**Chapter 21. Setting Up a Home Or Small Office Network**

[Network technology overview](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#network_technology_overview)

[Choosing an ISP](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#choosing_an_isp)

[Connecting Windows 8 to your network](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#connecting_windows_8_to_your_network)

[Manually configuring Windows 8 networking](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#manually_configuring_windows_8_networkin)

[Fine-tuning wireless settings](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#fine-tuning_wireless_settings)

[Routers](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#routers)

[Choosing home networking technologies](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#choosing_home_networking_technologies)

[Designing a wireless network](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#designing_a_wireless_network)

[Web applications](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#web_applications)

WITHOUT an Internet connection, a PC is nothing more than an expensive brick. Getting connected to the Internet can be a very simple task, but getting everything you can out of your home network can be a very complex task.

This chapter provides an overview of networking technologies and describes how to select an Internet service provider (ISP), how to configure Windows 8 networking, how to choose a router and wireless access point, how to get the best performance out of your home network, and how to configure common network services such as email, file hosting, and web hosting.

**NOTE**

For information about sharing files and printers, including how to use homegroups, read [Chapter 24](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch24_html).

**NOTE**

For information about configuring firewalls and port filtering on your home office network, including how to switch a network between public and private or public and work/home, refer to [Chapter 19](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch19_html).

**NOTE**

For information about Bluetooth and mobile networks (such as 3G networks), refer to [Chapter 22](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch22_html).

**NOTE**

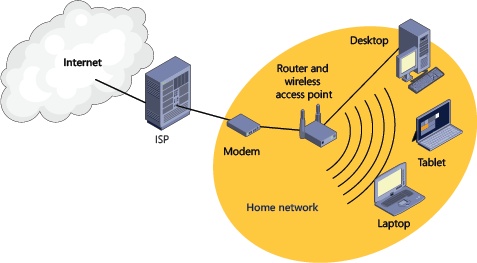
For information about troubleshooting network problems, including performance problems, refer to [Chapter 23](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch23_html).

**Network technology overview**

To configure Windows 8 and optimize a home network, you need to understand just the basics of home networking, including typical home network architectures and common technologies, such as IP addressing, NAT, DHCP, and DNS. The sections that follow provide that overview.

**The architecture of a home network**

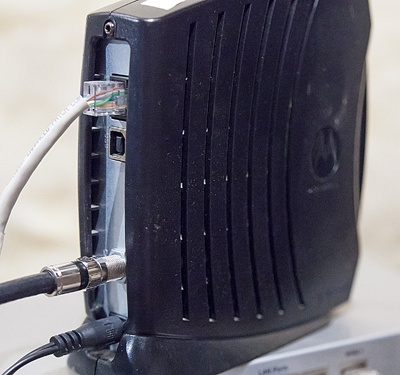
[Figure 21-1](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#several_elements_are_included_in_a_typic) shows a typical home network. In this diagram, the solid lines connecting the different devices represent Ethernet cables, and the wireless signals represent Wi-Fi.



*Figure 21-1. Several elements are included in a typical home network architecture.*

Here’s a description of the most important components of a home network:

* **Internet** The Internet is really a group of thousands of companies, universities, and individuals who have agreed to connect their networks to each other using routers, cables, and computers. Your home network becomes part of the Internet once you connect to it.
* **Internet service provider (ISP)** As mentioned in the previous bullet point, the Internet is a bunch of organizations that have agreed to connect to each other. The biggest organizations, known as Tier 1 ISPs, usually connect to each other and exchange data for free. Unless you’ve spent billions to run cables across continents and oceans, the Tier1 ISPs probably won’t want to connect you to their network for free. Instead, you have to pay a business that already has an Internet connection to borrow their network. This business is your Internet service provider (ISP). Today, the biggest ISPs are cable, phone, and satellite companies. Other types of ISPs exist, but the big ISPs are used most often because they already had connections to people’s homes and knew how to sell them services when the Internet became popular.
* **Modem** Short for MOdulator DEModulator, a modem sends Internet communications across whatever type of Internet connection you have. Typically modems have two network connectors: one specific to your connection with your ISP (such as a coaxial connection for a cable provider or a phone connection for a DSL provider) and a wired Ethernet connection. You usually rent your modem from your ISP. [Figure 21-2](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#a_cable_modem_sends_your_network_communi) shows a cable modem’s connectors. Today, many modems have routers and wireless access points built into a single device.



*Figure 21-2. A cable modem sends your network communications across a cable TV provider’s network.*

* **Router** While you can connect a PC directly to your modem’s Ethernet connection, nowadays most people have multiple PCs on their home network that need Internet access. A router’s job is to combine the communications from every network device in your home and forward them to your ISP. Routers always have at least two Ethernet ports: one to connect to the modem, and one to connect to a PC. Routers usually provide Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) services, described later in this chapter, and firewall services, described in [Chapter 19](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch19_html). Most ISPs will rent you a router; however, if you’re technically savvy, you can save yourself some money by buying your own. Routers are also called gateways.
* **Wireless access point** Wireless access points connect Wi-Fi devices, such as laptops, tablets, and smartphones, to your router. Many routers include a wireless access point, or you can buy a separate wireless access point. Wireless access points are described in more detail in [Designing a wireless network](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#designing_a_wireless_network) later in this chapter.
* **Wired Ethernet clients** For the best performance, you can connect desktop PCs and other stationary devices, such as an Xbox 360, to your router with an Ethernet cable.
* **Wireless clients** Wireless clients never connect to the network as fast as wired clients. However, wireless clients aren’t tethered with a cable, which allows you to move around your house and even your yard with a moderately fast Internet connection. Often, wireless networking is fast enough for your purposes. Particularly if you have a strong wireless signal, wireless networks can offer satisfactory performance for tasks such as browsing the web and online gaming.

**IP addresses**

Just like every home has a mailing address and every phone has a phone number, every device connected to the Internet has an IP address. Standard IP addresses, known as IPv4 addresses, use a sequence such as 192.168.4.20.

There are about 4 billion possible IP addresses. That’s a big number, but it’s not nearly big enough, because billions of devices are already connected to the Internet, and we haven’t done a very good job of efficiently assigning the 4 billion addresses we do have. So, if every device needs its own IP address and we don’t have enough addresses, what do we do?

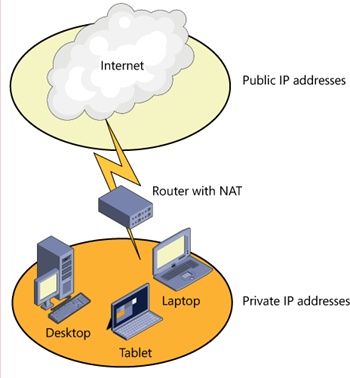
The long-term answer is to implement an entirely new addressing scheme: IPv6. There are about 340,000,000,000,000,000,000,000,000,000,000,000,000 IPv6 addresses, which should last us a while. IPv6 addresses use a sequence such as fe80::95aa:b974:daac:9df9%13. Unfortunately, using the new IPv6 addressing scheme requires a major overhaul of the Internet, and the Internet is a big place, so that overhaul isn’t happening quickly.

**NAT**

The short-term answer to the lack of IPv4 addresses is Network Address Translation (NAT). NAT lets multiple devices share a single Internet connection, and it’s the way the vast majority of devices connect to the Internet today.

You don’t need to be an expert in NAT to set up your home network, but what you should understand is that your ISP is going to give you one valid IP address, known as a public IP address. Your router is going to use that IP address. Every other device on your network is going to use a private IP address.

Private IP addresses have been set aside for use on home and business networks. You can’t access them directly from the Internet, but you can access them across a local area network. These private IP addresses will be 192.168.*something.something*, 10.*something.something.something*, or 172.16-31.*something.something*. [Figure 21-3](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#routers_use_nat_to_allow_many_devices_to) shows how a router with NAT connects the Internet’s public IP addresses to your network’s private IP addresses.



*Figure 21-3. Routers use NAT to allow many devices to share a single public IP address.*

If you’re curious what your IP addresses are, open the Command Prompt desktop app. At the command prompt, type **ipconfig** and press Enter. There’s way too much information in there, but just look for the IPv4 Address line:

Windows IP Configuration

Ethernet adapter Local Area Connection 1:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::95aa:b974:daac:9df9%13

**IPv4 Address. . . . . . . . . . . : 192.168.2.7**

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.2.1

That’s your private IP address, and it’s assigned by your NAT device. It’s the address your device uses to communicate with other devices on your home network.

