

# Understanding Wireless Networking

*Wireless networks allow you* to create a network without running cables. You can also expand an existing wired network by adding a wireless access point as a bridge for wireless clients to your wired network. Two important pieces of knowledge you'll need are an understanding of current wireless networking standards and an understanding of wireless security methods.

IEEE 802.11 includes several different wireless standards, including 802.11a, b, g, and n. To get the most out of your wireless network, you need to use compatible protocols. Some work together, but others don't. IEEE 802.11n provides the greatest flexibility and speeds.

Wireless security had a rocky start, and early wireless security methods weren't secure at all. However, wireless security has increased significantly over the years, and it is possible to create a more secure wireless network today. You just need to know how.

When you have networks in buildings separated by long distances, you can use point-to-point wireless bridges to connect them, even if the buildings are miles away.

- ▶ **Exploring basic wireless components**
- ▶ **Comparing networking standards and characteristics**
- ▶ **Comparing network security methods**
- ▶ **Using wireless networks**
- ▶ **Understanding point-to-point wireless**

## Exploring Basic Wireless Components

Wireless networking is virtually everywhere today: homes, airports, restaurants, and hotels. Even some cities offer citywide wireless Internet access. With newer technologies, we are seeing wireless speeds near that of gigabit.

Before digging in to the details of wireless standards and security methods, it's important to understand some of the basics of wireless networks. This section covers these topics:

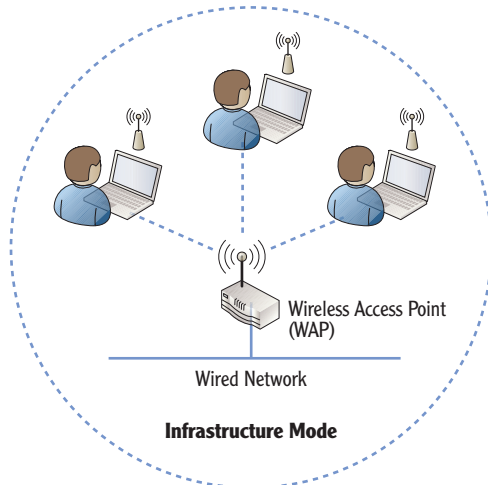
- ▶ Using wireless access points and adapters
- ▶ Naming the wireless network
- ▶ Comparing CMA/CD and CSMA/CA

## Using Wireless Access Points

▶  
When a WAP is not used, clients connect using ad hoc or peer-to-peer mode. Ad hoc wireless has additional security risks beyond WAP-based networks.

A *wireless access point (WAP)* is a device that is located between a wired LAN and wireless clients. It bridges the two networks, giving the wireless clients access to the wired network. When a WAP is used, the wireless network is working in infrastructure mode.

Consider Figure 12.1, which shows a basic wireless network with a WAP bridging the wireless clients to a wired network.



**FIGURE 12.1** Wireless network using infrastructure mode

Once the wireless clients connect, they are able to access resources on the wired network through the WAP. The number of clients you can connect to the WAP depends on bandwidth. As you add more wireless clients, performance slows down for all the wireless clients. Just as with wired networks, high-bandwidth speeds are desirable in wireless networks. Different standards support different speeds, with 802.11n providing the best performance today.

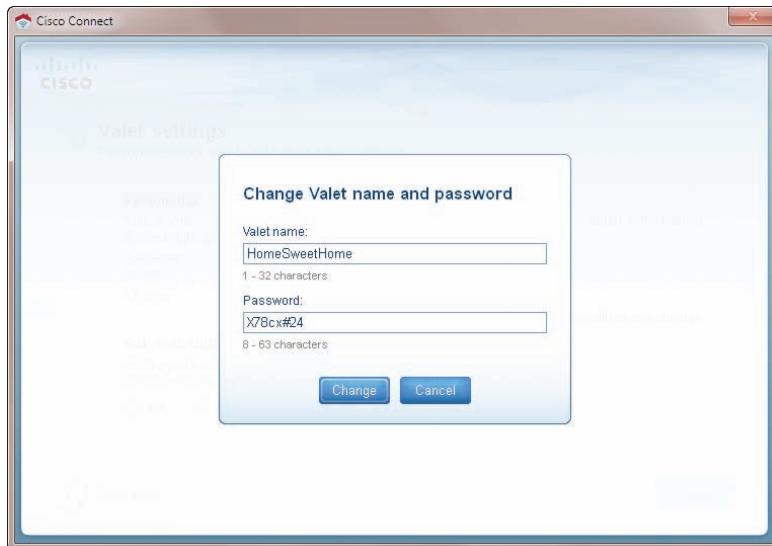
Wireless clients have wireless adapters that must be configured to connect to the WAP. Many laptops include a built-in adapter, but there are also USB wireless

adapters that you can plug into a USB port and adapter cards that you can plug into a slot inside the computer. The adapter must be configured with settings that are compatible with the WAP.

## Naming the Wireless Network

Every wireless network includes a *service set identifier (SSID)*. The SSID is simply the network name. You can name a wireless network just about anything you want as long as you don't exceed the maximum length of 32 characters.

Any wireless device that connects to the WAP uses the SSID, and the SSID is one of the primary items you need to know when configuring wireless devices. Most WAPs include a setup screen that allows you to name the SSID. For example, Figure 12.2 shows a setup screen for the Cisco Valet wireless router.



**FIGURE 12.2** Wireless router setup screen

Most WAPs also give you the option of turning SSID broadcast off or leaving it on. When SSID broadcast is on, the WAP broadcasts the name of the wireless network. One benefit is that other wireless devices can easily see it and connect, as long as other security settings are configured properly.

There was a time when IT professionals consistently recommended disabling SSID broadcast. However, Microsoft recommends against this. Let me repeat that. Microsoft recommends that SSID broadcast is not disabled but instead that the WAP should be configured to broadcast its SSID.

Even though the setup screen uses a more user-friendly name of “Valet name,” this is the SSID. Notice it can be up to 32 characters.

Many people consider this point debatable. However, if you're taking a Microsoft exam, don't disable the SSID broadcast for security reasons.

## WHAT'S THE DIFFERENCE BETWEEN A WAP AND A WIRELESS ROUTER?

A WAP provides connectivity to a wired network for wireless clients. You can think of this as a bridge between the wireless clients and the wired clients.

