How to set up your wireless network

There are several steps involved in securing your wireless network. I recommend that you take these steps in order and only change one item at a time. While this may seem time-consuming, it makes it much easier to trace any mistakes you might make entering keys and securing your wireless LAN. This is especially true if you have several wireless machines to worry about!

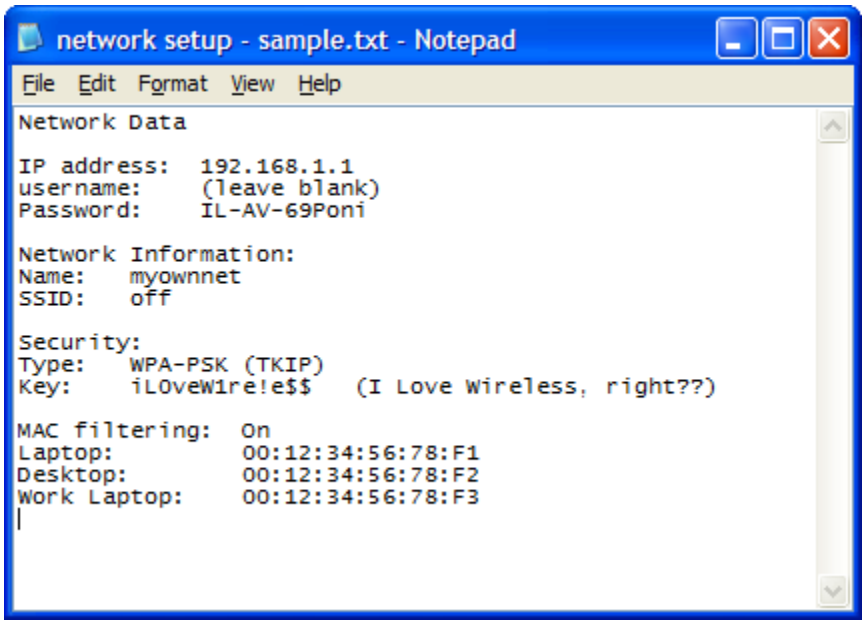
The steps to take are listed below:

1) Create a file for your settings.
2) Log in to your wireless router.
3) Change your administrative password.
4) Change the name of your wireless LAN.
5) Enable security settings on your router.
6) Enable security settings on each wireless client.
7) (Option for greater security) Enable wireless MAC filter.

So let's get started! If you are simply reloading settings after your router "burped", feel free to jump ahead to the applicable sections and reload your information. However, if this is your first time setting up your LAN, let's start by getting everything together and in one place.

1 - Create a file for your settings

It's really easiest if you start by creating (or finding) all the settings you will need beforehand. I like to start with a short text file that I create so that I can open it without any specific type of word-processing software being installed on the machine. Here's a sample of what I mean:



Note that you can download this file from www.stakenet.com to help you get started.

First, I enter the IP address and username I need to access the router—a minor point, but it saves me from having to remember it later.

Next, I create my administrative password for the router. It should be something secure, but not too difficult for you to remember (and something other than "admin", please!!!) Perhaps a word or phrase with numbers substituted for letters or words. You can also add special characters, so consider using "@" for an "a", an "$" for an "s" or other possibilities. You can see I've used a license plate, but anything is possible…

Now, choose a name for your network. Select something that is unique without being too identifiable (your address or last name would not be the best choice). I've noticed that a lot of people use names of pets, but you might prefer something different.

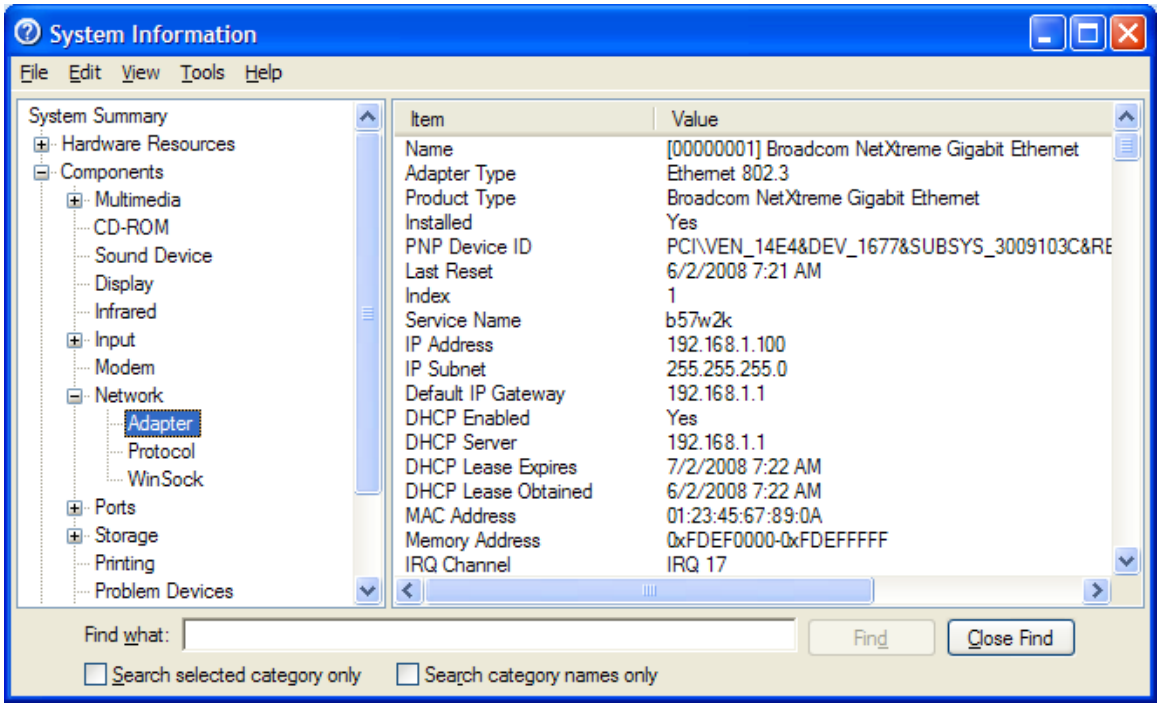
Time for some research: You will need to know some information about each of your wireless devices, not only the MAC address, but also you need to know the highest level of security that ***every*** device in your network will support. So it's time to do some sleuthing. For each wireless device, you need to check both: **MAC address** and **best wireless mode** for each device (laptop, wireless card, or whatever). Remember that the MAC address is a series of 12 hexadecimal characters (from 0-9 and A-F) separated by colons (:) into groups of 2.

