CHAPTER 23

Exploring Wireless Networking

Wireless networks are very common today. They're easy to set up, and many home users, small offices, and home offices use them. You'll also see them in many medium-to-large organizations. As an A+ technician, you need to have a basic understanding of wireless components, wireless protocols, wireless security, and how to configure a wireless network. This chapter covers what you'll need for the A+ exams and on the job.

Exam 220-801 objectives in this chapter:

- 2.5 Compare and contrast wireless networking standards and encryption types.
  - Standards
    - 802.11 a/b/g/n
    - Speeds, distances and frequencies
  - Encryption types
    - WEP, WPA, WPA2, TKIP, AES
- 2.6 Install, configure, and deploy a SOHO wireless/wired router using appropriate settings.
  - MAC filtering
  - Channels (1 – 11)
  - SSID broadcast (on/off)
  - Wireless encryption
  - DHCP (on/off)
  - WPS (Wi-Fi Protected Setup)

Exam 220-802 objectives in this chapter:

- 2.5 Given a scenario, secure a SOHO wireless network.
  - Change default user-names and passwords
  - Changing SSID

    - Setting encryption
    - Disabling SSID broadcast
    - Enable MAC filtering
    - Antenna and access point placement
    - Radio power levels
    - Assign static IP addresses
- 4.5 Given a scenario, troubleshoot wired and wireless networks with appropriate tools.
    - Common symptoms
        - No connectivity
        - Intermittent connectivity
        - Slow transfer speeds
        - Low RF signal
    - Tools
        - Wireless locator

REAL WORLD **WIRELESS HOME NETWORKS AND PORTABLE HOT SPOTS**

When I'm teaching classes and wireless topics come up, I frequently ask how many people have wireless networks where they live. Years ago, only about 25 percent of the people in the class had one. Today, 90 percent or more of the students usually say that yes, they have wireless networks.

Additionally, in several classes I've taught, students have their own portable Wi-Fi hot spots. They set the hot spot up, and it provides them with Internet connectivity for their laptops and other wireless devices. I don't mean to imply that everyone has to have a wireless network. However, because they are so popular, any A+ technician certainly needs to understand them.

Wireless Components

Wireless local area networks (WLANs) have become quite popular. They're easy to set up, and they provide a great deal of flexibility to users. For example, a homeowner can set up a wireless network without running any cables. Other people in the home can access the network from just about any room, or even on the porch.

The tradeoff is that a WLAN isn't always as fast or reliable as a wired network. WLANs are susceptible to interference, which can slow down performance. Additionally, users that are farther away from the wireless network have slower speeds.

EXAM TIP

WLANS are flexible and easy to install. A wired network is often faster and more reliable, but it is more expensive.

WLANs have some basic components. It's important to understand what the components are before you can get a full idea of how they're configured on a network.

Wireless Access Point

A *wireless access point (WAP)* includes a transmitter and a receiver (called a *transceiver*) and acts as a bridge for wireless clients to a wired network. Organizations use WAPs to provide access to their network for wireless devices.

EXAM TIP

A wireless access point is often referred to simply as an *access point*. You might see this in documentation and on exam questions. That is, even if the word "wireless" is omitted from a question referring to an access point, a wireless network is implied.

Wireless Router

A *wireless router* is a WAP with extra capabilities. It's common to find wireless routers used in home networks and small office/home office (SOHO) networks. It bridges wireless clients to a wired network just as a WAP does, but it often does much more. Some of the extra capabilities of a wireless router include the following:

- **Wired connections.** Many wireless routers include both wired and wireless capabilities.
- **Internet connectivity.** The wireless router is connected to the Internet. Any user connected to the router can access Internet resources.
- **Switch component.** The router also acts as a switch to connect devices to each other. For example, users can share data with others using a homegroup on Windows 7 systems.
- **Dynamic Host Configuration Protocol (DHCP).** DHCP provides IP addresses and other settings for the clients. It's common to provide the IP address of a router as the default gateway for clients and the IP address of a Domain Name System (DNS) server to resolve host names to IP addresses.
- **Network Address Translation (NAT).** The router issues private IP addresses to internal clients with DHCP, but the Internet uses public IP addresses. NAT translates the private IP addresses to public and public back to private for the clients. NAT also provides a layer of protection by hiding internal addresses.

- **Firewall.** Many routers include basic firewalls. These allow you to create access control lists (ACLs) to allow or block certain types of traffic. Many routers also include port forwarding capabilities so that you can access internal clients from the Internet through the firewall.

Figure 23-1 shows a typical network configuration that uses a wireless router. Wired clients connect directly to the router by using cables, such as twisted-pair cable, and wireless clients connect using wireless network interface cards. The router provides a connection to the Internet through an Internet Service Provider (ISP) for all users.

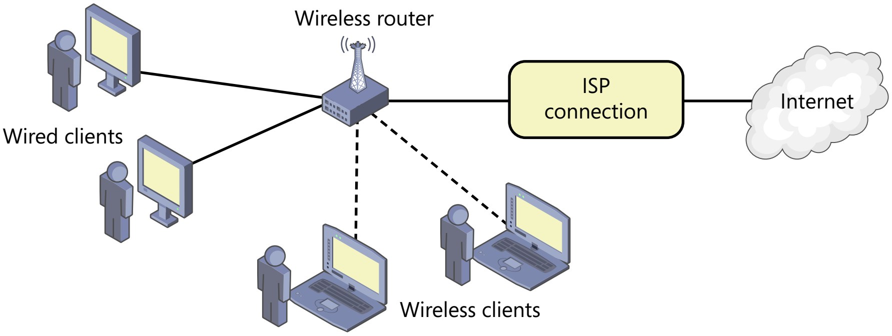


FIGURE 23-1 Wireless network.

The wired clients will have consistently high speed and reliability through the wireless router. In contrast, the wireless clients might have slower speeds or unreliable connections, depending on a variety of factors. For example, moving the wireless client farther away from the router will often degrade connection performance.

It's not apparent from Figure 23-1, but the clients can also communicate with each other through the wireless router. This is because wireless routers include a switch component.

NOTE **WIRELESS ISOLATION MODE AND HOTSPOTS**

To protect user privacy, many wireless hot spots prevent clients from communicating with each other. This is achieved by enabling wireless isolation mode on the wireless router.

Figure 23-2 shows a rear view of the same wireless router shown in Figure 23-1. The wired clients plug into the RJ-45 connections on the back of the router. Wireless clients connect using wireless transmissions. Figure 23-2 also shows the wide area network (WAN) connection found on many wireless routers. You connect the WAN port to the Internet.

The connection to the ISP can be different depending on how you connect to the Internet. For example, if you're using broadband cable, you need to install a modem between the wireless router and the ISP's connection. Some ISPs give users all-in-one devices that connect them to the ISP and also have wireless built right into them.