In contrast, a wireless router is a WAP with additional components. It includes routing components to route traffic between different networks (such as from the Internet through an ISP to a private network). The wireless router often includes a switch component so that you can plug in wired connections to the wireless router and provide connectivity for them.

When you need wireless connectivity in an enterprise, a simple WAP (instead of a wireless router) will often be enough. The WAP connects the wireless devices to the wired network. Other devices on the wired network provide services such as routing and Internet access.

In summary, a wireless router always includes the basic capability of a WAP in addition to routing capabilities. It usually includes even broader capabilities such as that of a switch and DHCP. However, a wireless access point does not include additional capabilities.

There are few reasons Microsoft makes this recommendations:

**Disabling SSID Broadcast Doesn't Enhance Security** Wireless security is primarily provided by authentication and encryption. Disabling the SSID broadcast doesn't help or hinder either authentication or encryption.

**Disabling SSID Broadcast Does Not Truly Hide the SSID** Since the frequency ranges used by different wireless protocols are well known, any receiver can capture frames sent by the wireless devices. The SSID is included in probe requests sent by clients, and attackers can use wireless sniffers to discover the SSID.

**Disabling SSID Broadcast Requires Clients to Broadcast the SSID** When you disable SSID broadcast on the WAP, clients must initiate the connection. Since clients don't know whether they are close to a wireless network, they must constantly send out probes looking for WAPs until they connect. When a client is away from the network (such as in a coffee shop, hotel, or airport), it is sending out probes as often as every 30 seconds with the SSID name. You can disable automatic connection, but this requires additional work on the part of the user.

You'll also need to configure the wireless device with the security used by the WAP. This usually includes setting the passphrase and configuring it to use WPA2.

The different security methods are explained later in this chapter. Older methods are WEP and WPA. The current method is WPA2.



## Comparing CSMA/CD and CSMA/CA

Ethernet uses *Carrier Sense Multiple Access Collision Detection* (CSMA/CD). If a collision occurs, it detects it, and the two parties then retransmit the data.

Wireless networks cannot detect collisions, so they use *Carrier Sense Multiple Access/Collision Avoidance* (CSMA/CA) instead. CSMA/CA prevents a wireless node from transmitting when another node is doing so.

In other words, if one computer wants to send data to another, it will first listen to see whether anyone else is transmitting. If no other device is transmitting, it will send data. However, if it hears data transmissions, it will wait for a random period and recheck the airwaves. This method of transmission reduces the chance of a collision in a wireless environment.

An optional method of improving this process is with Request to Send/Clear to Send (RTS/CTS) packets. Figure 12.3 shows how this works.



**FIGURE 12.3** The RTS/CTS process

In the figure, PC-1 first sends an RTS frame to the other computer asking whether it's clear. PC-2 then sends back a CTS frame indicating it's clear to send. All nodes within hearing distance (including the intended recipient) allow the sender adequate time to send the packet.

## Comparing Networking Standards and Characteristics

Although wireless technologies have grown significantly in the past few years, there really aren't that many standards that are commonly used. Chapter 7 introduced the common wireless standards, and Table 12.1 shows them here with some of their characteristics. The following sections in this chapter explore these standards in more depth.

Chapter 3 introduced CSMA/CD, and Chapter 8 explained it in much more depth.

The RTS/CTS process is not required. Most wireless devices support adding it if required to decrease collisions.

**TABLE 12.1** Current wireless standards

Standard	Speed	Frequency	Comments
802.11a	54 Mbps	5 GHz	Less susceptible to interference
802.11b	11 Mbps	2.4 GHz	Can configure specific channels
802.11g	54 Mbps	2.4 GHz	Widely deployed
802.11n	300 Mbps	2.4 GHz or 5 GHz	Newer and quickly overtaking 802.11g in popularity

## Comparing FHSS, DSSS, and OFDM

Any devices that use radio frequency (RF) signals are susceptible to interference. For example, some cordless phones use this same frequency band as many wireless devices. When more than one device transmits on the same frequency at the same time, it causes interference. For a wireless LAN, this interference can negatively affect performance.

To combat the interference problems, wireless technologies adapted different methods of transmitting data on these bands. They are as follows:

- ▶ Frequency-hopping spread spectrum (FHSS)
- ▶ Direct-sequence spread spectrum (DSSS)
- ▶ Orthogonal frequency division multiplexing (OFDM).

Since these are often referenced for the different technologies, it's worthwhile explaining them.

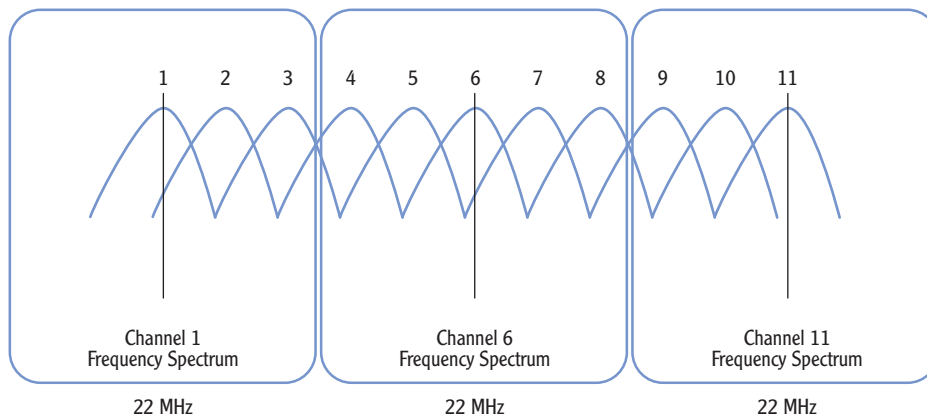
FHSS hops between frequencies in a pseudorandom pattern. It starts with a center frequency known to the transmitter and receiver and then quickly changes, or *hops*, between different frequencies. The transmitter and receiver synchronize these hops so they know what frequency is next.

These random frequencies are in 1 MHz increments and do not use more than 1 MHz at any given time. FHSS was introduced with the original 802.11 specification but isn't used with any of the current IEEE 802.11 specifications. It is used with Bluetooth wireless networking.

IEEE 802.11b uses DSSS. It uses the full bandwidth (or spectrum) of the transmitted frequency and can use one of 11 possible channels in the United States, as shown in Figure 12.4.

