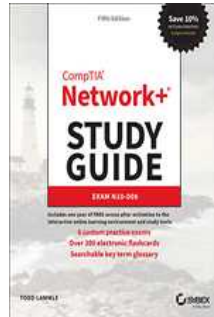


Chapters *To Go*



CompTIA Network+ Study Guide: Exam N10-008, 5th Edition

by Todd Lammler

Sybex. (c) 2021. Copying Prohibited.

Reprinted for Srilakshmi Pamarthi, Training

none@books24x7.com

Reprinted with permission as a subscription benefit of **Skillport**,

All rights reserved. Reproduction and/or distribution in whole or in part in electronic, paper or other forms without written permission is prohibited.



Chapter 12: Wireless Networking

The following CompTia Network+ Exam Objectives are Covered in This Chapter

- **2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.**
 - Networking devices
 - Access point
 - Wireless LAN controller
- **2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.**
 - 802.11 standards
 - a
 - b
 - g
 - n (WiFi 4)
 - ac (WiFi 5)
 - ax (WiFi 6)
 - Frequencies and range
 - 2.4GHz
 - 5GHz
 - Channels
 - Regulatory impacts
 - Channel bonding
 - Service set identifier (SSID)
 - Basic service set
 - Extended service set
 - Independent basic service set (Ad-hoc)
 - Roaming
 - Antenna types
 - Omni
 - Directional
 - Encryption standards
 - WiFi Protected Access (WPA)/WPA2 Personal [Advanced Encryption Standard (AES)/Temporal Key Integrity Protocol (TKIP)]
 - WPA/WPA2 Enterprise (AES/TKIP)
 - Cellular technologies
 - Code-division multiple access (CDMA)

- Global System for Mobile Communications (GSM)
- Long-Term Evolution (LTE)
- 3G, 4G, 5G
- Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)

If you want to understand the basic wireless LANs (WLANs) most commonly used today, just think 10BaseT Ethernet with hubs. What this means is that our WLANs typically run half-duplex communication—everyone is sharing the same bandwidth, and only one user is communicating at a time.

This isn't necessarily bad; it's just not good enough. Because most people rely on wireless networks today, it's critical that they evolve faster than greased lightning to keep up with our rapidly escalating needs. The good news is that this is actually happening—and it even works securely! We'll discuss these newer, faster technologies in this chapter.

The goal in this chapter is to introduce you to wireless networks and the technologies in use today. I'll also cover the various components used, the IEEE 802.11 standards, wireless installation, and of course, wireless security.

Note To find Todd Lammle CompTIA videos and practice questions, please see www.lammle.com.

Introduction to Wireless Technology

Transmitting a signal using the basic 802.11 specifications works a lot like transmitting with a basic Ethernet hub: They're both two-way forms of communication, and they both use the same frequency to both transmit and receive, often referred to as *half-duplex*. Wireless LANs (WLANs) use radio frequencies (RFs) that are radiated into the air from an antenna that creates radio waves. These waves can be absorbed, refracted, or reflected by walls, water, and metal surfaces, resulting in low signal strength. So, because of this innate vulnerability to surrounding environmental factors, it's pretty apparent that wireless will never offer us the same robustness as a wired network can, but that still doesn't mean we're not going to run wireless. Believe me, we definitely will!

We can increase the transmitting power and we'd be able to gain a greater transmitting distance, but doing so can create some nasty distortion, so it has to be done carefully. By using higher frequencies, we can attain higher data rates, but this is, unfortunately, at the cost of decreased transmitting distances. And if we use lower frequencies, we get to transmit greater distances but at lower data rates. This should make it pretty clear to you that understanding all the various types of WLANs you can implement is imperative to creating the LAN solution that best meets the specific requirements of the unique situation you're dealing with.

Also important to note is the fact that the 802.11 specifications were developed so that there would be no licensing required in most countries—to ensure that the user has the freedom to install and operate without any licensing or operating fees. This means that any manufacturer can create wireless networking products and sell them at a local computer store or wherever. It also means that all our computers should be able to communicate wirelessly without configuring much, if anything at all.

Various agencies have been around for a very long time to help govern the use of wireless devices, frequencies, standards, and how the frequency spectrums are used. [Table 12.1](#) shows the current agencies that help create, maintain, and even enforce wireless standards worldwide.

Table 12.1: Wireless agencies and standards

Agency	Purpose	Website
Institute of Electrical and Electronics Engineers (IEEE)	Creates and maintains operational standards	www.ieee.org
Federal Communications Commission (FCC)	Regulates the use of wireless devices in the US	www.fcc.gov
European Telecommunications Standards Institute (ETSI)	Chartered to produce common standards in Europe	www.etsi.org
Wi-Fi Alliance	Promotes and tests for WLAN interoperability	www.wi-fi.org
WLAN Association (WLANA)	Educates and raises consumer awareness regarding WLANs	www.wlana.org

Because WLANs transmit over radio frequencies, they're regulated by the same types of laws used to govern things like AM/FM radios. In the United States, it's the Federal Communications Commission (FCC) that regulates the use of wireless LAN devices, and the Institute of Electrical and Electronics Engineers (IEEE) takes it from there and creates standards based on what frequencies the FCC releases for public use.

The FCC has released three unlicensed bands for public use: 900 MHz, 2.4 GHz, and 5 GHz. The 900 MHz and 2.4 GHz bands are referred to as the Industrial, Scientific, and Medical (ISM) bands, and the 5 GHz band is known as the Unlicensed National Information Infrastructure (U-NII) band. [Figure 12.1](#) shows where the unlicensed bands sit within the RF spectrum.

So it follows that, if you opt to deploy wireless in a range outside the three public bands shown in [Figure 12.1](#), you need to get a specific license from the FCC to do so. Once the FCC opened the three frequency ranges for public use, many manufacturers were able to start offering myriad products that flooded the market, with 802.11AC/AX being the most widely used wireless network found today.

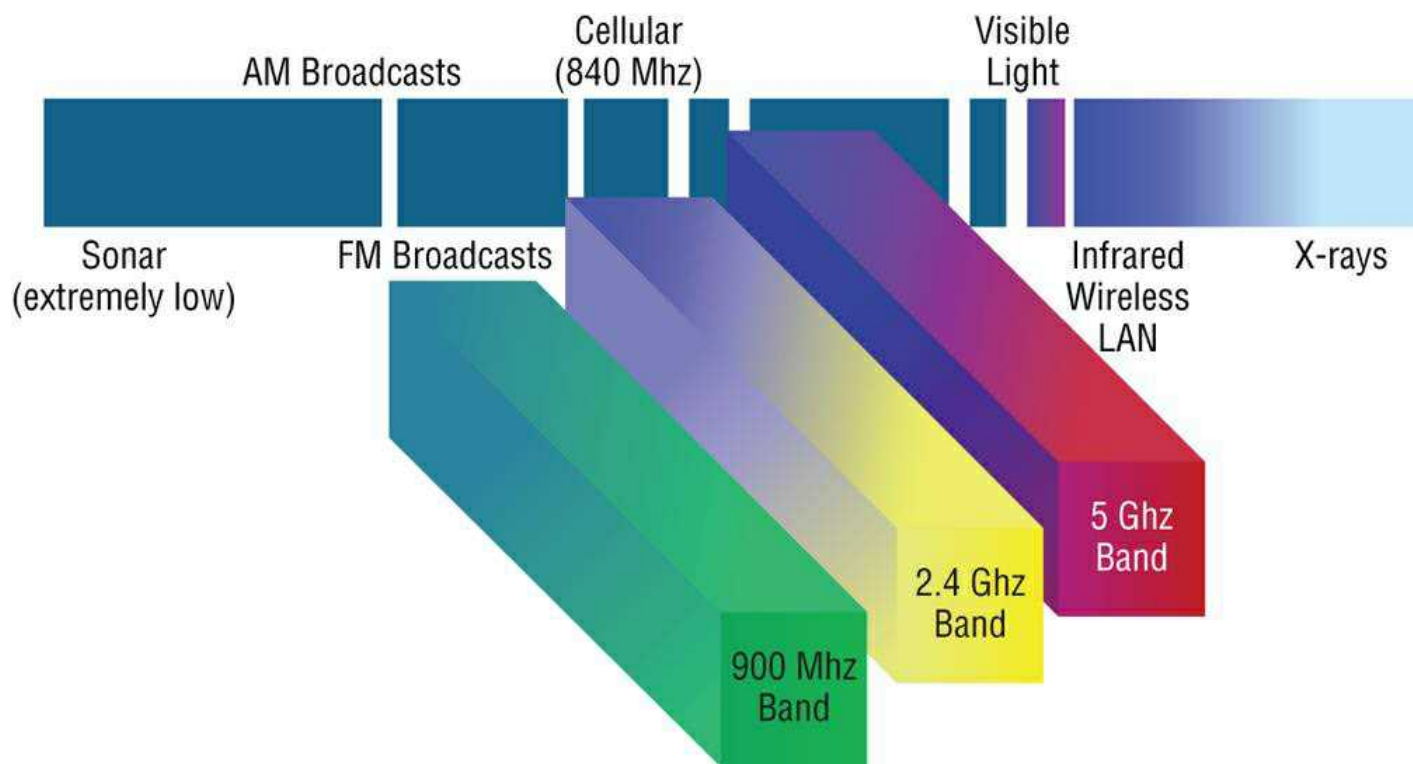


Figure 12.1: Unlicensed frequencies

[Figure 12.2](#) shows the WLAN history that is important to us. Although wireless transmissions date back many, many years, the type we really care about is wireless as related to WLANs starting in the 1990s. Use of the ISM band started in early 1990, and it's deployed today in multiple environments, including outdoor links, mesh networks, office buildings, healthcare facilities, warehouses, and homes.

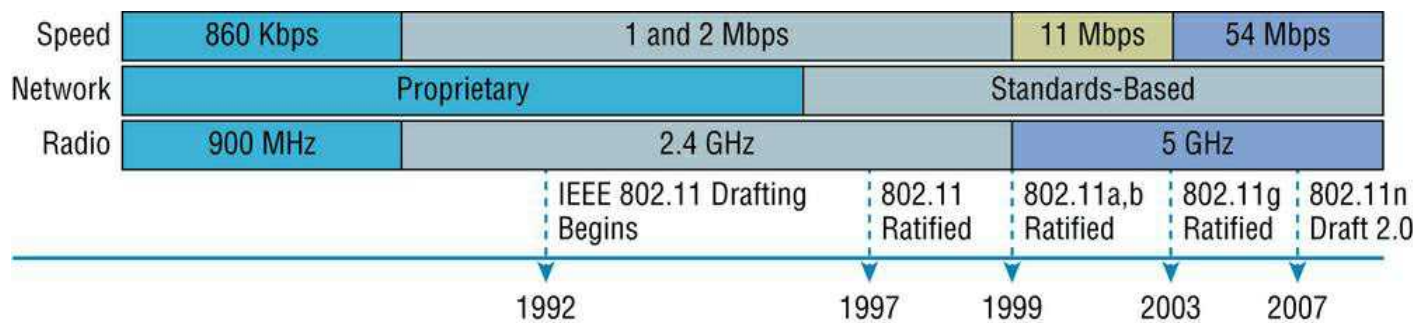


Figure 12.2: Wireless LAN history

802.11ac (now referred to as WiFi 5) was released in December 2013, 802.11ax (WiFi 6) was released in 2019, and although they are not shown in [Figure 12.2](#), I'll discuss these in detail throughout this chapter.

The Wi-Fi Alliance grants certification for interoperability among 802.11 products offered by various vendors. This certification provides a sort of comfort zone for the users purchasing the many types of products, although in my personal experience, it's just a whole lot easier if you buy all your access points from the same manufacturer.

In the current US WLAN market, there are several accepted operational standards and drafts created and maintained by the IEEE. We'll now take a look at these standards and then talk about how the most commonly used standards work.

Cellular Technologies

As part of implementing the appropriate cellular and mobile wireless technologies and configurations, consider the following

options:

- **GSM** Global System Mobile (GSM) is a type of cell phone that contains a subscriber identity module (SIM) chip. These chips contain all the information about the subscriber and must be present in the phone for it to function. One of the dangers with these phones is cell phone cloning, a process where copies of the SIM chip are made, allowing another user to make calls as the original user. Secret key cryptography is used (using a common secret key) when authentication is performed between the phone and the network.
- **FDMA** Frequency-division multiple access (FDMA) is one of the modulation techniques used in cellular wireless networks. It divides the frequency range into bands and assigns a band to each subscriber. This was used in 1G cellular networks.
- **TDMA** Time-division multiple access (TDMA) increases the speed over FDMA by dividing the channels into time slots and assigning slots to calls. This also helps to prevent eavesdropping in calls.
- **CDMA** Code division multiple access (CDMA) assigns a unique code to each call or transmission and spreads the data across the spectrum, allowing a call to make use of all frequencies.
- **3G** This third generation (3G) of cellular data networks was really a game changer at 1G and 2G and allowed the basics to get smartphones working and achieving usable data speeds (sort of), but 2 Mbps was a lot of bandwidth in the 1990s and really provided us with the start of smartphone applications, which lead to more research and technologies and of course the plethora of applications we now have.

The 2G networks handled phone calls, basic text messaging, and small amounts of data over a protocol called MMS. When 3G connectivity arrived, a number of larger data formats became much more accessible, such as HTML pages, videos, and music, and there was no going back!

- **4G** The term 4G stands for fourth generation of speed and connection standards for cellular data networks. The speeds really helped push smartphones to customers as it provided from 100 Mbps up to 1 Gbps, but you'd have to be in a 4G mobile hotspot to achieve the maximum speed.
- **LTE** Most of 4G networks were called Long-Term Evolution (LTE), which was also called 4G LTE. Although 5G has taken over and 6G is probably here to stay, LTE is still prevalent in many markets, and I still see it on my phones at times. The reality is that in the 2000s your phone would display "4G," but it couldn't really provide what the standard mandated.

When the cellular standards bodies set the minimum speeds for 4G, they could never reach those speeds, even though cell carriers spend millions trying to get them. Because of this, the regulating body decided that LTE (which really was just the pursuit of the 4G standard) could be labeled as 4G as long as it provided an improvement over the 3G technology speeds.

- **5G** This stands for "fifth generation" of cellular technology and is a standard for mobile telecommunications service that is significantly faster than today's 4G technology, up to 100xs faster.

Since this technology has been out for years, you know you can upload or download videos and use data-intensive apps or other applications much more quickly and smoothly than what we had in the past with 3G and 4G.

This is because 5G technology utilizes a higher-frequency band of the wireless spectrum called millimeter wave that allows data to be transferred much more rapidly than the lower-frequency band dedicated to 4G.

However, the millimeter wave signals don't travel as far so you need more antennas spaced closer together than the previous wireless 3G and 4G.

[Table 12.2](#) shows us the comparisons between 3G, 4G, and 5G.

Table 12.2: Cellular comparisons

Technology	3G	4G	5G
Deployment	1990	2000	2014
Bandwidth	2 Mbps	200 to 1000 Mbps	1 to 10 Gbps
Standards	WCDMA, CDMA-2000	CDMA, LTE, WiMAX	OFDM, MIMO, nm Waves
Technology	CDMA/IP	Unified IP, LAN/WAN	Unified IP, LAN/WAN

The 802.11 Standards (Regulatory Impacts)

Building on what you learned in Chapter 1, "Introduction to Networks," wireless networking has its own 802 standards group—remember, Ethernet's committee is 802.3. Wireless starts with 802.11. And even cellular networks are becoming huge players in our wireless experience. But for now, we're going to concentrate on the 802.11 standards committee and subcommittees.

IEEE 802.11 was the first, original standardized WLAN at 1 Mbps and 2 Mbps. It runs in the 2.4 GHz radio frequency. It was ratified in 1997, although we didn't see many products pop up until around 1999 when 802.11b was introduced. All the committees listed in [Table 12.3](#) made amendments to the original 802.11 standard except for 802.11F and 802.11T, which produced stand-alone documents.

Note One type of wireless networking that doesn't get a whole lot of attention is infrared wireless. Infrared wireless uses the same basic transmission method as many television remote controls—that's right, infrared technology. Infrared is used primarily for short-distance, point-to-point communications, like those between a peripheral and a PC, with the most widely used for peripherals being the IrDA standard.

Table 12.3: 802.11 committees and subcommittees

Committee	Purpose
IEEE 802.11a	54 Mbps, 5 GHz standard
IEEE 802.11ac	1 Gbps, 5 GHz standard (WiFi 5)
IEEE 802.11ax	Published in Feb 2021, successor to WiFi 5, works in 1 to 6 GHz range to get over 10 Gbit/s
IEEE 802.11b	Enhancements to 802.11 to support 5.5 Mbps and 11 Mbps
IEEE 802.11c	Bridge operation procedures; included in the IEEE 802.1D standard
IEEE 802.11d	International roaming extensions
IEEE 802.11e	Quality of service
IEEE 802.11F	Inter-Access Point Protocol
IEEE 802.11g	54 Mbps, 2.4 GHz standard (backward compatible with 802.11b)
IEEE 802.11h	Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) at 5 GHz
IEEE 802.11i	Enhanced security
IEEE 802.11j	Extensions for Japan and US public safety
IEEE 802.11k	Radio resource measurement enhancements
IEEE 802.11m	Maintenance of the standard; odds and ends
IEEE 802.11n	Higher throughput improvements using multiple-input, multiple-output (MIMO) antennas (WiFi 4)
IEEE 802.11p	Wireless Access for the Vehicular Environment (WAVE)
IEEE 802.11r	Fast roaming
IEEE 802.11s	ESS Extended Service Set Mesh Networking
IEEE 802.11T	Wireless Performance Prediction (WPP)
IEEE 802.11u	Internetworking with non-802 networks (cellular, for example)
IEEE 802.11v	Wireless network management
IEEE 802.11w	Protected management frames
IEEE 802.11y	3650–3700 operation in the US

Now let's discuss some important specifics of the most popular 802.11 WLANs.

2.4 GHz (802.11b)

First on the menu is the 802.11b standard. It was the most widely deployed wireless standard, and it operates in the 2.4 GHz unlicensed radio band that delivers a maximum data rate of 11 Mbps. The 802.11b standard has been widely adopted by both vendors and customers who found that its 11 Mbps data rate worked pretty well for most applications. But now that 802.11b has a big brother (802.11g), no one goes out and just buys an 802.11b card or access point anymore—why would you buy a 10 Mbps Ethernet card when you can score a 10/100 Ethernet card for the same price?

An interesting thing about all 802.11 WLAN products is that they have the ability to data-rate-shift while moving. This allows the person operating at 11 Mbps to shift to 5.5 Mbps, then 2 Mbps, and finally still communicate farthest from the access point at 1 Mbps. And furthermore, this rate shifting happens without losing the connection and with no interaction from the user. Rate shifting also occurs on a transmission-by-transmission basis. This is important because it means that the access point can support multiple clients at varying speeds depending on the location of each client.

The problem with all 802.11b communication lies in how the Data Link layer is dealt with. In order to solve problems in the RF spectrum, a type of Ethernet contention management was created called *carrier sense multiple access with collision avoidance* (CSMA/CA).

CSMA/CA also has an optional implementation called a *Request to Send, Clear to Send (RTS/CTS)* because of the way that hosts must communicate with the access point (AP). For every packet sent, an RTS/CTS and acknowledgment must be received, and because of this rather cumbersome process, it's kind of hard to believe it all actually works when you use this!

To get a clear picture of this, check out [Figure 12.3](#).

