

Secure your home wireless network

While visiting a friend, I connected my laptop to his wireless network without any password; took all of 2 minutes. “Hey, how come your wireless isn’t secured?” I asked. Turned out, that’s the way his internet provider set it up. Briefly, I explained how anyone could drive by with a laptop, login to his wireless, and then access his computers. Since he does a lot of corporate work from home, securing his wireless was definitely a priority. In about 15 minutes, I secured his wireless network with the settings I’ll detail below.

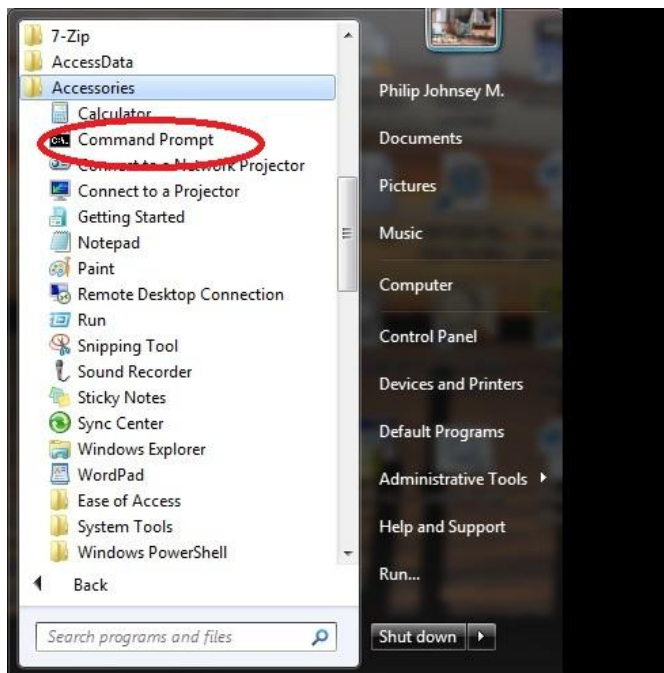
Leaving your network unsecured is like leaving your door to your house unlocked. Regardless of how you use your network, it should be secured and it’s not as difficult as you may think and will help protect your information.

Most of my writings are short, but this one has a lot of screen shots so it appears to be long. I suggest reading through the entire document to understand what is happening before changing the settings.

Setting the router password:

Every wireless router has a password that is used to set it up and configure it for home use. If someone else has this password, they can access your wireless router and change the configuration. This could keep you from using your own network. The process of changing the password is easy, just getting there can be a bit tedious.

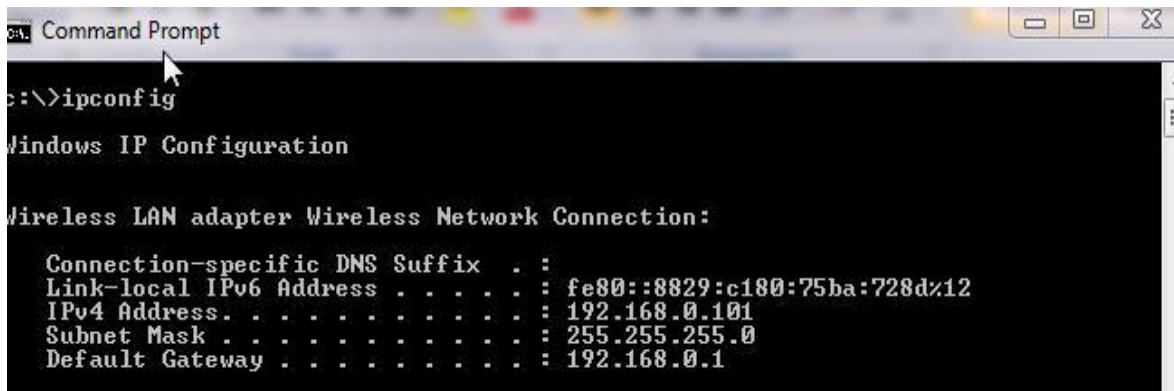
First off, we have to find the address of your wireless router. If you’re using a Windows flavor (XP, Vista, 7), select All Programs, then Accessories, then Command Prompt:



