Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**6**

**Wireless Networking**

* [Chapter Introduction](javascript://)
* **6-1**[Characteristics of Wireless Transmissions](javascript://)
  + **6-1a**[The Wireless Spectrum](javascript://)
  + **6-1b**[Channel Management](javascript://)
  + **6-1c**[Antennas](javascript://)
  + **6-1d**[Signal Propagation](javascript://)
* **6-2**[802.11 WLAN Standards](javascript://)
  + **6-2a**[802.11 Innovations](javascript://)
  + **6-2b**[Access Method](javascript://)
  + **6-2c**[Association and Wireless Topologies](javascript://)
  + **6-2d**[IEEE 802.11 Frames](javascript://)
* **6-3**[Implementing a Wi-Fi Network](javascript://)
  + **6-3a**[Determine the Design](javascript://)
  + **6-3b**[Configure Wi-Fi Connectivity Devices](javascript://)
  + **6-3c**[Configure Wi-Fi Clients](javascript://)
* **6-4**[Wi-Fi Network Security](javascript://)
  + **6-4a**[WPA (Wi-Fi Protected Access)](javascript://)
  + **6-4b**[WPA2 (Wi-Fi Protected Access, Version 2)](javascript://)
  + **6-4c**[Personal and Enterprise](javascript://)
  + **6-4d**[Other Security Configurations](javascript://)
  + **6-4e**[Security Threats to Wi-Fi Networks](javascript://)
* **6-5**[Troubleshooting Wi-Fi Networks](javascript://)
  + **6-5a**[Wi-Fi Network Tools](javascript://)
  + **6-5b**[Avoid Pitfalls](javascript://)
* **6-6**[Chapter Review](javascript://)
  + **6-6a**[Module Summary](javascript://)
  + **6-6b**[Key Terms](javascript://)
  + **6-6c**[Review Questions](javascript://)
  + **6-6d**[Hands-On Projects](javascript://)
  + **6-6e**[Capstone Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Introduction

### Objectives

After reading this module and completing the exercises, you should be able to:

* **1**Describe characteristics of wireless transmissions
* **2**Explain 802.11 standards and innovations
* **3**Plan a Wi-Fi network
* **4**Secure a Wi-Fi network
* **5**Troubleshoot a Wi-Fi network

**On the Job**

I’ve installed wireless network equipment for the past 15 years. Our company builds and repairs computers and installs wireless networks and surveillance systems in office buildings, warehouses, and homes. We work with both directional wireless and open-space, broadcast wireless.

When installing a wireless AP, we’re always careful to take note of any device specifications, such as the AP’s range, and we must consider what obstacles are in the device’s line of sight. We evaluate any walls, ceilings, and other obstacles that come in between the source of the wireless signal and the various locations of receiving devices, such as printers, computers, and cell phones.

One installation comes to mind that really baffled us. It was an older home here in Dalton, Georgia, and was built around the early 1900s.

The house wasn’t huge, and we installed an AP in the kitchen area. We initially tested the signal in the kitchen and, as expected, received four bars of signal strength. Next, we walked into the living room, which was just on the other side of the wall from the kitchen. In the living room, however, we barely received one bar.

We put in a higher wattage output AP and upon repeating the test, we still just received 1 bar in the living room. As part of our investigation, we went into the attic and discovered that this wall between the kitchen and the living room was built of plaster instead of sheetrock. Further investigation revealed that underneath the plaster was a layer of chicken wire. A little research revealed that in the old days, some walls incorporated chicken wire in the internal structure to hold the plaster against the wall. This wall was like a fortress, blocking our wireless signal.

We installed a second AP in another room to solve the problem. The moral to this story is, when installing wireless, beware of what an impact a single wall can have, especially in older homes.

**Scott Merritt, Service Mgr.**

**Dalton Computer Services, Inc.**

For decades, radio and TV stations have transmitted analog signals through the air. Air provides an intangible means of transporting data over networks and is often used in conjunction with wired technologies.

This module first looks at how wireless transmissions work, regardless of the type of wireless technology used. These wireless characteristics apply to satellite, Bluetooth, Wi-Fi, cellular, and other wireless signals. Some of these wireless signals, such as satellite and cellular, can travel long distances and will be discussed in more detail later in this course. This module explores how to set up, manage, secure, and troubleshoot local wireless networks that you might find in an enterprise setting or that you might set up in your own home.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 6-1Characteristics of Wireless Transmissions

### Certification

* 1.2

Explain the characteristics of network topologies and network types.

* 2.1

Compare and contrast various devices, their features, and their appropriate placement on the network.

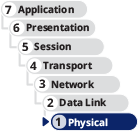
* 2.4

Given a scenario, install and configure the appropriate wireless standards and technologies.

* 5.4

Given a scenario, troubleshoot common wireless connectivity issues.

Average reading time: 30 minutes



In previous modules, you learned about signals that travel over a physical medium, such as a copper or fiber-optic cable. LANs that transmit signals through the air via RF (radio frequency) waves are known as WLANs (wireless local area networks). Wireless transmission media is now common in business and home networks and necessary in some specialized network environments such as IoT (Internet of Things). Wired and wireless signals share many similarities, including use of the same layer 3 and higher protocols, for example. However, the nature of the atmosphere makes wireless transmission vastly different from wired transmission at lower OSI layers. You’ll start by looking at what wireless signals are, and then you’ll study how they’re transmitted.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1aThe Wireless Spectrum

All wireless signals are carried through the air by electromagnetic waves. The [**wireless spectrum**](javascript://), commonly called the airwaves, is the frequency range of electromagnetic waves used for data and voice communication. As defined by the FCC (Federal Communications Commission), which controls its use, the wireless spectrum spans frequency ranges or [**bands**](javascript://) between 9 kHz and 300 GHz. (Recall that a Hz or hertz is one cycle per second.) [Table 6-1](javascript://) lists from low to high the frequency ranges commonly used for wireless network connections and data transfer. Many of these technologies are covered in this module or later in this course. Others are briefly described next. Notice in the table that several of the bands cover a frequency range that is further subdivided into channels. Some bands have only a single frequency, called a fixed frequency, for that band.

**Table 6-1**

### Frequency ranges of wireless technologies listed from low to high frequencies

| **Technologies** | **Frequency range (band) in kHz, MHz, or GHz** | **Description** |
| --- | --- | --- |
| RFID | 125 kHz–134.2 kHz | The lowest of several frequency ranges for RFID and approved for global use |
| NFC | 13.56 MHz | Fixed frequency |
| Z-Wave | 90.842 MHz | Fixed frequency |
| Cellular | 824 MHz–896 MHz | Commonly called the 800 band |
| RFID | 858 MHz–930 MHz | One of several bands assigned to RFID |
| Cellular | 1850 MHz–1990 MHz | Commonly called the 1900 band |
| Wi-Fi: 802.11b/g/n/ax | 2.4 GHz–2.4835 GHz | 11 or 14 20-MHz channels |
| ZigBee | 2.4 GHz–2.4835 GHz | 16 channels |
| Bluetooth | 2.4 GHz–2.4835 GHz | 79 channels |
| RFID | 2.446 GHz–2.454 GHz | Highest frequency range for RFID |
| ANT+ | 2.457 GHz | Fixed frequency |
| Wi-Fi: 802.11a/n/ac/ax | 5.1 GHz–5.8 GHz | 24 20-MHz channels or  (802.11n and above)  12 40-MHz channels or  (802.11ac and above)  6 80-MHz channels or  2 160-MHz channels |
| Wi-Fi:  802.11ax (Wi-Fi 6E) | 5.925 GHz–7.125 GHz | 59 20-MHz channels or  29 40-MHz channels or  14 80-MHz channels or  7 160-MHz channels |
| IR | 300 GHz–300,000 GHz | 10 channels plus 4 near-infrared channels |

Enlarge Table

The following list gives a brief explanation of the wireless technologies in [Table 6-1](javascript://) that are not covered elsewhere in this course. Most of these technologies are used for various purposes in supporting [**IoT (Internet of Things)**](javascript://) networks, which include a wide range of devices not normally considered to be a computing device. Due to the diverse nature of IoT devices and purposes, many kinds of wireless technologies are employed to better serve the needs of these connections:

* [**RFID (Radio Frequency Identification)**](javascript://) uses electromagnetic fields to store data on a small chip in an RFID tag, which includes an antenna that can both transmit and receive, and possibly a battery. The tag holds 1–8 KB of data, such as a serial number, credit card information, or medical data, which it can transmit to a nearby reader. RFID is commonly used for inventory management. Because the tag does not need to be precisely positioned close to the reader, an employee can quickly scan a shelf of several items to determine what’s in stock and what needs to be re-ordered without having to scan each individual item. An RFID tag might also be embedded in the customer’s credit card, allowing for so-called “contactless” payment.
* [**NFC (near-field communication)**](javascript://) is a form of RFID and transfers data wirelessly over very short distances (usually 10 cm or less). A tiny antenna embedded in the device sends its radio signal at a fixed frequency of 13.56 MHz. The signal can also be transmitted in one direction by an NFC tag, or smart tag, such as when employees need to access a secure area of a building. Other uses of NFC tags include ticketing, cashless payment, shopping loyalty or membership programs, identification, data sharing, and PC logon capabilities. NFC tags, such as the ones shown in [Figure 6-1](javascript://), require no power source other than the receiving device’s power field. The NFC tag collects power from the smartphone or other device by magnetic induction, which is a form of wireless power transmission. Once power is introduced to the NFC tag by the receiving device’s proximity, the tag transmits its data. They can be programmed to transmit stored data, launch apps, direct a browser to a web page, or change device settings. This makes them useful even for casual, personal use, such as changing your phone’s settings when you pass through your front door at home or when you get into your car.

* **[Z-Wave](javascript://)** is a smart home protocol that provides two basic types of functions: signaling to manage wireless connections, and control to transmit data and commands between devices. A Z-Wave network controller, called a hub, receives commands from a smartphone or computer and relays the commands to various smart devices on its network. Devices on the network are identified by a 1-byte Node ID, and the entire network has a 4-byte Network ID. Multiple Z-Wave networks can coexist in the same space because the Network ID prevents communication outside of a device’s Z-Wave network. Z-Wave transmissions offer a range of up to 100 m per hop, and they can tolerate up to four hops through repeaters. Z-Wave–controlled devices can serve as repeaters on a Z-Wave mesh network.
* Based on the 802.15.4 standard, [**ZigBee**](javascript://) is a low-powered, battery-conserving wireless technology. It is designed to handle small amounts of data and is therefore ideal for use in ISM (industrial, scientific, and medical) sensors. ZigBee is also used in IoT devices for purposes such as building automation, HVAC control, AMR (Automatic Meter Reading), and fleet management. The protocol is known for its relative simplicity and reliability when compared to other technologies such as Bluetooth, and its level of security, which is accomplished using 128-bit AES encryption.
* [**Bluetooth**](javascript://), defined by IEEE 802.15.1 specifications, is named after a medieval king of Denmark named Harald Bluetooth, who fought to merge several Danish tribes under a single government. Like its namesake, Bluetooth technology unites separate entities—such as mobile devices, PCs, and accessories—under a single communications standard. Bluetooth operates in the radio band of 2.4 GHz to 2.4835 GHz and hops between frequencies within that band (up to 1600 hops/sec) to help reduce interference. Most Bluetooth devices require close proximity to form a connection, with the exact distance requirements depending on the class of Bluetooth device.
* [**ANT+**](javascript://) (pronounced ant plus) technology is based on the ANT protocol, which is an ad hoc wireless protocol operating at about 2.4 GHz. This is one less acronym to learn, as the term ANT simply refers to the insect, which is small in size and a tenacious worker. The ANT protocol was originally developed in 2004 by ANT Wireless, a division of Dynastream Innovations. The company is currently owned by Garmin. While ANT+ is a proprietary protocol, it is also open source and therefore used by many manufacturers in addition to Garmin. ANT+ gathers and tracks information from sensors that are typically embedded in heart rate monitors, GPS devices, and other activity monitoring devices. Garmin’s smartwatches, for example, track an athlete’s activity levels and geographic movement, and then wirelessly sync this data to the person’s smartphone, computer, and web-based accounts such as Strava (a social media site for athletic activities) or Facebook. Unlike Bluetooth, ANT+ can also sync data from multiple devices for the same activity, such as a smartwatch, smartphone, bicycle computer (like the one shown in [Figure 6-2](javascript://)), or fitness equipment such as a treadmill.

* **[IR (infrared)](javascript://)** technology has found new life in the world of IoT, where it’s used primarily to collect data through various sensors. IR is also commonly used in remote controls such as the one that comes with the projector shown in [Figure 6-3](javascript://). Infrared standards are defined by the IrDA (Infrared Data Association) at the website [irda.org](http://irda.org/" \t "_blank). IR exists just below the spectrum that is visible to the human eye, with longer wavelengths than red light. Because it’s a form of light, IR requires a nearly unobstructed [**LOS (line of sight)**](javascript://) between the transmitter and receiver—some devices use a scatter mode that reflects IR signals off nearby surfaces in order to circumvent some obstacles, but IR cannot pass through these obstacles. This limitation can actually be used to increase the security of IR transmissions. An LED in a device creates the invisible radiation, which is then detected by a sensor’s semiconductor material that converts the signals into electrical current. IR sensors are used to collect information such as the following:
  + Presence or level of liquid, based on the quality of a reflection
  + Variations in reflections from skin caused by variations in blood flow, which can be used to monitor heart rate
  + Proximity to the device, which can trigger an action such as steering a vehicle away from an obstacle
  + Commands from a control device, such as a game or TV remote control

**Figure 6-1**

These programmable NFC tags have sticky backs for attaching to a flat surface like a wall, desk, or car dashboard



**Figure 6-2**

A cycling computer can track location, speed, elevation, and more



Enlarge Image

[iStock.com/piola666](http://istock.com/piola666" \t "_blank)

**Figure 6-3**

This remote control contains an IR transceiver to communicate with the projector

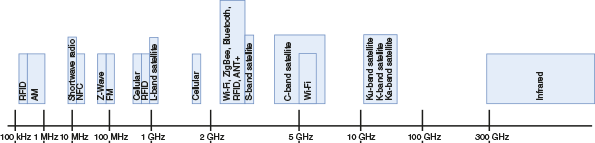


Enlarge Image

[Figure 6-4](javascript://) shows where these bands fit in the wireless spectrum. Frequency bands used for AM, FM, and satellite communications are included in [Figure 6-4](javascript://) for comparison and to show where potential overlap of signals might occur.

**Figure 6-4**

The wireless spectrum



Enlarge Image

Notice in [Figure 6-4](javascript://) that Wi-Fi, Bluetooth, ZigBee, ANT+, as well as some satellite signals share the frequency ranges around 2.4 GHz. How do these technologies share these airwaves without one signal interfering with another? Let’s explore how channels are managed to reduce interference caused by overlapping channels.

**Note 6-1**

The airwaves are considered a natural resource. In the United States, the FCC grants organizations in different locations exclusive rights to use each frequency and specifies which frequency ranges can be used for what purposes. Other countries have similar regulatory agencies to manage the impact of transmitted signals on airwave availability for public, private, and government use. The ITU (International Telecommunication Union) is a United Nations agency that sets standards for international telecommunications including wireless frequency allocations and satellite orbits. Some bands can only be used with a license (for example, a band devoted to television, FM, AM, or ham radio). Others, such as Wi-Fi bands and CB (citizens band) radio, are available for public use without a license so long as radios using these bands conform to restrictions on the signal transmission strength. In the case of Wi-Fi, this means you can own and use a consumer-grade Wi-Fi device without acquiring a license granted by the FCC to use the band.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1bChannel Management

A band used by a wireless device is defined by its overall frequency range. To allow multiple devices to share the same band, the band is subdivided into channels, and channels are further subdivided into narrowband channels. Most wireless devices implement one of two technologies to take advantage of the frequencies within its band to avoid interference:

* [**FHSS (frequency hopping spread spectrum)**](javascript://)—A short burst of data is transmitted on a particular frequency within the band, and the next burst goes to the next frequency in the sequence. Frequency hopping can happen hundreds of times a second. FHSS is cheaper to implement than DSSS and performs better than DSSS in crowded, indoor environments.
* [**DSSS (direct sequence spread spectrum)**](javascript://)—Data streams are divided and encoded into small chunks, called chips, which are spread over all available frequencies within one of three wide channels, all at the same time. The process of dividing and encoding the data is called chipping, and the spreading ratio used to transform the data is called the chipping code, which is unique to each device. DSSS uses the available bandwidth more efficiently than FHSS and tends to have a higher throughput.