I like to enter the MAC addresses for each device—wired as well as wireless devices—along with a brief description of the device or computer it applies to. Keep this with your network setup information—you'll be able to use it for MAC address filtering, and also if you choose to limit access to specific machines using time clock or keyword filtering functions, you'll have the information already (my wife uses this to keep me off of eBay!!!)

Finding MAC Addresses:

You can find information about Encryption support and MAC addresses in each individual instruction manual, or possibly on a sticker on the wireless card or laptop. If you have trouble finding the MAC address, you can dig around in the OS to find it:

> -- In Windows (XP or Vista), go to System Information instead: "**All Programs**", "**Accessories**", "**System Tools**" then "**System Information**". Now, select "**Components**", "**Network**", and "**Adapter**" to find all adapters. Look for your wireless adapter listed under Name and/or Product Type. Find the "**MAC Address**" information and copy this into your network setup file. Here's a screenshot from system information (the MAC address is third line from the bottom: **01:23:45:67:89:0A**).



ALTERNATE METHOD: If you can't figure out the MAC address for a particular device—this could occur if it is a Mac, gaming console, or other non-standard device (like when I set up an iTouch for a customer's daughter), you can temporarily attach the wireless device to your router and go to the router's status page to view DCHP clients connected. Each client will have a DHCP address and the corresponding MAC address next to it. If you did this before setting your network encryption, don't forget to enable encryption afterwards, as your network is wide open until you do!

Best Encryption Mode:
Regarding the best wireless mode for each device, some will support **WiFi Protected Access (WPA)**, while some will only support the older **Wired Equivalent Protocol (WEP)** protocol.

If any device is limited to WEP, you are forced to use WEP only for your encryption. If you are in this situation, I would *strongly* urge you to consider upgrading that device to support WPA access (with a new wireless adapter, perhaps???)...

Create PassPhrase:
Next, you will want to create a passphrase. This should be unique, and can include upper- and lowercase letters, numbers, and special characters. Do not use words or names, as they can be subject to dictionary searches. You can start with words, and then substitute other characters "@" for "a", "$" for "s", "!" for "l", and so on. One example would be: "iL0veW1re!e$$" as I have used in the example above. Don't make it too short it must be between 8-64 characters in length, as required by WPA. **NOTE:** If you are forced to use WEP, you will need either a 13 or 26 character passphrase.

(If you have trouble creating a passphrase, you can try these sites and use their passphrase generators to create—and in some cases manage—your WEP and WPA keys):

For WPA Keys:
http://www.yellowpipe.com/yis/tools/WPA_key/generator.php
http://soroban.co.uk/wepkeygen.htm

For WEP keys:
http://www.andrewscompanies.com/tools/wep.asp
http://clariondeveloper.com/wepgen/
http://soroban.co.uk/wepkeygen.htm

Once you have all the information, save the file (and your keys) somewhere on your computer (**My Documents** directory, perhaps?) and possibly on a memory stick as well for ease of transporting to the other machines. Once everything is finalized (*after* your network is up and running), I suggest printing out the information as well. As you change your encryption keys (every 3-6 months or so?) make sure to update your information.

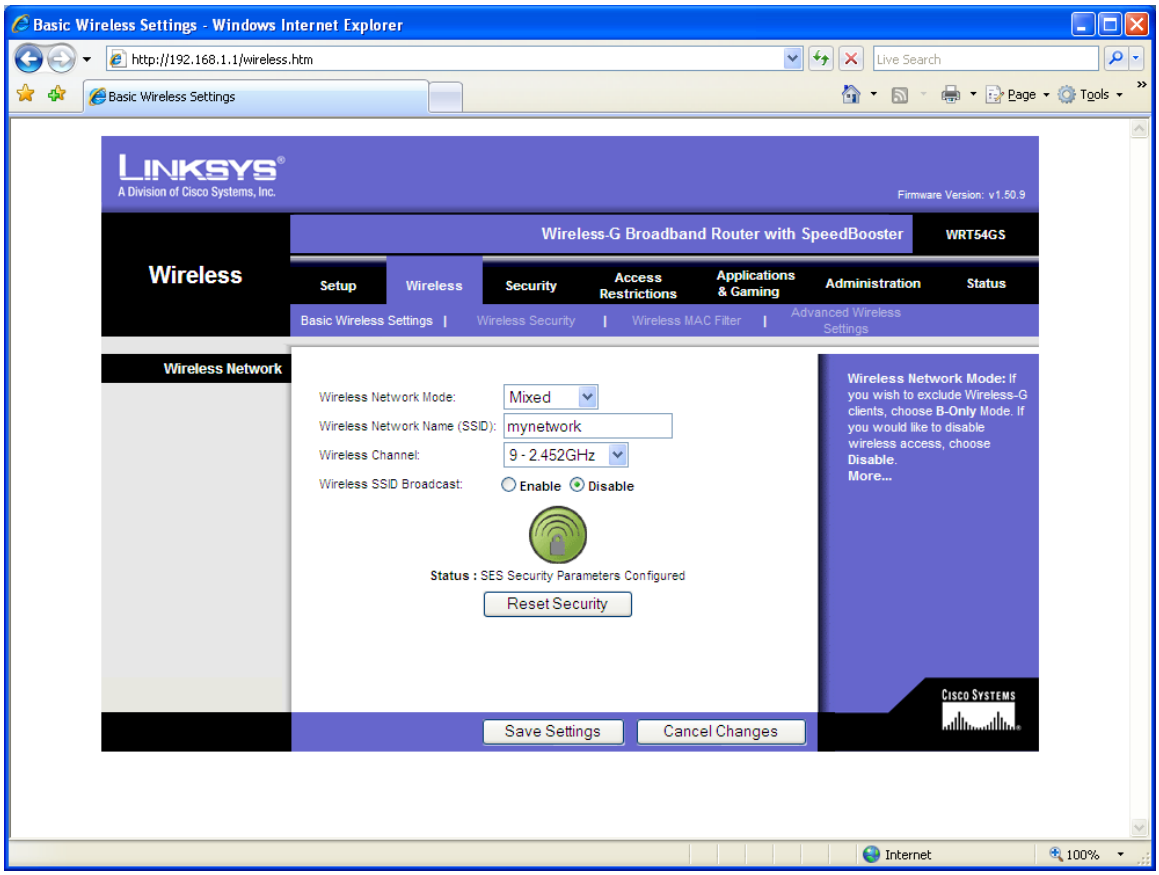
Now we are armed with all the information we need, let's ***really*** get started!!!

