The Future Is Now

Wireless Networks and Security

This new wave in technology has probably excited and interested you in just how you might implement it in your home and/or office. Imagine all your computers at your office or home interconnected together with no wires, giving you the freedom to relocate a computer with the flick of a switch. How convenient is that? This article will attempt to familiarize you with the wireless terminology used and perhaps give you an idea of what to look for.

The world of information technology is ever changing and constantly evolving with better and faster techniques. Wireless network technology is no different and it too has been pushing towards higher speeds. As you may know, these speeds, measured in Megabits per second or Mbps, are very important in any network environment. This speed is more commonly referred to as Bandwidth. Bandwidth is defined as the amount of information that can be carried along a cable in a given time period measured in seconds.

A few years ago The Institute of Electrical and Electronics Engineers (IEEE) set a standard for wireless technology and called it 802.11b, commonly referred to as “Wireless-B” networks. This standard can deliver speeds up to 11Mbps. Today, there is a new standard called 802.11g and it operates at speeds up to 54Mbps and it is more commonly referred to as “Wireless-G” networks. If you are someone who has already implemented wireless-B networks at your home or office and were wondering if this new technology is compatible with your existing network, the answer is yes. Both of these wireless standards share the same radio frequency band of 2.4GHz.

So just how beneficial will wireless networks be for your office or home? Have you ever considered computers sharing the same high-speed Internet connection via cable? How about using the new 802.11g standard to maximize speeds and continue to use the existing 802.11b hardware, a great cost saving feature since you will not be required to upgrade any of your existing 802.11b hardware? If you have just moved into a new home or perhaps a new office and the contractor has not wired for a computer network, you are in position to implement a wireless-G network. Before you do, you will want to consider the security of these high-speed radio frequency waves as well what might interfere with the performance of your wireless network.

First, in order to implement security, you will need a wireless router called WRT54G because this is more or less your central hub for wireless connections, also commonly referred to as a Wireless Access Point. This is the device that normally controls the central high-speed cable or DSL Internet connection. Linksys is the heavyweight manufacturer when it comes to wireless access point technology and has a product out called the WAP54G, that allows you to connect laptops and PCs to your network. Wireless access points are essential in your wireless network environment because they offer encryption of all wireless data transmissions.

Wired Equivalent Privacy (WEP) is the encryption scheme used for your data communications and utilizes a combination of 64-bit and 128-bit keys to provide access to control your network. Higher encryption levels mean higher levels of security but at the same time also mean a decrease in network performance because the network will have to encrypt and decrypt data transferred between the computers on the wireless network. Keep in mind that a 128-bit WEP encrypted wireless network will NOT communicate with a 64-bit WEP encrypted wireless network. The encryption levels must be the same throughout the entire wireless network. All wireless devices that support the 802.11b standard use 64-bit encryption levels.
P

hysicians generally over-estimate the level of patient compliance. Studies have shown that noncompliance can range from 20% to 80%, depending on the kind of treatment. On average, patients will follow their physicians’ treatment plans roughly 50% of the time. (Hippocrates Magazine, February/March 2001).

This doesn’t necessarily mean that 50% of patients are intentionally non-compliant or don’t follow some of the treatment put forward by their physicians.

1. Despite a population that has access to more medical information than ever before, or maybe because of it, patients don’t always understand why you have decided on a particular treatment plan for them, or they may disagree with it.

Before the patient leaves the exam room, ask them to let you know what they understand about their medication or treatment and clarify any areas of confusion.

2. Another reason that many patients give for not continuing with medication is that they don’t like the side effects, or don’t understand the side effects.

- Inform patients of possible side effects and how long they may last and what they can do to alleviate them, if anything. Ask them to call your office before stopping any medication so that you can discuss alternatives with them.

3. The more pills a patient takes, the less likely he or she is to take them all. This may be because some pills have to be taken once a day, others twice a day, some before meals, some after meals, and it becomes complicated.