**FHSS made it difficult for unintended recipients to receive the data, but it wasn't that effective at limiting interference problems.**

**Bluetooth is a wireless technology used for short distances creating personal area networks (PANs). A PAN transmits data to devices that a person is carrying or wearing.**



**FIGURE 12.4** DSSS channels

Each DSSS channel has a spectrum of 22 MHz. Channel 1, channel 6, and channel 11 can each be used without interfering with each other. This is useful if you have multiple wireless access points located close to each other for different networks. DSSS uses the center frequency of the channel and then modulates the signal out from the center frequency consuming the entire 22 MHz spectrum. DSSS is resistant to interference, and it allows multiple users to share a single channel.

OFDM splits the radio frequency signal into smaller subsignals and transmits data simultaneously across these different frequencies. Each subsignal includes a separate data stream. You can compare this to multiplexing used with cable TV. A single cable includes multiple TV channels, and a TV can tune to any single channel. 802.11a and 802.11g use OFDM. 802.11n uses an enhanced OFDM by combining it with multiple antennas.

## IEEE 802.11

IEEE created 802.11 as the first Wi-Fi standard in 1997. It maxed out at a speed of 2 Mbps, with an actual throughput of less than .7 Mbps, which was simply too slow for most applications. It used FHSS.

It was also highly susceptible to radio interference from other devices using the 2.4 GHz frequency. This includes devices such as baby monitors, cordless telephones, video cameras, microwave ovens, and Bluetooth devices.

Combined with the slow speed and high susceptibility to interference, the original specification was never widely adopted.

WAPs used as wireless repeaters use the same center channel. WAPs physically close to other WAPs for different wireless networks use different channels.

## WIRELESS GOVERNING BODIES

Four governing bodies overlook wireless technology. They are the Federal Communications Commission (FCC), Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standards (ISO), and the Wi-Fi Alliance.

**IEEE** The IEEE sets the ISO standards for the wireless IEEE 802.11 family to ensure consistency. You can visit the IEEE and ISO websites at [www.ieee.org/index.html](http://www.ieee.org/index.html) and [www.iso.org/iso/home.html](http://www.iso.org/iso/home.html).

**Wi-Fi Alliance** The Wi-Fi Alliance is the trade association that promotes wireless technology. It approves products that meet their interoperability guidelines, and these products can use the Wi-Fi logo. For more information on the Wi-Fi Alliance, you can visit its website at [www.wi-fi.org](http://www.wi-fi.org).


**FCC** The Federal Communications Commission (FCC) regulates wireless frequencies and modulation types. The FCC also regulates the use of unlicensed Instrument, Scientific, and Medical (ISM) frequency bands that are used in Wi-Fi communications. You can view the FCC website at [www.fcc.gov](http://www.fcc.gov).

## IEEE 802.11a

IEEE designed 802.11a with a different frequency band to avoid the interference in the crowded 2.4 GHz frequency band. Instead, IEEE uses 5 GHz. It can achieve a raw speed of 54 Mbps, which was significantly higher than the max of 2 Mbps for 802.11. However, the higher frequency of 5 GHz had a trade-off of a shorter range.

The advertised range of 802.11a is approximately 30 meters (100 feet). However, you were only able to achieve the full 54 Mbps speed at close ranges of between 50 feet and 100 feet.

Unfortunately, this different frequency also caused logistics problems. The 5 GHz components were difficult to manufacture, and first-generation components often didn't live up to the advertised specifications. Because of this, the release of 802.11a was slow. IEEE 802.11a and IEEE 802.11b actually made it to market at about the same time.

 The maximum range of wireless is achievable only in ideal conditions. Obstructions such as walls and trees absorb the signal, reducing the distance.



## WIRELESS SPEEDS AND DISTANCES

The advertised speeds of different wireless devices represent the maximum speeds in ideal conditions. In the real world, these speeds are rarely achievable.

For example, IEEE 802.11g advertises a speed of 54 Mbps. If the wireless access point is 5 feet away from the wireless device, you can probably achieve a speed of 54 Mbps. However, if you move the wireless device farther and farther away, at some point errors creep into the transmission.

Devices automatically correct for errors by slowing down the transmission speed. If there are errors at 54 Mbps, the devices try slower and slower speeds until they are able to achieve an error-free transmission. In other words, depending on the distance, interference from other transmissions, and obstructions, an advertised speed of 54 Mbps could be reduced to 6 Mbps.

Because of the manufacturing problems with 802.11a's 5 GHz components, more users adopted 802.11b than 802.11a.

## IEEE 802.11b

IEEE 802.11b was another improvement over the original IEEE 802.11 specification. Like 802.11, it operates at 2.4 GHz but increased the speed from 2 Mbps to a speed of 11 Mbps. The increase in data throughput speed from 802.11's 2 Mbps was a major performance increase. The migration to 802.11b was rampant.

As mentioned previously, 802.11b uses DSSS, which improved the reliability of the signals. Also, DSSS has configurable channels. For example, if your neighbor is using channel 6 at full power, you can change your network to channel 1, and neither network will interfere with other. Changing to a lesser used channel increases performance without any additional cost.

## IEEE 802.11g

IEEE 802.11g uses OFDM, which brought a significant increase in speed up to 54 Mbps. It uses the same 2.4 GHz frequency as 802.11b, making both b and g wireless devices compatible with each other.

Users loved the increased speed, and 802.11g quickly became a favorite, both in homes and businesses. IEEE 802.11g is widely available, but the advances of 802.11n will likely overtake 802.11g devices in market share within a couple of years.

802.11b devices can work with 802.11g devices, but connections between them will operate at the slower 11 Mbps speed.

Some devices are advertised as a/b/g compatible. They can operate at 5 GHz for 802.11a devices and operate at 2.4 GHz for 802.11b and 802.11g devices.

As mentioned, 802.11g increased the speed to 54 Mbps. One of the reasons for this speed increase is the change in the modulation type. IEEE 802.11g uses OFDM. The average distance for maximum performance is still rated between 80 feet and 100 feet, but some vendors advertise distances as great as 150 feet. The maximum distance will always vary depending on obstructions, RF interference, and even atmospheric conditions.

## IEEE 802.11n

The need for speed brought 802.11n to our wireless networks. It advertises speeds of up to 300 Mbps and includes the possibility of reaching 450 Mbps. The improvements in speed are primarily because of equipment changes.

