

SECURING YOUR WIRELESS NETWORK

A home wireless network is an easy and convenient way to share an Internet connection and other resources among the computers in your home. While a couple of people that I know leave their wireless networks available to anyone and everyone, most of us want to keep our home wireless networks private. If you're looking at wireless home networking for the first time, you may want to review these previous Tech Tips on wireless networking.



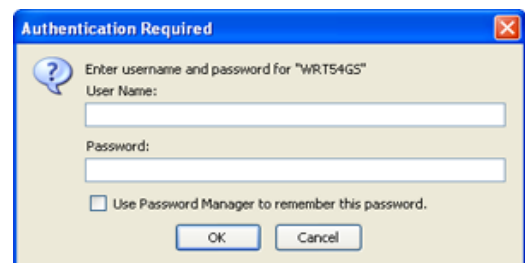
The core of your wireless network is the router. By carrying out some easy-to-do configuration on your router, you can ensure that only the people who you want to have access to your network will be able to.

Note: The procedures in this Tech Tip for configuring a router are for a Linksys WRT54GS router. You'll probably have to modify the specific instructions if you're using a router from another vendor, but the concepts are

the same.

Passwords on Your Router

You configure most routers using a Web browser. When connect to the router, you need to log in. Every router has a default password, like admin. As this article points out, most people don't bother to change that password. Doing that is simple, though.



Log into your router. Then, click **Administration > Management**.

Enter a password in the **Router Password** and **Re-enter to confirm fields**. You should rotate this password regularly. I generally do it every two weeks to a month. If you need to create a strong and secure password, then

check out the Strong Password Generator Web site.

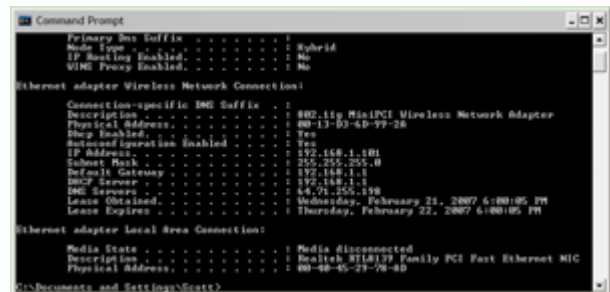
Locking Down MAC Addresses



All ethernet adapters, which enable users to access a network, each have a unique 12-digit identifier called a MAC address. MAC is short for Media Access Control, and it's a way for the network to ensure that a computer is allowed to access a network. Most routers allow you to specify which MAC addresses are allowed to connect to your network.

How do you find a MAC address? If you're using a computer with a wireless card, you can find the MAC address by flipping the card over and looking for a block of characters like this: 00:A0:C9:14:C8:29.

If, on the other hand, your computer has a built-in wireless card, and the MAC address isn't on the sticker on the bottom, you can use the tools on the system to find the MAC address. In Windows, click **Start > Run**. In the Run



```
Command Prompt
Primary DNS Suffix . . . . . : 
Mode Type . . . . . : Hybrid
IP Filtering Enabled . . . . . : No
VLMF Proxy Enabled . . . . . : No

Ethernet adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : 802.11g MiniPCI Wireless Network Adapter
Physical Address. . . . . : 00-13-02-6D-77-28
Pkg. Enabled. . . . . : Yes
Autonomous Operation Enabled . . . : Yes
IP Address. . . . . : 192.168.1.181
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCP Leases . . . . . : 14, 01, 255, 538
Lease Expires . . . . . : Thursday, February 21, 2007 6:00:05 PM
Lease Expires . . . . . : Thursday, February 22, 2007 6:00:05 PM

Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
Description . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
Physical Address. . . . . : 00-0B-0E-29-78-00
```

dialog box, type cmd and then click OK. This opens a command prompt. At the command prompt, type ipconfig /all. Look for the section Ethernet Adapter Wireless Network Connection. Your MAC address is the third entry, beside the heading Physical Address.



On a Mac running OS X, do this: select **About this Mac** from the **Apple menu**. On the dialog box that appears, click More Info. Then, select **Network** from the menu on the side of the dialog box. Look for the Wireless Address setting.

Now that you have the MAC address, you can enter it into your router. Select **Wireless > MAC Address > Wireless Mac Filter**. Then, click **Enable**. Click the **Permit only PCs listed to access the wireless network option**, and then click the **Edit MAC Filter List** button.