- Ask patients if they have trouble keeping track of all their medication. If so, help them devise a plan to ensure they take all their medications. Especially for some of your elderly patients, you may want to customize a daily calendar for them, showing exactly when each pill must be taken.

4. It’s not only in taking medication that patients can be non-compliant, of course. If there are lifestyle changes, such as dietary changes for diabetics or hypertensives, some patients simply don’t follow their doctor’s advice. This is more likely to occur if their disease is asymptomatic.

- It’s doubly important that patients who feel well but need treatment understand the consequences of not following the treatment plans.

In addition to the ‘cut back on salt’ or ‘reduce calories’ spiel, ask your receptionist or nurse to photocopy low sodium or low-fat diets, or a list of suitable foods or recipe books that patients can take home with them.

The more information you provide your patients on the consequences of not following treatment plans, the greater the chances are of your patients being compliant.

This article first appeared in The Practice Manager in February 2003.

Wireless Networks (continued from page 1)

Another router security feature offers a Network Address Translator (NAT) to protect you from Internet intruders. The NAT is an “out of sight, out of mind” device also known as a hardware firewall that shields your internal network from being visible to the outside world. You might be wondering at this point how the data are transported between the wireless access point and the other client computers on the wireless network. There is a wireless technology called 802.11x that is an industrial strength authentication and authorization protocol used between the client and the wireless access point. Another great security feature is Media Access Control (MAC) address filtering. Each computer has its own MAC address and the WRT54G will permit only a small list of certain MAC addresses to access the wireless access point, to gain control of the internal network, and perhaps even to share the Internet connection.

Like all radio frequency devices, the signal strength is very important in determining how efficient your wireless network will be. The location of your wireless access point and the client computers will be important. Wireless B and wireless G devices operate at a radio frequency of 2.4GHz, and if you have devices such as cordless phones that operate within this range, the performance of your wireless network will most likely be affected. Be sure to check your existing devices around your office and home to make sure they are compatible with your wireless network environment.

Moving on to the components required to setup a wireless network, you will need a wireless access point router and a radio card. In order for your computer to detect the wireless access point and transfer data between the two, you will require a radio card installed on the client computer. They are very similar to Network Interface Cards (NIC) and there are two different flavours, one for Laptops called the PCMCIA radio card and one for PCs called a PCI (or ISA) WLAN card. The reception quality is excellent within 100 feet of the wireless access point and can be improved if an antenna is used.

In conclusion, when purchasing your wireless products, be sure they are a wireless fidelity (Wi-Fi) compliant product. Wi-Fi is essentially a seal of approval saying that the manufacturer’s product is compliant with the IEEE’s specifications. And please be aware that security is always evolving. As secure as it might be today, the landscape continually changes.

A&L's Softwords - June 2003
Practicing medicine is as much running a business as running a medical clinic. Nothing brings the message closer to home as when you find that your billing has been delayed or halted and you are unable to get information off to OHIP. Cash flow may not be what is expected when you write a cheque and find out you went into overdraft or worse, bounced a cheque. There are many reasons for this happening and we’ve seen it happen in the last few months. Reasons range from fires that destroy offices, hardware that breaks down, computers that get stolen, or the inability to access/enter information because of the SARS outbreak. The physician is ultimately responsible for all information that is entered, correctly or incorrectly, timely or untimely.

A few offices have come across incidences where a transmission was assumed to have occurred properly. Many offices have computer modems attached to the same phone line as their fax machines and that is the norm. No need to pay for extra lines when they’re not required. However, if the fax is in use, the modem will not be able to transmit. While you are transmitting, you will not be able to receive faxes. In either case, the total time involved is usually less than 5 minutes. In a few cases this year, some clients have found that they were not paid the amounts expected. After checking the user’s “Transmission Events Log,” it was found that the transmission had failed on the day of the cutoff. Or the OHIP EDT Batch Edit Report did not show that MOH received the batch. No subsequent transmissions were done until the following month, thus missing the opportunity to find out and confirm MOH had received the file properly for the pay period in question.