IEEE 802.11n uses *maximum-input maximum-output* (MIMO) antenna technology. MIMO includes multiple antennas at both the receiver and the transmitter to minimize errors and increase the data throughput. An intriguing improvement is the concept of smart antennas. These intelligent ears grab multiple streams of data and combine them to ensure lightning fast speed.

These multiple antennas also increase the distance of 802.11n devices. Even as far as 300 feet away, tests indicate that 802.11n networks still operate as high as 70 Mbps.

Even though 802.11n wasn't formally approved by IEEE until late in 2009, devices based on proposed draft versions of the standard started hitting the market in 2007. The Wi-Fi alliance began certifying products in 2007 based on the 802.11n proposal.

Another benefit is that IEEE 802.11n is backward compatible with 802.11a, 802.11b, and 802.11g devices. It is important to realize that being backward compatible does not mean that the older devices will operate at the newer speeds. If you want to achieve the 300 Mbps speed, both the WAP and the wireless device need to be 802.11n.

## Comparing Network Security Methods

One of the biggest concerns with wireless is security. Since the signals are broadcast over the air, they are easily intercepted. However, multiple security technologies are available today. Some are better than others are, and some aren't secure at all. It's important to know which security methods to implement in different wireless networks.

When wireless networks were first created, they had a primary goal of being easy to use. Designers wanted to make it easy for devices to connect to each

▶  
Actual data throughput is usually closer to 180 Mbps, but this is still much better than a perfectly operating 802.11g wireless network at 54 Mbps.

▶  
Many companies wanted to be first to market 802.11n products to grab market share. By late 2009, there were already many 802.11n devices available.

other and easy to transmit data between each other. The designers did a good job with this goal.

Later, they decided to add some security features. Unfortunately, their first attempt at security was not very successful. Because of this, many people still think of wireless networks as not being secure. However, it is possible to provide strong security for wireless networks today.

If you plan on using a wireless network, you need to know what security methods are available. More, you should know what methods are actually secure. Table 12.2 introduces the wireless security methods, and the following sections explore them in more depth.

**TABLE 12.2** Wireless security methods

Security method	Security level	Comments
Wired Equivalent Privacy (WEP)	Low, cracked in 2001	Not recommended for use unless nothing else is available.
Wi-Fi Protected Access (WPA)	Medium, cracked in 2008	Interim fix for WEP until release of WPA2.
Wi-Fi Protected Access 2	Strong	WPA2 support is required for all Wi-Fi certified devices.
802.1x	Strongest when used with WPA2	802.1x (also known as Enterprise mode) authenticates clients before granting wireless access.

Figure 12.5 shows the wireless security page of Cisco wireless router. This model supports several different security modes. Notice that WPA and WPA2 both support Personal and Enterprise modes.

The figure also shows a RADIUS mode. RADIUS is short for Remote Authentication Dial-in User Service. IEEE 802.1x can use RADIUS and has a back-end server to provide authentication.

## Wired Equivalent Privacy

*Wired Equivalent Privacy* (WEP) was the first security model used on IEEE 802.11 wireless networks. Its intent was to offer privacy equivalent to a wired Ethernet network. The key here is the word *intent*. It failed.

Personal and Enterprise modes are covered in more depth later in this section.

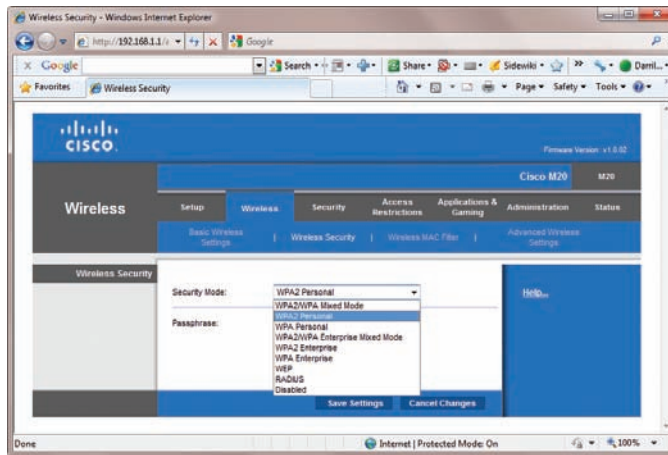


FIGURE 12.5 Viewing security modes for a wireless router

## WIRELESS NETWORK THEFTS

Hardly a day goes by when network security (or the lack of it) isn't mentioned in the news. Wireless security has been especially problematic in the past. Early attempts to lock down wireless networks were woefully lacking, and many businesses simply didn't understand the risks. They transmitted some data using insecure methods, and other transmissions didn't use any security at all.

For example, in 2003 and 2004, hackers stole information from more than 45 million credit cards from TJ Maxx and Marshalls stores. Wireless networks transmitted all of this information. Customers who returned merchandise without receipts had to provide driver's license numbers, and it's estimated that 455,000 of these customers had their data stolen. This represents one of the biggest wireless thefts (if not the biggest), but there have certainly been many more.

Hackers were able to capture these wireless transmissions and harvest the data. Some data was sent without any security. Other data was sent using the insecure WEP. The stolen data was used to steal identities and make fraudulent charges on the credit cards.

Instead, attackers learned ways to listen to the data, capture it, and decrypt it. WEP had multiple faults including the following:

**Its Use Was Optional** Instead of a secure by default strategy, WEP had to be enabled. Many wireless users didn't understand its use and didn't enable it.

**Weak Encryption** WEP used RC4, which is a stream cipher. Attackers are able to crack RC4 using freely available software downloaded from the Internet.

**Poor Key Management** Encryption keys are secret strings of data used to encrypt and decrypt data. They must be secret between the parties, changed often, and not repeated. However, keys used by WEP are not secure. An eavesdropping attack can determine the encryption key within a minute.

**Cracking Software Widely Available** Once attackers understood the cracks, they wrote and distributed tools to attack wireless networks.

## WAR DRIVING

*War driving* is the act of driving a car through an area and scanning for wireless networks. Attackers war drive to locate wireless networks and determine the security used to protect them. When attackers locate wireless networks with weak security, they sit in their car with a wireless receiver and capture the wireless transmissions.

Attackers use modified antennas to improve the reception. For example, you can create a rudimentary directional antenna with a can. You remove the top of the can, empty it, and then run a wire from the can to the wireless receiver. You can then point the can in different directions to capture wireless signals. This directional antenna significantly increases the reception distance. Now, instead of an attacker sitting in the parking lot or outside your home, they can be further away.

