connector for an external antenna.

- **Split (indoor/outdoor) hardware architecture**—Indoor/outdoor architecture splits the wireless hardware. The microwave part of the equipment is placed outdoors, near the antenna. The low-frequency part of the equipment is placed indoors. The two halves of the radio are connected with either coax or fiber. With a split architecture, coax cable losses between the microwave section and the antenna are almost eliminated, consequently improving the wireless performance.
- **Integrated antenna/radio**—With increasing frequency, wireless equipment (especially 802.11b) equipment is becoming available with the radio physically located inside the antenna. Integrated equipment has the same advantage as split-architecture equipment—eliminating transmission line losses to improve wireless performance. The connection from the antenna/radio to the end user network is made with Ethernet cable. Power-over-Ethernet (PoE) to the antenna and radio is provided using the nondata conductors in the Ethernet cable.
- **Multifrequency management commonality**—A few equipment vendors now offer a wireless equipment family that operates on different frequency bands but can be managed from a common management platform. This equipment provides management economies for those wireless ISPs that need to deploy wireless systems on different bands.
- **Antenna alignment aids**—Some equipment, especially split architecture or integrated antenna and radio equipment, provides visual or aural antenna alignment aids. These aids, typically a series of LEDs or an audible tone, help the installer align the antenna for the highest signal level without leaving the antenna location.
- **Availability of FCC-certified antenna systems**—Most equipment vendors provide at least one antenna system that is FCC-certified for use with the equipment. Some vendors provide a number of certified antenna systems. The more vendor-certified antenna systems are available, the more flexibility you have to use an antenna system that provides the service-area coverage that you need.

Data Link Layer Features

The sections that follow describe features that operate at the data link layer.

Bridging Features

Bridging takes place at the data link layer and is based on the MAC addresses of the end user equipment. The typical wireless bridge contains a table of MAC addresses and bridge ports. Packets are forwarded to the correct bridge port based on the MAC address table information. Your data link layer feature evaluation includes the following features.

MAC Address Table Size

The MAC address table of a wireless bridge is finite in size. The table might be large enough to contain one or two thousand MAC addresses or small enough to contain only one. In most cases, the MAC address table size is larger than the number of simultaneous end user connections.

Number of Simultaneous Connections

Each wireless AP or bridge is designed to connect to only a specific number of end users at the same time. In general, the more simultaneous users it supports, the higher the cost of the wireless bridge or AP.

TIP Sometimes, an equipment vendor's advertising confuses the MAC address table size with the number of simultaneous end user connections. For example, an advertisement might state that one AP can support up to 1000 users. The ad might fail to mention that only 128 of the users can be connected at the same time. This type of error can be caused by an error on the part of the person preparing the advertisement. This person might be unclear about MAC address table size versus the number of simultaneous connections. If you see claims like this that appear to be excessive or too good to be true, ask the vendor to confirm that the advertised information is correct.

A wireless bridge is designed to support many wireless users, typically from 50 to several hundred. One special type of wireless bridge is called an *Ethernet converter*. Originally, an Ethernet converter was designed to bridge between one Ethernet port (on one computer) and a wireless WAN. Currently, Ethernet converters are available that support bridging between up to eight computers and the wireless WAN. This expanded Ethernet converter is called a *super Ethernet converter (SEC)*.

Spanning Tree Protocol

Most wireless point-to-point bridges implement the 802.3 Spanning Tree Protocol. In bridged networks, it is important to avoid routing loops (more than one simultaneous path). The 802.3 Spanning Tree Protocol senses the presence of routing loops and disables one route to avoid looping.

Switching

Wireless APs occasionally contain a built-in switch. The switch allows Ethernet connectivity from the AP to a number of Ethernet devices without needing to purchase an external switch.

Support for VLAN Tagging

Virtual LAN (VLAN) tagging allows the definition of a VLAN, as opposed to a geographically located LAN. Support for VLAN tagging allows the wireless device to support the operation of a VLAN.

