How WiFi Works

If you've been in an airport, coffee shop, library or hotel recently, chances are you've been right in the middle of a wireless network. Many people also use wireless networking, also called WiFi or 802.11 networking, to connect their computers at home, and some cities are trying to use the technology to provide free or low-cost Internet access to residents. In the near future, wireless networking may become so widespread that you can access the Internet just about anywhere at any time, without using wires.

WiFi has a lot of advantages. Wireless networks are easy to set up and inexpensive. They're also unobtrusive -- unless you're on the lookout for a place to watch streaming movies on your tablet, you may not even notice when you're in a hotspot. In this article, we'll look at the technology that allows information to travel over the air. We'll also review what it takes to create a wireless network in your home.

First, let's go over a few WiFi basics.

What Is WiFi?

A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:

1. A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
2. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

The radios used for WiFi communication are very similar to the radios used for walkie-talkies, cell phones and other devices. They can transmit and receive radio waves, and they can convert 1s and 0s into radio waves and convert the radio waves back into 1s and 0s. But WiFi radios have a few notable differences from other radios:

- They transmit at frequencies of 2.4 GHz or 5 GHz. This frequency is considerably higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to carry more data.
- They use 802.11 networking standards, which come in several flavors:
- **802.11a** transmits at 5 GHz and can move up to 54 megabits of data per second. It also uses **orthogonal frequency-division multiplexing** (OFDM), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.
- **802.11b** is the slowest and least expensive standard. For a while, its cost made it popular, but now it's becoming less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 megabits of data per second, and it uses **complementary code keying** (CCK) modulation to improve speeds.
- **802.11g** transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.
- **802.11n** is the most widely available of the standards and is backward compatible with a, b and g. It significantly improved speed and range over its predecessors. For instance, although 802.11g theoretically

moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. 802.11n can transmit up to four streams of data, each at a maximum of 150 megabits per second, but most routers only allow for two or three streams.

- **802.11ac** is the newest standard as of early 2013. It has yet to be widely adopted, and is still in draft form at the **Institute of Electrical and Electronics Engineers (IEEE)**, but devices that support it are already on the market. 802.11ac is backward compatible with 802.11n (and therefore the others, too), with n on the 2.4 GHz band and ac on the 5 GHz band. It is less prone to interference and far faster than its predecessors, pushing a maximum of 450 megabits per second on a single stream, although real-world speeds may be lower. Like 802.11n, it allows for transmission on multiple spatial streams -- up to eight, optionally. It is sometimes called **5G WiFi** because of its frequency band, sometimes **Gigabit WiFi** because of its potential to exceed a gigabit per second on multiple streams and sometimes **Very High Throughput (VHT)** for the same reason.
- Other 802.11 standards focus on specific applications of wireless networks, like wide area networks (WANs) inside vehicles or technology that lets you move from one wireless network to another seamlessly.
- WiFi radios can transmit on any of three frequency bands. Or, they can "frequency hop" rapidly between the different bands. Frequency hopping helps reduce interference and lets multiple devices use the same wireless connection simultaneously.

As long as they all have wireless adapters, several devices can use one router to connect to the Internet. This connection is convenient, virtually invisible and fairly reliable; however, if the router fails or if too many people try to use high-bandwidth applications at the same time, users can experience interference or lose their connections. Although newer, faster standards like 802.11ac could help with that.

Next, we'll look at how to connect to the Internet from a WiFi hotspot.

WiFi Hotspots

A **WiFi hotspot** is simply an area with an accessible wireless network. The term is most often used to refer to wireless networks in public areas like airports and coffee shops. Some are free and some require fees for use, but in either case they can be handy when you are on the go. You can even create your own mobile hotspot using a cell phone or an external device that can connect to a cellular network. And you can always set up a WiFi network at home.

If you want to take advantage of public WiFi hotspots or your own home-based network, the first thing you'll need to do is make sure your computer has the right gear. Most new laptops and many new desktop computers come with built-in wireless transmitters, and just about all mobile devices are WiFi enabled. If your computer isn't already equipped, you can buy a **wireless adapter** that plugs into the PC card slot or USB port. Desktop computers can use USB adapters, or you can buy an adapter that plugs into the PCI slot inside the computer's case. Many of these adapters can use more than one 802.11 standard.

