As a network administrator, you probably seldom discuss or even think about the cable that a well-paid somebody threaded through the walls and ceilings in your corporate and branch offices. Why would you think about those thousands of feet of Category 5 or fiber-optic cable? After all, the dozens of cable runs from your company’s LAN infrastructure to offices and conference rooms are still necessary evils, right? Wrong.

Although you may choose to use cable throughout your company’s LAN, the truth is you no longer have to. Using wireless LAN (WLAN) technology, you can augment existing networks or create new ones.

You can, in other words, go wireless. The question is, should you?

ONCE YOU GO WIRELESS . . .

Why would you consider incorporating WLAN technology into your company’s network plan? The short answer is because WLAN technology affords conveniences with which wired LAN technology simply can’t compete.

For example, using WLAN technology to extend an existing wired network considerably reduces the amount of cable required to provide users with network connections. For wireless network segments, you don’t need one cable run per computer, nor do you need to haul spare runs to offices and conference rooms. Granted, you still need to make some cable runs but only to a few carefully placed WLAN access points, which function like on- and off-ramps between wired and wireless network segments. (For more information, see “What Is a WLAN” on p. 12.)

With these few access points hard-wired to the LAN infrastructure, users can access the network from virtually anywhere in your organization—and they won’t have to search for spare Ethernet plugs to make the connection. Using WLAN technology and skipping a few cable runs may also simplify the task of setting up (and maybe later moving) a network segment. Best of all, because WLAN technology requires less cable to pay for and install, your company may save a little money and time.

You can also use WLAN technology in place of a wired LAN—in which case, you won’t need to install cable at all. In fact, in spaces or situations where installing cable is impractical or flat-out impossible, the option of creating an independent WLAN is both attractive and logical. For example, you may want to compare the costs of a wired versus a wireless LAN system if you’re setting up shop in a wood-frame building laden with concrete fire blocks. You should certainly consider going wireless if you work in an old, all-brick building.

Furthermore, all-wireless networks don’t have to be permanent. In any setting—class and conference rooms, parking lots, restaurants—you can create temporary, peer-to-peer networks as long as you and the people with whom you want to share files have laptops equipped with compatible WLAN cards. These temporary wireless networks enable you to exchange files without requiring you to plug in to an Ethernet network or to the Internet.

In fact, with WLAN technology, you don’t necessarily need to plug in to the Internet at all—ever. Instead, you can connect to the Internet cable-free by subscribing to a wireless Internet service, which is available from public access companies such as MobileStar (www.mobilestar.net), Wayport (www.wayport.net), and SkyNet Global (www.skynetglobal.com). With a subscription and a laptop equipped with a WLAN card (that your provider supports), you can connect to the Internet without a telephone jack in sight.

Making the connection can be as simple as launching your browser in any area where your provider has an access point—and these providers have more access points than you may think. The companies just mentioned collectively have access points at select hotels, airports, clubs, and even coffee houses in most major metropolitan areas in the United States and in many cities throughout the world. You could sit in a crowded terminal in the Seattle-Tacoma International Airport, in Starbucks on Polk Street in San Francisco, or in the Four Seasons.
FEATURE Cordless and Cable-Free

Hotel in Paris and wirelessly surf the web, access e-mail messages, or even download files from your company’s network (by way of a virtual private network [VPN], of course).

If wireless Internet access sounds appealing to you, you’re not alone. Users of wireless Internet access services vouch for their appeal. For example, Ken Dulaney, vice president of Gartner Group’s mobile division, is sold on the wireless Internet service to which he subscribes: “Once you go wireless,” Dulaney claims, “you never go back.”

AS GOOD AS IT SOUNDS?

Dulaney makes this statement despite his misgivings about WLAN technology. When discussing the use of WLAN technology to extend wired networks, Dulaney cautions, “Don’t use wireless [technology] when you can use wire.”

This type of comment coupled with your pre-existing doubts about WLAN technology probably destroys any visions you may have of cable-free conveniences—particularly those you picture in an office setting. For example, you have probably read about several existing and emerging WLAN specifications and may be wondering whether any of today’s WLAN specifications will be viable tomorrow.

You may also wonder whether WLAN technology is fast and reliable enough for real networking. Perhaps you question whether WLAN systems today are any easier to manage and any more cost effective than those you may have experimented with a couple of years ago.

Undoubtedly, you have questions about the much publicized security issues associated with WLAN technology: Just how safe is a network when some of the connections are made via invisible radio waves?

