Wireless Networking Basics

Angus B. Grieve-Smith
March 5, 2004

What is Wireless Networking?

The standard way that computers in a home or office connect to each other and the Internet is through Ethernet cables. Wireless Ethernet (also known as **Wi-Fi** or IEEE **802.11**) allows your computers to communicate using the Ethernet protocol over the same radio channels used by cordless phones and baby monitors. There are also devices that allow you to connect your computer to cell phone networks, but I will focus on wireless Ethernet for this article.

When would I need wireless networking?

Old-fashioned wires are still faster, more secure and more reliable than wireless networking. There are three sets of circumstances where wireless networking is an advantage: (1) you need to set up a network fast, and don't have time to run wires, (2) you want people to be able to move their laptops around the workspace, and (3) you want to make your network available to visitors with wireless-enabled laptops, or you want to bring your wireless-enabled laptop to another office, coffee shop or public space. Keep in mind that if your laptop's batteries run down, you'll have to plug it in to a power supply, so you won't be completely wireless.

How do I set up wireless networking?

There are two components to wireless networking. The **wireless adaptor** connects to the computer; it may be built-in or it may plug in to a laptop's PC Card slot, to a PCI slot on a desktop computer, or to a USB port. The **wireless access point** is a small device that connects to your local area network (LAN) or the Internet via Ethernet cables.

How much does wireless networking cost?

Wireless adaptors usually sell for between $50 and $100 apiece (that's per computer), and wireless access points for $60-90.

How secure is wireless networking?

Not very. The factory default settings on most access points leave the network wide open for anyone in radio range (up to five blocks) to connect. Most routers come with the Wireless Encryption Protocol (**WEP**), which provides some security, but many hackers can break through WEP. There is a small subculture of **warchalkers** and **wardrivers** who travel around looking for unsecured wireless networks. Most are just trying to avoid paying for broadband internet connections. Some use it to hide their identities for illegal activities: a man was arrested in Ontario in 2003 for driving very slowly in the wrong direction on a one-way street at 3AM, and police discovered that he was wearing no pants and using other people's networks to download child pornography onto his laptop. Other people use insecure wireless networks to get into an organization's computers and obtain sensitive information.

Angus Grieve-Smith is an independent computer consultant. More information can be found at <http://www.grieve-smith.com/> or by contacting Angus by phone at (718) 205-8665.