

## **The Securities and Insecurities of Wireless Networks Today**

Everyone is looking for a way to make things easier and more convenient, especially when it comes to technology. Everything that was once new and revolutionary became old and drab because it was stuck in one place due to wires. When laptop computers became smaller and more portable, the need for wireless connectivity became blatantly obvious. Having a wired connection does not allow us to keep up with the fast-paced society that we live in today. Around the early 1990's, teams of engineers greatly expanded our options for portable technology. "Wireless technologies are without any doubt shaping the beginning of the new millennium. The principal of computing any time, anywhere, is becoming reality."

Around 1991, "Wi-Fi" or "Wireless Fidelity" was invented by Vic Hayes of Lucent and Agere Systems in the Netherlands. Its initial design was meant for cashier systems and the first products on the market were called "WaveLAN." This first attempt at wireless only supported speeds of 1 Mb/s to 2 Mb/s. In the past 15 years, things have definitely come a long way. The speeds have increased dramatically from their initial design and have given the world of wireless technology infinite possibilities.

The typical Wi-Fi system includes one or more Access Points and one or more clients. An Access Point broadcasts its SSID (Service Set Identifier or Network Name) via packets called beacons, which are broadcasted every 100 ms. These beacons are transmitted at 1 Mb/s and are relatively short, therefore having little influence on performance. One downside of wireless networks is that the signals are transmitted

through the air in the same manner as a non-switched Ethernet network, therefore collisions can occur just as they can in a non-switched LAN.

Two major standards have been created and implemented into mainstream use across the globe. 802.11b and g operate in the 2.4 Ghz band and transmit at speeds of 11 and 54 Mb/s respectively. 802.11b was the first standard to become widely implemented. Developed in 1999, it was the first of many to increase the mobility of technology. It has a range of 150 feet indoors and 300 feet outdoors. This standard is fast enough to surf the internet and perform basic online functions, but quickly became outdated as users demanded a faster connection to their networks.

802.11a was developed as a remedy to this issue. This standard was much faster than 802.11b at 54 Mb/s. It operates at 5 Ghz and generally only has one third the range of b and g networks because the higher frequency is more easily absorbed. This standard was also much more expensive, therefore it never became widely implemented in businesses or homes.

The next standard of 802.11g was introduced in June 2003 and has much in common with 802.11b. This standard was a further development in speed within the same frequency as 802.11b and is the fastest standard in use today.

As everything in the computer world seems to work, the demand for further range and speed continued. In January 2004, IEEE announced that it had formed a task group to develop a new standard called 802.11n. This new standard builds upon previous modifications of 802.11n to use MIMO or multiple-input, multiple-output. This uses multiple transmit and receive antennas to allow for increased data throughput through

multiplexing. This standard has been held back because of bugs and complications, but is expected to be released

Wireless is used in countless different locations and for many different reasons today. The 802.11 standard can be found in hospitals or doctors offices to tie their PDA's, laptops, and tablets into the network. Retail businesses everywhere use wireless for point of sale computers, items which are on display, and even barcode scanners. Coffee shops, restaurants, hotels, and book stores also often offer free wireless for customers and sometimes non-customers.

Most people do not know that their internet traffic across these unsecured networks is often clear text and can be exposed or "sniffed" by a large number of easily available freeware programs. I feel that businesses should not only secure and protect their wireless networks to keep out unwanted traffic, but also keep an eye out for their customers, who might not have much technical know-how. If a business can not go the extra mile and hold itself liable for the customers' well being and security online, they should not offer internet service to the public.

Residential wireless networks have been proven to be the most incredibly insecure networks of all. In most places, there are so many routers and access points in the same area with completely default settings, straight out of the box with no configuration that the signals bounce off one another, causing interference, and sometimes confuse the average user into thinking they are connected to their own signal, when in reality they are connected to their neighbor's, releasing sensitive information into foreign networks unknowingly.

Wireless network security is vitally important, no matter what the application is. Whether you are logging on to simply check your email in a coffee shop or are setting up a wireless network in your home or business, you need to know what it takes to protect your information.

Securing a home network is amazingly easy if you simply take the time and have a little patience to see the project through to the end. If you follow a few simple steps, it will be over before you know it:

First you will want to interface the router or access point. This can be done by opening your computer's web browser and typing in the router's IP address, found in the documentation which came with the hardware (usually 192.168.1.1 or a similar address.) If possible, these steps should be completed from a computer which is wired into your network. This is much more reliable because your wireless system must be refreshed whenever changes are applied.