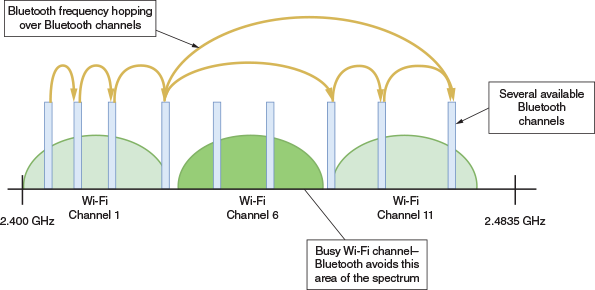
Here’s a breakdown of how each wireless standard in the 2.4 GHz range uses its allotted band; you’ll learn more about each of these standards later in this module:

* Wi-Fi, commonly used for wireless Internet access, uses DSSS. In the United States, the FCC has defined 11 channels within the 2.4-GHz band for Wi-Fi and 24 channels in the 5-GHz band. (Other countries might have 14 Wi-Fi channels for the 2.4-GHz band.) In the United States, each channel is 20 MHz wide. A Wi-Fi [**AP (access point)**](javascript://), which is the central connectivity device for Wi-Fi clients on a network, is manually configured to use a selected group of channels. Wi-Fi client devices scan the entire band for active channels.
* Bluetooth, commonly used to connect wireless personal devices, uses FHSS to take advantage of the 79 channels allocated to the Bluetooth band. In a network of Bluetooth devices (called a piconet), one device is designated the master and provides a clock the other devices use to coordinate their channel hopping. Because Bluetooth transmissions are constantly hopping channels, interference and collisions are less likely to cause significant problems.
* ZigBee, commonly used in ISM (industrial, scientific, and medical) devices, uses DSSS and 16 channels.

Even with the frequency spread of FHSS or DSSS to avoid interference, collisions can still happen. Each technology has a procedure to follow when it senses a collision. For example, when a Bluetooth device senses a collision with a Wi-Fi channel, it backs off using the frequencies in that Wi-Fi channel for a short time, giving Wi-Fi the opportunity to finish its transmission, as shown in [Figure 6-5](javascript://). Wi-Fi devices use a “listen before transmit” strategy to find a silent channel. More details about how Wi-Fi handles collisions are covered later in the module.

**Figure 6-5**

Bluetooth frequency hopping avoids a busy Wi-Fi channel



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

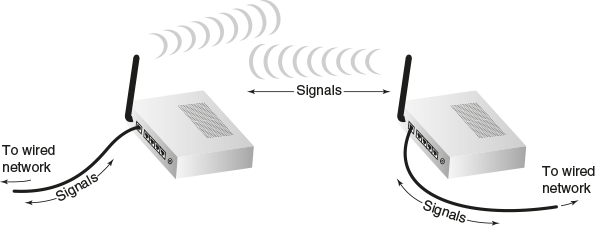
## 6-1cAntennas

The air provides no fixed path for signals to follow, so signals travel without guidance. Contrast this to wired media, such as STP or fiber-optic cable, which do provide a fixed signal path. The lack of a fixed path requires wireless signals to be transmitted, received, controlled, and corrected differently than wired signals. Part of this work is done at a hardware level.

Just as with wired signals, wireless signals originate from electrical current traveling along a conductor. The electrical signal travels from the transmitter to an antenna, which then emits the signal as a series of electromagnetic waves into the atmosphere. The signal moves through the air and eventually reaches (or rather, passes) its destination. At the destination, another antenna detects the signal going by, and a receiver converts it back to current. [Figure 6-6](javascript://) illustrates this process.

**Figure 6-6**

Wireless transmission and reception



Enlarge Image

Notice that antennas are used for both the transmission and reception of wireless signals. As you might expect, to exchange information, two antennas must be tuned to the same frequency so they can communicate on the same channel. Thus, each type of wireless service requires an antenna specifically designed for that service. The service’s specifications determine the antenna’s power output, frequency, and radiation pattern. An antenna’s [**radiation pattern**](javascript://) describes the relative strength over a three-dimensional area of all the electromagnetic energy the antenna sends or receives. Radiation patterns can be used to classify antennas into two basic categories:

* [**Directional antenna**](javascript://) (also called a unidirectional antenna)—Issues wireless signals along a single direction. This type is used when the source needs to communicate with one destination, as in a point-to-point link or in a specific area. A satellite downlink (for example, the kind used to receive digital TV signals) uses directional antennas.
* [**Omnidirectional antenna**](javascript://)—Issues and receives wireless signals with (somewhat) equal strength and clarity in all directions, although in the real world, an omnidirectional antenna is never perfectly balanced. This type is used when many receivers or mobile receivers must be able to pick up the signal in many directions. TV and radio stations use omnidirectional antennas, as do most towers that transmit cellular signals and most mobile devices.

The geographical area that an antenna or wireless system can reach is known as its [**range**](javascript://). Receivers must be located within a transmitter’s range to receive accurate signals consistently. Even within an antenna’s range, however, signals may be hampered by obstacles and rendered unintelligible. Choosing the correct type of antenna for the application can help solve the problem.

Typical users might not put much thought into a wireless device’s antenna, as the antenna is usually attached directly to the device or even embedded within it (such as with a smartphone or laptop). However, network technicians need to be more aware of what antennas devices have, and they also need some basic knowledge on other types of antennas and how to work with them.

Consider a situation where you need to transmit high volumes of data wirelessly between two segments of your network. In addition to connecting multiple nodes within a LAN, wireless technology can be used to connect two different parts of a LAN or two separate LANs. Such connections might use a fixed link with directional antennas between two access points, as shown in [Figure 6-7](javascript://).

**Figure 6-7**

An outdoor unidirectional antenna that transmits across a nearby football field



Because point-to-point links must transmit in only one general direction, they can apply more energy to signal propagation through a unidirectional antenna. This allows them to achieve a greater transmission distance than mobile wireless links can offer. For example, access points connecting two WLANs could be located up to 1000 feet apart.

When using a separate antenna, such as the one you see in [Figure 6-7](javascript://), keep in mind that you must use cabling to connect the antenna to the network, and in many cases, antennas use coax cable. However, Wi-Fi and similar wireless signals will rapidly degrade over even a few feet of coax cable. This attenuation, or signal loss, over the antenna cable typically necessitates placing a network access point in close vicinity to the antenna.

You can determine the gain or loss of an access point attached to an external antenna by considering initial power output of the AP, signal loss along the antenna cable (attenuation), and signal gain from the antenna itself—which is measured in dBi (decibels relative to isotrope) and is a theoretical ratio used to measure antenna performance. This overall calculation is referred to as [**EIRP (effective isotropic radiated power)**](javascript://) and is measured in dBm (decibels relative to one milliwatt). Now that you understand the components, you can see that the formula for this calculation is simple addition and subtraction:

Of course, the AP’s and antenna’s performance aren’t the only factors that determine the quality of the signal received by the client. The wireless client’s own antenna, distance to the wireless client, and noise in the environment all affect the power of the received signal. [**RSSI (received signal strength indicator)**](javascript://) measures in dBm the power of the signal on the receiver’s end. The scale used for this measurement varies by manufacturer, but typically, because RSSI is shown as negative numbers, closer to 0 is better. [Table 6-2](javascript://) shows relative RSSI levels commonly used.

**Table 6-2**

### RSSI levels

| **RSSI (dBm)** | **Rating** | **Effect** |
| --- | --- | --- |
| −30 dBm | Excellent | Typically only achieved when the client is very close to the AP. |
| −50 dBm | Good | Provides reliable delivery of time-sensitive data, such as with VoIP or streaming video. |
| −70 dBm | Acceptable | Minimum required for reliable data delivery. |
| −80 dBm | Not good | Minimum required for basic connectivity. |
| −90 dBm | Unusable | Will experience difficulty establishing a connection. |

In a project at the end of this module, you’ll have the opportunity to measure RSSI for Wi-Fi networks in your area. For now, let’s see what kinds of environmental factors can affect the drop in power between transmission and reception.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1dSignal Propagation

[**Propagation**](javascript://) refers to the way in which a wave travels from one point to another. Ideally, a wireless signal would travel directly in a straight line from its transmitter to its intended receiver. This straight-line propagation, known as LOS (line of sight), maximizes distance for energy used and results in reception of the clearest possible signal. However, because the atmosphere is an unguided medium and the path between a transmitter and a receiver is not always clear of obstacles, wireless signals do not usually follow a straight line.

**Note 6-2**

Satellite and infrared transmissions require a clear line of sight. However, some signals might be blocked in what appears to be a clear line of sight. For example, many energy-efficient windows are covered with a film that filters out certain layers of sunlight. Even though you can see through the window, a satellite signal, such as an XM radio satellite signal, might not be able to get through.

When an obstacle stands in a signal’s way, the signal might pass through the object, it might be absorbed by the object, or it might be subject to any of the following phenomena, depending upon the object’s geometry and its constituent materials:

* **Attenuation**—As with wired signals, wireless signals also experience attenuation. After a signal is transmitted, the farther it moves away from the transmission source, the more it weakens. Similar to wired transmission, wireless signals can be amplified by increasing the power of the transmission or extended by repeating the signal from a closer broadcast point using a repeater (also called a [**wireless range extender**](javascript://)), such as the one designed for a home network shown in [Figure 6-8](javascript://).

* **[Fading](javascript://)**—As a signal runs into various obstacles, its energy will gradually fade, which causes the strength of the signal that reaches the receiver to be lower than the transmitted signal’s strength. Excessive fading can cause dropped connections or slow data transmission.
* [**Interference**](javascript://)—Electromagnetic waves in the atmosphere can interfere with wireless communications similar to how EMI (electromagnetic interference) affects wired transmissions. Because wireless signals cannot depend on a conduit or shielding to protect them from extraneous EMI, they are more vulnerable to noise than wired transmissions are. The proportion of noise to the strength of a signal is called the [**SNR (signal-to-noise ratio)**](javascript://). Signals traveling through areas in which many wireless communications systems are in use—for example, the center of a metropolitan area—are the most apt to suffer from interference and, therefore, will exhibit a lower SNR than signals traveling through a relatively clear environment.
* [**Refraction**](javascript://)—As a wave travels into and through a different transmission medium, such as when traveling through glass or other solids, the wave’s direction, speed, and wavelength are altered, or refracted. Imagine how light waves are altered when entering the water in a pool. If you’re underwater looking back at the surface, the image you see is distorted.
* [**Reflection**](javascript://)—The wave encounters an obstacle and reflects, or bounces back, toward its source. A wireless signal will bounce off objects whose surface dimensions are large compared with the signal’s average [**wavelength**](javascript://) (the distance from the crest of one wave to the crest of the next wave). In the context of a wireless LAN, whose wavelengths are approximately 12 cm, such objects include walls, floors, ceilings, and the Earth—anything with a large, flat surface. In addition, signals reflect more readily off conductive materials, such as metal, than off insulators, such as concrete.
* [**Scattering**](javascript://)—When a wireless signal encounters an object that has small surface dimensions compared with the signal’s wavelength, it’s diffused or scattered in multiple directions. Scattering is also related to the roughness of the surface a wireless signal encounters. The rougher the surface, the more likely a signal is to scatter when it hits that surface. In an office building, objects such as chairs, books, plants, and computers cause scattering of wireless LAN signals. For signals traveling outdoors, precipitation such as rain and mist also cause scattering.

* **[Diffraction](javascript://)**—A wireless signal is diffracted, or split into secondary waves, when it encounters an obstruction. The secondary waves continue to propagate generally in the direction in which they were split. If you could see wireless signals being diffracted, they would appear to be bending around the obstacle. Objects with sharp edges—including the corners of walls and desks—cause diffraction.

**Figure 6-8**

Wi-Fi range extender

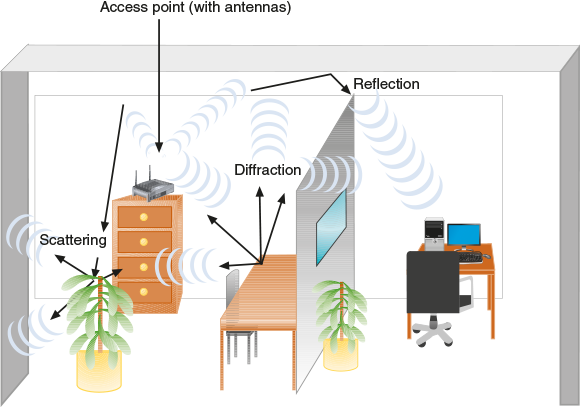


Jill West

Wireless signals follow many different paths to their destination. Such signals are known as multipath signals. [Figure 6-9](javascript://) illustrates multipath signals caused by reflection, scattering, and diffraction.

**Figure 6-9**

Multipath signal propagation



The multipath nature of wireless signals is both a blessing and a curse. On one hand, because signals bounce off obstacles, they have a better chance of reaching their destination. The downside to multipath signaling is that, because of their various paths, multipath signals travel different distances between their transmitter and a receiver. Thus, multiple instances of the same signal can arrive at a receiver at different times. This might cause signals to be misinterpreted, resulting in data errors. Error-correction algorithms detect the errors, and sometimes the sender must retransmit the signal. The more errors that occur, the slower the throughput.

Many standards have been developed to account for—and even take advantage of—the various characteristics of wireless transmissions. The best known is IEEE’s 802.11 standards, also known as Wi-Fi. Let’s look more closely at these core standards for wireless networks.

**Remember This…**

* Explain what a WLAN is.
* Describe regulatory impacts of wireless bands and channels.
* Compare directional and omnidirectional antennas.
* Explain EIRP and RSSI.

**Self-Check**

1. Which of the following statements is false?

Answer

* 1. Each Wi-Fi channel contains multiple frequency bands.
  2. Wi-Fi functions on two different frequency bands.
  3. Each Wi-Fi channel contains multiple frequencies.
  4. Wi-Fi spreads its data across all available frequencies within a wide channel.

1. Which of the following statements is true?

Answer

* 1. A satellite dish receives signals equally from any direction.
  2. A fish aquarium full of clear water won’t negatively affect a Wi-Fi signal.
  3. A Wi-Fi client connects to a range extender that connects to an AP.
  4. A smartphone always directs its signal toward the closest cell tower.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 6-2802.11 WLAN Standards

### Certification

* 1.2

Explain the characteristics of network topologies and network types.

* 2.1

Compare and contrast various devices, their features, and their appropriate placement on the network.

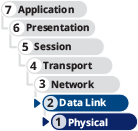
* 2.4

Given a scenario, install and configure the appropriate wireless standards and technologies.

* 4.2

Compare and contrast common types of attacks.

Average reading time: 29 minutes



WLANs define operations at OSI layers 1 and 2. Just like wired LANs, they support the same TCP/IP higher-layer OSI protocols (such as IP, TCP, and UDP) you’re already familiar with. This compatibility ensures that wireless and wired transmission methods can be integrated on the same network.

The most popular OSI physical and data link layer standards used by WLANs are popularly referred to as Wi-Fi. [**Wi-Fi (wireless fidelity)**](javascript://) is a collection of wireless standards and their amendments, extensions, and corrections developed by IEEE’s 802.11 committee. Notable wireless standards developed by the IEEE 802.11 committee and its task groups are 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.

The 802.11 standards employ various technologies at the physical layer. In addition, 802.11n and later standards modify the way frames are used at the MAC sublayer, which, as you’ve already read, is the lower portion of the data link layer that is specifically involved with managing MAC addresses in message frames. Recall that layer 2’s other sublayer is the LLC sublayer, which is primarily concerned with multiplexing, flow and error control, and reliability.

[Table 6-3](javascript://) summarizes the technical details of the 802.11 standards. The following list gives a more detailed description of each standard.

**Table 6-3**

### Technical details for 802.11 wireless standards

| **Standard** | **Frequency band** | **Maximum theoretical throughput** | **Geographic range** |
| --- | --- | --- | --- |
| 802.11b (Wi-Fi 1) | 2.4 GHz | 11 Mbps | 100 m |
| 802.11a (Wi-Fi 2) | 5 GHz | 54 Mbps | 50 m |
| 802.11g (Wi-Fi 3) | 2.4 GHz | 54 Mbps | 100 m |
| 802.11n (Wi-Fi 4) | 2.4 GHz or 5 GHz | 600 Mbps | Indoor: 70 m Outdoor: 250 m |
| 802.11ac (Wi-Fi 5) | 5 GHz | Wave 1 (3 data streams): 1.3 Gbps  Wave 2 (4 data streams): 3.47 Gbps  Wave 3 (8 data streams): 6.93 Gbps | Indoor: 70 m Outdoor: 250 m |
| 802.11ax (Wi-Fi 6 and Wi-Fi 6E) | 2.4 GHz or  5 GHz or  (Wi-Fi 6E only) 6 GHz | 9.6 Gbps | Indoor: 70 m Outdoor: 250 m |

Enlarge Table

### Exam Tip

In preparation for the CompTIA Network+ exam, memorize every detail shown in [Table 6-3](javascript://).

