CHAPTER EIGHTEEN

18 Wireless Security and Implementation Considerations

Objectives

This chapter covers the following Cisco-specified objectives for the "Explain and select the appropriate administrative tasks required for a WLAN" section of the 640-802 CCNA exam:

- **Identify and describe the purpose of the components in a small wireless network (including: SSID, BSS, ESS)**
- **Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point**
- **Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2)**
- **Identify common issues with implementing wireless networks**

Outline

Study Strategies

- The ICND2 and CCNA exams are designed to test on a general understanding of wireless concepts rather than hands-on configuration of wireless devices
- Be sure to have an in-depth understanding of the different wireless security standards (WEP, WPA, and WPA2). Cisco considers these important since this represents the core of your wireless network security architecture
- When focusing on implementation, be sure to understand how to deploy close proximity 802.11b/g wireless access points without causing them to interfere with each other

Introduction

Okay. I admit it. I (Jeremy) drove to a friend's house and arrived a bit early, so I decided to spend a few minutes in the car checking my email. I pulled my laptop out of the back and did a quick wireless scan of the neighborhood. Two SSIDs appeared: Linksys and Netgear, both without security. I joined the Linksys network and checked my online web mail. (I prefer to think of this as "borrowing" the Internet connection rather than "stealing" wireless.) That's when a bearded man with a tattered shirt and loaded shotgun came out the front door. Sorry; I just needed a dramatic twist.

Harmless enough, right? *Wrong!* Imagine a strange individual walking into your front office with a laptop and saying, "Would you mind if I plugged into that wall jack over there?" Yes, I would mind. That would undermine every written security standard we have in our organization. But that's exactly what happens when you fail to properly understand and implement the security standards available for wireless networks. Keep in mind that not all wireless security is created equal. Some security standards (such as WEP) may give you a false sense of security, because many network intruders eat WEP security keys for breakfast. This is why a good comprehension of wireless security is absolutely necessary, even for the novice network administrator.

Understanding the Threats

Introducing wireless networking into your organization opens the door to three new types of attacks on your network: war driving, direct hacking, and employee ignorance. Let me explain each of these in detail.

War Driving

You know you've entered a new realm of network security when "driving" becomes one of the intrusion efforts. This term actually originated from the days of old, when a similar method known as war dialing was in place. In the 1980s, most businesses connected offices through dialup connections, typically using modems. War dialing would consist of a hacker randomly dialing through the phone number range in his local area (for example, setting up his modem to dial numbers 100-0000 through 999-9999 in the U.S.). The dialing itself was not the hacking attempt; rather, it was a scan for phone numbers responding to modem signals.

War driving uses a similar concept. An intruder mounts an 802.11-compatible wireless antenna on his vehicle and drives through the city, identifying available wireless networks. When combined with a Global Positioning System (GPS) device, war-driving software (such as KisMet or KisMac) can be very accurate in pinpointing the available wireless networks on a map of the city. When the intruder returns home, he can analyze the available networks and plot his next steps of attack.

Keep in mind that war driving can discover wireless networks even if they are encrypted, authenticated, and/or using a "hidden" (nonbroadcast) SSID.

Direct Hacking

The direct hacking effort typically begins after the war-driving scan of the area is complete. The intruder then identifies what network(s) he wants to attack. The hacking effort can come in many forms:

- **Breaking into the WLAN:** As soon as the intruder has identified available wireless networks, he can try to break the encryption and/or authentication system. Although this can be accomplished (with much effort) from the attacker's home, it is usually attempted within range of the wireless signal. For example, the attacker can sit in the parking lot and attempt to break into the building's wireless network. If he is successful, he joins the wireless network and begins scanning the internal network of your organization to find available resources.
- **Decrypting data:** Because wireless network communication is transmitted into the air, anything that your users access from a wireless device has the potential to be captured by an intruder's wireless sniffer software. If this data is sent unencrypted, the intruder can simply reassemble the packets to regenerate the original file (such as a Microsoft Word document, an Adobe Acrobat PDF file, or even a VoIP conversation). If the data is encrypted, the intruder captures the data and returns home to attempt to break the encryption keys. If he is successful, he can reassemble the original files and steal corporate data.
- **Attempting a wireless DoS attack:** The final effort that can be accomplished by direct hacking methods is to unleash a denial of service (DoS) attack on the wireless network. If the intruder is successful, the wireless access point that he attacks is rendered inoperable to your company. This type of attack is not as common in a WLAN environment, because most companies have not yet moved critical network services to the wireless network. The hacker's efforts would be seen as more of a temporary inconvenience than a major network issue.

Employee Ignorance

Employee ignorance was the best term I could come up with for this category of security threat. Depending on the individual employee, I suppose you could substitute "insolence," "rebellion," or "stupidity" for the word "ignorance." Here's the concept: Your company policy dictates that you will not run wireless networking because of security threats. However, the "ignorant" employee has a laptop he really wants to use with wireless technology, which gives him the freedom to roam between areas while remaining connected to the network. The

employee takes networking into his own hands and connects a low-end wireless access point to the network jack in his cubicle. With the click of a Cat 5 cable, your network security has been reduced to nothing, and a gaping hole into the network is now broadcast to the outside world. This same issue can occur even if your company provides a WLAN network and the user is just outside the range of the wireless signal. If appropriate detection measures are not taken, this massive hole in your network security can go undiscovered for months!