If you want to know your public IP address, visit [http://ipchicken.com](http://ipchicken.com/). You’ll see the address your ISP has assigned to your router. However, since your router is using NAT, it’s the address every device on the Internet sees when you communicate.

**DHCP**

Odds are that you’ve never manually assigned an IP address to a device. Your ISP uses Dynamic Host Configuration Protocol (DHCP) to assign a public address to your router. In turn, your router uses DHCP to assign private addresses to devices on your home network.

When a network device wakes up, it sends out a message to its local network looking for a DHCP server, and the DHCP server responds with an IP address the device can use. If you don’t have a DHCP server on your network, the device will either completely fail to connect or use APIPA to make up an IP address that looks like 169.254.*something.something*.

**INSIDE OUT: UNDERSTANDING AUTOMATIC PRIVATE IP ADDRESSING (APIPA)**

That 169.254.*something.something* address is an APIPA address. APIPA assigns PCs a random address on the 169.254 network if the PC is configured for automatic IP addressing but no DHCP server is available.

Nobody would ever intentionally use APIPA. APIPA doesn’t use a router, and therefore, PCs with an APIPA address can’t get to the Internet. Without being able to communicate on the Internet, your supply of bacon jokes and cat memes is reduced, rendering your computer useless.

APIPA is designed to let people share files and folders across an ad hoc network. Basically, if you don’t know anything about networking, APIPA at least lets you communicate with other PCs in the same location. Without APIPA, the PCs wouldn’t be able to communicate on the network at all.

During my years of working at ISPs, I had to learn everything there is to know about DHCP. I don’t want you to waste the brain space, but do try to remember these points:

* Computers and devices try to retrieve DHCP addresses when they start. Therefore, restarting everything (possibly including your modem and router) often fixes DHCP problems.
* Your ISP probably uses DHCP to assign an IP address to your router. If your router complains that it can’t contact a DHCP server, make sure your modem is connected and working. Then call your ISP.
* Your router assigns IP addresses to devices on your home network. If a device on your network complains that it could not contact aDHCP server, make sure your router is connected and working.
* If a PC has an APIPA IP address like 169.254.*something.something*, it couldn’t contact the DHCP server. Check your router.
* Because each component of your network receives an address from DHCP when it starts, it’s important to restart devices in the following sequence: modem, router and wireless access point, and finally PCs and other devices. Wait about a minute after restarting each device before restarting the next.

**DNS**

Every computer, including server computers that host websites, has its own IP address, yet you’ve probably never typed an IP address into your web browser. Instead, you type a more friendly name, such as contoso.com.

Domain Name Service (DNS) converts names such as contoso.com to one or more IP addresses. To see it in action, open the Command Prompt desktop app and run the command **nslookup contoso.com**. You’ll see output that resembles the following, which shows the IP address associated with the name contoso.com in bold:

Server: dns.fabrikam.com

Address: 10.8.8.8

Non-authoritative answer:

Name: contoso.com

Addresses: **64.4.6.100**

Many names associated with websites have more than one IP address because the website uses more than one computer to return webpages.

To resolve names to IP addresses, your computer sends queries to its DNS server. DHCP configures the DNS server at the same time it configures your computer’s IP address.

If your DNS server fails, the experience is almost like completely losing your Internet connection. Basically, it’s like borrowing someone else’s phone; it would work just fine if you memorized everyone’s phone number, but it’s not 1995 anymore, and you’re probably accustomed to looking up people by their name.

As with DHCP, there’s a great deal to know about DNS. All you really need to know is:

* DNS translates names to IP addresses.
* DHCP automatically configures PCs with the IP address of a DNS server.

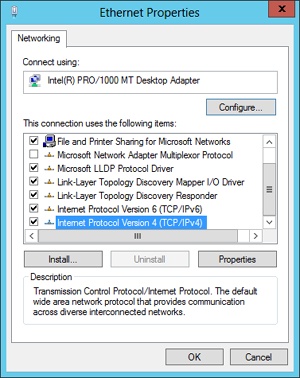
**TROUBLESHOOTING: I CAN’T CONNECT TO THE INTERNET**

If you’re like me, you get a bit frantic when you lose your Internet connection. Most of the time, I just tell people to relax and do something that doesn’t require the Internet, like staring at their useless PC, or frantically refreshing their web browser while shaking their fist at their ISP.

If your Internet seems to be offline, it’s possible that it’s just your DNS server. To test that theory, open a command prompt and type **ping 8.8.8.8**. If you see “Request timed out,” your Internet really is offline. However, if you see “Reply from 8.8.8.8,” your DNS server is simply offline.

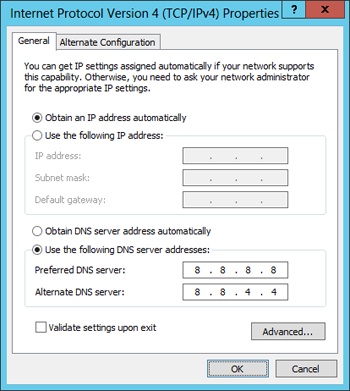
Your ISP typically uses DHCP to configure your computers to connect to the ISP’s closest DNS servers, and that’s usually the best choice. If they’re offline, though, you can configure your PC to connect to a public DNS server to work around the problem. Follow these high-level steps:

1. Open the Network And Sharing Center.
2. Click Change Adapter Settings.
3. Right-click your adapter, and then click Properties.
4. Click Internet Protocol Version 4, as shown in [Figure 21-4](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#manually_configure_ip_settings_by_using_), and then click Properties.



*FIGURE 21-4. MANUALLY CONFIGURE IP SETTINGS BY USING THE ADAPTER’S PROPERTIES DIALOG BOX.*

1. Select Use The Following DNS Server Addresses. In the Preferred DNS Server and Alternate DNS Server boxes, type 8.8.8.8 and 8.8.4.4, as shown in [Figure 21-5](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#use_8888_and_8844_if_your_isps_dns_serve). Click OK. These two addresses are public DNS servers provided by Google, and I chose them only because the numbers are easy to remember. You can find other public DNS servers at <http://pcsupport.about.com/od/tipstricks/a/free-public-dns-servers.htm>.



*FIGURE 21-5. USE 8.8.8.8 AND 8.8.4.4 IF YOUR ISP’S DNS SERVERS ARE UNAVAILABLE.*

1. Click Close.

If DNS really was your only problem, you should now be able to access the Internet.

**Choosing an ISP**

There are many different types of ISPs out there. If you live in a big city, you might have a dozen different options for Internet access. If you live in a rural area, you might have only one or two.

In order from most to least preferred, my personal preference for Internet connection types are:

* **Fiber optic** Incredibly high-speed fiber optic connections are currently available only in limited areas because the ISP has to physically drag expensive cable out to everyone’s house. However, the performance is unmatched. In the United States, Verizon and Google are currently offering fiber optic Internet services in limited locations.
* **Cable** Cable ISPs send Internet communications across the same wiring used for cable TV services. Performance can be very good, but ultimately it depends on the ISP. Most cable TV providers also offer Internet access.
* **DSL** DSL ISPs send Internet communications across dedicated phone circuits. The performance is much slower than offered by fiber optic or cable connections. Local phone companies usually offer DSL-based Internet access.
* **Wireless** Some urban areas have ISPs that offer home Internet access using wireless connections. These can be based on Wi-Fi or they might use the same mobile wireless networks used by your phones.
* **Satellite** Satellite Internet connections advertise high bandwidth, but it takes so long to bounce a signal from your house into orbit and then back down to Earth that the connections suffer from high latency. If you live in a rural area without other offerings, it’s better than nothing.

While I recommend starting at the top of the list and working your way down, not all ISPs are created equal. There are many different factors to consider:

* **Pricing** Cost is important for most of us. Your television or phone provider will often bundle Internet access in with other services, allowing you to save some money.
* **Downstream bandwidth** If you download large files or stream video, downstream bandwidth is very important to you. Besideschoosing the Internet connection with the fastest advertised rates, do some online research to determine how your ISP performs in the real world. Especially during peak hours (typically after working hours), your actual available bandwidth is likely to be much lower than the advertised service rate.
* **Upstream bandwidth** Upstream bandwidth is the speed at which you can upload files to the Internet, and if you play online games or upload videos, it’s very important to you. ISPs usually give you more downstream bandwidth than upstream bandwidth, because most people’s web usage is like having a conversation with an eight year old—you ask a short question and you receive an extremely verbose response that includes a story about turtles and four knock-knock jokes.
* **Reliability and customer service** In the last few years, ISPs have gotten to be almost as reliable as television and phone services. However, some ISPs have more failures than others. Online research and talking to people in your neighborhood are the two best ways to evaluate an ISP’s reliability.
* **Business services** If you run a business, you might need business services. These services tend to include priority customer service, higher bandwidth, static IP addresses (as opposed to DHCP-assigned IP addresses), and permission to host web servers on your premises. Business services often cost much more than personal services.