The Payment Card Industry Security Standard Council sets standards for credit card processing. They prohibit the use of WEP on any wireless networks processing credit cards today.

## Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) was the initial security improvement over WEP. WPA works on WEP-designed hardware without any additional cost to the consumer. This usually required a flash upgrade to upgrade the firmware on existing WEP hardware.

The intent behind WPA was to improve upon WEP's weaknesses and reduce the complexity of configuration. You learned earlier that one of WEP's weaknesses was manual key management. It was optional but cumbersome and oftentimes avoided. With WEP, you can use the same key for as long as you choose, but when you do change the key, it has to be changed on all devices within your wireless network. It increased the administrative workload, and many users simply overlooked this step.

Flashing the wireless device is similar to flashing the BIOS on a computer. It installs new software in the programmable read-only memory (PROM).

TKIP changes keys without requiring the user to change the passphrase. In WEP, similar keys were reused for encryption until the passphrase was changed.

You can configure a Windows Server 2008 server as an 802.1x server. 802.1x authentication servers are covered in more depth later in this section.

WPA is still better than WEP. However, the preferred security solution for wireless networks today is WPA2.

AES is an extremely strong and widely respected encryption algorithm. Many different applications encrypt data with AES, including nonwireless applications.

With WPA, rekeying the encryption keys are mandatory, and with each data frame, a new key is created automatically. Temporal Key Integrity Protocol (TKIP) managed the keys and provided several other technical improvements.

You can configure WPA in two different modes:

- ▶ Personal mode, or preshared key (PSK) mode
- ▶ Enterprise mode

Personal mode requires manual configuration similar to WEP but not with the upkeep of changing the key. The initial shared key is a string of characters such as a password or passphrase. Once you enter the initial shared key, TKIP is responsible for encryption and automatic rekeying, which eliminates the need for manual rekeying.

Enterprise mode requires authentication with a back-end server known as an 802.1x server. After authentication, the access point negotiates a separate and unique key with each client.

The significant difference between WPA Enterprise and Personal mode is in authentication. With WPA Personal mode, every wireless client uses the same passphrase, which doesn't individually identify any of the clients. Any client with the passphrase is granted access. With WPA Enterprise mode, authentication takes place at an authentication server, and each client requires a specific account and credentials (such as a username and password).

It may not be obvious, but the primary purpose of WPA was to provide a temporary secure solution while designers created a more secure solution. Designers fully expected that researchers or attackers would crack WPA. They were right. Researchers cracked WPA in 2008.

## WPA2

WPA2 is the updated version of WPA and is standardized as IEEE 802.11i. WPA2 supports encryption with the Advanced Encryption Standard (AES) algorithm. The U.S. government adopted AES as their encryption standard, and it is considered the strongest symmetric encryption available.

One drawback to WPA2 is that it requires hardware that is different from the hardware used with WEP and WPA. At this point, all new hardware is WPA2 compatible, but you may run across older hardware that isn't compatible. If so, you can use the older TKIP with WPA2.

WPA2 supports both Personal and Enterprise mode just like WPA. Personal mode uses a preshared key, and Enterprise mode requires an 802.1x server.

**WPA2 Personal Mode** WPA2 Personal (or WPA2-PSK for preshared key) is for home users and small businesses that are not using an authentication server. Anyone that has the passphrase and name of the network can connect. It combines the passphrase and the network name to create unique encryption keys for clients.

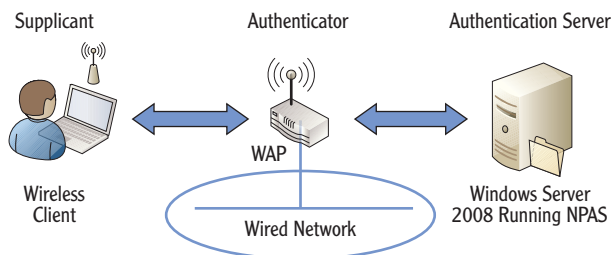
**WPA2 Enterprise Mode** WPA2 Enterprise Mode uses 802.1x for authentication. This requires a back-end server such as a Windows Server 2008 server running Network Policy Access Services to authenticate clients. Wireless clients are not granted access to the wireless network unless they can authenticate.

## Using an IEEE 802.1x Authentication Server

IEEE 802.1x provides port-based security. In short, it provides an authentication mechanism for either 802.3 (wired Ethernet) or 802.11 networks. 802.1x includes three elements in the authentication process:

- ▶ Supplicant: Client
- ▶ Authenticator: Access point
- ▶ Authentication server: Running RADIUS and EAP

Consider Figure 12.6. It shows the wireless client as the supplicant, the WAP as the authenticator, and a back-end server as the authentication server.



**FIGURE 12.6** WPA2 enterprise authentication

The authenticator acts like a security guard and ensures the supplicant has adequate credentials before providing access to other networks. When the supplicant first connects, the access point sends the credentials to the authentication server,

◀ The Wi-Fi Alliance requires all new wireless devices to support WPA2 in order to be certified with the Wi-Fi logo.

◀ Authentication means the clients must provide credentials such as a username and password. More advanced authentication can require smart cards or fingerprints.

In a Microsoft environment, the authentication server will often check the credentials against an Active Directory database. Active Directory hosts accounts and their credentials.

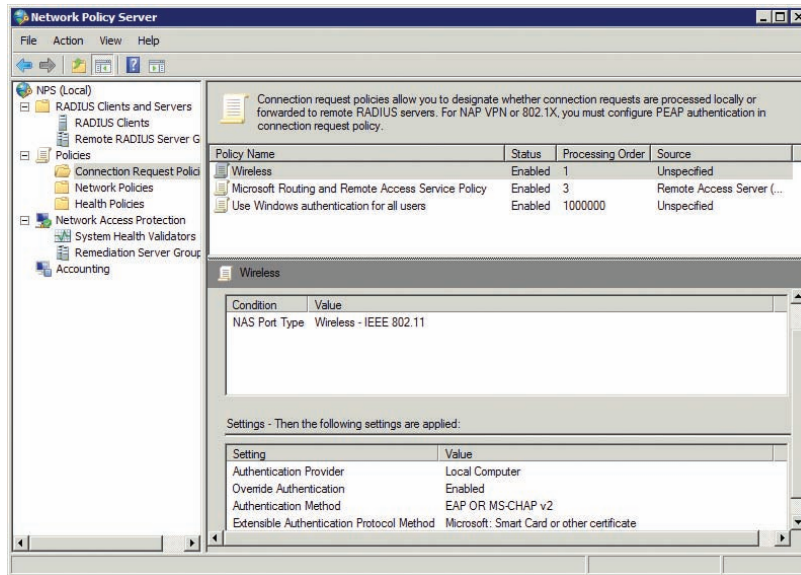
◀

The configuration of NPAS is beyond the scope of this book. However, Network Access Protection is covered in the Microsoft Windows Security Essentials book in this series.

and the authentication server checks the credentials against its database. If the credentials are valid, the authentication server confirms them to the authenticator, and the authenticator grants access to the client.