MAC Sublayer Features

The MAC layer is a sublayer of the data link layer (Layer 2) in the OSI reference model. MAC features can be either standards-based or proprietary. In all cases, the primary purpose of the MAC sublayer is to provide reliable data delivery over the inherently noisy and collision-prone wireless medium. The MAC sublayer performs the following general functions:

- **Error control**—The MAC sublayer implements a frame-exchange protocol with an acknowledgment procedure. This procedure maximizes the chance that every packet is delivered error free across the wireless link.
- **Congestion management**—The MAC sublayer works to minimize congestion on the wireless medium. The MAC sublayer utilizes several methods to determine which station is allowed to gain access to the wireless medium. The 802.11b MAC specifications contain both a CSMA/CA contention-based access scheme and a polling-based access scheme. Most 802.11b equipment does not implement the polling feature.
- **Packet aggregation**— The MAC sublayer can maximize throughput by aggregating several small packets together into one larger packet. This reduces the number of times the wireless equipment must switch back and forth between receive and transmit (the switching time is also called the *turnaround time*), thereby making more time available to pass data traffic.
- **Data protection**—Encryption (in general) can take place at several different layers; however, WEP encryption takes place at the MAC level. 64-bit and 128-bit WEP encryption schemes are in common use.

Data Link Layer Security Features

The following sections analyze data link layer security features that might be offered by the equipment that you are evaluating.

MAC Address Access Control Lists

When providing wireless Internet access, it is desirable to deny access to any end user whose account is not current or who is not authorized to use your network. Most APs allow you to configure an access control list (ACL). Unless the ACL contains the specific MAC address of an end user, that end user will not be allowed to connect to the AP.

Protocol Filtering

Protocol filtering permits you to deny bridging based on the Layer 2 packet protocol. Protocols such as IPX, NetBEUI, DECNet, or AppleTalk can be denied.

MAC Address Pair Filtering

In bridged networks, it is occasionally desirable to provide filtering for specific address pairs. The filtering can either allow a connection between two specific MAC addresses, or it can deny a connection between two specific MAC addresses.

Authentication

Authentication is the process that a network uses to determine if an end user is allowed to connect to the network. Authentication schemes require an exchange of management frames between the authenticator (the network) and the end user who is requesting network access. Simple authentication schemes provide minimal security, whereas more complex schemes provide higher levels of security.

Several network layers are typically involved in the authentication process; however, because Layer 2 plays a prominent role, authentication is outlined here.

Open-system authentication is the least secure; it simply requires a station to identify itself to an AP and request that it be granted authentication.

A more secure authentication system is shared-key authentication using WEP. The shared key is distributed to all stations that are authorized to use the network. The stations use the shared key to respond to challenge text sent to them by the AP. If a station responds to the challenge text correctly, the AP grants network access.

A more secure authentication system is based on one of the 802.1x authentication types defined in the Extensible Authentication Protocol (EAP). EAP is defined in RFC 2284 and includes a number of different authentication methods. 802.1x requires using three entities:

- A supplicant (the station requesting authentication)
- The authenticator (typically the AP)
- The authentication server (such as a Remote Authentication Dial-In User Service [RADIUS] server)

EAP implementations typically allocate a new encryption key each time a wireless user begins a new session. A number of wireless vendors provide proprietary authentication features that are based on EAP and 802.1x. In the future, 802.11i wireless standards will likely evolve out of the current 802.1x standards.

Encryption

Sending an unencrypted packet over the air increases the chances that an unauthorized person could intercept and decode the packet. A variety of encryption schemes make it harder for this to occur. In addition to WEP encryption (already described), other available encryption schemes include the following:

- **Data Encryption Standard (DES)**—A 64-bit encryption standard with a user-selected encryption key.
- **Triple DES (3DES)**—Uses three 64-bit keys. The first key encrypts the data, the second key decrypts the data, and the third key re-encrypts the data.
- **Advanced Encryption Standard (AES)**—The most current U.S. Government-approved encryption standard. It uses a Rijndael (pronounced "rain-doll") algorithm with either a 128-bit, 192-bit, or 256-bit encryption key. AES requires a math coprocessor; therefore, it might not be compatible with existing 802.11b hardware. The upcoming 802.11i standard includes AES.

Data Link Layer Proprietary Security Features

Some currently available wireless products contain a combination of proprietary Layer 2 security features and industry-standard security. It is beyond the scope of this chapter to list these product combinations here; however, they include combinations of encryption, per-session key exchange, and frame authentication to provide high levels of security.

Network Layer Features

Routing takes place at the network layer. All wireless equipment currently available performs bridging; however, some models of wireless equipment also perform routing. Just as there is a wide range of routing features available with conventional (wired) routers, there is also a wide range of features available with wireless routers.

NOTE Later in this chapter, there is an additional discussion of the advantages and disadvantages of selecting wireless equipment that includes routing.

Routing Features

The following sections contain descriptions of some of the routing protocols and features that are often available in wireless routers.