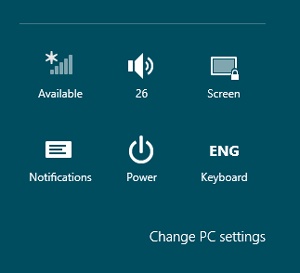
**Connecting Windows 8 to your network**

Windows 8 makes it very easy to connect to your network. If you use a wired Ethernet connection, simply plug in the cable, and Windows will take care of the rest automatically (in most cases). If your PC doesn’t have an Ethernet port, you can connect a USB Ethernet adapter, as shown in [Figure 21-6](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#use_a_usb_ethernet_adapter_to_connect_pc).



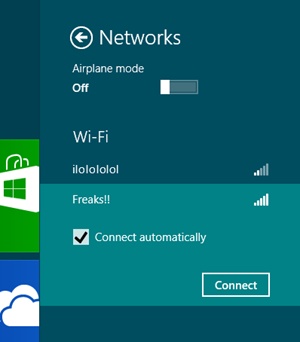
*Figure 21-6. Use a USB Ethernet adapter to connect PCs without wired Ethernet ports.*

If you use a wireless network, you’ll need to choose the network to connect to and type a password. Open the Settings charm. If Windows is not currently connected to a network but one is available, the network icon will display Available, as shown in [Figure 21-7](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#the_settings_charm_displays_available_wh).



*Figure 21-7. The Settings charm displays Available when it can connect to a wireless network.*

Select the network icon. Windows 8 lists every wireless network that it can connect to. Select the name of your wireless network. If this is your home network, select Connect Automatically, as shown in [Figure 21-8](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#windows_8_displays_all_available_wireles). Then select Connect. When prompted, type your wireless network password.



*Figure 21-8. Windows 8 displays all available wireless networks.*

**Manually configuring Windows 8 networking**

For most networks, DHCP will automatically configure your computer’s settings. Some ISPs require you to manually configure IP settings. If you connect to a network that does not use DHCP, ask the network administrator to assign you an IP address and provide you the subnet mask, default gateway, and DNS servers.

Windows 8 (and earlier versions of Windows as well) support an alternate configuration. With an alternate configuration, Windows attempts to retrieve an IP configuration from DHCP, but if it can’t find one, it uses the static IP settings you specify as the alternate configuration.

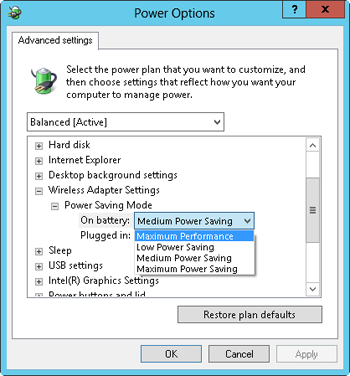
This type of configuration is useful for mobile computers that sometimes connect to networks with a DHCP server but at other times connect to a single network with static IP addressing. For example, your home network almost certainly uses DHCP. However, some business networks still use static IP addressing. If you attempt to connect your PC to your work’s network, it won’t be able to find a DHCP server, and therefore won’t be able to connect to the network.

If you specify an alternate configuration, the PC’s default configuration will still be to use DHCP when you connect to your home network or to hotspots. However, when no DHCP server is available, Windows will apply the alternate configuration. Therefore, if you specify the IP settings required for your static network as the alternate configuration, you will be able to use your PC on both networks without changing any configuration settings each time you connect.

Follow these steps to set up an alternate configuration:

1. Open the Network And Sharing Center.
2. Click Change Adapter Settings.
3. Right-click your adapter, and then click Properties.
4. Click Internet Protocol Version 4, and then click Properties.
5. Select the Alternate Configuration tab and fill in the required fields with the information provided by your ISP or network administrator. The alternate configuration applies static IP settings when a DHCP server isn’t available. You could configure your static IP settings using the General tab, but your PC would use those settings for every network it connected to, preventing it from connecting to most networks that do use DHCP.

[Figure 21-9](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#use_an_alternate_configuration_when_you_) shows a completed alternate configuration.



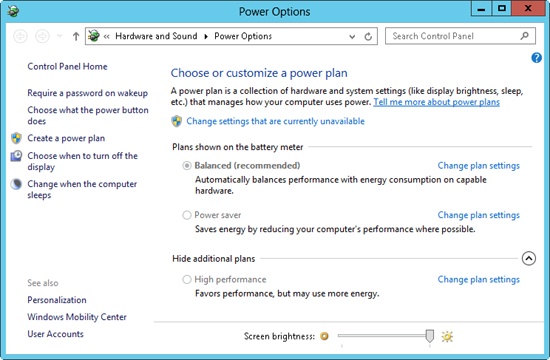
*Figure 21-9. Use an alternate configuration when you roam between multiple networks and one uses static IP settings.*

1. Click OK.
2. Click Close.

If you need to configure IP settings on a desktop computer that only ever connects to a single network, use the General tab of the Internet Protocol Version 4 Properties dialog box to configure the settings. This prevents the computer from connecting to networks that use DHCP, but it can slightly speed up your networking.

**Fine-tuning wireless settings**

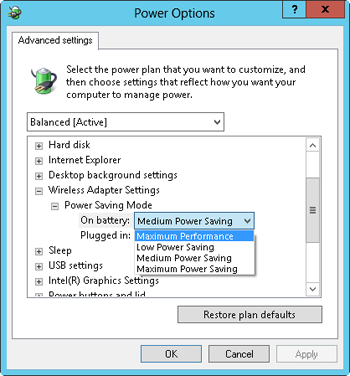
Search Settings for **power** , and then select Power Options. As shown in [Figure 21-10](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#power_options_have_a_profound_effect_on_), Windows displays the power plans available, with the currently selected plan shown in bold.



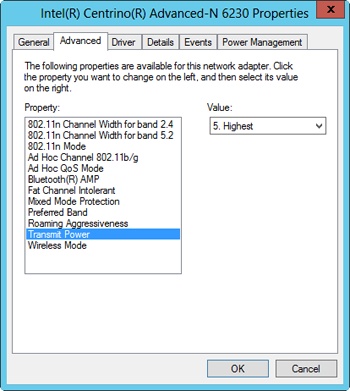
*Figure 21-10. Power options have a profound effect on your wireless network performance.*

Select Change Plan Settings next to your current power plan. Near the bottom of the window, select Change Advanced Power Settings. In the Power Options dialog box, select Change Settings That Are Currently Unavailable. Then expand Wireless Adapter Settings and Power Saving Mode, and set On Battery and Plugged In to the performance level of your choice (as shown in [Figure 21-11](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#the_advanced_power_options_control_how_m)). Naturally, Maximum Performance gives you the best performance but drains your battery the fastest. At times, however, you might not be able to connect to a wireless network unless you set the Power Saving Mode to Maximum Performance.

Many wireless adapters have settings that you can modify from the adapter properties dialog box. To edit these, search Settings for**network connections**. Then select View Network Connections. Right-click your wireless adapter, select Properties, and then click the Configure button to view the adapter’s properties dialog box. The Advanced tab, as shown in [Figure 21-12](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#adapter_driver_settings_often_have_usefu), has settings that are specific to your wireless adapter. These vary too much for me to describe all the settings for you, but if you have unusual circumstances and a solid understanding of wireless networking, you can fine-tune them to improve your wireless performance.



*Figure 21-11. The advanced power options control how much power your wireless adapter receives.*



*Figure 21-12. Adapter driver settings often have useful configuration options.*

**Routers**

Routers are a key component of your network. They connect your PCs both to the Internet and to each other. You can choose from hundreds of different routers, each with different performance, price, security, and usability.

The sections that follow describe how to choose a router and perform the initial configuration.

**Choosing a router**

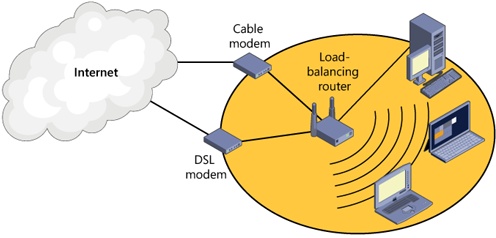
Most people can purchase a router that will suit their needs for less than US$30 (and often, you can spend less than US$20). As with all electronic equipment, I recommend shopping online and choosing products that are well reviewed.

