Title:
Wireless Router & Security: A Step-By-Step Guide

Word Count:
909

Summary:
Setting up a wireless router is easy. Essentially you turn your cable or DSL modem off and your wireless router on. Then, you connect the router to the modem with a cable, and turn the modem back on. You are more or less done. The wireless network wizard on your computer will pick up the router and, if your ISP does not have any special requirements, away-you-go, you are on the Internet.

For ease of setup and configuration, manufacturers ship wireless routers with all sec...

Keywords:
wireless router, wireless network, security

Article Body:
Setting up a wireless router is easy. Essentially you turn your cable or DSL modem off and your wireless router on. Then, you connect the router to the modem with a cable, and turn the modem back on. You are more or less done. The wireless network wizard on your computer will pick up the router and, if your ISP does not have any special requirements, away-you-go, you are on the Internet.

For ease of setup and configuration, manufacturers ship wireless routers with all security disabled. Therein lies the problem. If you do not take any further steps to secure your router, and a surprising number of people don’t, your network will be wide open to all passersby and strangers. It’s like you’ve hung out a sign, “The door is open. Please come in and help yourself.”

The problem is not that strangers will be able to use your router to access the Internet but that, without further protection, would-be intruders will be able monitor and sniff out information you send and receive on your network. Malicious intruders can even hop on to your internal network; access your hard drives; and, steal, edit, or delete files on your computer.

The good news is that it is relatively easy to secure your wireless router. Here

are three basic steps you should take.

1. Password protect the access to your router's internal configuration

To access your router's internal setup, open a browser and enter the routers setup URL. The URL will be specified in the manual. The URLs for D-Link and Linksys routers, two major manufacturers of wireless routers, are http://192.168.0.1 and http://192.168.1.1, respectively.

For Linksys routers, leave the user name blank and type "admin" (without the quotes) in the password field and press enter. To change the password, simply click on the Password tab and enter your new password.

For other routers, please consult your manual. Alternately, you can search on the Internet with the term "default login for ". Don't be surprised to find quite a number of pages listing default login parameters for many different routers, even uncommon ones.

2. Change the default SSID (Service Set IDentifier)

The SSID is the name of a WLAN (Wireless Local Area Network). All wireless devices on a WLAN use SSIDs to communicate with each other.

Routers ship with standard default SSIDs. For example, the default SSID for Linksys routers is, not unsurprisingly, "Linksys". As you can see, if you don't change the default SSID of your router a would-be intruder armed with a few common SSIDs from major manufacturers will be able to find your wireless network quite easily.

To change the SSID, click on the Wireless tab. Look for an input item labeled SSID. It will be near the top. Enter a new name for network. Don't use something like "My Network". Use a name that is be hard to guess.

3. Disable SSID broadcast

Wireless enabled computers use network discovery software to automatically search for nearby SSIDs. Some of the more advanced software will query the SSIDs of nearby networks and even display their names. Therefore, changing the network name only helps partially to secure your network. To prevent your network name from being discovered, you must disable SSID broadcast.

In the same screen that you changed the name of your network, you will see options for SSID broadcast. Choose "Disable SSID" to make your network

invisible. Now save all your settings and log out.

Since your wireless network is now invisible, you will have to configure your computers to connect to your wireless network using the new name. On Windows XP, start by clicking on the wireless icon in the Notification Area and proceed from there.

With these three steps, your network now has basic security. However, if you keep sensitive information on your computers, you may want to secure your wireless network even further. For example, you can

- Change the channel your router uses to transmit and receive data on a regularly basis.
- Restrict devices that can connect to the router by filtering out MAC (Media Access Control) addresses.
- Use encryption such as WEP and WPA.

As with most things in life, security is a trade off between cost (time, money, inconvenience) and benefit (ease of use). It is a personal decision you make. However for the majority of home uses, the three basic steps plus WEP/WPA encryption provides reasonably strong security.

Turning on encryption is a two-step process. First you configure your router to use encryption using an encryption key of your choice. And then, you configure your computer to use the encryption key. The actual process of configuring your router for encryption varies from router to router. Please consult the router's manual.

There are even stronger methods for ensuring security. A strong and robust security method is RADIUS (Remote Authentication Dial In User Service). Using RADIUS requires additional hardware and software. However, there are companies that offer RADIUS security as a subscription based service. The fees are reasonable and dropping.

Therefore for example, if you run a business on your wireless network, have sensitive data on your computers such as credit card information, and have a number of users who access your network, you should consider using RADIUS. Since the service sector for RADIUS is dynamic and growing, a search on the Internet with terms like "RADIUS subscription" or "RADIUS service" is probably the best way to locate one.