Static IP Routing

Every wireless router includes static IP routing. Static routing enables you to configure permanent IP routes.

Dynamic IP Routing

Some wireless routers include dynamic IP routing. These routers support one or more dynamic routing protocols. The most common of these supported protocols include the following:

- **Routing Information Protocol (RIP) v1 and v2**—RIP is an interior routing protocol. It is a distance-vector metric protocol that routes packets based on the number of routing hops needed to reach the destination. RIP is relatively easy to implement, but it does not take into account the bandwidth of each hop.
- **Open Shortest Path First (OSPF)**—OSPF is also an interior routing protocol. It is a link-state metric protocol. OSPF routes packets based on the shortest distance, the least delay, and the most bandwidth available to reach the destination.

Dynamic Host Configuration Protocol Server

A Dynamic Host Configuration Protocol (DHCP) server allows the allocation and reuse of IP addresses as end users need them. The DHCP server allocates an address when a DHCP client logs on. When the client logs off, the IP address is returned to the address pool, ready to be reused when another client logs on.

Network Address Translation

Like DHCP, Network Address Translation (NAT) expands the pool of usable IP addresses. NAT allows the use of a pool of private nonroutable IP addresses within a network. When IP traffic needs to be routed over the Internet, NAT translates the nonroutable addresses to an Internet-routable address.

Point-to-Point Protocol over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) allows an ISP to authenticate end users. Some wireless routers support PPPoE by passing PPPoE packets to the PPPoE server.

Bandwidth Management

Wireless equipment occasionally includes bandwidth management features. This allows the bandwidth available to and from each MAC or IP address to be throttled or limited to a

specified level. This feature allows you to manage your total available bandwidth, to offer different service levels to different groups of end users, and to serve more end users. Some equipment allows end user bandwidth to be throttled at different speeds in different (downstream and upstream) directions.

NOTE Some wireless routers allow you to allocate bandwidth based on either the IP address of the end user or the MAC address of the end user.

Quality of Service (QoS)

Quality of service functionality is not one, but a set of features that work together to prioritize different service levels for different users. One use, for example, is to prioritize the handling and thereby reduce the latency for voice over IP (VoIP) packets.

Roaming

Roaming is the ability of an end user to move from AP to AP within the same subnet while maintaining a network connection. 802.11b APs usually include roaming capabilities. The vast majority of wireless WANs provide service to fixed end user locations; therefore, roaming is not used. If you need to design or deploy a wireless WAN that includes roaming, you should evaluate the following:

- **Reassociation speed**—The length of time it takes for an end user to be switched from one AP to another.
- **Tunable parameters**—Any other AP parameters that are designed specifically to enable smooth roaming.
- **Compatibility issues**—AP-to-AP communication standards are not specified in 802.11b. If you anticipate building a network that supports roaming, you should plan to buy all of your APs from the same vendor.

Network Layer Security Features

The following network layer security features are often available on wireless routers.

IP Address Access Control Lists

Some wireless routers allow specific IP addresses to be included in an ACL. Addresses in the list can either be denied or allowed network access.

Firewalls

Wireless routers sometimes contain firewall features. These features allow traffic to flow outward from a local network to the Internet. Traffic flowing inward from the Internet to the local network is filtered or blocked.

Virtual Private Networks

Virtual private network (VPN) features include IP Security (IPSec) encryption capabilities and tunneling capabilities, such as the Point-to-Point Tunneling Protocol (PPTP).

Application Layer Features

Application layer features play a significant role in the network design, configuration, management, monitoring, and security of your wireless network.

Network Design

Many factors of network design, including terrain, distance, buildings, trees, and the presence of other networks, influence the design of your network. Sometimes, relatively expensive tools (such as spectrum analyzers) are needed to assist during the network design process. Sometimes, however, inexpensive tools are available to help you with network design.

Some wireless LAN equipment vendors include site survey utility software along with their wireless equipment. These usually display signal strength, noise level, signal-to-noise ratio (SNR), and signal quality information. Although these utilities are often designed for indoor use, they are useful to show you how well a signal from your AP is being received at different locations within your desired outdoor coverage area. These utilities are also useful for antenna alignment. Sometimes, low-cost (or free) hardware-specific utilities are available that function like a low-cost spectrum analyzer. Although these low-cost utilities do not have the full range of regular spectrum analyzer features, they do cover the entire 2.4-GHz band and show which channels are in use by other networks.