* **[802.11b](javascript://)**—In 1999, the IEEE released its 802.11b standard, which separates the 2.4-GHz band into 22-MHz channels. Among all the 802.11 standards, 802.11b was the first to take hold and has been retroactively dubbed Wi-Fi 1. It is also the least expensive of all the 802.11 WLAN technologies. However, most network administrators have replaced 802.11b with faster standards.
* [**802.11a**](javascript://)—Although the 802.11a task group began its standards work before the 802.11b group, 802.11a (now called Wi-Fi 2) was released after 802.11b. The higher throughput of 802.11a, as compared with 802.11b, is attributable to its use of higher frequencies, its unique method of modulating data, and more available bandwidth. Perhaps most significant is that the 5-GHz band is not as congested as the 2.4-GHz band. Thus, 802.11a signals are less likely to suffer interference. However, higher-frequency signals require more power to transmit, and they travel shorter distances than lower-frequency signals. As a result, 802.11a networks require a greater density of access points to cover the same distance that 802.11b networks cover. The additional access points, as well as the nature of 802.11a equipment, make this standard more expensive than either 802.11b or 802.11g. For this and other reasons, 802.11a is rarely preferred.
* [**802.11g**](javascript://)—IEEE’s 802.11g WLAN standard, now referred to as Wi-Fi 3, was designed to be just as affordable as 802.11b while increasing its maximum theoretical throughput with different data modulation techniques. In addition, 802.11g benefits from being compatible with 802.11b networks. This was a significant advantage at the time when network administrators were upgrading their wireless access points to the 802.11g technology while still needing to offer wireless access to older computers.
* [**802.11n**](javascript://)—In 2009, IEEE ratified the 802.11n standard, which is now named [**Wi-Fi 4**](javascript://). However, it was in development for years before that, and as early as mid-2007, manufacturers were selling 802.11n-compatible transceivers in their networking equipment. The primary goal of IEEE’s 802.11n committee was to create a wireless standard that provided much higher effective throughput than the earlier 802.11 standards, and they succeeded. 802.11n boasts a maximum throughput of 600 Mbps, making it a realistic platform for telephone and video signals. IEEE also specified that the 802.11n standard must be backward-compatible with the 802.11a, b, and g standards. This is made possible because 802.11n uses both the 2.4-GHz and the 5-GHz frequency bands.
* [**802.11ac**](javascript://)—Officially approved in early 2014, 802.11ac ([**Wi-Fi 5**](javascript://)) operates on the 5-GHz band and exceeds benchmarks set by earlier standards by increasing its useful bandwidth and amplitude. 802.11ac is the first Wi-Fi standard to approach Gigabit Ethernet capabilities, providing better support for more wireless clients at a time. In fact, 802.11ac access points function more like a switch than a hub in that they can handle multiple transmissions at one time over the same frequency spectrum. This standard was deployed in three waves, with each successive release offering higher speeds by using more data streams.

* **[802.11ax](javascript://)**—The most current Wi-Fi standard at the time of this writing is 802.11ax, commonly called [**Wi-Fi 6**](javascript://), which operates in both the 2.4 GHz and 5 GHz frequency ranges. Improvements include further development of modulation and multiuser technologies, which you’ll read about shortly, to increase data speeds and transmission distances. An interesting technique called BSS coloring also reduces interference from neighboring Wi-Fi networks. While theoretical maximum speeds for 802.11ax reach near 10 Gbps, actual speeds are expected to run only about 30–60 percent faster than actual Wi-Fi 5 speeds. More significantly, however, Wi-Fi 6 can support higher speeds for more network clients at the same time, which is particularly important for smart home environments with potentially dozens of IoT devices, or for a stadium or conference center environment with hundreds or thousands of Wi-Fi clients.
* [**Wi-Fi 6E**](javascript://)—Building on improvements of 802.11ax, Wi-Fi 6E will use the currently unlicensed 6 GHz frequency range. At a total of 1200 MHz, this range is wider than either the 2.4 GHz (70 MHz wide) or 5 GHz (500 MHz wide) ranges, allowing far more available channels and much higher speed transmissions but at shorter distances.

**Note 6-3**

The actual geographic range of any wireless technology depends on several factors, including the power of the antenna, physical barriers or obstacles between sending and receiving nodes, and interference in the environment. Therefore, although a technology is rated for a certain average geographic range, it might actually transmit signals in a shorter or longer range at various times under various conditions.

A more relevant measure of an AP’s performance in a particular environment is how well it saturates its range with a strong, fast signal. This is one of the primary advantages of 802.11ac and 802.11ax over 802.11n: The newer standards do a better job of providing faster transmissions throughout their geographic range. So, for example, at 75 m, the signal from an 802.11ac AP will be more effective than the signal from an 802.11n AP under the same conditions.

Regardless of the standard followed, all 802.11 networks share many features and innovations in common. For example, all 802.11 networks follow the same access method, as described in the following section. In addition, some newer innovations give the later standards a significant performance boost over earlier standards.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-2a802.11 Innovations

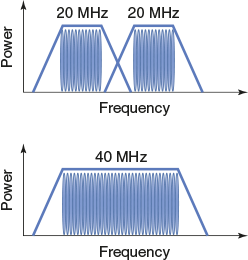
Although some of their physical layer services vary, all the 802.11 standards use half-duplex signaling. In other words, an antenna on a wireless node using one of the 802.11 techniques can either transmit or receive, but it cannot do both simultaneously unless the node has more than one transceiver installed. Some wireless access points can simulate full-duplex signaling by using multiple frequencies. But the transmission for each antenna is still only half-duplex.

Despite this physical limitation, beginning with 802.11n, several innovations have been implemented that contribute to making later 802.11 standards much faster and much more reliable:

* [**Channel bonding**](javascript://)—Beginning with 802.11n, two adjacent 20-MHz channels can be combined, or bonded, to make a 40-MHz channel, as shown in [Figure 6-10](javascript://). In fact, bonding two 20-MHz channels more than doubles the bandwidth available in a single 20-MHz channel. That’s because the small amount of bandwidth normally reserved as buffers against interference at the top and bottom of the 20-MHz channels can be assigned to carry data instead. Because the 5-GHz band contains more channels and is less crowded (at least, for now), it’s better suited to channel bonding than the 2.4-GHz band. The newer standards take channel bonding to a higher level by supporting 20-, 40-, and 80-MHz channels, with optional use of 160-MHz channels.
* [**MIMO (multiple input-multiple output)**](javascript://)—First available in 802.11n, multiple antennas on the access point and on a client device process incoming or outgoing data simultaneously. [Figure 6-11](javascript://) shows an 802.11n/802.11ac dual-band SOHO router with three antennas. There are some multiantenna 802.11g devices available, but these antennas take turns processing the data stream. 802.11n/ac devices, however, simultaneously process data through two or more antennas. As you learned earlier, wireless signals propagate in a multipath fashion. Therefore, multiple signals cannot be expected to arrive at the same receiver in concert. MIMO uses this phenomenon to its advantage by adjusting either the phase or amplitude of signals from each antenna. This improves the transmission in two ways:
  + **Signal quality and range**—Spatial diversity of the different antennas eliminates noise in the transmission, which also increases the distance it can effectively travel. Each antenna receives a slightly different version of the signal, and the strengths of each signal are summed.
  + **Signal capacity**—Spatial multiplexing adds a new data stream between each additional pair of antennas, thereby increasing the amount of data being transmitted and received. This effect increases linearly with the addition of each pair of antennas.
* [**MU-MIMO (multiuser MIMO)**](javascript://)—Related to MIMO, MU-MIMO is an even newer technology implemented by 802.11ac Wave 2 and newer products that allows multiple antennas to service multiple clients simultaneously. The antennas use different spatial streams that rely on clients being positioned relatively far apart from one another. This feature reduces congestion and thereby contributes to even faster data transmission. As with MIMO, however, a MU-MIMO access point can only be used at full capacity when the involved client devices also support MU-MIMO technology. In reality, MU-MIMO is currently only available for downstream (AP to client) transmissions and is rarely implemented in indoor environments where clients are located in close proximity to each other.
* [**OFDMA (Orthogonal Frequency Division Multiple Access)**](javascript://)—Improving upon an earlier technology called OFDM, OFDMA supports more efficient multiuser functionality for 802.11ax devices. In essence, OFDMA allows the 802.11ax AP to subdivide each channel into smaller frequency allocations for each client, such as 2 MHz or 4 MHz of each 20-MHz channel. The AP can then transmit multiple small frames to multiple clients at one time using parts of the channel.
* **Frame aggregation**—Beginning with 802.11n, networks can use one of two techniques for combining multiple data frames into one larger frame: A-MSDU (Aggregated Mac Service Data Unit) or A-MPDU (Aggregated Mac Protocol Data Unit). Both approaches combine multiple frames to reduce overhead. 802.11ac uses A-MPDU for all transmissions by default. 802.11ax continues to use A-MPDU but with additional enhancements that allow for more flexibility in choosing which frames can be aggregated. To understand how frame aggregation works, suppose three small data frames are combined into one larger frame. Each larger frame will have only one copy of the same addressing information that would appear in the smaller frames. Proportionally, the header fields take up less of the aggregated frame’s space. In addition, replacing four small frames with one large frame means an access point and client will have to exchange one-quarter the number of messages to negotiate media access and error control.

**Figure 6-10**

Channel bonding



**Figure 6-11**

Dual-band SOHO router with three antennas

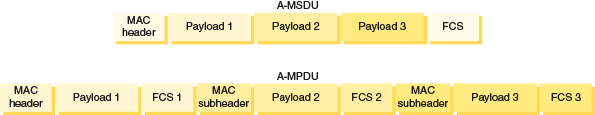


Source: [Amazon.com](http://amazon.com/" \t "_blank)

[Figure 6-12](javascript://) illustrates the lowered overhead accomplished by both A-MSDU and A-MPDU. The advantage of A-MSDU over A-MPDU is that more of the frame’s information is combined with other frames transmitted at the same time. The potential disadvantage to using larger frames is the increased probability of errors when transmitting larger blocks of data. Therefore, the advantage of A-MPDU is that each frame added to the mix retains some of its error checking data, resulting in greater reliability.

**Figure 6-12**

A-MSDU and A-MPDU aggregated frames



Enlarge Image

Note that not all the techniques listed here are used in every 802.11 implementation. Further, reaching maximum throughput depends on the number and type of these strategies used. It also depends on the band the network uses, environmental factors, and capabilities of wireless clients. Considering these factors, an 802.11 network’s actual throughputs vary considerably.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-2bAccess Method

You’ve learned that the data link layer, specifically the MAC sublayer, is responsible for appending physical addresses to a data frame and for governing multiple nodes’ access to a single medium. Like 802.3 (Ethernet), 802.11 appends 48-bit physical addresses to a frame to identify its source and destination. The use of the same physical addressing scheme allows 802.11 networks to easily blend with other IEEE 802 networks, including Ethernet (802.3) networks. However, 802.11 networks use a different access method than Ethernet networks do.

Wireless devices are not designed to transmit and receive simultaneously and so cannot prevent collisions. Instead, 802.11 standards specify the use of [**CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**](javascript://) procedures to access a shared medium. Compared with CSMA/CD (Carrier Sense Multiple Access with Collision Detection), CSMA/CA minimizes the potential for collisions, but cannot detect the occurrence of a collision and so cannot take steps to recover from the collisions that do occur. [Figure 6-13](javascript://) illustrates the basic process. The steps are as follows:

1. Step 1

Using CSMA/CA, a node on an 802.11 network checks for existing wireless transmissions (the green circle in [Figure 6-13](javascript://)) before it begins to send data.

* + If the source node detects no transmission activity on the network, it waits a brief, random amount of time and then sends its transmission.
  + If the source does detect activity, it waits a brief period before checking the channel again.

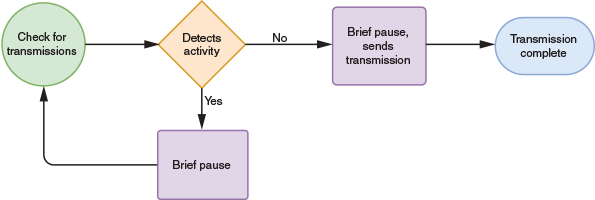
1. Step 2

The destination node receives the transmission and, after verifying its accuracy, issues an ACK (acknowledgment) packet to the source.

* + If the source receives this acknowledgment, it assumes the transmission was properly completed.
  + Interference or other transmissions on the network could impede this exchange. If, after transmitting a message, the source node fails to receive acknowledgment from the destination node, it assumes its transmission did not arrive properly, and it begins the CSMA/CA process anew.

**Figure 6-13**

CSMA/CA uses ACK messages to confirm successful transmission



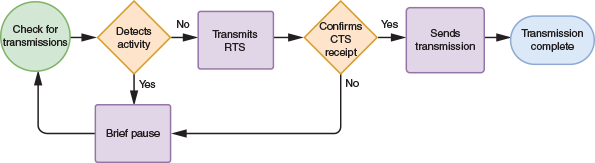
Enlarge Image

The use of ACK packets to verify every transmission means that 802.11 networks require more overhead than 802.3 networks. A wireless network with a theoretical maximum throughput of 1 Gbps will, in fact, transmit less data per second than a wired Ethernet network with the same theoretical maximum throughput.

Nodes that are physically located far apart from each other on a wireless network present a particular challenge in that they are too far apart to collaborate in preventing collisions. This is called the hidden node problem, where a node is not visible to other nodes on the other side of the coverage area. One way to ensure that packets are not inhibited by other transmissions is to reserve the medium for one node’s use. In 802.11, this can be accomplished through the optional [**RTS/CTS (Request to Send/Clear to Send)**](javascript://) protocol. [Figure 6-14](javascript://) illustrates the CSMA/CA process when using RTS/CTS.

**Figure 6-14**

CSMA/CA with the optional RTS/CTS protocol



Enlarge Image

When using RTS/CTS, a source node issues an RTS signal to the access point requesting the exclusive opportunity to transmit. If the access point agrees by responding with a CTS signal, the access point temporarily suspends communication with all nodes in its range and waits for the source node to complete its transmission. When used, RTS/CTS decreases network efficiency. However, it can be worthwhile when transmitting large packets.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-2cAssociation and Wireless Topologies

Suppose you bring your laptop to a local café, turn it on, and soon your laptop prompts you to log on to the café’s wireless network to gain access to the Internet through its hotspot. This seemingly simple process, known as [**association**](javascript://), involves a number of packet exchanges between the café’s access point and your computer. Association is another function of the MAC sublayer described in the 802.11 standard.

While a wireless device is on and has its wireless protocols running, it periodically surveys its surroundings for evidence of an access point, a task known as [**scanning**](javascript://). A device can use either active scanning or passive scanning:

* **Active scanning**—The wireless client takes the initiative:
  + The device transmits a special frame, known as a **probe**, on all available channels within its frequency range.
  + An AP detects the probe frame and issues a probe response containing all the information a device needs to associate with the AP, including a status code and node ID, or station ID, for that device.
  + The device can agree to associate with that AP. The final decision to associate with an AP, at least for the first time, usually requires the consent of the user.
  + The two nodes begin communicating over the frequency channel specified by the AP.
* **Passive scanning**—The AP takes the initiative:
  + A wireless-enabled device listens on all channels within its frequency range for a special signal, known as a beacon frame, issued periodically from an AP. The beacon frame contains information that a wireless node requires to associate itself with the AP, including the network’s transmission rate and the [**SSID (service set identifier)**](javascript://), a character string used to identify an access point.
  + The device—usually with the consent of the user—can choose to associate with the AP.
  + The two nodes agree on a frequency channel and begin communicating.

When setting up a WLAN, most network administrators use the AP’s configuration utility to assign a custom SSID, rather than the default SSID provided by the manufacturer. The default SSID often contains the name of the manufacturer and perhaps even the model number of the access point, which can give hackers a head-start on cracking into the network. Changing the SSID contributes to better security and easier network management, though you should keep the following tips in mind:

* Disguise the nature of the network identified by the SSID to avoid giving hackers more information than necessary. For example, it’s probably not a good idea to name the Accounting Department’s access point “Acctg.”
* Minimize confusion for employees by using easily recognized—though uncommon—SSIDs. The point of this is to increase security on client devices as they travel to other areas, so they don’t inadvertently attempt to connect to networks with an identical name.

IEEE terminology includes a couple of notable variations to the standard service set configuration. These terms reflect the most common wireless topologies as well:

* [**IBSS (independent basic service set)**](javascript://) using an [**ad hoc topology**](javascript://)—A small number of nodes closely positioned transmit directly to each other without an intervening connectivity device, as shown in [Figure 6-15](javascript://).
* [**BSS (basic service set)**](javascript://) using an [**infrastructure topology**](javascript://)—A group of nodes share an access point, as shown in [Figure 6-16](javascript://). The AP accepts wireless signals from multiple nodes and retransmits them, usually on a wired connection, to the rest of the network. To cover its intended range, an access point must have sufficient power and must be strategically placed so that all connected nodes can communicate with it. The identifier for this group of nodes is known as a [**BSSID (basic service set identifier)**](javascript://).
* [**ESS (extended service set)**](javascript://) using a [**mesh topology**](javascript://)—Several access points work as peer devices on the same network, as illustrated in [Figure 6-17](javascript://), where the AP devices cooperate to provide more fault-tolerant network access to clients across a larger geographical range. These APs are configured and managed by a [**wireless LAN controller**](javascript://), which might be used only initially to configure the APs, or the APs might remain connected to the wireless controller for continued management. Clients that belong to the same ESS share a special identifier called an [**ESSID (extended service set identifier)**](javascript://). In practice, many networking professionals don’t distinguish between the terms SSID and ESSID. They simply configure every access point in a group or LAN with the same SSID.