You will now see a black screen with white letters:



Now type in the following: `ipconfig` and press enter. You will see your network settings:



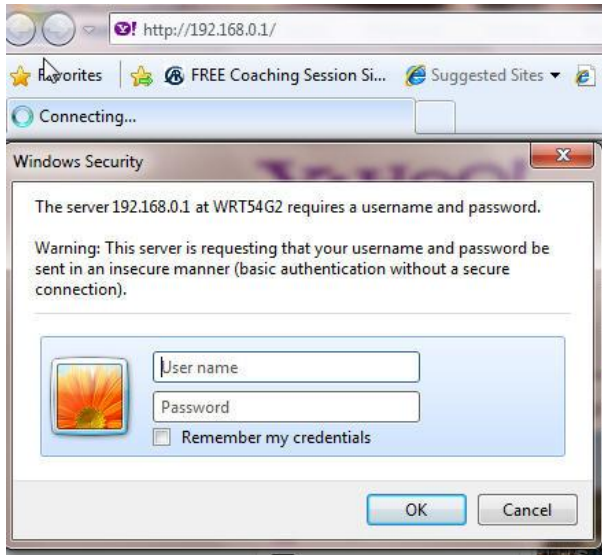
These network settings are how your pc communicates to the internet and each one has a very specific, important function:

The IPv4 address is your current network address & is specific to your machine. (it's just like your home address).

The gateway address is actually the address of your wireless router. A router allows your pc out onto the internet, hence the name gateway.(simple explanation).

Leave this screen available so you can refer back to it and open up an internet browser (Explorer, Mozilla, Chrome, Safari, etc). In the address bar (where you type www.google.com), type in the **gateway numbers**& press enter.

You'll be prompted for a username and password, like below:

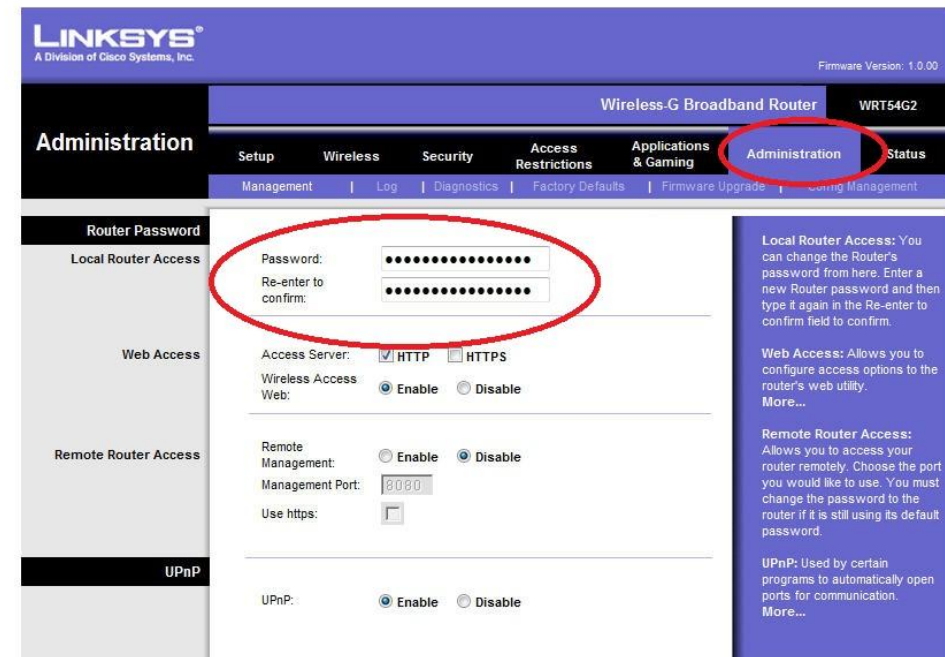


If you set up the router yourself, you'll know this password. If your internet provider set this up, you may or may not have the password. In the case of my friend, he didn't know the password. A quick internet search for his model router yielded the default password. If you don't know the password, you have a few options:

- 1) search the internet for your specific brand's default password
- 2) contact your internet service provider (ISP)
- 3) contact the routers manufacturer.