Find the page titled "Wireless Settings" and disable your Default SSID. This is the name of your router, as seen by your computer. The broadcast of a default SSID such as "Linksys, Default, Netgear, 3COM," or many others, shows neighbors or passers by that your network is more than likely completely wide open and insecure. Do not

change this option to any company or person's name, or anything which can be easily guessed.

Second, straight out of the box, your router's SSID is broadcasted publicly through the air waves. Disabling this option will make it much more difficult for anyone to trace down and connect to your network.



Third, you should change the default password needed to access your router. Default passwords are set by the manufacturer and are easily available by simply searching Google. When this password is changed, you take away a hacker's ability to interface the router as you have been doing in these past few steps and change settings as if they were inside your home.

**LINKSYS**  
A Division of Cisco Systems, Inc.

Firmware Version : v4.20.8 - HyperWRT 2.1b1+tofu6.2

**Administration** | **Wireless-G Broadband Router** | **WRT54G**

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management

---

**Router Password**

**Local Router Access**

Router Password :

Re-enter to confirm :

---

**Web Access**

Access Server :  HTTP  HTTPS

Wireless Access :  Enable  Disable

Web :

---

**Remote Router Access**

Remote Management :  Enable  Disable

Management Port :

Use https :

---

**UPnP**

UPnP :  Enable  Disable

---

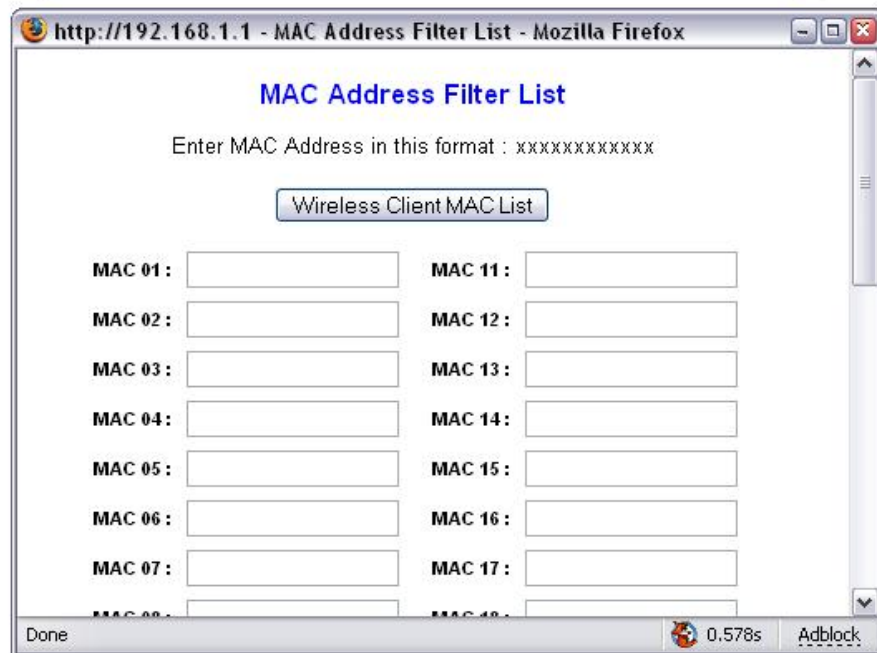
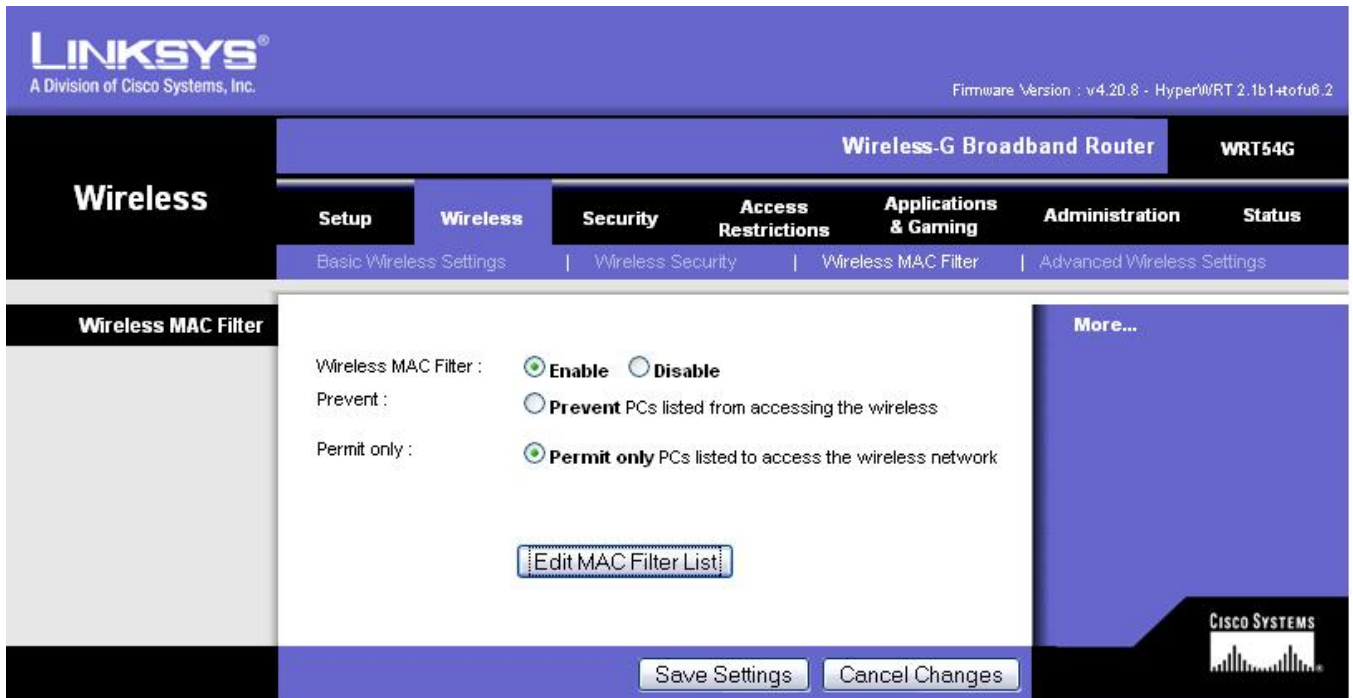
**Local Router Access :** You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