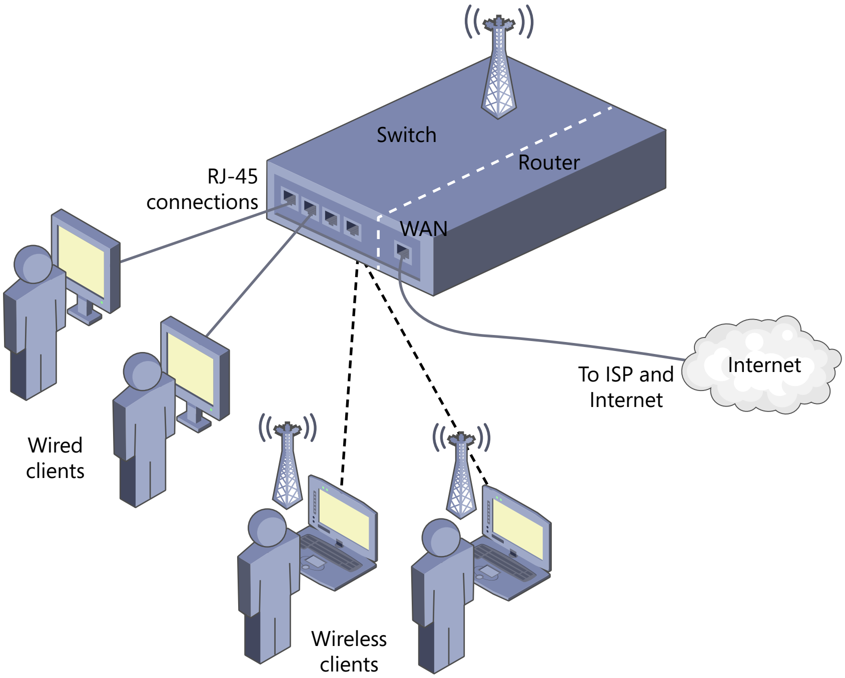


FIGURE 23-2 Wireless router showing switch and router components.

Wireless Device

Wireless devices are any devices that can connect to the network by using wireless technologies. In general, you can think of a wireless device as a laptop computer. However, there are more possibilities.

Many devices, such as wireless phones, tablets, and gaming systems, include wireless capabilities. For example, a Windows 7 Phone can connect to a cellular phone network for Internet access. However, when the phone is in range of a wireless network, you can configure it to connect to the Internet through the wireless network. It's often quicker and doesn't count against data limits for the phone.

You need to configure the wireless device by using the same configuration as the wireless router or WAP. This includes using the same wireless protocol and wireless security.

Infrastructure Mode vs. Ad-Hoc Mode

When you connect through a WAP or wireless router, as shown in Figure 23-1, you are using *infrastructure mode*. In contrast, an *ad-hoc* network is a wireless network without a WAP or router.

Ad-hoc is Latin for *as needed,* which is a good way of thinking about this. You create the network only when you need it. Imagine you and a friend both have wireless laptops and you want to connect the two computers together to share data or to play a game. One of you creates the ad-hoc network, and the other person joins the network. Similarly, if you have a wired Internet connection on one device, you can share it with someone else through an ad-hoc connection.

Wi-Fi and Wi-Fi Alliance

Wireless is often referred to as *Wi-Fi*, short for wireless fidelity. Generically, Wi-Fi is any WLAN based on one or more of the 802.11 standards.

Wi-Fi is also a trademark of the Wi-Fi Alliance. The Wi-Fi Alliance is a trade association that promotes standardization of wireless products and certifies wireless products.

✓ **Quick Check**

1. **What's a benefit of a wireless network over a wired network?**
2. **When you compare a WAP and a wireless router, which has more capabilities?**

Quick Check Answers

1. **Flexibility in user locations and a lower cost.**
2. **A wireless router includes a WAP and also has additional capabilities, such as routing, DHCP, NAT, and firewall capabilities.**

Wireless Standards

Common wireless networks use the *802.11* standards. When preparing for the A+ exam, it's important to know the wireless standards and some common characteristics. Three important characteristics of wireless standards are as follows:

- Maximum speed (data throughput)
- Frequency
- Range (distance)

Higher data throughputs result in faster downloads for the user. Wireless devices attempt to connect at the highest speed they can negotiate without errors. For example, if a wireless laptop is in the same room as a wireless router, it will probably connect at the highest speed possible. However, another laptop on a different floor or separated by walls will connect at a slower speed. Interference also results in slower connections.

Each device within the wireless network must use the same frequency range. The two frequency ranges used with 802.11 wireless networks are 2.4 GHz and 5.0 GHz.

Range refers to how far the wireless signal can travel. You'll find a wide assortment of distances quoted for the different wireless protocols. For example, some people say that 802.11a has a range of 150 feet and that 802.11g has a range of 300 feet. Others say that the ranges are 115 and 125 feet, respectively.

You can often modify the range by increasing the strength of the signal, modifying the position of the antenna, and eliminating interference in the environment. It isn't critical to know the exact range of any of the protocols, but you should know their ranges compared to each other.

NOTE **DIRECTIONAL ANTENNAS EXTEND RANGE**

You can also extend the range of a wireless network with a directional antenna. Most devices use omni antennas, which transmit and receive in all directions. A directional antenna transmits and receives in a single direction and has a much greater range. Attackers can use a cantenna (a simple can attached to a wire) as a directional antenna; they can use it to connect to wireless networks from far away.

Table 23-1 shows the maximum speed and frequency used by the common wireless protocols, and the approximate indoor distances. Notice that 802.11n has the highest speeds and the highest range. These two characteristics are primary reasons why 802.11n is becoming so popular today.

TABLE 23-1 802.11 Characteristics

Protocol	Maximum Speed	Frequency	Indoor Distances
802.11a	54 Mbps	5.0 GHz	Lowest range ~30 m (100 feet)
802.11b	11 Mbps	2.4 GHz	Medium range ~35 m (115 feet)
802.11g	54 Mbps	2.4 GHz	Medium range ~38 m (125 feet)
802.11n	600 Mbps 300 Mbps common	2.4 & 5.0 GHz	Highest range ~70 m (230 feet)

Many wireless devices support multiple protocols. For example, you can purchase an 802.11n wireless router and it will work with devices using 802.11a, b, and g. Today, most devices are either 802.11g or 802.11n, but you might run across some older devices using 802.11a or 802.11b.

802.11n uses *multiple-input multiple-output (MIMO)* technologies with multiple antennas. Instead of having a single powerful antenna to transmit and receive, MIMO devices use multiple antennas to transmit and receive data. It's common to see MIMO devices that support 300-Mbps speeds, but the speeds can be as high as 600 Mbps.

EXAM TIP

Know the maximum data throughput and frequencies used by each of the wireless protocols listed in Table 23-1. IEE 802.11n is the newest, and it uses MIMO to achieve higher throughputs.

Antenna and Access Point Placement

Wireless devices use antennas to transmit and receive data, and how you position the antennas and access points affects these transmissions. First, it's important to realize that most antennas are omni-directional. That is, they transmit or receive in all directions.

If you live in a single empty room, you would place the WAP in the middle to give you the best performance throughout the room. Of course, it's highly unlikely that you live in a single empty room. Instead, you probably live in a multiple-room residence, which might even have more than one floor. Any physical objects such as walls, floors, ceilings, and furniture can absorb the signal.

Wireless networks are also susceptible to interference from a wide variety of sources. Electromagnetic interference (EMI) can come from equipment such as magnets and even fluorescent lights. Radio frequency interference (RFI) can come from other transmitters. Many cordless phones, baby monitors, and microwaves transmit on the same frequency that wireless devices use, and they can interfere with the signal. It's best to place the WAP at least three feet away from any of these devices.