2 – Login to your wireless router

First, log in to the router by opening a web browser and entering the address for your router. This is normally 192.168.1.1 or 192.168.0.1 (depending on manufacturer).

You will be presented with a login screen. Enter your password (or if applicable, username and password). Linksys units have no username and use "admin" as their password (all lowercase!)

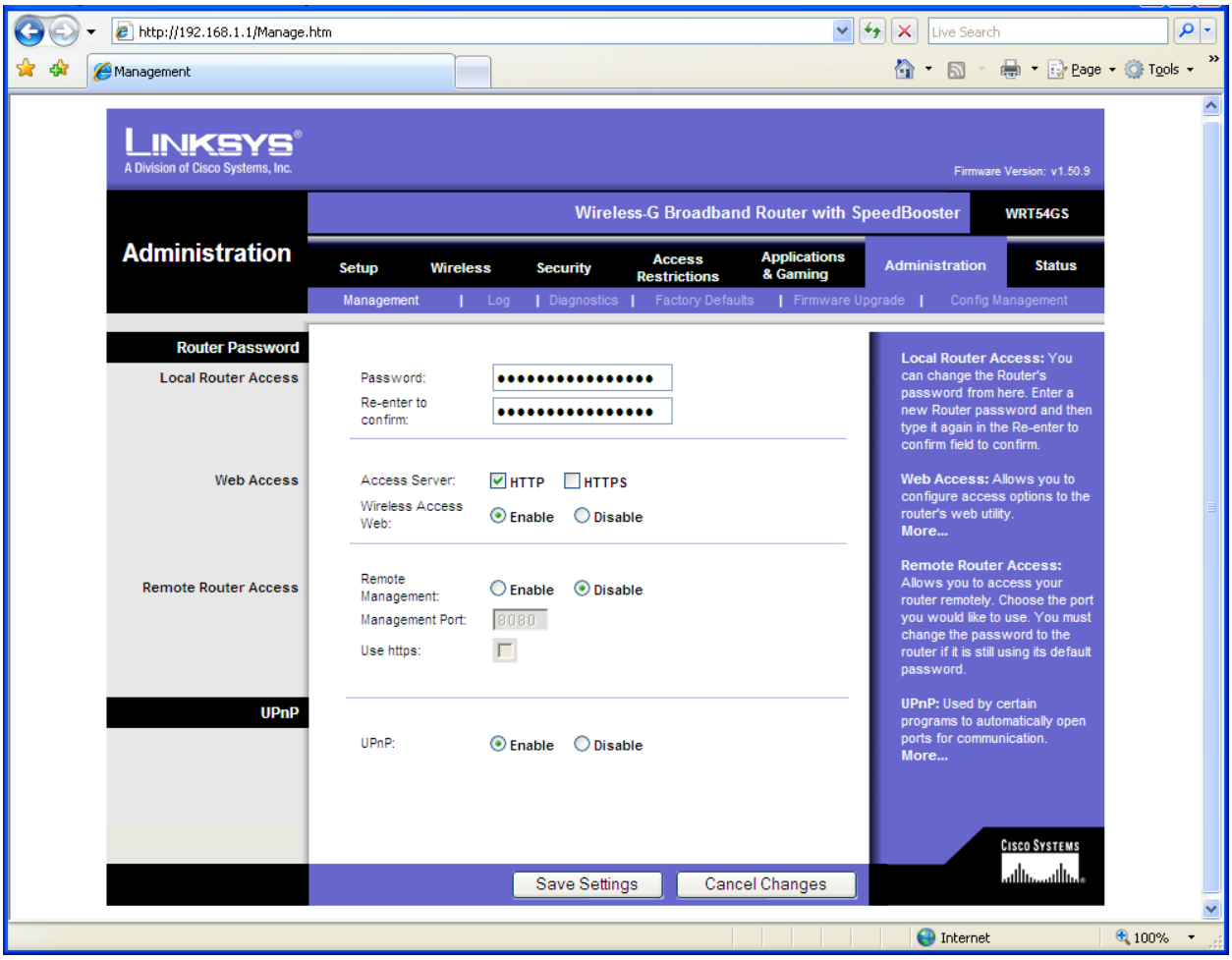
Once logged in, you will see the basic screen:



(Note that my screenshots are all taken from configuration pages on the Linksys router, but yours should be similar…)

3 - Change your administrative password

Now let's change the router password. Select the "Administration" tab, second from the right. You will see the following screen:



Type in an administrative password for the router, and type it in the second box to confirm. It should be something secure, but not too difficult for you to remember. Perhaps a word or phrase with numbers substituted for letters or words. You can also add special characters, so consider using "@" for "a", an "$" for "s", "!" for "l" or other possibilities you might come up with yourself. Be creative here!