Once you've installed a wireless adapter and the drivers that allow it to operate, your computer should be able to automatically discover existing networks. This means that when you turn your computer on in a WiFi hotspot, the computer will inform you that the network exists and ask whether you want to connect to it. If you have an older computer, you may need to use a software program to detect and connect to a wireless network.

Being able to connect to the Internet in public hotspots is extremely convenient. Wireless home networks are convenient as well. They allow you to easily connect multiple computers and to move them from place to place without disconnecting and reconnecting wires. In the next section, we'll look at how to create a wireless network in your home.

Building a Wireless Network

If you already have several computers networked in your home, you can create a wireless network with a **wireless access point**. If you have several computers that are not networked, or if you want to replace your Ethernet network, you'll need a wireless router. This is a single unit that contains:

A wireless router allows you to use wireless signals or Ethernet cables to connect your computers and mobile devices to one another, to a printer and to the Internet. Most routers provide coverage for about 100 feet (30.5 meters) in all directions, although walls and doors can block the signal. If your home is very large, you can buy inexpensive range extenders or repeaters to increase your router's range.

As with wireless adapters, many routers can use more than one 802.11 standard. Normally, 802.11b routers are slightly less expensive than others, but because the standard is older, they're also slower than 802.11a, 802.11g, 802.11n and 802.11ac routers. 802.11n routers are the most common.

Once you plug in your router, it should start working at its default settings. Most routers let you use a Web interface to change your settings. You can select:

- **The name of the network, known as its service set identifier (SSID)** -- The default setting is usually the manufacturer's name.
- **The channel that the router uses** -- Most routers use channel 6 by default. If you live in an apartment and your neighbors are also using channel 6, you may experience interference. Switching to a different channel should eliminate the problem.
- **Your router's security options** -- Many routers use a standard, publicly available sign-on, so it's a good idea to set your own username and password.

Security is an important part of a home wireless network, as well as public WiFi hotspots. If you set your router to create an open hotspot, anyone who has a wireless card will be able to use your signal. Most people would rather keep strangers out of their network, though. Doing so requires you to take a few security precautions.

It's also important to make sure your security precautions are current. The Wired Equivalency Privacy (WEP) security measure was once the standard for WAN security. The idea behind WEP was to create a wireless security platform that would make any wireless network as secure as a traditional wired network. But hackers discovered vulnerabilities in the WEP approach, and today it's easy to find applications and programs that can compromise a WAN running WEP security. It was succeeded by the first version of WiFi Protected Access (WPA), which uses Temporal Key Integrity Protocol (TKIP) encryption and is a step up from WEP, but is also no longer considered secure.

To keep your network private, you can use one or both of the following methods:

- **WiFi Protected Access version 2** (WPA2) is the successor to WEP and WPA, and is now the recommended security standard for WiFi networks. It uses either TKIP or Advanced Encryption Standard (AES) encryption, depending upon what you choose at setup. AES is considered the most secure. As with WEP and the initial WPA, WPA2 security involves signing on with a password. Public hotspots are either open or use any of the available security protocols, including WEP, so use caution when connecting away from home. WiFi Protected Setup (WPS), a feature that ties a hard-coded PIN to the router and makes setup easier, apparently creates a vulnerability that can be exploited by hackers, so you may want to turn off WPS if possible, or look into routers that do not have the feature.
- **Media Access Control** (MAC) address filtering is a little different from WEP, WPA or WPA2. It doesn't use a password to authenticate users -- it uses a computer's physical hardware. Each computer has its own unique

MAC address. MAC address filtering allows only machines with specific MAC addresses to access the network. You must specify which addresses are allowed when you set up your router. If you buy a new computer or if visitors to your home want to use your network, you'll need to add the new machines' MAC addresses to the list of approved addresses. The system isn't foolproof. A clever hacker can **spoof** a MAC address -- that is, copy a known MAC address to fool the network that the computer he or she is using belongs on the network.

