

**Speed, Wireless, & Security Presented by Judie Coleman  
Oakmont PC Users Club -- March 17, 2008**

Everyone always wants their computing experience to be "fast".  
There are 3 areas that impact on how "fast" your computer experience is.

- 1) Speed of your computer (not covered here).
- 2) Speed of your internal network (see below)  
(computer to computer, computer to internet gateway – router or modem)
- 3) speed of your internet access (modem to internet) (see below)

**Measuring:**

use **bits** for bandwidth or speed /// use **Bytes** for size of files and disks and RAM.

**Bit** = small **b** (K**b** - kilobit) = 1 or 0  
(you generally use **bits** when you talk about bandwidth)  
Bits in binary are either 0 or 1. Thus **bit** = **binary digit**.

**Byte** = capital **B** (K**B** - kiloByte) (there are 8 **bits** in a **Byte**)  
(you generally use **Bytes** when you look at the size of a file or disk or RAM).

**K** = 1,000 (**thousand**) example: Kbps = **Kilobits** per second  
(1 **thousand** bits per second)

**M** = 1,000,000 (**million**) example: Mbps = **Megabits** per second  
(1 **million** bits per second)

**G** = 1,000,000,000 (**billion**) example: Gbps = **Gigabits** per second  
(1 **billion** bits per second)

**(Very Approximate) External Speeds (Inside to Outside)  
From Modem to Internet**

i.e., how fast a web page downloads

<b>Speed</b>	<b>Approx Time to Transfer 1 MegaByte</b>	<b>Approx Time to Transfer 50 MegaBytes</b>	<b>Sample Pricing</b>
28.8 Kbps (old modems)	4.5 minutes	3.8 hours	
56.6 Kbps (modem)	2.3 minutes	2 hours	
384 Kbps (slow DSL)	17 seconds	14.5 minutes	Sonic DSL: \$18.95/month
1 Mbps	8 seconds	6.5 minutes	
1.5 Mbps (T1) (Med DSL)	5 seconds	4 minutes	Sonic DSL: \$29.95/month
3 Mbps (Med Fast DSL)			Sonic DSL: \$34.95/month
10 Mbps (fast cable modem) (Fast DSL)	1 second	40 seconds	
<b>Wired Internal Speeds</b>			
100 Mbps (internal wired)	>1 second	4 seconds	
1000 Mbps=1 Gbps (internal wired)	zip-ity-	-do!	

**Cable modem speeds get slower the more it is shared.** It is the same bandwidth line going to your and your neighbors' houses, so the more that bandwidth is shared, the slower it gets. If you are first on your block to get cable, your speeds will be very fast. As more people on your block get cable, your speeds may get slower.

**DSL speeds get slower the farther you are from the "Center".** Before you purchase DSL, they can tell you how far you are from the "Center" and what speeds you are likely to get. DSL bandwidth is not shared. The speed you get will stay constant no matter how many people on your block get DSL.

**Internal Speeds (Inside)  
Computer to Computer & Computer to Router/Modem**

**Wired Speeds**  
Wired Speeds are (mostly) Constant

<b>Wired</b>	100 Mbps	Most network are 100 Mbps
	1000 Mbps (Gbps)	Newest – the transition to Gigabit networks is going on now

**Wireless Speeds**  
Actual Wireless Speeds depend on the amount of interference, etc. (see below)

<b>Wireless</b>	<b>802.11a</b>	Up to 54 Mbps	5.5 Ghz frequency Range: 30-40 feet
	<b>802.11b</b>	Up to 11 Mbps	2.4 Ghz frequency Range: 100-150 Feet
	<b>802.11g</b>	Up to 54 Mbps	2.4 Ghz frequency Range: 100-150 feet
	<b>802.11n</b>	Up to 480 Mbps	(Newest) MIMO Range depends .....