Deploying a Secure Wireless Network

Although volumes could be (and have been) written on wireless security, I would just like to discuss the 10,000-foot view of wireless security. This will give you an idea of the areas of focus when you are considering using wireless networking technology in your organization. As soon as you understand these areas, you can begin digging deeper into the technology to find the right fit for your wireless design.

TIP

The CCENT and CCNA certifications require only a foundational understanding of wireless security topics, which are discussed in this book.

Wireless security can be broken into three major categories: encryption, authentication, and detection.

Wireless Encryption

Objective:

- Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2)

When you're ready for a technology roller coaster ride, begin studying the history of wireless encryption standards. I mentioned in the preceding chapter that wireless networking technology is so amazing that companies began using it long before the security standards were heavily tested and proven to withstand attacks. So, fasten your seat belt, and let's ride through the evolution of wireless encryption standards, starting where it all began: with WEP.

Wired Equivalent Privacy (WEP)

The WEP standard was the first measure of security released for wireless networking. This encryption method was based on the simple concept of using preshared keys (PSKs) to generate an encryption algorithm. Here's an overview of how the WEP encryption algorithm works:

The WEP standard uses an encryption formula called RC4. This is essentially a mathematical formula that takes every piece of data you want to encrypt and scrambles it. The missing piece of this formula is the PSK, which you enter. This is visually demonstrated in Figure 18.1.

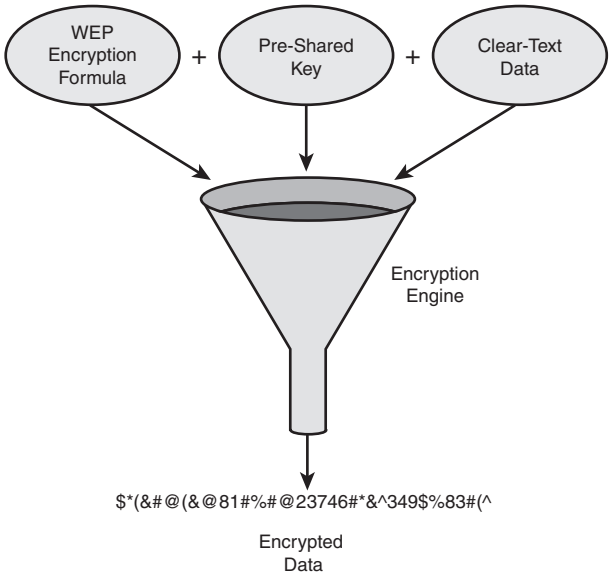

FIGURE 18.1 The mechanics of WEP encryption.

When the wireless access point receives data, it uses the reverse formula to decrypt the data. So, for WEP to work successfully, you must manually enter the PSK on both the wireless client and the wireless access point.

When WEP was originally released (in 1997), it used 64-bit encryption, which is considered weak by today's standards. You can compare 64-bit encryption to a math formula with 64 steps. Each step scrambles the original data more and more.

NOTE

The more bits you use for encryption, the more complex your encryption algorithm, and the more difficult it is to break. However, the more bits you use for encryption, the harder it is for your network device to communicate because of the processing power needed. This may result in slower network communication.

Unfortunately, within a few years of WEP's initial release, *major* security vulnerabilities were found. The wireless standards groups improved the strength of the WEP algorithm by releasing a 128-bit version in 2002, which some people refer to as WEP2. Although it makes the algorithm slightly more difficult to break, many flaws in the underlying design of WEP caused this security standard to crumble.

Wireless security was suffering in a huge way when WPA was released.

TIP

Remember that WEP offers 64-bit and 128-bit encryption strengths. Also, keep in mind that the WEP standard allows only static, preshared keys.

Wi-Fi Protected Access (WPA)

The wireless networking industry faced a major issue. A newer encryption algorithm was needed to combat the weaknesses of WEP, but the more complex encryption algorithms would require more-powerful 802.11-compatible wireless hardware to process the algorithm. By this point, the industry had already purchased millions of wireless access points and wireless cards, so simply saying, "Sorry! Go ahead and scrap all that equipment and buy new stuff." was not an option. In 2003 the Wi-Fi Alliance (a group of extremely smart people sponsored by many organizations) stepped forward and proposed WPA. WPA used a new encryption algorithm called Temporal Key Integrity Protocol (TKIP). TKIP ran on the same wireless hardware that was originally created, and it used a 128-bit encryption algorithm. It was engineered to dramatically increase the number of encryption keys that could be used and virtually eliminated the attacks that were successful on WEP keys. Although WPA was not flawless, it was a tremendous step forward from the original WEP standard.

Wi-Fi Protected Access, Reloaded (WPA2 and 802.11i)

WPA was never meant to solve the world's wireless security problems. Although it was *much* more secure than WEP, it did have the weakness of using the same old hardware that WEP used. Inherent in that hardware were a few security weaknesses that simply could not be overcome by changing the encryption formula. For that reason, the Wi-Fi Alliance quickly (in 2004) proposed an alternative standard casually called WPA2 and officially called 802.11i.