**Figure 6-15**

An ad hoc WLAN



Enlarge Image

**Figure 6-16**

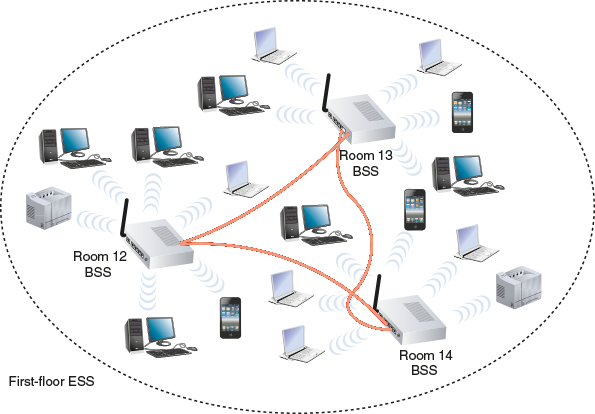
An infrastructure WLAN



Enlarge Image

**Figure 6-17**

A network with multiple BSSs form an ESS—devices can be moved from one room to the next without losing network connectivity



Enlarge Image

A wireless controller might be a physical device installed locally, such as the one shown in [Figure 6-18](javascript://), or it might be cloud-based, VM-based, or embedded in one of the APs. Centralized wireless management is made possible by a lightweight wireless protocol, such as Cisco’s proprietary LWAPP (Lightweight Access Point Protocol) or Cisco’s newer CAPWAP (Control and Provisioning of Wireless Access Points), both of which direct all wireless frames to the controller by adding extra headers to the frames. The wireless controller can provide centralized authentication for wireless clients, load balancing, and channel management so that neighboring APs don’t try to use overlapping channels. The controller manages AP redundancy by directing wireless traffic to alternate APs when an AP fails. Wireless controllers can also detect the presence of unauthorized APs, called [**rogue access points**](javascript://), by recognizing when an unauthorized AP attempts to connect to the network.

**Figure 6-18**

Use a wireless controller to configure, deploy, and manage APs



Enlarge Image

Within an ESS, a client can associate with any one of many APs that use the same ESSID. This allows users to [**roam**](javascript://), or change from AP to AP, without losing wireless network service. As devices roam between APs within a single ESS, connecting to a different AP requires [**reassociation**](javascript://). This is an automatic process that occurs when:

* A mobile device moves out of one AP’s range and into the range of another.
* The initial AP is experiencing a high rate of errors. On a network with multiple APs, network managers can take advantage of the nodes’ scanning feature to automatically balance transmission loads between access points.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

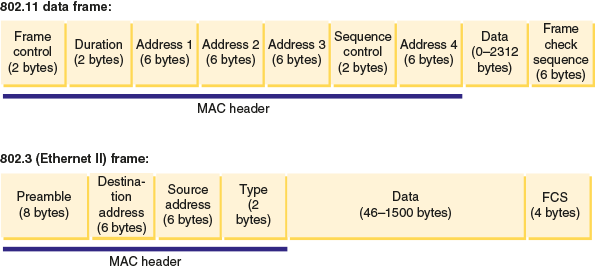
## 6-2dIEEE 802.11 Frames

You have learned about some types of overhead required to manage access to the 802.11 wireless networks—for example, ACKs, probes, and beacons. For each of these functions, the 802.11 standard specifies a frame type at the MAC sublayer. These frame types are divided into three groups:

* **Management frames**—Involved in association and reassociation; examples of this type of frame include probe and beacon frames.
* **Control frames**—Related to medium access and data delivery; examples of this type of frame include ACK and RTS/CTS frames.
* **Data frames**—Responsible for carrying data between nodes. An 802.11 data frame is illustrated in [Figure 6-19](javascript://). Compare the 802.11 data frame with the Ethernet II data frame also shown in [Figure 6-19](javascript://). As you can see in the figure, the 802.11 data frame carries significant overhead—that is, it includes a large quantity of fields in addition to the data field.

**Figure 6-19**

Basic 802.11 data frame compared with an 802.3 Ethernet II frame



Enlarge Image

The 802.11 data frame’s fields are summarized in [Table 6-4](javascript://).

**Table 6-4**

### Fields in an 802.11 data frame

| **Field name** | **Length** | **Description** |
| --- | --- | --- |
| Beginning of header:  Frame control | 2 bytes | Holds information about the protocol in use; the type of frame being transmitted; whether the frame is part of a larger, fragmented packet; whether the frame is one that was reissued after an unverified delivery attempt; the type of security the frame uses; and more. |
| Duration | 2 bytes | Indicates how long the field’s transmission will take so other nodes know when the channel will be available again. |
| Address 1 | 6 bytes | Source address. |
| Address 2 | 6 bytes | Transmitter address. |
| Address 3 | 6 bytes | Receiver address. |
| Sequence control | 2 bytes | Indicates how a large packet is fragmented. |
| Address 4 | 6 bytes | Destination address. |
| Data | 0–2312 bytes | Includes the data originally sent by the source host, plus headers from higher layers. The Data field is not part of the frame header or trailer—it is encapsulated by the frame. |
| Trailer:  Frame check sequence | 6 bytes | Uses a cyclical code to check for errors in the transmission. |

Notice that the 802.11 data frame contains four address fields; by contrast, the 802.3 (Ethernet II) frame has only two. The transmitter and receiver addresses refer to the access point or another intermediary device (if used) on the wireless network.

Another unique characteristic of the 802.11 data frame is its Sequence Control field. This field is used to indicate how a large packet is fragmented—that is, how it is subdivided into smaller packets for more reliable delivery. Recall that on wired TCP/IP networks, error checking occurs at the transport layer of the OSI model and packet fragmentation, if necessary, occurs at the network layer. However, in 802.11 networks, error checking and packet fragmentation are handled at the MAC sublayer of the data link layer. By handling fragmentation at a lower layer, 802.11 makes its transmission—which is less efficient and more error-prone—transparent to higher layers. This means 802.11 nodes are more easily integrated with 802.3 networks and prevent the 802.11 conversations of an integrated network from slowing down the 802.3 conversations.

**Remember This…**

* Compare 802.11 standards and their frequencies and ranges.
* Explain channel bonding.
* Describe how to configure IBSS, BSS, and ESS wireless networks.

**Self-Check**

1. What was the first 802.11 standard to implement channel bonding?

Answer

* 1. 802.11n
  2. 802.11ax
  3. 802.11g
  4. 802.11ac

1. Which type of identifier allows wireless clients to roam freely from AP to AP?

Answer

* 1. BSSID
  2. IP address
  3. ESSID
  4. Transmitter address

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 6-3Implementing a Wi-Fi Network

### Certification

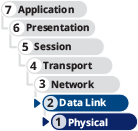
* 2.1

Compare and contrast various devices, their features, and their appropriate placement on the network.

* 3.2

Explain the purpose of organization documents and policies.

Average reading time: 22 minutes



Now that you understand how wireless signals are exchanged, what can hinder them, and which physical and data link layer standards they follow, you are ready to put these ideas into practice. This section first describes the WLAN topologies and how to design small WLANs, which are the types you might use at home or in a small office. Then you’ll walk through the process of installing and configuring access points and clients on larger wireless networks.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-3aDetermine the Design

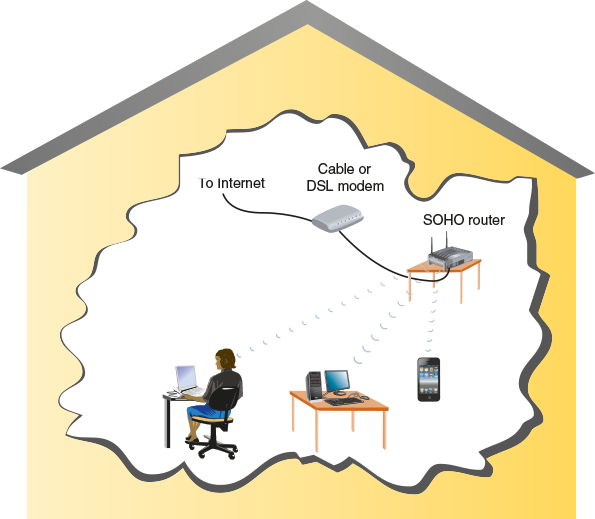
The design of a wireless network, the networking devices used, and the wireless technologies implemented are all affected by the network’s environment, the number and expectations of users, and the networked devices that will need to be supported. Let’s consider several forms of wireless networks you might work with.

### SOHO Networks

A home or small office network, called a SOHO network, generally requires only one central AP and possibly some range extenders. The AP device often combines switching, routing, and other network functions as well. In this case, the device is more accurately called a wireless router or SOHO router, and it connects wireless clients to the LAN in addition to serving as their gateway to the Internet. [Figure 6-20](javascript://) illustrates the typical arrangement of a home or small office WLAN and is described next.

**Figure 6-20**

Home or small office WLAN arrangement

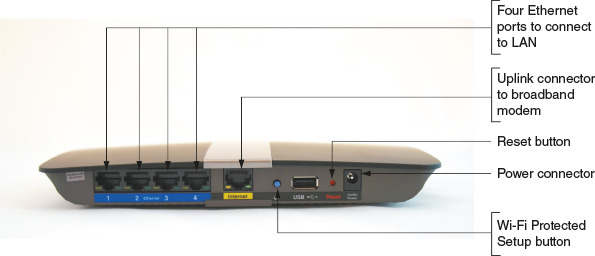


Enlarge Image

* The ISP’s signal comes into the premises through a cable or DSL modem.
* The modem connects to the SOHO router using an RJ-45 cable. This cable is inserted into the SOHO router’s WAN port, which is set apart from the other data ports and might be labeled “Internet” or remain unlabeled. Notice the yellow port on the SOHO router in [Figure 6-21](javascript://).
* The additional ports allow for wired access to the router, which contains switch hardware inside the device to manage connected devices. An AP that does not include routing or switching functions would lack these extra ports and act much like a wireless hub.

**Figure 6-21**

Connectors and ports on the back of a Cisco SOHO router



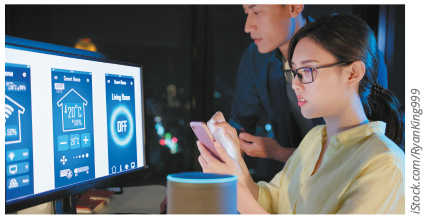
Enlarge Image

Many home or office networks include IoT devices and even expandable IoT networks. Today, networking is no longer limited to computing devices. All sorts of things can be connected to a network, from toasters, refrigerators, bathroom scales, and garage doors to watches, lamps, cars, thermostats, doorbells, and even the kitchen sink. This IoT (Internet of Things) is made up of any device that can be connected to the Internet—that is, any sensor, computer, or wearable device that talks to other devices over a network.

One of the fastest-growing areas of IoT is personal monitoring devices, such as health monitors, exercise equipment, GPS locators, and smartwatches. Another exploding IoT market interconnects smart home devices. You might already be familiar with Amazon Echo, Apple HomePod, or Google Home. These voice-controlled [**smart speakers**](javascript://) and their embedded personal assistant apps (such as Alexa, Siri, and Google Assistant) can interlink a plethora of devices, from locks and lights to security cameras and coffee pots. You can control these devices through voice commands while interacting with a smart speaker, or you can control IoT devices through an app on your smartphone (see [Figure 6-22](javascript://)). All these connected devices within a home create a type of LAN called a HAN (home area network).

**Figure 6-22**

This engineer team is designing app screens for a voice-controlled speaker that can manage many smart home devices



[iStock.com/RyanKing999](http://istock.com/RyanKing999" \t "_blank)

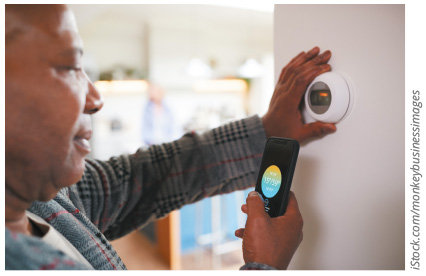
Let’s briefly look at what some of these smart home devices might offer to better understand how the network should be designed to support them:

* [**Smart thermostat**](javascript://)—More sophisticated than programmable thermostats, a smart thermostat allows users to adjust temperature settings based on daily schedules, shifting activity levels inside the home, current weather conditions outside, and in response to voice commands. You can control your home’s temperature remotely from a smartphone (see [Figure 6-23](javascript://)), such as when the outdoor temperature drops unexpectedly while you’re away from home. Further, the thermostat itself will monitor activity levels to automatically adjust its schedule for optimized energy savings and offer tips to save even more on utility bills. Some smart thermostats can be linked with other environmental control devices, such as smart humidifiers and air purifiers.
* [**Smart doorbell**](javascript://)—This device monitors an entryway for movement. To minimize false alarms from animals, you can set it up to filter out everything except movement caused by humans. It allows users to communicate with visitors remotely by video, even while away from home. Some smart doorbells can play a pre-recorded message, and a few offer AI-powered facial recognition to identify familiar faces. The video feed can be stored locally on the device’s onboard storage drive (such as a microSD card), on a hub device inside the house, or to the cloud. Many smart doorbells now come with rechargeable batteries, so no wiring is required for installation.
* [**Security camera**](javascript://)—These devices come with rechargeable batteries, wireless capability, and significant weather proofing to maximize installation options. Some cameras can also be connected to a solar panel so they don’t need to be taken down to recharge. Many of these cameras can be installed almost anywhere, even on a tree trunk, for optimal perspective on a monitored area (see [Figure 6-24](javascript://)). The camera sends alerts and video feeds through Wi-Fi to a smartphone app where the user can remotely monitor covered areas, such as entryways and parking areas. Most of today’s cameras include some type of night vision capability, and many include two-way audio similar to a smart doorbell.

* **[Smart refrigerator](javascript://)**—Also called a smart fridge, this device uses RFID or barcode tracking to detect items stored in the refrigerator, and it alerts users when essential items are running low or have expired. Many smart fridges also include interior cameras so you can see what’s inside it from the store. Unfortunately, smart fridges are still much more expensive than so-called dumb fridges and are wracked with problems in terms of dropped services from the manufacturer or quickly outdated smart technology.

**Figure 6-23**

A smart thermostat can be controlled by voice or by a smartphone app or smartwatch app



[iStock.com/monkeybusinessimages](http://istock.com/monkeybusinessimages" \t "_blank)

**Figure 6-24**

This wireless security camera distinguishes between humans and animals to send more useful alerts and reduce false positives



Jill West

Now that you have a better understanding of the diversity of devices your wireless network might need to support, consider these factors when deciding where to install a SOHO WLAN’s access point:

* **Distance**—Consider typical distances between the AP and its clients, and distance restrictions for the 802.11 standard your AP is using. If your home or small office spans three floors, and clients are evenly distributed among the floors, you might choose to situate the AP on the second floor.
* **Type and number of obstacles**—Consider the type and number of obstacles between the AP and its clients. If your three-story building is constructed like a bunker with massive concrete floors, you might consider installing a separate AP on each floor. If a building or office space is long and narrow, you might need two APs on the same floor—one at each end of the building. Remember from the [On the Job](javascript://) story at the beginning of this module, sometimes obstacles can be more consequential than they at first appear.
* **Coverage**—Place the AP in a high spot, such as on a shelf or rack or in a drop ceiling.
* **Interference**—Make sure the AP is not close to potential sources of interference, including cordless phones, fluorescent lights, or microwave ovens.

### Corporate Network

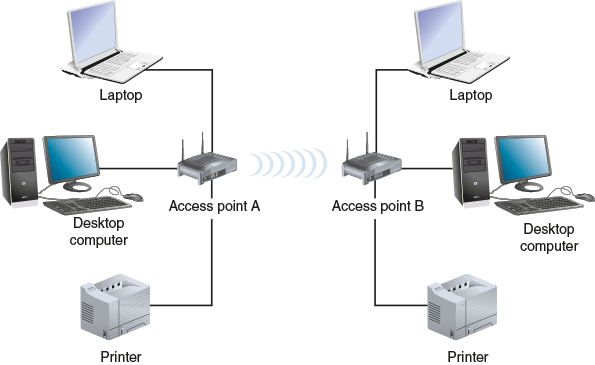
Larger wireless networks warrant a more systematic approach to access point placement. Before placing APs in every data room, it’s wise to conduct a site survey. A [**site survey**](javascript://) assesses client requirements, facility characteristics, and coverage areas; the resulting site survey report will help you determine an AP arrangement that will ensure reliable wireless connectivity within a given area.

