



Global Knowledge®

Expert Reference Series of White Papers

# Wireless Networking 101

# Wireless Networking 101

Brent Mossberger, CCNA, CCSI

---

## Introduction

Why would a person or organization be interested in deploying wireless communication in their home or business? Given the variety of reasons (and the fact that businesses must consider problems that may not face the average home user), let's focus on the most common reason for both groups: flexibility.

For home users, this means they have the ability to download files, check e-mails, or watch streaming videos from anywhere within their home without the burden of running CAT 5e UTP (unshielded, twisted pair) cable to every room with jacks six feet apart. Many people had one wired connection in their house, usually in an office, and now they want to be able to open their laptop and connect to the Internet from anywhere within their homes. With wireless connections, they can surf the Internet, check e-mails, and watch streaming videos, all while working in the kitchen preparing dinner or in the living room while watching TV.

As far as businesses are concerned, flexibility means the ability of employees to take their "desktop" with them and connect to the network resources they need to get their job done. They can work in the lunch room, a meeting room, or pick up their laptop (which may have a specific application or confidential data stored on it) and bring it to the conference room while maintaining physical security. Being able to haul your laptop around with you and connect wherever you are simplifies things in a way that we could only dream of "back in the day."

This being said, there are some things to think about before jumping into the wireless world. As is usually the case in the wonderful world of networking, whenever one thing becomes simpler, it almost always complicates something else. In this case, security and connectivity are going to be our main concerns.

## Basic Connectivity

Wireless communication refers to the transmission of electromagnetic waves (radio frequencies) and the electronic data carried on those waves. The upside of wireless communication is that we can transmit signals to and from locations that would be impractical using wires or cables.

The downside is that these waves can be interfered with in numerous ways. You have probably experienced this while driving down the road listening to your FM radio. Signals tend to be weaker or stronger depending on the distance between the receiver (your car's antenna) and transmitter (the radio stations transmitting antenna). In addition, simply driving through a small valley or under high voltage wires can disrupt transmission. The price for flexibility is that we have to expect and deal with these sorts of challenges in a wireless environment.

The FCC has provided several frequency ranges that wireless transmissions, such as the wireless access points that we are familiar with, we are permitted to use. Much in the way that FM radio stations must use frequencies between 88.1 MHz and 108.1 MHz, we are given the ranges of 2.4 GHz through 2.4835 GHz (let's just call it 2.4 GHz shall we?) In addition, we're allowed to use the 5.725 GHz through 5.850 GHz range. These frequency ranges are broken into smaller "channels" that can be used to transmit data.

However, since these channels overlap, not all of the channels are made available for us to transmit on. For example, the 2.4 GHz range is broken into 11 22MHz-wide channels but because of the tendency for transmissions to overlap from one channel into the next, only 3 channels, (1, 6 and 11) are typically used. The 5 GHz range is broken into 23 non-overlapping 20MHz channels.

One nice thing is that these ranges provide no "exclusive use," which means, unlike FM radio stations, we don't have to purchase the right to transmit exclusively in that range. We can all use them without paying a fee. These ranges are called the ISM (industry, scientific, and medical) frequency band. Of course, when anything is free people will basically step on each other to get access to it. That means that there are a number of devices that transmit in these ranges; mostly in the 2.4 GHz range: cordless phones, baby monitors, wireless game controllers, microwave ovens, etc. A wireless network must compete, potentially, with many of these devices.

## How Do We Put Data on the Radio Waves?

This is a great question to ask, but a detailed answer is beyond the scope of this white paper. However, to put it simply, we use a process called "modulation." Modulation refers to the changing of a tone or signal (think of the sine wave and making it longer or shorter, narrower or wider) and adding "data" to that wave using something called "encoding." Now, there are several modulation techniques and several encoding techniques used on each of them, but let's just touch on one or two.

### DSSS – Direct Sequence Spread Spectrum

Remember the 2.0 GHz – 2.4 GHz frequency range? Well, that frequency range is broken into 11 channels, each of which is actually a 22 MHz wide frequency range in itself. DSSS takes the data and spreads it across the entire 22 MHz channel and uses a "chipping code" to represent the bits for data encoding. The idea of chipping simply explained is that instead of sending one bit to represent one bit we use a string of 11 bits to represent either a 1 or a 0. Why do this? Well, if you're sending one to one and that bit is lost, then you've lost the entire bit and there is no way of knowing whether the lost information was a 0 or a 1, but if you send one string of 11 bits to represent a one and a separate (and opposite) string of 11 bits to represent a zero then you could lose up to half of the transmission and still be able to determine whether the transmitted data is a 1 or a 0.

Maybe an example will help. I have an important document to send to you. If I send the whole document on one airplane and that airplane goes down, we've lost the whole document, but if I send every 11th word on 11 different planes then if one plane is lost you can probably reproduce the data, right? This is the same general idea. (Transmission loss is much more likely to occur than a plane crash, by the way.) 802.11b uses DSSS transmission, modulation, and encoding techniques and provides speeds of up to 11Mbps.