Network Management

Network management system (NMS) capabilities vary widely between different models of wireless equipment. Look for some of the following features:

- **Access method**—Methods used to access the NMS include serial port access, telnet access, generic Windows browser access, and proprietary Windows-based software. Generic browser access is probably the easiest method to use.

- **Wireless link statistics**—An NMS that provides statistics for each individual wireless link in a point-to-multipoint system is important to allow effective network monitoring. At a minimum, the following statistics should be available for each end user link and each AP: signal strength, noise level, and percentage of packets that need to be retransmitted.
- **Graphical usage statistics**—Make network management easier. You can identify light or heavy traffic patterns, perform usage-based billing based on either IP or MAC address, and see when bandwidth usage peaks.
- **Simple Network Management Protocol (SNMP)**—SNMP-based NMSs are fairly standard today. Some wireless equipment uses proprietary management software; however, many third-party management programs can manage SNMP-based systems.
- **Antenna-alignment utilities**—Generate wireless link traffic and allow the system administrator to see real-time statistics while turning the antenna to receive the highest signal.
- **Flood ping capability**—Floods a network with ping packet traffic. This test allows the system administrator to test the wireless link while simulating a traffic load.

Application Layer Security Features

The capability to interface with Remote Authentication Dial-In User Service (RADIUS) servers is possibly the most important Layer 7 security feature for wireless equipment.

Major Network Feature Decisions

Your network feature decisions have a major impact on the equipment that you choose to purchase and on the success and profitability of your wireless WAN. The following sections describe those decisions.

Market Versus Equipment Cost

The market that you choose to serve—commercial, residential, or some mixture of the two—largely determines the price range for the wireless equipment that you purchase, install, and resell. If you serve primarily residential users, you need to purchase lower-cost equipment. If you provide higher-value service by providing more bandwidth and additional value-added services to businesses, you can select higher-cost equipment with a larger feature set.

802.11b Compatibility—Yes or No?

If you choose to use 802.11b equipment for your wireless WAN, you gain some significant advantages and, at the same time, you face several disadvantages. The following sections discuss these advantages and disadvantages.

Advantages of 802.11b Compatibility

The advantages of using 802.11b equipment include the following:

- **Cost**—802.11b equipment is available at the lowest cost of any wireless equipment.
- **Availability**—802.11b equipment is widely available.

NOTE At the time of this writing, 802.11a equipment that is operating in the 5-GHz U-NII bands (with bandwidths up to 54 Mbps) is beginning to become available. This equipment is currently designed for use in indoor LANs and not in outdoor WANs. Further product development might make outdoor versions available in the future.

Disadvantages of 802.11 Compatibility

The disadvantages of using 802.11b equipment outdoors include the following:

- **Security**—Although newer security mechanisms are being developed to supplement the current wired equivalent privacy (WEP) security, there is a somewhat greater chance of security being compromised because many people are familiar with 802.11b technology and more hacking tools are available.
- **Interference**—As more 802.11b APs are deployed, spectrum congestion and interference between wireless networks become more of an issue.
- **Support**—Most 802.11b equipment sold today is designed for low-cost in-home use. The level of vendor support for this equipment is likely to be low, especially when the equipment is used in an outdoor WAN environment. Vendors focus on supporting the equipment in its intended (indoor LAN) use and not in the outdoor WAN environment.

Bridged Versus Routed WANs

Every wireless WAN is interconnected with a wired network that includes routing. During the design phase of your wireless WAN, you need to determine how your WAN will interoperate with your wired network. Based on your determinations, you will select wireless equipment that either performs bridging only or that performs both bridging and routing. The following questions can help you decide whether to purchase wireless equipment with built-in routing or whether to use external routers (or perhaps, no routers):

- **IP-based network services**—What advanced IP-based network services are already provided in your existing wired network? What IP-based network services will you need to provide immediately over your wireless network when it is first placed into service? What additional IP-based services (such as voice-over-IP) will you want to offer later to your wireless network users?
- **Edge routing**—Relative to your existing core routers, where do you need edge routing? If edge routing is (or will soon be) needed, is it better to select wireless equipment that includes this routing functionality initially, or is it better to select wireless bridges and add external routers later between a customer's wireless bridge and their LAN?
- **Multiple wireless backbone links**—If you anticipate using multiple wireless backbone links to provide extended wireless area coverage, you are more likely to deploy routing within the wireless backbone. You might decide that selecting wireless equipment with built-in routing is more practical or economical than using external routers.

