What's New in Wireless? Getting Up to Speed by Howie Fenton, NAPL

Preview

Wireless networking (or "Wi-Fi") is the next wave of networking for business. While wireless networks offer significant advantages, they also have their own set of challenges in terms of speed, distance, and security. Here's how they're being addressed.

Introduction

Computer networks are an essential component of graphic communications companies, helping organizations share information and resources.

Beginning with the initial creation of Ethernet networks in the early 1970s, networks have depended on wires to connect them. The original Ethernet cabling was inflexible and about the width of a finger. It was followed by Coax cabling and then by today's much thinner and more flexible standard, Unshielded Twisted Pair.

But regardless of the thickness and flexibility of the wires, you still had to drill holes or push wires through ceilings to connect your company. Until wireless—which is poised to explode.

Wireless network can be an attractive options for organizations that:

- Are in a building that is difficult to wire.
- Have areas that are too far to wire (front office, pressroom, shipping, etc.).
- Must accommodate home users who are reluctant to drill holes through walls or floors.

Some design, prepress, and printing companies are already using Wi-Fi networks and a number of others are considering them. Wireless networks are growing in popularity as the technology becomes easier to install, the data-transfer rates increase, security issues are addressed, and their prices drop. As a result, sales of Wi-Fi networks are expected to surge over the next few years.

Originally, Wi-Fi was a term designating one of the wireless standards known as 802.11b, but people now use it interchangeably for all wireless protocols or connections. A wireless network is a network that allows a computer to connect with other computers, a server, or the Internet from as far as 300 feet away.

Typically, however, the range is less than 300 feet because of the interference of such things as walls, weather conditions, cordless phones, microwave ovens, and for some Macintosh laptop computers the installation of a WiFi card inside a Titanium case which acts like a shield.

Wi-Fi networking today is used most commonly today with laptop computers, allowing users to maintain communication with the network or the Internet while moving around their offices or from their homes. Some printing companies are offering Wi-Fi access in the front office for sales staff and CSRs. Another potential use for wireless is to provide network access for staff in traditionally "un-networked" areas, such as the pressroom, the bindery, and shipping and warehouse areas.

Setting Standards

The most commonly used Wi-Fi network protocol is the IEEE 802.11b (IEEE—the Institute of Electrical and Electronics Engineers—is responsible for setting international electrical / electronics standards.)

The 802 committee develops standards for local area networks (LANs) and wide area networks (WANs).

The 802.11 committee develops standards for wireless LANs; the 802.11b standard has a maximum data transfer rate of 11 megabits per second, considered slow in today's broadband networking world and considerably slower than a wired connection.

While the "b" standard is adequate for most front- and home-office applications and for Internet surfing, it is not fast enough to handle the large graphic files used in print production. (The lower frequency space will grow even more crowded with the arrival of computer and consumer peripherals supporting the Bluetooth wireless standard, which runs in the same 2.4-GHz neighborhood as 802.11b.)

The Need for Speed

Addressing the need for speed is 802.11a, a new wireless standard that offers speeds as high as 54 Mbps, a vast improvement over the "b" flavor and well into the territory covered by 100-Mbit Ethernet wiring.

The faster "a" flavor devices run in the 5-GHz frequency band, unlike the "b" flavor, which uses the 2.4-GHz spectrum. The higher frequency is less vulnerable to interference from cordless phones, microwave ovens, etc.

However, the "a" standard has its issues too. Its carrying range is limited to about 80 feet from a base station, about half that of 802.11b; and the products supporting it are relatively new and carry a premium price.

Worse still, 802.11a is completely incompatible with 802.11b—the two standards run at different frequencies. The 802.11a wireless network may give you better speed, but it won't talk to any of the popular (and inexpensive) wireless cards or adapters on the market.

The solution appears to be the 802.11g standard, which operates at the same frequency as "b" but can drive data almost five times faster . The "g" standard offers "the best of both worlds," through its support for the current installed base of 802.11b devices as well as its improved 54-Mbps performance.

