IN THIS ISSUE:
~ Wireless Networks

COMING NEXT MONTH:
~ PGP Encryption

READY NET GO … NEWS

September 2008 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

Extend your wireless range

1) Upgrade your wireless router and network adapters to 802.11n. This standard is still in draft mode but should be ratified soon (2009) and offers much greater range and security features.

2) Make sure the laptop has the best possible line of sight with the access point or wireless router. If you can put the access point high on a shelf or attach it near the ceiling in a large room (preferably in the middle of the room), the greater the signal strength will be for the most users.

3) Upgrade your notebook's wireless omni-directional antenna with a high-gain, range-boosting, directional external antenna. Directional antenna's focus the signal in a specific area as opposed to a 360-degree pattern.

4) Install wireless repeaters or access points. Configure them to communicate on the same network and you instantly have extended your wireless range.

5) Update your router's firmware and network adapter's drivers.

6) Look for common devices that also use the same 2.4 GHz frequency such as cordless phones and microwaves. Switch out these devices for 5.8 GHz or 900 MHz frequencies and you'll free up your interference issues.

7) You will get better performance in some cases if you purchase the wireless router and network adapter from the same company. For example: Linksys Wireless-G Broadband Router with SpeedBooster and Linksys Wireless-G Notebook Adapter with SpeedBooster

Setting up a Wireless Network

Wireless networking or Wi-Fi (Wireless Fidelity) uses radio waves to transmit data much like cell phones and radios. Setting up a wireless network can add convenience to your computing life by allowing you to move freely without the constraints of cables.

While wireless networks have advantages, **they are not as secure or fast as wired networks**. Wireless networks are also more prone to errors and lost connections. So if performance is your goal, stick with a wired network despite the perceived inconvenience. Here are some potential scenarios where setting up a wireless network can be beneficial:

1) You cannot physically run cables due to budget or access constraints (can't open the walls).
   a. Your home has plaster walls and no Ethernet jacks or you are renting temporarily and don't have the ability to install a wired network. Keep in mind that you can always run cable in wiremold or in a raceway on the wall's surface if you can't physically open the walls or gain access from above or below.

2) You need to be able to move around your office or home safely and frequently or you don't have quick access to installed network jacks.

   For instance:
   a. Medical office needs to move freely with a laptop between patient rooms and the front desk.
   b. Warehouse needs wireless handheld PCs/laptops to track inventory oftentimes on ladders or in tight spaces.
   c. You travel frequently and you need access to the Internet and email in public places such as airports, hotels, cafés, etc.
   d. Large, open rooms where cables will become a trip hazard; busy, public spaces where many people will congregate such as theaters, churches, halls, etc.

WWW (Websites Worth Watching)

1. www.repairpal.com - Need some advice on car repairs? Want to know how much it should cost to fix in your area? New site presents info in an easy to understand manner.
2. www.howtocleanstuff.net – Need ideas on how to clean things around your home and yard? Check out this site for user submitted tips and techniques.

Wireless Standards

Three standards that are widely accepted are: **802.11b**, **802.11g**, and **802.11n (draft)**. There are many others but for the purposes of this newsletter we will discuss only these three.

Standard	Data rate (max)	Frequency band	Range (indoor)
802.11b	11 Mb/s	2.4 GHz	35 meters (~115 ft)
802.11g **	54 Mb/s	2.4 GHz	38 meters (~125 ft)
802.11n (draft)	300 Mb/s	2.4 or 5 GHz	70 meters (~230 ft)

Note that cordless phones, microwaves and wireless radios also operate in the 2.4 GHz range so interference may occur and impede signals.

** Also note that some manufacturers' proprietary features currently allow greater speed/range options for Wireless-G (802.11g) products. Examples: SuperG, MiMo, Xtreme G, SpeedBooster

Wireless-G Network Adapter by Linksys
This adapter plugs into the PCMCIA port on your laptop and allows signals to be received from your wireless router so you can access network and Internet data without cables. External USB network adapters are also available.

Important Considerations

Two of the most important considerations when using a wireless network are **signal strength** and **security**.

In order to get the best signal, you'll have to take into consideration that walls, ceilings, floors and objects such as furniture and equipment all impede radio signals. If you have several obstructions, you may have to use more than one access point in order to boost signal strength. Each access point should have no more than 25 clients.

You want to be able to move freely around your office or home but you also may not want the business next to you or your neighbors to gain access to your network. When it comes to security, remember that radio signals are only limited by obstructions. Even though you have a concrete, steel, or wood wall between you and the outside world, the radio signal may still get through and be accessible to others. This is why every wireless network requires a security measure. Keep in mind as well that if you are in a public space, you should always err on the side of caution and that the connection you establish may not be secure. In these situations, think twice before logging into your bank account or transmitting personal information over the wireless connection unless you have multiple security protocols in place such as https, WPA, and VPN.

Differences between WEP and WPA Security Protocols

WEP – *Wired Equivalent Privacy* – Initial security measure created for wireless protection. Numerous attacks prompted the need for increased security controls which led to WPA. If you are currently using WEP encryption, discontinue using it and switch to either option below. If your wireless hardware only supports WEP encryption, you will need to purchase new hardware.

WPA – *Wi-Fi Protected Access* – Much greater security controls (increased authentication and encryption measures as well as a secure message verification system) makes intrusions into the LAN more difficult than with WEP-enabled devices. All wireless configurations should at least have WPA enabled. WPA is acceptable for non-corporate, non-government use.

WPA2 – *Wi-Fi Protected Access (Revised)* – Referred to as 802.11i – Best security standard currently offering the most protection options. Like WPA, WPA2 uses a pre-shared key (password) to encrypt data during transmission. If you have WPA and want to upgrade to WPA2, there might be a firmware upgrade available. Check your router manufacturers' website.

The biggest difference between WPA and WPA2 is the security mechanism. WPA uses Temporal Key Integrity Protocol (TKIP) where a 128-bit key is changed over time during use and WPA2 uses Advanced Encryption Standard (AES) with Cipher-Block Counter Mode Protocol (CCMP). Either system can be used by consumers or in a general business environment and should be a part of every wireless connection.