

Wireless Networking, Part 2: Setup and Security

The first installment in this two-part series of Tech Tips provided an introduction to the basic capabilities and hardware involved in wireless networking. In the final installment of this two-part series, we will look at some of the basic setup and security considerations that should be addressed. The physical installation of a wireless network may be easier than a wired network, but the more difficult part is setting up the software and security to make sure everything stays up and running without incident.

Although this Tech Tip is by no means an exhaustive resource on configuring a wireless network, it will provide information and pointers that can be applied to most typical installations. Many of these tips are general enough that they may provide some good advice for those utilizing wired networks as well.

For the sake of this article, we will assume that the hardware has been successfully installed physically, and that the user is now prepared to set up and secure the system through software. Wireless devices, especially routers / access points, generally include a web-based configuration utility that allows the user to customize the hardware to meet their needs. The hardware will most likely work with minimal configuration, but to make it work so that the integrity of the network is protected may take a few more steps.

In addition to the configuration interface provided with the wireless networking hardware, Microsoft has integrated a "Wireless Network Setup Wizard" with the release of Windows XP Service Pack 2 that will lead a user of any expertise through the installation of their network. In addition, the "Microsoft Broadband Network Utility" will help them monitor and maintain the network just as easily once it is set up.

Change Default Password

Routers, whether wired or wireless, require a password for configuring the various settings, and all of them ship with extremely simple default passwords. The first step taken in setting up the router should be to change the default password to something more difficult to guess. Longer passwords that use a combination of letters and numbers are preferable as they make hacking attempts that much more difficult.

Change Router IP Address

Most routers ship with a default IP (Internet Protocol) address, something like 192.168.1.1, which is utilized by the user for accessing the configuration utility interface, as well as by the network itself for negotiating the LAN and WAN connections. The configuration utility of most routers will include a page that will allow for the default IP address to be manually changed by the user. Although changing the default IP address doesn't provide a great amount of security since it can easily be discovered anyway, it may deter intrusion by local users that may be casually scanning the network.

Configure Router or Access Point Use

In the first part of this series of Tech Tips, I mentioned that almost all routers intended for home use can also double as wireless access points, and this is generally accomplished by clicking a check box within the control panel software. If a wireless router is being added to a network with an existing router and broadband connection, the new device needs to be set to access point mode. Otherwise, there could be a conflict as the network may not know where to expect the internet connection, since it will now have two routers that both want to serve as the gateway. If

the wireless router is replacing an existing router, or is the only one on the network, this should not be an issue as these devices generally ship configured to operate as a router by default.

Broadcasting the SSID

The SSID, or Service Set Identifier, is basically the name assigned to a particular wireless network. The user can choose just about any name they want, as long as it is less than 32 characters long, and they just need to be sure that all computers on the network are configured to use the same name. Two steps related to the SSID can be taken to help improve the security of the network:

First, change the default SSID to a unique name that includes a combination of letters and numbers that doesn't reveal anything personal about you or your network. Second, disable the broadcast of the SSID once all of your computers are successfully connected, even if your router / access point recommends broadcasting it. I have used a few wireless routers, and all of them have a check box in the control panel for enabling/disabling the broadcast of the SSID, and they have all recommended leaving broadcasting enabled. Broadcasting the SSID allows new computers to easily find your network, and then all they have to do is access it given the proper credentials. Broadcasting your SSID puts it out there for anyone within range to see, and it just allows would-be hackers to get one step closer to compromising your security. In a home environment, there are probably few computers that need to access the network, and if more are ever added, you can temporarily enable the broadcast to get them set up.

DHCP Server

The DHCP (Dynamic Host Configuration Protocol) Server is a feature of most routers that makes adding new computers extremely simple. Whenever a new computer connects to the network, the router will assign an IP address to it, instead of the user having to assign an IP address to each manually while sitting at that particular computer. This makes configuring a network very easy, but it also leaves the network vulnerable, as any new computer detected will be welcomed to the neighborhood and assigned an IP address automatically. Two different approaches can be taken to improve security, as related to the DHCP server:

One method, and the best as far as security is concerned, is to disable the DHCP server. This will require that all computers that are authorized to connect to the network be configured manually, but it will prevent unauthorized computers from obtaining an IP address. The second method, which doesn't provide bulletproof security, is better than doing nothing. In general, a DHCP server can support up to 250 computers, and by default leaves a range of addresses readily available for that many to connect. If disabling the DHCP server doesn't seem convenient for a user, they can limit the DHCP server to only provide as many IP addresses as they know they need. If you know there will never be more than five computers connected, limit the range of available IP addresses to a total of five within the configuration utility.

Different Levels of Encryption

All wireless components support some sort of encryption, which simply scrambles the information being sent across the network so that it can not easily be read by anyone else connected to the network. There are different types and levels of encryption, and a brief overview is provided for them below:

WEP, or Wireless Equivalency Protocol, was the first format of encryption available on wireless networks. WEP allows the network administrator to assign an encryption string to be shared by all computers authorized to access the wireless network. The encryption through WEP is either 64bit, 128bit, or 256bit, where the higher number represents greater encryption, and the strings can be generated by the administrator as a series of letters and numbers.

WPA, or "Wi-Fi Protected Access," is an improvement over WEP that starts off with a similar master encryption string and then mathematically derives encryption keys to keep the security dynamic. WPA continually changes the encryption keys used for each packet of data, and due to the extra processing required to support this protocol the overall throughput of the connection may suffer slightly. Despite the potential for decreased speed, WPA is considered to be far more robust than WEP, and should be implemented where possible. In some instances, WEP encryption has actually been defeated, making WPA all that more appealing.

Although most components support both of these encryption formats, and users can select the type they wish to use from within the control software, not all do. All devices on the network must be set to operate at the same level of encryption, which may mean that some devices will force others to be less secure than they are capable of. For example, a wireless network setup around this router (<http://www.geeks.com/details.asp?invtid=DI-824VUP&cat=NET>) could support either WEP or WPA encryption. When two computers are added to this network using one of these network adaptors (<http://www.geeks.com/details.asp?invtid=WN-4054P&cat=NET>) in one case, and one of these network adaptors (<http://www.geeks.com/details.asp?invtid=PBW006-N&cat=NET>) in the other case, things change. Note that the second adaptor does not support WPA; therefore the whole network must now be configured to use WEP to accommodate it.

Router Position

As discussed in the first part of this Tech Tip, wireless devices can have a range of up to a few hundred feet in free space. When installed inside a home, this range may decrease greatly due to walls, floors and other obstructions, but the signal may still be strong enough to carry beyond the confines of the dwelling. A simple step that may help reduce the strength and reach of the network signal outside the house is to position the router / access point as close to the center of the house as possible. The potential for someone to detect the network from outside the home when positioned like this is now much less than if the router was placed near a window, for example.

Final Words

There are definitely additional issues that could be considered when setting up a wireless network, but covering these basics will make a wireless network much more secure than it was straight out of the box. Many people are confident that no one would be interested in their home network and feel security is just one more headache of technical mumbo-jumbo that they would rather not deal with. Whether a hacker wants access to personal files on the network or to simply gain unauthorized access to the Internet, a few simple steps are worth the peace of mind to know you are as secure as possible.