Even the most basic routers offer these features:

* Password-protected management by using a web browser.
* DHCP services to automatically assign IP addresses to PCs and other devices on your home network.
* NAT to allow multiple devices to share a single public IP address.
* Port forwarding or virtual servers to allow you to host a server on your home network.
* Universal Plug and Play (UPnP) to allow apps, such as online games and instant messaging apps, to automatically configure the router to receive incoming connections.

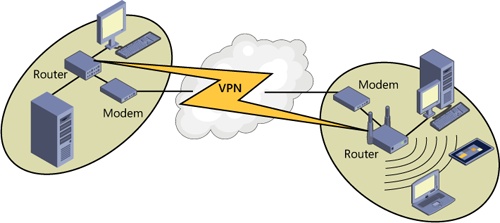
Those features are enough for most users. Some higher-end routers also offer the following features, which might be important to some users:

* **Wireless networking** Some, if not most, new routers include a wireless access point. You can buy a separate router and wireless access point, but you might as well save yourself some setup time and buy a router with wireless networking built in. Look for routers that support Wireless N.
* **Printer sharing** Many routers allow you to connect a USB printer directly to them, and then print from any PC on your network. This feature is very important if you have a USB printer that cannot directly connect to the network and your printer isn’t connected to a desktop PC. If your printer is connected to a desktop PC, you can simply share the printer, as described in [Chapter 24](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch24_html).
* **External drive sharing** Some routers allow you to connect an external hard drive (such as a USB hard drive) and share it across the network. Called *network attached storage* (NAS), this feature can be useful for sharing files between PCs and providing a destination for backing up files when all your PCs are mobile.
* **Web monitoring and filtering** Some routers can record the URLs that devices on the internal network visit or only allow devices to visit an approved list of websites. The monitoring and filtering can be circumvented if one of the devices uses a VPN (unless you also disable VPNs), but it’s harder to bypass than features like Family Safety in Windows 8.
* **Dynamic DNS** Updates DNS servers if your IP address changes. This allows you to assign a DNS name to your home network, such as home.conotoso.com, and have the name automatically updated if your ISP assigns you a new IP address (which they might do from time to time).
* **Quality of Service (QoS)** Prioritizes outgoing traffic based on the computer or app sending it. This is useful for ensuring that a game or server is responsive to other people on the Internet. It typically isn’t useful for prioritizing incoming traffic, so you can’t use it to keep a file transfer from slowing down video streaming, for example.
* **Multiple Internet connections** Some routers, such as the Duolinks SW24 2 Port Dual WAN Load Balancing Router that I use (about US$170), can connect to two different Internet connections and then distribute traffic across both connections for better performance, or automatically switch between the connections when one fails. This can allow you to combine cable and DSL connections, for example, to keep you connected to the Internet if one fails. [Figure 21-13](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#some_routers_allow_you_to_combine_multip) illustrates this scenario. If your ISP is unreliable, or you can’t afford to be without an Internet connection (for example, if you often work from home), multiple links can be very important. Be sure to connect your router and modems to an uninterruptable power supply (UPS) so they don’t go offline if you lose power.



*Figure 21-13. Some routers allow you to combine multiple Internet connections for speed and resiliency.*

* **Virtual private networking (VPN)** Some routers support connecting with a VPN, as shown in [Figure 21-14](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#vpns_extend_your_network_across_the_inte). You can use a VPN to connect to resources on your home network while travelling. VPN capabilities can also securely connect two remote networks without configuring the PCs on those networks. For example, if you have separate networks at home and at a small business that you run, you could connect the networks with a VPN and access resources on each as if they were all in the same building.



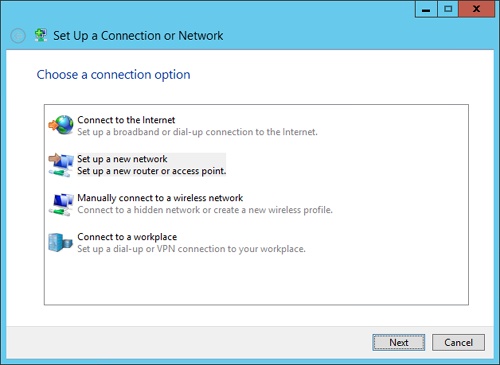
*Figure 21-14. VPNs extend your network across the Internet.*

**Configuring a router or wireless access point**

Sometimes, you can simply plug in your router and have everything work automatically. At other times, you need to configure your router to your ISP’s specifications. If your router supports Wi-Fi, you must configure your router to specify a unique SSID (the name of your wireless network) and to create a network password.

Refer to your router’s manual for instructions on how to configure it. Some routers include a software tool that you need to run, while others simply have you open your browser and visit a local IP address such as [https://192.168.1.1](https://192.168.1.1/).

Windows 8 does have a tool capable of configuring some routers. To try it, open the Network And Sharing Center and then click Set Up A New Connection Or Network. In the wizard, select Set Up A New Network, as shown in [Figure 21-15](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#you_can_use_the_set_up_a_connection_or_n).



*Figure 21-15. You can use the Set Up A Connection Or Network wizard to configure a new router.*

Then follow the prompts that appear. Windows 8 will prompt you for a network name, security key, security level, and encryption type. For detailed information about different Wi-Fi encryption technologies, refer to [Designing a wireless network](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#designing_a_wireless_network) later in this chapter.

After you buy a router and get it connected to your network, you should immediately check to see whether the router manufacturer has released any firmware updates for the router. Most routers do not automatically update their firmware. However, router firmware updates often contain critical security updates to fix serious vulnerabilities that might allow uninvited guests into your home network.

**Choosing home networking technologies**

There are many ways you can connect your PCs and other network devices (such as your smartphone) to your home network. Most people simply need to set up a router with a built-in wireless access point and then connect every device to the wireless network.

Some of us, however, have more demanding needs. For example, if you stream HD video across your network (as described in[Chapter 16](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch16_html)), a wireless network might not be fast enough. If you transfer large files between PCs on your network, you might find wireless networks take an annoyingly long time to copy files.

The sections that follow describe different home networking types.

**Wireless Ethernet**

If a PC or network device doesn’t support wireless networking, you can connect it in a couple of different ways:

* **USB wireless adapters** To connect a desktop PC to a wireless network, connect a USB wireless adapter, which you can buy for less than US$20.
* **Wireless bridges** If a device does not support USB network adapters, such as older gaming systems and digital video recorders (DVRs), but it does have a wired Ethernet connection, use a wireless bridge. Wireless bridges connect to your Wi-Fi network like any wireless client, but they also include a wired Ethernet port. Use an Ethernet cable to connect your device to your wireless bridge, and then configure the wireless bridge to connect to your wireless network. Wireless bridges typically cost between US$40 and $100. For best results, choose a wireless bridge made by the same manufacturer that produced your wireless access point.

**NOTE**

For more information about setting up Wi-Fi, refer to [Designing a wireless network](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#designing_a_wireless_network) later in this chapter.

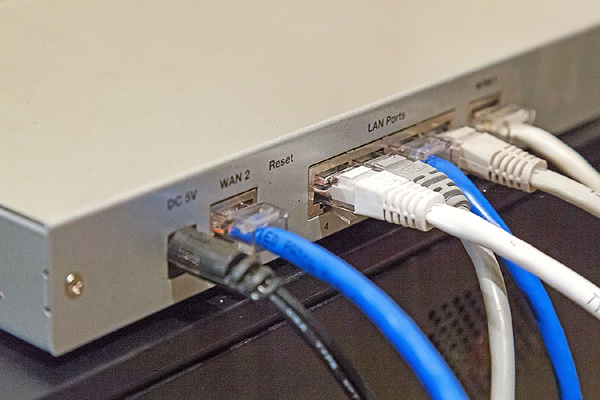
**Wired Ethernet**

Wired Ethernet always provides the best performance. The downside, of course, is the wire. However, for stationary network devices such as desktop PCs, DVRs, Home Theater PCs, and game consoles, wired Ethernet provides the consistent high performance you need.