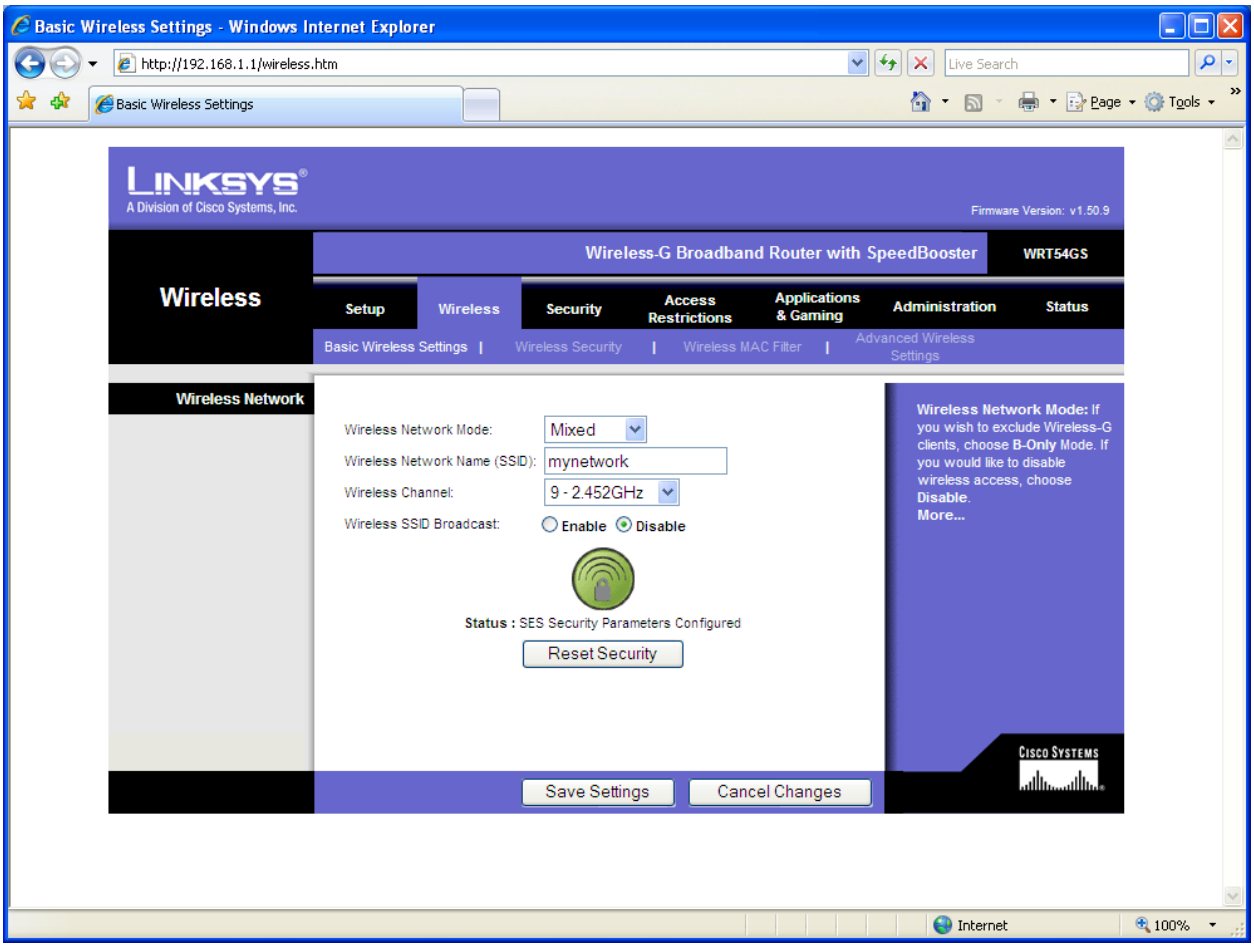
You will have to type the password in both boxes and make sure you overwrite the dots in the password box and the confirmation box. Now, click "**Save Settings**".

You will know that the password has been changed when you are presented with the login box again. The router is now waiting for you to enter the new password, so login with the new password (don't forget there is no username on Linksys products!)

4 - Change the name of your wireless LAN

Next, let's change the name of the wireless LAN itself. This makes it easier to tell that you are connecting to your own LAN (instead of one of your neighbor's!)

While still logged in, click on the "**Wireless**" tab to see the following screen:



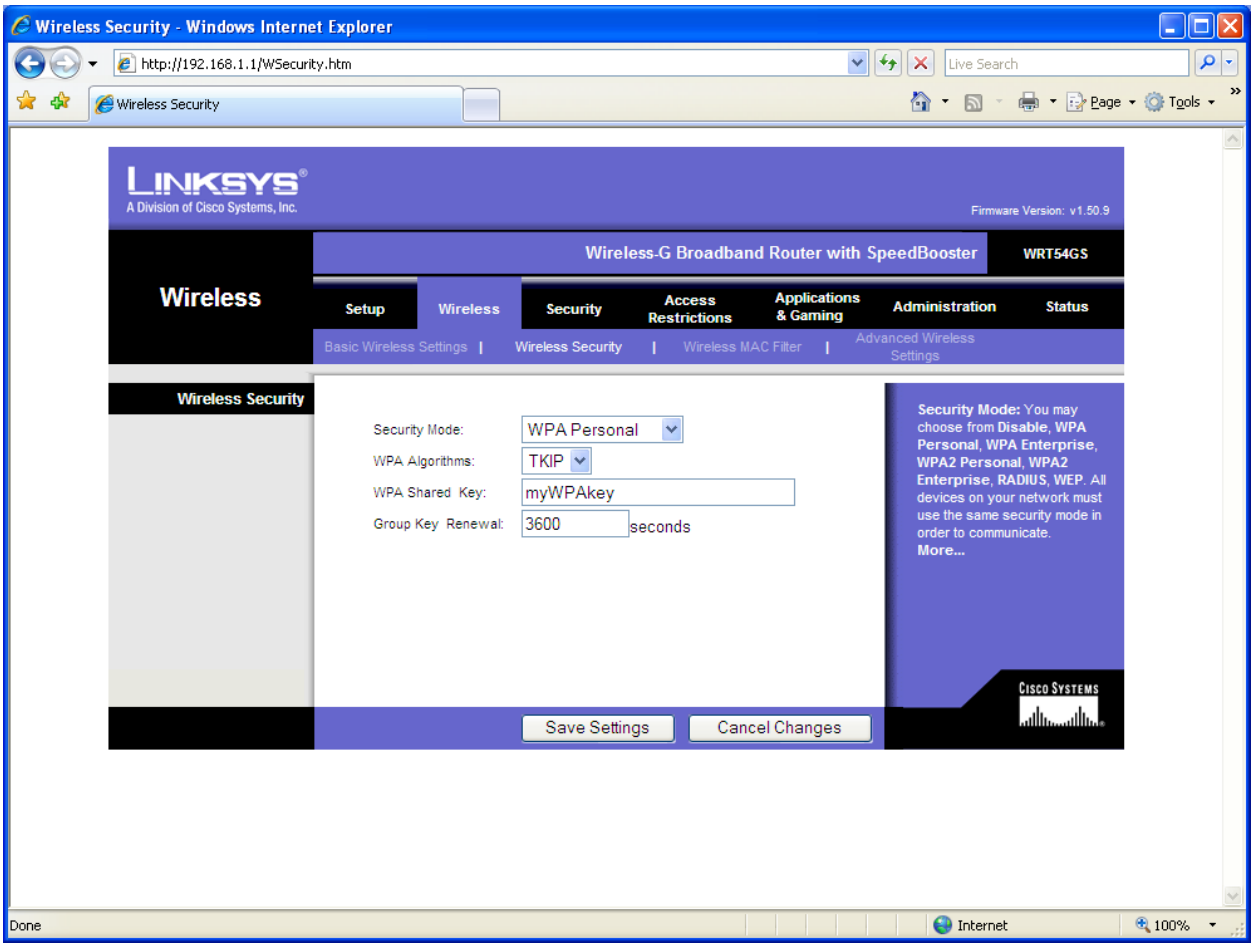
Enter your new wireless name in the "**Wireless Network Name (SSID)**" box. You definitely don't want it to say "linksys", "belkin", "2wire" or "d-link", etc. Select something that is unique without being too identifiable (your address or last name would not be the best choice). I've noticed that a lot of people use names of pets, but you might prefer something different.

Now, go to the "**Wireless SSID Broadcast**" line, and select the "**Disable**" radio button. This prevents others from seeing your well thought out and unique LAN name, and they can't connect if they don't know the name.

This is also the page where you can change the channel if you find another LAN broadcasting on the same channel as yours. Simply pull down the channel box and select a new channel to see if you get a better connection. Don't forget to "**Save Settings**" before you leave this page.

5 - Enable security on your router

Now it is time to enable security on your router and each individual wireless client. Select the **"Wireless"** tab again, and now select the **"Wireless Security"** submenu. Your screen should look like this:



There are several steps to take here:

1) First, select the best highest security mode all your devices can support. If you can select **"WPA Personal"**, then do so. If one of your devices will only support **"WEP"**, then select that instead. You might also consider upgrading that device to support WPA access in the future...

2) For your WPA Algorithm, select "**TKIP**".

3) Now, create and enter a WPA shared key or ***passphrase***. This should be unique, and can include upper and lowercase letters, numbers, and special characters. One example would be: "iL0veW1re!e$$" Don't make it too short, it must be between 8-64 characters in length.

Again, be sure to "**Save Settings**" before you leave this page. Note that you will lose your wireless connection until you enter the settings on the device (next).