You can add the Network Policy and Access Services (NPAS) role to a Windows Server 2008 server and configure it as an 802.1x server. Any clients that are not authenticated will not be allowed access to the network. You can also configure NPAS to grant nonauthenticated clients access to isolated networks.

Figure 12.7 shows a Windows Server 2008 server with the NPAS role added.



**FIGURE 12.7** Network Policy Server role in a Windows Server 2008 server

You can see a Wireless policy in Figure 12.7 (named *Wireless*). It is configured with a value of Wireless – IEEE 802.11 to authenticate 802.11 wireless clients. Additionally, it is configured to authenticate the clients using EAP or MS-CHAPv2. EAP supports the usage of smart cards, and MS-CHAPv2 is a secure method of authenticating username and passwords.

## Using Wireless Networks

Wireless networking offers many advantages over wired network configuration such as ease of installation and elimination of wires. Once the wireless network is configured, users can share resources such as files, folders, printers, and more, just as they can in a wired network.



## MAC FILTERING DOES NOT PROVIDE REALISTIC SECURITY

On many wireless routers, you can configure media access control (MAC) address filtering. The goal is to ensure that only computers with the specified MAC address can access the wireless router. On the surface, this sounds very secure since MAC addresses are theoretically unique.

However, it's very easy for an attacker to spoof a MAC address. In other words, the attacker can modify packets so that it looks like the attacker's packets are coming from an approved MAC address. Although using MAC filtering doesn't cause any harm, it won't stop an experienced attacker from entering your network.

More and more wireless networks are popping up in both homes and businesses today. The following sections expand on the use of wireless in these different environments.

## Home Wireless Networks

The primary piece of equipment used to create a wireless network in a home (or small business) is a wireless router. It's important to realize that a wireless router has many different components:

**Wireless Access Point** The wireless access point provides connectivity for the wireless devices. It includes a bridge to bridge the wired and wireless devices together.

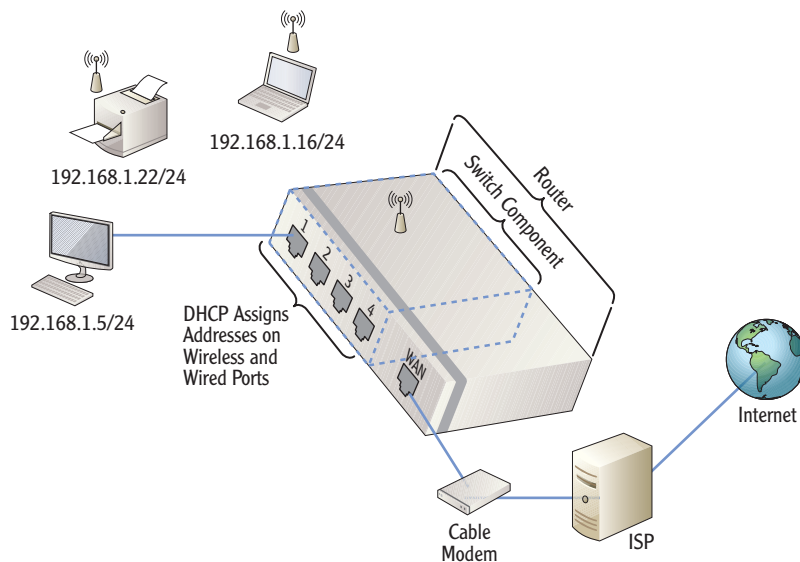
**Switch** The switch provides connectivity between wired and wireless devices. All of the devices connected to the switch ports have the same network ID and share the same broadcast domain.

**Router** In a home network, the router is usually connected directly to the cable modem or to another Internet connection. It routes traffic from the internal switch to the Internet (and back).

**DHCP** DHCP provides IP addresses and other TCP/IP configuration information to all the devices on the switches network.

Figure 12.8 shows the rear view of a wireless router with the extra components. The first four ports are typical wired ports that connect with the wireless router's switch component. The device also connects wireless connections through the switch. DHCP provides TCP/IP information to all the ports connected to these switch ports and has assigned addresses to a wired computer, a wireless printer, and a wireless laptop.

You can connect wired and wireless devices using the wireless router's WAP and switch components without connecting it to a WAN. This creates a private network.



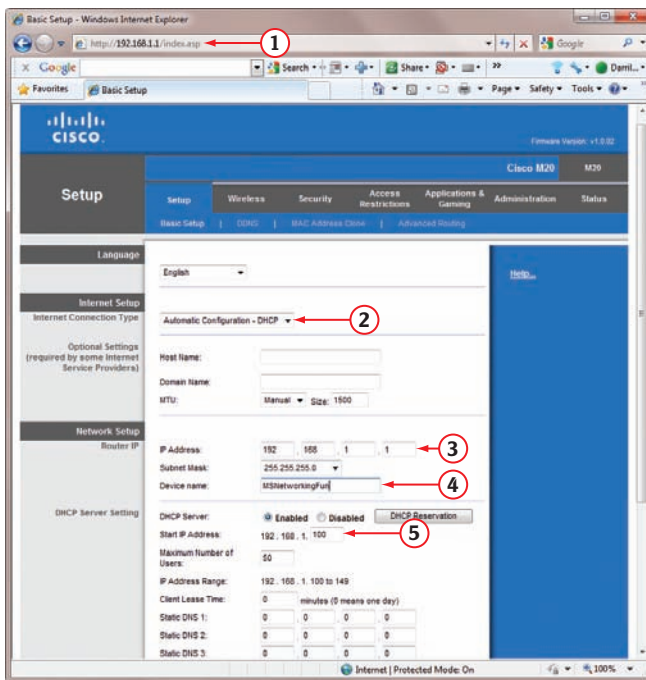
**FIGURE 12.8** Wireless router rear view

The routing component routes any traffic destined for the Internet through the WAN port. This usually connects to a DSL modem, cable modem or other broadband device to the Internet service provider (ISP).