**NOTE**

***Creating a wired home network*** Watch the video at <http://aka.ms/Win8book/wired>.

To connect wired Ethernet devices, use an Ethernet switch, as shown in [Figure 21-16](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#use_an_ethernet_switch_to_connect_comput). Most routers come with a four-port Ethernet switch built in. If you need more ports, you can purchase inexpensive switches to expand your network. With most modern switches, you can simply connect an Ethernet cable from your router to the new switch. With older switches, you might need to use a special crossover Ethernet cable. Either way, remember that the cable you use to connect your router and your switch will consume one port on each device, so purchase a switch with more ports than you need.



*Figure 21-16. Use an Ethernet switch to connect computers across a wired network.*

There are several wired Ethernet standards: 10 Mbps, 100 Mbps, and 1000 Mbps (also known as gigabit). Faster is always better, so look for switches and adapters that support 1000 Mbps. Faster speeds are backward compatible, so they will work fine with devices designed for 10 Mbps or 100 Mbps networks.

When purchasing Ethernet cables, look for Category 6 Ethernet, commonly called “Cat6.” Category 7 cables are beginning to appear, but they require special connectors that are not yet commonly supported.

What if your home is too large to easily run Ethernet cables to every device? I know, first-world problems, right? There are a few ways you can lay Ethernet cables to connect hard-to-reach places:

* **Within walls** You can run cables through your basement or attic and then raise them or drop them through the hollow spaces in your walls. If you didn’t already know this, I strongly suggest hiring an electrician or alarm company to run your cabling. Be sure to useplenum cable rated for use inside walls and to follow your local building codes to minimize the risk of fire.
* **Under carpeting** You can purchase flat Ethernet cables that can be run under carpeting without making a noticeable bump. For best results, avoid high-traffic areas. Prolonged walking over a cable might damage it, even when protected by carpeting.
* **Along baseboards and doorframes** You can run Ethernet cables along baseboards and doorframes so people don’t trip over them. They can be ugly, however. Purchase far more Ethernet cable than you think you need; many people underestimate the length of cable they need to follow walls and doors.

These are the best solutions. Unfortunately, they’re also quite difficult. Powerline networking, HPNA, and coaxial networking provide much easier ways to extend your wired Ethernet network, but they don’t offer the same high level of performance.

**Ethernet over coax**

With the proper adapter, you can use existing cable TV wires for Ethernet networking within homes. This is perfect if you have cable TV jacks in the rooms where you want to connect your wired Ethernet device.

Basically, you need to purchase a pair of Ethernet over coax adapters. Each adapter has two ports: a coax port and an Ethernet port. Connect one adapter’s Ethernet port to your router and its coax port to a coax connection in your home. Connect the second adapter’s Ethernet port to your wired network device and its coax port to another coax connection in your home. Assuming the two coax ports are connected within your walls, you should be able to use the coax as a reliable and moderately high-speed network extension.

Many homes are prewired for cable TV. However, that doesn’t mean that every single coax connection is plugged in. Often, the coax wires run to a single point in your home (usually near your circuit breaker or fuse box), and only those cables that are currently connected to TVs are plugged in. If your Ethernet over coax adapters can’t communicate, make sure the other end of the cable is connected.

**Ethernet over phoneline**

Though phone cable and Ethernet cable look similar, Ethernet cabling uses eight wires, while telephones use only two wires (though telephone cable might have more wires). Unfortunately, telephone cable simply hasn’t proven to be reliable enough for home networking. At the least, performance doesn’t match options such as wireless networking and home powerline networking.

However, if you need to connect two buildings that have a dedicated phone connection, you can purchase an Ethernet extender kit that works with single-pair wire such as a telephone connection. StarTech makes several products for both single-pair and coaxial cabling. For more information, visit <http://www.startech.com/Networking-IO/Media-Converters/Ethernet-Extenders>.

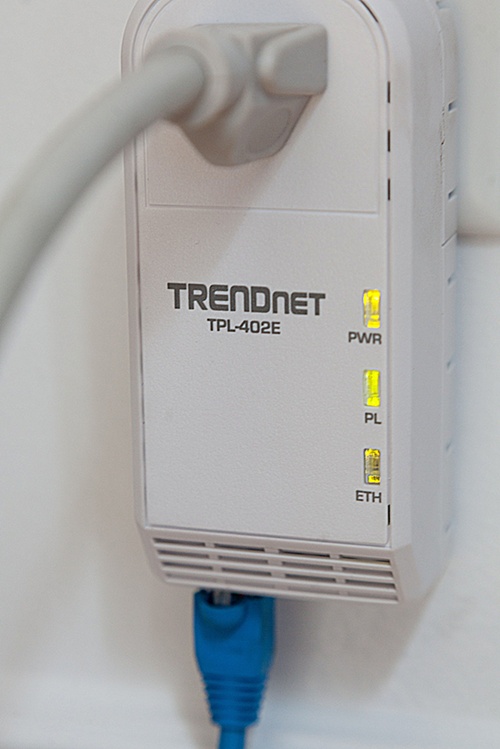
**Powerline networking**

Besides cable TV and phone connections, most modern homes have power connectors in every room. While these cables aren’t designed for network communications, they do closely resemble a wired network: they’re made from copper, distributed throughout your house, well shielded, and all connect to a single hub—your circuit breaker or fuse box.

Unfortunately, they also have dangerously high network current flowing through them, dozens of different non-network devices using them, and links often have fuses, circuit breakers, and other less-than-ideal connectors.

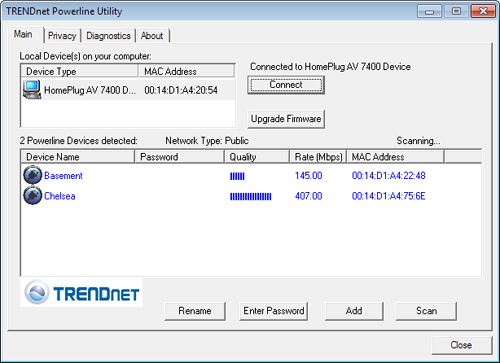
Nonetheless, several companies make powerline networking adapters. As for Ethernet over coax adapters, you always use powerline networking adapters in pairs: one at your router, and the other at the network device you are connecting.

As shown in [Figure 21-17](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#powerline_adapters_turn_your_homes_power), the adapters have two connectors: a wired Ethernet connector and a power plug. Plug it directly into your wall (don’t plug it into a power strip), and then connect the Ethernet adapter to your router or PC. When a pair is active, they automatically connect and allow networking. If you need to connect multiple network devices in one location, you can purchase powerline adapters with multiple Ethernet ports.



*Figure 21-17. Powerline adapters turn your home’s power grid into an Ethernet network.*

[Figure 21-18](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#powerline_networking_performance_varies_) shows the powerline network adapters in my own home and their current performance (as rated by the adapter vendor’s tools). Different homes have different levels of performance. In general, the newer your home is and the better quality the wiring, the better performance you will get. However, I’ve used powerline adapters with success in homes that predate electricity, using retrofit electrical wiring from the 1920s.



*Figure 21-18. Powerline networking performance varies, but it is almost always faster than wireless.*

**Designing a wireless network**

Setting up your wireless network doesn’t have to be complicated; often, your ISP will plug in a wireless access point for you, and all you have to do is type your password.

On the other hand, the setup is often not that simple. Many of us have more demanding network requirements than any standard wireless access point can provide. We need better performance, a bigger range, and better security.

The sections that follow provide detailed information about setting up wireless networks for a variety of different household scenarios.

**NOTE**

***Creating a wireless home network*** Watch the video at <http://aka.ms/Win8book/wireless>.

**Choosing a wireless network standard**

Wireless networks are extremely popular, and wireless network vendors are constantly releasing new wireless standards that offer better range and performance. Fortunately, these wireless standards are backward-compatible, making choosing a standard easy: always buy equipment for the latest standard.

From newest to oldest, and best to worst, common wireless standards include:

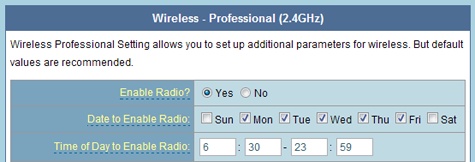
* **802.11n** From 2009, 802.11n offers bandwidth up to about 80 Mbps (though performance of all wireless networks drops with distance and interference). To improve performance, set the channel bandwidth to 20/40 MHz. 802.11n is backward-compatible with 802.11g, 802.11b, and 802.11a. However, performance drops dramatically when an 802.11n wireless access point must communicate with clients using older standards. For best performance, upgrade all of your clients to 802.11n and then set the wireless access point to 802.11n-only mode.
* **802.11g** From 2003, 802.11g offers bandwidth up to about 30 Mbps. 802.11g is backward-compatible with 802.11b devices; however, like 802.11n, 802.11g performs best in 802.11g-only mode.
* **802.11b** From 1999, 802.11b offers bandwidth of about 5 Mbps.
* **802.11a** Technically faster than 802.11b, 802.11a isn’t compatible with most wireless access points and wireless devices, and for that reason should be avoided.