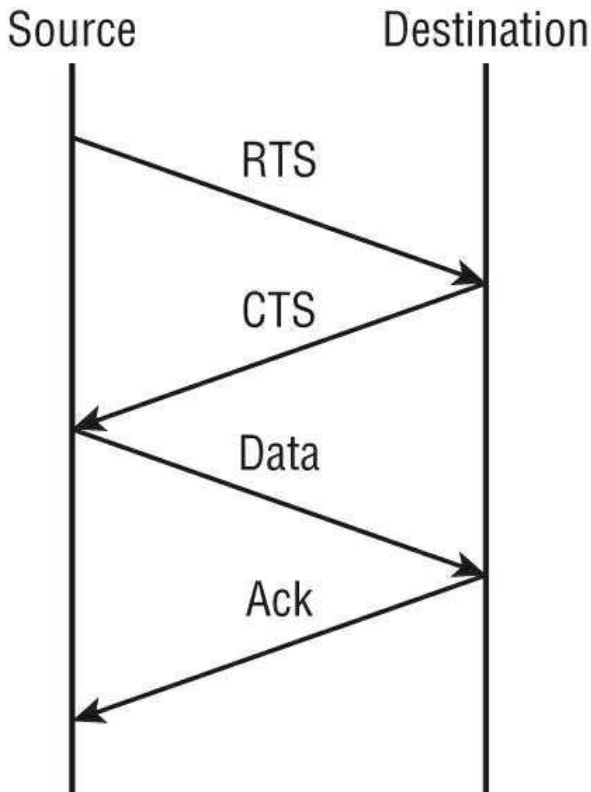


Figure 12.3: 802.11b CSMA/CA

2.4 GHz (802.11g)

The 802.11g standard was ratified in June 2003 and is backward compatible to 802.11b. The 802.11g standard delivers the same 54 Mbps maximum data rate as you'll find in the 802.11a range but runs in the 2.4 GHz range—the same as 802.11b.

Because 802.11b/g operates in the same 2.4 GHz unlicensed band, migrating to 802.11g is an affordable choice for organizations with existing 802.11b wireless infrastructures. Just keep in mind that 802.11b products can't be "software upgraded" to 802.11g. This limitation is because 802.11g radios use a different chipset in order to deliver the higher data rate.

But still, much like Ethernet and Fast Ethernet, 802.11g products can be commingled with 802.11b products in the same network. Yet, for example, and completely unlike Ethernet, if you have four users running 802.11g cards and one user starts using an 802.11b card, everyone connected to the same access point is then forced to run the 802.11b signal modulation method—an ugly fact that really makes throughput suffer badly. So to optimize performance, it's recommended that you disable the 802.11b-only modes on all your access points.

To explain this further, 802.11b uses a *modulation technique* called *direct-sequence spread spectrum (DSSS)* that's just not as robust as the *orthogonal frequency-division multiplexing (OFDM)* modulation used by both 802.11g and 802.11a. 802.11g clients using OFDM enjoy much better performance at the same ranges as 802.11b clients do, but—and remember this—when 802.11g clients are operating at the 802.11b rates (11 Mbps, 5.5 Mbps, 2 Mbps, and 1 Mbps), they're actually using the same modulation 802.11b uses.

So, regarding the throughput of different WLAN standards, you know that 802.11b has a top throughput of 11 Mbps, and 802.11g has a top throughput of 54 Mbps. But with that said, do you really think we're actually getting that type of throughput? The answer is absolutely not! This is because in reality, about 70 percent or more of the RF bandwidth is used for the management of the wireless network itself! The actual bandwidth the user experiences using an application is called *goodput*, even though you won't hear this term used a lot. Just remember that *goodput* refers to the actual data throughput, not the theoretical number that the standards describe.

[Figure 12.4](#) shows the 14 different channels (each 22 MHz wide) that the FCC released in the 2.4 GHz range.

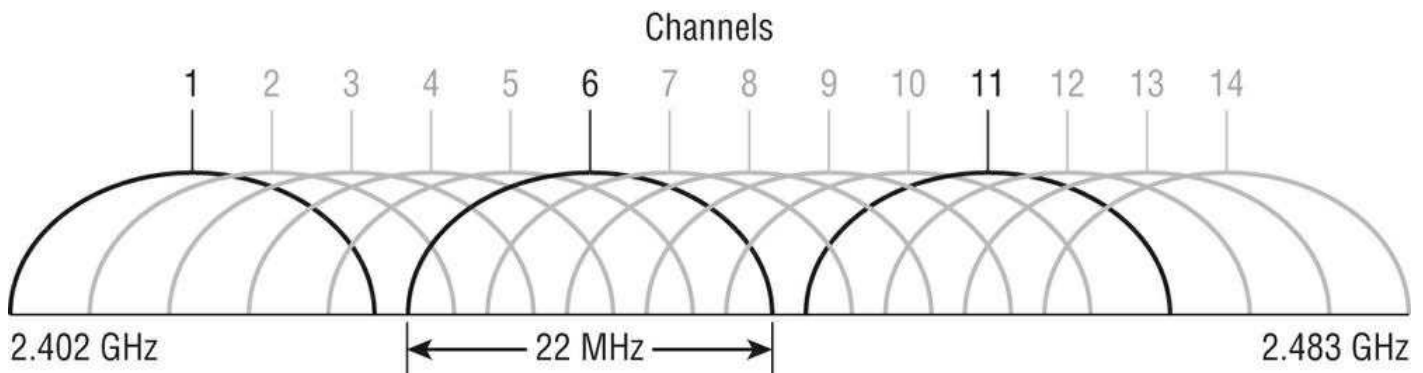


Figure 12.4: ISM 2.4 GHz channels

In the United States, only 11 channels are configurable, with channels 1, 6, and 11 being non-overlapping. This allows you to have three access points in the same area without experiencing interference. You must be aware of the channels when installing APs in a large environment so you do not overlap channels. If you configure one AP with channel 1, then the next AP would be configured in channel 11, the channel farthest from that configured on the first AP.

5 GHz (802.11a)

The IEEE ratified the 802.11a standard in 1999, but the first 802.11a products didn't begin appearing on the market until late 2001—and boy, were they pricey! The 802.11a standard delivers a maximum data rate of 54 Mbps with 12 non-overlapping frequency channels. [Figure 12.5](#) shows the U-NII band.

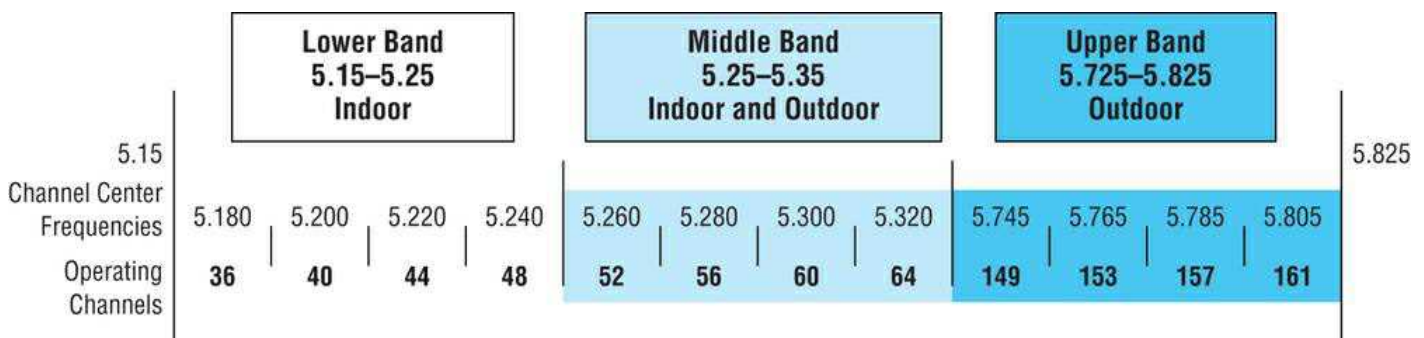


Figure 12.5: U-NII 5 GHz band has 12 non-overlapping channels (US)

Operating in the 5 GHz radio band, 802.11a is also immune to interference from devices that operate in the 2.4 GHz band, like microwave ovens, cordless phones, and Bluetooth devices. 802.11a isn't backward compatible with 802.11b because they are different frequencies, so you don't get to just "upgrade" part of your network and expect everything to work together in perfect harmony. But no worries—there are plenty of dual-radio devices that will work in both types of networks. A definite plus for 802.11a is that it can work in the same physical environment without interference from 802.11b users.

Similar to the 802.11b radios, all 802.11a products also have the ability to data-rate-shift while moving. The 802.11a products allow the person operating at 54 Mbps to shift to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 9 Mbps, and finally, still communicate farthest from the AP at 6 Mbps.

There's also an extension to the 802.11a specification called 802.11h, which is described next.

5 GHz (802.11h)

The FCC added 11 new channels in February 2004, and in 2008, we were finally able to begin using these channels based on manufacturers' releases of more 802.11a 5 GHz products. This means that we gained access to up to 23 non-overlapping channels! And there are even two new features to the 5 GHz radio that are part of the 802.11h specification: *Dynamic Frequency Selection (DFS)* and *Transmit Power Control (TPC)*.

- **Dynamic Frequency Selection (DFS)** This cool feature continuously monitors a device's operating range for any radar signals that are allowed to operate in portions of the 5 GHz band as well as 802.11a before transmitting. If DFS discovers any radar signals, it'll either abandon the occupied channel or mark it as unavailable to prevent interference from occurring on the WLAN.
- **Transmit Power Control (TPC)** Even though it's been employed by the mobile phone industry for a long time, this

technology has some handy new uses. You can set the client machine's adapter and the access point's transmit power to cover various size ranges—a feature that's useful for many reasons. For one, setting the access point's transmit power to 5 milliwatts (mW) reduces cell range, which works great if you've got a compact area with high-density usage.

Further advantages include the fact that TPC enables the client and the access point to communicate with less power. This means the client machine can fine-tune its transmit power dynamically so it uses just enough energy to preserve its connection to the access point and conserve its battery power plus reduce interference on the neighboring WLAN cells—sweet!

2.4 GHz/5 GHz (802.11n)

802.11n builds on previous 802.11 standards by adding *multiple-input, multiple-output (MIMO)*, which employs multiple transmitters and receiver antennas to increase data throughput. 802.11n can have up to eight antennas, but most of today's access points use four. These are sometimes referred to as *smart antennas*, and if you did have four of them, two would be used for transmitting simultaneously with the other two receiving simultaneously. This setup allowed for much higher data rates than 802.11a/b/g. In fact, the marketing people claim it provided about 250 Mbps, but personally, I've never really seen that level of throughput with 802.11n. Even if what they're saying is true, exactly how would that help if all you've got is a 100 Mbps DSL connection to the Internet?

Note 802.11n allows for communication at both the 2.4 GHz and 5 GHz frequencies by using channel bonding.

Unlike 802.11a and 802.11g, which are locked into using the 5.0 GHz and 2.4 GHz spectrums, respectively, with 802.11n you can allow one, the other, or both spectrums in your WLAN! Listed next are some additional components of 802.11n that give people reason to say 802.11n has greater reliability and predictability:

- **40 MHz Channels** 802.11g and 802.11a use 20 MHz channels, and tones on the sides of each channel are not used to protect the main carrier, which means that 11 Mbps are unused or wasted. However, 802.11n aggregates two 40 MHz carriers to double the speed from 54 Mbps to 108 Mbps, and add the 11 Mbps that we gain from not wasting the side tones and we have 119 Mbps.
- **MAC Efficiency** 802.11 protocols require acknowledgment of each and every frame. 802.11n can pass many packets before an acknowledgment is required, which saves you on overhead. This is called *block acknowledgment*.
- **Multiple-Input, Multiple-Output (MIMO)** Several frames are sent by several antennas over several paths and are then recombined by another set of antennas to optimize throughput and multipath resistance. This is called *spatial multiplexing*.
- **Multuser Multiple-Input, Multiple-Output (MU-MIMO)** MU-MIMO is an enhancement over the original MIMO technology. It allows antennas to be spread over a multitude of independent access points. MU-MIMO does not directly affect data rates. What it does do, though, is help multiple devices like Wi-Fi routers coordinate when they communicate with one another better and faster than before. Overall, because MU-MIMO allows multiple devices to transmit at once, it makes more efficient use of channels.

So What Is Wi-Fi?

You may have seen products that are 802.11 compliant with a small sticker on them that says "Wi-Fi." You might be able to guess that this rather odd phrase stands for Wireless Fidelity, but you may not know what its implications are. Simply put, that sticker indicates that the product in question has passed certification testing for 802.11 interoperability by the Wi-Fi Alliance. This nonprofit group was formed to ensure that all 802.11a/b/g/n/ac/ax wireless devices would communicate seamlessly. So, Wi-Fi is a good thing.

5 GHz (802.11ac)

802.11ac is a Wi-Fi standard that works in the 5 GHz range and delivers up to 1 gigabit throughput that was approved by the 802.11 standards committee in January 2014. Still, just as it is with 802.11n, you won't find that the speeds described in the standard actually line up with the marketing material.

For example, for a single link, which is basically one host to AP, the best throughput you can hope to get would be 500 Mbps, which is fantastic if it actually happens! But unless you have a Gigabit Internet connection, 802.11ac won't really help so much. To be fair, in a small network, or if you're transferring files in your internal WLAN or to your internal network, this new specification could actually be useful.

At this point, you're probably wondering how these people can claim to achieve these theoretical rates, right? That's an excellent question! They get these values by increasing the RF band usage from 20 MHz wide channels with 802.11a/b/g to 40 MHz with

802.11n and up to 160 MHz wide channels with 802.11ac. But again, for typical commercial 802.11ac products, 80 MHz would be a lot more realistic. The problem with this scenario centers on the fact that if any interference is found in the 80 MHz wide channel, it drops down to 40 MHz wide channels. Worse, if interference is still found at that level, it will drop even further down to 20 MHz wide channels.

In addition to the wider channels, we can also get more MIMO spatial streams than we can with 802.11n—up to eight, where 802.11n only supported four. Furthermore, and optionally, a downlink of multiuser MIMO (MU-MIMO) supports up to four clients and, most important, a modulation of QAM-256 compared to QAM-64 with 802.11a/g.

The last thing I want to point out is the fact that 802.11n had added fields in the wireless frame to identify 802.11a and 802.11g as high throughput (HT), whereas 802.11ac adds four fields to identify the frames as very high throughput (VHT).

WiFi 6 (802.11ax)

So, what is WiFi 6 and is it faster than WiFi 5? Well, I would hope so since it is one number greater than 5, but that is only because this is the sixth generation of Wi-Fi with enough changes to possibly give us twice the speed, but only time will tell if that is true.

To say that 802.11ax and Wi-Fi 6 are the same thing would definitely be true, and it's great marketing right now for the Wi-Fi manufacturers.

[Figure 12.6](#) shows the difference between 802.11ac (WiFi 5) and 802.11.ax (WiFi 6), and the first thing you should notice is that ax uses both 2.4 and 5 GHz, where ac uses only 5 GHz, and ax has more OFDM symbols and a higher modulation, which provides superior data rates.

TABLE 1: COMPARING WIFI 5 AND WIFI 6 STANDARDS		
Parameter	WiFi 5 (802.11 ac)	WiFi 6 (802.11 ax)
Frequency	5 GHz	2.4 and 5.0 GHz
Bandwidths (channels)	20, 40, 80+80, 160 MHz	20, 40, 80+80, 160 MHz
Access	OFDM	OFDMA
Antennas	MU-MIMO (4 × 4)	MU-MIMO (8 × 8)
Modulation	256QAM	1024QAM
Maximum data rate	3.5 Gb/s	9.6 Gb/s
Maximum users/AP	4	8

Figure 12.6: Comparing WiFi 5 to WiFi 6

This newer Wi-Fi 6 technology includes the following benefits:

- Denser modulation using 1024 Quadrature Amplitude Modulation (QAM), enabling a more than 35 percent speed burst.
- Orthogonal frequency-division multiple access (OFDMA) based scheduling to reduce overhead and latency.

- Robust high efficiency signaling for better operation at a significantly lower received signal strength Indicator (RSSI).
- Better scheduling and longer device battery life with Target Wake Time (TWT).

Comparing 802.11 Standards

Before I move on to wireless installations, take a look at [Figure 12.7](#), which lists, for each of the IEEE standards in use today, the year of ratification as well as the frequency, number of non-overlapping channels, physical layer transmission technique, and data rates.

	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac
Ratified	1997	1999	1999	2003	2010	2013
Frequency Band	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz–5 GHz	5 GHz
No. of Channels	3	3	Up to 23	3	Varies	Varies
Transmission	IR, FHSS, DSSS	DSSS	OFDM	DSSS, OFDM	DSSS, CCK, OFDM	OFDM
Data Rates (Mbps)	1, 2	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	100+
						1000+

Figure 12.7: Current standards for spectrums and speeds

I mentioned earlier that 802.11b runs DSSS, whereas 802.11g and 802.11a both run the OFDM modulation technique (802.11ac runs up to OFDM 256-QAM).

Range and Speed Comparisons

Now let's take a look at [Table 12.4](#), which delimits the range comparisons of each 802.11 standard and shows these different ranges using an indoor open-office environment as a factor. (We'll be using default power settings.)

Table 12.4: Range and speed comparisons

Standard	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Speed	11 Mbps	54 Mbps	54 Mbps	300 Mbps	1 Gbps	3.5+ Gbps
Frequency	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5/6 GHz
Range ft.	100–150	25–75	100–150	>230	>230	Unknown

You can see that to get the full 54 Mbps benefit of both 802.11a and 802.11g, you need to be between 75 feet and 150 feet (maximum) away, which will likely be even less if there happen to be any obstructions between the client and the access point. 802.11n gives more distance than all three standards shown in [figure 12.7](#) (up to twice the distance), and understand that 802.11ac won't give you more distance than 802.11n, but certainly more speed; however, 802.11ax is our future with more than three times the speed of 802.11ac.

Wireless Network Components

Though it might not seem this way to you right now, wireless networks are less complex than their wired cousins because they require fewer components. To make a wireless network work properly, all you really need are two main devices: a wireless access point and a wireless NIC, the latter of which is typically built into your laptop. This also makes it a lot easier to install a wireless network because, basically, you just need an understanding of these two components in order to do so.

Wireless Access Points

You'll find a central component—like a hub or switch—in the vast majority of wired networks that serves to connect hosts together and allow them to communicate with each other. It's the same idea with wireless networks. They also have a component that connects all wireless devices together, only that device is known as a *wireless access point (WAP)*, or just AP. Wireless access points have at least one antenna (typically two for better reception—a solution called *diversity*, and up to eight to support 802.11ac/ax) and an Ethernet port to connect them to a wired network. [Figure 12.8](#) shows an example of a typical wireless access

point.



Figure 12.8: A wireless access point

You can even think of an AP as a bridge between the wireless clients and the wired network. In fact, an AP can be used as a wireless bridge (depending on the settings) to bridge two wired network segments together.

In addition to the stand-alone AP, there is another type of AP that includes a built-in router, which you can use to connect both wired and wireless clients to the Internet (the most popular home brand being Linksys, a division of Cisco). In summary, an AP can operate as a repeater, bridge (switch), or router, depending on its hardware and its implementation.

These devices are usually known as (surprise) wireless routers. They're usually employed as network address translation (NAT) servers by using the one ISP-provided global IP address to multiplex numerous local IP addresses that are generally doled out to inside clients by the wireless router from a pool within the 192.168.x.x range.

Wireless Network Interface Card

Every host that wants to connect to a wireless network needs a wireless *network interface card (NIC)* to do so. Basically, a wireless NIC does the same job as a traditional NIC, but instead of having a socket to plug some cable into, the wireless NIC has a radio antenna. In addition to the different types of wireless networking (I'll talk about those in a minute), wireless NICs (like other NICs) can differ in the type of connection they use to connect to the host computer.

[Figure 12.9](#) shows an example of a wireless NIC.



Figure 12.9: A wireless NIC

The wireless card shown in [Figure 12.9](#) is used in a desktop PC. There are various options for laptops as well. All new laptops have wireless cards built into the motherboard.

Note These days, it's pretty rare to use an external wireless client card because all laptops come with them built in, and desktops can be ordered with them too. But it's good to know that you can still buy the client card shown in [Figure 12.9](#). Typically, you would use cards like the one shown in the figure for areas of poor reception because they can have a better range—depending on the antenna you use, or because you want to upgrade the built-in card to 802.11n/ac/ax. It might be cheaper and easier to just buy a new PC these days.

