



Help Desk
Sunday, June 27, 2004

Warnings About Wireless

By Al Gordon

It probably wouldn't surprise you to hear that there was traffic congestion in your neighborhood, or that you had nosey or freeloading neighbors. It might be a little surprising, though, to learn this was happening with your wireless computer network.

Wireless wonders are proliferating in the home and office like a herd of silicon-based bunnies. Cordless telephones. Wireless intercoms and baby monitors. Cordless headphones. Wireless keyboards and mice. Cordless weather centers. Wireless doorbells.

On top of which comes the spectacular growth of wireless computer networking. Like so much in the realm of technology, wireless started out as a rare and expensive product and quickly became cheap and widespread. So prevalent, in fact, that the market already is moving from its initial technology (called "802.11b") to a newer version ("802.11g") that is about five times faster. (There also are "802.11a" products aimed mainly at corporate users.) The "b" and "g" standards collectively are sometimes known as "WiFi," which is an industry trademark. Consumers need to be wary of that label since it applies both to the original technology and the new, faster one, so this is one case when you need to pay attention to the "802.11_" technical jargon.

All of these cordless and wireless devices are basically little 2-way radios. Problem #1 is that many of them are occupying the same set of

radio frequencies and interfering with each other. Problem #2 is that, as with all radio transmissions, anyone with the right electronic equipment can pick up the signal.

Eric Deming, a Belkin Corporation product manager responsible for their networking products says that wireless traffic congestion, "is a problem we see coming especially from cordless phones." Whatever device "has the stronger signal will drown out" other equipment, he said.

I found this out myself while testing networking products and experiencing connection problems. A check with wireless monitoring software disclosed to my astonishment that at various times of the day, I was picking up more than a dozen other networks in my condominium building. And some of them had signals almost as strong as my network's. Two years ago, I had the airwaves almost all to myself.

What do you do to deal with the traffic?

The first step, say the experts, is to find the best possible location for your primary wireless transmitter, called an "access point." Most consumers use a "wireless router," in which the access point is built into a network "router," a device that manages traffic on your network. The access point should be in a place that's central to where you will be working, but as far away as possible from sources of interference. In a home, that mainly means cordless phones and also microwave ovens. In the office, it could be pretty much anything. Admittedly, being central to work but away from equipment is a taxing geometrical exercise; obviously, you will need to find a compromise layout.

The next step is to actually read the instructions for your access point/router and learn how you change its settings. For virtually all consumer equipment this is done by using your internet

browser to connect to a control panel built into the access point. When you get there, you will see that device can be set to various channels, 1-11. By default, most are set to 6 or 11. So you want to put your access point on a channel no one else is using.

If all that fails, you can add more access points or high-sensitivity antennas to your network to boost signal strength. But try the placement and channel changing techniques first before you spend the money on additional equipment.

Once you have learned how to change your wireless settings to improve performance, you want to move on to deal with snoopers and freeloaders. Another thing that shocked me when I detected those dozen other nearby networks was that two-thirds of them were totally unsecured – no encryption (encoding of your transmissions), not even a change in the factory provided network name (called a “SSID,” it usually is initially set to the manufacturer’s name). You want to change the network name to something that will let you distinguish it from the others, and you want to turn on data encryption.

Without encryption, anyone can intercept your data. More important – because it happens more frequently – anyone can use your network to get internet access. Were I less scrupulous, I could be using one of those other networks in my building instead of paying a service provider. So unless you have some burning desire to provide free internet service for your neighborhood, secure your system.

Al Gordon is a Massachusetts-based media and political consultant who also writes about technology. You can read more of his articles at www.tnpcnewsletter.com/al and e-mail him at eagle@algordon.com.