Many wireless routers use the range of 192.168.1.0/24. The wireless router uses 192.168.1.1 and is the default gateway for computers connected via the wireless router. The router routes traffic from the switch to the WAN port, and the WAN port provides connectivity to the Internet via an ISP.

You can configure most routers through a web interface. Figure 12.9 shows one of the pages in the web interface for a Cisco M20 wireless router. This is the Basic setup page with some items highlighted.

1. This is the URL using the IP address of the router (192.168.1.1).
2. The router is using DHCP to receive a public IP address from the ISP.
3. The router's internal private IP address is 192.168.1.1.
4. The device name is the first 15 characters of the SSID (the network name). If the SSID is 15 characters or less, the device name will be the same.
5. DHCP settings indicate how many IP addresses the wireless router can issue and the range of addresses. In the figure, the range starts at 192.168.1.100 and issues 50 addresses.



**FIGURE 12.9** Cisco M20 web interface

All wireless routers have default IP addresses, administrator names, and default passwords. Table 12.3 shows some of the defaults for common brands.

**TABLE 12.3** Common wireless router defaults

Brand	Default IP address	Administrator name	Default password
Cisco	192.168.1.1/24	admin	admin
Linksys	192.168.1.1/24	Admin or blank on older systems	admin
Netgear	192.168.0.1/24	admin	password
3COM	192.168.1.1/24	admin	admin

Most wireless routers today are extremely simple to set up. About all you really need to do is enter or change the network name (SSID), change the administrator password from the default, and choose the security method (usually WPA2 Personal). Many have installation wizards that lead you through the process.

It's important to change the default password of the administrator account. If not, an attacker can access the network and make changes, even out locking the owner.

Many wireless routers have additional capabilities. For example, some include a VPN that allows you access a home network from a remote location.

## Wireless Networks in a Business

Wireless networking in the business environment has grown exponentially in recent years with no end in sight. The advantages to wireless networking in a business are as follows:

- ▶ Reduced costs compared to wired networks
- ▶ Better flexibility over wired networks
- ▶ Greater mobility between offices
- ▶ Improved scalability

The primary difference between using wireless networks in a home or small office and using wireless in a business is that businesses will usually use wireless access points only, and not wireless routers.

Configuring a wireless network in a business is very similar to configuring a wireless network at home. You need to name the network with an SSID and configure the security. As a reminder, the most secure security you can use in a business wireless network is WPA Enterprise, which uses 802.1x for authentication.

One difference in businesses is the use of repeaters. Since a business can be considerably larger than a home, a single WAP may not cover the entire business. Instead, you add additional WAPs as repeaters.

There are two terms worth defining in the context of wireless repeaters:

**Basic Service Set (BSS)** A BSS is a wireless network composed of one WAP and one or more wireless devices. For many wireless networks, a single WAP is enough.

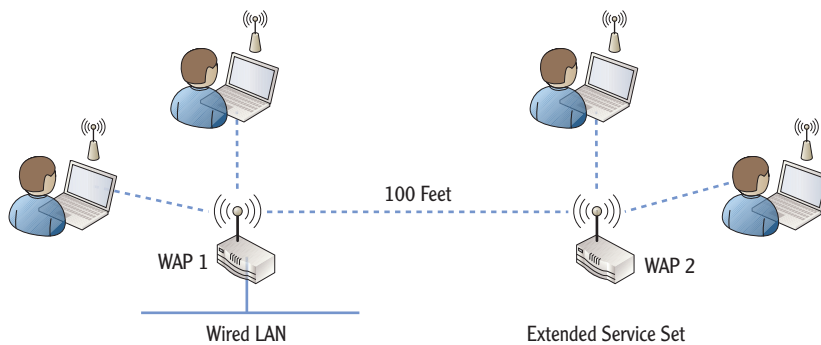
**Extended Service Set (ESS)** An ESS is a wireless network with more than one WAP, with each WAP supporting one or more wireless devices. Additional WAPs act as repeaters and extend the range of the wireless network. All devices in the ESS use the same SSID, and the same broadcast channel.

Figure 12.10 shows an ESS network. WAP2 is extending the range of the wireless network.

The key to success when adding repeaters is device placement. If a repeater is placed too far from the root WAP, a device may get dropped while roaming. If a repeater is placed too close, the two WAPs may interfere with each other. In Figure 9.6, a repeater has been added at approximately 100 feet (about 30 meters) from the root access point, which is a reasonable distance, but testing may dictate that you need to adjust the distance.

Computers connected in ad hoc mode (a wireless network without a WAP) form an Independent Basic Service Set (IBSS).

The placement of WAPs in business networks also becomes a network security issue, because the signals can easily bleed outdoors and across parking lots and streets.



**FIGURE 12.10** Extended service set with a repeater

The repeater ensures that users who are out of range of the root WAP will still have adequate signal strength to stay connected. As users roam between repeaters, wireless devices will connect with the strongest signal automatically, allowing for optimal performance.

## Understanding Point-to-Point Wireless

*Point-to-Point* (P2P) wireless is useful when you need to connect two networks using wireless technologies instead of traditional wired connections. It's sometimes cost prohibitive to run cable between two points. The distance between points may be a few hundred feet, or a few miles, with 25 miles typically being the maximum.

For example, Figure 12.11 shows a main office with a newly leased building 10 miles down the road. Each building includes an internal network, but they need connectivity between each other.

Many technologies support the P2P wireless bridge. These include microwave, infrared, and laser-optics radio transmission. Most of these are limited to line of sight, but there are other considerations.