There are a number of reasons for not being able to transmit. From lines being busy or inaccessible to having a bad connection, phone cords falling out of the connection or forgetting to push the transmit button. With the HERO* program, checking the Transmission Event Log after each transmission will give you peace of mind. In the A&L Medical System, ensuring that the OHIP EDT Batch Edit Report shows your acknowledgment of previous submitted batches will ensure prompt payment. Good work habits will help avoid problems. It has been suggested to all A&L clients to batch and transmit a minimum of at least once a week. The worse case scenario is that you get paid three of four submissions.

Other examples we encountered included new staff failing to enter information into the computer. Another was due to SARS. At the very least, physicians and other staff should know the rudimentary functions of the A&L software programs and be able to enter new patients, bill, batch and transmit. Everything else can be learned later. However, a number of offices called in a panic to enter billings so that there would be payment the following month.

Be sure that more than one person has learned your billing software. Ask your staff to show you how it works or ask your physician if they would like to learn a part of the program. It can make your life a whole lot easier.

Just how much is your data worth? Well, the data that you backup are useless if they cannot be restored. What would be the point of backing up all the claims and patient information if none of it could ever be restored, let alone quickly and efficiently? Imagine the frustration of trying to restore a backup that you spent countless hours performing only to realize that it was done incorrectly or even worse, inaccurately. Backups should ease your mind so that in the event of a disaster or catastrophe, you can quickly restore from them. When was the last time you actually checked to see if your backups were updated and backed up correctly, and how did you ensure that the data were accurate? This article will attempt to convey how important backups are, how important is to keep them up to date and make sure that you can actually restore from them.

Some of the more common hardware backup solutions implemented by medical offices to backup the A&L System applications are given here. The data sources include ZIP drives, CD-RW (re-writeable), CD-R (writeable), floppy disks and tape backup devices. As you can see there are several different types of devices, and the choice made will depend on the backup methods and the amount of data to be backed up. Some computer systems may not have CD writers installed or perhaps do not have a ZIP drive or tape device, but rather a floppy disk drive. Some may include a secondary hard drive or even Universal Serial Bus (USB) memory sticks. USB Memory sticks are also a popular choice for backups because of their small size and portability. It is extremely convenient to transport data between two USB equipped computers. There is also the option of backing up your data onto DVDs and there are several types of DVD formats that must be considered and this will be covered in one of our future articles.

There are several aspects that need to be taken into account when considering backup options and some of these include both the size of the data to be backed up and the capacity of the backup storage device, use of compression utilities, efficiency of the backup process and the ability to overwrite existing backups. The cost of the backup storage devices and the ability to transport your backups easily will also influence your decision on what method you select. In the event of a fire or a flood, the ability to transport your backups is important because you might want to keep one copy in a secure fire- and flood-proof location in the office and a second copy at a remote location, such as your home or third party data storage facilitator, for further security. Another scenario: You may have a complete computer malfunction and require a third party to restore from the backups to a brand new machine.

From the size of the data to be backed up to the capacity of the backup storage device, one can be compromised when using floppy disks with spanning (copying a large file or system backup across two or more storage discs). If you wish to try and squeeze all the backup data onto a single storage disc and avoid spanning altogether, you might want to consider compression utilities that can squeeze the data into manageable sizes.

*(HERO is a registered trademark of HTN Inc.)
How Much Is Your Data Worth?  (Continued from page 3)

So what are some of the utilities that can be utilized to compress the data before they is transferred over to the backup media? There are several utilities that will allow you to compress the data including, WinZip, WinRar, PKZIP, and PKARC. These compression utilities can compress all your backup files and then copy to the backup storage device. This extra step in your backup process is most definitely worth considering if space comes at a premium. Keep in mind that if you compress your data, you must have an equivalent utility to de-compress the files during the restoration process.