Basically, buy 802.11n gear whenever possible, and know that your older wireless gear will connect to it just fine.

**Choosing a wireless access point**

Like routers, wireless access points (and the wireless access points built into many routers) have a variety of features. You probably don’t need any of these features, but you should be aware of them so that if one of them sounds particularly useful, you can seek out a wireless access point that supports that feature.

* **Guest access** Some wireless access points (particularly those designed for businesses) provide support for a second Wi-Fi network to be used by guests. These guest networks are often unencrypted so that guests do not have to know a password. The wireless access point often requires the user to confirm a usage agreement before accessing the Internet, and may limit the amount of time they use the network connection. In home environments, most people provide their guests access by just telling them the Wi-Fi password, but maybe you don’t trust your friends that much.
* **Weatherproofing** If you frequently use Wi-Fi outdoors, you might want to purchase a wireless access point that you can mount outdoors. Such wireless access points are ruggedized to withstand the weather.
* **Proprietary speed improvements** While all wireless access points support some basic standard, such as 802.11g or 802.11n, some also support proprietary modes that advertise performance increases when you use wireless network adapters from the same brand. These really can offer speed improvements, but you won’t benefit when using the wireless adapters built into your mobile devices.
* **Wireless bridging** Some wireless access points can also function as bridges. Rather than being a wireless access point, they act as a Wi-Fi client, and their wired Ethernet ports allow wired clients to connect to your network across the wireless network. For more information, refer to [Choosing home networking technologies](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#choosing_home_networking_technologies) earlier in this chapter.
* **Scheduling** Even the most serious geeks among us sleep at some point. Some wireless access points support scheduling (as shown in[Figure 21-19](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#some_wireless_access_points_support_sche)), so they shut their radio off at specific times of day or on some days of the week. Not only does this reduce the risk that your network will be abused, but it can save power.



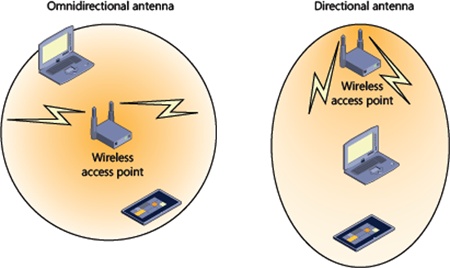
*Figure 21-19. Some wireless access points support scheduling, which can reduce abuse and save power.*

* **Replaceable antennas** Many modern wireless access points have internal antennas for a clean appearance. However, they might not give you ideal reception. If you have a particularly large area to cover or you want to send wireless signals in a specific direction, choose a wireless access point with replaceable antennas, as shown in [Figure 21-20](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#swap_out_the_antennas_on_a_wireless_acce). Most include an omnidirectional antenna that transmits evenly in all directions. You can also install directional antennas that transmit in a specific direction.



*Figure 21-20. Swap out the antennas on a wireless access point to control your signal direction.*

[Figure 21-21](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#omnidirectional_antennas_send_signals_in) compares omnidirectional and directional antennas.



*Figure 21-21. Omnidirectional antennas send signals in all directions, while directional antennas focus the output in one direction.*

**INSIDE OUT: UNDERSTANDING WI-FI PERFORMANCE**

Here are a few facts that will be helpful when you’re optimizing your Wi-Fi performance:

* Directional antennas don’t increase power output, they simply focus it in one direction. Therefore, if you replace an omnidirectional antenna with a directional antenna, you’re adding power in one direction while taking power away in every other direction. To reinforce this important point: no antenna can increase your router’s power output.
* No antenna is perfectly omnidirectional; most transmit power in a relatively flat circle rather than a sphere. Therefore, you might get better performance between any two points by tilting or turning your wireless access point. Have someone with a mobile PC stand where you hope to get more signal, and then make minor adjustments to the wireless access point to optimize the signal at that location.
* Wi-Fi requires two-way communications. If your wireless access point can transmit two miles but your laptop can only transmit 100 feet, your wireless range is still going to be limited to 100 feet.

You can get directional antennas for PCs. Look for USB Wi-Fi adapters that support external antennas. Some stick to the back of a laptop and allow you to point them to a nearby wireless access point. They won’t work well if you’re constantly moving around, but if you’re stationary, they can greatly extend your range.

**Choosing wireless encryption**

Wireless access points support several different types of encryption. Only a handful of them are appropriate for home use, however. In order from most to least preferred, they are:

* **WPA2 (Personal)** The latest and greatest in wireless security, WPA2 isn’t easily cracked. In fact, as of the time of this writing, no widespread crack would be any more effective than a brute force attack, which requires trying every single password combination. Security experts seem to agree that as long as your password isn’t easily guessed, WPA2 passwords cannot be cracked by current computing hardware. Most recent Wi-Fi devices support WPA2, but older wireless devices might not.
* **WEP (128-bit)** The WEP protocol has some cryptographic flaws that make it much easier to crack. Under ideal circumstances, it can be cracked by a skilled attacker in a few minutes. There’s a great deal of information on the Internet talking about how secure 128-bit WEP is, and I even wrote some of it. That information is now outdated; the hackers won, and no version of WEP is secure.
* **WPA (Personal)** The original version of WPA, this version has flaws that make it easily cracked.
* **WEP (64-bit)** Never a good choice for wireless security, 64-bit WEP can often be cracked in a few seconds.

Your wireless access point probably also supports enterprise authentication modes, which might be labeled WPA2-Enterprise, RADIUS, or802.1X. These modes require an authentication infrastructure that most home environments will not have.

If you’re interested in wireless encryption cracking techniques, check out AirCrack-NG (at <http://www.aircrack-ng.org/>) and theBackTrack Linux live CD (at <http://www.backtrack-linux.org/>). It’s important to understand threats to your security so you can protect yourself, but you should never use your skills to attack. I learned that from Mr. Miyagi.

Note that each of these wireless encryption standards authorizes devices using a password. That’s a good choice for home use, but it’s a terrible choice for all but the smallest of businesses. The problem with passwords is that you can’t revoke someone’s access to your wireless network without changing the password, and changing the password requires you to update every wireless device. It’s a nuisance, but if you give someone your wireless network password and you no longer trust them, you’ll need to change the password on your wireless access point and then reconfigure every single wireless device. Yes, it’s one more reason not to break up with your girlfriend.

**INSIDE OUT: WIRELESS MAC FILTERING**

Wireless access points support MAC address filtering. MAC addresses are hardware addresses that uniquely identify every network adapter. Whereas an IP address identifies a host on the Internet, a MAC address identifies a host only on the local network.

You can see the MAC address of your PC by opening a command prompt and then running the command **ipconfig /all**. Look for the Physical Address line, as the following output demonstrates:

C:\>ipconfig /all

Ethernet adapter Local Area Connection 1:

Connection-specific DNS Suffix . :

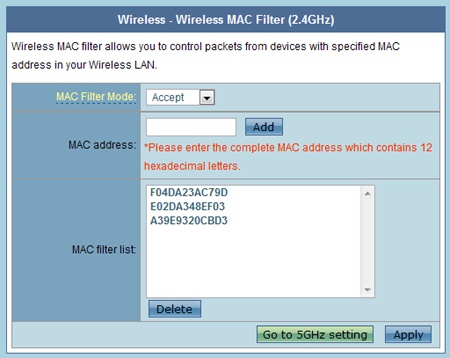
Description . . . . . . . . . . . : RTL8168D/8111D Gigabit Ethernet

**Physical Address. . . . . . . . . : F0-4D-A2-3A-C7-9D**

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

With MAC filtering, you look up the MAC address of every wireless adapter on your network and type them into your wireless access point, as shown in[Figure 21-22](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#wireless_mac_filtering_doesnt_improve_se). Then, you can enable MAC filtering, and your wireless access point will ignore requests from any other adapter.



*FIGURE 21-22. WIRELESS MAC FILTERING DOESN’T IMPROVE SECURITY ENOUGH TO JUSTIFY THE INCONVENIENCE.*

In theory, this means that only clients with the network adapters you approve can connect to your wireless network. This would provide near-perfect wireless authentication without requiring a password, except for one critical flaw: MAC addresses are broadcast unencrypted. Therefore, any moderately sophisticated attacker could identify valid MAC addresses and impersonate them.

