IN THIS ISSUE:
~ Wireless Networking

COMING NEXT MONTH:
~ Power Protection

READY NET GO … NEWS

April 2005 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

Reasons for Going Wireless

There are **two reasons** why setting up a wireless network is advantageous:

1) You physically cannot run cable in the walls due to physical or monetary constraints.
2) You need mobile access. For instance:
    a. Doctor's office with tablet PC needs to move around from room to room without risk of patients tripping on wires.
    b. Large warehouse with tablet/handheld PCs need access up and down long aisles.
    c. Public access places such as airports, hotels, café's etc.

If your situation does not fit into either of these categories, a wired network is still the best option. Keep in mind that wireless networks are **slower, less secure** and **more prone to failures** than wired networks.

Generally, there is no cost savings with going wireless. What is saved in running cables is spent in new hardware, installation/testing, increased maintenance costs and costs associated with lost productivity.

Before jumping into a wireless network, do a full cost/benefit analysis to see if switching over is the best plan.

So you want to go Wireless…!

If you've been toying with the idea of breaking free from all those wires, we can help you decide if wireless networking is right for you.

Background

Wireless networking has been available for many years and individuals as well as businesses have been taking advantage of the conveniences. Although the idea of searching the web or accessing files on another computer without plugging into another device or wall jack is appealing, wireless networking is not the best option for all people or for all situations.

How Wireless Works

There are two types of wireless networks:

1) Peer-to-Peer – computers communicate through wireless networking interface cards rather than through cables and hubs/switches/routers.
2) Access Point – computers communicate through either a dedicated hardware access point (similar to a hub) or through a computer with a built-in software access point.

Typical indoor ranges are 150-300 feet but can be shorter based on the building materials and location of the computer(s). Outdoor ranges will be greater but still dependent on environmental conditions/obstacles.

WWW (Websites Worth Watching)

1. www.howtocleananything.com – Got a mess that you just can't get out? Search here for handy solutions.

2. www.homemadesimple.com – Tips on organizing, cleaning, planning parties and more.

3. www.healthyhousekeeper.com – More ideas on cleaning your home top to bottom.

Wireless Standards

There are currently four wireless standards based on the 802.11 radio frequency band. Unfortunately, devices operating under one standard may not be compatible with other standards so if you have an older wireless network and you wish to add to it, you will have to find products that are compatible with your older equipment or buy all new equipment.

The four standards are:

1) **802.11b** – supports bandwidth up to 11mbps which is close to traditional Ethernet speeds. It operates in the 2.4Ghz range so can encounter interference with microwave ovens, cordless phones and other devices using the same range.
2) **802.11a** – supports bandwidth up to 54 Mbps. Geared to business customers due to higher pricing. It operates in the 5 GHz range which limits its range but has less interference than 802.11b. The "a" standard is not widely used and is not compatible with "b" or "g" standards.
3) **802.11g** – supports bandwidth up to 54 Mbps and operates in the 2.4 GHz range giving the best range and speed. Higher costs than 802.11b products but because they operate in the same frequency, 802.11g network adapters will work with 802.11b network adapters. Most widely used standard – best option for new networks.
4) **802.11i** (aka WPA2) – latest standard developed to address security issues that the other standards cannot control.

Two of the most important considerations when using a wireless network are signal strength and security. 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. In order to get the best signal, you'll have to take into consideration walls, ceilings, floors and objects such as furniture and equipment. Each access point should have no more than 25 clients. To boost signal strength, you may have to use more than one access point.

For security, remember that radio signals are only limited by obstructions. Even though you have a concrete 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 has to have security measures in place.

Differences between WEP and WPA Security

WEP – *Wired Equivalent Privacy* – Initial security measure created for wireless protection. Numerous attacks prompted the need for increased security controls which led to WPA.

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 have WPA enabled.

MAC Address Filtering – *Media Access Control* – Every hardware device has a unique MAC address. By setting the wireless access point to only allow access via listed MAC addresses, you are preventing unknown users from gaining access to your network.

Whichever wireless network standard you choose, make sure that you implement reliable tools for monitoring the network. Some software programs will give you instant access to unauthorized activity and provide a lockdown capability which adds further security controls.