Once you're logged in, you'll see a lot of options and screens to navigate. It looks daunting, but we're just going to look at a few critical sections.

Go to the Administration tab and enter a new password in the password fields.



Important Note!!!

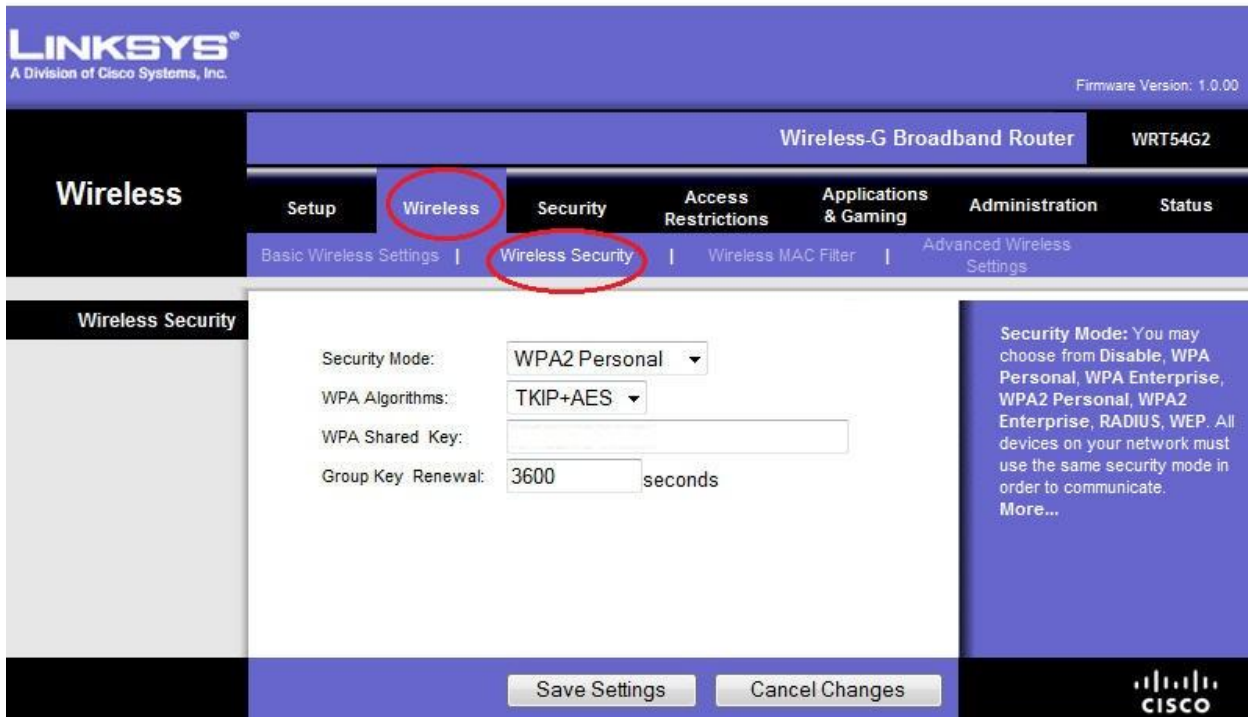
Be sure to write down the username and password and save it somewhere you remember. I recommend a little notepad by the pc to document all passwords.

At this point, all we've done is changed the password to the router. This will deter someone else from logging in and changing your router settings. However, people can still access your wireless network uninhibited.

Setting the wireless password & authentication:

This next step is where we set the password required to access the wireless network. Changing this will kick people off your network so make sure everyone is offline. You don't want to hear "what happened to my work" from somewhere upstairs.

In the same interface that we changed the router password, look for a tab named **Wireless** and then under that select **Wireless Security**:



The screenshot shows the Linksys web interface for a Wireless-G Broadband Router (WRT54G2). The top navigation bar includes 'Wireless', 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Wireless' tab is selected, and the 'Wireless Security' sub-tab is also selected. The main content area is titled 'Wireless Security' and contains the following configuration options:

- Security Mode: WPA2 Personal (dropdown menu)
- WPA Algorithms: TKIP+AES (dropdown menu)
- WPA Shared Key: (empty text input field)
- Group Key Renewal: 3600 seconds (text input field)

On the right side, there is a blue box with the following text: "Security Mode: You may choose from Disable, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, WEP. All devices on your network must use the same security mode in order to communicate. More..."