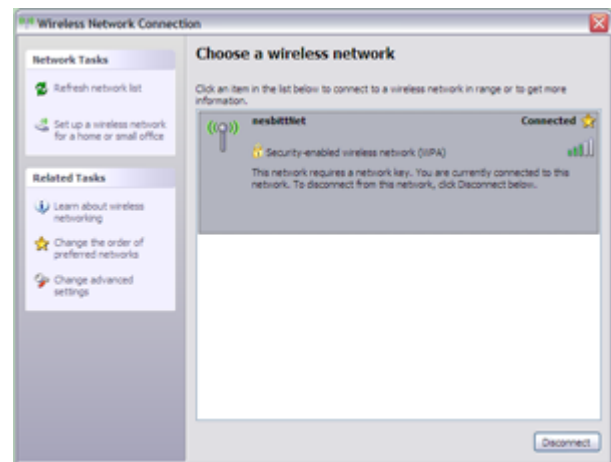
Type the MAC addresses, one to a field, in this dialog box. Then, click **Save Settings**.

The beauty of using this method is that you can give friends or guests access to your network and then easily remove their access privileges later on.



Encryption

If you want to keep your data safe, encryption is a must. Encryption not only enables authorized users to securely access your network, but it also ensures that their data is kept safe from prying eyes. Most routers give you a choice of two encryption schemes: Wireless Protected Access (WPA) and Wired Equivalent Privacy (WEP). Of the two, WPA is the more secure option.



WPA uses a password to encrypt data and to restrict access to your network. When someone tries to access your network for the first time, they'll have to enter the password.

Add or change the password by selecting **Wireless > Wireless Security**. Select **Pre-Shared Key** from the **Security Mode** dropdown list. Then, enter your passphrase in the **WPA Shared Key** field and click **Save Settings**.



As with the router password, it's a good idea to rotate your password frequently. Once again, the Strong Password Generator Web site comes in handy.

Enabling the Firewall

A firewall on your computer can help keep unwanted visitors out. The same applies to the firewall on a wireless router. And a router firewall is easy to set up. To do so, click **Security > Firewall**. Then, click the **Firewall Protection: Enable** option. Also, click the **Block Anonymous Internet Requests** option. This will ensure that any unsolicited attempts to access your router will be denied.

Keep in mind, though, that some cable Internet providers (like mine) don't play nicely with router firewalls. You might find that your connection gets intermittently dropped or you lose it all together.



Other Things You Can Do

All routers are identified by a Service Set Identifier (SSID). This is just the name of your network. Every router comes with a default SSID (mine was 'linksys'). People use the SSID to identify your network. And malicious users can use the SSID to break into your wireless network. So, you should change your router's SSID. Do this by selecting **Wireless > Basic Wireless Settings**. Enter a unique name in the **Wireless Network Name (SSID)** field.

To make it easy for others to jump aboard your wireless network, routers by default broadcast their SSIDs to the world. Once again, malicious users can take advantage of this information to jump on or take control of your wireless network. You can do this by clicking the **Wireless SSID Broadcast: Disable** option on the **Basic Wireless Settings** screen.

As I mentioned earlier, you log into your router using a Web browser. You can do this either from the computer directly connected to the router, or from anywhere on the Web. Being able to remotely administer your router can be useful, but it also opens the door to someone else logging on and



gaining control of your router. You can disable remote administration by selecting **Administration > Management** and then selecting the **Remote Administration: Disable** option.

If, on the other hand, you really want to enable secure remote administration of your router click **Administration > Management**. Then, select the **Remote Administration: Enable** and Use **https options**. Selecting the Use https option creates a secure connection to your router from a browser.

Conclusion

Adding a bit of security to your wireless network is easy and doesn't take a lot of time. That said, one of the people who I talked to while researching this TechTip commented that no matter how well you secure your wireless network, there will always be someone who can break in. But, that's true for any other kinds of security, too. If someone is determined enough, a deadbolt on your door won't stop them from entering your home. However, the fact that you've put some security in place will put off most people trying to illegally use or hijack your wireless network, and that alone is worth the effort.

Source: <http://www.geeks.com/techtips/2007/techtips-04mar07.htm>