You can also change other router settings to improve security. For instance, you can set it to block WAN requests to keep the router from responding to IP requests from remote users, set a limit to the number of devices that can connect to your router and even disable remote administration so that only computers plugged directly into your router can change your network settings. You should also change the Service Set Identifier (SSID), which is your network name, to something other than the default so that hackers can't immediately tell what router you are using. And selecting a strong password never hurts.

Wireless networks are easy and inexpensive to set up, and most routers' Web interfaces are virtually self-explanatory. For more information on setting up and using a wireless network, check out the links on the next page.

Author's Note: How WiFi Works -- Bernadette Johnson

I worked on an update to the content of this article, and I think it's amazing that in a few scant years we've gone from mostly wired to mostly wireless data transfer, via WiFi in our homes and public places, as well as cell phones. Of course, a lot of the infrastructure still uses wires, but the fact that we can communicate via both radio waves and electricity traveling through wires is pretty incredible. A big thanks to the inventors of the telegraph and every communication innovation that came after.

I remember the days when most mere mortals didn't have modems and couldn't get on the net, even if they had computers. Perhaps I'm projecting my experiences onto everyone else, but when I was a kid, our computer was this tool we used in isolation, save for the times friends would come over to play video games. My computer programmer aunt was the only person I knew who had a modem. It was the type where you put your phone directly onto a cradle and some crazy analog communication went on.

When modems became widespread, they were still these clunky external things that we hooked up to our computers to noisily and slowly dial up to a larval Internet. They tied up the phone line, so you couldn't keep them connected indefinitely, and if you didn't want to run up an astronomical phone bill you had to make sure you were using a phone number for a local access point. Modems went internal and got a bit faster, but now dial-up is going the way of the dodo bird due to the ubiquity of affordable broadband services in the home like DSL and cable.

With an astounding jump in bandwidth, and the ability of our computers to connect wirelessly, many of us are online all the time, and free to compute all over the house or even away from home. I've surfed the net, streamed shows and downloaded books while on vacation via hotel, airport and other hotspots. And I fall asleep nightly streaming Netflix on my WiFi-only tablet at home. Which is great, aside from the fact that I really should be resting. But insomnia and information overload are topics for another time.

Sources

- Borisov, Nikita, Ian Goldberg and David Wagner. "Security of the WEP algorithm." University of California, Berkeley. (Aug. 7, 2008) http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Bouvier, Dan. "Get The Jump On Next-Gen Enterprise-Class Wireless Access Points." Electronic Design. February 12, 2009, Volume 57, Issue 3, Pages 45-48. (April 14, 2013)
- Bradley, Tony. "802.11ac 'Gigabit Wi-Fi': What You Need to Know." PC World. April 27, 2012. (April 21, 2013) http://www.pcworld.com/article/254616/802_11ac_gigabit_wi_fi_what_you_need_to_knobraw.html