WPA2 uses a completely different encryption standard known as Advanced Encryption Standard (AES). This encryption standard was standardized by the U.S. government and has been extensively analyzed and tested. The WPA2 standard left behind the old hardware and required that users purchase new wireless hardware (both cards and access points).

To ease the transition, WPA2 hardware can run in backward-compatibility mode to support the original WPA and even WEP standards. This allows an organization to upgrade its wireless access points to the new hardware and still support the older WEP- and WPA-compliant clients. As the clients upgrade to newer wireless devices, WPA2 (and thus AES encryption) can be used.

TIP

WPA uses TKIP encryption, and WPA2 uses AES.

Wireless Authentication (802.1x)

The wireless encryption we've discussed so far does indeed secure the data, but it has a couple of weaknesses. First, using a preshared key system means that you must go to every wireless device and accurately enter the PSK before the device can communicate on the network. Likewise, keeping the same PSK for an extended amount of time increases the chances of the encryption algorithm's being hacked, so it's a good idea to change the PSK on a regular basis. In a small network of 10 or so wireless devices, this may not be a big deal, but in a large network with hundreds or even thousands of wireless devices, this can be a full-time job. The second issue presented by a PSK system is the inability to remove access. For example, if you are using a PSK among your 50 laptop users on the network, and one of the users leaves the company, you must change the PSK for the 49 other wireless users to eliminate the security vulnerability from the former employee.

Simply relying on a shared PSK among all devices is not a secure or scalable solution for business. What was needed was a method of wireless authentication. This would allow you to have a system of granting or restricting access based on a variety of criteria, such as usernames and passwords or certificates. The industry responded with the ultimate authentication method, which we now know as 802.1x.

Usually when we think of network authentication, we think of accessing an operating system. For example, when you log into a Microsoft Windows domain, you must authenticate using a username and password to gain access to shared resources on the Windows-based servers. When you Telnet to a Cisco device, you must authenticate to gain access to manage the device using the Cisco IOS. 802.1x takes authentication to an entirely new level. Now, you must authenticate to gain access to the Layer 2 LAN network fabric. Now, to access the wireless access point and use the 802.11 network, you must authenticate. You can also apply 802.1x to LAN network switches. When a device plugs into an Ethernet port, it must authenticate before it gains access to that port and, thus, the network.

Think of the possibilities as soon as you begin using network authentication! When a user leaves the company, you can negate her user account on a Microsoft Windows server. This will cause her to lose the ability to log on to the Windows workstation and, at the same time, lose the ability to even plug into a switch port or attach to the wireless network! Talk about cutting off a user! Now, let me give you the basics of how this works.

802.1x designates three network devices that participate in network authentication: the supplicant, the authenticator, and the authentication server. Figure 18.2 shows the placement of these devices.

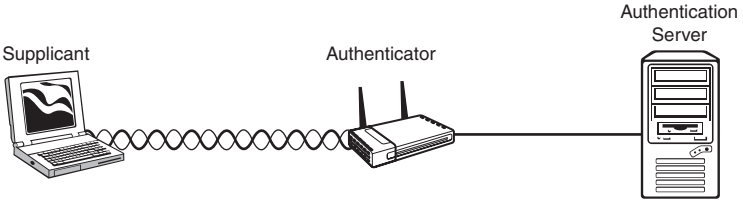

FIGURE 18.2 Equipment participating in 802.1x authentication.

When the user wants to access the network, he must first send his authentication credentials (such as a username and password) to the authenticator, which forwards them to the authentication server. When the authentication server receives the credentials, it checks them against its database and then tells the authenticator whether the device has passed authentication. If the device fails authentication, its access to the network is terminated or severely limited, depending on how you (as the administrator) decide to restrict the device. If the device passes authentication, the supplicant and authentication server generate a dynamic encryption key known as the session key. This provides the same security as the PSK but does not require you to enter a PSK on the client or wireless access point.

I could say much more about network authentication, but, as I said at the beginning of this section, this is a 10,000-foot overview of the concepts. You now know what network authentication is all about and what it is used for. It's now up to you to continue past the CCNA in your Cisco studies to determine the best method to implement network authentication. Proceed into that world with a grave warning: Don't let the EAP monsters eat you alive! Don't worry; you'll know what I mean when you get there.

TIP

Keep in mind that WPA and WPA2 standards allow for static PSKs or dynamic keys when used with 802.1x. WEP allows only static PSKs.

Wireless Intrusion Prevention System (IPS)

By using wireless network authentication and encryption, we have addressed the concerns of war driving and network hackers. But what about those pesky users who plug unauthorized wireless access points into the network? For that we have wireless IPS. You can think of IPS as introducing a variety of detection lasers into your network. I think back to the 1996 movie *Mission Impossible* with Tom Cruise. In one scene, Cruise (well, Ethan Hunt, to be exact) must retrieve a chip from a secured computer room by twisting and contorting his body through a variety of lasers projected around the room. In the same sense, deploying wireless IPS for your network sets up a variety of "sensors" that detect when a policy has been violated. The minute a rogue access point shows up in the network, the system can alert you, pinpointing the location of the access point on a map of your campus. Amazing!

Network-wide IPS can detect a variety of additional suspicious movements around the network, in both the wired and wireless worlds. However, discussing the rest of those detections is part of the Cisco Certified Security Professional (CCSP) certification.