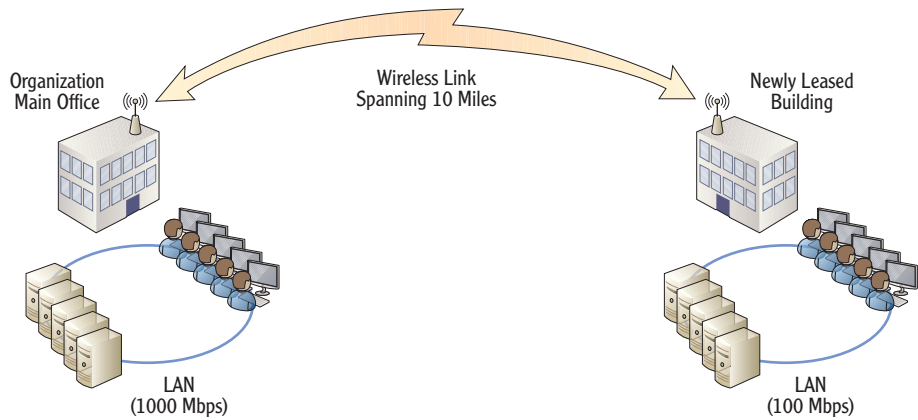
The first step in configuring a wireless bridge is performing a site survey. This is to ensure that the area is free from radio frequency interference and line-of-sight obstructions. Wireless radio waves in the 2.4 and 5.0 GHz range do not penetrate building structures or trees very well. You also need to know the height of the transceivers on both buildings because this affects the distance. Higher buildings allow longer distances.

If the area is clear of radio interference and physical obstructions, you still don't have a green light. The area underneath and above the line of direct sight has to be considered. This area is the Fresnel zone, as shown in Figure 12.12.

Cell phones roam in this way. They automatically switch between wireless towers to the tower providing the strongest signal.

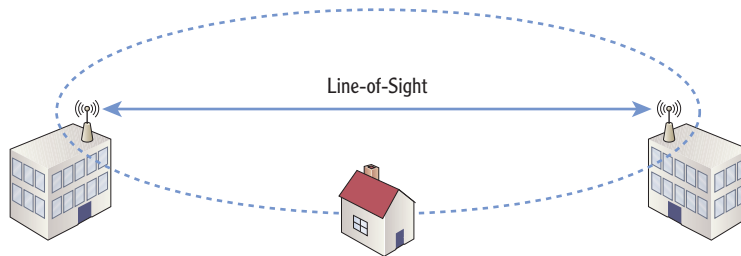
P2P wireless connections are also called wireless bridges or P2P wireless bridges. They bridge two or more wired networks with a network connection.

Line of sight indicates that there is a clear path between the two bridges. The curvature of the earth limits the line of sight.



**FIGURE 12.11** P2P wireless bridge

Performing a site survey and determining the Fresnel zone can be complex. The point to remember is that there's more to it than just adding two wireless bridges.



**FIGURE 12.12** Evaluating the Fresnel zone

The *Fresnel zone* is the area underneath and above the direct line of sight between the two points. In the figure, a house is penetrating the lower boundary of the Fresnel zone. Structures within the Fresnel zone have a tendency to absorb radio waves, and blockage greater than 40 percent will render your wireless connection unreliable.

Another consideration with the bridge is alignment of the directional antennas between the two points. It will require special equipment and expertise to have these two antennas focused toward each other.

Bridge antennas are typically the dish type (parabolic) directional antennas or Yagi directional antennas. A directional antenna has the best performance in a specific direction and can be pointed or directed at specific locations. In contrast, omni-directional antennas receive signals from all directions.

When the distances are farther than the eye can see, engineers use riflescopes (without the rifles) to focus and align the wireless bridges with each other.

## THE ESSENTIALS AND BEYOND

In this chapter, you learned about many of the wireless components, standards, and security methods. A WAP bridges wireless devices to a wired network. A wireless network has an SSID, which is simply the name of a wireless network. Several different wireless standards are used, including 802.11a, b, g, and n. 802.11a uses a frequency of 5 GHz. 802.11b and g use 2.4 GHz, and 802.11n uses either 2.4 GHz or 5 GHz. Security standards include WEP (old and insecure), WPA (cracked in 2008), and WPA2 (strong). You can increase security by using WPA2 with 802.1x, which adds authentication. In businesses, you can extend a wireless network by adding repeaters. You can also connect two buildings that are miles apart by using Point-to-Point (P2P) wireless bridges.

### ADDITIONAL EXERCISES

- ▶ Draw a network for a home network that includes wired connections and wireless connections and provides connectivity to the Internet.
- ▶ Imagine that you came across a WRT54G router but you don't have the username and password. Look on the Internet to learn how to reset this router.
- ▶ List the different types of wireless standards including their speeds and frequencies.
- ▶ List the different types of security methods used with wireless.

### REVIEW QUESTIONS

1. Which of the following statements about the service set identifier (SSID) are true? (Choose all that apply.)
  - A. The SSID is an alphanumeric value that identifies the vendor's device type.
  - B. The SSID is an alphanumeric information field with a maximum value of 32 bits.
  - C. The SSID is a logical network name for a wireless network.
  - D. The SSID identifies the security encryption method.
2. True or false. 802.11 networks use CSMA/CD.
3. What frequency does an 802.11a network use?
  - A. 11 Mbps
  - B. 54 Mbps
  - C. 2.4 MHz
  - D. 5 GHz
4. Which of the following frequency ranges does 802.11b use?
  - A. 2.4 GHz
  - B. 4.1 GHz
  - C. 2.4 MHz
  - D. 5 GHz

(Continues)

**THE ESSENTIALS AND BEYOND** *(Continued)*

5. What frequency does an 802.11n network use? (Choose all that apply.)
  - A. 54 Mbps
  - B. 300 Mbps
  - C. 2.4 MHz
  - D. 5 GHz
6. What is the maximum speed of an IEEE 802.11b network?
  - A. 2 Mbps
  - B. 11 Mbps
  - C. 54 Mbps
  - D. 300 Mbps
7. True or false. IEEE 802.11n networks can operate at speeds as high as 300 Mbps.
8. Of the following security methods, which one is the most secure?
  - A. WEP Personal Mode
  - B. WEP Enterprise Mode
  - C. WPA2 Personal Mode
  - D. WPA2 Enterprise Mode
9. True or false. A WAP and a wireless router are the same thing.
10. Your company is planning to lease a second building, which is about 2 miles away. You're asked how the networks between the two buildings can be connected. What would you suggest?
  - A. Add roaming WAPs.
  - B. Connect the buildings with a P2P bridge.
  - C. Extend the network by adding additional WAPs.
  - D. Run a twisted pair between the buildings.