With that said, MAC address filtering can theoretically improve security by making it more difficult to connect to your wireless access point. However, it’s a nuisance that isn’t typically worth the effort. After all, every time you get a new computer, replace a network adapter, or have a friend over, you have to look up the 12-digit hexadecimal MAC address and configure your wireless access point before they can connect. Security is always a compromise between protection and convenience, and in the case of MAC filtering, the trade-off isn’t typically worth it.

**Choosing a SSID**

The SSID is the name of your wireless network. It appears when you browse networks, but it has no impact on security. Wireless access points allow you to hide a SSID, but there’s no security benefit, and a hidden SSID is more difficult to connect to.

Choosing a proper SSID is very important, however, because all your neighbors can see it. Some suggestions include:

* TurnYourMusicDown
* PartyFriday8pmBringBeer
* PickUpAfterUrDog
* Honeypot
* PrettyFly4AWiFi
* iH8uChet

You get the idea (and so does my neighbor, Chet, who never brings beer).

**INSIDE OUT: WHAT IS A HONEYPOT?**

In network security, a honeypot is a trap. It’s like a geeky version of those stings and undercover operations you see in police shows.

For example, a security engineer might set up a honeypot on their network. The honeypot looks exactly like a real computer to other users connected to the network. However, nobody knows about it, and it serves no useful function to legitimate users.

The honeypot records every detail of incoming network requests. If anyone attempts to connect to the honeypot, the security engineer knows they’re up to no good, because there’s no legitimate reason to be connecting to this computer. While the security engineer could monitor any computer on the network for attacks, it’s particularly easy to monitor a honeypot because the security engineer doesn’t have to filter out legitimate requests from potentially malicious requests—every connection request (except his own) is unwanted.

Honeypots can often be configured to impersonate vulnerable computer systems. For example, they might appear to be a PC running Windows XP without important security updates. An attacker would see this as tempting and attempt to break into it. Meanwhile, the honeypot is recording the attacker’s every action, allowing the security engineer to identify the techniques the attacker is using, gather evidence that might be admissible in court, and possibly even personally identify the attacker so that a law enforcement agency could take action.

Wireless honeypots exist, and they’re a bit scary. They appear to be a wireless access point, and they might even give people who connect to them Internet access. If someone connects to the honeypot, they’re obviously an uninvited guest, since nobody would ever invite anyone to use a honeypot. Once the uninvited guest connects to the honeypot, it’s possible for the security engineer to use special equipment to track the client’s wireless signal back to the origin, which is the attacker who is physically within range of the honeypot’s wireless signal. It’s one of the few cases in network security where you can physically confront an attacker.

You wouldn’t ever set a honeypot’s SSID to “Honeypot,” because then an attacker would know it was a trap. However, by naming a legitimate Wi-Fi network Honeypot, you might scare away potential attackers who think it’s a trap. Anyway, I’m breaking my own personal rule by explaining a joke, buthoneypots are too much fun to not talk about.

**Providing wireless access throughout your house**

Oh, the burdens of the first-world lifestyle: your house is so large that Wi-Fi doesn’t work well, or at all, in some places. Until some philanthropist finally takes pity on us and founds a charitable organization to offer relief to those of us with subsatisfactory Wi-Fi performance, we’ll have to get our hands dirty to get the coverage we need.

The first step to getting coverage throughout your house is choosing the right location for your wireless access point. Your ISP probably plugged it in next to your router, which might be in your basement or some other infrequently used part of your house. You should move it to a central part of your house. If you can’t run an Ethernet cable from your modem to where you would like your wireless access point, then use powerline networking or Ethernet over coax, as described earlier in this chapter.

Try to position your wireless access point away from interfering objects. The worst interferers are large metal objects such as filing cabinets and refrigerators. Power cords are bad, too.

If you want to use your PC outside (which is a great idea; I’m writing this on my patio), be aware that window screens completely scramble wireless signals. To get coverage in your backyard, position your wireless access point near an outside wall or window, but not near any screens. Screens have this really confusing effect on wireless signals: your PC will show that it has a strong connection to the wireless network, but your performance will be terrible or unreliable.

**Using two wireless access points**

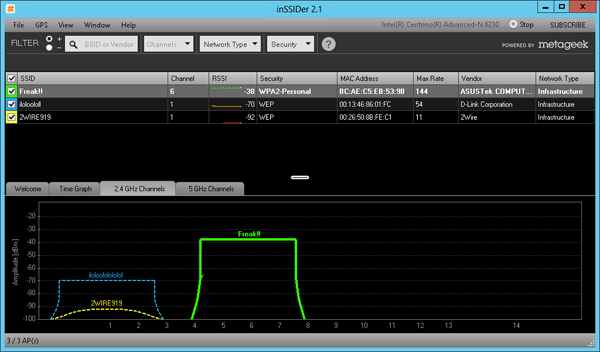
If you followed the advice in the previous section but still don’t have coverage, you can add a second wireless access point in a different part of your house and connect it to your router using powerline networking or Ethernet over coax.

If you set up a second wireless access point using a different SSID, your house will have two wireless networks. That’s not great, though. Not only will you need to configure devices to connect to both networks, but your wireless devices won’t always connect to the strongest network in the house; they’ll connect to the network they were most recently connected to. So, you might have a connection with five bars available, but Windows will stay connected to the distant Wi-Fi network with just one bar. You could manually switch networks as you moved around your house, but that’s a nuisance.

Here’s a better way to configure that second wireless access point:

* Change its IP address to something other than the IP address of your first wireless access point or your router, but keep it on the same network. For example, if your first wireless access point has the IP address 192.168.1.1, change the IP address for the second wireless access point to 192.168.1.2 or 192.168.1.3. As long as you change just the last number, you should be okay. Don’t use the same IP address as any other device on your network, however.
* Turn off DHCP on the second wireless access point. Wireless clients will still get their IP addresses from your router.
* Set the second wireless access point to a different channel. In the United States, we use channels 1, 6, and 11. So, you could set your first wireless access point to 11, and your second to 1 or 6. If a neighbor has a wireless access point that might interfere, it would be good to avoid that channel, too.
* Choose the same security settings, including the key.
* Set the SSID to the same name as your first wireless network.

Use inSSIDer, available at <http://www.metageek.net/products/inssider/>, to analyze the performance of your Wi-Fi networks and to determine the channels your neighbors are using. As shown in [Figure 21-23](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#use_inssider_to_analyze_wireless_network), inSSIDer displays the relative signal strength of different visible Wi-Fi networks. If you are attempting to improve the wireless strength at a specific location, this app is a great way to determine how signal strength changes as you move or tilt the wireless access point.



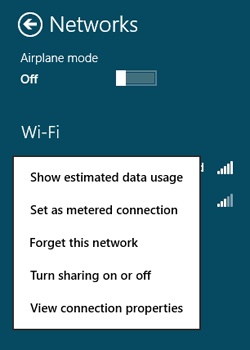
*Figure 21-23. Use inSSIDer to analyze wireless networks around you.*

**Managing wireless networks**

Windows 8 does not include the Manage Wireless Networks tool that you might be familiar with in Windows 7. However, it provides some basic wireless networking management using commands on a shortcut menu.

Open the Settings charm, and then select the network icon. On the Networks page, right-click a network name to view the menu shown in[Figure 21-24](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#right-click_networks_to_access_additiona). As a reminder, on the touch interface, you can right-click by holding your finger on the screen until a box appears.

Choose Forget This Network to prevent Windows 8 from automatically reconnecting to the network in the future. If you ever want to connect to the network, you’ll need to select it and then retype the wireless password.



*Figure 21-24. Right-click networks to access additional settings.*

**TROUBLESHOOTING: I CHANGED THE SETTINGS ON MY WIRELESS ACCESS POINT, AND NOW I CAN’T CONNECT**

If you ever tweak the settings on your wireless access point and find you can’t connect, right-click the network and click Forget This Network. Then reconnect. This is often enough to allow you to connect in the future without problems.

Showing your data usage is a good way to track the cost of connections that charge per gigabyte, such as a connection from a mobile network provider. Note that it’s only accurate if you remember to reset the connection on the same day that your billing cycle restarts.

Windows 8 is a bit more conservative with its network usage on metered networks. Therefore, if a wireless provider is charging you by the amount you use a network, you should right-click it and then select Set As Metered Connection.

**Web applications**

Most individuals and small businesses need a few different web services beyond simply browsing the web. The sections that follow discuss the most important web services.

