

Securing Your Wireless Network

By Joey Heape, I.T. Director, SC Bar

There's old saying that goes something like "locks are to keep honest people honest." That goes for wireless network security. If someone wants to get in to your wireless network they probably can. But, who said you had to make it easy for them. And the old adage takes into account that if the door is locked and cannot be opened with a twist of the knob the person of questionable character moves on.

Like locking your doors there are ways to keep your wireless network from being used by your neighbors. We are going to look at a few ways to make your wireless network a little safer and harder to get into. The examples I will use are found on a Netgear WGT624v2 wireless router. This router can be purchased at Best Buy or Circuit City. There are many varieties in the Netgear line but this one I happened to be familiar with. Most of the settings discussed can be found on the other brands. The settings may be named differently but they control that same type of settings. While this setup is not Fort Knox it will help in keeping risk to a minimum.

Wireless Settings:

In the screen shot below there are couple of things to note. First is the Name (SSID). The SSID is basically your wireless network name. When you look at the wireless connections on your laptop or wireless workstation the Name or SSID will show up in the window. This means that the receiver has found your wireless network.

The next thing to notice is the Security Options. Notice that this one is set to WEP. Now most people will argue that WEP is not secure. Just remember the door knob. We are just making in difficult. I use WEP because my laptop's built in wireless adapter does not support WPA-PSK. I'll mention that most of the settings here will be driven by the ability of my laptop's wireless adapter card.

The security key will need to be copied from the router and entered into the settings on your laptop or workstation. If you type in a word in the passphrase and click generate the router will generate the key. The key will need to be typed into the settings of your wireless adapter.

Setup Wizard

- Setup
- Basic Settings
- Wireless Settings
- Content Filtering
- Logs
- Block Sites
- Block Services
- Schedule
- E-mail
- Maintenance
- Router Status
- Attached Devices
- Backup Settings
- Set Password
- Router Upgrade
- Advanced
- Wireless Settings
- Port Forwarding / Port Triggering
- WAN Setup
- LAN IP Setup
- Dynamic DNS
- Static Routes
- Remote Management
- UPnP
- Logout

Wireless Settings

Wireless Network

Name (SSID):

Region:

Channel:

Mode:

Security Options

Disable

WEP (Wired Equivalent Privacy)

WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)

Security Encryption (WEP)

Authentication Type:

Encryption Strength:

Security Encryption (WEP) Key

Passphrase:

Key 1:

Key 2:

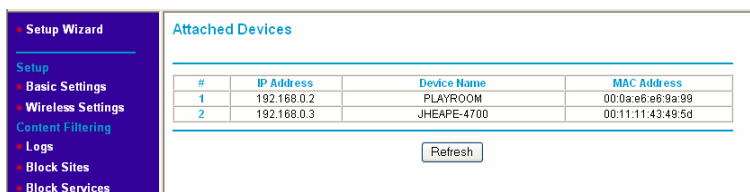
Key 3:

Key 4:

http://192.168.0.1/WLG_adv.htm

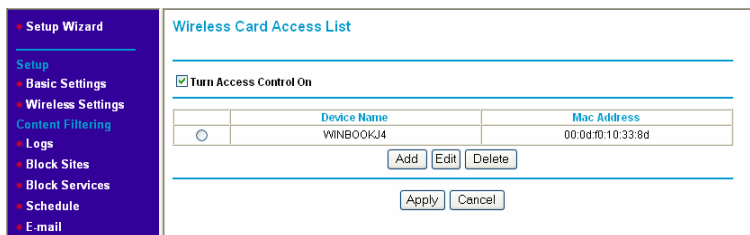
MAC Address:

Another setting we will look at is the MAC address. The Netgear has the ability for you to enter a MAC address the will restrict access by MAC address. What's a MAC address? Suffice it to say that there are no two network adapters in the world with the same MAC address. However, MAC addresses can be spoofed. But, it's difficult to find out a MAC address unless someone has direct access to your computer or knows how to sniff packets on a network. You can find your MAC address by going to Start>Run and typing CMD. In the DOS window type IPCONFG /all and look for the numbers next to the Physical Address of the wireless adapter. Or, once your are connected to your wireless network goe to Attached Devices like the screen below shows. Write down the MAC address of your laptop.



#	IP Address	Device Name	MAC Address
1	192.168.0.2	PLAYROOM	00:0a:e6:a6:9a:99
2	192.168.0.3	JHEAPE-4700	00:11:11:43:49:5d

Next go into the Setup Access List under the Advanced Wireless Settings and add your MAC address here and check the box “Turn Access Control On”. (see screen shot).



Device Name	Mac Address
WINBOOKJ4	00:0d:10:10:33:8d

Now the only machine that can access your wireless network is the one in this list.

Running under the Radar

Now that you are connected your wireless network there's one more thing I would suggest you do. Keep mind that if you are connected your wireless profile should be saved in your laptop's settings. Which means, there's no need to be broadcasting the SSID or name of your network. I turn off “Enable SSID Broadcast”. This way, when your neighbor fires up his laptop your network won't show up in list of networks.

The last thing I would suggest is if you are not using the wireless part of your network turn the radio off. Occasionally, I'll work at the kitchen table which is where I use my laptop. But I will go several weeks and not use the wireless part of the network. No need to give anyone a door knob to turn.

Using Someone Else's Wireless Network

I had the privilege of going to one of the finest hotels in the east recently to find that they offered a wireless network. If you find yourself with the opportunity of using someone else's wireless network make sure you have:

1. turned on the firewall (in Windows XP) for your wireless adapter, or use a personal firewall of some type.
2. use an anti-virus program with recent signatures,
3. use an anti-spyware program with recent signatures.