Wireless Antennas

Wireless antennas act as both transmitters and receivers. There are two broad classes of antennas on the market today: *Omni directional* (or point-to-multipoint) and *directional*, or *Yagi* (point-to-point). Yagi antennas usually provide a greater range than Omni antennas of equivalent gain. Why? Because Yagis focus all their power in a single direction, whereas Omnis must disperse the same amount of power in all directions at the same time. A downside to using a directional antenna is that you've got to be much more precise when aligning communication points. This is why a Yagi is really only a good choice for point-to-point bridging of access points. It's also why most APs use Omnis, because often, clients and other APs could be located in any direction at any given moment.

To get a picture of this, think of the antenna on your car (if you still have an antenna on your car!). Yes, it's a non-networking example, but it's still a good one because it clarifies the fact that your car's particular orientation doesn't affect the signal reception of whatever radio station you happen to be listening to. Well, most of the time, anyway. If you're in the boonies, you're out of range—something that also applies to the networking version of Omnis.

The television aerials that *some* of us are old enough to remember rotating into a specific direction for a certain channel are examples of Yagi antennas. (How many of you labeled your set-top antenna dial for the actual TV stations you could receive?) Believe it or not, they still look the same to this day!

Both Omnis and Yagis are rated according to their signal gain with respect to an actual or theoretical laboratory reference antenna. These ratings are relative indicators of the corresponding production antenna's range. Range is also affected by the bit rate of the underlying technology, with higher bit rates extending shorter distances. Remember, a Yagi will always have a longer range than an equivalently rated Omni, but as I said, the straight-line Yagi will be very limited in its coverage area.

Both antennas are also rated in units of decibel isotropic (dBi) or decibel dipole (dBd), based on the type of reference antenna (isotropic or dipole) of equivalent frequency that was initially used to rate the production antenna. A positive value for either unit of measure represents a gain in signal strength with respect to the reference antenna. *Merriam-Webster* defines *isotropic* as "exhibiting properties (as velocity of light transmission) with the same values when measured along axes in all directions." Isotropic antennas are not able to be produced in reality, but their properties can be engineered from antenna theory for reference purposes.

It's pretty much a given that antennas operating with frequencies below 1 GHz are measured in dBd while those operating above 1 GHz are measured in dBi. But because this rule doesn't always work definitively, sometimes we have to compare the strength of one antenna measured in dBd with another measured in numerically equivalent dBi in order to determine which one is stronger. This is exactly why it's important to know that a particular numerical magnitude of dBd is more powerful than the same numerical magnitude of dBi.

I know this sounds pretty complicated, but because the relationship between these two values is linear, it really makes the conversion a lot easier than you might think. Here's how it works: At the same operating frequency, a dipole antenna has about 2.2 dB gain over a 0 dBi theoretical isotropic antenna, which means you can easily convert from dBd to dBi by adding 2.2 to the dBd rating. Conversely, subtract 2.2 from the dBi rating and you get the equivalent dBd rating.

Armed with what you've learned about the difference between Omni and Yagi antennas and the difference between dBd and dBi gain ratings, you should be able to compare the relative range of transmission of one antenna with respect to another based on a combination of these characteristics. For example, the following four antenna ratings are given in relative order from the greatest to the least range:

- 7 dBd Yagi (equivalent to a 9.2 dBi Yagi)
- 7 dBi Yagi (longer range than 7 dBi Omni)
- 4.8 dBd Omni (equivalent to a 7 dBi Omni)
- 4.8 dBi Omni (equivalent to a 2.6 dBd Omni)

Note If you're having an intermittent problem with hosts connecting to the wireless network and varying signal strengths at different locations, check the location of your antennas in the office or warehouse to make sure you're getting the best coverage possible.

So now that you understand the basic components involved in a wireless network, it's time to use what you learned about the standards we use in our everyday home and corporate wireless networks and the different ways that they're actually installed.

Installing a Wireless Network

Let's say you just bought a wireless AP for your laptop to use to connect to the Internet. What's next? Well, that all depends on the type of installation you want to create with your new toys. First, it's important you understand where to place the AP. For example, you don't want to place the AP on or near a metal filing cabinet or other obstructions. Once you decide on the AP's placement, you can configure your wireless network.

There are two main installation types, ad hoc and infrastructure mode, and each 802.11 wireless network device can be installed in one of these two modes, also called *service sets*.

Ad Hoc Mode: Independent Basic Service Set

This is the easiest way to install wireless 802.11 devices. In this mode, the wireless NICs (or other devices) can communicate directly without the need for an AP. A good example of this is two laptops with wireless NICs installed. If both cards were set up to operate in ad hoc mode, they could connect and transfer files as long as the other network settings, like protocols, were set up to enable this as well. We'll also call this an *independent basic service set (IBSS)*, which is created as soon as two wireless devices communicate.

To set up a basic ad hoc wireless network, all you need are two wireless NICs and two computers. First (assuming they aren't built in), install the cards into the computers according to the manufacturer's directions. During the software installation, you'll be asked if you want to set up the NIC in ad hoc mode or infrastructure mode. For an ad hoc network, you would obviously go with the ad hoc mode setting. Once that's done, all you've got to do is bring the computers within range (90–100 m) of each other, and voilà—they'll "see" each other and be able to connect to each other.

[Figure 12.10](#) shows an example of an ad hoc wireless network. (Note the absence of an access point.)

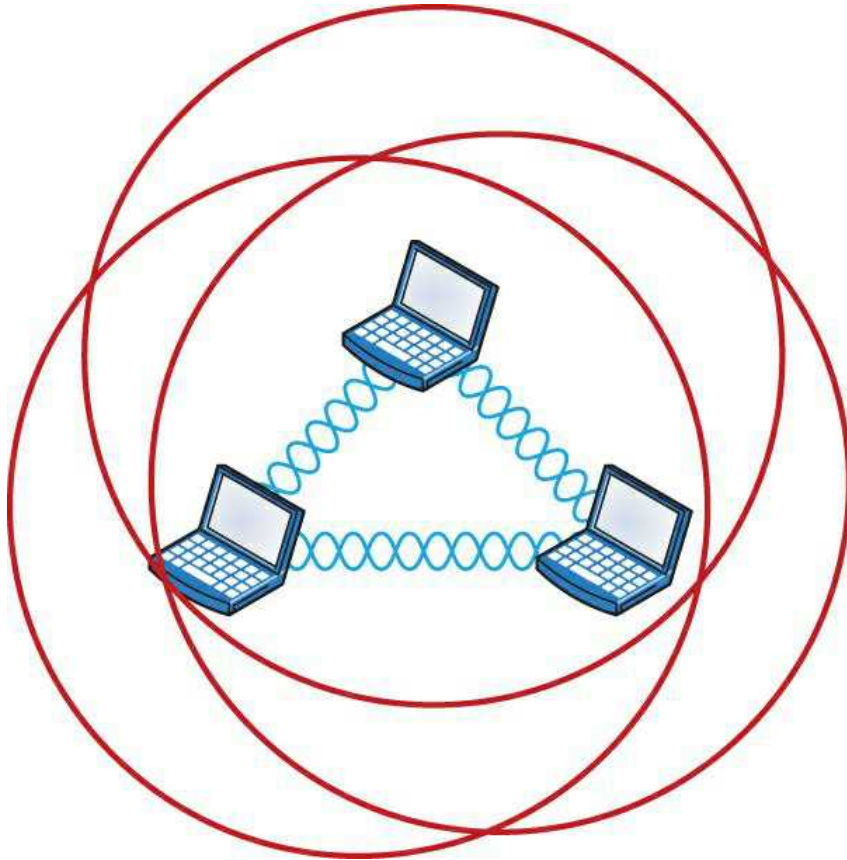


Figure 12.10: A wireless network in ad hoc mode

An ad hoc network would not scale well and really is not recommended due to collision and organization issues. With the low costs of APs, this type of network is just not needed today.

Infrastructure Mode: Basic Service Set

The most common use of wireless networking equipment is to give us the wireless equivalent of a wired network. To do this, all 802.11 wireless equipment has the ability to operate in what's known as infrastructure mode, also referred to as a *basic service set (BSS)*, which is provided by an AP. The term *basic service area (BSA)* is also used at times to define the area managed by the AP, but BSS is the most common term used to define the cell area.

In infrastructure mode, NICs communicate only with an access point instead of directly with each other as they do when they're in ad hoc mode. All communication between hosts, plus with any wired portion of the network, must go through the access point. A really important fact to remember is that in this mode, wireless clients actually appear to the rest of the network as though they were standard, wired hosts.

[Figure 12.11](#) shows a typical infrastructure mode wireless network. Pay special attention to the access point and the fact that it's also connected to the wired network. This connection from the access point to the wired network is called the *distribution system (DS)* and is referred to as wireless bridging.

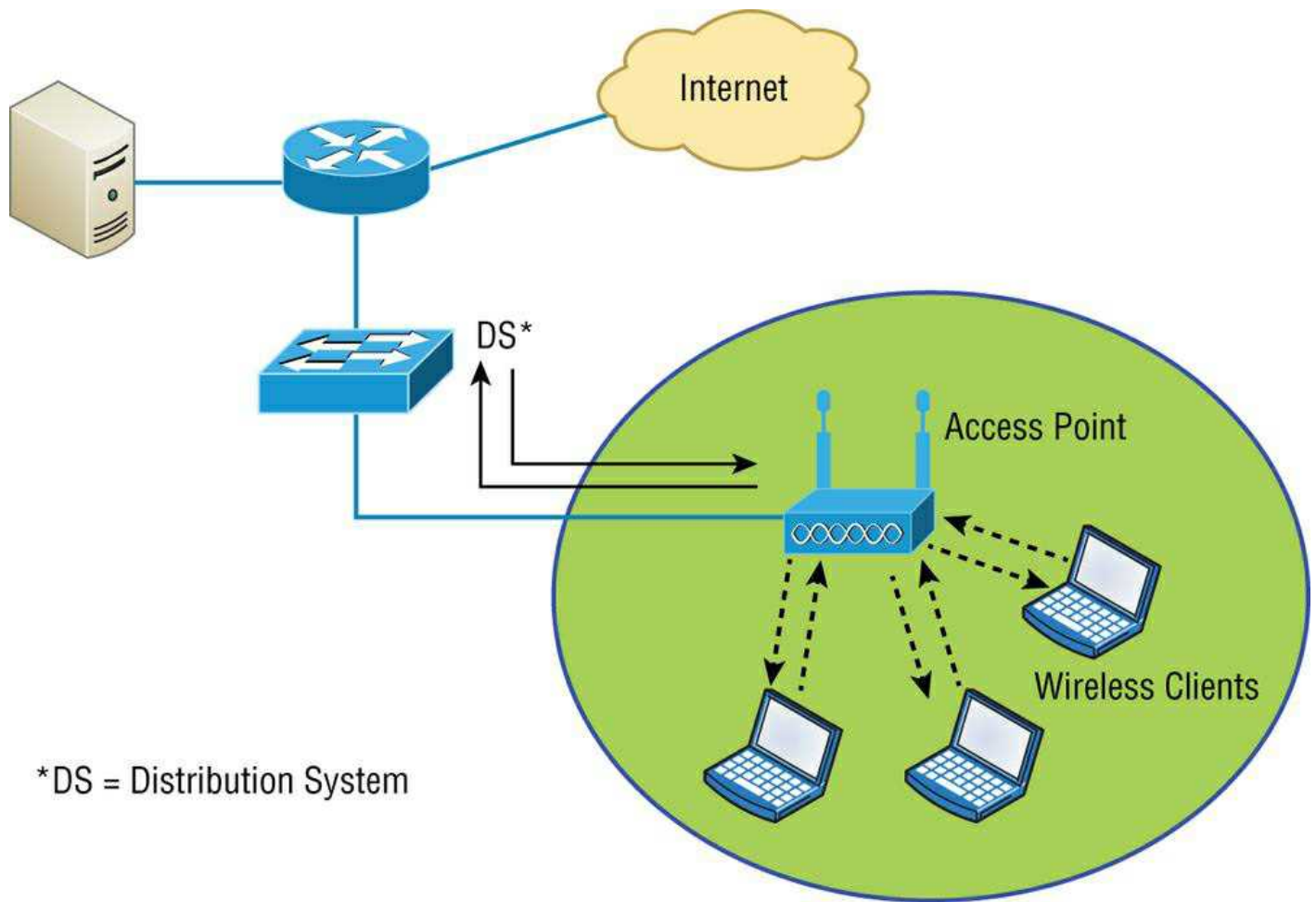


Figure 12.11: A wireless network in infrastructure mode

When you configure a client to operate in wireless infrastructure mode, you need to understand a couple of basic wireless concepts—namely, SSID and security. The *service set identifier (SSID)* refers to the unique 32-character identifier that represents a particular wireless network and defines the basic service set. Oh, and by the way, a lot of people use the terms *SSID* and *BSS* interchangeably, so don't let that confuse you! All devices involved in a particular wireless network must be configured with the same SSID.

It is good to know that if you set all your access points to the same SSID, mobile wireless clients can roam around freely within the same network. Doing this creates an *extended service set (ESS)* and provides more coverage than a single access point. [Figure 12.12](#) shows two APs configured with the same SSID in an office, thereby creating the ESS network.

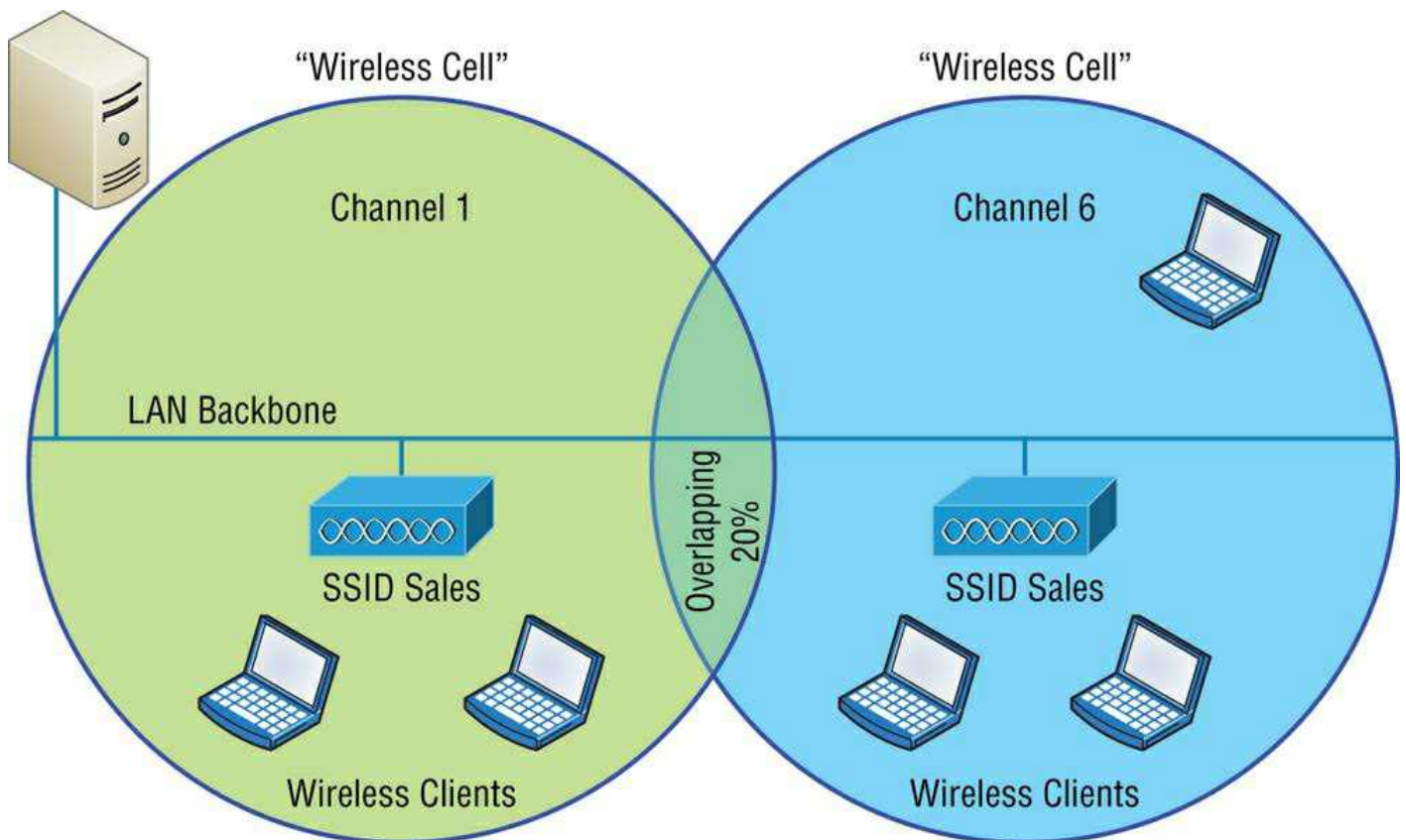


Figure 12.12: Extended service set (ESS)

For users to be able to roam throughout the wireless network—from AP to AP without losing their connection to the network—all AP signal areas must overlap by 10 percent of their signal or more. To make this happen, be sure the channels on each AP are set differently. And remember, in an 802.11b/g network, there are only three non-overlapping channels (1, 6, 11), so careful design is super important here!

Wireless Controllers

You'd be hard pressed to find an enterprise WLAN that doesn't use wireless controllers. In fact, every wireless enterprise manufacturer has a controller to manage the APs in the network.

By looking at [Figure 12.13](#), you can see the difference between what we call stand-alone APs and the controller solution. In a stand-alone solution, all the APs have a full operating system loaded and running, and each must be managed separately.

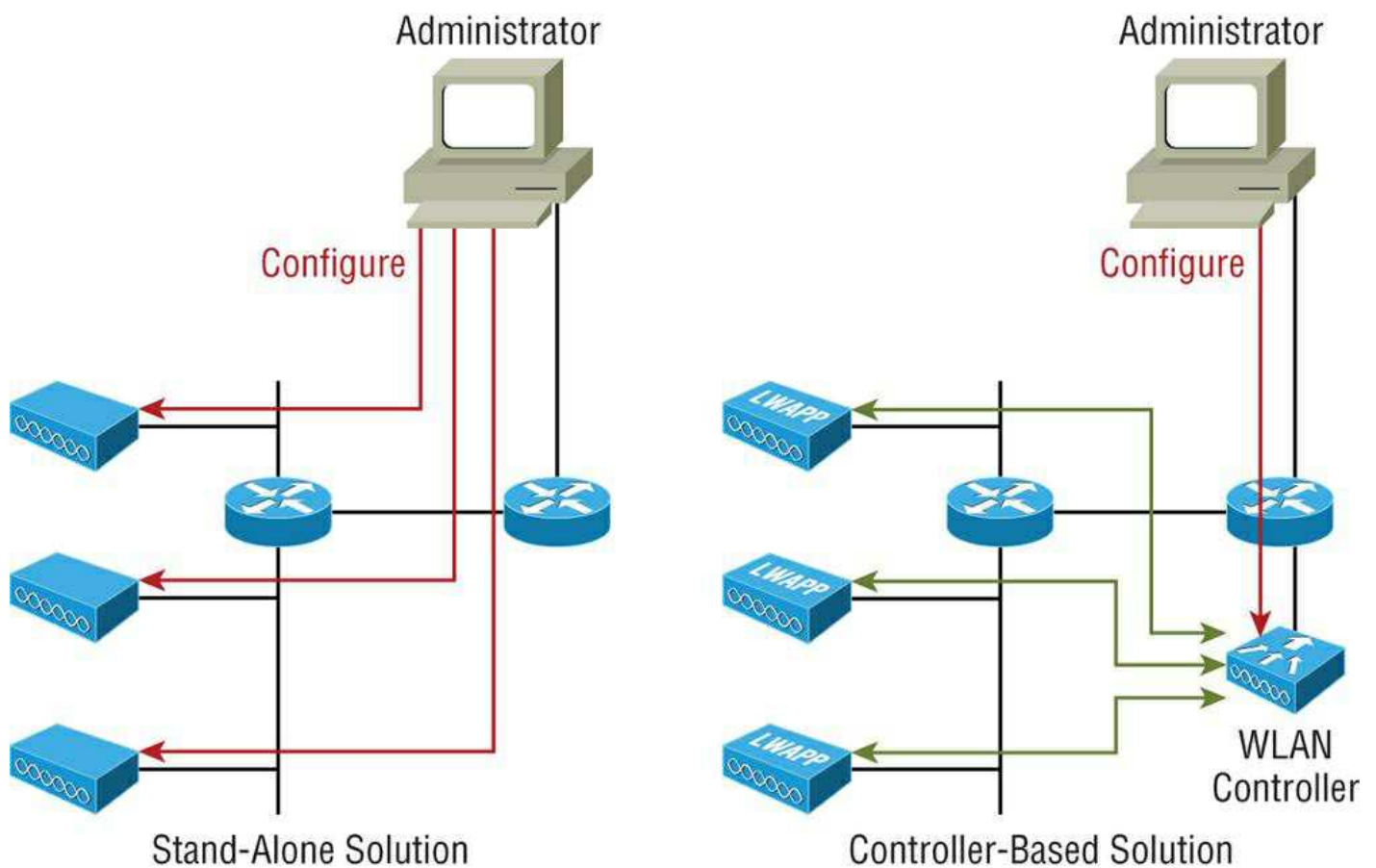


Figure 12.13: Stand-alone and controller-based wireless networks

In the controller-based system, the APs are what we refer to as lightweight, meaning they do not have a full operating system running on them. The controller and AP split duties—a solution known as *split MAC*. APs running with a controller are referred to as lightweight, but you'll also hear the term *thin AP*, whereas you'll hear the term *thick* when referring to APs that run a full OS.