Placing the antenna vertically or horizontally also affects the transmission. Point your finger to the sky as if it were a vertically placed antenna. Positioned this way, an antenna transmits the strongest outwards from you, but not as strongly up and down. This is good for a one-floor residence. If you change the position so that it is horizontal, the signal is strongest above and below. This works well for a multi-floor residence.

With all that in mind, where should you place the WAP? It often takes a little trial and error if you want the signal to reach multiple locations. You can set up the WAP and then use a wireless device to check the signal strength. For example, you can configure the WAP and then use the signal strength meter in Windows to see the signal strength as someone else moves the WAP or the antenna.

The steps in the Configuring Wireless Settings on Windows 7 later in this chapter show how you can access the wireless signal strength meter and include a graphic of the meter.

Channels

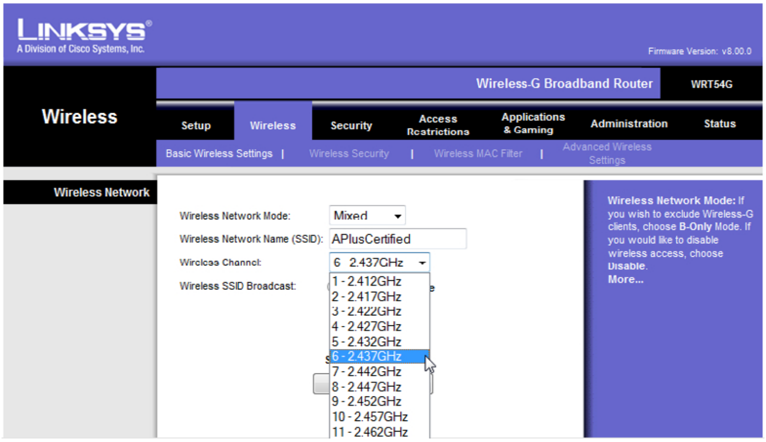
802.11 protocols use frequency bands beginning with 2.4 GHz or 5.0 GHz. However, these are starting frequencies, and each frequency includes multiple channels.

You normally don't have to change the channels. However, if you are experiencing excessive interference on one channel, you can switch to a different channel with less interference.

EXAM TIP

The stated frequency of wireless protocols identifies the beginning frequency, but each protocol includes multiple channels in the frequency range. You can change channels if there is excessive interference in a channel.

Figure 23-3 shows the options for changing the channel on a wireless router. This router chose channel 6 by default, which is common, but any of the channels can be selected.



Wireless Network Mode: Mixed

Wireless Network Name (SSID): APlusCertified

Wireless Channel: 6 2.437GHz

Wireless SSID Broadcast:

Wireless Network Mode: If you wish to exclude Wireless-G clients, choose **B-Only** Mode. If you would like to disable wireless access, choose **Disable**.
More...

FIGURE 23-3 Changing the channel on a wireless router.

These channels work similarly to how a radio channel works. When you tune to a radio station's center frequency, you get the best reception, but you can often still hear a station if you tune it to a close frequency. Of course, radio stations are aware of this, and you'll rarely have two radio stations right next to each other, interfering with each other's broadcast. This isn't the case with the wireless channels.

The wireless channel frequencies shown in Figure 23-3 are the center frequency for each channel, and each channel is 22 MHz wide. Therefore, channel 6 is actually 2.426 GHz to 2.448 GHz, with a center frequency of 2.437 GHz. Figure 23-4 shows how the 22-MHz channels overlap with each other. Only channels 1, 6, and 11 are marked and highlighted. You can see that these channels do not overlap with each other.

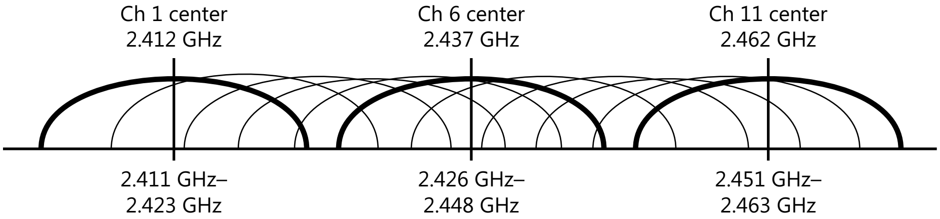


FIGURE 23-4 Wireless channels.

It's common for devices to default to channel 6. If you have multiple wireless devices in the same area, they might all be broadcasting on channel 6 and interfering with each other. They still work, but the interference forces them to retransmit traffic and can reduce performance. With that in mind, you can often improve wireless performance by changing to channel 1 or channel 11.

Many wireless devices will automatically scan the channels for wireless networks. That is, if you change the channel on a WAP or a wireless router, you usually don't have to change the channel on the wireless devices. For example, Windows 7 doesn't require you to manipulate the channel even if you've changed the channel on a wireless router.

EXAM TIP

If there are any other wireless networks near you, you can often improve the performance of your network by changing the channel. Channels 1, 6, and 11 are recommended for use because they do not overlap with each other. If other networks are using channel 6, you can change yours to 1 or 11 and avoid interference from the other networks.

Radio Power Levels

Many WAPs also include settings to adjust the radio power levels. All the devices transmit and receive radio frequency (RF) signals over the air to communicate. If you turn up the radio power of the WAP, you can increase the distance of the transmission.

Alternatively, if you don't want people outside the home or office to receive the signal, you can turn down the radio power levels. This limits the distance the signal travels, but it isn't a reliable security measure. A dedicated attacker can use a directional antenna to access the network.

NOTE **LOWER POWER LEVELS EQUAL SLOW CONNECTIONS**

Lowering the power level can affect users within your WLAN. Wireless devices connect to the WAP by using the fastest speed they can achieve without errors, and if the RF level is too low, it can result in intermittent connectivity or slow transfer speeds.

✔ Quick Check

1. What is the maximum speed of 802.11g?
2. What wireless protocol provides the greatest speed and range?

Quick Check Answers

1. 54 Mbps.
2. 802.11n.

Wireless Security

One of the most important concerns with wireless networks is security. Because data is transmitted over the air by using frequencies anyone can learn, the transmissions need to be protected. One of the most important security protections you can use is to configure the wireless network with a secure security protocol. Several wireless security measures are discussed in the following sections.

Encryption Types

Encryption scrambles data so that it can't be read or interpreted by unauthorized individuals. Encryption codes have been around since at least the time of Julius Caesar and the Roman Empire, but they are much better today than they were back then.

Wireless includes three security protocols, and they use different encryption types. The three available security protocols are as follows:

- **Wired Equivalent Privacy (WEP).** *WEP* is an older security protocol. It has been cracked and should not be used.
- **Wi-Fi Protected Access (WPA).** *WPA* was introduced as a short term replacement for WEP. It provided significant improvements over WEP and used existing hardware. Sometimes you have to upgrade the firmware on wireless devices to use WPA. When required, wireless device vendors usually provide free downloads that you can use to upgrade the device's capabilities and use WPA.
- **Wi-Fi Protected Access version 2 (WPA2).** *WPA2* is a permanent replacement for WEP and WPA. It requires more advanced hardware, but almost all hardware sold today supports WPA2.

EXAM TIP

WPA2 is the most secure wireless security protocol. If your wireless device shows support only for WEP, you can often upgrade the hardware's firmware to get support for WPA or WPA2. This is similar to upgrading the BIOS for a computer, but you're instead upgrading the firmware on a network interface card or wireless router.