At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'. The Cisco logo is visible in the bottom right corner.

Security Mode will be set to disabled, change it to **WPA2 Personal or similar**. If you have older machines, the WPA2 might not work. You'll find out soon enough and as you can see, it's easy to change.

Under the Algorithms select **TKIP+AES**.

The WPA Shared key may be generated for you or you may have to enter it. If you create one, make it alphanumeric which is more difficult to guess. Then write it down and save it.

Save the changes and you'll quickly find you've lost your wireless access.... That is a good; it means the security is working. All you need to do is reconnect and when prompted for a password, enter the one you just created. If your laptop is Windows, you'll need to reconnect using the wireless icon in the lower right corner of your pc.



The middle icon is the wireless one on Windows 7 & Vista.

If you use a MAC, it works similar just find either the settings or wireless tab. You only have to enter this password once because the computer will remember.

Now test all of your laptops, tablets, or pcs that connect to your wireless and make sure they all work.

If not, you may have to change the encryption. You can always set the security back to disabled and that will allow everyone back on. From there you can try different options till you find one that works.

Okay, so we've set a password for your router and set a password for users to access your network. You can stop here or continue reading for more security options.

Limiting the number of connections to your network:

Out of the box, the router will be set for unlimited connections. Aside from your devices, that means everyone else can connect. You could connect the whole neighborhood! While this is fine for wireless access points, we want our home network to have limited access. Lucky for us, this is probably the easiest setting to change.

We're back to our familiar configuration page: select **Setup** and then **Basic Setup**. A few lines down you'll see an option to limit DHCP users. Change this number to reflect the number of devices that connect. I had mine set initially for 2 connections, then my girlfriend brought a new tablet pc home and couldn't connect it to wireless. A few unsuccessful connection attempts and then I remembered I had limited the connections. So it does work well. Just have to remember you set it so you don't spend hours troubleshooting why an extra device can't connect. If you want to bump that connection number up by 1 or 2 connections extra, that could save you headaches down the road.

See screenshot on the next page:

LINKSYS
A Division of Cisco Systems, Inc. Firmware Version: 1.0.00

Wireless-G Broadband Router WRT54G2

Setup

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

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: WRT54G2

Host Name:

Domain Name:

MTU: Auto

Size: 1500

Local IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

DHCP Server: Enable Disable

Starting IP Address: 192.168.0.100

Maximum Number of DHCP Users: 4

Automatic Configuration - DHCP: This setting is most commonly used by Cable operators.

Host Name: Enter the host name provided by your ISP.

Domain Name: Enter the domain name provided by your ISP. [More...](#)

Local IP Address: This is the address of the router.

Subnet Mask: This is the subnet mask of the router.

DHCP Server: Allows the router to manage your IP addresses.

Okay so at this point, we've implemented the following:

- 1) Password to access your wireless router
- 2) Password to access your wireless network
- 3) Limited the number of people who can connect