Wireless Implementation Guidelines

Objectives:

- Identify and describe the purpose of the components in a small wireless network. (Including: SSID, BSS, ESS)
- Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point

Now that you've read an overview of the wireless security considerations, let's talk about planning to implement wireless technology. There's much more to planning a wireless LAN deployment than putting a few wireless access points in place. You need to understand how the topology, distance, and placement of wireless access points can affect the efficiency of your wireless LAN.

Understanding Wireless Topologies

Webster's Dictionary defines "topology" as a branch of mathematics concerned with properties of geometric configurations (such as point sets) that are unaltered by elastic deformations (as stretching or twisting) that are homeomorphisms. The CCENT and CCNA exams stop short of requiring a full understanding of homeomorphism (or elastic deformation, for that matter). However, the exams do require you to have some knowledge of the placement of wireless access points in your corporate network. The first piece to understand is that anyone can deploy a wireless network in one of two forms: ad hoc or infrastructure.

Ad hoc wireless networks technically use an Independent Basic Service Set (IBSS) topology. This means that each wireless device independently manages the wireless network. This type of wireless network originates from and includes the wireless device, as shown in Figure 18.3.

This type of network can be created by users on-the-fly to share files or services with others. For example, someone on an airplane might want to share a folder of files with the person next to her. She can create an ad hoc wireless network and allow the other person to join and access the shared files over a network connection.

Ad hoc networks typically are very limited in range and security capabilities. You may want to consider restricting laptops in your corporation from starting ad hoc wireless networks, because they could be considered a potential security vulnerability.

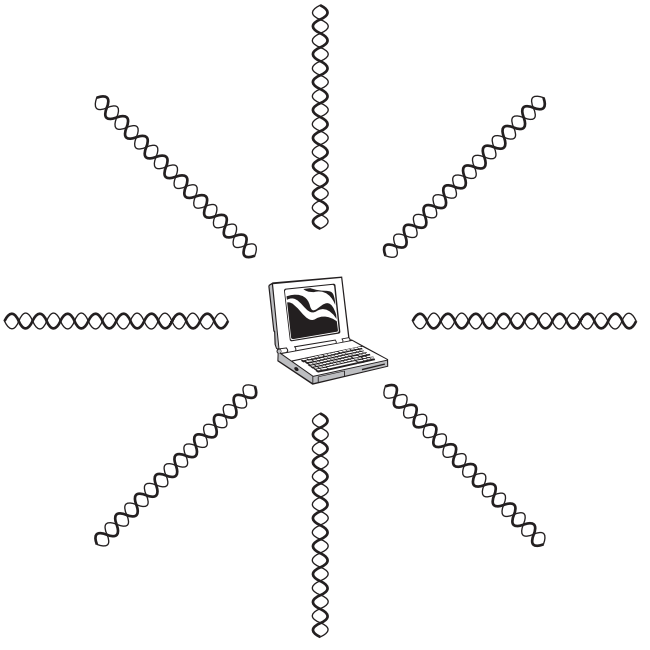

FIGURE 18.3 Ad hoc wireless networking.

Infrastructure wireless networks are a far more common topology. This involves using a dedicated piece of equipment (typically a wireless access point) to initiate and manage the wireless network. Wireless access points can be configured to use one of two infrastructure modes: Basic Service Set (BSS) or Extended Service Set (ESS). The BSS is the simplest form of wireless network. It includes a single wireless access point managing a group of clients, as shown in Figure 18.4.

An ESS is a wireless topology (note the word change from "network" to "topology") that includes two or more wireless access points providing extended wireless coverage across the network, as shown in Figure 18.5.

In Figure 18.5, notice that the wireless coverage overlaps. Wireless best practices state that you should have a 10 to 15% overlap in your wireless coverage. This allows you to implement seamless roaming, allowing a wireless client to move between access points with no service interruption. This is not as critical for data clients, such as laptops. Rather, real-time wireless clients such as 802.11-compatible cell phones, cordless VoIP phones, and some PDAs benefit from the overlapping coverage. Imagine dropping a phone call anytime you moved more than 300 feet in the network! More steps are involved in implementing seamless wireless roaming, but the 10 to 15% overlapping coverage is the starting point.

The second thing to notice in Figure 18.5 is that the channels are different on the two wireless access points. One of the wireless access points uses Channel 11, and the other uses Channel 6. This prevents the two wireless access points from interfering with each other. This channel concept is more fully discussed in Chapter 17, "Understanding Wireless Networking."

