Setting Up a Wireless Home Network

“Wireless is wonderful for convenience, but security is an issue.”

by Pete Choppin

In recent years, wireless networking for the home has seen a huge jump. More and more people are opting to install a wireless network. It is replacing wired networks as the standard for home networks.

It's no wonder. Wireless networks have several advantages over wired networks. There are fewer expenses, and printers and scanners are easier to share with other computers. Wireless networks make it easier to connect entertainment centers to your computer. Many other applications and appliances are making their way into the wireless age as well, such as your refrigerator, stereo, watches, key chains, baby video monitors … the list goes on.

This article discusses the basics of home wireless networks, required equipment and how to secure your network.

Wireless vs. Wired

Obviously, one of the biggest draws for wireless popularity is that a wireless network eliminates the use of expensive network cables that are difficult to install and limit the types of devices and the number of connections available for your network. This is not to say that a wired network has no advantages. Security is a huge concern for home users. Because wireless technology transfers data over the air, the data you transfer is especially vulnerable to security hacks. It is much more difficult to infiltrate a wired network. This would require a physical connection to the wire. All that someone needs to do to hack a wireless network is capture the data with a receiver.

Another advantage of a wired network over wireless is speed. Wired networks can reach speeds of up to 1,000 megabits per second, whereas wireless speeds are in the range of 20 to 200Mbps. Both wired and wireless technologies are getting faster, but it doesn't look like wireless is likely to pass up or even catch wired network speeds.

Yet the popularity of wireless networking is rising, and rising quickly. Even with higher security risks and slower speeds, wireless networks are almost the preferred technology. It isn't that people don't want speed and security, but it seems that the convenience of not having to be tethered to a wire is so appealing that users are willing to compromise on speed and risk a certain level of security in order to have the ability to use any network-capable device anywhere in a house.

Still, speed and security are critical points that need to be addressed, and we will go over these soon.

Choosing a Wireless Standard

You may have seen certain standards out there that are referred to as "802.11" and a letter with it such as 802.11a, 802.11b, 802.11g and 802.11n. I won't bore you with how this all came about. The important thing to know about these standards is that the ones to look for are 802.11g and 802.11n. The advantage of these newer standards is mainly speed. You will

likely see equipment that is using 802.11 g/n standards.

Dual-Band N Routers

Dual-band a/b/g/n routers support both bands for 11n. They enable 11a and 11n users to transmit at 5GHz and 11b/g and 11n users to transmit at 2.4GHz; however, both bands may run simultaneously or only one band at a time. Simultaneous support provides load balancing and offers the most compatibility with all four standards (a, b, g and n).

Planning Your Wireless Network

Setting up and installing a wireless home network can be quite easy. In most cases, once you unpack the equipment and install it, you can be up and running in a matter of minutes. But there are a few things you should know when planning your network. Here are a few things to consider.

• Do you still plan to have any computers on a wired connection?

• Will you connect any printers to the wireless network?

• Will the wireless router be directly connected to the Internet, or will you have other routers, switches or modems in use?

• Do you plan to have VoIP for phone connections?

• What kind of data do you need to secure, and how will you configure the security?

Hardware and Software

Your network infrastructure, or the hardware pieces that connect everything, for a wireless network are fairly simple. You will need an access point, which, for a home, is typically a wireless router and wireless receivers. Each computer, laptop or other device that needs to connect to the network will need a wireless receiver. This is usually built into the device.

Software to connect wireless devices and configure the network is a little more complicated, although it is fairly easy to configure. Let's start with the router.

Configuring the Router

There are four main areas that need to be configured on your router: the password into the router configuration, Network Name (SSID), the channel on which the router broadcasts, and the security.

Router Configuration Password—Every router comes from the manufacturer with a user name and password. This would not be a problem, except that each manufacturer sets this exactly the same on their routers. The passwords to each router have now become well known. Most people who are familiar with setting up routers know the passwords to the more common routers, so it is a very good idea to modify this password when you first configure your router.

Most routers have administration settings that allow you to change the router password, similar to this:

Network Name (SSID)—Wireless networks are identified by a name that is broadcast over the air. This is done so when your device picks up the network from the receiver, you are able to identify which network you are looking at. Remember, it is possible to have several networks available in one area, so identifying specific networks may be helpful. However, this is sometimes exploited by hackers who are looking for an easy network to jump onto. This is especially true when the network name has not been changed from the default name. Additionally, it is possible to disable broadcasting the network name for additional security. This isn't a foolproof method, but it is one more layer of security you may want to add.

The Network Name (often referred to as the SSID) can be changed in the basic wireless settings of most routers:

Network Channel—Wireless networks operate on signal channels. Most wireless routers have 12 channels available. You can set the router to any channel you wish, but the preferred channels are 1, 6 and 11. These are considered non-overlapping, which means they should not interfere with or collide with channels broadcasting similar frequencies. You can also try each and see which one provides the most stable connection for you.

The channel settings should be in the same area as the network name:

Security—Wireless networks, although not as secure as a wired network, have much better security than in the past. The first attempts at securing wireless signals proved to be unsuccessful, but this has changed over the years.

Securing a wireless network requires encrypting the signal. Most every wireless router is equipped with fairly strong 128-bit security using WPA encryption. WPA requires setting a PSK (Pre-Shared Key). To do this, simply set the router security with WPA2 and create a PSK that you will use to connect to the router. The PSK is similar to a password; therefore, anyone who wants to connect to your network will need to have this key.

The settings to enable wireless security are usually in a special security area of the configuration, similar to this:

Step 1—Open the Security Screen

Choose the Security Mode

Choose the Encryption Type

Create Your PSK (Pre-Shared Key)

Remember to Save Settings

That is about everything that you need to do on the wireless router. You could add more advanced security such as MAC filtering. It is a good practice, but the drawback is that for any device you want to have access to the network, you will have to go into the router and add the MAC address for each device. When you consider that this might include all laptops, PDAs, appliances, wireless printers and video equipment, it may become cumbersome. So unless you have a need for really strong security, you will probably be safe just using WPA2 security.

Connecting Devices

Now that your wireless router is configured and secured, you will need to connect your laptops, PDAs and other wireless-capable devices. Since each device has unique settings, it would not be very practical to describe every device in this article. But there are some basic things in common you will need to know. To connect a device, you will need to find the wireless setting on that device. On a laptop, this is usually down in the system tray where a small wireless icon will show. This is down near the clock on the bottom right corner of the screen.

Simply click on the wireless icon and look for your network name. When you connect to that network, you will be prompted for the PSK phrase that you configured on the router.

Other devices such as PDAs have specific settings, but will still need the network name and the PSK. You will have to refer to the manual to find the settings for these devices.

Wireless networks for the home can be an easy way to connect your devices, especially when there is not already a preinstalled wiring system. Rather than trying to feed network wires through walls and ceilings, simply install a wireless router and connect your devices. As long as it is properly secured, a wireless network is a great way to be connected and have the freedom to move anywhere in the house.