The "g" standard also has its share of caveats. Wireless gurus claim the carrying range of 802.11g access points will be less than the 802.11b models, although no one is sure by how much. And the radio frequency interference issues won't go away

The Wi-Fi 802.11 Family

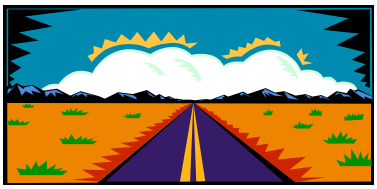
- **802.11** – Provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a** –An extension to 802.11 that provides up to 54 Mbps in the 5GHz band. It uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. Carrying range is limited to about 80 feet
- **802.11b** – An extension to 802.11 that provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. Theoretical carrying range of 300 feet
- **802.11g** – Provides 20+ Mbps in the 2.4 GHz band. Carry range is uncertain and may be 100-200 feet.

What's New in Wireless? Getting Up to Speed by Howie Fenton, NAPL

On September 24, 2003, the IEEE begun to develop a standard that will further raise the effective throughput of wireless local area networks (WLAN) to at least 100 Mbps (megabits per second), more than triple the current speed.

The standard will create parity between wired and wireless systems, so companies can extend their use of wireless networks to areas where the rate of existing wireless products has been insufficient. The higher-speed standard, IEEE P802.11n will help meet the expanding bandwidth needs of designers, prepress, and print production professionals.

Going the Distance



The new IEEE 802.16 standard promises to deliver more distance than the current standard, whose distance capabilities were not adequate for some users. The 802.16 standard is an up-and-coming contender as a wireless alternative to DSL, cable modem, leased lines, and other broadband network access technologies.

In another advantage, IEEE 802.16 could help reach those businesses and homes that have been just out of reach with other broadband solutions. Sometimes called the "last mile" problem, this issue has plagued the data and telecom carrier industries.

Intel has already pledged to develop a chip based on the 802.16 standard and claims equipment based on its chips will have a range of up to 30 miles and the ability to transfer data, voice, and video at speeds of up to 70 Mbps.

While 802.16 products will not be widely available for at least another year or so, the standard itself should play an important role in your future network plans. This standard has the potential to slash your long-haul network/internet access costs and allow you to deploy a broadband to your offices in a region, which could reduce the requirement for leasing circuits or fiber, enable data center consolidation, and generate additional cost savings.

One of the main issues of Wi-Fi networking is security. The data sent by wireless networks through walls and ceilings can be picked up with sensitive antennas—much more sensitive than the ones your equipment uses—miles away.

As a result, a new breed of hacker is emerging who practices the art of "wardriving"—driving around with notebook computers search for open access to wireless networks. (The term wardriving does not derive from the word "war" but from the hacker term "warez"—pronounced "wearz", which refers to pirated software.)

Some wardrivers even make maps of access points (an activity called "warchalking") and post them on the Internet.

Geeky Security Stuff

Today the main security tool is the built-in WEP (Wired Equivalent Privacy) encryption that's required as part of the Wi-Fi certification program. Security experts have found flaws in WEP, however, that prevent it from providing even a minimal reliable level of security for serious applications.

Businesses had a strapped-together system they could use that's still under development, called 802.1x/EAP, but standardization is still coming together, and it ultimately relies on WEP as well in its current version.

In November 2002, the Wi-Fi Alliance, a group that certifies 802.11a and 802.11b devices as interoperable, released an interim replacement for WEP and other aspects of Wi-Fi security that will change the landscape. This new standard is called WPA (Wi-Fi Protected Access).

The 802.11i was a compromise solution that looks backwards to fix WEP and forward to replace it without losing compatibility. The new protocol also fixes packet integrity by using a more complex method of detecting tampering, and putting this information in the encrypted part of the signal (frame) instead of sending it in the clear.

The forward-looking part of 802.11i adds Advanced Encryption Standard (AES) for an impregnable way of hiding of data. AES is quite widely used and has been adopted by the U.S. government.

The 802.11i spec also includes support for the 802.1x and EAP (Extensible Authentication Protocol) protocols. 802.1x is a way of defining roles so that a client has limited access—to a single port only—until the access point it is trying to connect to queries it and relays its messages back and forth to an authentication server that can authenticate the client's identity.

In Closing

As wireless technology continues to effectively address the core issues of speed, distance, and security, we will begin to see wireless networks everywhere, used to connect and provide Internet access from all types of devices from computers and the Internet to PDAs and TVs.

Your Author

Howard "Howie" Fenton is best known for his articles, seminars at shows and consulting. He is the senior consultant of digital technology at NAPL. He audits 35 companies and presents over 100 seminars a year.

For more information

- call 720 872-6339,
- visit www.howiefenton.com, or
- email HowieAtPre@aol.com.