Take another look at [Figure 12.13](#). You can also see that the administrator isn't managing each AP independently when using the WLAN controller solution. Instead, the administrator configures the controller, which in turn pushes out the configuration needed for each AP. Controllers allow us to design and implement larger enterprise wireless networks with less time and tedium, which is very important in today's world!

One feature that also gives controllers the ability to provide a great solution is when you're dealing with a location that's overloaded with clients because it utilizes VLAN pooling, or virtual LAN pooling. This is very cool because it allows you to partition a single large wireless broadcast domain into multiple VLANs and then either statically or randomly assign clients into a pool of VLANs. So, all clients get to keep the same SSID and stay connected to the wireless network, even when they roam. They're just in different broadcast domains.

In order for split MAC to work in a wireless controller network, the APs and controller run a protocol to enable them to communicate. The proprietary protocol that Cisco used was called Lightweight Access Point Protocol (LWAPP), and it's pictured in [Figure 12.14](#).

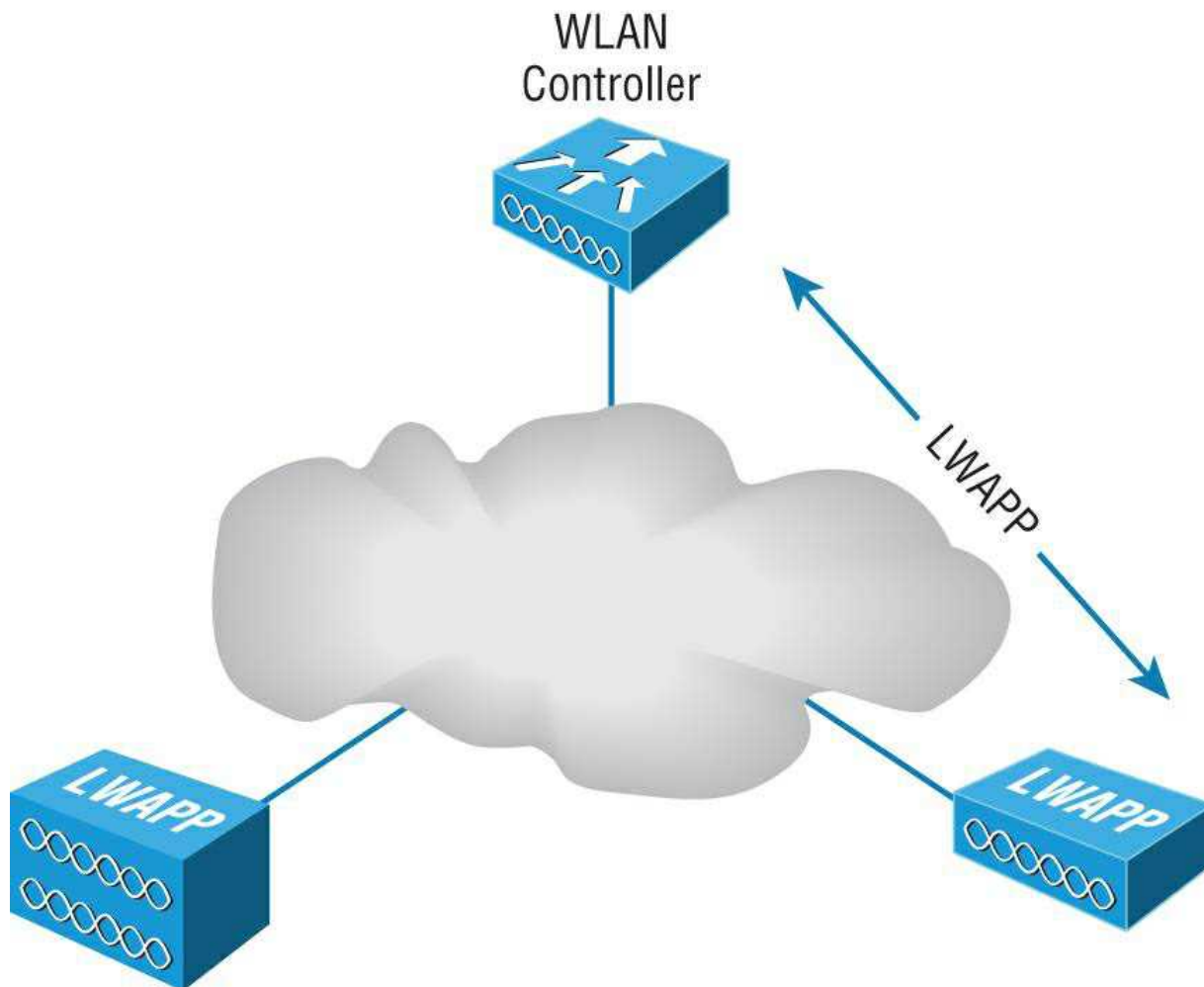


Figure 12.14: LWAPP

Keep in mind that LWAPP isn't used too much these days, but a newer, more secure protocol called Control and Provisioning of Wireless Access Points (CAPWAP), which also happens to be nonproprietary, has replaced it to become the standard that most controller manufacturers use today.

Mobile Hot Spots

Let's say you're in a location that doesn't have an AP installed, or they want to charge you for access, and you want to connect your laptop, tablet, or even play a game. What can you do?

You've got a couple of options, but they all include the cellular network as an infrastructure. Not to be an ad for AT&T, but [Figure 12.15](#) shows a mobile hot spot device that connects your laptop, tablet, media devices, or even a gaming device to the Internet at decent speeds. Pretty much all cellular vendors sell a version of these hot spots now.



Figure 12.15: Mobile hot spot

But let's say you don't want to carry yet another device around with you, and you just want to use your phone instead. [Figure 12.16](#) shows how I turned my iPhone into an AP for my laptop. First, I went to Settings and then chose Personal Hotspot. If that option doesn't show up for you, just give a quick shout to your carrier and have it enabled.

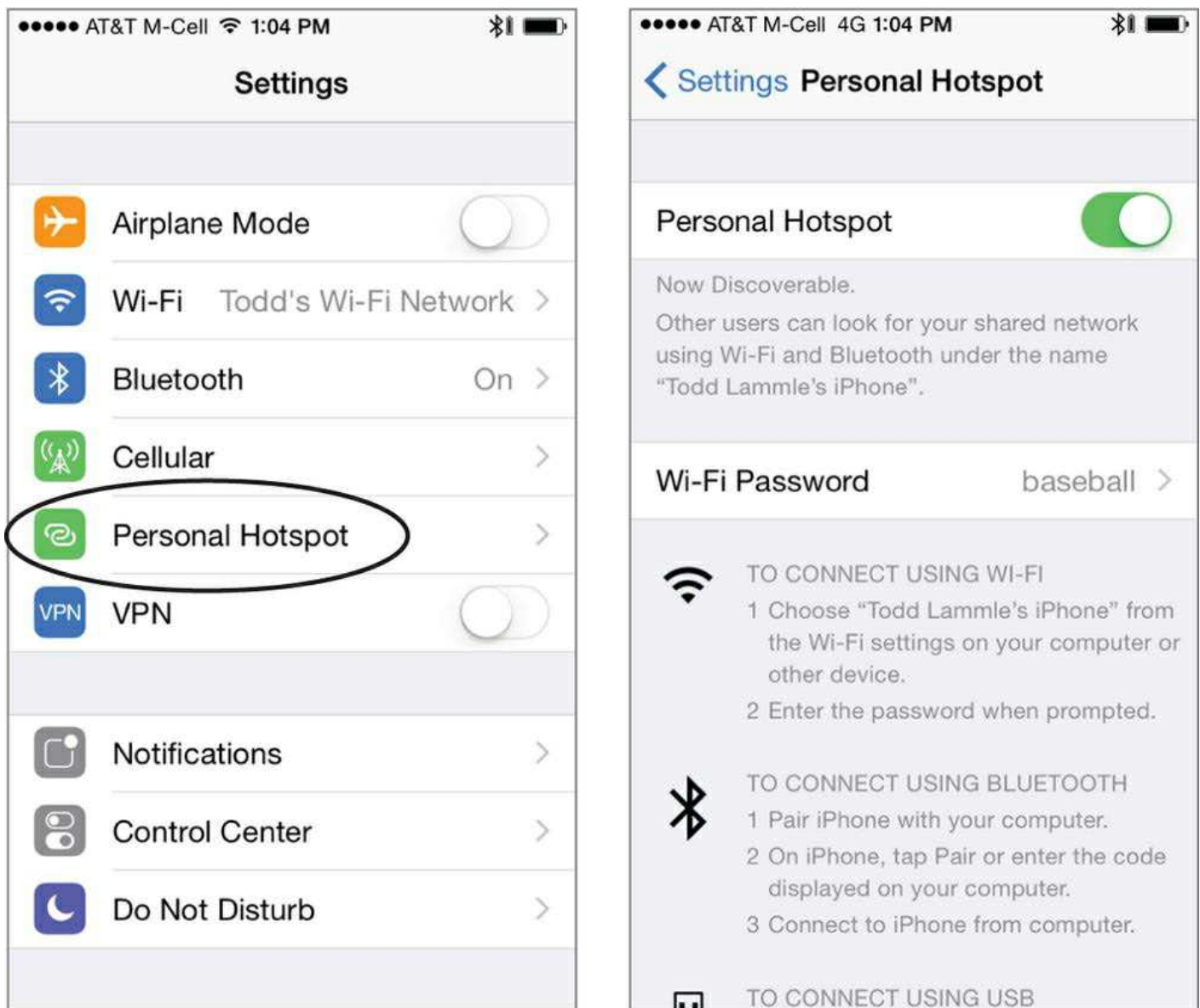


Figure 12.16: iPhone hot spot

I pay very little to AT&T for my AP capability, but I still have to pay for my usage, so I use it only when I'm someplace like an airport and I want security without paying for access to their Internet wireless. Airport wireless hot spots are notoriously slow anyway, and you'd be dead in the water if you intend to use this type of wireless networking for something like gaming, which requires a ton of bandwidth!

Signal Degradation

Something that's really important to consider when installing a wireless network is signal degradation. Because the 802.11 wireless protocols use radio frequencies, the signal strength varies according to many factors. The weaker the signal, the less reliable the network connection will be and so the less usable as well. (Think dropped calls!) There are several key factors that affect signal strength:

- **Distance** This one is definitely on the obvious side—the farther away from the WAP you get, the weaker the signal you get. Most APs have a very limited maximum range that equals less than 100 meters for most systems. You can extend this range to some degree using amplifiers or repeaters, or even by using different antennas.
- **Walls and Other Barriers** Also easy to imagine is the fact that the more walls and other office barriers a wireless signal has to pass through, the more attenuated (reduced) the signal becomes. Also, the thicker the wall, the more it interrupts the signal. So in an indoor office area with lots of walls, the range of your wireless network could be as low as 25 feet! You really have to be careful where you place your APs!
- **Protocols Used** This one isn't so apparent, but it certainly is a factor that affects, and can even determine, the range of a

wireless LAN. The various wireless 802.11 protocols have different maximum ranges. As discussed earlier and illustrated in [Figure 12.7](#), the maximum effective range varies quite a bit depending on the 802.11 protocol used. For example, if you have a client running the 802.11ac protocol but it connects to an AP running only the 802.11n protocol, you'll only get a throughput of 600 Mbps to the client.

- **Interference** The final factor that affects wireless performance is outside interference. Because 802.11 wireless protocols operate in the 900 MHz, 2.4 GHz, and 5 GHz ranges, interference can come from many sources. These include wireless devices like Bluetooth, cordless telephones, cell phones, other wireless LANs, and any other device that transmits a radio frequency (RF) near the frequency bands that 802.11 protocols use.

Other Network Infrastructure Implementations

We've discussed the wireless LANs (WLANs) created by installing APs, but there are other technologies, like personal area networks (PANs), that create wireless infrastructures too. By far, the best known is the ever-popular Bluetooth, but there are other wireless technologies we can use as well, and we'll take some time to explore these soon.

For now, it's back to Bluetooth, which happens to have a fantastic history behind it! The technology was actually named after a fabled 10th century Viking king, Harald I (Harald "Blatand" Gormsson), who was faced with the challenge of dealing with many disparate tribes; he needed to communicate with them all and they needed to get along with each other. Blatand, who it's said got his unique nickname due to sporting an unfortunately prominent blue tooth, was having a really tough time getting this to happen. However, the Viking king was a famously great diplomat possessing a wonderful way with words, and he effectively and nonviolently united ancient Norway and Denmark into a single territory via his powerful communication skills. Incidentally, *Blatand* just happens to translate into *Bluetooth* in English.

Fast-forward to modern times and a Scandinavian company called Ericsson and a highly gifted technological innovator, Jim Kardach. As one of the founders of Bluetooth, Kardach's challenge was a decent, modern-day analogy of the ancient Viking king's—he was faced with making disparate phones, computers, and other devices communicate and cooperate effectively. To answer the challenge, Kardach came up with an elegant, technological wireless solution to make all these disparate devices communicate and play well with each other. To come up with an equally cool name for the brilliant innovation, he did some research, discovered the legend of the ancient Viking king, and codenamed the new technology Bluetooth. It stuck! Now all that was left was to create a super slick logo for it. Today's Bluetooth icon is actually the legendary king's initials in ancient Viking runes merged together—how cool is that?

Bluetooth 1.0 was far slower than what we have now. Data speeds capped off at 1 Mbps and the range only reached as far as 10 meters.

When Bluetooth 2.0 came out, GFSK was taken out in favor of two newer schemes: p/4-DQPSK and 8DPSK, which used changes in the waveforms' phase to carry information, as opposed to frequency modulation. These two schemes resulted in unprecedented data speeds of 2 Mbps and 3 Mbps, respectively. Bluetooth 3.0 further improved data speeds with the addition of 802.11 for up to 24 Mbps of data transfer, although this was not a mandatory part of the 3.0 specification.

Because of the large amount of energy that was required from Bluetooth versions 1.0 to 3.0, also known as Bluetooth Classic, small devices would continue to suffer from short battery life, making early versions of Bluetooth impractical for IoT use.

In order to meet the increasing demand for wireless connectivity between small devices, Bluetooth 4.0 was introduced to the market with a new category of Bluetooth: Bluetooth Low Energy (BLE). Geared toward applications requiring low power consumption, BLE returns to a lower data throughput of 1 Mbps using the GFSK modulation scheme. Although BLE's max data throughput of 1 Mbps may not be suitable for products that require a continuous stream of data like wireless headphones, other IoT applications only need to send small bits of data periodically. An example are fitness wearables that relay small amounts of temperature data to your smartphone only when requested (from a mobile app, perhaps). With the focus on keeping energy demands low, Bluetooth Low Energy makes many coin-cell battery-operated IoT applications (e.g., beacons) feasible. The most recent version of the Bluetooth protocol, Bluetooth 5.0, is an improvement of the previous BLE standards. It is still geared toward low-powered applications but also improves upon BLE's data rate and range. Unlike version 4.0, Bluetooth 5.0 offers four different data rates to accommodate a variety of transmission ranges: 2 Mbps, 1 Mbps, 500 kbps, and 125 kbps. Because an increase in transmission range requires a reduction in data rate, the lower data rate of 125 kbps was added to support applications that benefit more from improved range.

To delve a little deeper into wireless technologies, the idea of PANs is to allow personal items such as keyboards, mice, and phones to communicate to our PC/laptop/display/TV wirelessly instead of having to use any wires at all—over short distances of up to 30 feet, of course. This idea of the wireless office hasn't quite come to fruition completely yet, but you have to admit that Bluetooth really has helped us out tremendously in our offices and especially in our cars!

There are two other network infrastructure implementations in the PAN area: infrared (IR) and near-field communication (NFC).

Like Bluetooth, IR has some history behind it, but the technology's idea only goes back to about 1800 because that's when it was first said that the energy from the sun radiates to Earth in infrared. We can use IR to communicate short range with our devices, like Bluetooth-enabled ones, but it isn't really as popular as Bluetooth to use within network infrastructures. Unlike Wi-Fi and Bluetooth, the infrared wireless signals cannot penetrate walls and only work line-of-sight. The rates are super slow and most transfers are only 115 Kbps—up to 4 Mbps on a really good day!

The other implementation I want to cover is called near-field communication (NFC). For NFC to work, the actual antenna must be smaller than the wavelength on both the transmitter and receiver. For instance, if you look at a 2.4 GHz or 5 GHz antenna, they are the exact length of one wavelength for that specific frequency. With NFC, the antenna is about one-quarter the size of the wavelength, which means that the antenna can create either an electric field or a magnetic field but not an electromagnetic field.

NFC can be used for wireless communication between devices like smartphones and/or tablets, but you need to be near the device transmitting the RF to pick up the signal—really close. A solid example would be when you're swiping your phone over a QR code or contactless payment terminal.

Technologies That Facilitate the Internet of Things (IoT)

Internet of Things (IoT) is the newest buzzword in IT and it means the introduction of all sorts of devices to the network (and Internet) that were not formerly there. Refrigerators, alarm systems, building service systems, elevators, and power systems are now equipped with networked sensors allowing us to monitor and control these systems from the Internet.

These systems depend on several technologies to facilitate their operations:

- **Z-Wave** Z-Wave is a wireless protocol used for home automation. It uses a mesh network using low-energy radio waves to communicate from appliance to appliance. Residential appliances and other devices, such as lighting control, security systems, thermostats, windows, locks, swimming pools, and garage door openers can use this system.
- **ANT+** ANT+ is another wireless protocol for monitoring sensor data such as a person's heart rate or a bicycle's tire pressure as well as for controlling systems like indoor lighting and television sets. ANT+ is designed and maintained by the ANT+ Alliance, which is owned by Garmin.
- **Bluetooth** Some systems use Bluetooth. Bluetooth was discussed earlier in this chapter.
- **NFC** Some systems use near-field communication. NFC was discussed earlier in this chapter.
- **IR** Some systems use infrared. Infrared was discussed earlier in this chapter.
- **RFID** While RFID is mostly known for asset tracking, it can also be used in the IoT. Objects are given an RFID tag so they are uniquely identifiable. Also, an RFID tag allows the object to wirelessly communicate certain types of information.

Truly smart objects will be embedded with both an RFID tag and a sensor to measure data. The sensor may capture fluctuations in the surrounding temperature, changes in quantity, or other types of information.

- **802.11** Finally, 802.11 can also be used for IoT communication. 802.11 was discussed earlier in this chapter.

Installing and Configuring WLAN Hardware

As I said earlier, installing 802.11 equipment is actually fairly simple—remember that there are really only two main types of components in 802.11 networks: APs and NICs. Wireless NIC installation is just like installing any other network card, but nowadays most, if not all, laptops have wireless cards preinstalled, and that's as easy as it gets! And just as with connecting an Ethernet card to a LAN switch, you need the wireless network card to connect to an access point.