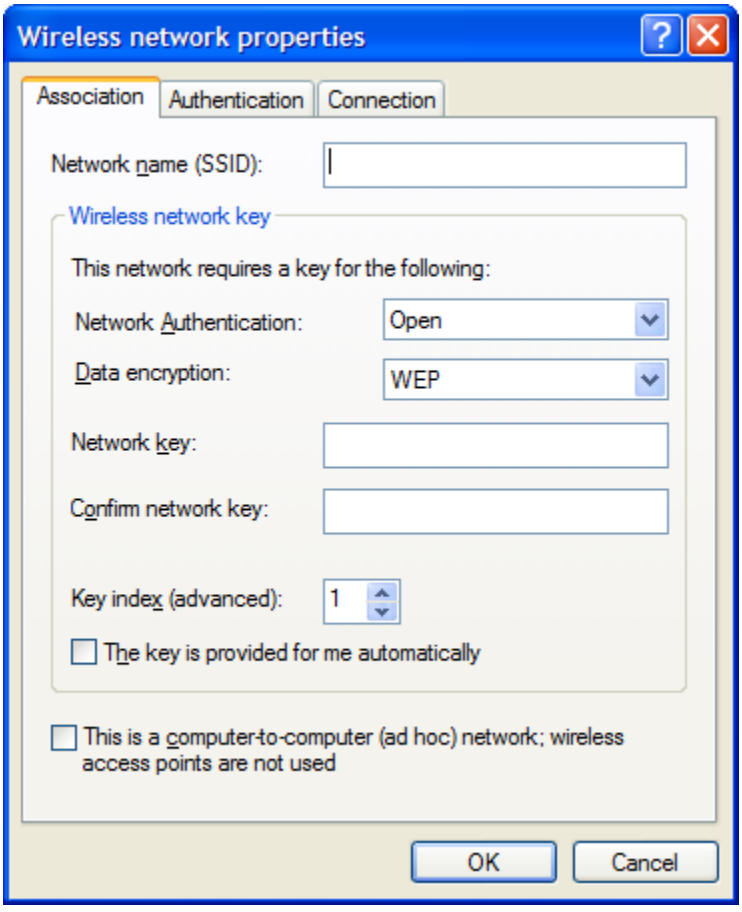
6 - Enable security on your clients

Now it's time to enter security settings for each wireless client/computer. It ***really*** helps to have all of your setup information (that we saved in the .txt file earlier) stored on a USB key as you set up your clients. I recommend this especially when you have a complex passphrase, so that you can copy and paste it from the text file and enter it in each machine without error!

Probably the easiest way to do this is through the "**Network Connections**" under "**Network and Internet Connections**" option in Control Panel, then "**View Available Wireless Networks**." (Another path is to right-click on the wireless icon in the system tray, and "**View Available Wireless Networks**.")

When the **Wireless Network Connection** page opens up, go to the left side, under "**Related Tasks**" and select "**Change the Order of preferred networks**."

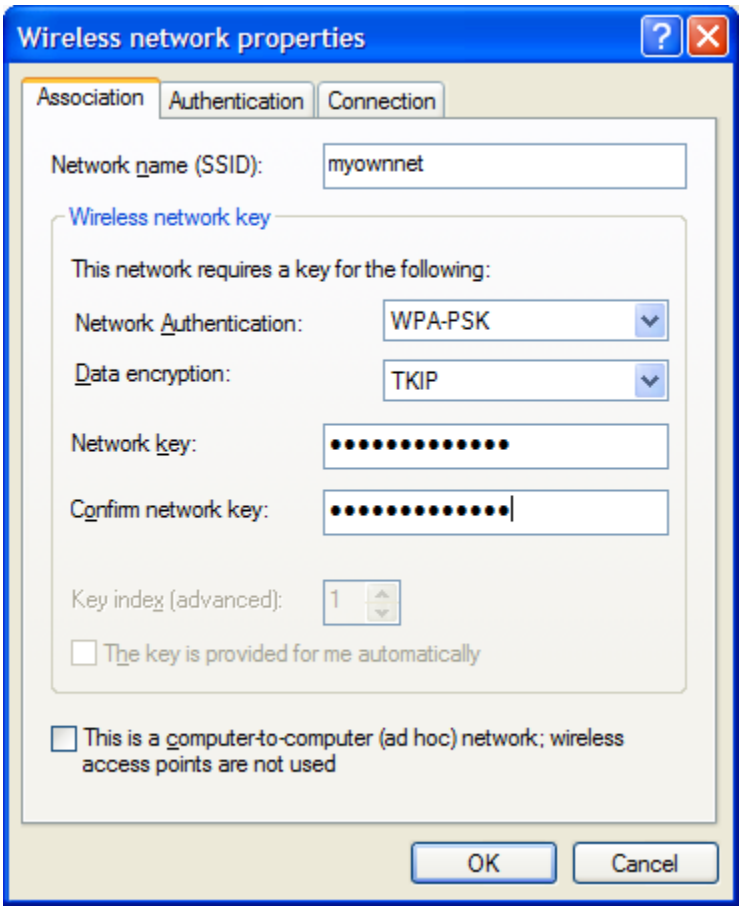
Under the "**Preferred Networks**" window, click "**Add**" to open up the configuration window:



(Make sure to **uncheck** both boxes at the bottom of this screen)

Now, enter your SSID, and set the appropriate encryption level (WPA-PSK preferred) and data encryption (TKIP or AES).

Once these are set, enter the passphrase (under Network Key) and then re-enter this passphrase in the next block. Notice that the passphrase will not show (but instead show as dots). If you copied the passphrase from your setup file, you can right-click and paste in each field if you like:



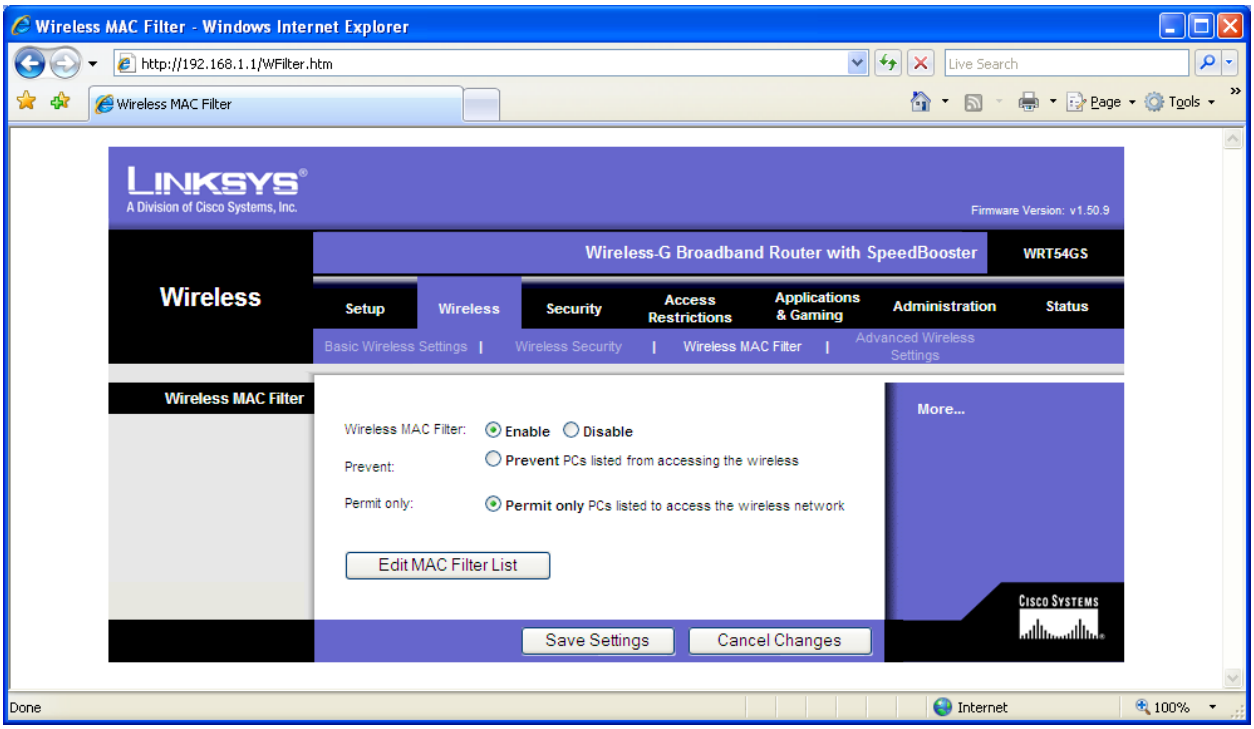
Click "**OK**" and your settings will be saved. At this point, your wireless device should connect to the router automatically.

If the device does not connect, go back and make sure all the setup information has been entered the same in both the router and the laptop or card.

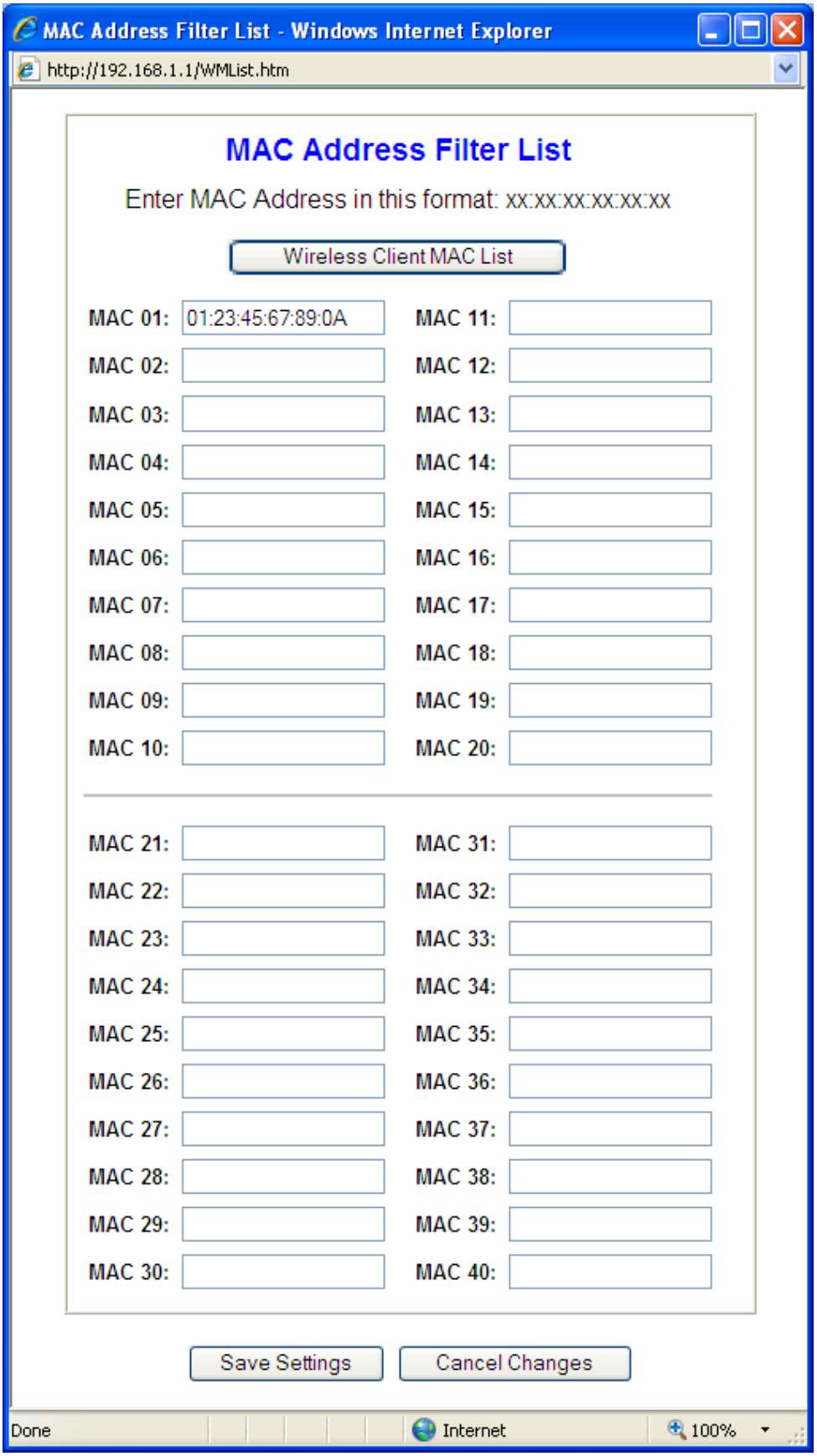
7 - Enable wireless MAC filter

While your network is set up now, and is secured, there is an important additional step that you can take (and that I recommend for every network installation). This is to enable filtering based on the individual MAC address of each wireless device. Now, log into the router again, and get to the right page for MAC filtering.