**Email**

Everyone needs email, and there are dozens of different companies quite excited to provide an email address for you. Microsoft is one such company, and millions of people use the free Hotmail service (also known as Outlook.com). Since you probably already have an account, Facebook also allows you to receive email by sending messages in the format *<username>*@facebook.com.

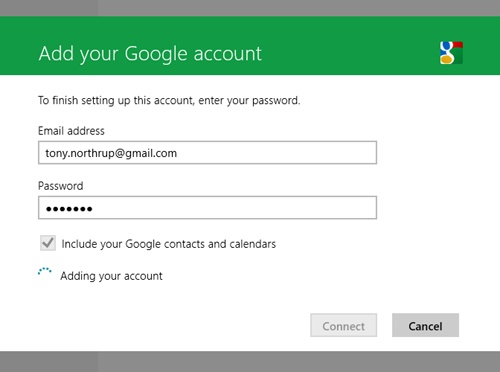
However, I don’t recommend any service that requires you to use its domain name. Using Hotmail as an example, you’ll be required to use an email address such as *<yourname>*@hotmail.com. If you ever discover a better email service, you then have to tell all your friends about your new address, and that’s a nuisance.

I recommend getting your own domain name so that you aren’t tied to another organization. For example, even though you could contact me at [tony.northrup@facebook.com](mailto:tony.northrup@facebook.com), the email address on my business card is [tony@northrup.org](mailto:tony@northrup.org).

Getting my last name as a domain name isn’t that hard. It requires registering a custom domain name, which costs about $10 a month. Dozens of different domain name registrars, such as godaddy.com, will register a domain name for you and even host your email. Then, you simply need to configure the Mail client in Windows 8 with the email server settings the registrar provides. Your domain name registrar will probably charge you for email services, however.

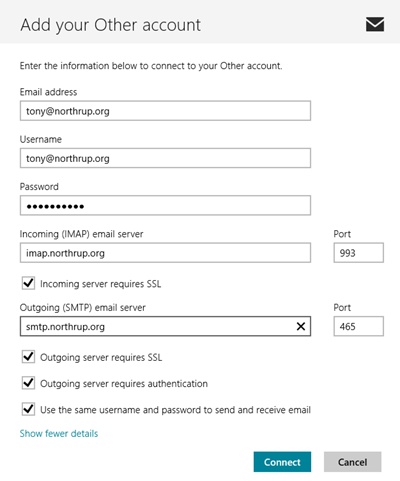
**Configuring Mail**

The first time you launch Mail, it prompts you for information it needs to connect to your mail server. At a minimum, Mail needs to gather your email address and password, as shown in [Figure 21-25](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#mail_can_usually_connect_using_just_your).



*Figure 21-25. Mail can usually connect using just your email address and password.*

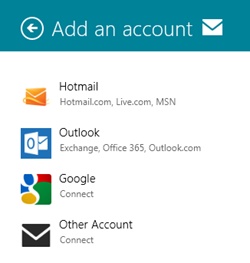
Mail actually needs much more information to connect to your account, including your user name, your IMAP server address, and yourSMTP server address. It’s pretty smart, though, and can usually figure out those details without making you look them up. If Mail is unable to determine your settings, it will prompt you, as shown in [Figure 21-26](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#mail_might_need_to_prompt_you_for_additi). Ask your system administrator for the missing details, or simply search the Internet for “*<mail service>* IMAP SMTP server.”



*Figure 21-26. Mail might need to prompt you for additional information.*

**Adding extra mail accounts**

Mail can download your email from all your different accounts. Though Mail prompts you to configure your first email account, you need to use the Settings charm to add more accounts. After opening the Settings charm with Mail open, select Accounts, select Add An Account, and then select your account type, as shown in [Figure 21-27](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#mail_can_access_all_of_your_email_accoun). Use the Hotmail link for Live and MSN mail. Use the Outlook link if you use Outlook.com or Office 365, or you’re connecting to a business’s email system and it uses Microsoft Exchange Server for email. If you use Gmail or Google Apps, select the Google link. If none of these apply, or you’re not sure, select Other Account.



*Figure 21-27. Mail can access all of your email accounts.*

Rather than configuring Mail with more than one account, consider forwarding all your mail to a single account. For more information, read [Centralizing your email services](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#centralizing_your_email_services) later in this chapter.

**Learning to live without POP**

Mail in Windows 8 can download your messages using only IMAP. That’s different from the mail clients included with earlier versions of Windows, which supported both IMAP and POP (also called POP3).

You’re not missing much, because POP is an outdated protocol that isn’t well suited to the modern world. POP downloads messages from the server to the local computer, creating a copy of the message. Most POP clients also remove the message from the server. Creating a local copy of every email message creates a couple of challenges:

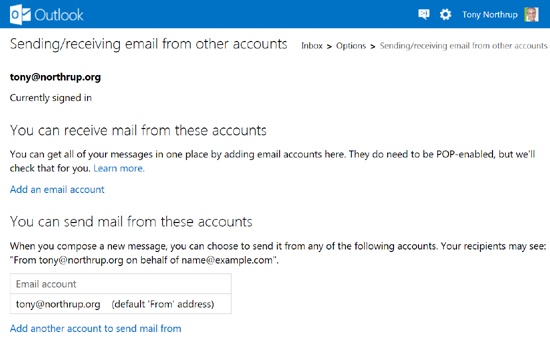
* It fills up your PC’s drive. Over time, mail storage can consume many, many gigabytes of free space (especially if you don’t regularly clean your spam folder).
* It takes longer to download. When you use IMAP, mail doesn’t download attachments until after you view the message. When you use POP, mail has to download the entire message, including all attachments. You’ll discover how frustrating this is the first time you’re waiting for an important message and someone sends you a 10 megabyte (MB) picture of their cat that you have to watch download for several minutes.
* It doesn’t allow you to synchronize messages across multiple devices. Most people check their email from several places, including their smartphone and their PC. If you use POP, Mail will remove the messages from the server, preventing you from reading them from your phone.

**Centralizing your email services**

Now that you hate POP as much as I do, what can you do if your mail server doesn’t support IMAP? That should be an extremely rare situation, but if that’s the case for you, you can use an email service that downloads messages from your POP server.

This is also useful if you regularly check more than one email account. Instead of separately logging in to each email account, forward all your messages to a single account.

For example, you can configure Windows Live Hotmail or Outlook online to download messages from your POP server. Then, you can configure Mail (and your other email clients) to connect to Hotmail or Outlook online. To do this, open your account settings and then select Sending/Receiving Email From Other Accounts. As shown in [Figure 21-28](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#hotmail_outlook_and_other_email_services), you can add accounts to check email and use different accounts to send email.



*Figure 21-28. Hotmail, Outlook, and other email services can move messages from all your accounts to a single server.*

Other email services, including Office 365, Gmail, and Google Apps, support downloading email from other services.

**File hosting**

Email attachments have size limits, and those size limits depend on both the sender and the recipient’s email servers. So, there’s no single size limit.

Most email services can send messages with attachments up to 8 MB in size. Some allow larger files, while some only allow smaller files.

When you need to send larger files, you’ll need file hosting. The Microsoft solution to this is SkyDrive, as discussed in [Chapter 13](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch13_html). SkyDrive is integrated throughout Windows 8, making it simple to share large files across the Internet. [Chapter 13](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch13_html) also discusses third-party file-hosting alternatives.

**Web hosting**

Many small businesses also need web hosting. Individuals often needed web hosting in the past, but today, sites like Facebook.com and YouTube.com take care of most people’s hosting needs.

If you also run a small business, you might still need to host a website. If you’re not familiar with setting up a website, hire a website designer from a site such as [elance.com](http://elance.com/). They can handle everything for you.

If you’re familiar with HTML and CSS, or you want to be, you can simply find a web hosting provider. I recommend most small businesses seek out a WordPress hosting provider. WordPress is a very popular and free web hosting application that supports thousands of different plug-ins that add features to your website. WordPress is perfect for making mostly static websites, but it also has amazing blogging capabilities if you plan to regularly add new content to your website.

Naturally, you should purchase your own domain name (as discussed in the section [Email](http://ezproxy.madisoncollege.edu:2097/9780735670518/ch21_html#email) earlier in this chapter) for your business website. Your domain name registrar will try very hard to sell you web hosting services, but they’re rarely the best value. You can host your website with any provider, and although the steps you take to configure your site are outside the scope of this book, your web designer should have no problem setting it up.