Suppose you are the network manager for a large organization whose wireless clients are distributed over six floors of a building. On two floors, your organization takes up 2000 square feet of office space, but on the other four floors, your offices are limited to only 200 square feet. In addition, clients move between floors regularly, and the lobby-level floor has less wireless traffic than the others. Other building occupants are also running wireless networks. Let’s see what activities might contribute to developing a thorough site survey report in this situation:

* Study building blueprints to identify potential obstacles, clarify the distances your network needs to span on each floor, and anticipate wireless demand from devices that tend to occupy each floor during the course of business.
* Consider whether any Wi-Fi access points will be used as a [**wireless bridge**](javascript://) to connect two networks or two remote portions of one network, as shown in [Figure 6-25](javascript://). The throughput demands of a wireless bridge connected to another AP can be significantly higher than typical Wi-Fi clients.
* Determine whether certain floors require multiple APs. Visually inspecting the floors will also help determine coverage areas and best AP locations.
* Measure the signal coverage and strength from other WLANs to inform your decision about the optimal strength and frequency for your wireless signals.
* Test proposed access-point locations. In testing, a “dummy” AP is carried from location to location while a wireless client connects to it and measures its range and throughput. (Some companies sell software specially designed to conduct such testing.)
* Test wireless access from the farthest corners of your space. This testing will reveal unforeseen obstacles, such as EMI issued from lights or heavy machinery.
* Consider the materials used in objects that aren’t always present in the environment, such as stocked inventory in a warehouse.
* Consider how the wireless portions of the network will integrate with the wired portions. Access points connect these two portions of your overall network.

**Figure 6-25**

A wireless bridge provides remote wired access



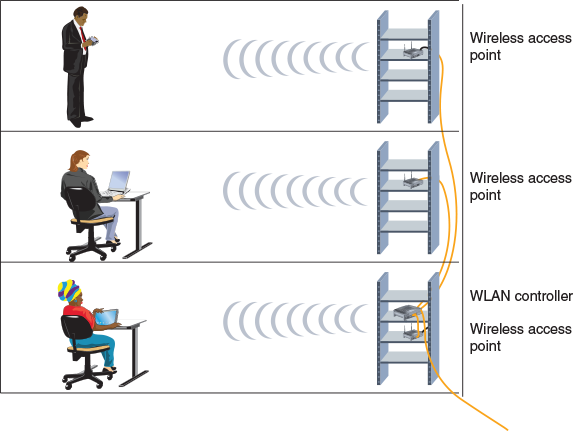
Enlarge Image

The site survey can be completed more efficiently with the use of wireless survey tools such as site survey software. Popular examples include NetSpot, VisiWave, the iBwave Wi-Fi Suite, and inSSIDer by MetaGeek. After the initial setup, you can use these programs to monitor wireless network performance and possible interference or intrusion by other wireless signals in the area. Many of these programs, for example, offer a heat map feature that maps Wi-Fi signals and other noise in your location. An accurate heat map can also pinpoint gaps in Wi-Fi coverage, called dead zones, throughout the building to ensure that employee productivity isn’t adversely affected by dropped Wi-Fi connections or unnecessarily slow connections.

After a site survey has identified and verified the optimal quantity and location of access points, you are ready to install them. Recall that to ensure seamless connectivity from one coverage area to another, all APs must belong to the same ESS and share an ESSID. Configuring APs, including assigning ESSIDs, is described in the next section. In preparation, [Figure 6-26](javascript://) shows an example of an enterprise wireless network.

**Figure 6-26**

An enterprise-scale wireless network



Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-3bConfigure Wi-Fi Connectivity Devices

You have learned that access points provide wireless connectivity for mobile clients on an infrastructure WLAN. APs vary in which wireless standards they support, their antenna strength, and other features, such as support for voice signals or the latest security measures. You can buy a small AP or SOHO router for less than $50. More sophisticated or specialized APs cost much more—for example, those designed for outdoor use, as on city streets or at train platforms. However, as wireless networking has become commonplace, even the least expensive devices are increasingly sophisticated.

The setup process for a SOHO router is similar regardless of the manufacturer or model. The variables you will set during installation include the following:

* Administrator password (which is different than the Wi-Fi password used by Wi-Fi clients to associate with the AP)
* SSID (and determine whether it’s broadcast)
* Security options such as type and credentials needed to associate with the AP
* Whether or not DHCP and related options are used, note that most network administrators do not configure their wireless access point as a DHCP server and, in fact, doing so when another DHCP server is already designated will cause addressing problems on the network

In the Hands-On Projects at the end of this module, you will practice installing and configuring a SOHO router. If something goes awry during your SOHO router configuration, you can force a reset of all the variables you changed. Wireless routers feature a reset button on their back panel. The following steps describe how to reset a SOHO router:

1. 1

Disconnect all data cables and unplug the power cable.

1. 2

Using the end of a paper clip, depress the reset button while you plug the power cable back in.

1. 3

Continue holding down the button for at least 30 seconds (the required duration varies among manufacturers; check your router’s documentation for the duration yours requires).

1. 4

Release the button; at this point, the router’s values should be reset to the manufacturer’s defaults.

After successfully configuring your SOHO router, you are ready to introduce it to the network. In the case of a small office or home WLAN, this means using a patch cable to connect the device’s WAN port to your modem’s LAN port. Afterward, clients should be able to associate with the access point and gain Internet access. The following section describes how to configure clients to connect to your WLAN.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-3cConfigure Wi-Fi Clients

Wireless access configuration varies from one type of client to another. A gaming or media device will require a slightly different process than a laptop or tablet, and an IoT device such as a smart plug or a smart lock will differ yet again. The specific steps vary by device type and manufacturer. In general, as long as an AP is broadcasting its SSID, clients in its vicinity will detect it and offer the user the option to associate with it. If the AP uses encryption, you will need to provide the right credentials to associate with it successfully. Later in this module, you’ll have the chance to change some of the security settings on a wireless Windows client.

In an enterprise environment, configuring clients for wireless access to the network can entail a much more involved, two-part process:

* [**Onboarding**](javascript://)—Users or network technicians install a specific app, called an agent, on a user’s device, whether the device is a smartphone, laptop, or tablet. This gives the device trusted access to certain portions of the network. Access to email services, file-sharing services, and certain network administrative features might all be controlled by the device’s permission levels enabled by on-boarding that device. The agent might also scan the device for any needed OS or security updates, required security settings (such as timeouts or sign-in requirements), and any existing malware.
* [**Offboarding**](javascript://)—The reverse procedure involves removing the agent. For security purposes, network administrators need a feature that allows them to do this remotely in case a device is lost or stolen. This feature, called a [**remote wipe**](javascript://), clears a device of important information, permissions, and apps without having physical access to the device. It might even allow you to completely disable the device, making any network or data access impossible.

Onboarding and offboarding policies are especially critical in a [**BYOD (bring your own device)**](javascript://) environment where IT staff must ensure the safety of the network while allowing access by a wide range of employee-owned devices using network resources. These policies might specify a minimum version OS and a requirement to keep the OS updated, certain access restrictions such as minimum password length and an automatic timeout, and permissions to monitor device activity or to wipe data from the device with or without further notice.

**Applying Concepts 6-1**

### Explore a Linux Wireless Interface

As with Windows operating systems, most Linux and UNIX clients provide a graphical interface for configuring their wireless interfaces. Because each version differs somewhat from the others, describing the steps required for each graphical interface is beyond the scope of this course. However, iwconfig, a command-line utility for viewing and setting wireless interface parameters, is common to nearly all versions of Linux and UNIX. The following steps, which can be performed on a Linux machine or a Linux VM, provide a basic primer for using the iwconfig command:

1. 1

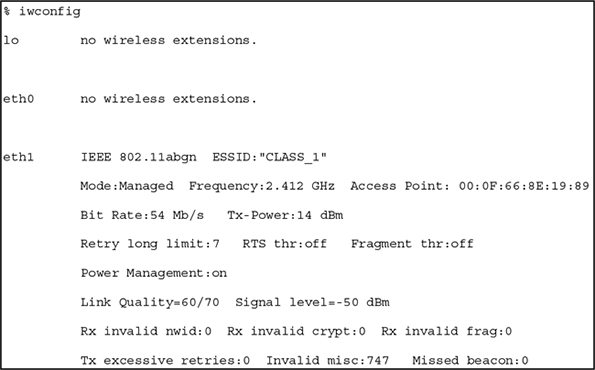
Make sure your wireless NIC is installed and that your Linux or UNIX workstation or host machine is within range of a working AP. You must also be logged into Linux or UNIX as root or a user with root-equivalent privileges. (Recall that the root user on UNIX or Linux systems is comparable to an administrative user on Windows systems.)

1. 2

Open Terminal and enter **iwconfig**. The output should look similar to that shown in [Figure 6-27](javascript://).

**Figure 6-27**

Output from the iwconfig command



Enlarge Image

1. 3

Here’s a brief description of the output:

* + lo indicates the loopback interface.
  + eth0 represents an interface that is not wireless (that is, a wired NIC).
  + eth1 represents the wireless interface; on your computer, the wireless NIC might have a different designation.
  + iwconfig also reveals characteristics of the AP’s signal, including its frequency, power, and signal level.

1. 4

For more detailed information about this command, enter **man iwconfig**. Using the iwconfig command, you can modify the SSID of the access point you choose to associate with, as well as many other variables. Some examples are detailed in [Table 6-5](javascript://). The syntax of the following examples assumes your workstation has labeled your wireless NIC eth1.

**Table 6-5**

### Sample iwconfig commands

| **Command** | **Description** |
| --- | --- |
| iwconfig eth1 essid CLASS\_1 | Instructs the wireless interface to associate with an AP whose SSID (or ESSID, as shown in this command) is CLASS\_1. |
| iwconfig eth1 mode Managed | Instructs the wireless interface to operate in infrastructure mode (as opposed to ad hoc mode). |
| iwconfig eth1 channel auto | Instructs the wireless interface to automatically select the best channel for wireless data exchange. |
| iwconfig eth1 freq 2.422G | Instructs the wireless interface to communicate on the 2.422 GHz frequency. |
| iwconfig eth1 key 6e225e3931 | Instructs the wireless interface to use the hexadecimal number 6e225e3931 as its key for secure authentication with the AP. (The number 6e225e3931 is only an example; on your network, you will choose your own key.) |

In this and the previous section, you have learned how to configure wireless clients and access points. Optimized configurations help increase network efficiency as well as securing network resources from damage or intrusion. The following section explains some key points about securing a wireless network.

**Remember This…**

* Describe IoT devices, including refrigerators, smart speakers, smart thermostats, and smart doorbells.
* Identify information generated by a site survey.
* Explain the primary points of onboarding and offboarding policies.

**Self-Check**

1. Which device on the network will require the greatest throughput capacity?

Answer

* 1. Smart speaker
  2. Wireless LAN controller
  3. Wireless bridge
  4. Smart thermostat

1. Which off-boarding policy can protect proprietary corporate information if a smartphone is lost?

Answer

* 1. Remote wipe
  2. Trusted access
  3. OS update requirements
  4. Site survey

**You’re Ready**

You’re now ready to complete [Project 6-1: Configure a SOHO Router](javascript://), or you can wait until you’ve finished reading this module.

**You’re Ready**

You’re now ready to complete [Project 6-2: Modify SOHO Router Wireless Settings](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 6-4Wi-Fi Network Security

### Certification

* 2.4

Given a scenario, install and configure the appropriate wireless standards and technologies.

* 4.1

Explain common security concepts.

* 4.2

Compare and contrast common types of attacks.

* 4.3

Given a scenario, apply network hardening techniques.

* 5.4

Given a scenario, troubleshoot common wireless connectivity issues.

Average reading time: 26 minutes

As you have learned, most organizations use one or more of the 802.11 protocol standards on their WLANs. By default, the 802.11 standard does not by itself offer any security. The client only needs to know the access point’s SSID, which many access points broadcast. Network administrators may prevent their access points from broadcasting the SSIDs, making them harder to detect. However, this does not provide true security. Two solutions to this problem are authentication and encryption:

* **Authentication**—Allows a wireless client to log on to the network, either by providing the correct password for the SSID or by providing user credentials that might be processed by an authentication server. The authentication process can be somewhat strengthened with [**MAC filtering**](javascript://), or MAC address filtering, which prevents the AP from authenticating any device whose MAC address is not listed by the network administrator. (MAC filtering can also be instituted on a switch.) But it can be time consuming to maintain a current list of all approved MAC addresses, and, as you’ve seen, MAC addresses are easily impersonated.
* **Encryption algorithms**—Scramble data transmitted over the airwaves into a format that cannot easily be interpreted if the signal is intercepted. The purpose of encryption is to keep information private. Many forms of wireless encryption exist, with some being more secure than others.

Let’s explore some of the available techniques for securing wireless networks with authentication and encryption, beginning with an outdated technology called WEP.

### Legacy Networking: WEP (Wired Equivalent Privacy)

For some measure of security, 802.11 allows for optional encryption using the [**WEP (Wired Equivalent Privacy)**](javascript://) standard. In fact, WEP offered two forms of authentication, neither of which is secure:

* **OSA (Open System Authentication)**—No key is used at all. The wireless access client, knowing only the access point’s SSID, requests authentication. The AP generates a single-use code for that session only, and the computer accepts the code. However, no encrypted data can be sent over this temporary connection, and any device can be authenticated. In fact, no real authentication occurs.
* **SKA (Shared Key Authentication)**—All wireless access clients use the same key, which can then be used to encrypt transmissions. When configuring WEP, you establish a character string that is required to associate with the access point, also known as the network key. The user must provide the correct key before the client can gain access to the network via the access point. The network key can be saved as part of the client’s wireless connection’s properties. WEP uses the same key both to authenticate network clients and to encrypt data in transit. However, the key can be cracked, compromising the security of all clients on the network.

The first implementation of WEP allowed for 64-bit network keys, and current versions of WEP allow for more secure 128-bit or even 256-bit network keys. However, one of the most significant disadvantages of WEP is that it uses a shared encryption key for all clients and the key might never change. WEP’s use of the shared key for authenticating all users and for encrypting data makes it more susceptible to discovery than a dynamically generated, random, or single-use key. Even 128-bit network keys can be cracked in a matter of minutes. Moreover, WEP does not offer end-to-end data transmission security.

WEP was replaced with a quick-fix improvement called WPA when IEEE devised a new wireless security standard called 802.11i that included the subset standard WPA. The following sections explore the progressive improvements made to the 802.11i standard, eventually resulting in the development of the more secure and reliable WPA2.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4aWPA (Wi-Fi Protected Access)

A significant disadvantage to WEP is that it uses the same network key for all clients and the key is static, which means it won’t change without manual intervention. Due to this inherent insecurity, a replacement security technology was developed, called [**WPA (Wi-Fi Protected Access)**](javascript://), which dynamically assigns every transmission its own key. 802.11i incorporates an encryption key generation and management scheme known as [**TKIP (Temporal Key Integrity Protocol)**](javascript://), pronounced tee-kip, to improve security for legacy WEP-based devices. TKIP accomplished three significant improvements:

* **Message integrity**—Uses a message integrity code, called Michael, that ensures incoming packets are, in fact, coming from their declared source. This is also called packet authentication.
* **Key distribution**—Assigns every transmission its own key.
* **Encryption**—Includes encryption originally provided by [**RC4 (Rivest Cipher 4)**](javascript://), a now insecure encryption cipher that is still widely used.

In reality, TKIP was a quick fix, designed more as an integrity check for WEP transmissions than as a sophisticated encryption protocol. WPA’s TKIP uses the same encryption mechanism as WEP but with improved algorithms to wrap the older WEP transmissions in a more securely encrypted transmission. However, you’ll still find modern wireless network devices offering TKIP to provide compatibility with older wireless clients.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4bWPA2 (Wi-Fi Protected Access, Version 2)

The data confidentiality methods used in WPA were replaced by stronger technologies for the updated version, [**WPA2**](javascript://), which can be enabled on most consumer-grade APs today. [**CCMP**](javascript://), which is short for [**Counter Mode with CBC (Cipher Block Chaining) MAC (Message Authentication Code) Protocol**](javascript://), improves wireless security for newer devices that can use WPA2. Acronyms within acronyms are only the beginning of what makes this protocol so interesting. Whereas TKIP was meant to be backward-compatible as much as possible, CCMP is more future-focused. CCMP helps ensure data confidentiality with both encryption and packet authentication by providing the following:

* **Message integrity**—CCMP includes CBC-MAC, which ensures incoming packets are, in fact, coming from their declared source, and does so using the block cipher algorithm AES, described next.
* **Encryption**—CCMP also uses [**AES (Advanced Encryption Standard)**](javascript://), which provides faster and more secure encryption than TKIP for wireless transmissions. AES relies on a more sophisticated family of ciphers along with multiple stages of data transformation.

**Note 6-4**

Two similar types of cipher algorithms are stream ciphers and block ciphers. The essential difference is that stream ciphers encrypt one byte (or possibly one bit) at a time, while block ciphers encrypt much larger chunks, or blocks, in each calculation.