The two encryption types used with wireless security protocols are as follows:

- **Temporal Key Integrity Protocol (TKIP).** WPA uses *TKIP*. It was designed so that WPA would be more secure than WEP while allowing users to use the same hardware. Even though legacy hardware supports TKIP, it sometimes requires a firmware upgrade for it to work.
- **Advanced Encryption Standard (AES).** WPA2 uses *AES*. It provides a stronger security combination than either WEP or WPA with TKIP. Beyond wireless, AES is used worldwide as an encryption standard in many different applications.

Table 23-2 summarizes the three wireless security protocols.

TABLE 23-2 Wireless Security Algorithms

Protocol	Strength	Comments
WEP	Weak	Don't use.
WPA	Stronger than WEP	Use only if hardware doesn't support WPA2. Might need to upgrade firmware. Uses TKIP.
WPA2	Strongest	Recommended for use today. Uses AES.

WPA and WPA2 also support Personal mode and Enterprise mode. Personal mode is simple to set up and used in most home networks and SOHOs. Enterprise Mode is used in larger organizations.

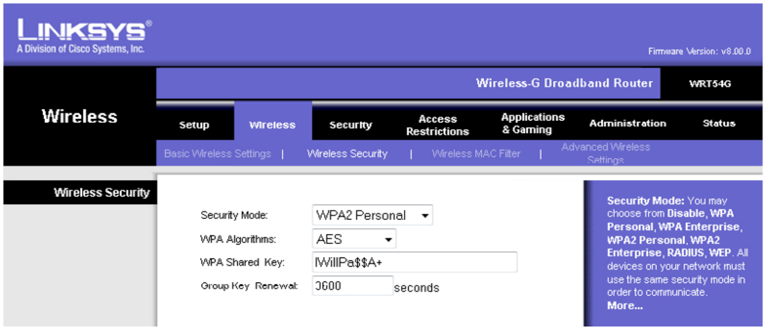
Wardriving

Wardriving is the practice of driving around looking for wireless networks. Attackers often use wardriving to discover wireless networks that are not secured or that are secured using easily beatable security such as WEP. When they discover a wireless network, they probe it to determine how far they can get in.

In some cases, attackers can access computers and resources in the wireless network. If the administrator password has not been changed on the wireless router, they can manipulate the settings and actually lock out the owner.

Personal Mode

Personal mode uses a preshared key or passphrase. Every wireless device must have the same passphrase as the wireless router. Figure 23-5 shows a setup page for a Linksys wireless router with the security mode set to WPA2 Personal and the shared key as IWillPa$$A+.


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v8.00.0
Wireless-G Droadband Router
WRT54G
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security

Security Mode: WPA2 Personal

WPA Algorithms: AES

WPA Shared Key: IWillPa$$A+

Group Key Renewal: 3600 seconds

Security Mode: You may choose from **Disable, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, WEP**. All devices on your network must use the same security mode in order to communicate. **More...**

FIGURE 23-5 Wireless network.

The security mode is sometimes identified as security type, and the shared key is sometimes called a passphrase, network security key, or something similar. The important point to remember is that every wireless device must be configured with the same settings. In Figure 23-5, every device must be using WPA2 Personal with a key of IWillPa$$A+.

NOTE **PASSPHRASE**

The passphrase or shared key should be strong so that it can't be easily guessed. Strong passphrases include a mixture of uppercase and lowercase letters, numbers, and symbols, and are at least eight characters long.

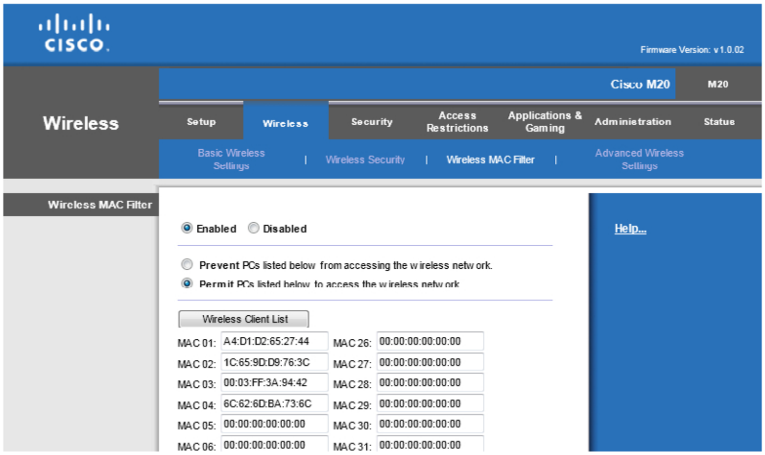
Enterprise Mode

Larger organizations sometimes use Enterprise mode. Enterprise Mode uses a Remote Authentication Dial-in User Service (RADIUS) server to authenticate clients. Users need a user name and password to access the wireless network.

MAC Filtering

Another security feature you can use is media access control (MAC) filtering. Each network interface card (NIC) has a theoretically unique MAC address assigned to it, and you can restrict access to a wireless network based on this address. I say theoretically unique because you are unlikely to see any two NICs with the same MAC address in the same network. However, manufacturers have a finite number of addresses and sometimes have to reuse them.

Figure 23-6 shows the Wireless MAC Filter page for a wireless router. As configured, it will allow only computers with the MAC address listed in MAC01 through MAC04 to connect. If a computer with a different MAC address tries to connect, the connection is blocked.



● Enabled ○ Disabled

○ Prevent PCs listed below from accessing the wireless network.
● Permit PCs listed below to access the wireless network

MAC 01:	A4:D1:D2:65:27:44	MAC 26:	00:00:00:00:00:00
MAC 02:	1C:65:9D:D9:76:3C	MAC 27:	00:00:00:00:00:00
MAC 03:	00:03:FF:3A:94:42	MAC 28:	00:00:00:00:00:00
MAC 04:	6C:62:6D:BA:73:6C	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00

FIGURE 23-6 Filtering systems based on the MAC address.

EXAM TIP

MAC filtering is one of the methods you can use to restrict access to a wireless network. Computers that don't have matching MAC addresses cannot connect unless they know how to change their computer's MAC address.

On the surface, this might seem secure. After all, there are billions of MAC addresses and the possibility of someone guessing one of these is astronomically low. However, attackers can learn the MAC addresses that you're allowing and change their system to use the same MAC address.

It's relatively easy to change the MAC address for any NIC to match the MAC address of another NIC. Chapter 19, "Exploring Cables and Connectivity," includes steps to manipulate the duplex settings for a NIC and points out the setting for the MAC address.

In summary, you can use MAC filtering to restrict access, but be aware that a knowledgeable attacker can beat it. Additionally, if you have many computers on your wireless LAN, it might become an administrative burden to keep track of MAC addresses.

Wi-Fi Protected Setup

One of the challenges with wireless is that it can be complex to set up and create a secure environment. *Wi-Fi Protected Setup (WPS)* was developed by the Wi-Fi Alliance to make it easier for users to set up a secure wireless network. Two common WPS methods are as follows:

- **Push button.** Users press a button on the WAP and press a software button on the wireless device. The two devices communicate with each other and set up a secure connection. A complex preshared key is still used, but the user doesn't need to enter it.
- **PIN.** A PIN is assigned to a WAP and/or a wireless device. Users need to enter only the PIN of the other device to create a connection. For example, if the WAP has a PIN of 12345678, the user enters this PIN by using software on a laptop computer or other wireless device to make the connection. Just as with the push button method, a complex preshared key is still used for WPA2, but the user doesn't need to enter it.