## OFDM – Orthogonal Frequency Division Multiplexing

The basic idea behind OFDM (my favorite acronym because you sound smart just saying it) is that the main frequency range is once again divided into channels, but these channels are subdivided into smaller “sub-carriers.” The channels are typically 20 MHz wide, and the sub-carriers are 300 KHz. That gives you about 52 sub-carriers. Each of these sub-carriers can carry a smaller amount of data than the whole channel, but the data is transmitted on all sub-carriers simultaneously and in parallel, giving us much higher throughput. OFDM is used by both 802.11a in the 5 GHz range and 802.11g in the 2.4 GHz range and provides for speeds of up to 54Mbps.

## What Influences Wireless Transmissions?

Because we are transmitting electronic signals into the air using radio waves, there are many situations that can detrimentally effect our transmissions. To understand how these problems occur, it is important to have some basic terminology.

- **Wavelength** is the amount of distance between crests of a sine wave. Different technologies generate different wavelengths. For example, an AM wavelength is several hundred meters long, while waveforms created by your access point at home are probably no more than a few centimeters long.
- **Frequency** is the number of waveforms that occur in a specified period of time.
- One complete waveform is referred to as a **cycle**.
- When one cycle occurs in one second, it is referred to as **1 Hertz**.
- **Amplitude** is the vertical distance between the crests in a wave. (Highest peak to lowest valley)

One of the first things to understand about wireless transmission is something called **Free Path Loss**. This is basically techno speak for “the farther away a signal moves from its transmission point, the less strong it is.”

Another thing that can affect our transmissions is **absorption**. The idea here is that some objects can absorb radio waves and, therefore, reduce the distance, or possibly stop entirely, our transmission. Anything that will absorb noise (sound waves) will absorb data waves as well: walls, partitions, ceilings, etc.

Still another possible problem involves something called **Reflection**. Reflection happens when radio waves bounce off of something and travel in a different direction. Things like mirrors, glass, monitors, paintings, or pictures under glass can cause reflection.

**Scattering**, another type of interference, happens when a signal impacts objects that have many reflective or jagged edges. The most common example this might be transmitting a signal through a rainstorm. Since raindrops are reflective, the signal reflects in many different directions distorting or weakening the signal. Even the curvature of the earth can interfere with a radio signal when it is being transmitted across long distances.

## How about the Hardware?

There are as many different types of antennas as there are methods of transmitting data. Let’s mention a few of them here. First, most antennas fall into one of two categories, **directional** or **omni-directional**. The wireless access point in your house probably uses an omni-directional antenna called a dipole antenna. It covers a

relatively small area and radiates a coverage pattern shaped like a doughnut. Its area is wider than it is high and is good for small indoor environments. Directional antennas include the wall mounted "patch" antenna that is physically flat and generally mounted on a wall to cover a wide hallway or the offices on one side of a floor, for example. It generates a somewhat wide and tall signal that extends outward from the antenna and looks a bit like a rectangle.

The **yagi** antenna is an indoor antenna that looks physically like a square baton and is usually mounted over doorways to provide coverage for long hallways. You might also use multiple yagis for coverage in a large warehouse environment. The yagi creates a coverage area of around 80 degrees and looks like the piece of pie I had for dessert last night.

Then there is the big daddy of wireless antennas; the Parabolic Dish. We've all seen these on top of houses for satellite TV service. The parabolic dish generates a very narrow radiation pattern and is generally used to connect two physically distant networks together. Parabolic dish antennas can achieve connectivity at distances of up to 25 miles, depending on several variables, including the frequency range the transmission is occurring on.

## How Collisions Are Handled

In wireless technology there is no wire to listen for jamming signals on because there is only one transmitting antenna, and it is either listening or transmitting. Because of this problem, we use a process called CSMA/CA or collision avoidance, as opposed to collision detection. Basically, what happens is that the station that wants to transmit listens on its channel until it determines that channel is clear and then transmits a signal indicating to other workstations that it is going to transmit data, the approximate size of the transmission, how long it will take, and that they should not send in the meantime. The transmitting station then listens again for a short period of time and then transmits its data.

## IEEE Standards and 802.11 Protocols

**802.11** was the original wireless standard developed in 1997. It used Frequency Hopping Spread Spectrum modulation in the 2.4 GHz frequency band and operated at 1 or 2Mbps.

**802.11b** was a fairly rapidly created supplement that used Direct Spread Spectrum modulation, also in the 2.4 GHz band, and operated at 1, 2, 5.5, and 11Mbps. It achieved greater speed by using a more efficient encoding mechanisms than 802.11.