**Web Access :** Allows you to configure access options to the router's web utility.  
**More...**

**Remote Router Access :** Allows you to access your router remotely. Choose the port you would like to use. You must change the password to the router if it is still using its default password.

**UPnP :** Used by certain programs to automatically open ports for communication.  
**More...**

Fourth, MAC address filtering is an excellent way to keep unwanted computers from connecting to your network at all. If their computer's hardware MAC address is not in your router's access list, they will not be able to connect. MAC address filtering can be bypassed by sniffing the wireless traffic and picking out MAC addresses from the packets, allowing the hacker to spoof his MAC address to match your legitimate address.



Fifth, Wireless coverage should not exceed the perimeter of your property. There is no need for excessive coverage in a small home, therefore some routers give the option to attenuate your signal via the web-based setup utility mentioned in steps 1-3.

Finally, the sixth step in securing your wireless network is to implement some type of encryption. WEP (Wired-Equivalent Privacy) is the least secure and most easily compromised method of wireless security, so you should steer clear of it. The next step up is WPA (WiFi Protected Access). This builds on WEP encryption by scrambling the key and integrity-checking it to ensure it hasn't been tampered with. WPA2 is the newest encryption standard. It is similar to WPA but includes the added security of AES encryption, required by some businesses and government agencies. The drawback of this new standard is that some older hardware does not accept it, and Windows XP does not support it without a patch. This makes it much harder to implement in networks that need to be widely accepted to many users.

Even if you do not follow all of these instructions, doing some is better than doing nothing at all. You do not always have to buy a state of the art security system for your home, but locking your front door and closing your blinds is always a good idea.

“Behaviors are difficult to control and people are often under trained or unaware of what security is all about. At the same time, secure information is a critical facet of success for all organizations in today's networked world.”

References:

1. Awan, Irfan. "Performance Evaluation of Wireless Networks." International Journal of Wireless Information Networks Volume 13 (2006)
2. "Complete Guide to Wi-Fi Security." JiWire. 14 April 2006  
<<http://www.jiwire.com/wi-fi-security-introduction-overview.htm>>
3. Johnson, Everett C. "Security Awareness: switch to a better programme." Network Security Issue 2 (2006): 15-18.
4. "MIMO (Multiple-input multiple-output)." NetworkWorld. 16 April 2006.  
<<http://www.networkworld.com/details/6830.html>>
5. "Wi-Fi." Wikipedia. 16 April 2006 <<http://en.wikipedia.org/wiki/Wi-Fi>>