While this sounds like it's a great resource to make the setup easier, it has a significant flaw. An open source software tool named Reaver that allows an attacker to easily discover the WPS PIN has been publicly available since early 2012. With the PIN, the attacker can discover the WPA or WPA2 passphrase and access the network. The only way to prevent this attack is to disable WPS on the WAP.

In the real world, it's highly recommended that you disable WPS to eliminate the risk. However, CompTIA objectives were created before this was widely known. At that point, WPS was recognized as a great feature that makes it easy for users to set up a secure wireless network.

EXAM TIP

Security experts recommend disabling WPS to eliminate risks. However, don't be surprised if you see a question that asks about the easiest way to set up security on a wireless network and WPS is the only logical answer.

Quick Check

1. What security protocol is not secure and should not be used?
2. What security protocol is the most secure?
3. What can you enable to restrict which devices can connect?

Quick Check Answers

1. WEP.
2. WPA2.
3. MAC filtering.

SSID

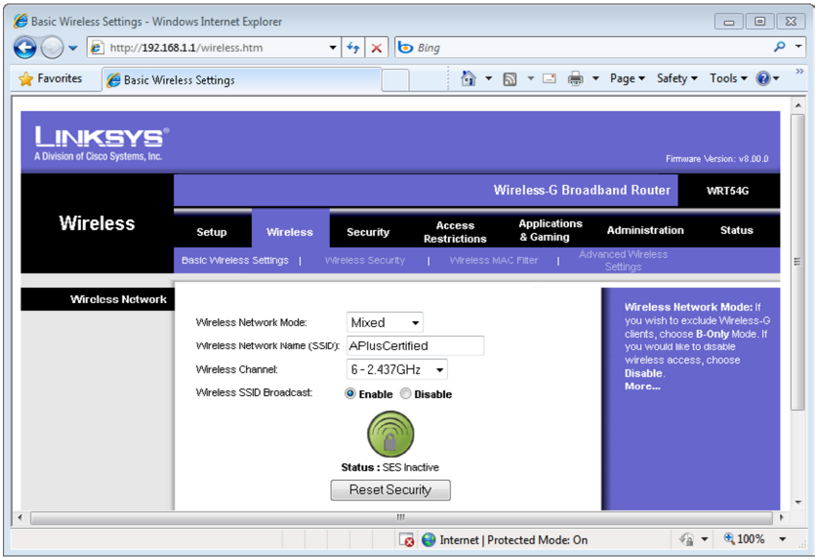
Wireless networks are identified by the *service set identifier (SSID)*. The SSID is also known as the name of the wireless network. Many wireless routers have default SSIDs, such as Linksys or belkin54g, but some require you to give them a name when you're setting them up. All of them allow you to change the SSID, and an SSID can be up to 32 characters long.

Figure 23-7 shows a setup page for a Linksys wireless router. You can see that the Wireless Network Name (SSID) is identified as APlusCertified and that the SSID broadcast is set to Enable.

NOTE **SSIDS ARE CASE-SENSITIVE**

Because SSIDs are case-sensitive, an SSID of APlusCertified is not the same as apluscertified. If you don't enter the SSID exactly, it won't be recognized.

This device supports both 802.11b and 802.11g devices by selecting Mixed as the Wireless Network Mode. It also allows you to select a different wireless channel. In Figure 23-7, it's using channel 6 of the 2.4-GHz frequency range. If you're experiencing interference on a channel, you can change it to get better performance, as mentioned in the Channels section earlier in the chapter.



Wireless Network Mode: Mixed

Wireless Network Name (SSID): APlusCertified

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ● Enable ○ Disable

Status : SES Inactive

Wireless Network Mode: If you wish to exclude Wireless-G clients, choose **B-Only** Mode. If you would like to disable wireless access, choose **Disable**. **More...**

FIGURE 23-7 Linksys wireless router setup page.

Understanding SSID Broadcast

When SSID broadcast is enabled, the wireless router periodically sends out special packets that announce its presence. These broadcasts allow other wireless devices to easily see it and connect.

If you have a laptop, you might see other wireless networks from your neighbors. The SSID broadcast provides this information to advertise the wireless network.

Enabling or Disabling SSID Broadcast

As a general rule, it's recommended that SSID broadcast be enabled. That's not a typo. Wireless protocols are designed to work with WAPs and wireless routers advertising their presence with SSID broadcast enabled.

However, you might run across documentation indicating that SSID broadcast should be disabled to hide a wireless network. Other documentation indicates that disabling it provides no security. So, what's true?

The short answer is that disabling SSID broadcast doesn't provide any security. It does hide the network from some wireless devices. However, this reduces usability because it makes it difficult for some devices to connect. It does not hide the network from a knowledgeable attacker.

NOTE **HIDING A WIRELESS NETWORK**

There are cases where hiding the network by disabling the SSID broadcast makes sense. For example, if a company creates a WLAN for specific visitors, it might be appropriate to disable SSID broadcast. This hides it from most users so that they won't be distracted by it or try to connect to the visitors network. Only the visitors are given the SSID.

Many packets in standard wireless transmissions include the SSID, even if SSID broadcast is disabled. Free applications are available that anyone can install on a wireless-enabled laptop computer to capture these wireless transmissions. With just a few clicks, anyone can identify the SSID even if SSID broadcast is disabled. Therefore, disabling the SSID doesn't protect it from an attacker.

Some people might tell you that the SSID is the password, but this is not true. WEP, WPA, and WPA2 all support a passphrase. This is sometimes called a network security key or a shared key. However, this passphrase or key is different from the SSID.

However, CompTIA test writers don't necessarily understand that disabling the SSID doesn't provide security, or they might simply disagree with it. You might run across a test question that asks about hiding the wireless network. Disabling the SSID broadcast might be the best answer for the exam. However, it's important to remember that disabling the SSID doesn't provide any security.

EXAM TIP

The best way to protect a wireless network is by using a strong security protocol such as WPA2 and a strong passphrase that can't be easily guessed. You can hide a wireless network from some wireless devices by disabling the SSID, but this doesn't provide any security.

Renaming the SSID

From a security perspective, you should rename the SSID from the default. This reduces the amount of information available to anyone that can see your network.

For example, imagine that the default SSID for your wireless router is LinksysWRT54G. If you didn't change this, anyone that saw it would know you have a Linksys router with the model of WRT54G. They could download the manual from the Internet, and they might find a vulnerability. Then again, if you renamed the SSID to MyWiFi and someone saw it, they wouldn't have any information based on the name.

EXAM TIP

If the wireless router or WAP has a default SSID, you should rename the SSID after changing the administrator password.

✓ **Quick Check**

1. What is another name for the SSID?
2. What should you do with the SSID to provide security?

Quick Check Answers

1. Wireless network name.
2. Change the name. Disabling the SSID broadcast hides the wireless network from some network devices but does not provide security.

Configuring Wireless Network

When you you're configuring a wireless network, the first step is to install and configure the WAP or wireless router. Most wireless devices provide a web-based interface, and you can use this to configure the settings. Additionally, most have default settings so that you can easily log in, but these defaults need to be changed.