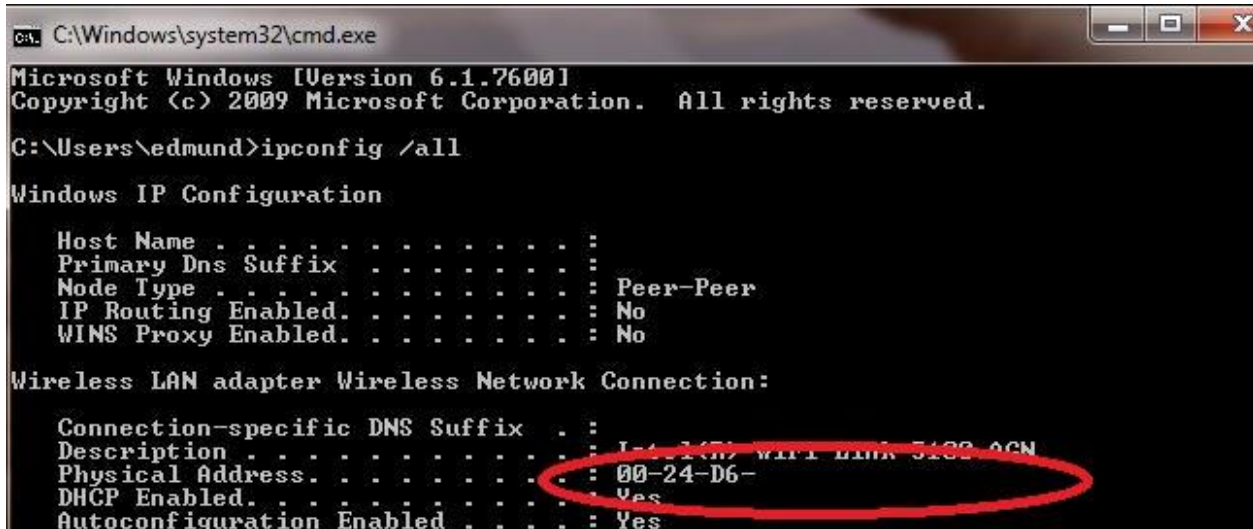
This is pretty good security and you can easily stop here. If you want to secure it even further by only allowing your own machines to access the network, read on....

Limiting connections by only allowing your devices a connection.

When someone knocks on your door, you look out the peephole. If you recognize them you open the door, if not, you take extra precautions. You can set your wireless network to only allow connections it knows.

Every device that connects to the network has a specific hardware number. In computer terms this is known as the MAC address. Since these settings are unique to each device, it's a popular way to filter access.

The first step is to find your MAC address(s) and document them. Open a command prompt (start/accessories/command prompt) and type the following: ipconfig /all



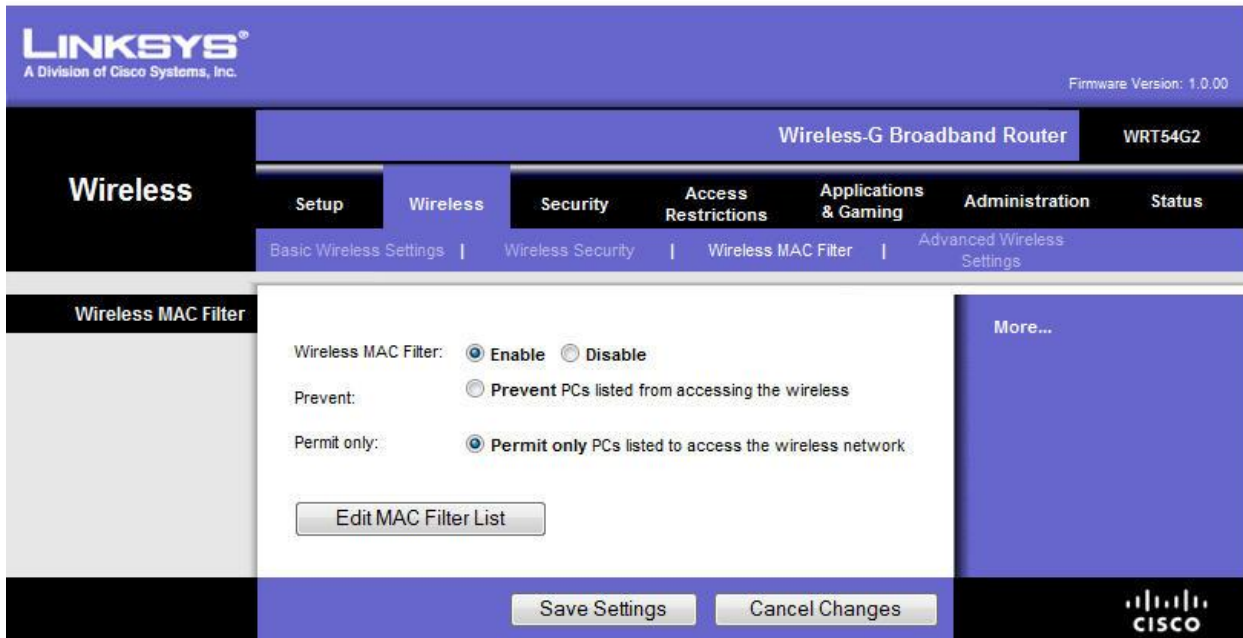
This will show all of your network settings.