Backbone Feature Decisions

Your backbone supplies the bandwidth that your APs distribute wirelessly to your end users. The following sections describe some key decisions that you will make as you select backbone equipment.

Backbone Capacity

Your first backbone decision is to determine how much throughput you need. This throughput decision is affected by the following factors:

- **Market needs**—How much throughput do your markets require? A backbone link that serves businesses located in several cities needs to provide more throughput than a link that serves only one or two small residential areas.
- **Number of users**—The number of wireless end users and the nature of their needs determine the amount of throughput that your backbone needs to provide.
- **Simplex versus duplex backbone**—Backbone equipment can be either simplex or duplex. A duplex backbone can provide up to 50 percent more throughput than a simplex backbone. Duplex backbone costs are generally higher because a duplex link contains two complete transmitting systems and two complete receiving systems.
- **Overselling ratio**—Internet usage is bursty. Most Internet users use bandwidth intermittently; therefore, ISPs can oversell bandwidth knowing that not all users will be on all the time. The number of times that you resell the same bandwidth (your overselling ratio) affects the amount of backbone bandwidth that you need. Your ISP experience combined with your observation of the usage patterns on your network help you determine your best overselling ratio and your backbone bandwidth needs.

Wired Versus Wireless Backbone

If economical wired backbone connectivity is available at your wireless AP location, it makes sense for you to use that wired connectivity. If wired backbone connectivity is not available or if the cost is too high, a wireless distribution system is the logical choice.

License-Free Versus Licensed Backbone

After you choose to use a wireless backbone, it is important for you to evaluate and compare the cost and the bandwidth of licensed wireless backbone equipment with the cost and the bandwidth of license-free wireless backbone equipment.

The advantages of using a license-free wireless backbone are

- **Cost**—The cost is generally lower.
- **Availability**—Equipment is generally available more rapidly.
- **Licensing**—There is no licensing cost, licensing paperwork, or licensing delay.

The disadvantage of using a license-free wireless backbone is that interference from other license-free networks is a possibility, and it is your responsibility to ensure that license-free equipment does not interfere with licensed equipment.

Given these advantages and disadvantages, it makes sense to use a license-free wireless backbone if you are reasonably certain that interference levels (both from other networks and from your own network) will remain reasonably low.

Dedicated Versus Shared Backbone Bandwidth

Wireless backbone links can be either of the following:

- Dedicated to providing only backbone bandwidth.
- Shared between backbone bandwidth and last-mile bandwidth. Examples of shared bandwidth include mesh networks and 802.11b repeaters that both connect end users and provide backbone connectivity for other APs.

Heavy bandwidth demands at one AP can cause slow performance at other APs. If possible, try to avoid sharing wireless link bandwidth between backbone use and last-mile access use. If you choose to share backbone bandwidth, you might find it necessary to use additional routers throughout the backbone to allocate and manage the bandwidth demands.

AP Feature Decisions

The list that follows describes some of the key decisions that you need to make as you select your AP equipment:

- **Frequency band**—Your choice of frequency band is probably the most important equipment decision that you will make. The difference in wireless propagation characteristics and interference levels between the license-free bands means that a poor decision here might result in an unusable network. Before making this decision, you should review the propagation characteristics of each band (discussed earlier in this chapter). You should also perform a wireless site survey (see Chapter 4, "Performing Site Surveys") to determine potential interference levels on a frequency band before you select equipment for that band. The information in Chapter 8 can help you if you find high levels of interference.
- **NLOS environment**—If you are considering buying equipment that operates in an NLOS environment, you need to either rule out or verify the range claims that the equipment manufacturer has made. You can do this by visiting an ISP that has the equipment deployed in an NLOS environment that is similar (such as the same density of trees and the same type of obstructions) to yours.
- **Modulation type**—Your choice of modulation type (DSSS, FHSS, or proprietary) is an important factor in the ultimate success of your network. Choose a modulation type that is compatible with the level and the type of interference in your coverage area.
- **802.11b or proprietary**—Every organization needs to match its budget to its mission. If your budget is modest, the lowest-cost indoor 802.11b equipment might be your only choice. A somewhat larger budget allows you to choose higher-cost 802.11b equipment with expanded feature and management capabilities. An even larger budget allows you to choose from the full range of wireless equipment.
- **Hot spot use**—802.11b APs deployed for hot spot use should be 802.1x-capable to implement improved security and to interface to external authentication and accounting servers.
- **End user polling**—Some APs implement end user polling as an option to the 802.11b CSMA/CA and RTS/CTS collision-avoidance mechanisms. If you plan to serve more than about 25 busy end users from one AP, polling increases your network reliability and performance.
- **Bandwidth management**—A few APs contain a bandwidth management capability that allows you to set bandwidth for each end user link. If the AP that you choose does not include this feature, consider adding this capability with an external bandwidth manager.
- **Support**—Vendor support is important when your wireless customers are looking to you to provide reliable Internet service. Talk with other wireless network operators to assess the availability of driver and firmware upgrades, as well as the response time and quality of support from their equipment vendors.