From a macro perspective, here are the steps you'll follow to set up a network with a wireless router:

1. Turn on the wireless router.
2. Connect your computer to the wireless router.
3. Start a web browser and log on to the administration page.
4. Change the administrator password.
5. Configure the wireless protocol, the SSID, and the wireless security on the wireless router.
6. Configure wireless clients with a compatible wireless protocol, the SSID, and the same wireless security.

Changing Default User Names and Passwords

Table 23-3 shows some common administrator names, passwords, and IP addresses for many wireless routers. Anyone that has this book knows these defaults, and it's also easy to do a quick search on the Internet to discover them. With this in mind, it's important to change the default password and, if possible, change the default user names.

TABLE 23-3 Access Information for Wireless Routers

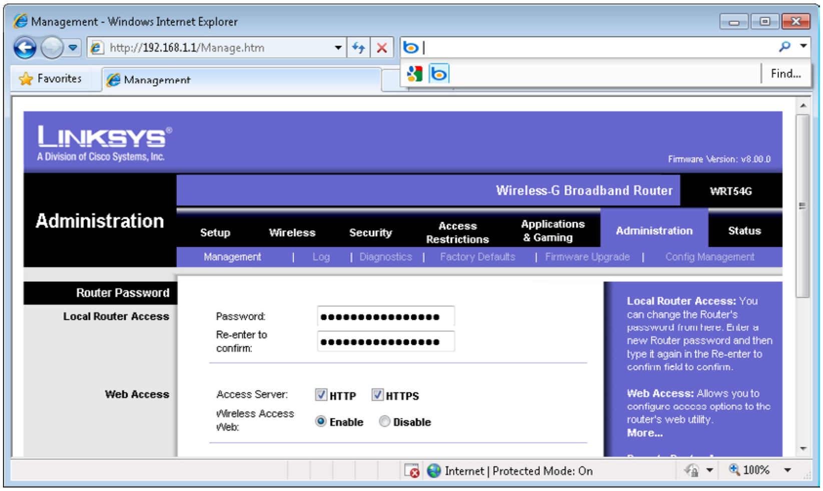
Vendor	Administrator name	Password	Starting IP
Belkin	Admin (or blank)	admin (or blank)	192.168.1.1
Dlink	Admin (or blank)	admin (or blank)	192.168.0.1
Linksys	Admin (or blank)	admin	192.168.1.1
Netgear	Admin	password	192.168.0.1

Wireless routers have an instruction manual or setup guide you can use. In short, you can either plug your computer directly into one of the RJ-45 connectors or use the wireless connection and connect using the defaults. After you're connected, you can open a web browser to access the administration page.

You enter the starting IP into the web browser to connect. This displays the administration page for the wireless router and prompts you to log in. Enter the default administrator name and password used for your router.

One of the first things you should do is change the default password for the administrator account. If you don't, an attacker or a practical joker can log in and start changing your settings. Some wireless routers include a reboot capability. If a malicious user can log in, they can interrupt connectivity by repeatedly rebooting it.

Figure 23-8 shows the page used to change the password on a Linksys router. I was able to access this page by clicking on the Administration menu item after logging in. Note that this is different from the security key or passphrase used for wireless security. Figure 23-5 showed the security key setting for this network.


Management - Windows Internet Explorer
http://192.168.1.1/Manage.htm
Favorites
Management
Find...
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v8.00.0
Wireless-G Broadband Router
WRT54G
Administration
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management
Router Password
Local Router Access
Web Access
Internet | Protected Mode: On
100%

Password: ●●●●●●●●●●●●●●●●

Re-enter to confirm: ●●●●●●●●●●●●●●●●

Access Server: ☑ HTTP ☑ HTTPS

Wireless Access Web: ● Enable ○ Disable

Local Router Access: You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

Web Access: Allows you to configure access options to the router's web utility.
More...

FIGURE 23-8 Changing the default password for the administrator account.

EXAM TIP

After configuring the wireless network, it's important to change the administrator password from the default. Otherwise, anyone that knows the default login information can log in to your wireless network and reconfigure it.

Next, you'd configure the wireless security with the passphrase. As mentioned in the Wireless Security section, WPA2 provides the best security, so it should be selected whenever possible. Additionally, you should use a strong passphrase or security key.

After you've configured security on the wireless router, you can configure the same security on any wireless network device.

Configuring Wireless Settings on Windows 7

Wireless devices have configuration menus that you can use to configure the wireless connection. The three primary pieces of information you need are as follows:

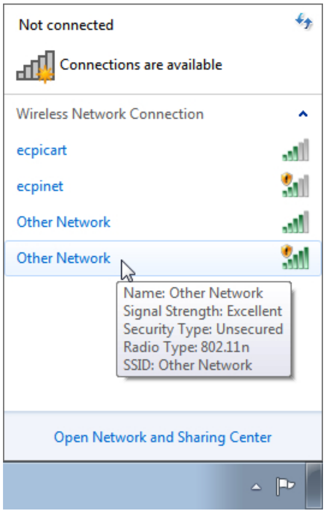
- SSID
- Security (such as WPA or WPA2)
- Passphrase or preshared key

EXAM TIP

If SSID broadcasting is enabled, you often don't need to enter the SSID or the security type. Instead, these will be automatically selected when you try to connect. However, the passphrase won't be available automatically. If you enter the incorrect passphrase on a wireless device, it won't be able to connect, so this is one of the things you should double-check if you're unable to connect after configuring the device.

You can use the following steps to configure wireless settings on a Windows 7–based computer:

1. Click Start, Connect To. You'll see a display similar to the following graphic on the far right of the taskbar. In the display, I'm hovering my mouse over one of the networks, and it shows details about the network.



Not connected

Connections are available

Wireless Network Connection

ecpicart

ecpinet

Other Network

Other Network

Name: Other Network
Signal Strength: Excellent
Security Type: Unsecured
Radio Type: 802.11n
SSID: Other Network

NOTE **WIRELESS MIGHT NEED TO BE ENABLED**

If your system does not have wireless capabilities, you will not see the Connect To choice. If Connect To is not available, double-check to ensure that a wireless NIC is installed and enabled. Laptops commonly have a button or switch for wireless access that needs to be enabled.

2. Click the wireless network that you want to connect to, and click Connect.
3. If the network is not using security, you'll be connected automatically. If the network is secured, you'll be prompted to type in the network security key. Type it in and click OK.

IMPORTANT **ENSURE FIREWALL IS ENABLED**

If you are connecting to a wireless network that is not using security, you should ensure that your firewall is enabled and blocking all incoming connections. For example, on Windows 7, click Start, type in **Windows Firewall**, and select Windows Firewall within the Control Panel. Ensure that it's set to Public networks so that it blocks incoming connections.

You can also create a wireless connection manually. This is useful if you're not near the wireless network or the network is not broadcasting its SSID.

1. Click Start, Connect To. Click Open Network And Sharing Center.
2. Select Manage Wireless Networks from the menu on the left. If your system does not have wireless capabilities, you will not see the Manage Wireless Networks option.
3. Click Add.