The Wi-Fi Alliance ([wi-fi.org](http://wi-fi.org/" \t "_blank)) released the next iteration, WPA3, in 2018 and has begun to certify WPA3 devices. Some touted features of the new standard include disallowing legacy protocols, ability of users to choose their own passwords, more advanced encryption and authentication methods, and better protection of data in transit. In particular, WPA3’s new handshake design was intended to close a security vulnerability in WPA2’s handshake that leaves the hash of the password vulnerable during the initial association process. However, researchers are already identifying flaws in the design and security of WPA3 and believe that another round of security enhancements will be necessary.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4cPersonal and Enterprise

On many wireless routers and access points, you might have noticed options for WPA-Personal and WPA-Enterprise, or WPA2-Personal and WPA2-Enterprise. The Personal versions of WPA and WPA2 are sometimes referred to as WPA-PSK or WPA2-PSK, where [**PSK**](javascript://) stands for [**Pre-Shared Key**](javascript://). This is the common configuration on home wireless networks in which you need to enter a passphrase for your device to authenticate to the network. The passphrase and the SSID characters are then used to calculate a unique encryption key for each device.

The most secure Wi-Fi communication is made possible by combining a RADIUS authentication server with WPA or WPA2, known as WPA-Enterprise or WPA2-Enterprise, respectively. While you’ll learn more about RADIUS later, for now, understand that [**RADIUS (Remote Authentication Dial-In User Service)**](javascript://) is an open source authentication and authorization service. A RADIUS server can be used to offer a central authentication point for wireless, mobile, and remote users. In the context of Wi-Fi, a RADIUS server is used in cooperation with an authentication mechanism called EAP.

[**EAP (Extensible Authentication Protocol)**](javascript://) differs from other authentication protocols in that it only provides the framework for authenticating clients and servers. It does not perform encryption or authentication on its own. Instead, it works with other encryption and authentication schemes to verify the credentials of users and devices. One of EAP’s advantages is its flexibility. It is supported by nearly all modern operating systems and can be used with many different authentication methods. For example, although the typical network authentication involves a user ID and password, EAP also works with biometric methods, such as retina or hand-scanning.

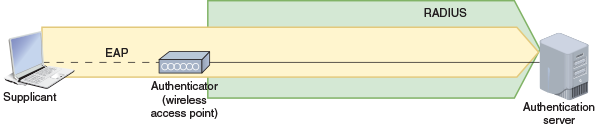
EAP functions alongside RADIUS by organizing communications with the network client devices, while RADIUS handles the actual authentication on the server. In this case, EAP messages are encapsulated inside RADIUS messages between the network device, such as a switch or access point, and the RADIUS server. [Figure 6-28](javascript://) shows how EAP and RADIUS handle different portions of the interaction.

The three main EAP entities, as shown in [Figure 6-28](javascript://), are the following:

* **Supplicant**—The device requesting authentication, such as a smartphone or laptop
* **Authenticator**—The network device that initiates the authentication process, such as a wireless access point
* **Authentication server**—The server that performs the authentication

**Figure 6-28**

EAP messages are encapsulated in RADIUS messages



Enlarge Image

The conversation between these entities looks something like the diagram shown in [Figure 6-29](javascript://). The steps are described next:

1. Step 0

The wireless device associates with the access point, usually with WPA2. The process begins with Step 0 here because association is an essential precursor to the authentication process, but it’s not part of that process.

1. Step 1

The supplicant requests authentication, and the authenticator initiates the authentication process by asking a newly connected supplicant to verify itself.

1. Step 2

After the supplicant responds, the authenticator forwards that information to the authentication server, such as a RADIUS server.

1. Step 3

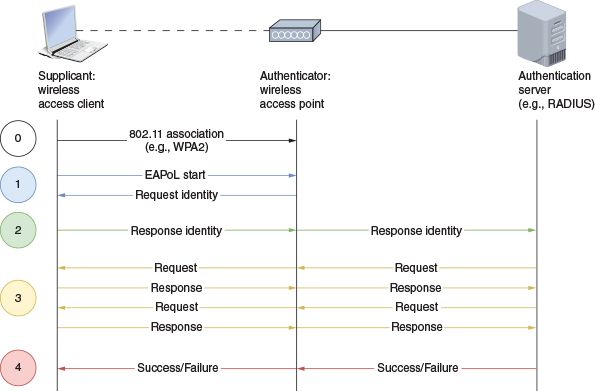
The server usually sends more than one request in response. In its first request, it asks the supplicant’s identity and indicates the type of authentication to use. In subsequent requests, the server asks the supplicant for authentication information to prove the supplicant’s identity. The supplicant responds to each of the server’s requests in the required format.

1. Step 4

If the responses match what the server expects, the server authenticates the supplicant. Otherwise, authentication fails.

**Figure 6-29**

If a RADIUS server is used here, EAP communications between the authenticator and the RADIUS server are encapsulated in RADIUS messages



Enlarge Image

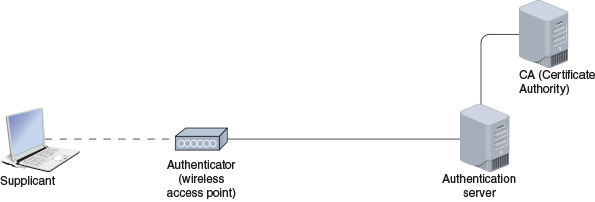
EAP is adaptable to new technology. It was originally designed to work only on point-to-point connections, usually on a WAN. However, it was adapted to work on both wired and wireless LANs in the [**802.1X**](javascript://) standard, dubbed **[EAPoL (EAP over LAN)](javascript://)**. In this case, EAP is carried by Ethernet messages. To accomplish this, 802.1X allows only EAPoL traffic over any switch or AP port connected to a wired or wireless client until that client has authenticated with the authentication server. This is called PNAC (port-based network access control), or sometimes port-based authentication. Today, 802.1X is primarily used on wireless LANs.

Several versions and adaptations of EAP exist. Some of the most common versions include the following:

* **EAP-TLS**—Similar to how HTTPS uses SSL/TLS encryption to secure HTTP transmissions, EAP-TLS uses TLS encryption to protect communications. EAP-TLS also uses PKI (public-key infrastructure) certificates to exchange public keys and authenticate both the supplicant and the server through mutual authentication. While these certificates can be a challenge to set up, the resulting authentication strength is often worth the trade-off in convenience. [Figure 6-30](javascript://) shows the addition of a CA (Certificate Authority) to the network to help manage the certificates needed by EAP-TLS.
* **PEAP (Protected EAP)**—While EAP-TLS is certificate-based, PEAP and EAP-FAST are tunnel-based. PEAP (Protected EAP) creates an encrypted TLS tunnel between the supplicant and the server before proceeding with the usual EAP process. As shown in [Figure 6-31](javascript://), PEAP is called the outer method. Then another form of EAP is used for the inner method, which is the process that occurs inside the protected tunnel. The most common inner method is EAP-MSCHAPv2, which runs a session inside the tunnel, perhaps to a RADIUS server and beyond to Active Directory.
* **EAP-FAST (EAP-Flexible Authentication via Secure Tunneling)**—Also a form of tunneled EAP, this technology was developed by Cisco and works similarly to PEAP, except faster. The most important difference with EAP-FAST is that it uses PACs (Protected Access Credentials), which are somewhat similar to cookies that websites store on a user’s computer to track their activities. A PAC is stored on the supplicant device for speedier establishment of the TLS tunnel in future sessions.

**Figure 6-30**

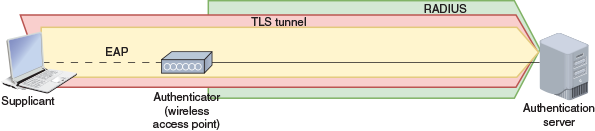
EAP-TLS requires a Certificate Authority



Enlarge Image

**Figure 6-31**

PEAP creates an encrypted TLS tunnel



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4dOther Security Configurations

Some additional security options you might want to enable on your wireless network include the following:

* **AP and antenna placement**—It might seem like a simple thing but it’s important to think about where you place your AP in your home or business area. Placing the AP near an outside wall might result in a weak signal on the far side of your building but leave a strong signal vulnerable to attack from someone parked nearby. Positioning the AP in the center of its intended range increases the strength of the signal for approved users while reducing the likelihood that anyone outside of that area can get a strong enough signal to connect to the network. Also, some APs have antennas that can be positioned to optimize signal reach. Consider what antenna placement will give the best signal where you want it and reduce the strength of the signal outside your building or other intended range. Similarly, experiment with various power levels to determine the needed transmission power to reach your intended range while not overly extending your range outside the area you manage.

* **[Geofencing](javascript://)**—This more sophisticated security technique detects a Wi-Fi client’s geographical position and activates resources or access according to that location. For example, a shopping mall or store might use geofencing to offer customers Internet access and targeted marketing information (such as coupons) while not making these resources available to people outside a defined area. Deploying a mesh network of APs makes it possible to track a Wi-Fi client device’s physical movement throughout the network.
* [**Guest network**](javascript://)—Many establishments—and homeowners, for that matter—create an isolated guest network through their Wi-Fi router/access point. The guest network has a separate SSID and passphrase and can be managed with different rules or time restrictions. This is a smart security precaution, as it gives guests access to Internet service through an open network without opening the doors to the entire LAN on that router. Parents, also, might want to give their children use of an SSID with more limited network access to enforce household rules regarding Internet use.
* [**Wireless client isolation**](javascript://)—This technique is similar to a guest network but simpler. Wireless client isolation allows a wireless client onto the network but imposes firewall rules to restrict that client’s ability to communicate with only the default gateway, not other devices on the network. Like with a guest network, wireless clients are able to communicate with the Internet but have no access to other network resources.
* [**Captive portal**](javascript://)—If you do provide a guest network, either at home or at a business, be sure to set up a captive portal. This is the first page a new client sees in the browser when connecting to the guest network, and it usually requires the user to agree to a set of terms and conditions before gaining further access to the guest network. The captive portal should remind users of the following details:
  + They are connecting to a network that does not provide user authentication or data encryption. This means data is not secure when transmitted over this connection.
  + They should be careful about what data they transmit, even over email, while using the guest network.
  + They should take extra care to avoid engaging in any illegal activity through the network connection, as that activity could be traced back to your public IP address.

**Note 6-5**

Captive portals can cause issues of their own. For example, if you’ve configured custom DNS servers for your network, you might find that clients trying to associate with your network will sometimes get stuck on the captive portal page or not be able to pull it up at all. Firewalls or pop-up blockers in the browser can block the captive portal, and browsers configured with autofill options might also fail to properly load a captive portal page. In some cases, the browser cannot successfully open the captive portal page because the browser was first trying to reach a secure website using HTTPS, and HTTPS doesn’t cooperate with the interference of the captive portal. You can get around this limitation by having the wireless client first navigate to a nonsecure web page, such as [neverssl.com](http://neverssl.com/" \t "_blank), and that can trigger the captive portal to open successfully.

* **IoT access considerations**—Think about how best to give network access to your IoT devices. Hardening your IoT network starts with changing default device names, usernames, and passwords for those devices, creating strong passwords, and using the strongest encryption settings the devices offer. Where possible, use two-factor authentication so you not only provide a password to access device settings, but you also get a one-time code sent to your smartphone for authentication. Many cybersecurity experts recommend creating an entirely separate Wi-Fi network for all IoT devices, such as a guest network (and use a strong password on the guest network). Disable features you’re not using, and update software and firmware when those updates become available. Finally, don’t access your IoT software and devices when using a public network, such as at a coffee shop.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4eSecurity Threats to Wi-Fi Networks

Wireless transmissions are particularly susceptible to eavesdropping. Several additional security threats to wireless networks are discussed in the following list:

* **War driving**—A hacker searches for unprotected wireless networks by driving around with a laptop or smartphone configured to receive and capture wireless data transmissions. (The term is derived from the term war dialing, which is a similar tactic involving old, dial-up modems.) War driving is surprisingly effective for obtaining private information. Years ago, the hacker community publicized the vulnerabilities of a well-known store chain, which were discovered while war driving. The retailer used wireless cash registers to help customers make purchases when the regular, wired cash registers were busy. However, the wireless cash registers transmitted purchase information, including credit card numbers and customer names, to network APs in cleartext (in other words, unencrypted). By chance, a person in the parking lot who was running a protocol analyzer program on his laptop obtained several credit card numbers in a very short time. The person alerted the retailer to the security risk (rather than exploiting the information he gathered). Needless to say, after the retailer discovered its error, it abandoned the use of wireless cash registers until a thorough evaluation of its data security could be conducted.
* **War chalking**—Once hackers discover vulnerable access points, they make this information public by drawing symbols with chalk on the sidewalk or a wall within range of a wireless network. The symbols, patterned after marks that hobos devised to indicate hospitable places for food or rest, indicate the access point’s SSID and whether it’s secured. Alternatively, many websites offer maps of these open networks, as reported by war drivers.
* [**Evil twin**](javascript://)—Clients running Linux, macOS, or a modern version of Windows will first attempt to associate with a known access point. This feature can result in network devices connecting to rogue access points, or access points offering a connection to the Internet without the authorization of the area’s network administrator. One type of rogue access point, an evil twin, can be used to trick a device into connecting to the wrong network by broadcasting the same SSID as the authorized network or another SSID that appears just as legitimate to the user. Suppose another user brings their own AP to a café and its signal is twice as strong as the café’s AP. Your laptop will automatically recognize the other user’s stronger AP as the best option. If the user has configured their AP with the same SSID as the café’s, and if you’ve configured your laptop to trust that SSID, your laptop might complete association to this evil twin AP without your knowledge. The person controlling the evil twin could then steal your data or gain access to another network that trusts your system. Note that a user can create a rogue access point inadvertently, too—for example, by bringing an AP to work, using software to turn a workstation into an AP, or creating a hotspot with a smartphone. As a network technician, you should check regularly for evil twins or other rogue access points within your network’s geographical area. Especially be on the lookout for access points that show a stronger signal than your corporate AP because Windows lists SSIDs by signal strength, and users are accustomed to selecting the SSID at the top of the list.
* **WPA attack**—These attacks, also called WPA cracking, involve an interception of the network keys communicated between clients and access points.
* **WPS attack**—WPS (Wi-Fi Protected Setup) is a user-friendly—but not very secure—security setting available on some consumer-grade APs. Part of the security involves requiring a PIN (personal identification number) to access the AP’s settings or to associate a new device with the network. The problem is that the PIN can be easily cracked through a [**brute force attack**](javascript://), which means simply trying numerous possible character combinations to find the correct combination. This gives the attacker access to the network’s WPA2 key. The PIN feature in WPS should be disabled if possible.

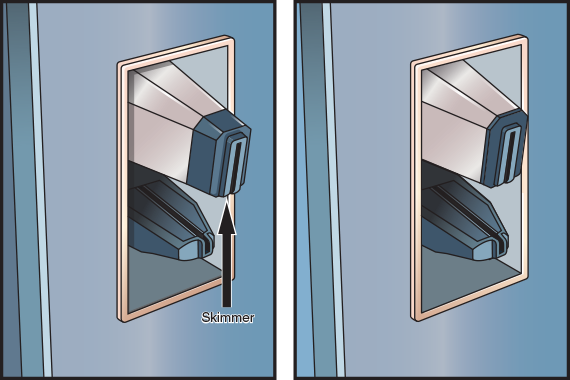
### Caution

Not all wireless threats are related to Wi-Fi. The prevalence of RFID chips in credit cards has contributed to the upsurge of a type of fraud called skimming. The culprit installs a card reader, or skimmer, on a payment terminal, such as a gas pump or ATM. The skimmer collects data stored on the magnetic strips or on RFID chips in cards used at that terminal. Physical contact is required to collect data from a magnetic strip, but the RFID chip can transmit data to a skimmer several inches away. The criminal returns later to collect the device along with the stolen data it has accumulated.

Always examine a payment terminal for signs of tampering. If it looks different than nearby terminals, a skimmer might be cleverly disguised right in front of you, such as the one shown in [Figure 6-32](javascript://). The skimmer is designed to detach easily so the thief can retrieve it quickly, so pull on the payment terminal a little to see if anything budges. Consider googling for images of credit card skimmers, ATM skimmers, and gas pump skimmers. The more familiar you are with what to look for, the safer you’ll be. If you see something suspicious, call the police and don’t use that terminal.

**Figure 6-32**

Skimmers on payment terminals can be surprisingly difficult to spot



In a similar scam, thieves steal information from your credit card while it sits snugly in your wallet. A thief can swipe an RFID reader near the victim’s pocket or bag and collect information from enclosed RFID credit cards, which is called electronic pickpocketing. Many manufacturers sell RFID-blocking wallets of varying quality and effectiveness. You can also wrap your wallet or cards in a layer of aluminum foil. In all circumstances, pay close attention to the people who stand near you in checkout lines, shopping areas, restaurants, and other public spaces.

Most newer credit cards contain a different kind of chip called an EMV (Europay, Mastercard, and Visa) chip that generates a unique transaction number each time it’s activated. However, some EMV credit cards also include RFID technology for contactless payments, which can still transmit your credit card information to a snooping thief.

**Applying Concepts 6-2**

### Examine Wireless Security Settings

Now that you understand some of the security options available for a wireless network connection, let’s explore how to check the current settings on your AP and change them if necessary. Using a Windows 10 computer that is connected to a local network via Wi-Fi, complete the following steps:

1. 1

Open the Network and Sharing Center. Under View your active networks, click the Wi-Fi connection and then click **Wireless Properties**.