The AP installation can be fairly simple as well. Take it out of the box, connect the antenna(s) if necessary, connect the power, and then place the AP where it can reach the highest number of clients. This last part is probably the trickiest, but it really just involves a little common sense and maybe a bit of trial and error. Knowing that walls obstruct the signal means that putting the AP out in the open—even indoors—works better. And you also know it should be placed away from sources of RF interference, so putting it next to the microwave or phone system is probably a really bad idea too. Near a metal filing cabinet is also not so good. So just experiment and move your AP around to find the spot that gives you the best signal strength for all the clients that need to use it.

Now that you have the hardware installed, it's time to configure it, right? Let's get started.

No worries—configuring your AP and NIC to work together isn't as tricky as it sounds. Most wireless equipment is designed to work almost without configuration, so by default, you can pretty much turn things on and start working. The only things you need

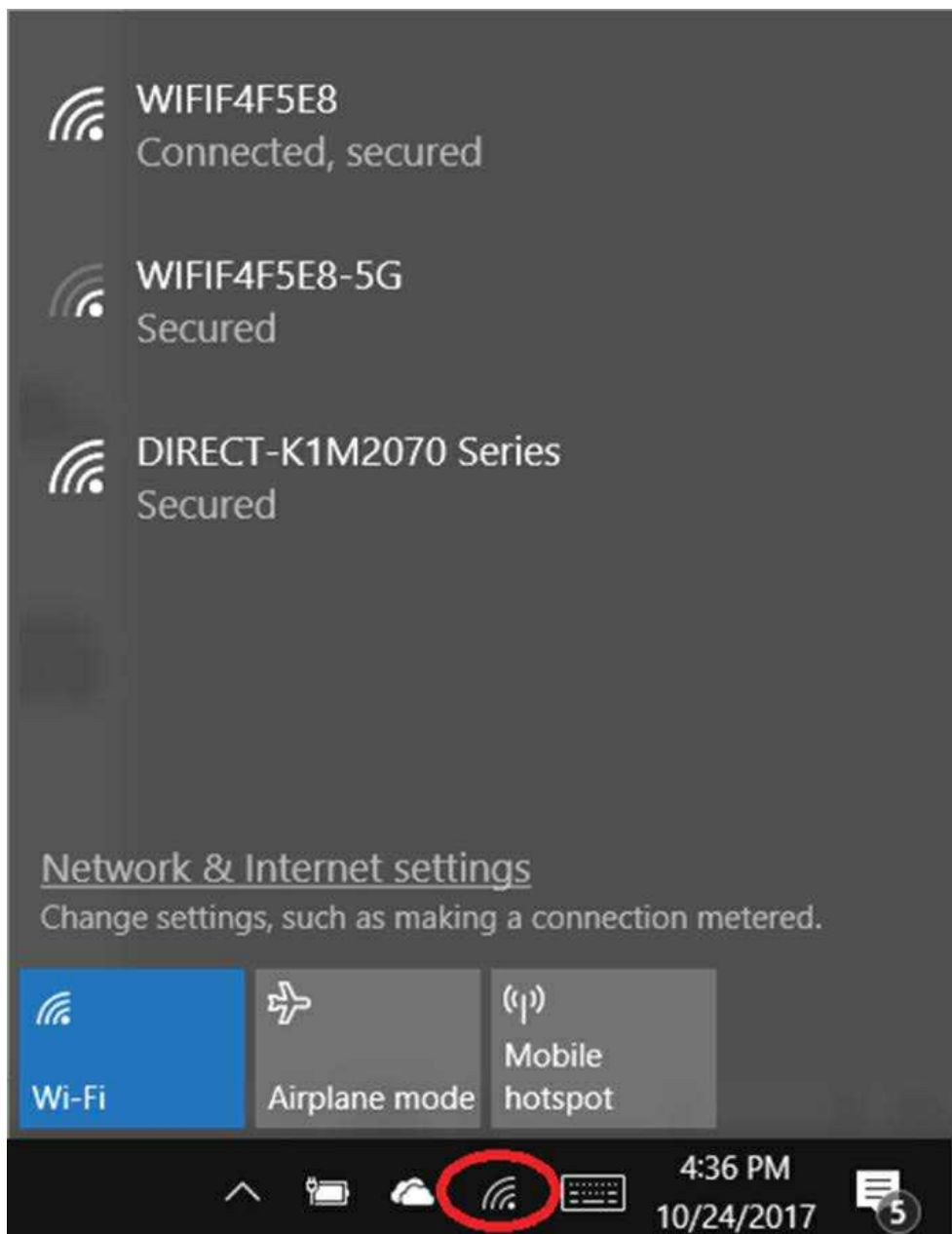
to configure are customization settings (name, network address, and so on) and security settings, and even these aren't required. But because I do highly recommend configuring them, I'll take you through that now.

NIC Configuration

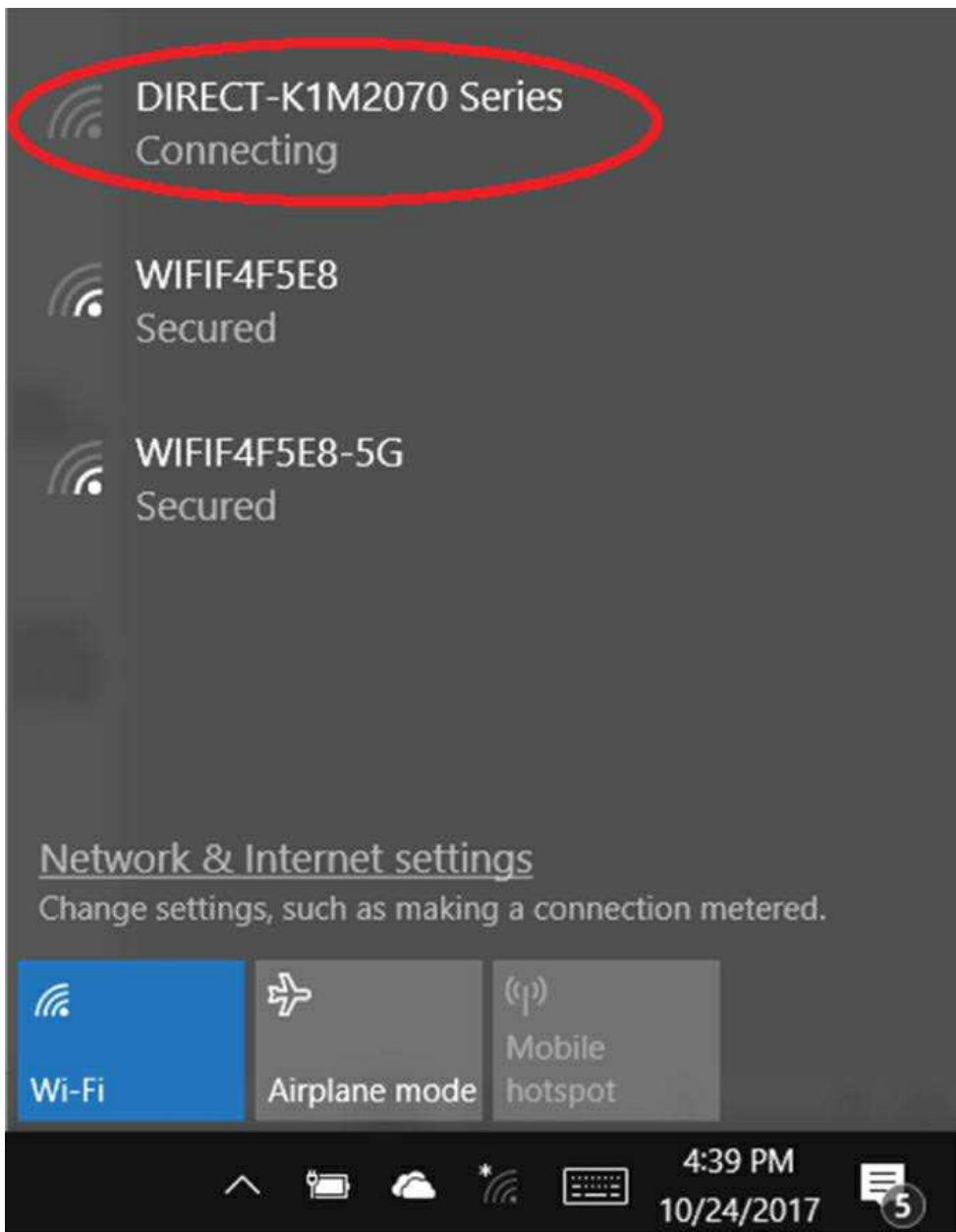
Windows hosts and servers include software to automatically configure a wireless connection, and they do so automatically if you install a wireless NIC—assuming that somehow you have a Windows machine without a wireless NIC installed on the motherboard. And if you have one without a NIC installed, your Windows machine is really old!

Configuring a Windows client is pretty simple, but what do you do if you can't get it to actually work afterward? If this happens to you, searching for the solution could eat up a serious amount of your time! Following these steps could save you from that frustrating quest:

1. To find a wireless network, just go to the lower-right corner of your screen and click the icon that looks like a wireless wave. You will see the box below.



2. Double-click the network you want to join, and click Connect Anyway, even if it's an unsecured network. You'll then see a screen showing that it's trying to connect.



3. If you're using security, the AP will ask you for your credentials.
4. Check your TCP/IP settings to find out if you're not really connected to the Internet and troubleshoot from there.

AP Configuration

Once you've successfully configured your workstation(s), it's time to move on and configure the AP. There are literally hundreds of different APs out there, and of course, each uses a different method to configure its internal software. The good news is that for the most part, they all follow the same general patterns:

1. First of all, out of the box, the AP should come configured with an IP address that's usually something similar to 192.168.1.1. But check the documentation that comes with the AP to be sure. You can just take the AP out of its box, plug it into a power outlet, and connect it to your network, but in order to manage the AP, you've got to configure its IP address scheme to match your network's.
2. You should receive a DHCP address from the AP when you connect, but if you don't get one, start by configuring a workstation on the wired network with an IP address (192.168.1.2 or similar) and subnet mask on the same subnet as the AP's. You should then be able to connect to the AP to begin the configuration process. Usually, you do this via a web browser or with a manufacturer-supplied configuration program.
3. Once you have successfully connected to the AP, you then get to configure its parameters.

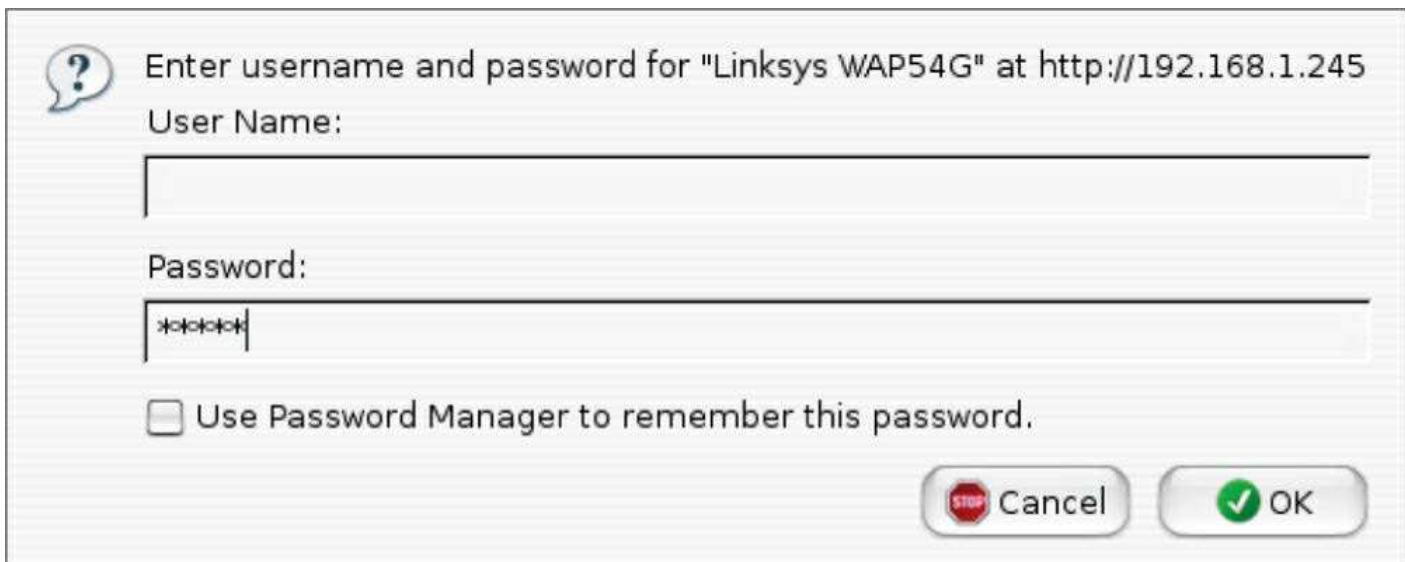
Following are the minimum parameters common to APs that you should configure for your AP to work properly. (Remember, typically an AP works right out of the box, but it is unsecure too!)

- **SSID** As I mentioned earlier, this is the name of the wireless network that your AP will advertise. If this new AP is to be part of an existing wireless network, it needs to be configured with the same SSID as the existing network. In a network with only one AP, you can think of the SSID as the "name" of the AP.
- **AP IP Addresses** Remember, even though most APs come preconfigured with an IP address, it may not be one that matches the wired network's IP addressing scheme. So it follows that you should configure the AP's IP addresses (including the address, subnet mask, and default gateway addresses) to match the wired network you want it connected to. An AP does not need an IP address to work in your network. The IP address of the AP is used only to manage the AP.
- **Operating Mode (Access Point or Bridging)** Access points can operate in one of two main modes: *Access Point mode* or *Bridging mode*. Access Point mode allows the AP to operate as a traditional access point to allow a wireless client transparent access to a wired network. Alternatively, two APs set to Bridging mode provide a wireless bridge between two wired network segments.
- **Password** Every access point has some kind of default password that's used to access the AP's configuration. For security reasons, it's a good idea to change this as soon as you can to connect to and configure the AP.
- **Wireless Channel** 802.11 wireless networks can operate on different channels to avoid interference. Most wireless APs come set to work on a particular channel from the factory, and you can change it if other networks in the area are using that channel, but be aware that no particular channel is any more secure than another. Wireless stations do *not* use channel numbers as the criteria when seeking a connection. They only pay attention to SSIDs!
- **WEP/WPA** Although it isn't a requirement per se, I definitely recommend enabling security right from the start as soon as you turn on the AP. Commercial APs typically come configured as an open network so that it's easy to log in, whereas enterprise APs come unconfigured and don't work until they are configured. WEP and Wi-Fi Protected Access (WPA) allow data to be encrypted before it's sent over the wireless connection, and all configuring entails is to enable it and pick a key to be used for the connections. Simple, easy-to-configure security is certainly worth your time!

So here's what you do: First, you'll be asked to enter one or more human-readable passphrases called *shared keys*—secret passwords that won't ever be sent over the wire. After entering each one, you'll generally click a button to initiate a one-way hash to produce a WEP key of a size related to the number of bits of WEP encryption you want. Entering the same passphrase on a wireless client causes the hash (not the passphrase) to be sent from the wireless client to the AP during a connection attempt. Most configuration utilities allow you to create multiple keys in case you want to grant someone temporary access to the network, but you still want to keep the primary passphrase a secret. You can just delete the key you enabled to permit temporary access after you don't need it anymore without affecting access by any primary LAN participants.

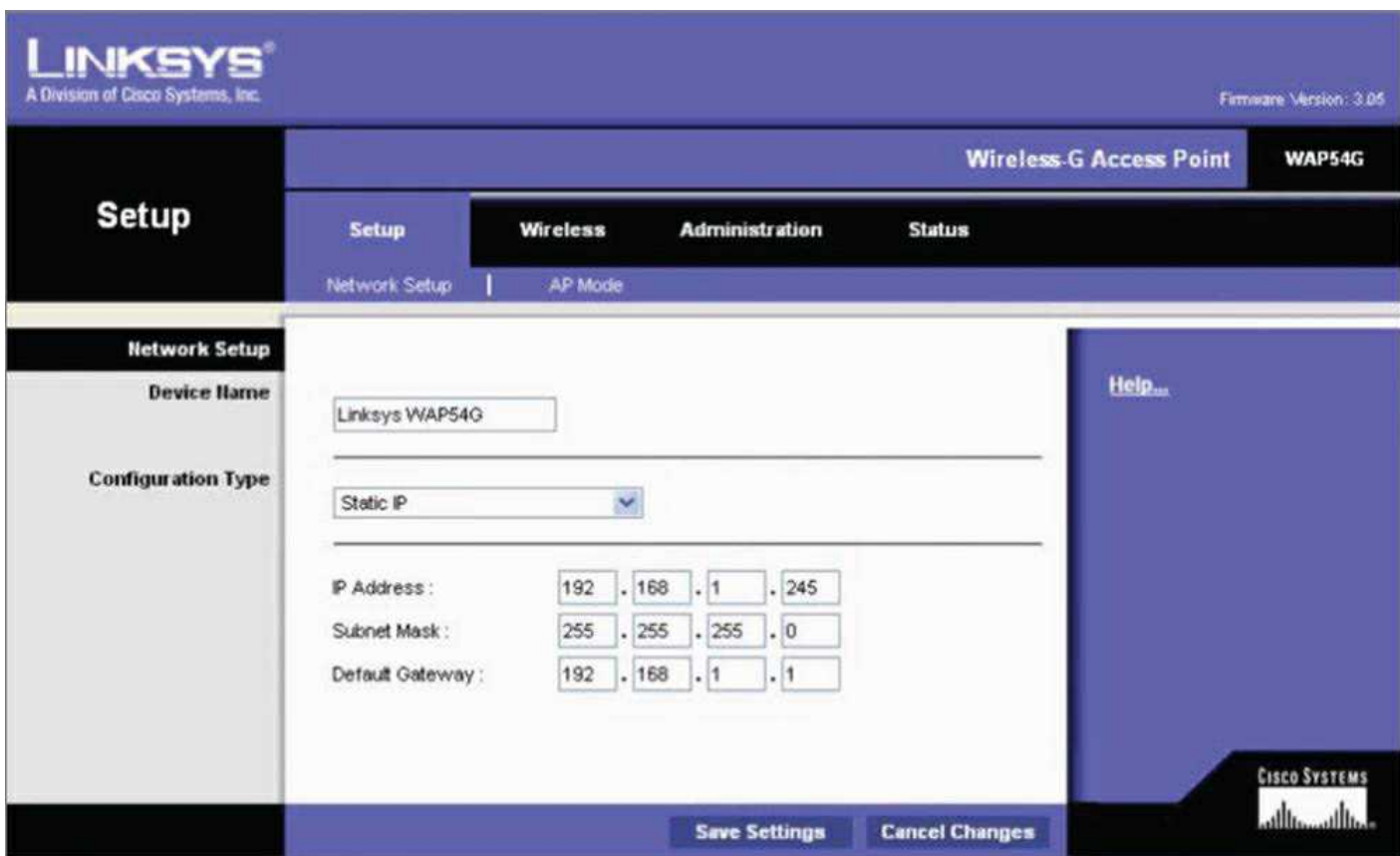
Here's an example of connecting to a Linksys access point (not a Linksys wireless router, which is a different device):

1. The first screen shows that I've connected using HTTP to configure the device. The IP address of the Linksys AP is 192.168.1.245. If it was a Linksys wireless router instead—the typical home DSL/cable modem wireless connection device around today—then the address would be 192.168.1.1.



A login dialog box with a question mark icon. The text reads: "Enter username and password for 'Linksys WAP54G' at http://192.168.1.245". Below this, there are two input fields: "User Name:" and "Password:". The password field contains six asterisks. Below the password field is a checkbox labeled "Use Password Manager to remember this password.". At the bottom right are two buttons: "Cancel" (with a red stop icon) and "OK" (with a green checkmark icon).

2. As you can see, there's no username required, and the password is just *admin*. Again, be sure not to leave this login configuration as the default! Once I click OK, I get taken to a screen where I can change my IP address.