These concerns point again to the implied question raised in the beginning of this article: Is the time really right for your company to go wireless? As you can guess, this question raised in the beginning of “What Is a WLAN?” on p. 12.

Ratified on September 16, 1999, the 802.11b standard has emerged as the wireless standard of choice. In fact, according to Allen Nogee, senior analyst for Cahner’s In-Stat Group, of the wireless products that shipped worldwide in 2000, 78 percent were based on 802.11b.

Analysts and wireless vendors alike agree that 802.11b has eliminated many barriers to the widespread adoption of WLAN technology. In other words, 802.11b has opened up the WLAN market, the revenues for which should be around U.S. $1.7 billion this year alone, according to Nogee.

That said, 802.11b may be only the tip of the wireless standard iceberg. Two other IEEE 802.11 standards are emerging: 802.11a and 802.11g. Products based on 802.11a will operate in the 5.15 to 5.35 GHz frequency band at a rate of 54 Mbps. Products based on 802.11g will operate in the 2.4 GHz band at a rate of greater than 20 Mbps.

According to Nogee, you can expect to see products based on 802.11a by the end of this year, and you may see products based on 802.11g as early as next year. Dulaney isn’t quite as optimistic, claiming that you’ll have to wait another “two years or so” to see 802.11a products.

Vendors are significantly more optimistic than either of these analysts: At NetWorld+Interop on May 11, Proxim, Intermec, TDK, and CardAccess announced they will make 802.11a products available by the third or fourth quarter of this year.

Regardless of when these higher-rate products will be available, you should understand a few things about 802.11a and 802.11g. The analysts with which Novell Connection spoke share a number of concerns about 802.11a. For one thing, Nogee points out, “there have been some concerns that the range and penetration of 802.11a products can’t match that of 802.11b.” Dulaney supports Nogee’s point, claiming that 802.11a will require “four times as many access points as 802.11b” to offer its impressive rate.

This requirement will obviously increase the cost of deploying 802.11a products, which will be considerably more expensive than 802.11b products to begin with.

A gain, vendors are much more optimistic about 802.11a. For example, Lynn Chroust of Proxim points out that moving from 802.11 to 802.11b products also required roughly four times as many access points. “Ultimately,” Chroust adds, “this didn’t slow the adoption of 802.11b.
because folks wanted the increased speed.” Chroust also says, in sharp contrast to the analysts’ speculation, that Proxim’s 802.11a products will be priced similarly to its current 802.11b products.

Enterasys is equally optimistic. Brian Murphy, Enterasys’ product marketing manager, asserts that 802.11a will deliver significant performance advantages over 802.11b—at equal ranges in nearly all scenarios. For example, with 802.11b, you can expect 11 M bps at 150 feet. With 802.11a, you can expect 24 M bps or better within the same range. To get the 54 M bps performance, you must be no farther than 50 feet from an access point.

A more important point to note about 802.11a products is that because they will operate in the 5.15 to 5.35 GHz band, they will not interoperate with 802.11b products. In contrast, 802.11g is basically an improved version of 802.11b. As a result, the 802.11g products you buy tomorrow will be compatible with the 802.11b products you buy today.

The bottom line, according to Nogee, is this: “If 11 M bps is fast enough for your needs, look at the 802.11b systems available today.” If you need a faster data rate, Nogee continues, wait for the 802.11g products. As for 802.11a, Nogee says Nogee, “give [it] some time to improve. [802.11a products] will be a viable option a few years down the line.”

THE PRICE IS RIGHT, RIGHT?

The simple answer to the question regarding whether WLAN systems are reasonably priced is, “You bet!” Since the proliferation of 802.11b products, prices of WLAN products have dropped dramatically over the last couple of years. You can now buy wireless PC and PCI cards for laptop and desktop computers for as little as U.S. $99 but more commonly for around U.S. $200. (For more information about the price of wireless products, see a list of products at www.ncmag.com.) Basic access points are available for as little as U.S. $699. For the enterprise, however, access points are more commonly about $1,200.

The number of wireless PC or PCI cards you need obviously depends on the number of desktop and laptop computers you plan to include in your WLAN. The number of access points you need also varies, depending on several factors such as how many users you have and how much traffic is expected. For example, Compaq Corp. says that each of its wireless LAN access points provides up to 11 Mbps radio data rate for the following user cases:

• 50 mostly idle users who check only an occasional text-based e-mail
• 25 users who check e-mail frequently and who download and upload medium-sized files
• 10 to 20 power users who constantly use the network and deal with large files

To extend capacity, Compaq points out, you simply add more access points. In addition, to optimize the network, you set the access points to different channels. Channels represent the specific frequency that access points and clients use to communicate with one another. You actually set each access point on a specific channel, but you do not set the channel for each client. Instead, clients generally associate with the access point that has the strongest signal. (For more information about channels, see “What Is a WLAN?” on p. 12.)