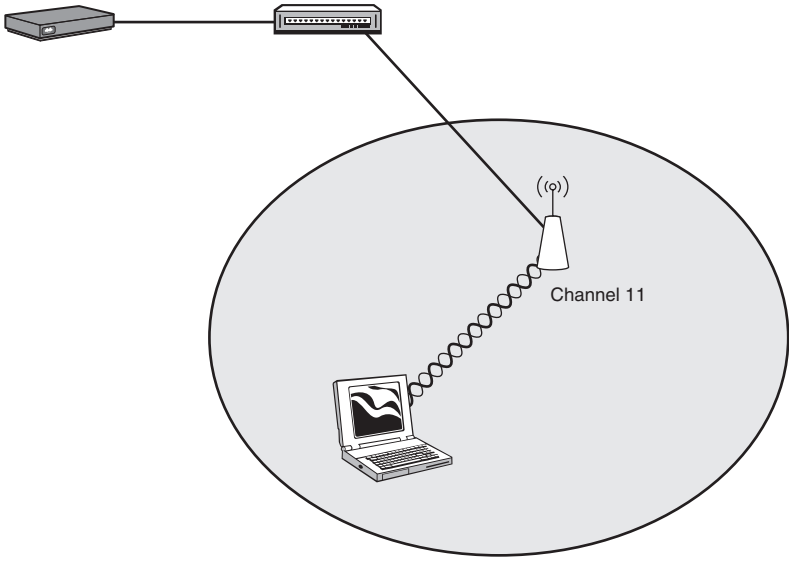

FIGURE 18.4 A single basic service set design.

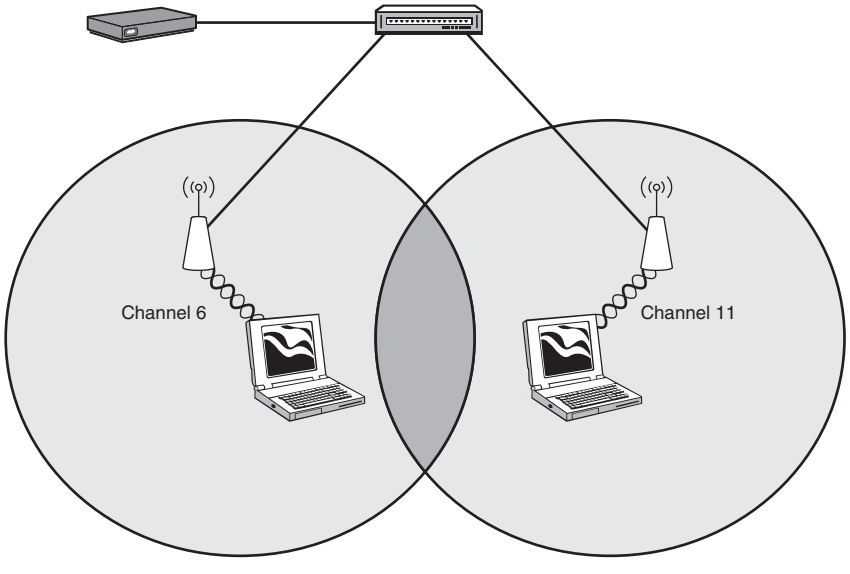

FIGURE 18.5 An extended service set design.

Understanding Wireless Data Rates

So you purchased a new 802.11g wireless access point and implemented it with clients running 802.11g cards. 54Mbps of pure wireless speed—right? Wrong! You may have purchased an access point capable of handling 54Mbps, but you will never reach that speed. *Never!* Repeated performance tests have revealed that actual data rates are about half of the theoretical data rate, on average. This means that your 802.11b access point typically averages about a 5Mbps actual data rate. 802.11g usually is in the 20Mbps range. You might be wondering why the standard says that you can handle 54Mbps when the actual throughput is much less. Well, there are many reasons.

Suppose you travel to the moon in an oxygen-free environment. You carry a single wireless access point and a single wireless card plugged into a single solar-powered laptop that does nothing but run the wireless card (no Bluetooth, no electrical interference). You sit with the wireless access point about 2 feet from the laptop and only send *or* receive data (never both). You *might* get close to the 54Mbps capability. But even that is stretching it. When you move from the world of cables into the world of wireless, you open yourself to an entirely different style of communication. One of the first considerations that you'll notice is the truth behind the range of the access point. Yes, in an obstruction-free environment, the 802.11b/g wireless signal can travel 300 feet. But couple that fact with the idea that higher data rates (11Mbps for 802.11b and 54Mbps for 802.11g) require stronger signals. You'll find that the data rates step down the farther you go from the access point. The following steps are defined for each standard:

- 802.11a and 802.11g:
  - Step 1: 54Mbps
  - Step 2: 48Mbps
  - Step 3: 36Mbps
  - Step 4: 24Mbps
  - Step 5: 18Mbps
  - Step 6: 12Mbps
  - Step 7: 9Mbps
  - Step 8: 6Mbps
- 802.11b:
  - Step 1: 11Mbps
  - Step 2: 5.5Mbps
  - Step 3: 2Mbps
  - Step 4: 1Mbps

So, when you picture wireless data rates coming from your wireless access point, think of them as a radial circle for each rate, with the rates continually decreasing the farther you go. This is represented in Figure 18.6.