CPE Feature Decisions

Price is often the top consideration in the selection of CPE. The competition between broadband DSL and cable Internet access providers has driven the cost of broadband service down. It can be difficult for broadband wireless companies to compete at these low price points. For this reason, wireless providers constantly seek to lower the cost of CPE. Business users usually understand that they need to pay for value received; in contrast, residential users often seek to pay little (or nothing) for their CPE. Try not to cut too many corners in seeking and deploying low-cost CPE. Although cost is important, it is more important to deploy reliable, supportable, and manageable networks. The following discussion can help you make these cost-benefit decisions:

- **Wireless card versus external radio-based CPE**—Traditionally, license-free broadband wireless equipment is mounted indoors with a coaxial cable running to the outdoor antenna. In the drive to minimize CPE costs, wireless IPSs often choose to install wireless network interface cards (NICs) in their customers' computers, rather than purchase full-size (and higher priced) wireless bridges or routers. If you choose to deploy NICs in customer computers as CPE, recognize that some customers might expect you to provide no-cost PC support indefinitely, and this can be a costly situation for you. Also, be aware that the software tools needed to adequately monitor the quality of the customers' connection might not be available. This, too, can increase your customer support costs and raise your costs above the level where you can make a reasonable profit.
- **Separate versus integrated radio and antenna**—An alternative to the traditional wireless model is the integrated radio and antenna model. To reduce CPE costs and installation costs, wireless ISPs are now using (wherever possible) integrated radio and antenna equipment. These integrated units combine the radio and the antenna into one plastic or fiberglass enclosure that is mounted outdoors in a location with an LOS path to the AP. The integrated unit connects to the end user PC or network through either an Ethernet cable or, in a few cases, through a universal serial bus (USB) connection. The wireless performance is better because there is no coaxial cable loss between the antenna and the radio.
- **Split radio architecture**—There is one additional equipment configuration for you to evaluate: the split architecture. Split architecture actually divides the wireless unit into two physical pieces: an indoor section and an outdoor section. The indoor section contains the lower-power, lower-frequency circuits. The outdoor section contains the higher-power, higher-frequency circuits and mounts just below the antenna. Split architecture provides the benefits of the integrated radio and antenna architecture but also allows a greater choice of antennas because the antenna and radio are not built into one unit. Split architecture is often the most expensive configuration; however, it might be the best in terms of both performance and flexibility.

Wireless Network Card Decisions

If you decide to deploy wireless 802.11b cards as the customer CPE or if wireless cards plug into the AP that you are using, you must evaluate the following wireless card characteristics:

- **Transmitter**—Outlined earlier in this chapter; wireless cards share these same characteristics. The key characteristic is transmitter power output. The ideal transmitter would have a power output of 100 to 200 mW with a software-configurable power level.
- **Receiver characteristics**—Also outlined earlier, the better the receiver sensitivity (when combined with good selectivity), the better your wireless system performance will be.
- **External antenna connector**—An antenna is the key element in any wireless system. A wireless card needs to have a connector that allows an external antenna to be attached.
- **Form factor**—The most frequently used wireless card form factor is PCMCIA; however, other form factors are sometimes used. These other form factors include industry-standard architecture (ISA), peripheral component interconnect (PCI), and Compact Flash (CF).

Mesh Network Feature Decisions

You can evaluate mesh network equipment using the same considerations that you do for all other wireless equipment. Keep the following differences in mind, however:

- **Network deployment process**—Deploying a mesh network is different from deploying a point-to-multipoint network. Every mesh network node serves as a repeater and relay point for other network nodes. Nodes that are located farther away from the Internet connection must be relayed through closer network nodes. Before distant nodes can be deployed, nodes must be deployed closer to the Internet node. To provide coverage to an entire geographical area, the area must be *seeded*. Some nodes must be installed initially even if no end user is available to pay for the cost of the node.
- **Bandwidth and throughput limitations**—Mesh networks share backbone bandwidth with last mile bandwidth, which can reduce the amount of bandwidth to each end user. Be sure to factor this throughput limitation into your evaluation process and into your business plans.
- **Maximum hop limitations**—The multihop nature of mesh networks increases network latency and reduces network throughput. You will be limited to a maximum number of hops, so be sure to factor this limitation into your business plan.