Thus, suppose you placed three access points (with a range of up to 100 feet each) in three adjacent offices and set each access point to a different channel. This setup would allow as many as 150 users to share a total maximum of up to 33 M bps, although no single user would ever have throughput speeds greater than 11 M bps. In reality, because clients typically associate with the access point from which they receive the strongest signal, the bandwidth would probably not be dispersed evenly among users. (For more information, visit Compaq’s web site, which incidentally has an excellent FAQ section: www.compaq.com/products/wireless/wlan.)

Nevertheless, for the sake of example, assume you can take Compaq’s numbers at face value. Based on these recommendations, you might strategically place three access points in three offices and provide at least 20 hyperactive users (the workaholics in your office) with wireless access to the network. To provide at least 20 users with full access, you would spend around U.S. $7,000 on hardware—U.S. $1,000 for each of the three access points and U.S. $200 for each PC or PCI card. That’s not bad, and don’t forget, you won’t have to pay for cable.

WHAT’S THE RETURN ON A WLAN INVESTMENT?

If you’re interested in a cost scenario that is a bit more concrete, you should be happy to learn that you can find results of a WLAN cost-benefit study on the Wireless LAN Alliance (WLANA) web site at www.wlana.com. WLANA is an alliance of WLAN vendors that attempts to educate anyone interested in WLANs.

For its study, titled “Wireless Local Area Networking: ROI/Cost-Benefit Evaluation: A Cost-Benefit Analysis of Wireless LANs,” the Wireless LAN Alliance (WLANA) found that WLANs offer a better return on your investment than cable. In fact, WLANs offer a return on investment nearly twice as fast as cable. To illustrate, WLANA researchers spent many hours attempting to educate anyone interested in WLANs. Their findings, however, have not been dispersed evenly among users. (For more information, visit Compaq’s web site, which incidentally has an excellent FAQ section: www.compaq.com/products/wireless/wlan.)

Nevertheless, for the sake of example, assume you can take Compaq’s numbers at face value. Based on these recommendations, you might strategically place three access points in three offices and provide at least 20 hyperactive users (the workaholics in your office) with wireless access to the network. To provide at least 20 users with full access, you would spend around U.S. $7,000 on hardware—U.S. $1,000 for each of the three access points and U.S. $200 for each PC or PCI card. That’s not bad, and don’t forget, you won’t have to pay for cable.
A wireless LAN (WLAN) is basically just what it sounds like—a network without wires. Like their wired counterparts, WLANs use a transmission media. However, unlike wired LANs, which channel network traffic through copper or fiber-optic cable, WLANs use radio frequencies as their transmission media, sending network traffic sailing over the air.

**AD HOC VERSUS INFRASTRUCTURE**

You can use WLAN technology to configure wireless networks that either replace a wired network or extend an existing one. The most basic WLAN configuration forms a peer-to-peer network sometimes called an independent WLAN but more commonly called an ad hoc WLAN.

In an ad hoc WLAN, laptop or desktop computers that are equipped with compatible WLAN adapters and are within range of one another can share and exchange files wirelessly. (See Figure 2 on p. 10.) The range varies, depending on the type of WLAN system. Laptop and desktop computers equipped with 802.11b WLAN cards can create ad hoc networks if they are within at least 500 feet of one another. (As you might expect, the closer the range, the greater the transmission speed.)

Setting up an ad hoc network is quite simple. You first use the wireless client software to select peer-to-peer operation mode. You then click Network Neighborhood, after which the wireless client searches for other nodes that are also operating in peer-to-peer mode. When your wireless client finds another node that is operating in peer-to-peer mode, you can access this node’s files and folders that are marked shared.

Although all-wireless ad hoc networks are unquestionably convenient, WLAN technology is used more frequently to extend existing wired networks. WLAN systems that provide cable-free connectivity between users and a wired LAN infrastructure are commonly called infrastructure networks.

**SETTING UP AN INFRASTRUCTURE WLAN—JUST THE GIST**

Infrastructure WLANs consist of two primary components: access points and PC (or PCI) cards. Using an ordinary RJ-45 cable, you can connect an access point to a wired Ethernet network. (Access points can be software that you run on a server, but the vast majority of them are separate pieces of hardware.)