**Wireless Speeds and Range vary depending on**

**Interference:** walls, microwaves, cell phones, water, etc.

**Noise:** on your channel

**Encryption:** can take 5% to 50% drag on your speed.

**It is said that if you get half the speed advertised from your wireless, you are doing good.**

If the speed you are getting seems fast enough for you, then don't worry about it.

## Wireless Encryption:

You need to understand that whatever wireless encryption is out there, there are many people dedicating every waking hour to cracking it. And they love to share what they learn with the world. See for yourself:

For "How To" Crack Wireless Encryption:  
Google using search terms "crack wep" or "crack wpa".

For videos on how to crack wireless encryption:  
Go to [www.youtube.com](http://www.youtube.com): use same search terms as above.

Note: most programs for cracking wireless encryption are run on Linux, not pc's.

<p><b>WEP</b> 64 bit (key) or 128 bit (key)</p>	<p>WEP = "Wired Equivalent Privacy" Composed of: 2 parts 1<sup>st</sup> part (24 bit) sent in plain text 2<sup>nd</sup> part (40 or 64 bit) easily crackable</p>	<p>Can be easily cracked in 2 to 15 minutes</p>
<p><b>WPA-TKIP (PSK)</b></p>	<p>WPA= "Wi-Fi Protected Access" TKIP = "Temporary Key Integrity Protocol" PSK= "Pre-Shared Key" TKIP Key: generates sequence of WEP keys based on master (shared) key (PSK) &amp; generates a new key every 10,000 packets.</p>	<p>Use a shared key 20 characters long, that is not in the dictionary. (Not all wireless devices let you create such a long key.) WPA Algorithms: If your devices support it, choose AES over TKIP. Uses software so more drag.</p>
<p><b>WPA2 (WPA-AES)</b></p>	<p>EAP= "Extensible Authentication Protocol" AES = "Advanced Encryption Standard" uses Rijndael algorithm –strong &amp; fast. Uses "substitution-permutation network" Supports: CCMP = "Counter Mode w/Cipher Block Chaining Message Authentication code Protocol" – as alternative to TKIP.</p>	<p>Rijndael algorithm is currently the most secure and fastest. WPA Algorithms: If your devices support it, choose AES over TKIP. WPA Shared Key: use at least 20 characters, nothing in dictionary, (use capitals, lower case, numbers, letters)  Uses hardware so less drag.  Download Microsoft Update for WPA2 (KB893357)</p>

## Basic Guidelines for Wireless Security (Using Linksys Wireless Router (WRT54G))

### Setup:

**Router Name:** Change the default Router Name.

**Local IP Address:** Make the Local IP Address unusual (write it down!)

**DHCP Server:** Limit the DHCP Server assigned IP addresses to the number of DHCP users.

### Administration

**Password:** Change the default password (at least 8 characters, use complexity rules)  
(write it down!)

**Access Server:** Change Router access from HTTP to HTTPS.  
(write this down with the IP Address)

### Basic Wireless Settings

**Wireless Mode:** Restrict to what your devices are (mixed, B-Only, G-Only)

**SSID:** Change default SSID to something that does not identify you or where you live.  
(Can & Will be seen on the outside, does not have to conform to complexity rules.)

**Channel:** Change to 1 or 11 (most people are on 6 so there's more "noise")

**SSID Broadcast:** Disable **AFTER** you have set up the client connections.

### Wireless Security:

**Security Mode:** In order of weakest to strongest: WEP, WPA, WPA2

**WPA Algorithms:** Chose AES over TKIP (if your devices support it)

**WPA Shared Key:** Always use at least 20 characters for the shared key using complexity rules:

Good source of randomly generated characters: <https://www.grc.com/passwords.htm>

**Group Key Renewal:** the more often keys are renewed,  
the safer you are, but the slower your network will go.

### Wireless MAC Filter:

In theory it is tighter security to limit access to the mac addresses of your devices.

However, mac addresses are not encrypted so can be easily spoofed.

And you have to remember to update this list every time you change a device on your network.

Weigh the hassle factor against slightly tighter security factor.