4. Select Manually Create A Network Profile.

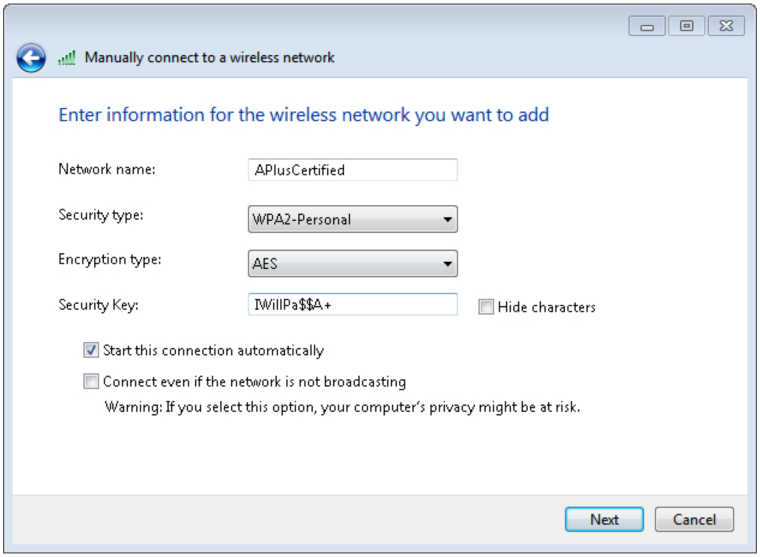
5. Enter the following information using the same information as you have on your wireless router or WAP:

   A. Enter the SSID as the Network Name.

   B. Select the Security Type used by the wireless network.

   C. Ensure the encryption type matches the wireless network.

   D. Enter the passphrase used on the wireless network as the Security Key. Your display will look similar to the following graphic.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: APlusCertified

Security type: WPA2-Personal

Encryption type: AES

Security Key: IWillPa$$A+ □ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

NOTE **COMPARE PRECEDING GRAPHIC TO OTHER FIGURES**

The network joined in the graphic is the same network shown earlier. Figure 23-5 shows the wireless router configured using the Security Mode of WPA2 Personal, and the WPA Shared Key is IWillPa$$A+. Figure 23-7 shows the wireless router with an SSID of APlusCertified, and Wireless SSID Broadcast is set to Enable. The preceding graphic shows the settings on the Windows 7 system.

Configuring DHCP

Most wireless routers include DHCP for ease of use. After a wireless device connects, the wireless router gives it an IP address and other IP information such as the default gateway address and DNS. For most wireless devices, this is enabled automatically so that you don't need to configure anything.

The wireless router will issue clients with the following information:

- **IP address and subnet mask.** This will be on the same subnet as the router. If the router has an IP of 192.168.1.1 with a subnet mask of 255.255.255.0, all addresses it issues will start with 192.168.1 and use a subnet mask of 255.255.255.0.
- **Default gateway.** This is the address of the router and provides a path to the Internet. It is commonly 192.168.1.1, but it can be different.
- **DNS.** The router will typically receive one or more addresses of DNS servers from the ISP. It gives this information to the DHCP clients.

If you are using a WAP or a wireless router on an internal network, you might not want to use DHCP from the wireless device. It could be that your network has another DHCP server. Or you might want to manually assign the IP information.

If you decide to disable DHCP and you are manually assigning information, you need to ensure that each wireless device has a static IP on the same subnet. For example, if the router uses 192.168.1.1 with a subnet mask of 255.255.255.0 as its address, all other devices need to have an address in the range of 192.168.1.2 through 192.168.1.254, with the same subnet mask of 255.255.255.0. If you use different settings on any computer, it won't be able to communicate with other devices on the network.

EXAM TIP

If you disable DHCP on the router but don't have another DHCP server and do not manually assign an IP address, many computers will assign an Automatic Private IP Address (APIPA). APIPA addresses start with 169.254. If you see an address like 169.154.4.5, it's an APIPA address. This indicates that the client is configured to use DHCP but could not reach a DHCP server.

Troubleshooting Wireless Connections

When troubleshooting wireless connections, the first thing to check is whether you have the wireless connection configured correctly. This includes double-checking the following configurations:

- **SSID.** Remember, the SSID is case-sensitive.
- **Security type such as WPA or WPA2.** For example, if the WAP is using WPA2, all devices must use WPA2.
- **Passphrase or security key.** These are also case-sensitive.

Typo mistakes in any of these are easy to make, and typos will stop you from connecting.

Another common check is to verify that the wireless connection is available and enabled. Many laptops have switches that enable and disable wireless. If this switch is turned off, wireless connectivity won't work.

For example, I have an HP laptop that has a touchpad above the keyboard. I can turn sound on or off and modify the volume with a touch. It has touch areas to pause, play, fast forward, and fast reverse CDs and DVDs. On the far right is an area that I can use to enable or disable wireless capabilities simply by touching it (even if I didn't mean to touch it). Users sometimes disable wireless capabilities on a computer without realizing it, so this is an important check.

EXAM TIP

If your computer has wireless capabilities but wireless is not working, check to ensure that wireless capabilities have not been disabled on the computer.

Common Symptoms

Some of the common symptoms of wireless connection problems and their likely solutions are the following:

- **No connectivity when initially setting up device.** If you can't connect at all, the best thing to do is check the basics, such as the SSID, security type, and passphrase as mentioned previously. Check to see whether other wireless devices are working, and if so, you know that the WAP is working. You can also check the device to ensure that wireless is enabled.
- **No connectivity for a device that was connected.** If a wireless device previously worked but is not working now, it could be the WAP or the device. To verify that it is working, check to see whether other wireless devices can connect to the WAP. If the WAP is working, you can usually just reset the wireless connection. For example, restarting a Windows-based system solves many ills and will reset the connection.

MORE INFO **CHAPTER 24, "CONNECTING AND TROUBLESHOOTING A NETWORK"**

You can also try running Windows Network Diagnostics on the NIC. Chapter 24 includes the steps you can use to do this for both wired and wireless NICs in the Troubleshooting Network Problems section.

- **Intermittent connectivity.** Occasionally, problems can cause a device to periodically disconnect from the WAP. The user will likely complain about being disconnected from the Internet. You might need to modify the antenna and access point placement as mentioned earlier in this chapter. The problem can also be due to interference from other wireless networks, so changing the channel might help. Last, you might want to check the radio power level on the WAP and consider increasing it.
- **Slow transfer speeds.** Devices and WAPs connect using the fastest speed they can achieve without errors. If there is interference from any source, devices and WAPs will use slower speeds. Check the same items you would check for an intermittent connection.

- **Low RF signal.** As mentioned previously, many WAPs allow you to adjust the RF power level. You can lower it so that it is harder for people outside your home or office to connect. Of course, if you lower it too much, people within your wireless network might have problems. The solution is simple: turn the power level back up on the WAP. If that doesn't resolve the problem, reposition the WAP and antenna.

NOTE **WIRELESS REPEATERS**

Some large organizations use wireless repeaters. They extend the range of a wireless network so that the same network can reach a farther distance. If the RF signal is low but you can't reposition the WAP, a wireless repeater can help.

Wireless Locator

A wireless locator is a portable device with a directional antenna that you can hook up to a laptop computer. The primary legitimate purpose is to locate rogue WAPs. For example, an attacker can hook up a WAP to a network and transmit the information wirelessly to capture it. A technician using the wireless locator will be able to detect this rogue WAP and pinpoint its location.