Once connected to the network, the access point thereafter functions like a wireless hub, passing data back and forth between the wired network and your wireless clients. The access point translates the digital data from the network into radio signals that wireless clients can understand.

Wireless clients are laptop or desktop computers equipped with PC or PCI cards, respectively. The PC (or PCI) card receives radio signals from the access point with which it is communicating and translates that signal into digital data that the PC can understand.

Access points and wireless clients communicate over channels within the 2.4 GHz frequency band. (For more information, see “No License Necessary” on p. 16.) A channel is a specific frequency within a given frequency band. For example, Channel 2 in the 2.4 GHz band runs specifically at 2.402 GHz. Channel 3 runs at 2.403 GHz.

The 2.4 GHz frequency band has a total of 80 channels, but different countries enable the use of different frequencies. For example, the United States and Canada use channels 1 through 11. When you set up a WLAN, you set the channel for each access point but not for each wireless client. Wireless clients search for and automatically set their channels to the channel associated with the access point that has the strongest signal, given the wireless client’s location.

Of course, you must set up multiple access points. Each access point provides wireless connectivity to any wireless client within the access point’s range of coverage. (A typical range in an 802.11b system is between 100 to 300 feet but can extend to as much as 500 feet.) The range of coverage is sometimes called a cell but is formally known as a basic service set (BSS). To ensure continuous connectivity to the network, you design your network so that cells overlap. (See Figure 1 on p. 8.)

When setting up a WLAN, you need to ensure, among other things, that access points with overlapping cells are set to different channels to avoid the possibility of cross-talk. Cross-talk occurs when access points pick up signals from other access points set to the same channel, causing client signals to collide. As you might expect, cross-talk degrades performance because access points have to sort through the mess of signals they get and then reconstruct the original and correct signals.

**DSSS VERSUS FHSS**

To transmit data over radio waves, which are also called carrier waves, WLAN devices must superimpose the data being transmitted onto the carrier wave. This process is called modulation. WLANs typically modulate carrier waves using one of two spread-spectrum modulation schemes: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Some 802.11 WLAN systems use FHSS, but all 802.11b WLAN systems and many 802.11 systems use DSSS.

FHSS hops from frequency to frequency in a pattern known to both the transmitter and receiver. Properly synchronized, the transmitter and receiver or, in the context of this discussion, the access point and the wireless client maintain a single logical channel. FHSS appears to be short-duration impulse noise to unintended receivers. Because FHSS uses bandwidth inefficiently, FHSS systems generally have lower data transmission rates than DSSS systems. The 802.11 systems that use FHSS have a throughput of only 1 Mbps.

DSSS creates a redundant bit pattern, called a chip or chipping code, for each transmitted bit. The transmitter and receiver both know the chipping code and are thus able to filter out signals that don’t use the same bit pattern.

The chipping code spreads data across the available bandwidth: The longer the chip, the more bandwidth consumed. The longer the chip, however, the greater the probability that the original data—even if partially damaged—can be recovered without the need for retransmission. To unintended receivers, DSSS signals appear as low-power noise.

DSSS creates a redundant bit pattern, called a chip or chipping code, for each transmitted bit. The transmitter and receiver both know the chipping code and are thus able to filter out signals that don’t use the same bit pattern.

The chipping code spreads data across the available bandwidth: The longer the chip, the more bandwidth consumed. The longer the chip, however, the greater the probability that the original data—even if partially damaged—can be recovered without the need for retransmission. To unintended receivers, DSSS signals appear as low-power noise.

DSSS uses bandwidth more efficiently than FHSS systems. Consequently, WLAN systems based on DSSS generally have higher throughput than their FHSS counterparts. For example, 802.11 systems based on DSSS generally offer a throughput of 2 Mbps, and 802.11b systems offer 11 Mbps throughput.
ARE WLANS FAST ENOUGH?