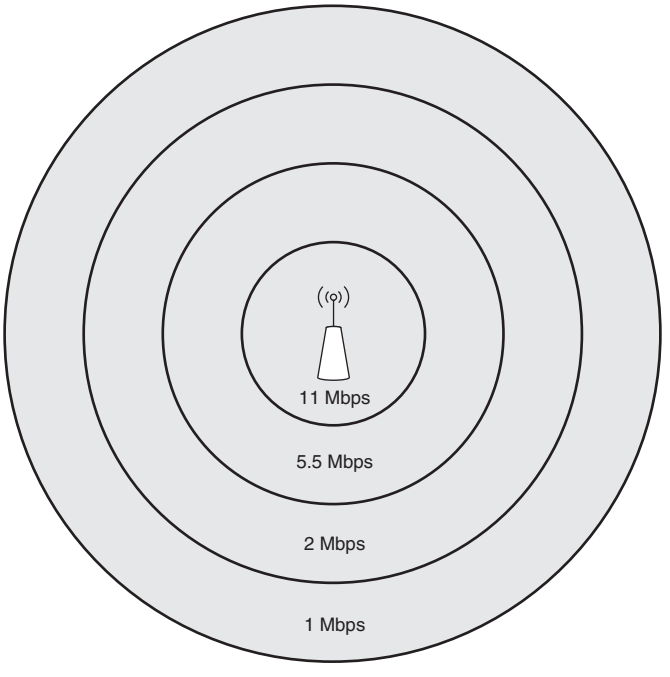

FIGURE 18.6 Wireless data rates.

You'll notice that no exact measurement is attached to each of the radial circles dictating speed around the wireless access point. That's because range is not the only criterion to consider when determining wireless data throughput. From Chapter 17, you'll remember that wireless shares the unlicensed FCC frequency bands with many other pieces of equipment. Bluetooth, other 802.11 wireless clients, cordless phones, and microwave ovens are just a few that can cause interference. Couple that with typical obstructions such as walls, cubicles, desks, and so on, and you have a wireless signal that varies from business environment to business environment. It is impossible to say just how far and "clean" the signal will be in your specific environment. Many companies make testing equipment that displays the signal strength and data rate to a laptop or PDA screen. This gives you a good idea of how wireless will fare in your environment.

NOTE

Because wireless technology uses a CSMA/CA mechanism, all clients adopt the speed of the slowest client on the access point. For example, if three wireless clients are attached to the wireless access point running at 24Mbps, and a wireless client some distance away attaches at 6 Mbps, all clients will run at the lowest speed!

The saving grace of wireless data rates is the fact that most users will not notice. Most devices that use a wireless signal are used for lower-bandwidth communication. For example, a wireless VoIP phone consumes about 100Kbps of bandwidth. Laptops used in wireless environments typically surf the net or check email. Most devices that handle large data file transfers or other high-bandwidth communication typically are hardwired.

General Wireless Implementation Steps

With all those considerations floating around your mind, here are the general steps to implement wireless:

1. **Ensure hardwired operation:** Before adding any wireless to the network, connect a device (such as a laptop) to the same switch port where you plan to connect your wireless access point. Ensure that it operates as expected, verifying VLAN assignment, DHCP operation, and Internet connectivity (if applicable).
2. **Install the wireless access point in your tested switch port:** Some access points will connect using straight-through Ethernet cabling, and others may require a cross-over cable.
3. **Configure a basic wireless network and test:** Keep this initial test extremely simple. Just implement a wireless SSID with no security. After it is configured, join the wireless network from a client, and test your connectivity. Ensure that the client obtains an IP address and can perform the same actions as when you use a hardwired connection.
4. **Add wireless security and test:** Implement the wireless security standard chosen for your network. It's usually best to begin with a preshared key system of security to keep it simple. After you have added the security, reconfigure the wireless client, and test again.

Working through these four steps, you have established a baseline for your wireless network. As you add more features or security standards on top of the existing foundation, you can return to a "last known good" configuration if something goes wrong.

Wireless Troubleshooting

Objective:

- Identify common issues with implementing wireless networks.

Wireless troubleshooting is far more complex than typical wired troubleshooting. Physical problems are much more elusive, because they deal primarily with interference rather than a simple cable break or failing switch port. For example, I recently deployed in a business a wireless network that worked great until 4 in the afternoon. As soon as we crossed the 4 p.m. barrier, all wireless connectivity was lost. After doing some spectrum analysis, we found that a nearby airport was using a device (we still aren't sure what it was) that completely flooded the 2.4GHz frequency range. The company decided to move to 802.11a (which was a fairly large network upgrade) to avoid this interference.

Likewise, wireless technology is fairly new to the industry. You may find that firmware for your access point has bugs and needs to be upgraded to a newer version to avoid persistent crashing (this happens far more often than you may realize). The following wireless troubleshooting checklist may be helpful as you attempt to diagnose the issue.

Client Troubleshooting

Most wireless issues are related to the client:

- **Verify that the wireless card is enabled:** Most new laptops have a button or switch that disables the wireless card to save battery life.
- **Move to a "known good" region of the building:** Do your testing in an area known to have a strong wireless signal. This may require using multiple wireless devices.
- **Verify that the client can identify the wireless network using the installed wireless utility:** If you are unable to identify wireless SSID(s) in your vicinity, the client's wireless card may be disabled, or the wireless access point may not be working.
- **Ensure that the wireless client has the correct wireless security information and supports your security standards:** You may need to re-enter the preshared key to ensure that you entered it correctly. Likewise, the wireless card may not support the wireless security on your network. Try connecting to an SSID that does not use security from the wireless device.