Wireless Equipment Environmental Decisions

Remember environmental considerations when evaluating wireless equipment:

- **Operating temperature range**—All wireless equipment is designed to operate correctly between certain specified temperatures. Indoor equipment is designed to operate within a narrower temperature range than outdoor equipment. If you choose to use indoor equipment outdoors, be sure to provide cooling for it in the summer. In severe winter climates, it might also be necessary to add a heat source to keep the equipment warm.
- **Radio frequency (RF) immunity**—Many models of broadband wireless equipment are not designed to be used in a high-level RF environment. For example, locating a wireless LAN AP designed for home use in the equipment vault of a mountaintop transmitter site can lead to operating failures. The high-power transmitter energy can either come down the antenna cable and overload the AP receiver, or the energy can pass through the plastic case of the AP and disrupt the AP operation. If you plan to deploy equipment like this, plan to use an external bandpass filter in the antenna system. Also plan to mount the AP in a shielded and grounded metal equipment case. As an alternative, you can select equipment designed for high-RF environments. This equipment is usually designed for mounting in a standard 19-inch metal equipment rack.

Wireless Amplifier Feature Decisions

Wireless network operators often add external bidirectional amplifiers to their wireless systems. *External* means that the amplifier is external to the wireless equipment. Bidirectional amplifiers actually contain two amplifiers: one to amplify the transmitter signal and one to amplify the incoming received signals.

In the United States, FCC regulations require that external power amplifiers be marketed and sold only as part of a complete legally certified radio-cable-amplifier-antenna combination. The purpose of this regulation is to minimize the use of illegal overpowered equipment. Excess transmitter power raises the noise level, increases interference, and makes it harder for other, legal networks to operate correctly. Unfortunately, some wireless WAN operators ignore this regulation and intentionally use external power amplifiers in violation of FCC regulations. This behavior can result in heavy fines and equipment confiscation and also decreases the usability of the license-free bands for everyone.

NOTE Illegal amplifier use is not the answer to making your WAN operate over longer distances. Often, a power amplifier actually decreases the receiving range of your WAN. In addition, using illegally high transmitter power causes substantial interference to other network operators who are operating legally. Finally, if illegal amplifier use increases, the FCC might be forced to step in with new, more restrictive regulations that could reduce license-free operating privileges for everyone. Resist the urge to amplify. Proper wireless network design and proper antenna system design provides you with the best network performance.

The following sections explain how external amplifiers work and how to use these amplifiers properly.

Transmit Amplification

On transmit, an external amplifier increases the transmitter power that reaches the antenna. This is useful when the power output of the transmitter is low and the cable length between the wireless equipment and the antenna system is long. Without an amplifier placed at the antenna, the high cable loss results in little signal reaching the antenna.

Here is an example of the correct way to use an amplifier. Start with a transmitter that has an output of 50 mW (+17 dBm). If the antenna cable has a loss of –14 dBm, the power reaching the antenna system is (+17 dBm – 14 dBm) = 3 dBm (2 mW). This is a low level of transmit power. If an amplifier with +14 dB of gain is added at the antenna, the +3 dBm that reaches the amplifier is amplified by +14 dB, resulting in a total of (3 dBm + 14 dB) +17 dBm (50 mW) reaching the antenna. The amplifier has added back the power that was lost in the antenna cable.

Receiver Amplification

On receive, an external amplifier mounted at the antenna performs two functions:

- It helps to overcome the signal loss that occurs in the antenna cable.
- It sets the SNR of the receiving system.

These two functions can lead to a small improvement in receiver performance if the amplifier has a good, low-noise design. In addition, a properly designed antenna should be used with the amplifier. If the antenna system design is poor, the amplifier can actually reduce the receiving range of the system.

Up/Down Converters

Up/down converters translate wireless signals from one frequency band to another. If the 2.4-GHz band is crowded in your area and the 5.8-GHz band is less crowded, you might want to use a 2.4-to-5.8 converter. Here is how this works. Each AP and end user station is equipped with a converter. Then, the following occurs:

- During transmit, each 2.4-GHz transmit signal is upconverted (translated up in frequency) to the 5.8-GHz band.
- During receive, the 5.8-GHz signal from the other station is downconverted to the 2.4-GHz band.