The Linksys Setup page for a Wireless-G Access Point WAP54G. The top header shows the Linksys logo and "A Division of Cisco Systems, Inc." with the firmware version "3.05". The main navigation bar includes "Setup", "Wireless", "Administration", and "Status". The "Setup" tab is active, showing "Network Setup" and "AP Mode". The "Network Setup" section has a "Device Name" field set to "Linksys WAP54G" and a "Configuration Type" dropdown set to "Static IP". Below these are three rows of IP configuration fields: "IP Address" (192, 168, 1, 245), "Subnet Mask" (255, 255, 255, 0), and "Default Gateway" (192, 168, 1, 1). At the bottom are "Save Settings" and "Cancel Changes" buttons. A "Help" link is on the right, and the Cisco Systems logo is at the bottom right.

3. It isn't vital for an AP to have an IP address, but it comes in handy for management purposes. You can change the IP address as well as the device name from this screen if you want to. I clicked the Wireless tab on top and this screen appeared.

Wireless

Wireless.G Broadband Router

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Network

Wireless Network Mode: Mixed

Wireless Network Name (SSID): linksys

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ☒ Enable ☐ Disable



Status : SES Security Parameters Configured

Reset Security

Save Settings Cancel Changes

4. From here, you can set the device to run b/g, only g, or hopefully the newer technologies, but if all you have is g, that will work too. You can also change the SSID from Linksys to another name, and I *highly* recommend doing this. The AP channel can also be changed, and you can turn off the AP beacons as well, which is also recommended, but understand that if you do this, you'll have to set the new SSID name in each of your clients! Last thing—you can see that by default, there's no encryption. Click the Wireless Security tab, and you'll get this screen.



5. From the pull-down menu, you get to choose from various wireless security options if you want to.

I'll talk more about security after I hammer on about site surveys for a bit—they really are that important!

Site Survey

I want to be sure you're completely clear about where I stand regarding site surveys. They are absolutely and vitally imperative to bringing a premium-quality—even just a reasonably viable—WLAN into this world! You should carry out a predeployment survey and a postdeployment survey, but keep in mind that your predeployment survey isn't actually your first step to begin this key process.

So, because you positively must know how to formulate and implement a solid site survey, I'm going to walk you through executing the three major steps to doing that effectively. And just to be really thorough, I'm also going to cover some issues commonly encountered as we progress through these steps.

- **Information Gathering** This is actually your first step, and during this stage, you must determine three key factors:
 - The scope of the network, including all applications that will be used, data types that will be present, and how sensitive these data types are to delay
 - The areas that must be covered and the expected capacity at each location
 - The types of wireless devices that will need to be supported, such as, for example, laptops, tablets, smartphones, IP phones, and barcode readers

During this phase, a key goal of mine would be to create a coverage model that maps to all areas that need coverage, along with those that don't, and have my client sign off in agreement to this document before I do anything else. You definitely want to do this too—just trust me!

- **Predeployment Site Survey** In this phase, I use live APs to verify the optimal distances between their prospective locations. I base this placement on the expected speed at the edge of the cell, the anticipated number of devices, and other information gathered in step 1. Usually, after I get one AP positioned, I'll place the next one based on the distance from the first, with special consideration given to any sources of interference I've found.
- **Postdeployment Site Survey** I utilize the postdeployment survey phase to confirm and verify that the original design and placements are happily humming along and problem free, when all stations are using the network. This pretty much never happens, so at this point, it's likely changes will need to be made—sometimes, significant ones—in order to optimize the performance of a WLAN operating under full capacity.

Providing Capacity

Now here's a big issue that frequently rears its ugly head: providing enough capacity in areas where many wireless stations will be competing for the airwaves. Remember that stations share access to the RF environment with all other stations in the BSS, as well as with the AP, so really, the only way to increase capacity is by increasing the number of APs in an area requiring serious density.

This can get complicated, but basically it comes down to placing APs on non-overlapping channels while still sharing the same SSID. Take a look at [Figure 12.17](#) for an example of this scenario.

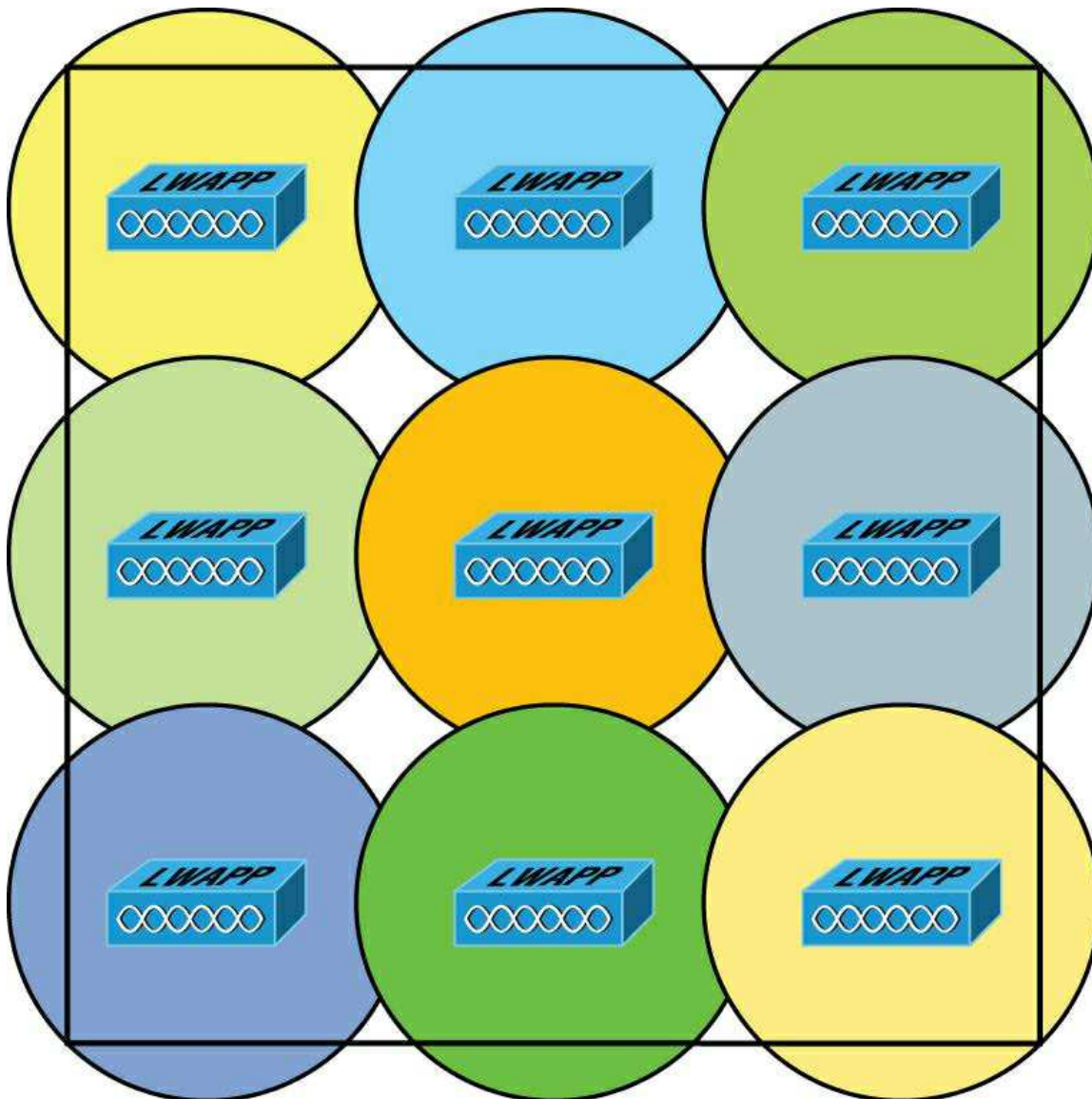


Figure 12.17: Basic coverage

In [Figure 12.17](#), nine APs have been configured in the same area using the three non-overlapping channels in the 2.4 GHz frequency (1, 6, and 11). Each shade represents a different channel. Even though the APs on the same channel have been positioned far enough away from one another so that they don't overlap much and/or cause interference, surprisingly, it's actually

better if there is some overlap. But bear in mind that the channels should be used in a way that no APs on the same channel overlap in a detrimental way. Another thing I want to point out that's not so ideal about this arrangement is that all the APs would have to run at full power. This isn't a good way to go because it doesn't give you much fault tolerance at all!

So, we've got two problems with our design: lack of overlap and lack of fault tolerance. To address both issues, you need more APs using 802.11ac or later, which would get you more channels and provide better throughput, as shown in [Figure 12.18](#).

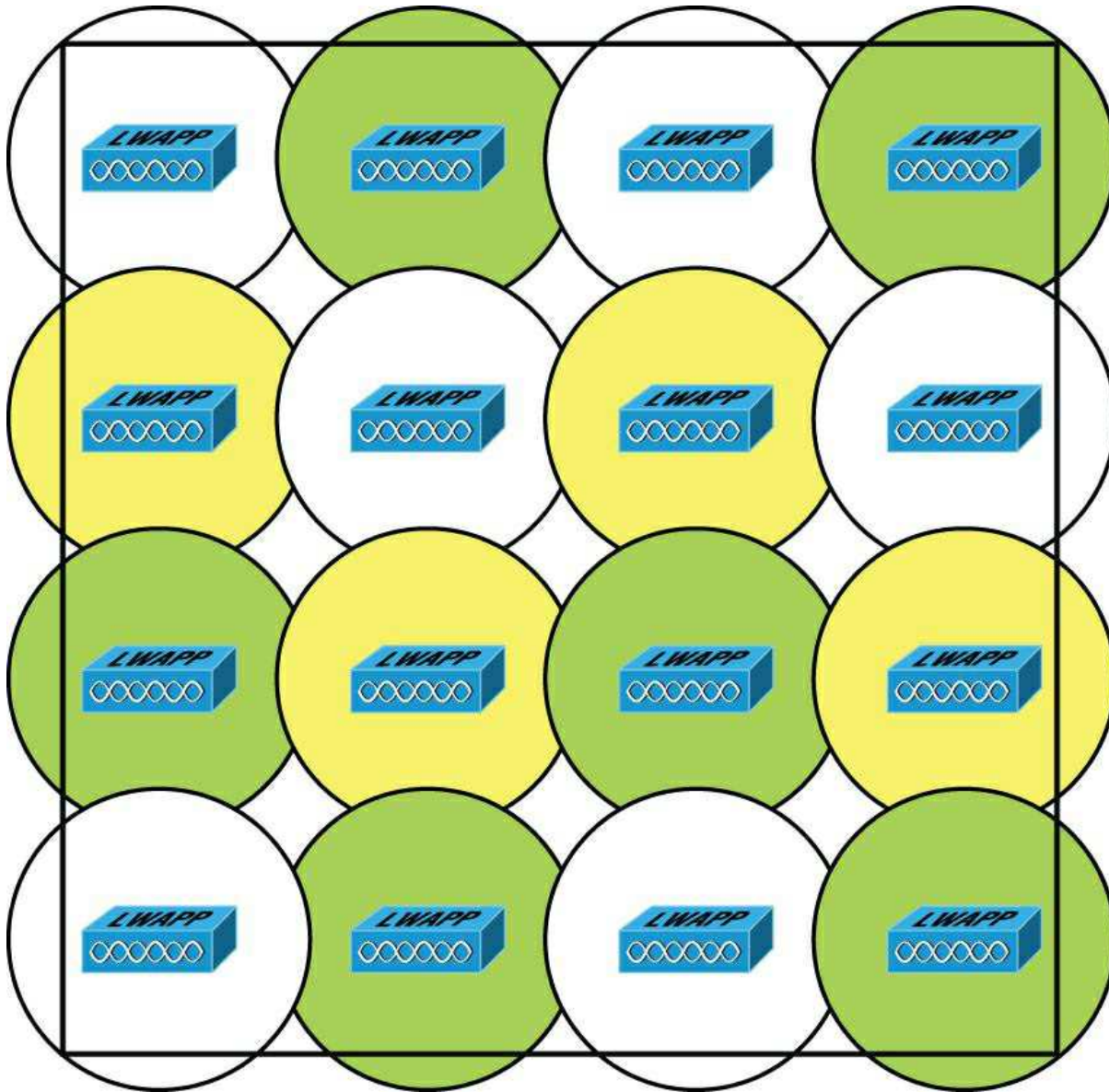


Figure 12.18: Enterprise design

A key benefit to this design is it would also gain the critical ability to run the APs at less than full power. This allows the controller to strategically boost the power of specific APs in the event of an AP outage in a given area.

When you know exactly the type of applications and activity a WLAN will need to support, you can then determine the data rate that must be attained in a particular area. Since received signal strength indicator (RSSI), signal-to-noise ratio (SNR), and data rate are correlated, the required data rate will tell you what the required RSSI or SNR should be as seen at the AP from the stations. Keep in mind that stations located at the edge of the cell will automatically drop the data rate and that the data rate will increase as a station moves toward the AP.

Multiple Floors

Another special challenge is a multistory building where WLANs are located on all floors. In these conditions, you've got to think about channel usage in a three-dimensional way, and you'll have to play nicely with the other WLANs' administrators to make this work! Facing this scenario, your channel spacing should be deployed as shown in [Figure 12.19](#).

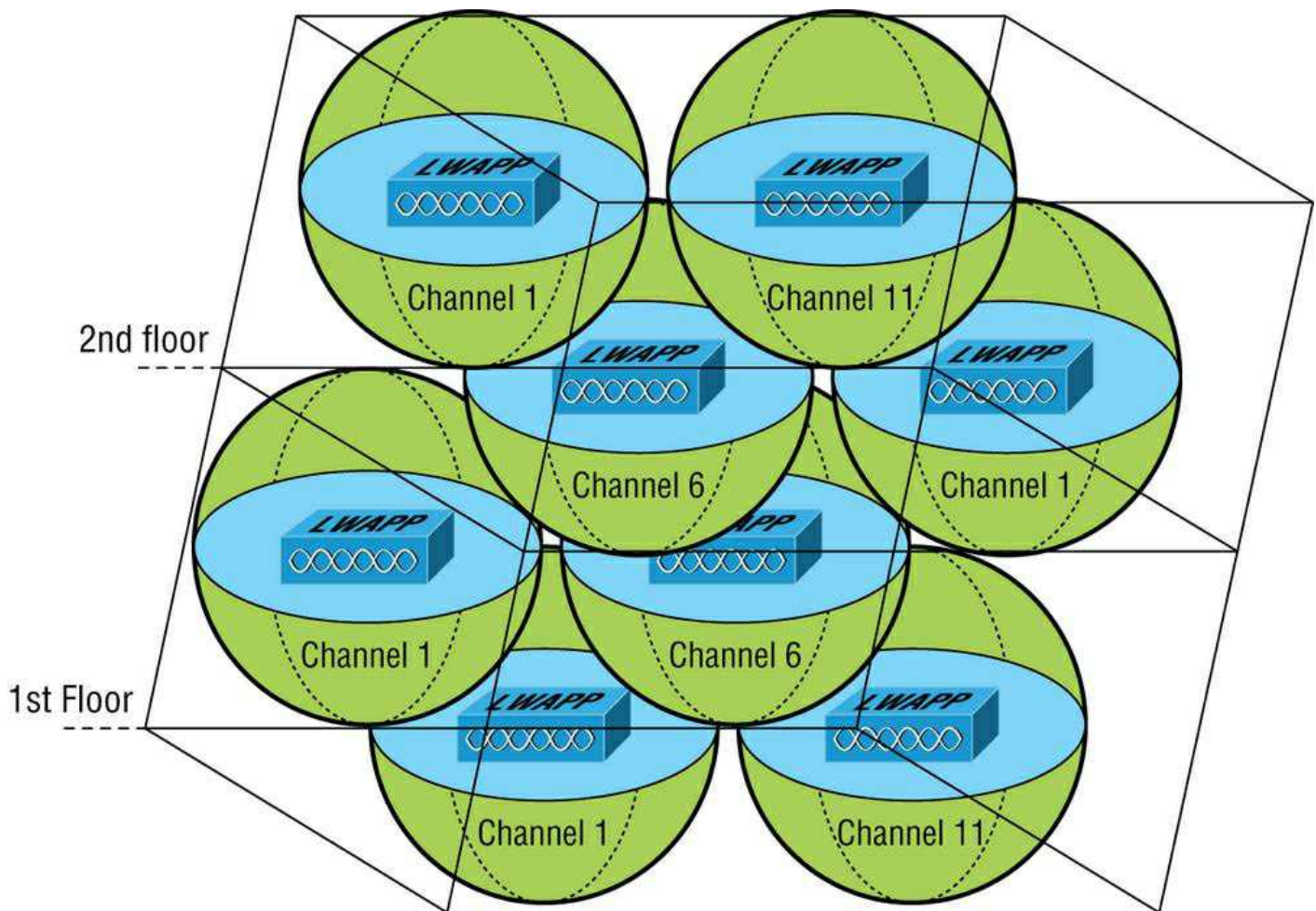


Figure 12.19: A multifloor installation

To prevent bleed from one floor to another, use semi-directional or patch antennas to control radiation patterns.

Location-Based WLAN

When using a location device such as the Cisco 2710, your restrictions get even tighter. The additional requirements for the location device to operate properly are as follows:

- APs should be placed at the edge even when they're not needed there for normal coverage purposes so that devices at the edge can be located.
- The density of APs must be higher. Each AP should be 50 to 70 feet apart—much closer than is normally required.
- Some APs will need to be set in monitor or scanner mode so that they won't transmit and interfere with other APs.

All of this means that the final placement will be denser and a bit more symmetrical than usual.

Site Survey Tools

There are some highly specialized, very cool site survey tools that can majorly help you achieve your goals. The AirMagnet Survey and Ekahau Site Survey tools make it possible to do a client walk-through with the unit running and you can click each location on the map.

These tools will gather RSSI and SNR from each AP in the range, and at the end of your tour, global heat map coverage will be magically displayed, as shown in [Figure 12.20](#).

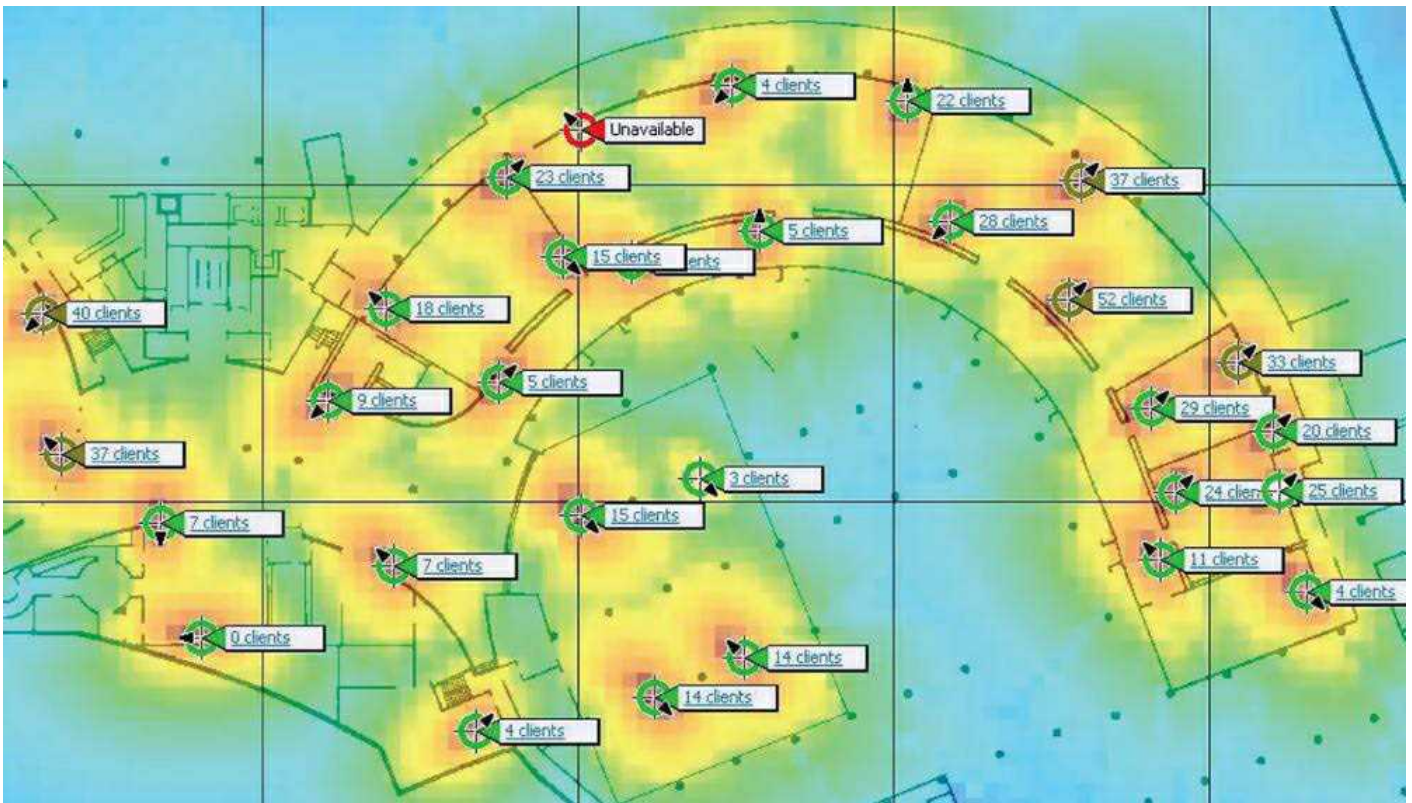


Figure 12.20: A heat map of a building

Wireless Security

So, wireless security is basically nonexistent on access points and clients. The original 802.11 committee just didn't imagine that wireless hosts would one day outnumber bounded media hosts, but that's actually where we're headed now. Also, unfortunately, just as with the IPv4 routed protocol, engineers and scientists didn't include security standards that are robust enough to work in a corporate environment. So we're left with proprietary solution add-ons to aid us in our quest to create a secure wireless network. And no—I'm not sitting here bashing the standards committees, because the security problems we're experiencing were also created by the US government because of export issues with its own security standards. Our world is a complicated place, so it follows that our security solutions would have to be as well.