Wireless Access Point Troubleshooting

Most troubleshooting that deals with the wireless access point focuses on physical considerations:

- **Verify that the wireless access point is running the latest firmware version:** Nothing is worse than spending hours on a problem that is related to a bug in the wireless firmware.
- **Test the wireless reception radius at different times of the day:** Because of the varying degrees of interference that may occur over time, it is best to run multiple tests on your signal strength. You can do this simply and inexpensively by carrying around a laptop and observing the reception at differing locations.
- **Verify your wireless channel configuration:** If you have multiple wireless access points or are in an area where other access points may interfere, verify (using wireless software) the most saturated and unsaturated channels. For 802.11b/g, use channels 1, 6, or 11 in the U.S. For 802.11a, many more channels are available, and you should test for the cleanest frequency.
- **Consider the materials around and close to the access point:** Try to avoid installing the access point near metal objects, which reflect the signal. Realize that a concrete block wall will absorb much more signal than a drywall barrier.

Chapter Summary

All in all, deploying a wireless network is not for the fainthearted. Installing a wireless access point in the network essentially broadcasts and extends your network beyond the walls of your organization into treacherous territory. Wireless intruders can begin capturing data and breaking into the network without your ever knowing an attack is happening. This is why it is so critical to understand the security considerations before you attach wireless equipment in your environment.

When securing your wireless network, not all security standards are created equal. The initial WEP system of security offered only 64-bit encryption. It was easily broken because of the key strength as well as a number of flaws that plagued the initial WEP deployment. WEP2 increased the key strength to 128-bit encryption, but it still suffered many of the other weaknesses of WEP. WPA was released to address many of those weaknesses, but it was considered an interim solution while network users began migrating to new hardware. Modern networks employ WPA2 (aka 802.11i) to ensure up-to-date security standards in the world of wireless.

In addition to locking down the wireless network, many implementation considerations must be taken into account. Wireless is susceptible to RF interference. This adds many physical layers of troubleshooting that did not exist in the wired environment. Ensuring that your wireless cells include an acceptable amount of overlap and differing channels lays the foundation for ensuring adequate wireless coverage for your organization.

Key Terms

- 802.11a/b/g/n
- WEP 64-bit
- WEP 128-bit
- WPA
- WPA2 (802.11i)
- 802.1x
- Wireless Intrusion Prevention System (IPS)
- Basic Service Set (BSS)
- Extended Service Set (ESS)
- Radio Frequency (RF)
- 2.4GHz band
- 5GHz band
- Wireless channels
- Wireless cells
- Wireless roaming
- Wireless data rate

Apply Your Knowledge

Review Questions

1. List the three encryption standards you can currently use with wireless networking.
2. Describe the differences between WEP, WPA, and WPA2. What type of encryption does each use? What are their strengths and weaknesses?
3. List three potential vulnerabilities of a wireless network.
4. Because a wireless access point forces all clients to use the speed of the slowest client, how do you think you should ideally deploy your wireless access points?
5. What is the process for successfully installing a wireless access point?

Exam Questions

1. What is a rogue access point?
   - ❍ **A.** An unauthorized access point that has been placed on your LAN
   - ❍ **B.** An access point configured to broadcast the corporate SSID
   - ❍ **C.** An access point using WEP or WEP2 security
   - ❍ **D.** An access point that has been compromised by an intruder

2. When designing a wireless ESS system, how much cell overlap is recommended?
   - ❍ **A.** None. Cell overlap can cause interference.
   - ❍ **B.** 5 to 10%
   - ❍ **C.** 10 to 15%
   - ❍ **D.** 15 to 20%

3. What scenario would be an ideal case to implement WEP security?
   - ❍ **A.** You are running a small business network environment implementing the 802.11a wireless standard
   - ❍ **B.** You would like to implement the 802.1x security standard using a Windows RADIUS server to authenticate users
   - ❍ **C.** You would like to implement increased security instead of or in addition to the typical WPA or 802.11i standards
   - ❍ **D.** You are required to implement wireless using older equipment that does not support WPA or WPA2

4. You are sitting in a library and would like to share files with a coworker sitting across the table. To accomplish this, the coworker connects to a wireless SSID managed by your laptop. What type of network topology is this?

   - ❍ **A.** Unsecure
   - ❍ **B.** Ad hoc
   - ❍ **C.** Basic Service Set
   - ❍ **D.** Extended Service Set

5. You are using a Cisco 7921 wireless VoIP device. While speaking to your coworker on the phone, you are walking through multiple wireless cells. What type of network topology is this?

   - ❍ **A.** Unsecure
   - ❍ **B.** Ad hoc
   - ❍ **C.** Basic Service Set
   - ❍ **D.** Extended Service Set

6. Your organization uses a wireless security standard that requires people to authenticate to a back-end server with a valid active directory username and password before they are granted access to the wireless network. Upon successful authentication, the dynamic encryption keys are generated for use during the wireless session. What type of network security is in use?

   - ❍ **A.** WEP
   - ❍ **B.** WEP2
   - ❍ **C.** WPA
   - ❍ **D.** 802.11i
   - ❍ **E.** 802.1x (EAPOL)

7. Which of the following accurately describes the difference between WPA and WPA2?

   - ❍ **A.** WPA integrates with WEP encryption standards, whereas WPA2 is not backward-compatible.
   - ❍ **B.** WPA uses TKIP encryption, and WPA2 uses AES.
   - ❍ **C.** WPA uses preshared keys, and WPA2 allows for back-end user authentication.
   - ❍ **D.** WPA is used on 802.11a networks, whereas WPA2 is compatible with 802.11a/b/g networks.

