Holzsager Technology Services, LLC
P.O. Box 535, Fair Lawn, NJ 07410-0535
(201) 797-5050 info@tech4now.com
Visit us on the Web at http://www.tech4now.com

Wireless Connectivity vs. Cabled Networks

By Fred W. Holzsager

Many of my neighbors in Fair Lawn are now able to confront a very promising dilemma—whether to install DSL or Cable broadband connectivity in their homes and/or offices. For some parts of our town, DSL may not yet be available, only broadband via cable modem (or "T1"). Along with the wonderful opportunity to enjoy high speed Internet access comes another "big" decision: "If I plan to share the high speed access with more than one computer in my home or office, shall we implement a hard-wired solution or a wireless one?"

Fair Lawn enjoys the new wave of technology through many avenues: the school system uses broadband—so the students enjoy a quick response while doing research; The Borough Offices are currently contemplating broadband access; many local businesses are already well dependent upon high speed Internet access (many of them also have the T1/T3 access pulls to their office for a more dedicated access method). For a home or business to benefit from broadband, a network is typically employed to share the "pricey" resource. Some users have spent large sums on sophisticated and powerful networking equipment not only to share the access amongst their employees, but control and restrict their access, as well. With the *commoditization* of DSL/Cable Routers, most homes or businesses with low end needs can also benefit from the advances made by technology to allow them to share this wonderful resource. Whether the individual purchases a device marketed by Linksys, D-Link, Belkin, Cisco (Linksys is now a Cisco product), SonicWall, WatchGuard, or Gigatech, for a modest sum, one can afford to share the connection. Now, the question is whether the connection should be established using a hard-wired solution or wireless.

There are some fundamentals to consider before committing to either:

1. ***Does the connection need to pass through concrete or lathe walls?***
2. ***Are the walls and location relatively old and "unfriendly" to having wires pulled within them?***
3. ***Is the data being passed over the private network of a confidential nature?***
4. ***How far from the Access Point will the client be located?***
5. ***Does a significant percentage of your computing occur on mobile devices?***

For most, these five questions will adequately help you identify the appropriateness or candidacy of your location for a wireless (Wi-Fi) LAN (WLAN).

In answering the first question, the age of the building can often become a critical factor. In many "Pre-War" buildings, the interior walls are composed of lathe applied to a steel mesh. Although it may afford stability and smooth walls, the cement used in the lathe, similar to concrete blocks (e.g., "cinder blocks"), may present a formidable barrier for the signal to pass through. Similar to a car passing under a concrete bridge while receiving an AM radio signal, the antenna's reach may be severely impaired to the

point that the wireless signal becomes too weak to be effective. The same solid structure used in creating the walls considered in the first question, has a subsequent consideration in the second question. Although a network cable may be passed through a drilled opening, installing a flush, wall mounted jack behind a desk becomes difficult. In such cases, the cable provider may suggest the use of channeling to conceal the wiring. If the cable provider does do a wall mounted jack in such a wall, the customer may expect to pay a premium for this service. Whereas, in the case of a plasterboard wall, flush mounted jacks are common.

The third question relates to the security of the transmission passed via the wireless signal station to the receiver. Should a company or home use a wireless solution if they have confidential information being passed over the "ether"? The answer is a *qualified* "yes." (If the nature of communications is HIGHLY confidential, hire an expert.) Wireless technology is a relatively new implementation for homes and small businesses, as a result, not all users are implementing the full arsenal of tools and countermeasures provided to secure the transmission. Amongst the tools are:

- **WEP** (Wired Equivalency Privacy or Wireless Encryption Protocol): A protocol encryption scheme designed to keep your data transmission safe from prying eyes. WEP uses an involved algorithm to scramble data before it's sent and a complementary algorithm to decode the data as it is received. WEP may use a 64-bit or 128-bit code to encrypt the data. Very often, it is simplified for the commercial end-user by implementing a "Passphrase" to generate the encryption code.
- **VPN** (Virtual Private Network): A VPN is effectively the use of the router as a gateway. Once at the gateway, a user must provide the requisite identification and passwords to gain authorized access to the network. The VPN is not limited to a wireless scenario, but is a powerful networking security method used in a multitude of situations.
- **MAC Addressing**: The MAC (Media Access Control) address is the hard coded, burned-in, unique number assigned to each and every network interface card. The "MAC" is 12 hexadecimal numbers paired off with the first 3 pairs representing the manufacturer and the last 3 pairs identifying the card. By registering each MAC address in the Wireless Router or Access Point, the system can limit its response to "trusted" systems and deny access to all others.

Some other features incorporated into the "basic" wireless security include naming the Station Signal Identifier (SSID) or Base SSID (BSSID) rather than operating with the default of "ANY" (accepts any signal) and not broadcasting the BSSID will also help restrict the access to the access point.

The fourth item, Signal Distance/Strength is pretty straightforward: Wi-Fi (IEEE 802.11B) can optimally reach up to fifty (50) meters. If you picture the transmitter on a mountain and the receiver on a flat field at that distance, the signal should transfer at UP TO 11Megabits per second (Mbps) (comparable with 10BaseT technology of 10Mbps). Add some obstacle interference, bad weather, or 2.4GHz cordless phones and you should expect less. The newer technology, 802.11G (a.k.a., "54G"), uses the same frequency as Wi-Fi, but has a shorter range. The feature in it's favor is that most 802.11G access points also support Wi-Fi (802.11B), the older technology. To extend the viable distance of a wireless network, sometimes a "bridge" may be introduced, but that adds to the level of complexity, too!

Other newer technology is also getting into the mix—*Bluetooth* technology may also be available on your access point to allow PDAs (Personal Digital Assistants) such as Pocket PCs and Palm Pilots to access your WLAN for Internet access. The catch with *Bluetooth* is that it communicates at 1Mbps at up to 8-10 meters in "open air" (*read* "clear line of sight").

Everyone enjoys having the freedom to choose. Many companies and individuals are now buying laptops as "desktop equivalents." By doing this, users are adding options to their workplace: *Shall we have the meeting in the conference room or outside at a picnic table?* Knowing that an attractive option can enhance employee retention, some organizations are opting to install Wireless Access Points at convenient locations for their workers. When providing the added "reach" to the office, it is imperative to employ as many security features as possible in order to reduce hacking, "warchalking," and other forms of compromise to the network. ("Warchalking" is the practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access. That way, other computer users can pop open their laptops and connect to the Internet wirelessly. It was inspired by the practice of hobos during the Great Depression to use chalk marks to indicate which homes were friendly.)

A wireless LAN can easily enhance your work/Internet experience. It is now easily affordable and readily available at your local computer merchant. As with any network, you are making an investment in an "infrastructure," so do not take the task too lightly or you may be disappointed by the results. A quality network is only as good as its design and components. For results you can live with, you may wish to consider acquiring the services of an expert that can help you determine the network's feasibility, extensibility, and most effective manner of implementation.

Now that you have a foundation to Wi-Fi, you can look forward to sunny summer days sitting on your deck or patio with a laptop while surfing the Internet. That is, of course, unless you live in a Brunetti Cape Cod with a concrete foundation, have the wireless router in your basement, and use a multi-channel 2.4GHz cordless phone.

If you think this is for you or if you are interested in learning more about the items discussed above, feel free to contact Holzsager Technology Services, Inc. at (201) 797-5050 or by e-mail at info@tech4now.com. For general information about other services for your home or office, kindly visit www.tech4now.com, there you may retrieve additional information bulletins and articles to help you use technology to your fullest advantage.