Upgrade your router, Part 1
By Michael Shalkey, Co-leader, Q&A Sessions, Channel Islands PCUG, CA
www.cipcug.org
jweighle (at) vcnet.com

What is a router?
When you purchase Internet access from a provider (the phone company or cable company) they normally provide a modem (a combined device for **mo**dulation and **dem**odulation of the analog signal of a telephone line or coax cable and your computer) but that was only providing internet to one device in your house.

A router is basically a very small computer that takes that one internet signal and shares it with up to 256 devices.

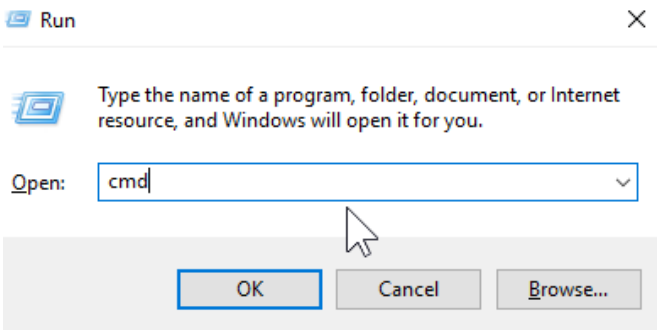
These days, your provider may even provide a combination device that does both, a modem/router that translates the signal (modulate and demodulate) as well as acts as a router – even sometimes a wireless router.

Here is the problem: Internet providers are notoriously cheap and will provide you the cheapest hardware to do the job. This means from the time it left the factory it will remain unchanged for years. Can you imagine what your computer would look like if it never was updated from the day it was first turned on yet accessed the internet every day? It would have been taken over by bad guys and even used to attack other people within the first week – perhaps the first hours.

Why don't internet providers update their own equipment? Money. It would take time and money to change things for their customers – and even if they found an easy and quick way to do it, the cost of handling the support phone calls if things were even slightly different afterwards would stop companies from changing anything.
Why YOU should update your equipment's software?

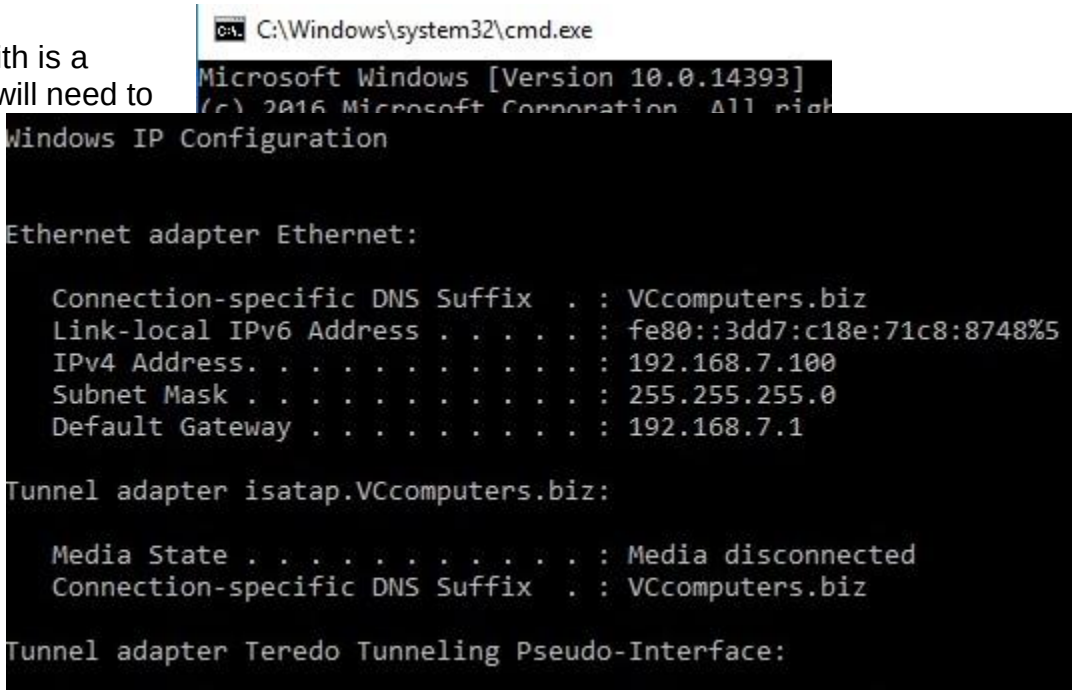
It has been recently reported that many hardware manufacturers have put in "back doors" to their equipment that don't require a username and password to connect and change settings on their hardware. Criminals have also found these back doors and can use them to see all the computers on your network and every internet search – including your usernames and passwords to banks, emails, and other sensitive sites. Also hackers know very well the default usernames and passwords for commercial routers so that even without a back door, they can access many routers.