**802.11g** was developed in 2003 and used DSSS modulation in the 2.4 GHz band, but it also used OFDM as a secondary modulation technique in order to allow for higher speeds of up to 54Mbps. It is only compatible with 802.11b at the lower speeds, since 802.11b does not use or understand OFDM.

**802.11a** uses the 5 GHz frequency range and OFDM as its exclusive modulation technique. Because of this, 802.11a transmits at speeds of up to 54Mbps and has less competition for bandwidth from other devices. On the downside, the higher frequencies generate more heat and have a shorter range. 802.11a was introduced later in the game and, as a result, was slower to be accepted as a standard.

**802.11n** is a newer standard that promises to allow transmission speeds of up to 100Mbps by using something called MIMO, which basically means instead of having ONE antenna that is either transmitting or sending, there are multiple antennas that can receive and send simultaneously. The information is then multiplexed over a single channel. (Multiplexing is a process of sending more than one conversation over a single connection.)

Most modern wireless adapters are listed as 802.11a/b/g, meaning they support all of these standards.

## Security

One of the main inhibitions to the widespread acceptance of wireless technology for quite some time was the perception (quite accurate) that wireless communication was very insecure. The first security hole was in how devices were allowed to connect to a wireless access point.

The access point broadcasts its presence to any devices that might be listening, allowing those devices to connect to them. This could be inconvenient if you are a home user and the access point is providing access to your Internet connection. At a minimum, some person that you don't know could connect and use your connection for their own purposes, whether they are legitimate or not. Worst case, the intruder could access the other devices that are connected to the access point and see or modify information on them.

The most obvious solution to this problem was to put a password on the access point and then make the access point ask any PC trying to connect for the password. If the password isn't correct then you're not allowed to connect. Problem solved? Not quite.

In the original standard, the password that your PC sent through the air to the access point was unencrypted - something we computer types call "being sent in the clear." That meant that anyone with a marginally sophisticated traffic sniffer could "watch" the transmission and document your password. They could then use it themselves to connect.

The next solution would seem obvious; we'll just encrypt the transmission so anybody who "watches" it will simply see a seemingly random string of characters. The original security standard, WEP (wired equivalency protocol) used a 40 bit encryption algorithm to "hide" the password from any uninvited guests.

One key point here is that the user data was in no way encrypted. It was still sent in the clear for anyone with the proper programs to look at. Unfortunately it took hackers about 10 minutes to break that encryption algorithm. (of course, I'm exaggerating, but it didn't take long.) There were a couple of other methods used to supplement WEP, but nothing that made it secure enough for most businesses to take seriously.

Therefore, it wasn't until the development of WPA and WP2 (these are collectively called the 802.11i standard, although WPA2 is the recommended standard) that wireless implementations were considered as a legitimate answer to business network communications needs.

WPA (Wi-Fi Protected Access) used an encryption mechanism called TKIP (Temporal Key Integrity Protocol), which was much more secure than WEP but did not require a hardware upgrade in the wireless equipment. Optionally, you could use the much more secure but more hardware-dependent AES encryption. WPA2 uses AES (Advanced Encryption Standard), which is an extremely secure mechanism. Both WPA and WPA2 protect both password transmission and data transmission and, in addition, allow for a centralized authentication system collectively referred to as 802.1x.

The beauty of centralized authentication is that both usernames and passwords are stored, and there is no need to set up passwords on every single access point. This wouldn't be a big deal to your average home user, but it is huge when you're a company deploying dozens or hundreds of access points and you want consistent authentication setup for all users. If you want to setup a single password system (for home use) you can select "personal mode" and if you want 802.1x (for business use) you can select "enterprise mode."

## Conclusion

Well, there you have it; a simple, straightforward description of basic wireless networking concepts. There is obviously much more to this topic than can be described here, but I hope your appetite has been whetted, and you pursue your interest in this fascinating area of networking. Wireless networking is big and only going to get bigger in the future.

## Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

[ICND1 – Interconnecting Cisco Network Devices 1](#)

[ICND2 – Interconnecting Cisco Network Devices 2](#)

[CWNA – Certified Wireless Network Administrator](#)

For more information or to register, visit [www.globalknowledge.com](http://www.globalknowledge.com) or call **1-800-COURSES** to speak with a sales representative. Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through classrooms, e-Learning, and on-site sessions, to meet your IT and business training needs.

## About the Author

Brent Mossberger has been working with computer networks since 1985 and has worked with most routed protocols including TCP/IP, IPX, and Appletalk in a support, design and maintenance role. He got involved with routing and switching in the early '90' and started out on Cabletron Switches and Cisco Routers. In the 25 years he's been working with networks, about half of the time he was self-employed and the other half worked in medium-sized corporate environments. He has taught networking classes for about 11 years and enjoys transferring knowledge to his students. While he does not have a formal degree, he learned everything he knows through hands-on, trial-by-fire experience.