Using lower-cost 2.4-GHz equipment, communication actually takes place on the less crowded 5.8-GHz band. The advantage of this approach is that it usually costs less than buying more expensive equipment for 5.8 GHz. The disadvantage of this approach is that only a few manufacturers supply frequency converters, so your choice is limited. Converters need to be mounted at the antenna.

Compatibility Issues

Several compatibility issues can reduce the reliability of your network and consume troubleshooting time. If you are deploying an 802.11b network, never assume that different brands of wireless cards and wireless APs will work reliably together. Even hardware that is wireless fidelity (WiFi)-certified sometimes has firmware, software, operating system, and feature differences that can result in certain equipment combinations that do not work together. In most cases, equipment manufacturers do not cause these issues intentionally. There have, however, been a few instances in which large equipment vendors have intentionally created incompatibilities to boost the sales of their equipment and hinder the sale of lower-cost competitive equipment.

Watch for the folowing incompatibility issues:

- **Operating system software**—New features might not work with older software versions, or older features might not work in newer software versions. This situation can require that you upgrade all your wireless equipment software simultaneously.
- **NIC firmware**—Upgrades might have features that do not work even though they did work in earlier versions. NIC firmware might work when matched with older versions of AP software but not with upgraded AP software versions.
- **MAC incompatibilities**—Different brands of equipment that should work together do not work together or some of the features do not work.
- **NIC drivers**—Drivers might not be available for your OS or, if available, they might not be upgraded to work with newer versions of your OS.
- **USB**—There might be incompatibilities between wireless USB devices and certain PC operating systems.

- **Network management**—Network management software and diagnostics software can be unavailable or can be limited in their capability to manage mixed-equipment networks.
- **Timing**—Equipment that has timing designed for indoor (several hundred foot) distances might not work outdoors at longer (several mile) distances.

Here are some of the things that you can do to minimize the loss of time and money caused by these incompatibilities:

- **Standardize**—As much as possible, standardize on one brand of equipment for your APs and your CPE. Minimize the mixing and matching of different wireless equipment brands that talk to the same AP. Using a different brand of equipment is fine for wireless backhaul links; however, the fewer types of AP/CPE equipment that you use, the more efficiently you will be able to support that equipment and the more reliable your service will be.
- **Test time**—Be sure to plan for enough test time between the time that you build an AP and the time that you begin service from that AP. The more dissimilar your equipment, the more test time you need.

Wireless Support Issues

The quality of support from wireless vendors varies widely and ranges from excellent to none. In addition, technology changes rapidly; new software, new hardware, new firmware, and new drivers constantly become available. To maximize your chances of receiving effective support, do the following:

- **Research**—During your equipment research process, be sure to visit other organizations that have deployed the equipment you are considering. Ask the organizations to comment about the quality of vendor support they are receiving, including warranty support.
- **Realistic approach**—There still is no free lunch. Be realistic with your support expectations. You deserve to be notified by your vendor when equipment problems are discovered. You should rightfully expect that your vendor would not discontinue support for equipment that you have purchased; however, after your warranty period has expired, it is not unreasonable for a vendor to charge for software upgrades or new and improved hardware. Expect to pay a reasonable amount to receive a high level of continuing vendor support. You need your equipment vendor to make a profit so that it will continue to be there when you need it.
- **Support groups**—A number of online support groups are available for specific brands of wireless equipment. Find a discussion group for your equipment and join it, if possible, even before you purchase your equipment. You, your end users, and the entire industry will benefit from this helpful and friendly sharing of information.

Review Questions

1. Why is it important to visit an actual deployment site before you purchase wireless equipment?
2. The electromagnetic waves that we call wireless exist at what layer of the seven-layer OSI reference model?
3. How is a packet like a hamburger sandwich?
4. Why does a wireless network need a big MAC?
5. Wireless bandwidth and wireless throughput are the same thing. True or false?
6. The communications range under NLOS conditions is about the same as the communications range under LOS conditions. True or false?
7. DSSS equipment hops from frequency to frequency. True or false?
8. Other things being equal, the higher the data rate, the shorter the communications distance. True or false?
9. If you start receiving interference from another network, the best thing to do is to get an amplifier. True or false?
10. Any 802.11b equipment works with any other 802.11b equipment. True or false?