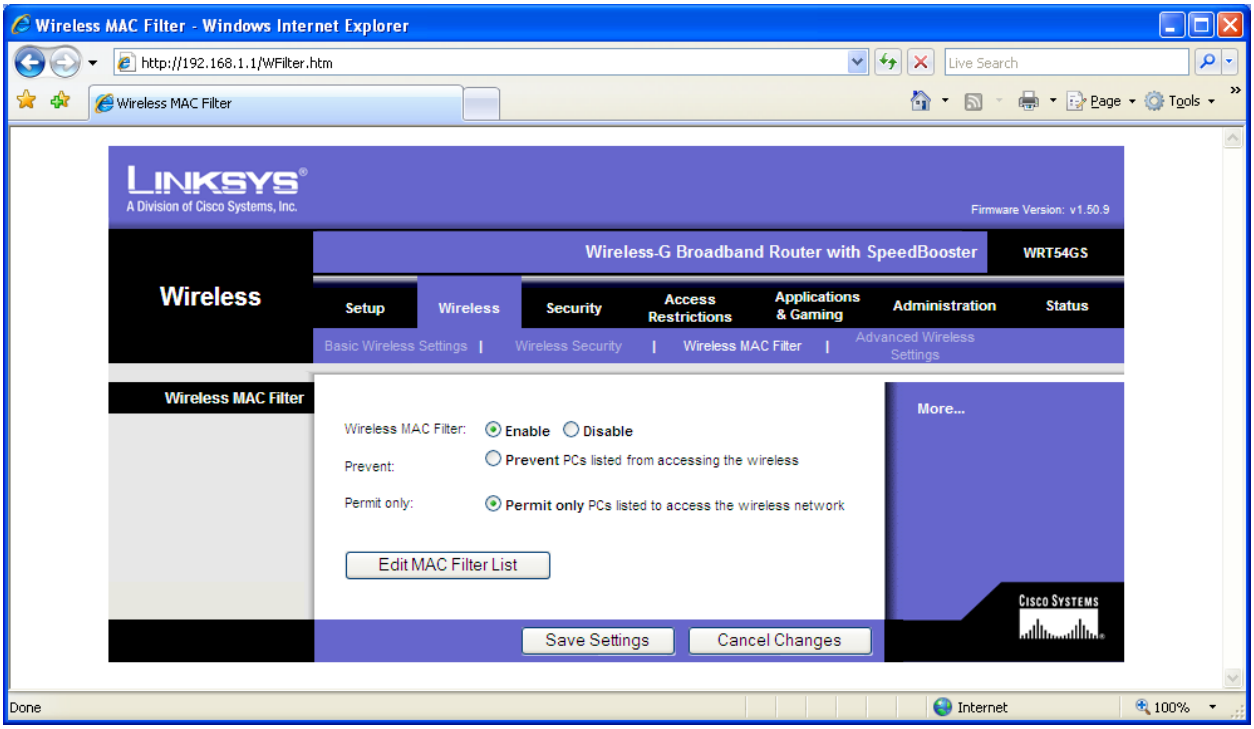
On Linksys routers, select the "**Wireless**" tab, and "**Wireless MAC Filter**" page. Enable the filter by selecting the "**Enable**" radio button and the "**Permit only**" radio button to show the following screen:



This page will enable you to access and control the MAC Filter List. Let's start by entering the MAC addresses for each wireless device on your network. Click on "**Edit MAC Filter List**" and, for each wireless device, enter the MAC address using the numbers 0-9 and letters A-F. In the example below, I have entered "**01:23:45:67:89:0A**" for the first MAC address. When finished, click on the "**Save Settings**" button:


MAC Address Filter List - Windows Internet Explorer
http://192.168.1.1/WMList.htm
MAC Address Filter List
Enter MAC Address in this format: xx:xx:xx:xx:xx:xx
Wireless Client MAC List
MAC 01: 01:23:45:67:89:0A
MAC 02:
MAC 03:
MAC 04:
MAC 05:
MAC 06:
MAC 07:
MAC 08:
MAC 09:
MAC 10:
MAC 11:
MAC 12:
MAC 13:
MAC 14:
MAC 15:
MAC 16:
MAC 17:
MAC 18:
MAC 19:
MAC 20:
MAC 21:
MAC 22:
MAC 23:
MAC 24:
MAC 25:
MAC 26:
MAC 27:
MAC 28:
MAC 29:
MAC 30:
MAC 31:
MAC 32:
MAC 33:
MAC 34:
MAC 35:
MAC 36:
MAC 37:
MAC 38:
MAC 39:
MAC 40:
Save Settings
Cancel Changes
Done
Internet
100%

Once your MAC addresses are loaded, make sure to "**Save Settings**" and then get back to the main MAC filtering page. Select the "**Wireless MAC Filter**" page again, and make sure you have selected both the "**Enable**" and "**Permit only**" buttons. Finally, select "**Save Settings**":



At this point, only the computers you have specified can access the network wirelessly. If you wish to test this, the easiest method would be to change one of the MAC filter entries (by changing one digit) and then verify that the specified device cannot access the net. It will be a simple matter to change it back and get that device back online.

You can also use the MAC filter function to prevent access by a specific MAC address, by selecting "**Prevent**" instead of "**Permit**" but this opens the network up to access by other users.

I'm always open to suggestions for revisions and improvements, please contact me!

(Rev1: System Information procedure and screenshot added for Vista users, 7/29/08)