

Suite 3
Woodhouse Corporate Centre
935 Station Street
Box Hill North, Victoria
3129, Australia
ABN: 83 078 025 813
Tel: +61-3-9896-7800
Fax: +61-3-9896-7801
Email: sales@eb2bcom.com
Web: www.eb2bcom.com



Microsoft's 7 tips for going wireless

By Monte Enbysk

Source: Taken from the Microsoft website-

http://www.microsoft.com/smallbusiness/issues/technology/broadband_mobility/7_tips_for_going_wireless.mspx

The scene is a familiar one at health-care facilities, professional offices, college classrooms and even your neighborhood cafe. People are taking laptop PCs wherever they want to check e-mail or surf the Internet.

They're getting network and Internet access through wireless networks, where devices are connected through radio signals rather than wires. Couldn't you use one for your small or home-based business?

More and more people are asking this question, as wireless LANs — or local-area networks — continue to get better and easier to use. Despite the tech slump of recent years, sales of wireless networks continued strong. Annual revenue from wireless LAN equipment is predicted to jump to \$4.5 billion in 2006 from \$969 million in 2000, according to Allied Business Intelligence, an Oyster Bay, N.Y., research firm.

Sales have risen as prices have dropped. A wireless network typically consists of at least one centrally located access point and separate network access cards for each computing device. An access point for a home or small office can cost as little as \$300, down from more than \$1,000 in recent years, and access cards range from \$80 to \$300 each, also down from more than a \$1,000. While wired systems (with cable networks) generally remain cheaper, you can install many wireless networks yourself and save on labour costs.

If you're upgrading your network or setting one up for the first time, here are seven things to consider in buying a wireless LAN.

1. **Know the different wireless LAN standards — 802.11b, 802.11a and 802.11g — and the pros and cons of each.** Most Wi-Fi (short for "wireless fidelity") networks to date have been based on the 802.11b standard, created in 1999. Long the most popular standard, 802.11b works well for many businesses. But it is no longer the standard of choice, with the advancements made by 802.11g. Its biggest shortcoming is in having the slowest maximum speed — it supports bandwidth of only up to 11 megabits per second (mbps). On the flip side,

802.11b has a signal range of 300 feet or so, about five times that of 802.11a, and can be purchased at the lowest cost of the three standards.

The biggest selling point of 802.11a is the faster speed — it supports bandwidth of up to 54 mbps. It also generally supports more simultaneous users than 802.11b and its regulated frequencies prevent signal interference from appliances and other devices. But the higher speed and bandwidth are countered by the reduction in transmission range or distance. "As the frequency and amount of data held go up, the range goes down — by simple laws of physics," says Joshua Wise, a wireless research analyst. Also, because 802.11a utilizes a different frequency than 802.11b, the two technologies are incompatible, meaning you can't mix the two and count on them to interoperate.

Time to talk about 802.11g: It's newer, the most promising of the three, and has been supported by wireless networks since 2002. 802.11g combines the best of both 802.11b and 802.11a — it supports bandwidth of up to 54 mbps and uses the same 2.4 GHz frequency as 802.11b to offer greater range than 802.11a. It also is backwards compatible with 802.11b, which means that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

It's drawback? Because it received Wi-Fi certification as recently as July 2003, it has fewer products on the market and they cost more than 802.11b (in time, this will change). Also, early tests found uneven performance, and that it was not clearly superior to either 802.11a or the lower-cost 802.11b. But 802.11g products have continued to improve and have increasingly become the best choice. (Get ready for even more alphabet soup in the not-too-distant future: 802.11e, 802.11h, 802.11i, 802.11n, and even a new set of numbers such as 802.15.)

2. **Dismiss the marketing hype and address your needs.** If mobility isn't important to your business, you may be wasting your time worrying about a wireless network. But more and more businesses today have workers who don't camp out in offices all day.

A wireless network is a boon to a business in a short-term location. You can pick up a wireless network and take it with you from building space to building space. It is also scalable; you can expand your network with additional access cards and another access point, if necessary.

Still, wireless networks aren't for every business, and should be considered complementary to wired systems, which likely always will offer greater speed and bandwidth capacity.

3. **Buy from trusted vendors that are "small-business friendly."** You have big guys (Cisco Systems, Cingular Wireless, 3Com and others), smaller guys (D-Link and LinkSys, among others) and numerous startups in this space. Some cater mostly to the more lucrative large enterprise market, while others have jumped in more recently to fill a niche in the small-business and home-office markets. Still others seek the best of both worlds.

The important thing here, says Kneko Burney, chief market strategist for business infrastructure and services at In-Stat/MDR, is to deal with a vendor that specializes in serving small businesses and that speaks your language — not the language of an IT administrator. "You don't want to end up with instructions you don't understand, or things you don't know how to use," she says.

4. **Buy wireless systems that interoperate with wired networks.** The beauty of wireless is the flexibility it offers your business to expand or relocate. Many systems can easily be hooked up to a wired system, now or in the future. Don't compromise this flexibility by buying a system that is difficult or impossible to integrate with a wired system. Check with your vendor about the integration capabilities.

Also, buy a system that can easily integrate with new-generation networks, as well as with different-branded networks. As your business grows, you may choose to put your more mobile employees, such as salespeople, on a different network than those who spend most of their time in the office. Again, you want flexibility.

5. **If you have more than six employees, consider hiring a consultant for installation and support.** Small wireless networks are generally easy to install yourself. The more users you have, the more complicated it becomes. Also, the greater the need for ongoing support.

If you haven't already, it may be time to hire a technology consultant to oversee network implementation and, if possible, serve your business's entire technology needs. Once you find one you can trust, work out a service agreement to cover installation and support as well as remote access, future integration with DSL, and so on.

6. **Beware of potential interference problems.** Wireless networks are known to slow down or fizzle out in certain room or office locations. It may be a microwave oven causing the bandwidth congestion, it may be a filing cabinet, or even a particular wall or floor.

Work with your vendor and/or consultant to determine what kind of interference you might expect and where the best place in your office might be to locate your access point. If you still find that your new wireless network works only in a tiny corner of your business, you've probably got a cheap and inferior system. Time to switch to something better.

7. **Last but not least, beware of security issues.** If you haven't read about the security holes in many wireless networks, you haven't been reading. When I said wireless networks aren't perfect, here is another reason why.

However, most of the networks penetrated intentionally or accidentally have been at larger businesses, hospitals and other organizations. "This not nearly as serious an issue in small businesses as it is in the larger enterprises," says Jason Smolek, research analyst for International Data Corp.

Still, be mindful of the possibility. That laptop user visiting your office may be wearing a sneaky smile for good reason. He just might have hacked into something of yours.