First step
If you do nothing else, first change the default username and password of your router. To access your router, first you must know it's address. From a command prompt (Windows key + R to open a Run window, type cmd and click OK)



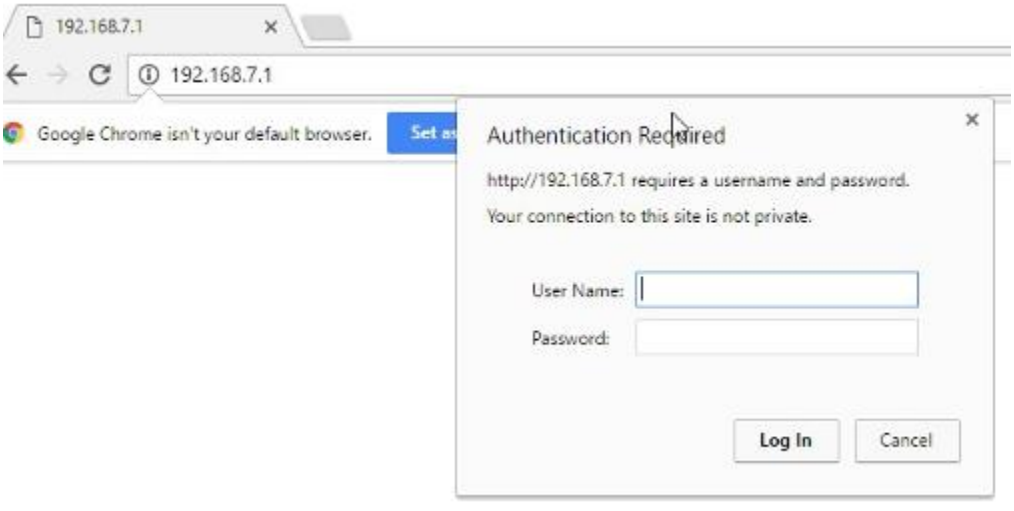
type ipconfig
and then the Enter key

What you will end up with is a bunch of numbers you will need to continue to the next step.



The Default Gateway is the "address" of your router.

The next step is to open the browser of your choice and in the address bar type the Default Gateway address. No www, but just the numbers as they appear. You should now be asked for your User Name and Password to view and change settings in this router. This is one of the main reasons to do all this work: the default usernames and passwords are known to all technicians and hackers around the world. If you want to know the username and password for yours, just Google the answer by putting in your model number ("Linksys WRT54G v3 default username password") and you will find most are user name of admin and password of admin.



The first thing you should do for safety is change that.

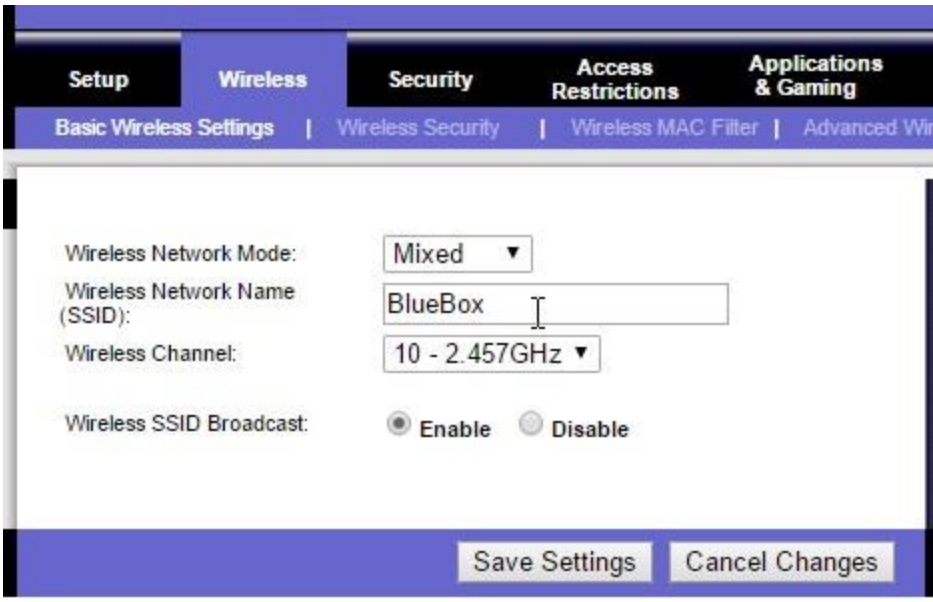
You can use any username and password you want but I recommend put a sticker or post-it note on the router itself with the username and password.

On this router that is done on the Administration tab and the Management screen. It doesn't allow you to change the username, but you CAN change the password. Again, be sure to write it down.

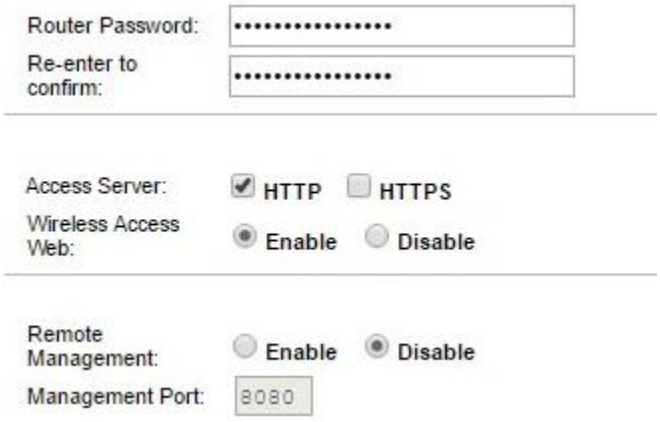
The next thing most people want to do is change the wireless network name (SSID Service Set Identifier) and password.

On this router that is found on the Wireless tab. In this example I have already changed my SSID to the name BlueBox.

On the Wireless Security tab you can change the password for the wireless by clicking on the Wireless Security tab. You can choose any password you like, but again, write it down.



One last thing you should always change is remote administration. On this router it is on the same screen as the one for changing to password.



If you really understand what these words mean, you'll understand why you want it disabled. Remote management means you don't have to be on your local network – in your house – in order to manage this router and change settings. I can't imagine a scenario where I would want to change settings in my router when I am not at home. I certainly can't imagine a scenario where I would want someone else to change settings in my router. I would HIGHLY recommend that this be set to Disable.

Next month we will go over changing the firmware on your router to have new features and security.