- Broida, Rick. "When Is It Time to Replace Your Router?" PC World. January 2013, Volume 31, Issue 1, Page 92. (April 14, 2013)
- Dipert, Brian. "802.11n: Complicated and About to Become Even Messier." EDN. May 28, 2009, Volume 54, Issue 10, Pages 6. (April 14, 2013)
- Fleisman, Glenn. "Ports and Networks." Macworld. January 2011, Volume 28, Issue 1, Pages 46-48. (April 14, 2013)
- Gann, Roger. "How to Secure a Wireless Network." Tech Radar. December 6, 2012. (April 21, 2013) http://www.techradar.com/us/news/internet/how-to-secure-a-wireless-network-1075710
- Hachman, Mark. "Netgear to Ship Next-Gen 802.11ac Wi-Fi Router in May." PC Magazine. April 2012. (April 14, 2013)
- Hall, David A. "Underneath the Hood of 802.11AC." Microwave Journal. December 2011, Volume 54, Issue 12, Pages 46-52. (April 14, 2013)
- Huang, Pi. "Understanding IEEE 802.11ac VHT Wireless." Electronic Design. July 16, 2012. (April 22, 2013) huhttp://electronicdesign.com/communications/understanding-ieee-80211ac-vht-wireless
- Geier, Jim. "802.11 WEP: Concepts and Vulnerability." Wi-Fi Planet. June 20, 2002. (Aug. 6, 2008) http://www.wi-fiplanet.com/tutorials/article.php/1368661
- IEEE. (Aug. 6, 2008) http://www.ieee.org
- IEEE. "Get IEEE 802: Local and Metropolitan Area Network Standards - 802.11." (April 14, 2013) http://standards.ieee.org/getieee802/download/802.11-2012.pdf
- IEEE. "IEEE Project - P802.11ac - IEEE Draft Standard." (April 21, 2013) http://standards.ieee.org/develop/project/802.11ac.html
- IEEE. "IEEE Standard for Information Technology -- Telecommunications and Information Exchange Between Systems -- Local and Metropolitan Area Networks -- Specific requirements." (Aug. 6, 2008) http://standards.ieee.org/getieee802/download/802.11-2007.pdf
- Johnson, Dave. "Wi-Fi Myths That Can Compromise Computer Security." CBS News. January 8, 2013. (April 21, 2013) http://www.cbsnews.com/8301-505124_162-57562362/wi-fi-myths-that-can-compromise-computer-security/
- Mathias, Craig. "802.11ac: The Next Wi-Fi Standard." PC World. June 2012, Volume 30, Issue 6, Page 18. (April 14, 2013)
- Miller, Lawrence C. "Wireless Security Protocols: WEP, WPA, and WPA2 (from 'Home Networking Do-It-Yourself For Dummies')." April 2011. (April 21, 2013) http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html
- Ngo, Dong. "5G Wi-Fi (802.11ac) explained: It's cool." CNET. May 18, 2012. (April 21, 2013) http://news.cnet.com/8301-17938_105-57437317-1/5g-wi-fi-802.11ac-explained-its-cool/
- Pash, Adam. "How to Crack a Wi-Fi Network's WPA Password with Reaver." Life Hacker. January 9, 2012. (April 21, 2013) http://lifehacker.com/5873407/how-to-crack-a-wi+fi-networks-wpa-password-with-reaver
- Rash, Wayne. "802.11n: The Wi-Fi Revolution Nobody Noticed." eWeek. November 23, 2009, Volume 26, Issue 20, Pages 14-15. (April 14, 2013)
- Spector, Lincoln. "How Safe is WPA2-Secured WiFi?" PC World. November 21, 2011. (April 21, 2013) http://www.pcworld.com/article/243713/how_safe_is_wpa2_secured_wifi_.html
- Strom, David. "Tutorial: How to Set Up WPA2 on Your Wireless Network." Computer World. August 24, 2006. (April 21, 2013) http://www.computerworld.com/s/article/9002706/Tutorial_How_to_set_up_WPA2_on_your_wireless_network_

- Sullivan, Mark and Ken Biba. "Mobile Hotspots: Which Are Fastest, Most Reliable?" PC World. October 18, 2010. (April 25, 2013) http://www.pcworld.com/article/208154/mobile_hotspot_wars.html
- Vaughan-Nichols, Steven J. "2013: The Year Gigabit Wi-Fi arrives." ZD Net. January 7, 2013. (April 22, 2013) http://www.zdnet.com/2013-the-year-gigabit-wi-fi-arrives-7000009480/vaug
- Wawro, Alex. "How to Lock Down Your Wireless Network." PC World. November 10, 2011. (April 21, 2013) http://www.pcworld.com/article/243290/how_to_lock_down_your_wireless_network.html
- Whitney, Lance. "Wi-Fi 802.11ac to drive wireless HD video in the home." CNET. January 23, 2012. (April 21, 2013) http://news.cnet.com/8301-1035_3-57363508-94/wi-fi-802.11ac-to-drive-wireless-hd-video-in-the-home/
- WiFi Alliance. "FAQ." (April 21, 2013) http://www.wi-fi.org/knowledge-center/faq
- WiFi Alliance. "Hotspot." (April 26, 2013) http://www.wi-fi.org/knowledge-center/glossary/hotspotswi