Wireless Threats

Protection of data and the authentication processes are certainly key threats, but there are other wireless security perils lurking out there as well. We'll dive deeper into the processes and procedures designed to mitigate these dangers in Chapter 14, "Organizational Documents and Policies," but I want to briefly discuss them here.

Rogue APs

First, there's the evil we call rogue APs. These are APs that have been connected to your wired infrastructure without your knowledge. The rogue may have been placed there by a determined hacker who snuck into your facility and put it in an out-of-the-way location or, more innocently, by an employee who just wants wireless access and doesn't get just how dangerous doing this is. Either way, it's just like placing an open Ethernet port out in the parking lot with a sign that says "Corporate LAN access here—no password required!"

Clearly, the worst type of rogue AP is the one some hacker has cleverly slipped into your network. It's particularly nasty because the bad guy probably didn't do it to simply gain access to your network. Nope—the hacker likely did it to entice your wireless clients to disastrously associate with their rogue AP instead! This ugly trick is achieved by placing their AP on a different channel from your legitimate APs and then setting its SSID in accordance with your SSID. Wireless clients identify the network by the SSID, not the MAC address of the AP or the IP address of the AP, so jamming the channel that your AP is on will cause your stations to roam to the bad guy's AP instead. With the proper DHCP software installed on the AP, the hacker can issue the client an address, and once that's been done, the bad guy has basically "kidnapped" your client over to their network and can freely perform a peer-to-peer attack. Believe it or not, this can all be achieved from a laptop while Mr. Hacker simply sits in your parking lot, because there are many types of AP software that will run on a laptop—yikes!

Mitigation

But you're not helpless—one way to keep rogue APs out of the wireless network is to employ a wireless LAN controller (WLC) to manage your APs. This is a nice mitigation technique because APs and controllers communicate using Lightweight Access Point Protocol (LWAPP) or the newer CAPWAP, and it just so happens that one of the message types they share is called Radio Resource Management (RRM). Basically, your APs monitor all channels by momentarily switching from their configured channel and by collecting packets to check for rogue activity. If an AP is detected that isn't usually managed by the controller, it's classified as a rogue, and if a wireless control system is in use, that rogue can be plotted on a floor plan and located. Another great benefit to this mitigation approach is that it enables your APs to also prevent workstations from associating with the newly exposed rogue.

Ad Hoc Networks

As you already know, ad hoc networks are created peer to peer or directly between stations and not through an AP. This can be a dangerous configuration because there's no corporate security in place, and since these networks are often created by unsophisticated users, you end up with the scenario I just described that's primed for, and wide open to, a peer-to-peer attack. It's even uglier if the laptop happens to connect to the corporate LAN through an Ethernet connection at the same time the ad hoc network is created, because the two connections could be bridged by a hacker to gain access straight up into the wired LAN itself!

Mitigation

When you've got a Cisco Unified Wireless Network (CUWN) in operation, ad hoc networks can be identified over the air by the kind of frames they send, which are different from those belonging to an infrastructure network. When these frames are identified, the CUWN can prevent harmful intrusions by sending out something known as deauthentication frames to keep your stations from associating via ad hoc mode.

Denial of Service

Not all attacks are aimed at the goal of stealing information. Sometimes the hacker just wants to cause some major network grief, like jamming the frequency where your WLAN lives to cause a complete interruption of service until you manage to ferret out the jamming signal and disable it. This type of assault is known as a denial of service (DoS) attack.

Mitigation

And this is how we deal with them. First, if someone is jamming the frequency, there isn't much, if anything, you can do. However, many DoS, on-path (formerly known as man-in-the-middle), and penetration attacks operate by deauthenticating, or disassociating, stations from their networks. Some DoS attacks take the form of simply flooding the wireless network with probe requests or association frames, which effectively makes the overwhelmed network unavailable for normal transmissions. These types of management frames are sent unauthenticated and unencrypted. Since deauthentication and disassociation frames are classified as management frames, the Management Frame Protection (MFP) mechanism can be used to prevent the deluge. There are two types of MFP you can use, referred to as infrastructure and client. Let's take a look at each of them now.

Infrastructure Mode

This sweet strategy doesn't require configuration on the station—only the AP. Controllers generate a specific signature for each WLAN, which is added to each management frame it sends, and any attempt to alter this is detected by the message integrity check (MIC) in the frame. Therefore, when an AP receives a management frame from an unknown SSID, it reports the event to the controller and an alarm is generated.

When an AP receives an MFP protected frame from an unknown SSID, it queries the controller for the key. If the BSSID isn't recognized by the controller, it will return an "unknown BSSID" message, which causes the AP to drop the frame.

Client Mode

Often rogue APs attempt to impersonate the company AP. With client MFP, all management frames between the AP and the

station are protected because clients can detect and drop spoofed or invalid management frames.

Passive Attacks

So far, the attacks I've talked about are in a category referred to as active attacks because in deploying them, the hacker is interacting with stations, the AP, and the network in real time. But beware—there are other ways into the fort!

Passive attacks are most often used to gather information to be used in an active attack a hacker is planning to execute later, and they usually involve wireless sniffing. During a passive attack, the hacker captures large amounts of raw frames to analyze online with sniffing software used to discover a key and decrypt it "on the fly." Or the data will be analyzed offline, which simply means the bad guy will take the data away and analyze it later.

Mitigation

In addition to the tools already described, you can use an intrusion detection system (IDS) or an intrusion protection system (IPS) to guard against passive attacks:

- **IDS** An intrusion detection system (IDS) is used to detect several types of malicious behaviors that can compromise the security and trust of your system. These malicious behaviors include network attacks against vulnerable services; data-driven attacks on applications; host-based attacks like privilege escalation; unauthorized logins; access to sensitive files; and malware like viruses, Trojan horses, and worms.
- **IPS** An intrusion prevention system (IPS) is a computer security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real time, to block or prevent those activities. For example, a network-based IPS will operate inline to monitor all network traffic for malicious code or attacks. When either is detected, it can drop the offending packets while still allowing all other traffic to pass.

Which approach you'll opt to go with depends on the size of your wireless network and how tight your security needs to be. The goal of a security mechanism is to provide three features:

- Confidentiality of the data
- Data integrity
- An assured identification process

And when faced with decisions about security, you need to consider these three things:

- The safety of the authentication process
- The strength of the encryption mechanism
- Its ability to protect the integrity of the data

Real World Scenario: War Driving

It's a fact—wireless networks are pretty much everywhere these days. You can get your hands on a wireless access point for less than \$100.00, and they're flying off the shelves. You can find APs in public places like shopping malls, coffee shops, airports, and hotels, and in some cities, you can just hang out in a downtown area and zero in on a veritable menu of APs operating in almost every nearby business.

Predictably, this proliferation of APs has led to a new hobby for those with enough skill: It's called *war driving*. Not for the technologically challenged, war driving involves driving around in a car with a laptop, a wireless NIC, and a high-gain antenna, trying to locate open APs. If one with high-speed Internet access is found, it's like hitting the jackpot. People do this aided by various software programs and Global Positioning Systems (GPSs) to make their game even easier. But it's not always innocent—war drivers can be a serious security threat because they can potentially access anything on your wireless LAN as well as anything it's attached to! Even though they're not a sinister threat most of the time, realize that in the very least, they're consuming precious resources from your network. So, if you happen to notice unusually slow-moving vehicles outside your home or business—especially those with computer equipment inside—know that you're the potential target of a war driver.

A good place to start discussing Wi-Fi security is by talking about the basic security that was incorporated into the original 802.11

standards and why those standards are still way too flimsy and incomplete to help us create a secure wireless network relevant to today's challenges.

Open Access

All Wi-Fi Certified small-office, home-office (SOHO) wireless LAN products are shipped in "open-access" mode, with their security features turned off. Although open access or no security may be appropriate and acceptable for public hot spots such as coffee shops, college campuses, and maybe airports, it's definitely not an option for an enterprise organization, and it's probably not even adequate for your private home network.

With what I've told you so far, I'm sure you agree that security needs to be enabled on wireless devices during their installation in enterprise environments. Yet surprisingly, many companies actually don't enable any WLAN security features. Obviously, the companies that don't enable security features are exposing their networks to tremendous risk.

The reason that the products are shipped with open access is so that any person who knows absolutely nothing about computers can just buy an access point, plug it into their cable or DSL modem, and voilà—they're up and running. It's marketing, plain and simple, and simplicity sells.

Service Set Identifiers, Wired Equivalent Privacy, and Media Access Control Address Authentication

What the original designers of 802.11 did to create basic security was to include the use of SSIDs, open or shared-key authentication, static WEP, and optional *Media Access Control (MAC) authentication/MAC filtering*. Sounds like a lot, but none of these really offer any type of serious security solution—all they may be close to adequate for is use on a common home network. But we'll go over them anyway.

An SSID is a common network name for the devices in a WLAN system that create the wireless LAN. An SSID prevents access by any client device that doesn't have the SSID. The thing is, by default, an access point broadcasts its SSID in its beacon many times a second. And even if SSID broadcasting is turned off, a bad guy can discover the SSID by monitoring the network and just waiting for a client response to the access point. Why? Because, believe it or not, that information, as regulated in the original 802.11 specifications, must be sent in the clear—how secure!

Note If you cannot see an AP when trying to perform a site survey, verify that the AP has SSID beaconing enabled.

Two types of authentication were specified by the IEEE 802.11 committee: open authentication and shared-key authentication. Open authentication involves little more than supplying the correct SSID—but it's the most common method in use today. With shared-key authentication, the access point sends the client device a challenge-text packet that the client must then encrypt with the correct WEP key and return to the access point. Without the correct key, authentication will fail and the client won't be allowed to associate with the access point. But shared-key authentication is still not considered secure because all an intruder has to do to get around this is detect both the clear-text challenge and the same challenge encrypted with a WEP key and then decipher the WEP key. Surprise—shared key isn't used in today's WLANs because of clear-text challenge.

With open authentication, even if a client can complete authentication and associate with an access point, the use of WEP prevents the client from sending and receiving data from the access point unless the client has the correct WEP key. A WEP key is composed of either 40 or 128 bits, and in its basic form, it's usually statically defined by the network administrator on the access point and all clients that communicate with that access point. When static WEP keys are used, a network administrator must perform the time-consuming task of entering the same keys on every device in the WLAN. Obviously, we now have fixes for this because tackling this would be administratively impossible in today's huge corporate wireless networks!

Finally, client MAC addresses can be statically typed into each access point, allowing MAC filtering, and any frames that show up to the AP without a known MAC address in the filter table will be denied access. Sounds good, but of course all MAC layer information must be sent in the clear—anyone equipped with a free wireless sniffer can just read the client packets sent to the access point and spoof their MAC address. If you have a small number of wireless clients and you don't want to deploy an encryption-based access method, MAC address filters may be sufficient.

Note If you cannot connect to an AP and you've verified that your DHCP configuration and WEP key are correct, check the MAC address filtering on the AP.

WEP can actually work if administered correctly. But basic static WEP keys are no longer a viable option in today's corporate networks without some of the proprietary fixes that run on top of WEP.

Geofencing

Geofencing is the process of defining the area in which an operation can be performed by using global positioning (GPS) or radio

frequency identification (RFID) to define a geographic boundary. An example of usage involves a location-aware device of a location-based service (LBS) user entering or exiting a geofence. This activity could trigger an alert to the device's user as well as messaging to the geofence operator.

Remote Authentication Dial-In User Service (802.1X)

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that offers us several security benefits: authorization, centralized access, and accounting supervision regarding the users and/or computers that connect to and access our networks' services. Once RADIUS has authenticated the user, it allows us to specify the type of rights a user or workstation has, plus control what it, or they, can do within the network. It also creates a record of all access attempts and actions. The provision of authentication, authorization, and accounting is called AAA, which is pronounced just like the automobile insurance company, "triple A," and it's part of the IEEE 802.1X security standard.

RADIUS has risen to stardom because of its AAA features and is often employed by ISPs, web servers, wireless networks, and APs as well as network ports—basically, by anybody who wants or needs a AAA server. And these servers are only becoming more critically important in large corporate environments, and that's because they offer security for wireless networks. From the Linksys security screen shown earlier, you can see that RADIUS is an available option. If you choose it, you'll be asked for the IP address of the RADIUS server so the AP can send authentication packets.

Figure 12.21 shows how the AP becomes an authenticator when you choose the RADIUS authentication method.

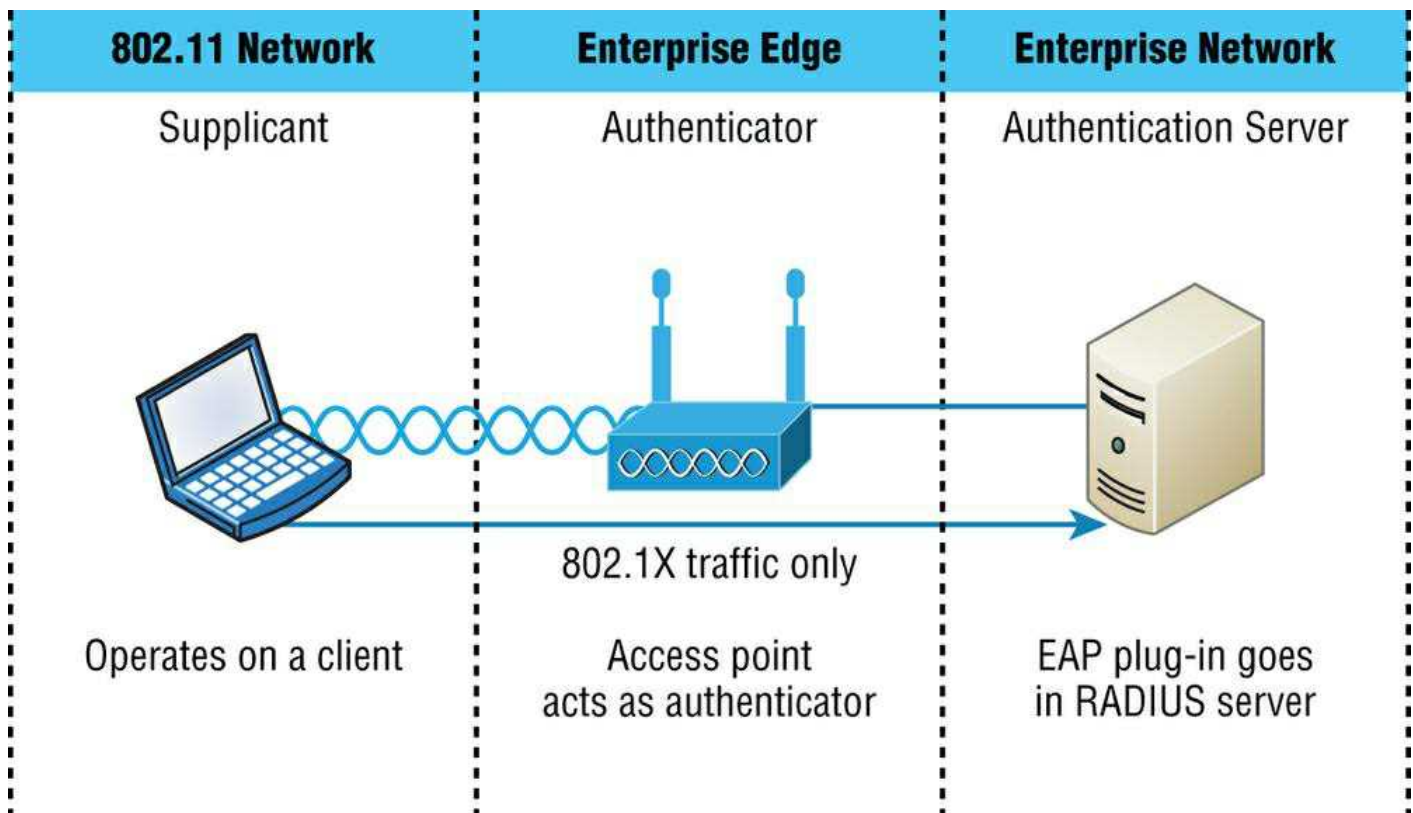


Figure 12.21: RADIUS authentication server

Now packets must pass through the AP until the user and/or host gets authenticated by the RADIUS server.

Temporal Key Integrity Protocol

Put up a fence, and it's only a matter of time until bad guys find a way over, around, and through it. And true to form, they indeed found ways to get through WEP's defenses, leaving our Wi-Fi networks vulnerable—stripped of their Data Link layer security! So someone had to come to the rescue. In this case, it happened to be the IEEE 802.11i task group and the Wi-Fi Alliance, joining forces for the cause. They came up with a solution called Temporal Key Integrity Protocol (TKIP). The Wi-Fi Alliance unveiled it back in late 2002 and introduced it as *Wi-Fi Protected Access (WPA)*. This little beauty even saved us lots of money because TKIP—say this like "tee kip"—didn't make us upgrade all our legacy hardware equipment in order to use it. Then, in the summer of 2004, the IEEE put its seal of approval on the final version and added even more defensive muscle with goodies like 802.1X and AES-CCMP (AES-Counter Mode CBC-MAC Protocol) upon publishing IEEE 802.11i-2004. The Wi-Fi Alliance responded positively by embracing the now-complete specification and dubbing it WPA2 for marketing purposes.

A big reason that TKIP doesn't require buying new hardware to run is that it just wraps around the preexisting WEP encryption key (which was way too short) and upgrades it a whole lot to much more impenetrable 128-bit encryption. Another reason for TKIP's innate compatibility is that both its encryption mechanism and the RC4 algorithm used to power and define WEP, respectively, remained the same.

But there are still significant differences that help make it the seriously tough shield it is, one of them being that it actually changes each packet's key. Let me explain: Packet keys are made up of three things: a base key, the transmitting device's MAC address, and the packet's serial number. It's an elegant design because, although it doesn't place a ton of stress on workstations and APs, it serves up some truly formidable cryptographic force. Here's how it works: Remember the packet serial number part of the transmission key? Well, it's not just your average serial number; it's special—very special.

TKIP-governed transmission ensures that each packet gets its very own 48-bit serial number, which is augmented with a sequence number whenever a new packet gets sent out, and not only serves as part of the key but also acts as the initialization vector. And the good news doesn't end there—because each packet is now uniquely identified, the collision attacks that used to happen using WEP are also history. Plus, the fact that part of the packet's serial number is also the initialization vector prevents something called *replay attacks*. It takes an ice age for a 48-bit value to repeat, so replaying packets from some past wireless connection is just not going to happen; those "recycled" packets won't be in sequence, but they will be identified, thus preventing the attack.