8. You are troubleshooting a wireless laptop for a user in your organization. The wireless laptop cannot identify any available wireless SSIDs in the region. Your personal laptop can identify three SSIDs from the same location. The user has previously connected to the corporate network without issue. You have noticed increased interference from a neighboring company during different times of the day. What is the most likely cause of this issue?

   - ❍ **A.** The client wireless network card is disabled.
   - ❍ **B.** The RF interference has become too heavy for the client to view the available SSIDs.
   - ❍ **C.** The client wireless card is using the wrong frequency.
   - ❍ **D.** The signal is being absorbed before reaching the client laptop.

9. You suspect that one of your network users has violated the corporate security policy by plugging in a personal wireless access point in his cubicle. What Cisco security solution would allow you to detect this issue?

   - ❍ **A.** Cisco ACS Server
   - ❍ **B.** Cisco wireless IPS
   - ❍ **C.** Cisco wireless 802.1x
   - ❍ **D.** MAC address security

10. A network user has issued a trouble ticket stating that she is experiencing file transfers well below the 54Mbps speed that her wireless laptop claims to achieve. What are three valid reasons for this?

    - ❍ **A.** RF interference
    - ❍ **B.** CSMA/CA transmission method
    - ❍ **C.** Proximity to the access point
    - ❍ **D.** The duplex setting on the client's laptop
    - ❍ **E.** The client has not implemented 802.1x

Answers to Review Questions

1. The three encryption standards are WEP, WPA, and WPA2.
2. WEP uses the RC4 encryption algorithm. WPA uses the TKIP encryption method, which is more secure than WEP but not as secure as the WPA2 standard, which uses AES encryption. WEP does not have many strengths other than compatibility; all wireless devices can support the WEP standard. WPA has the strength of being interoperable with older WEP-compatible hardware, but it still has a few security weaknesses. WPA2 supports extremely strong encryption, but it is not backward-compatible with older wireless hardware.

3. Wireless networks are vulnerable to war driving, direct hacking, and employee ignorance.
4. Wireless access points should be deployed in a "tight configuration." This means that you should have many access points broadcasting smaller, more high-speed signals rather than a few access points broadcasting weaker signals that reach a larger radius.
5. First, ensure hardwire operation. Then, install the access point and test a basic network SSID with no security. Finally, add security and perform a final test.

Answers to Exam Questions

1. **A.** Rogue access points typically are brought in by internal corporate users with nonmalicious or malicious intent. Regardless of the intent, the rogue access point adds an enormous security liability to your network.
2. **C.** Wireless best practices recommend a 10 to 15% overlap of wireless cells. This allows for seamless roaming by wireless devices. Answer A is true only if the wireless access points are configured to use the same channel (frequency range). Because of this, you should never have adjacent access points using the same channel.
3. **D.** Both WEP (64-bit) and WEP2 (128-bit) encryption methods have been found to be insecure. The only time they should be used is in a network environment that uses older equipment and is unable to support the newer security standards.
4. **B.** Ad hoc networks are wireless networks generated from a participating device in the network, such as a laptop. These laptops can use many of the same security methods as BSS or ESS wireless topologies.
5. **D.** An Extended Service Set (ESS) wireless topology is the combination of two or more Basic Service Set (BSS) networks. This allows client roaming (between wireless cells) without service interruption.
6. **E.** 802.1x (less commonly known as Extensible Authentication Protocol over LAN [EAPOL]) adds a secure authentication system to a LAN environment. This technology can be used to secure both wired and wireless LAN connections. The other answers represent varying encryption standards.
7. **B.** WPA was released as an interim solution to improve the security of WEP. It uses an encryption method known as TKIP, which is more secure than WEP but not as secure as the WPA2 standard, which uses AES encryption.
8. **A.** The most likely cause of this issue is that the client wireless card is turned off. This happens frequently with laptops, because manufacturers commonly put a switch or button on the case of the laptop that easily turns the laptop on or off. The fact that it could not see any wireless networks while your personal laptop sat next to it reveals that wireless networks are reaching the location through the interference. The card cannot be the wrong frequency, because it previously connected to the corporate network without issue.

9. **B.** The Cisco wireless IPS system identifies rogue wireless access points added to the network. The 802.1x and the Cisco ACS Server are primarily responsible for user authentication and privileges. MAC address security can help disable a port with a rogue wireless access point, but it cannot detect the rogue's existence.

10. **A, B, C.** Wireless is susceptible to many types of RF interference. Likewise, the farther the client is from the access point, the lower her speed becomes. Finally, wireless uses a CSMA/CA transmission method, which causes the amount of bandwidth to diminish the more clients you add to the access point.

Suggested Readings and Resources

1. Wikipedia 802.11 definitions, http://en.wikipedia.org/wiki/802.11
2. How WiFi Works, http://computer.howstuffworks.com/wireless-network3.htm
3. Chris Ward and Jeremy Cioara. *CCNA Practice Questions*. Que Publishing, 2008.
4. Toby Velte and Anthony Velte. *Cisco 802.11 Wireless Networking Quick Reference*. Cisco Press, 2005.