Your MAC address will be a series of alphanumeric numbers. It'll be something like 0A:B4:23:67:9Z. (I blacked part of mine out that's why it's so short) **Leave this screen open you can refer back to it.**

Go back to the wireless configuration menus we had open previously. Select **Wireless**, then find the tab labeled **Wireless MAC Filter**.

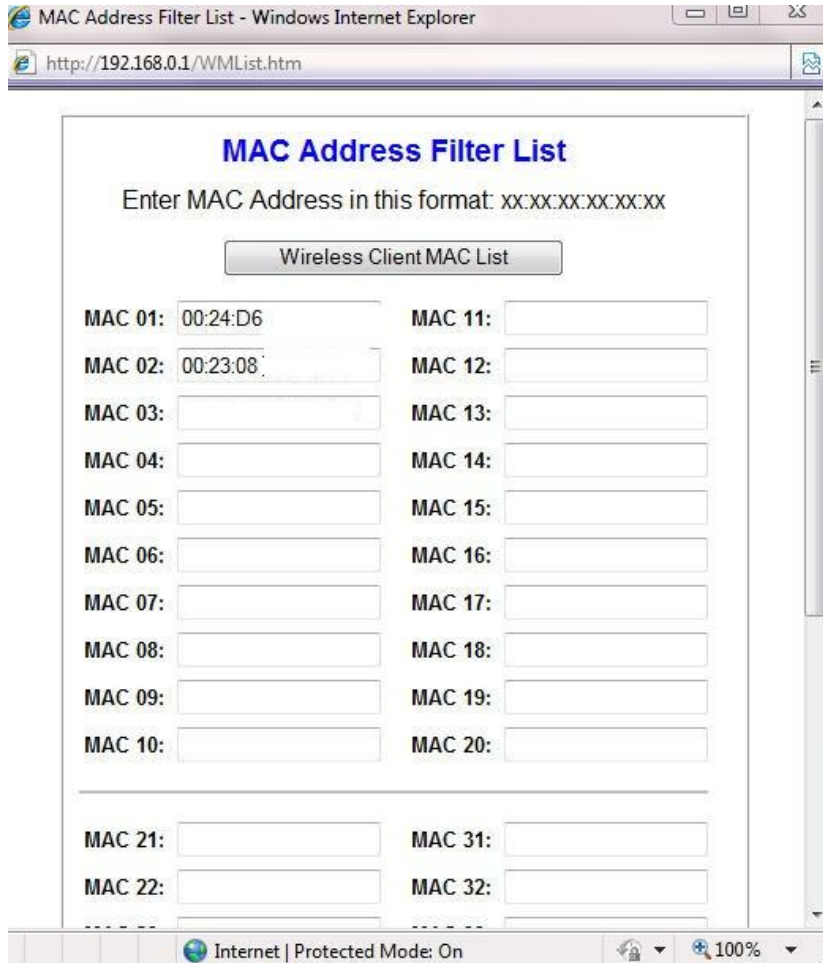
At the Wireless MAC filter setting, select enable.

Highlight radio button for Permit Only.



This will turn it on but you still need to tell it **what** to filter, so select the button on the bottom, labeled **Edit MAC Filter List**.

A page will open & you can enter your MAC address(s). Be sure you enter the numbers correctly. If not, you will not be able to access your own network.



Be sure to select OK/Save when complete so the settings hold. Now only the devices you know can access the network. If someone brings a laptop over and types in the password to your network, they still won't be able to access the network because their ID isn't on the list.

While these security settings aren't a perfect guarantee that someone will not access your network, they do make it much harder. Just like locked doors, sometimes a little deterrent is all that is required.