Now for what may be the truly coolest thing about TKIP keys: the base key. Because each base key that TKIP creates is unique, no one can recycle a commonly known key over and over again to gain access to a formerly vulnerable WEP wireless LAN. This is because TKIP throws the base key into the mix when it assembles each packet's unique key, meaning that even if a device has connected to a particular access point a bunch of times, it won't be permitted access again unless it has a completely new key granting it permission.

Even the base key itself is a fusion of something called *nonces*—an assortment of random numbers gleaned from the workstation, the access point, and each of these devices' MAC addresses, so this should also be referred to as a *session secret*. So basically, if you've got IEEE 802.1X authentication working for you, rest assured that a session secret absolutely will be transmitted securely to each machine every time it initiates a connection to the wireless LAN by the authentication server—unless you're using preshared keys, that is, because if you happen to be using them, that important session secret always remains the same. Using TKIP with preshared keys is kind of like closing an automatically locking security door but not enabling its security settings and alarm—anyone who knows where the secret latch is can get right in!

Wi-Fi Protected Access or WPA2 Pre-Shared Key

These are both essentially another form of basic security that's really just an add-on to the specifications. Even though you can totally lock the vault, as I mentioned in the previous section, WPA/WPA2 Pre-Shared Key (PSK) is a better form of wireless security than any other basic wireless security method I've talked about so far. And note that I did say basic! But if you are using only MAC address filters and/or WEP, and you find that interlopers are still using your network and dragging down the performance, adding this layer of security should help tremendously since it's a better form of access control than either of those measures.

Wi-Fi Protected Access (WPA) is a standard developed by the Wi-Fi Alliance, formerly known as the Wireless Ethernet Compatibility Alliance (WECA). WPA provides a standard for authentication and encryption of WLANs that's intended to solve known security problems. The standard takes into account the well-publicized AirSnort and on-path (man-in-the-middle) WLAN attacks. So of course we use WPA2 to help us with today's security issues.

The PSK verifies users via a password or identifying code (also called a *passphrase*) on both the client machine and the access point. A client gains access to the network only if its password matches the access point's password. The PSK also provides keying material that TKIP or Advanced Encryption Standard (AES) uses to generate an encryption key for each packet of transmitted data.

Although more secure than static WEP, PSK still has a lot in common with static WEP in that the PSK is stored on the client station and can be compromised if the client station is lost or stolen (even though finding this key isn't all that easy to do). It's a definite recommendation to use a strong PSK passphrase that includes a mixture of letters, numbers, and nonalphanumeric characters. With WPA, it's still actually possible to specify the use of dynamic encryption keys that change each time a client establishes a connection.

Note The benefit of WPA over a static WEP key is that WPA can change dynamically while the system is used.

WPA is a step toward the IEEE 802.11i standard and uses many of the same components, with the exception of encryption—802.11i (WPA2) uses AES-CCMP encryption. The IEEE 802.11i standard replaced WEP with a specific mode of AES known as the CCMP, as mentioned earlier. This allows AES-CCMP to provide both data confidentiality (encryption) and data integrity.

Note The highest level of wireless encryption you can run is WPA3-SAE.

The following screen shows that if you choose WPA2 Personal on the Linksys AP, you can then enter your passphrase—it's really called WPA2 Pre-Shared Key, but whatever.

The screenshot displays the Linksys web interface for configuring wireless security. The 'Wireless' menu is open, and the 'Wireless Security' sub-tab is selected. The configuration options are as follows:

Setting	Value
Security Mode:	WPA2 Personal
WPA Algorithms:	AES
WPA Shared Key:	I can put in 64 characters
Group Key Renewal:	300 seconds

At the bottom of the configuration area, there are two buttons: 'Save Settings' and 'Cancel Changes'.

You have a choice of TKIP or AES as the encryption, and by the way, you can choose up to a 64-character key—pretty tight!

WPA's mechanisms are designed to be implementable by current hardware vendors, meaning that users should be able to implement WPA on their systems with only a firmware/software modification.

Note The IEEE 802.11i standard has been sanctioned by WPA and is called WPA version 2.

Certificates and PKI

WPA2 can use the Extensible Authentication Protocol (EAP) method for authentication.

EAP isn't a single method but a framework that enhances the existing 802.1X framework. The EAP framework describes a basic set of actions that will take place, and each EAP type differs in the specifics of how it operates within the framework. These variables include things like whether they use passwords or certificates as well as the ultimate level of security provided. Some of the EAP methods require that certificates be used as the credential during authentication. This means that to implement those methods, you must have a Public Key Infrastructure (PKI) in your network. A PKI requires a certificate server that issues certificates to your users and/or devices. These certificates, which consist of a public/private key pair, must be securely installed on the devices and renewed at regular intervals.

In symmetric encryption, the two encryption keys are the same, just as they are with WEP keys, but in asymmetric encryption, the key used to encrypt is different from the key used to decrypt. In PKI, asymmetric keys are used, and the keys are called a public/private key pair. Certificates are binding regulations of a public/private key pair generated by a certificate server to a user or computer. As long as two parties trust the same certificate source, called the trusted certificate authority (CA), they can trust the certificate they're presented with for authentication. These keys can also be used for encryption and as digital signatures.

Despite the other uses of public/private keys, our focus here is the use of the certificates as a form of authentication and authorization. And as a means of identifying the device or the user, this is considered the highest form of authentication and

authorization when compared to names and passwords. What all this means is that as long as the AP or controller and the station or user trust the CA that issued the certificates, the certificate is trusted as a means of identification as well.

- **EAP** Extensible Authentication Protocol (EAP) is not a single protocol but a framework for port-based access control that uses the same three components that are used in RADIUS. A wide variety of these include certificates, a PKI, or even simple passwords.
- **PEAP** Protected Extensible Authentication Protocol, also known as Protected EAP or simply PEAP, is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel. It requires only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication.
- **EAP-FAST** EAP-FAST works in two stages. In the first stage, a TLS tunnel is established. Unlike PEAP, however, EAP-FAST's first stage is established by using a pre-shared key called a Protected Authentication Credential (PAC). In the second stage, a series of type/length/value (TLV)-encoded data is used to carry a user authentication.
- **EAP-TLS** EAP Transport Layer Security (EAP-TLS) is the most secure method, but it's also the most difficult to configure and maintain. To use EAP-TLS, you must install a certificate on both the authentication server and the client. An authentication server pair of keys and a client pair of keys need to be generated first, signed using a PKI, and installed on the devices. On the station side, the keys can be issued for the machine itself and/or for the user.

In the authentication stage, the station, along with the authentication server (RADIUS, etc.), exchange certificates and identify each other. Mutual authentication is a solid beneficial feature, which ensures that the station it's communicating with is the proper authentication server. After this process is completed, random session keys are created for encryption.

- **Preshared Key** Finally, a preshared key can be used to secure wireless transmissions. This is most labor intensive as it requires that all devices use the same key as the AP and that the keys be changed frequently to provide adequate security.

Note Tunneled Transport Layer Security (TTLS) provides authentication as strong as EAP-TLS, but it doesn't require each user to be issued a certificate. Instead, only the servers are issued certificates.

Summary

Like rock 'n' roll, wireless technologies are here to stay. And for those of us who have come to depend on wireless technologies, it's actually pretty hard to imagine a world without wireless networks—what did we do before cell phones?

So we began this chapter by exploring the essentials and fundamentals of how wireless networks function. Springing off that foundation, I then introduced you to the basics of wireless radio frequencies (RFs) and the IEEE standards. We discussed 802.11 from its inception through its evolution to current and near-future standards and talked about the subcommittees that create these standards.

All of this led into a discussion of wireless security—or rather, nonsecurity for the most part—which we went over in detail.

We finished the chapter by bringing you up to speed on TKIP and WPA/WPA2 security solutions—important tools used to protect the wireless LANs of today.

Exam Essentials

Understand the IEEE 802.11a specification. 802.11a runs in the 5 GHz spectrum, and if you use the 802.11h extensions, you have 23 non-overlapping channels. 802.11a can run up to 54 Mbps, but only if you are less than 50 feet from an access point.

Understand the IEEE 802.11b specification. IEEE 802.11b runs in the 2.4 GHz range and has three non-overlapping channels. It can handle long distances but with a maximum data rate of up to 11 Mbps.

Understand the IEEE 802.11g specification. IEEE 802.11g is 802.11b's big brother and runs in the same 2.4 GHz range, but it has a higher data rate of 54 Mbps if you are less than 100 feet from an access point.

Understand the IEEE 802.11n specification. IEEE 802.11n operates in the 2.4 GHz and 5 GHz range. Support for 5 GHz bands is optional. Its net data rate ranges from 54 Mbit/s to 600 Mbit/s. The standard also added support for multiple-input, multiple-output (MIMO) antennas.

Understand the IEEE 802.11ac specification. IEEE 802.11ac-2013 is an amendment that builds on 802.11n. Changes include wider channels (80 or 160 MHz versus 40 MHz) in the 5 GHz band, more spatial streams (up to eight versus four). Wave 2 products include additional features like MU-MIMO, 160 MHz channel width support, support for more 5 GHz channels, and four spatial streams with four antennas.

Understand the IEEE 802.11ax specification. IEEE 802.11ax is the successor to 802.11ac. It's marketed as Wi-Fi 6 (2.4 GHz and 5 GHz) and Wi-Fi 6E (6 GHz). It is also known as High Efficiency Wi-Fi, for the overall improvements to Wi-Fi 6. Data rates against the predecessor (802.11ac) is only 39 percent. For comparison, this improvement was nearly 500 percent for the other predecessors.

Understand the different WiFi standards, frequencies, and ranges. WiFi standards are 802.11a/b/g/n/ac/ax using 2.4 GHz and 5 GHz.

Remember the various service set identifiers (SSIDs). SSIDs can use a basic service set, an extended service set, an independent service set (ad hoc), and a roaming service set.

Remember the antenna types. WiFi antennas can be Omni directional or directional.

Remember the encryption standards. Encryption standards include Wi-Fi Protected Access (WPA), WPA2 Personal (Advanced Encryption Standard-AES), Temporal Key Integrity Protocol (TKIP), and WPA/WPA2 Enterprise (AES/TKIP).

Remember the cellular technologies. Technologies used in cellular communications include code division multiple access (CDMA), global System Mobile (GSM), Long-Term Evolution (LTE), and 3g, 4g, and 5g.

Understand MIMO/MU-MIMO. MIMO is multiple-input, multiple output, which is widely used in 802.11n and 802.11zc. MU-MIMO is multiuser multiple input, multiple output, which is used in the new 802.11ax protocol.

Remember the wireless LAN modulation techniques. Direct-sequence spread spectrum (DSSS) is the most widely used modulation technique, but it has speeds only to 11 Mbps. To get the higher speeds needed in today's WLANs, we use orthogonal frequency-division multiplexing (OFDM) in 802.11g/a/n and 802.11ac/ax networks.

Understand how WPA works in a WLAN. Wi-Fi Protected Access (WPA) is the security of choice in today's home and corporate networks. It provides both authentication and encryption (either TKIP or AES).

Written Lab

You can find the answers to the written labs in Appendix A. Write the answers to the following questions about wireless networking:

1. What is the maximum data rate of IEEE 802.11b?
2. What is the maximum data rate of IEEE 802.11g?
3. What is the maximum data rate of IEEE 802.11a?
4. What is the frequency range of IEEE 802.11b?
5. What is the frequency range of IEEE 802.11g?
6. What is the frequency range of IEEE 802.11a?
7. What is the possible bandwidth of 802.11ac?
8. Why would we use WPA instead of basic WEP?
9. Which IEEE committee has been sanctioned by WPA and is called WPA2?
10. The IEEE 802.11b/g basic standard has how many non-overlapping channels?

?

?

?

?

?

?

?

?

?

?

Answers

1. 11 Mbps
2. 54 Mbps
3. 54 Mbps
4. 2.4 GHz
5. 2.4 GHz
6. 5 GHz
7. 1 Gbps
8. The values of WPA keys can change dynamically while the system is being used.
9. The IEEE 802.11i standard has been sanctioned by WPA and is called WPA version 2.
10. Three

Review Questions

You can find the answers to the review questions in Appendix B.

1. You need to install wireless Internet access in an open warehouse environment. After installing the equipment, the technician notices varying signal strengths throughout the warehouse. How do you make sure there is full coverage? ?
 - A. Turn on broadcast key rotation.
 - B. Change the encryption method used on all the APs.
 - C. Change the antenna placement.
 - D. Use channel bonding.
 - E. Use channel shaping.
2. Which of the following uses a certificate on both the server and client to provide the best wireless security with 802.1X (and is hardest to implement)? ?
 - A. AES
 - B. TTLS
 - C. TLS
 - D. TKIP
3. What is the frequency range of the IEEE 802.11g standard? ?
 - A. 2.4 Gbps
 - B. 5 Gbps
 - C. 2.4 GHz
 - D. 5 GHz
4. Which devices can interfere with the operation of a wireless network because they operate on similar frequencies? (Choose two.) ?
 - A. Copier
 - B. Microwave oven
 - C. Toaster
 - D. Cordless phone
 - E. IP phone
 - F. AM radio
5. Which wireless standard allows you to channel-bond to increase bandwidth and uses both the 2.4 GHz and 5 GHz frequencies? ?
 - A. 802.11b
 - B. 802.11g
 - C. 802.11a
 - D. 802.11n
 - E. 802.11ac
6. Which of the following is considered a PAN? ?
 - A. AES
 - B. BSS
 - C. SSID
 - D. Bluetooth
7. How many non-overlapping channels are available with 802.11a? ?
 - A. 3
 - B. 12
 - C. 23

- D. 40
8. What is the maximum data rate for the 802.11a standard? ?
- A. 6 Mbps
 - B. 11 Mbps
 - C. 22 Mbps
 - D. 54 Mbps
9. You need to install wireless on multiple floors of a large building and maintenance area. What is your first concern before installing the APs? ?
- A. Authentication
 - B. Encryption
 - C. Channel overlap
 - D. AP configuration
10. What is the maximum data rate for the 802.11b standard? ?
- A. 6 Mbps
 - B. 11 Mbps
 - C. 22 Mbps
 - D. 54 Mbps
11. You connect a new host to your company's wireless network. The host is set to receive a DHCP address and the WPA2 key is entered correctly. However, the host cannot connect to the network. What can the problem be? ?
- A. DNS is not configured on the host.
 - B. MAC filtering is enabled on the AP.
 - C. The network has run out of wireless connections.
 - D. The host is enabled to run 802.11b and 802.11g.
12. Which is the highest encryption that WPA2 can use? ?
- A. AES-CCMP
 - B. PPK via IV
 - C. PSK
 - D. TKIP/MIC
13. Which additional configuration step is necessary in order to connect to an access point that has SSID broadcasting disabled? ?
- A. Set the SSID value in the client software to public.
 - B. Configure open authentication on the AP and the client.
 - C. Set the SSID value on the client to the SSID configured on the AP.
 - D. Configure MAC address filtering to permit the client to connect to the AP.
14. Which spread-spectrum technology does the 802.11b standard define for operation? ?
- A. IR
 - B. DSSS
 - C. FHSS
 - D. DSSS and FHSS
 - E. IR, FHSS, and DSSS

15. Which wireless LAN design ensures that a mobile wireless client will not lose connectivity when moving from one access point to another (roaming)? ?
- A. Using adapters and access points manufactured by the same company
 - B. Overlapping the wireless cell coverage by at least 10 percent
 - C. Configuring all access points to use the same channel
 - D. Utilizing MAC address filtering to allow the client MAC address to authenticate with the surrounding APs
16. You have installed a point-to-point connection using wireless bridges and Omni directional antennas between two buildings. The throughput is low. What can you do to improve the link? ?
- A. Replace the bridges with APs.
 - B. Replace the Omni directional antennas with Yagis.
 - C. Configure 802.11a on the links.
 - D. Install amps to boost the signal.
17. What does extended service set (ESS) ID mean? ?
- A. That you have more than one access point, and they are in the same SSID connected by a distribution system
 - B. That you have more than one access point, and they are in separate SSIDs connected by a distribution system
 - C. That you have multiple access points, but they are placed physically in different buildings
 - D. That you have multiple access points, but one is a repeater access point
18. What is one reason that WPA encryption is preferred over WEP? ?
- A. A WPA key is longer and requires more special characters than the WEP key.
 - B. The access point and the client are manually configured with different WPA key values.
 - C. WPA key values remain the same until the client configuration is changed.
 - D. The values of WPA keys can change dynamically while the system is used.
19. How wide are the channels used in 802.11n in order to gain the large bandwidth that the specification provides? ?
- A. 22 MHz
 - B. 20 MHz
 - C. 40 MHz
 - D. 100 MHz
20. 802.11n uses MIMO. How does this optimize throughput to gain the high-speed advantage that 802.11n provides? ?
- A. By specifying an acknowledgment of each and every frame, 802.11n provides better overhead.
 - B. Several frames are sent by several antennas over several paths and are then recombined by another set of antennas.
 - C. One frame at a time is sent, but faster than in 802.11g because multiple antennas are used (multiple-in, multiple-out).
 - D. MIMO packs smaller packets into a single unit, which improves throughput.

Answers

1. C. It is imperative that a good site survey is completed before you install your wireless network. Trying various types of antennas and their placements is the key to covering the whole wireless area.
2. C. TLS provides really good wireless security, but it's hard to implement because you need to install a certificate on your server and also on all your clients. TTLS only uses a server-side certificate.
3. C. The IEEE 802.11b and IEEE 802.11g both run in the 2.4 GHz RF range.
4. B, D. If you are running 802.11b/g frequency, then you can receive interference from microwave ovens and cordless phones.
5. D. 802.11n uses channel bonding of both the 2.4 GHz range and the 5 GHz range to get increased bandwidth of over 100 Mbps.
6. D. Bluetooth works wirelessly to connect our phones, keyboards, and so on in small areas, also known as personal area networks (PANs).
7. B. The IEEE 802.11a standard provides up to 12 non-overlapping channels, or up to 23 if you add the 802.11h standard.
8. D. The IEEE 802.11a standard provides a maximum data rate of up to 54 Mbps.

- 9.** C. If you have a large area to cover with wireless, you need to be concerned with channel overlap.
- 10.** B. The IEEE 802.11b standard provides a maximum data rate of up to 11 Mbps.
- 11.** B. If everything is correctly configured on the host, then MAC filtering would stop the host from connecting to the AP. If you try to connect and can't, check the AP's settings.
- 12.** A. The IEEE 802.11i standard replaced Wired Equivalent Privacy (WEP) with a specific mode of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol. This allows AES-Counter Mode CBC-MAC Protocol (AES-CCMP) to provide both data confidentiality (encryption) and data integrity.
- 13.** C. If you disable SSID broadcasting, which you should, then you must configure the SSID name on the clients that need to connect to the AP.
- 14.** B. The IEEE 802.11b standard uses direct-sequence spread spectrum (DSSS). If you are running 802.11g, it uses orthogonal frequency-division multiplexing (OFDM).
- 15.** B. If you are running an extended service set (meaning more than one AP with the same SSID), you need to overlap the cell coverage by 10 percent or more so clients will not drop out while roaming.
- 16.** B. You need to use directional antennas, like a Yagi, to get the best signal between antennas.
- 17.** A. Extended service set ID means that you have more than one access point, they all are set to the same SSID, and they are all connected together in the same VLAN or distribution system so users can roam.
- 18.** D. WPA is cool because it is easy to configure and works great. Type in a passphrase (assuming you're using a pre-shared key) and you're done. Plus, you have great security because the keys change dynamically.
- 19.** C. 802.11n uses two 20 MHz wide channels to create a 40 MHz wide channel, which provides over 100 Mbps wireless.
- 20.** B. 802.11n MIMO sends multiple frames by several antennas over several paths. The frames are then recombined by another set of antennas to optimize throughput and multipath resistance. This is called spatial multiplexing.