<table>
<thead>
<tr>
<th>Type of Backup Storage</th>
<th>Size in Megabytes (MB)</th>
<th>Re-writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIP Drive</td>
<td>Up to 250</td>
<td>YES</td>
</tr>
<tr>
<td>CD-RW</td>
<td>Up to 700</td>
<td>YES</td>
</tr>
<tr>
<td>Floppy Disks</td>
<td>Up to 1.44</td>
<td>YES</td>
</tr>
<tr>
<td>CD-R</td>
<td>Up to 700</td>
<td>NO</td>
</tr>
<tr>
<td>USB Memory Sticks</td>
<td>Up to 512</td>
<td>YES</td>
</tr>
<tr>
<td>Tape</td>
<td>Varies with capacity</td>
<td>YES</td>
</tr>
<tr>
<td>Secondary Hard drive</td>
<td>Varies with capacity</td>
<td>YES</td>
</tr>
</tbody>
</table>

Another consideration is the efficiency of the backup process. Efficiency really depends on the amount of data you will require to backup and the capacity of the storage device you choose, along with the speed of your computer system. Floppy disks are by far the slowest and most cumbersome method of backing up data when compared to others, especially when the size of the data is very large. However it could also be an affordable implementation if you have a small amount of data to backup, since floppy disk drives come with most computer systems.

The ability to overwrite your backups is also a major factor when deciding what type of media to choose. If you’re using CDs to backup your data, keep in mind that CD-R’s can only be written once whereas CD-RW’s can be written many times and hence can be used to recycle your backups. Tape is still prevalent in many medical offices that have several gigabytes of data, but the downside to using tape is it’s much slower process.

A brute force method of backing up your entire computer system is a System Backup, sometimes known as Ghosting/Imaging. Ghosting your computer system usually involves an extra hard drive of the same size as your current hard drive, or a storage device perhaps on a network drive that is sufficient to hold all the information occupied by your current hard drive. This method of backup involves a software program to initiate the process. It will allow you to clone your computer system and take a snap shot of your computer so that in the event of a hard disk failure or disaster, you can restore the entire computer system back to when the hard drive was ghosted or imaged. The advantage of ghosting your entire computer system is that you do not have to reload the drivers and/or the programs required to make your computer system operational again. This method of backup is for users who would like to backup the entire system rather than a single application. There is a similar feature with Microsoft’s Windows ME and Windows XP operating systems where you are allowed to create a restore point which is essentially a snap shot of your computer system at the time the restore point was created.

Once the backup files are copied over to the backup media, it is always a good idea to check the date, time and size of the file(s). This will allow you to verify that the data have been copied over to your backup storage device. Make sure that the date and time of the files correlate to when the backup took place. Also, consider whether the size of the backup file is greater than 0 bytes. If the file is 0 bytes this should indicate an unsuccessful backup and should be investigated for errors. If you fail to verify the backup process, you could have data that are very old. If your system encounters errors daily and you are not aware of the failure, you could have, as in one case, data as old as two years, when the last backup ran successfully. The advantages of verifying your backups are to ensure that the data in your backups are current and that data were transferred to your backup storage device. Just because the data are recent and the backups occurred, doesn’t mean the data are accurate. How do you know if the data copied to the backup storage device are correct and accurate?

Well, the next step is to try and reconstruct your A&L System from the backups to another computer in order to check the integrity of the data and ensure accuracy. Successful restoration ensures repeatable results and in the event of a disaster you can now rely on your backups for peace of mind. The restoration plan, however, includes a reconstruction phase and a testing phase; it should always be conducted (at a revision update or more or less often, if you decide) and your employees familiarized with an easy-to-follow set of written emergency instructions.

The person in charge of the backup process should also be in charge of how to restore the data from the backups. Also, it will be wise to have an alternative person who is equally knowledgeable should the primary person be on vacation or is not available for some reason.

Because you want your data to be retrieved seamlessly and to minimize any system downtime, this method will be a worthwhile investment that will save you time, resources, some major cost and headaches, and your data.