War drivers also use wireless locators. They can use the directional antenna and connect into networks even if they are well beyond the traditional broadcast range of the WAP.

Quick Check

1. **What is the first security change you should make when configuring a wireless router?**
2. **What three items are needed to configure a wireless device?**

Quick Check Answers

1. **Change the default administrator password.**
2. **SSID, security type, and passphrase or preshared key.**

Chapter Summary

- A wireless access point (WAP or access point) bridges wireless clients to a wired network.
- Wireless routers include a WAP and have additional capabilities. It's common for a wireless router to include DHCP, NAT, and a firewall.
- Infrastructure mode uses a WAP or a wireless router to connect devices. In ad-hoc mode, wireless devices connect without a WAP or wireless router.

- 802.11a uses 5 GHz and has a maximum speed of 54 Mbps.
- 802.11b uses 2.4 GHz and has a maximum speed of 11 Mbps.
- 802.11g uses 2.4 GHz and has a maximum speed of 54 Mbps.
- 802.11n uses 2.4 and 5 GHz and has a maximum speed of 600 Mbps. 802.11n uses MIMO for increased speed.
- The distance wireless signals travel is affected by many factors. You can adjust the antenna and access point placement, use a different channel, or adjust power levels to improve the reception. Devices typically use channel 6 by default, so you can select channel 1 or channel 11 to avoid interference from other networks using channel 6.
- WEP is an older security protocol and should not be used.
- WPA2 is the strongest security protocol and recommended for use today. WPA is better than WEP and should be used if hardware doesn't support WPA2.
- You can sometimes upgrade the firmware of wireless devices to support WPA or WPA2.
- Personal Mode uses a shared key or passphrase. Anyone with the key can access the WLAN.
- Enterprise mode uses an authentication server, and each user must have an account to access the WLAN.
- Wi-Fi Protected Setup (WPS) allows users to configure security for a wireless network by pressing a button or entering a PIN.
- The SSID is the network name. The default SSID should be renamed.
- You can disable SSID broadcast to hide the network from some wireless devices, but this does not provide security.
- When configuring a wireless router, one of the first steps is to change the defaults, such as the default administrator password.
- The three items you need when configuring a wireless device are: the SSID, the security type (such as WPA2-Personal), and the passphrase or shared key. If you can't connect, double-check these items.
- Most laptops include a switch that can disable wireless access. Check this if a wireless device can no longer connect to a WLAN.
- Technicians can use a wireless locator to locate rogue wireless networks. War drivers also use them when searching for wireless networks.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

1. What is the maximum speed of 802.11g?

   A. 11 Mbps

   B. 54 Mbps

   C. 300 Mbps

   D. 600 Mbps

2. Which of the following protocols uses multiple input multiple output (MIMO) antennas?

   A. 802.11a

   B. 802.11b

   C. 802.11g

   D. 802.11n

3. Which of the following protocols operate at 2.4 GHz? (Choose all that apply.)

   A. 802.11a

   B. 802.11b

   C. 802.11g

   D. 802.11n

4. Users regularly connect to a WLAN by using 802.11g. However, excessive interference is seriously degrading the connection. What can they do to improve performance?

   A. Disable the SSID broadcast

   B. Upgrade the network to 802.11b

   C. Configure the wireless router to use WPA2

   D. Change the channel used by the wireless router

5. You are configuring a wireless router. Which security type provides the highest level of security?

   A. WEP

   B. WPA

   C. WPA2

   D. 802.11n

6. You want to restrict which computers can access a wireless network. What can you do?

   A. Enable MAC filtering

   B. Change the default SSID

   C. Enable SSID broadcast

   D. Upgrade the firmware on the wireless network

7. What can you do to partially hide a wireless network?

   A. Disable WEP

   B. Disable WPA2

   C. Disable MAC filtering

   D. Disable SSID broadcast

8. You have just installed a wireless router for a new wireless network. Of the following choices, what should be one of the first things you do?

   A. Check the range of the wireless network

   B. Change the channel used by the router

   C. Change the default administrator password

   D. Upgrade the firmware

Answers

1. **Correct Answer:** B
   - **A.** **Incorrect:** 802.11a has a maximum speed of 11 Mbps.
   - **B.** **Correct:** The maximum speed of 802.11g is 54 Mbps.
   - **C.** **Incorrect:** 802.11n has a typical speed of 300 Mbps.
   - **D.** **Incorrect:** 802.11n has a maximum speed of 600 Mbps.
2. **Correct Answer:** A
   - **A.** **Incorrect:** 802.11a does not use MIMO.
   - **B.** **Incorrect:** 802.11b does not use MIMO.
   - **C.** **Incorrect:** 802.11b does not use MIMO.
   - **D.** **Correct:** 802.11n uses multiple input multiple output (MIMO) antennas.
3. **Correct Answer:** B, C, D
   - **A.** **Incorrect:** 802.11a operates at 5.0 GHz.
   - **B.** **Correct:** 802.11b operates at 2.4 GHz.
   - **C.** **Correct:** 802.11g operates at 2.4 GHz.
   - **D.** **Correct:** 802.11n operates at both 2.4 and 5.0 GHz.
4. **Correct Answer:** D
   - **A.** **Incorrect:** The SSID broadcast doesn’t impact interference on a network.
   - **B.** **Incorrect:** Changing to 802.11b is a downgrade not an upgrade, with a speed of 11 Mbps compared 54 Mbps for 802.11g. Additionally, it operates on 2.4 GHz so it will have similar problems with interference.
   - **C.** **Incorrect:** WPA2 is a strong security algorithm, but changing security won’t affect interference.
   - **D.** **Correct:** If a WLAN has excessive interference on one channel, you can change to a channel with less interference.
5. **Correct Answer:** C
   - **A.** **Incorrect:** WEP is weak and should not be used.
   - **B.** **Incorrect:** WPA can be used if devices don’t support WPA2.
   - **C.** **Correct:** WPA2 provides the highest level of security for wireless networks.
   - **D.** **Incorrect:** 802.11n does not provide security.

6. **Correct Answer:** A

   A. **Correct:** MAC filtering can be used to restrict access to a WLAN to computers with specific MAC addresses.

   B. **Incorrect:** Changing the default SSID is a good security practice, but it does not restrict access.

   C. **Incorrect:** Enabling SSID broadcast is good for usability, but it does not restrict access.

   D. **Incorrect:** Upgrading the firmware is sometimes useful when a device doesn't support WPA or WPA2, but it won't restrict access.

7. **Correct Answer:** D

   A. **Incorrect:** WEP is a legacy security protocol that shouldn't be used, and it doesn't hide a WLAN.

   B. **Incorrect:** WPA2 is a secure security protocol that should be used, but it doesn't hide the WLAN.

   C. **Incorrect:** MAC filtering can restrict which computers can connect to a WLAN, but it doesn't hide it.

   D. **Correct:** Disabling the SSID hides the WLAN from some wireless devices, but it isn't a reliable security measure.

8. **Correct Answer:** C

   A. **Incorrect:** You can check the range after setting up the router, but this isn't always necessary.

   B. **Incorrect:** You can change the channel if the default channel has interference, but this isn't always necessary.

   C. **Correct:** One of the first steps you should take is to change the default administrator password.

   D. **Incorrect:** You can upgrade the firmware to get extra capabilities, such as to use WPA or WPA2, but if it's a new router, this is probably unnecessary.