



Improving Your Wireless Internet Access

White Paper

Published: May 25, 2004

Produced by:

twentysix New York
a business solutions provider

62 West 45th Street
New York, NY 10036

www.26ny.com

Introduction

It makes little sense to run wires all over your house if you do not need to; it is both an inconvenience as well as an expense. You probably want to access the Internet with a laptop, but do not want to be confined to a wire.

If all you need is to share an Internet connection, wireless is the way to go – as long as you set it up correctly. Since your broadband connection will be much slower than even an 11MB wireless link, there is no performance benefit to running wires. However, if you want to share files quickly with other computers or stream video, you will need to run those wires.

For the purposes of this paper, it is assumed that wireless is what you want or already have, and you just need some tips to make it better. What can make wireless better? Two things: security and signal strength.

Security

If you open your wireless router, plug it in, and go through the configuration wizard provided by the manufacturer to get it running, you are completely unsecured.

Anyone in the reception range of your wireless router can see your network, attach successfully, and connect to your router and install a password that can prevent even you from accessing it.

In order to prevent that, there are three things you must do:

1. Use encryption.

Wired Equivalent Privacy (WEP) is your first line of defense. Configure your router and all your clients to use WEP. By default, the majority of wireless routers have it turned off. WEP keeps the casual snoopers at bay, but due to flaws in its design, the more serious hackers can still access your network.

Since September 2003, these holes have been patched, and WPA (Wi-Fi Protected Access) replaces WEP and keeps your network secure. To use WPA, you need to patch the software installed on your:

- Router
- Wireless cards
- Version of Windows

Contact your hardware manufacturer for a free upgrade; Windows XP updates are available at – <http://support.microsoft.com/default.aspx?kbid=815485>

2. Change the System ID.

Devices come with a default system ID called the SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). It is easy for a hacker to find out what the default identifier is for each manufacturer of wireless equipment so you need to change this to something else.

3. Do not broadcast your System ID.

Your SSID is your wireless network name; as long as you know what the ID is, you can let your wireless devices know manually when you configure the network. Do not broadcast it to the wireless world; it is one less thing they can use to attack you.

4. Use MAC address filtering.

You can limit access to your network by using Media Access Control (MAC) address filtering on your router, where you restrict access based on a unique code that is built into every Wi-Fi adapter (and Ethernet adapter) on your network. Find out what the MAC address is on each of your adapters, put that list into the router, and allow only those cards to access your network. If you are running Windows XP, the command "GetMAC" will give you the MAC address.

5. Disable remote access and enable the firewall.

Most wireless routers come with some type of firewall; make sure it is enabled. Also, disable wireless access to your router; if you need to administer it, you could do so from a wired workstation connected to the router.

Signal strength

The strength of the signal between the router and your computer has a direct affect on speed and reliability. Since the signal does not travel as well through walls and floors, proper placement of the wireless device is very important. Most people try a couple of places before they find one that suits their needs. Some just put it in a central location.

Regardless of placement, to get a better signal you can:

1. Replace the antennas that came with your router.

Higher gain antennas are available from Radio Shack; they are more powerful than the antennas that came with the router, and are not very expensive. Bring your old ones with you to make sure you get an exact replacement.

2. Add more wireless gateways.

You can add a second wireless router to your configuration to extend the signal of the first gateway. This functions as a 'repeater' and just extends the range of the first router. You can also connect two or more routers with a wire (standard network cable) to extend their range. This is useful when you have a lot of floors or walls that absorb the signals, or if you want to extend wireless for a longer distance.

3. Get a directional antenna.

You can get a relatively low cost directional antenna to connect to your router to broadcast directly to bad spots on your wireless network, or to where you know you will be. Also, you can get a directional antenna for your computer to point directly to your wireless router. Where you point the antennas (even the ones that came with the router) makes a difference.

twentysix
NEW YORK