1. 2

In the Wireless Network Properties dialog box, look for the following information on both the Connection and the Security tabs.

* 1. What are the network’s Name and SSID?
  2. Is the connection configured to connect automatically when the wireless network is in range?
  3. What are the network’s Security and Encryption types?

**Remember This…**

* Compare Wi-Fi encryption standards: WPA/WPA2 Personal and WPA/WPA2 Enterprise.
* Explain the roles of AES and TKIP in Wi-Fi encryption.
* Describe Wi-Fi authentication technologies: RADIUS, EAP, and 802.1X.
* Apply Wi-Fi security practices: MAC filtering, antenna placement, power levels, guest network isolation, geofencing, and captive portals.

**Self-Check**

1. Which Wi-Fi encryption standard was designed to use AES encryption?

Answer

* 1. WPA
  2. WPA2
  3. WEP
  4. WEP2

1. Which standard adapted EAP to WLANs?

Answer

* 1. 802.11g
  2. 802.11i
  3. 802.1X
  4. 802.3

**You’re Ready**

You’re now ready to complete [Project 6-3: Optimize Wireless Security on a SOHO Router](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 6-5Troubleshooting Wi-Fi Networks

### Certification

* 5.2

Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

* 5.4

Given a scenario, troubleshoot common wireless connectivity issues.

Average reading time: 22 minutes

You’ve already learned about several tools used to test copper and fiber-optic cables in Ethernet networks. Cable continuity and performance testers, of course, will tell you nothing about the wireless connections, nodes, or access points on a network. For that, you need tools that contain wireless NICs and run wireless protocols. As you learned earlier in the module, you can start gathering information about a wireless environment by viewing the wireless network connection properties on your workstation. However, this tells you only a little about your wireless environment—and it only applies to one workstation. To get the full picture of your wireless environment, you need to use more advanced wireless network tools, as described in the following section.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-5aWi-Fi Network Tools

Many applications can scan for wireless signals over a certain geographical range and discover all the access points and wireless nodes transmitting in the area. This is useful for determining whether an access point is functioning properly, whether it is positioned correctly so that all the nodes it serves are within its range, whether nodes and access points are communicating over the proper channels within a frequency band, and whether wireless signals are present that shouldn’t be. Here are two tools you need in your toolkit:

* [**Spectrum analyzer**](javascript://)—A device that can assess the quality of a wireless signal by scanning a band of frequencies for signals and noise. A spectrum analysis is useful, for example, to ascertain where interference is greatest.
* [**Wi-Fi analyzer**](javascript://)—Software that can evaluate Wi-Fi network availability as well as help optimize Wi-Fi signal settings or help identify Wi-Fi security threats. Identifying the wireless channels being used nearby helps you optimize wireless channel utilization in your vicinity.

Software tools that can perform wireless network assessment are often available for free and might be provided by the access point’s manufacturer. Following is a list of specific capabilities common to wireless network testing tools:

* Identify transmitting APs, nodes, and the channels over which they are communicating
* Measure signal strength from and determine the range of an AP
* Indicate the effects of attenuation, signal loss, and noise
* Interpret signal strength information to rate potential AP locations
* Ensure proper association and reassociation when moving between APs
* Capture and interpret traffic exchanged between APs and nodes
* Measure throughput and assess data transmission errors
* Analyze the characteristics of each channel within a frequency band to indicate the clearest channels

A Wi-Fi analyzer can help you identify the channels being used by area wireless networks. Wireless networks perform best when using channels not used by nearby networks. For this reason, it’s best to program the network for channels at the beginning, center, and end of the channel bandwidth. For example, recall that 2.4 GHz-band devices offer up to 14 channels, although most only offer 11 channels in the United States. In the United States, then, neighboring Wi-Fi networks typically use channels 1, 6, and 11 to minimize overlap. When all 14 channels are available, such as in many parts of Europe, the channel spread might still be 1-6-11 to maximize compatibility with devices from other areas of the world, or it might instead be 1-5-9-13 to maximize use of the available bandwidth.

If your wireless network is programmed for the same channel as your neighbor’s wireless network, you will get better performance by changing your network’s channel to part of the band not currently in use in your vicinity. In reality, many home routers are configured to automatically seek the least crowded channel.

**Note 6-6**

In a project at the end of this module, you’ll have the opportunity to practice using a Wi-Fi analyzer app on your smartphone.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-5bAvoid Pitfalls

You might have had the frustrating experience of not being able to log on to a network, even though you were sure you’d typed in your username and password correctly. Maybe it turned out that your Caps Lock key was on, changing your case-sensitive password. Or maybe you were trying to log on to the wrong server. On every type of network, many variables must be accurately set on clients, servers, and connectivity devices for communication to succeed. Wireless networks add a few more variables. Following are some wireless configuration pitfalls to avoid, according to the problem you’re facing.

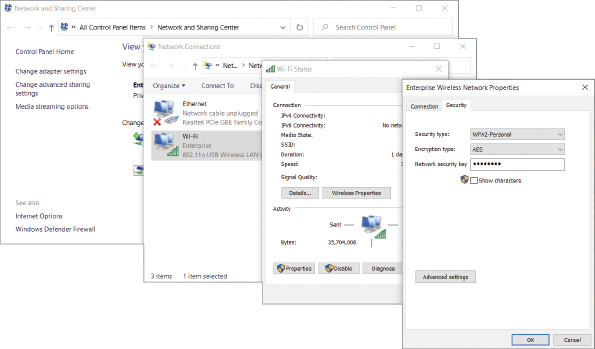
### No Connection

When you can’t get the Wi-Fi client to connect to the AP at all, consider the following common issues:

* **Wrong SSID**—Your wireless client must select the correct SSID. As you have learned, you may instruct clients to search for any available access point (or clients might be configured to do this by default). However, if the access point does not broadcast its SSID, or if your workstation is not configured to look for access points, you will have to enter the SSID during client configuration. Also, bear in mind that SSIDs are case sensitive. That is, MYHOUSE does not equal MyHouse.
* **Encryption protocol mismatch**—Your wireless client must be able to use and must be configured to allow the same encryption protocols that your access point offers. Most of the time, this is negotiated automatically between the AP and the client. To configure the security type manually on a Windows 10 client, open the Network and Sharing Center, click Change adapter settings, right-click the active connection and click Status, and then open the connection’s Properties dialog box. Click the Security tab to change the security type, encryption type, or network security key, as shown in [Figure 6-33](javascript://).
* **Incorrect passphrase**—Similarly, you must use a security key, or passphrase, that matches that of the access point. If incorrect, your client cannot authenticate with the access point.
* **Static channel utilization**—You have learned that the access point establishes the channel and frequency over which it will communicate with clients. Clients, then, automatically sense the correct channel and frequency. However, if you have instructed your client to use only a channel or frequency different from the one your access point uses, association will fail to occur.
* **Mismatched RF band**—Some wireless devices are designed to use only one Wi-Fi band. For example, when purchasing wireless security cameras, these devices might be limited to work only in the 2.4 GHz band. In that case, you’ll need an AP that offers a Wi-Fi standard on that band.
* **Mismatched standards (802.11 b/a/g/n/ac/ax)**—If your access point is set to communicate only via 802.11ac, even if the documentation says it supports 802.11n and 802.11ac, clients must also follow the 802.11ac standard. Clients might also be able to detect and match the correct type of 802.11 standard. However, if they are configured to follow only one standard, they won’t find an access point broadcasting via a different standard.
* **Long AP association time**—Sometimes a Wi-Fi client gets stuck waiting for the association process to complete. While this problem can be caused by many factors (for example, confirm the passphrase is correct), some of the most common issues are users trying to connect at the edge of the network’s covered range or moving throughout the network where the device must frequently reassociate with a nearby AP. A client trying to connect with a Wi-Fi network must be able to receive a strong enough signal from the AP in order to complete the association process because, if packets are missed due to a weak signal, the association will not complete.

**Figure 6-33**

Adjust a network connection’s security settings



Enlarge Image

### Slow Connections

When dealing with slow Wi-Fi connections, consider the following common issues:

* **Insufficient wireless coverage**—On a network, many factors can cause data errors and a resulting decrease in performance. Be sure to check the recommended geographic range for your AP, and keep clients well within that distance. If a client is too far from an AP or if there are too many obstacles between the two nodes, communication might occur, but data errors become more probable and slow down communication. You can confirm whether this is the problem by checking the RSSI level at the client’s location. Also remember to place your AP in a high spot for best signal transmission to clients.
* **RF attenuation/signal loss**—Each access point’s power level, or the strength of the signal the access point emits, should be optimized for the geographic area covered by that AP. Power levels that are too low will result in dropped signals as clients roam to the peripheral areas of the AP’s range. However, maxed out power levels will result in too much overlap between AP coverage areas, causing clients from other coverage areas to attempt to connect with APs that are farther away but transmitting the stronger signal. Begin with a 50 percent power setting, and make incremental changes as needed to optimize the amount of overlap between APs. You can use site survey information and a Wi-Fi analyzer to help you determine where dead spots might require a boost in transmission power or perhaps a range extender to fill in those areas with a strong signal. Also keep in mind that even if a client can receive a signal from a high-powered AP installed on the other end of the building, the return signal from the client might not be reliably strong enough to reach the AP, which is called a near–far effect.
* **Interference**—If intermittent and difficult-to-diagnose wireless communication errors occur, interference might be the culprit. Check for sources of EMI, such as fluorescent lights, heavy machinery, cordless phones, and microwaves in the data transmission path.
* **Channel overlap**—Using channels or frequencies that are too close to each other on the frequency spectrum can interfere with each other’s transmissions. You can use a Wi-Fi analyzer to determine which channels are being used by nearby wireless networks, and then utilize a less crowded channel. Most home routers are programmed to do this automatically. However, keep in mind that you might need to switch bands for your device to find a relatively clear channel.
* **Wireless standard specifications**—Each Wi-Fi standard (802.11 b/a/g/n/ac/ax) is restrained by specific throughput, speed, and distance limitations. Choosing the correct standard for a specific network’s needs can make a significant difference in the effectiveness of the signal. For example, a small home network might function fine with an older Wi-Fi standard if the homeowner only uses a few devices for checking email or surfing the web. However, consider a business that relies on VoIP for communicating with customers all day long, a homeowner who frequently streams movies online or spends a lot of time gaming, or a large warehouse where devices must communicate with the network from anywhere within the building. In all these cases, a newer Wi-Fi standard will offer more appropriate throughput rates and more reliable coverage distances.
* **Simultaneous wired and wireless connections**—A workstation is designed to transmit either via a wired or a wireless connection, but not both at the same time. When troubleshooting connection issues, consider whether the computer is making conflicting attempts to communicate with the network through both types of connections. You can resolve the issue by disabling the Wi-Fi adapter or by unplugging the Ethernet cable.
* **Problems with firmware updates**—Updates to a NIC or access point’s firmware can help patch vulnerabilities and increase functionality. The flip side of this issue, however, is that updates should be tested before being rolled out system wide.
* **Incorrect antenna type**—You might think that omnidirectional antennas would nearly always be the best choice when setting up Wi-Fi coverage. The idea is to place the AP in the center of its coverage area and then send the signal out in all directions. However, in many situations, installing unidirectional antennas instead will enhance a signal’s availability, directing the signal right where you need it while not wasting a signal in areas where you don’t. For example, suppose a company installs an omnidirectional antenna near a factory’s 30-foot-high ceiling. Because the antenna’s signal is broadcast in all directions from its location, distributing its signal strength in a spherical shape, the best possible signal would only be available to workers who could walk on the ceiling—obviously, that’s not a viable situation. To be useful, the signal needs to be directed down to the floor. A unidirectional antenna, in this case, can be positioned up high and pointed down to create a dome-shaped coverage that spreads out as it nears the plant floor, as shown in [Figure 6-34](javascript://).
* **Mismatched antenna polarization**—Radio waves radiating from an antenna emanate from the antenna either along the antenna’s vertical axis or along its horizontal axis. This is called the antenna’s [**polarization**](javascript://), and it’s important to know so you can position the antenna for maximum coverage through the intended range. Most Wi-Fi antennas are vertically polarized, meaning the antenna should point straight up to get the best coverage. However, some devices with multiple antennas might be intended to have antennas pointing in different directions, such as one diagonally to the left, another diagonally to the right, and a center antenna pointing straight up. But this is not always the case when a home router has multiple antennas—sometimes all the antennas should be pointed straight up. It’s important to check manufacturer recommendations for antenna orientation to optimize the signal’s reach.

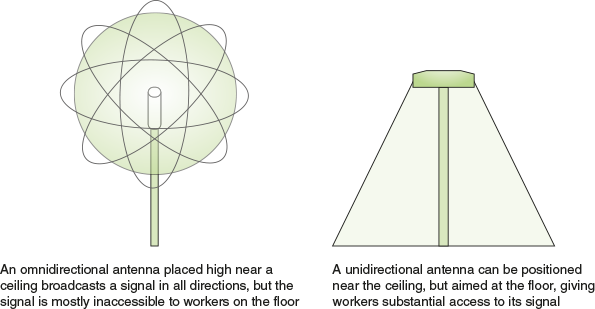
**Note 6-7**

Consider that Wi-Fi clients also have antennas with polarization limitations. For example, in most laptops, the Wi-Fi antenna is wrapped around the screen just inside the outer edge of the top lid. If you tip the laptop on its side, or if the laptop’s lid is oriented at an unusual angle, you’ll likely experience significantly decreased performance on its Wi-Fi connection. The better aligned the AP’s and client’s antennas are to each other, the better quality connection.

* **Client saturation or overcapacity**—APs vary in the number of device connections they can handle at any given time. A SOHO network’s AP might take 10–15 devices before becoming overwhelmed, whereas a high-powered, commercial AP can handle a much larger client load without exceeding its bandwidth saturation limitations. The Wi-Fi 5 and Wi-Fi 6 standards also provide the advantage of expanding available bandwidth while also managing that bandwidth more efficiently to support more clients. When shopping for a new AP, keep in mind that the actual, effective capacity in the real world will be significantly less than the AP’s advertised capacity.
* **Client disassociation issues**—If your Wi-Fi client device is frequently disassociating from the AP, confirm the AP is not using an overly crowded Wi-Fi channel and consider using a narrower channel (such as 20 MHz or 40 MHz) rather than a larger, bonded channel. Also check for interference in the area that could be degrading the signal and breaking the communication between AP and client.

**Figure 6-34**

A unidirectional antenna provides more efficient signal coverage in this situation



Enlarge Image

**Applying Concepts 6-3**

### Snail-Speed Wi-Fi

Your company recently rented new office space across town to make room for expansion in the Accounting Department, and part of your responsibility with the new acquisition was to install three new 802.11ac APs. You carefully planned and then installed each AP throughout the building to optimize wireless coverage and minimize dead zones. Each AP overlaps somewhat with one or both the other APs, and they’re all set with the same ESSID and channel so clients can roam freely. You’ve checked and double-checked the signal strength at each workstation and in all common work areas, such as meeting rooms, lobby, and even the lunchroom.

You completed the job just before the weekend, at the same time as the 19 accounting employees finished setting up their file cabinets and reception area furniture. Some of your fellow IT technicians completed workstation setup that same day; most of the workstations are connected to the network via Wi-Fi due to restrictions imposed by your company’s contract with the property owner. Today, Monday, the accounting personnel report for work at the new building.

At first, the new remote office’s network seems to be working fine. The local network is communicating well with the home office’s network, and everyone has access to all the files they need on the file servers. As everyone gets settled in for the day and starts their Monday duties, however, the network slows to a snail’s pace. It’s not long before you start to get complaints about emails being delayed, files not being accessible, and print jobs to network printers getting lost. You make a beeline across town to figure out what’s wrong.

During your investigation, you find that all the hosts on the local network are accessible. However, you find it odd that even though your ping tests are usually successful, sometimes they aren’t. You know the APs are all new devices, and you double-check their configurations to try to determine a common source for all the problems you’ve noted. Here’s a summary of the results you’ve gathered:

* All three APs are active and communicating successfully with your laptop.
* All three APs are configured with identical ESSIDs and other settings.
* For good measure, you also walk around the office space with your wireless analyzer to confirm again there are no significant dead zones or interference.

Why are wireless transmissions being lost in transit? Below are several possible resolutions. Select the best one and explain your reasoning:

1. One of the APs is faulty and not processing transmissions. It should be removed and replaced.
2. The NICs in the employees’ workstations were damaged during the move. Probably several just need to be reseated while some might need to be replaced.
3. The increased interference from people moving around in the office space is interfering with the Wi-Fi signals. Power levels on the APs needs to be increased.
4. The APs should not have the same ESSID. Rename each AP so their ESSIDs don’t match.
5. Three APs are insufficient for the wireless load of the Accounting Department. More APs should be added.
6. The APs are all part of the same LAN and should be separated into isolated LANs.
7. The workstation computers are programmed to search for and connect with the wrong ESSID, or the network keys are entered wrong. Every workstation’s wireless interface settings should be checked.
8. The APs are all programmed to use the same channel. They should be programmed for different channels.

**Remember This…**

* Use a spectrum analyzer or Wi-Fi analyzer to evaluate a Wi-Fi network’s signals.
* Explain the specifications and limitations of various Wi-Fi standards.
* Consider antennas, channels, AP settings, and information from a site survey in troubleshooting Wi-Fi problems.
* Describe how to diagnose and resolve common Wi-Fi issues, such as interference, channel overlap, SSID and passphrase problems, encryption protocol mismatch, insufficient wireless coverage, or client disassociation issues.

**Self-Check**

1. Which device will let you determine all frequencies within a scanned range that are present in a specific environment, not just Wi-Fi?

Answer

* 1. Wi-Fi analyzer
  2. Captive portal
  3. Wireless LAN controller
  4. Spectrum analyzer

1. Which problem would a low RSSI level indicate?

Answer

* 1. Mismatched standards
  2. Insufficient wireless coverage
  3. Incorrect passphrase
  4. Encryption protocol mismatch

**You’re Ready**

You’re now ready to complete [Project 6-4: Use a Wi-Fi Analyzer App on Your Smartphone](javascript://), or you can wait until you’ve finished the Review Questions for this module.

**You’re Ready**

After you finish the Hands-On Projects, you’re ready to complete the [Module 6 Capstone Projects](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 6-6a**Module Summary**

### Characteristics of Wireless Transmissions

* All wireless signals are carried through the air by electromagnetic waves. The wireless spectrum, commonly called the airwaves, is the frequency range of electromagnetic waves used for data and voice communication. As defined by the FCC (Federal Communications Commission), which controls its use, the wireless spectrum spans frequency ranges or bands between 9 kHz and 300 GHz. Recall that a Hz or hertz is one cycle per second.
* Due to the diverse nature of IoT (Internet of Things) devices and purposes, many kinds of wireless technologies are employed to better serve the needs of these connections, including RFID (Radio Frequency Identification), NFC (near-field communication), Z-Wave, ZigBee, Bluetooth, ANT+, and IR (infrared).
* Most wireless devices implement one of two technologies to take advantage of the frequencies within its band to avoid interference. FHSS (frequency hopping spread spectrum) consists of short bursts of data transmitted on a particular frequency within the band, and the next burst goes to the next frequency in the sequence. DSSS (direct sequence spread spectrum) creates data streams that are divided and encoded into small chunks, called chips, which are spread over all available frequencies within one of three, wide channels, all at the same time.
* An antenna’s radiation pattern describes the relative strength over a three-dimensional area of all the electromagnetic energy the antenna sends or receives. A directional antenna issues wireless signals along a single direction. This type is used when the source needs to communicate with one destination, as in a point-to-point link or in a specific area. An omnidirectional antenna issues and receives wireless signals with (somewhat) equal strength and clarity in all directions, although in the real world, an omnidirectional antenna is never perfectly balanced. This type is used when many receivers or mobile receivers must be able to pick up the signal in many directions.
* You can determine the gain or loss of an access point attached to an external antenna by considering initial power output of the AP, signal loss along the antenna cable (attenuation), and signal gain from the antenna itself. This overall calculation is referred to as EIRP (effective isotropic radiated power) and is measured in dBm (decibels relative to one milliwatt). In contrast, RSSI (received signal strength indicator) measures in dBm the power of the signal on the receiver’s end. The wireless client’s own antenna, distance to the wireless client, and noise in the environment all affect the power of the received signal.
* When an obstacle stands in a signal’s way, the signal might pass through the object, it might be absorbed by the object, or it might be subject to some other phenomena, depending upon the object’s geometry and its constituent materials. The multipath nature of wireless signals gives them a better chance of reaching their destination. However, multiple instances of the same signal can arrive at a receiver at different times. This might cause signals to be misinterpreted, resulting in data errors.

### 802.11 WLAN Standards

* Wi-Fi (wireless fidelity) is a collection of wireless standards and their amendments, extensions, and corrections developed by IEEE’s 802.11 committee. Notable wireless standards developed by the IEEE 802.11 committee and its task groups are 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.
* Beginning with 802.11n, several innovations have been implemented that contribute to making later 802.11 standards much faster and much more reliable: channel bonding, MIMO (multiple input-multiple output), MU-MIMO (multiuser MIMO), OFDMA (Orthogonal Frequency Division Multiple Access), and frame aggregation.
* 802.11 standards specify the use of CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) procedures to access a shared medium. Compared with CSMA/CD (Carrier Sense Multiple Access with Collision Detection), CSMA/CA minimizes the potential for collisions, but it cannot detect the occurrence of a collision and so cannot take steps to recover from the collisions that do occur.
* IEEE terminology includes a couple of notable variations to the standard service set configuration, including IBSS (independent basic service set) using an ad hoc topology, BSS (basic service set) using an infrastructure topology, and ESS (extended service set) using a mesh topology.
* The 802.11 data frame contains four address fields; by contrast, the 802.3 (Ethernet II) frame has only two. The transmitter and receiver addresses refer to the access point or another intermediary device (if used) on the wireless network. Another unique characteristic of the 802.11 data frame is its Sequence Control field. This field is used to indicate how a large packet is fragmented—that is, how it is subdivided into smaller packets for more reliable delivery.

### Implementing a Wi-Fi Network

* Many home or office networks include IoT devices and even expandable IoT networks. Today, networking is no longer limited to computing devices. All sorts of things can be connected to a network, from toasters, refrigerators, bathroom scales, and garage doors to watches, lamps, cars, thermostats, doorbells, and even the kitchen sink. The IoT is made up of any device that can be connected to the Internet—that is, any sensor, computer, or wearable device that talks to other devices over a network.
* Larger wireless networks warrant a more systematic approach to access point placement. Before placing APs in every data room, it’s wise to conduct a site survey. A site survey assesses client requirements, facility characteristics, and coverage areas; the resulting site survey report will help you determine an AP arrangement that will ensure reliable wireless connectivity within a given area.
* The setup process for a SOHO router is similar regardless of the manufacturer or model. The variables you will set during installation include administrator password, SSID, security options and credentials, and DHCP options.
* In an enterprise environment, configuring clients for wireless access to the network can entail a much more involved, two-part process: onboarding, which gives the device trusted access to certain portions of the network, and offboarding, which might include permissions to perform a remote wipe to clear a device of important information, permissions, and apps without having physical access to the device.

### Wi-Fi Network Security

* Authentication allows a wireless client to log on to the network, either by providing the correct password for the SSID or by providing user credentials that might be processed by an authentication server. Encryption algorithms can scramble data transmitted over the airwaves into a format that cannot easily be interpreted if the signal is intercepted. The purpose of encryption is to keep information private.
* WEP offered two forms of authentication, neither of which is secure: OSA (Open System Authentication) and SKA (Shared Key Authentication).
* WPA (Wi-Fi Protected Access) dynamically assigns every transmission its own key. 802.11i incorporates an encryption key generation and management scheme known as TKIP (Temporal Key Integrity Protocol), pronounced tee-kip, to improve security for legacy WEP-based devices. TKIP accomplished three significant improvements: message integrity, key distribution, and encryption.
* WPA2 uses CCMP, which is short for Counter Mode with CBC (Cipher Block Chaining) MAC (Message Authentication Code) Protocol and improves wireless security for newer devices that can use WPA2. Whereas TKIP was meant to be backward-compatible as much as possible, CCMP helps ensure data confidentiality with both encryption and packet authentication.
* The Personal versions of WPA and WPA2 are sometimes referred to as WPA-PSK or WPA2-PSK, where PSK stands for Pre-Shared Key. This is the common configuration on home wireless networks in which you need to enter a passphrase for your device to authenticate to the network. The passphrase and the SSID characters are then used to calculate a unique encryption key for each device.
* The most secure Wi-Fi communication is made possible by combining a RADIUS authentication server with WPA or WPA2, known as WPA-Enterprise or WPA2-Enterprise, respectively. RADIUS (Remote Authentication Dial-In User Service) is an open source authentication and authorization service. A RADIUS server can be used to offer a central authentication point for wireless, mobile, and remote users.
* Additional Wi-Fi security configuration options include central AP and antenna placement, geofencing, guest network, wireless client isolation, and captive portal. Also think about how best to give network access to your IoT devices. Hardening your IoT network starts with changing default device names, usernames, and passwords for those devices, creating strong passwords, and using the strongest encryption settings the devices offer. Where possible, use two-factor authentication. Many cybersecurity experts recommend creating an entirely separate Wi-Fi network for all IoT devices, such as a guest network. Disable features you’re not using, and update software and firmware when those updates become available. Finally, don’t access your IoT software and devices when using a public network, such as at a coffee shop.

### Troubleshooting Wi-Fi Networks

* A spectrum analyzer can assess the quality of a wireless signal by scanning a band of frequencies for signals and noise. A spectrum analysis is useful, for example, to ascertain where interference is greatest. A Wi-Fi analyzer can evaluate Wi-Fi network availability as well as help optimize Wi-Fi signal settings or help identify Wi-Fi security threats. Identifying the wireless channels being used nearby helps you optimize wireless channel utilization in your vicinity.
* Common problems that can prevent a wireless client from connecting with an AP include wrong SSID, encryption protocol mismatch, incorrect passphrase, static channel utilization, mismatched RF band, mismatched Wi-Fi standards, and stalled AP association. Common issues that can cause slow Wi-Fi connections include insufficient wireless coverage, RF attenuation, interference, channel overlap, insufficient wireless standards, simultaneous wired and wireless connections, problems with firmware updates, incorrect antenna type, mismatched antenna polarization, client saturation or overcapacity, and client disassociation issues.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 6-6b**Key Terms**

* [**802.11a**](javascript://)
* [**802.11ac**](javascript://)
* [**802.11ax**](javascript://)
* [**802.11b**](javascript://)
* [**802.11g**](javascript://)
* [**802.11n**](javascript://)
* [**802.1X**](javascript://)
* [**ad hoc topology**](javascript://)
* [**AES (Advanced Encryption Standard)**](javascript://)
* [**ANT+**](javascript://)
* [**AP (access point)**](javascript://)
* [**association**](javascript://)
* [**band**](javascript://)
* [**Bluetooth**](javascript://)
* [**brute force attack**](javascript://)
* [**BSS (basic service set)**](javascript://)
* [**BSSID (basic service set identifier)**](javascript://)
* [**BYOD (bring your own device)**](javascript://)
* [**captive portal**](javascript://)
* [**CCMP (Counter Mode with CBC [Cipher Block Chaining] MAC [Message Authentication Code] Protocol)**](javascript://)
* [**channel bonding**](javascript://)
* [**CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**](javascript://)
* [**diffraction**](javascript://)
* [**directional antenna**](javascript://)
* [**DSSS (direct sequence spread spectrum)**](javascript://)
* [**EAP (Extensible Authentication Protocol)**](javascript://)
* [**EAPoL (EAP over LAN)**](javascript://)
* [**EIRP (effective isotropic radiated power)**](javascript://)
* [**ESS (extended service set)**](javascript://)
* [**ESSID (extended service set identifier)**](javascript://)
* [**evil twin**](javascript://)
* [**fading**](javascript://)
* [**FHSS (frequency hopping spread spectrum)**](javascript://)
* [**geofencing**](javascript://)
* [**guest network**](javascript://)
* [**IBSS (independent basic server set)**](javascript://)
* [**infrastructure topology**](javascript://)
* [**interference**](javascript://)
* [**IoT (Internet of Things)**](javascript://)
* [**IR (infrared)**](javascript://)
* [**LOS (line of sight)**](javascript://)
* [**MAC filtering**](javascript://)
* [**MIMO (multiple input-multiple output)**](javascript://)
* [**MU-MIMO (multiuser MIMO)**](javascript://)
* [**NFC (near-field communication)**](javascript://)
* [**OFDMA (Orthogonal Frequency Division Multiple Access)**](javascript://)

* **[offboarding](javascript://)**
* [**omnidirectional antenna**](javascript://)
* [**onboarding**](javascript://)
* [**polarization**](javascript://)
* **probe**
* [**propagation**](javascript://)
* [**PSK (Pre-Shared Key)**](javascript://)
* [**radiation pattern**](javascript://)
* [**RADIUS (Remote Authentication Dial-In User Service)**](javascript://)
* [**range**](javascript://)
* [**RC4 (Rivest Cipher 4)**](javascript://)
* [**reassociation**](javascript://)
* [**reflection**](javascript://)
* [**refraction**](javascript://)
* [**remote wipe**](javascript://)
* [**RFID (Radio Frequency Identification)**](javascript://)
* [**roam**](javascript://)
* [**rogue access point**](javascript://)
* [**RSSI (received signal strength indicator)**](javascript://)
* [**RTS/CTS (Request to Send/Clear to Send)**](javascript://)
* [**scanning**](javascript://)
* [**scattering**](javascript://)
* [**security camera**](javascript://)
* [**site survey**](javascript://)
* [**smart doorbell**](javascript://)
* [**smart refrigerator**](javascript://)
* [**smart speaker**](javascript://)
* [**smart thermostat**](javascript://)
* [**SNR (signal-to-noise ratio)**](javascript://)
* [**spectrum analyzer**](javascript://)
* [**SSID (service set identifier)**](javascript://)
* [**TKIP (Temporal Key Integrity Protocol)**](javascript://)
* [**wavelength**](javascript://)
* [**WEP (Wired Equivalent Privacy)**](javascript://)
* [**Wi-Fi (wireless fidelity)**](javascript://)
* [**Wi-Fi 4**](javascript://)
* [**Wi-Fi 5**](javascript://)
* [**Wi-Fi 6**](javascript://)
* [**Wi-Fi 6E**](javascript://)
* [**Wi-Fi analyzer**](javascript://)
* [**wireless bridge**](javascript://)
* [**wireless client isolation**](javascript://)
* [**wireless LAN controller**](javascript://)
* [**wireless range extender**](javascript://)
* [**wireless spectrum**](javascript://)
* [**WPA (Wi-Fi Protected Access)**](javascript://)
* [**WPA2**](javascript://)
* [**ZigBee**](javascript://)
* [**Z-Wave**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 6-6c**Review Questions**

1. What is the lowest layer of the OSI model at which wired and wireless transmissions share the same protocols?
   1. Layer 4
   2. Layer 3
   3. Layer 2
   4. Layer 1
2. As you’re troubleshooting a dead zone in your office, which measurement will help you determine the edges of the dead zone?
   1. RSSI
   2. Channel
   3. EIRP
   4. Band
3. Which one of the following wireless transmission types requires a clear LOS to function?
   1. Bluetooth
   2. NFC
   3. IR
   4. Wi-Fi
4. Which of the following wireless technologies does not use the 2.4 GHz band?
   1. Z-Wave
   2. Bluetooth
   3. ZigBee
   4. Wi-Fi
5. Which function of WPA/WPA2 security ensures data cannot be read in transit?
   1. Message integrity
   2. Authentication
   3. Encryption
   4. Key distribution
6. Which protocol replaced TKIP for WPA2?
   1. CCMP
   2. WEP
   3. RADIUS
   4. RC4
7. Which 802.11 standard functions in both the 2.4-GHz and 5-GHz bands?
   1. 802.11g
   2. 802.11ac
   3. 802.11b
   4. 802.11ax
8. Which Carrier Sense technology is used on wireless networks to reduce collisions?
   1. CSMA/CD
   2. EAPoL
   3. CSMA/CA
   4. SSID
9. You’ve just completed a survey of the wireless signals traversing the airspace in your company’s vicinity, and you’ve found an unauthorized AP with a very strong signal near the middle of the 100-acre campus. Its SSID is broadcasting the name of a smartphone model. What kind of threat do you need to report to your boss?
   1. Rogue AP
   2. War driving
   3. Evil twin
   4. Hidden node
10. You just settled in for some study time at the local coffee shop, and you pause long enough to connect your smartphone to the Wi-Fi so you can listen to some music while you study. As you’re about to sign in, you realize that you clicked on an SSID called “Free Coffee and Internet.” What kind of security trap did you almost fall for?
    1. Guest network
    2. Captive portal
    3. Evil twin
    4. Brute force attack
11. To exchange information, two antennas must be tuned to the same .
12. What addresses does an 802.11 frame contain that an 802.3 frame does not?
13. When a wireless signal encounters a large obstacle with wide, smooth surfaces, what happens to the signal?
14. Signals traveling through areas in which many wireless communications systems are in use will exhibit a lower  due to the higher proportion of noise.
15. What is the primary difference between how WPA2-Personal and WPA2-Enterprise are implemented on a network?
16. Why do wireless networks generally experience a greater reduction in throughput compared with wired networks?
17. What size bonded channels do 802.11ac and 802.11ax support?
18. What feature of a site survey maps the Wi-Fi signals in your location?
19. You’re setting up a home network for your neighbor, who is a music teacher. She has students visiting her home regularly for lessons and wants to provide Internet access for their parents while they’re waiting on the children. However, she’s concerned about keeping her own data private. What wireless feature can you configure on her AP to meet her requests?
20. Which 802.11X authentication protocol is often used by WLANs?

Go to pg.

[**help**](javascript://)