The simple answer to the question, “Are WLANs fast enough?” is, in many cases, yes. As mentioned, 802.11b products operate at a rate of 11 Mbps, depending on a number of factors such as the distance between clients and access points. More specifically, and as you may expect, data transmission rates generally decrease the farther away wireless clients are from access points, as follows:

<table>
<thead>
<tr>
<th>Distance From Access Point</th>
<th>Data Transmission Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>U p to 100 feet</td>
<td>U p to 11 Mbps</td>
</tr>
<tr>
<td>U p to 150 feet</td>
<td>U p to 5.5 Mbps</td>
</tr>
<tr>
<td>U p to 300 feet</td>
<td>U p to 2 Mbps</td>
</tr>
</tbody>
</table>

In addition to range, other factors can affect the actual throughput you achieve on a WLAN. For one thing, 11 Mbps is the theoretical maximum throughput for 802.11b products. In reality, due to complexities in the 802.11b media access control (MAC) layer, 802.11b systems are actually capable of operating at about only 70 percent of this theoretical maximum, or at about 7.7 Mbps.

In fact, N ogee says that this percentage is optimistic. The high-rate WLAN systems N ogee has seen in “real-world situations” operate at about 50 percent of the theoretical maximum, or at about 5.5 Mbps. Enterasys’ B rian M urphy agrees: “70 percent assumes an optimal situation. People should plan for 5.5 to 6 Mbps.”

In addition, walls, metal objects, and even the number of people between access points and clients affect throughput. “All of these materials,” explains J ohn D rewry, senior director of Business Development in 3Com’s Wireless Connectivity Division, “have the ability to absorb, reflect, or attenuate a wireless signal in the 2.4 GHz range.” In some cases, these materials can block the wireless signal entirely.

Unfortunates, stating with assurance the degree to which range and throughput will be affected by the presence of various performance-inhibiting materials is simply impossible: “You just can’t say a seven-inch wall will impede so much,” says P eter B eardmore, Enterasys general manager. “It just doesn’t work that way.” A suming the obstacle doesn’t block the wireless signal entirely, however, you will simply have to reduce the range or get used to the throughput possible given the obstacle.

In any case, the impact of performance-inhibiting materials can be minimized with a good network design. The bottom line is that with a good network design, you can expect an actual throughput of at least 5.5 Mbps.

ARE WLANS EASY TO SET UP AND MANAGE?

The simple answer to the question regarding whether WLANs are easy to set up and manage is—wait, there is no simple answer. The answer to this question is subjective—even more so than the answer to other questions addressed in this article.

Some vendors claim that installing a wireless LAN is easier than installing a wired LAN, presumably basing this claim on the fact that you get to skip a step: You don’t have to lay cable. However, members of the press have been known to counter vendor claims, one going so far as to suggest that you would need a radio systems expert to properly design and set up a WLAN.

Physically setting up the basic components of a WLAN—that is, access points and wireless clients—isn’t difficult. (To get the gist of setting up a WLAN, see “What Is a WLAN?” on p. 12.) However, remember those obstacles (such as walls, metal, and people)? They can seriously complicate the task of setting up a WLAN.

To ensure your WLAN performs well, you must determine the optimum location for an access point—a location that minimizes the obstacles users encounter. Determining this optimum location is the tricky part about designing and setting up a WLAN.

**Figure 3.** Enterasys RoamAbout products, such as those shown here, provided wireless connectivity to the BrainShare 2001 network.
HOW TRICKY IS "TRICKY"?

Is deciding where to place access points so difficult that you need a radio systems expert to do the job? Beardmore says no, supporting his opinion by pointing out that Enterasys has a sales force of approximately 1,000 people, 45 percent of whom are "pre-sales engineers" whose core competencies are traditional network design. M urphy supports his coworker's claim, saying that depending on the circumstances, most companies can use their own IT people to install a successful WLAN.

3Com's Drewry agrees. You probably won't need a wireless expert, says Drewry, if your "coverage areas are well-defined, such as conference rooms and cafes." Drewry is quick to add, however, that if you are setting up a "sophisticated network that has stringent coverage requirements," you may need some help.

If your company's network is among the sophisticated variety, most vendors of WLAN systems offer consulting services or have value-added resellers who can help you design and install a WLAN. Enterasys also recommends seeking help if you are setting up outdoor wireless connections. (For one example of wireless LAN bridging, see "Out of the Trenches and Into the Air With a WLAN Bridge" on p. 18.)

If you are tackling the job alone, some vendors, such as Proxim, offer free training courses on WLAN installation and site survey techniques. In addition, most WLAN vendors—including Proxim, Enterasys, and 3Com—offer site survey tools. For example, 3Com's 11 Mbps AirConnect access point ships with a site survey utility that enables you to survey, log, and report radio parameters from multiple fixed locations. You can then determine where to best place 3Com's AirConnect access points.

Like 3Com, Enterasys includes a site survey utility with its wireless high-rate PC Card. With the RoamAbout Client Utility, you can wander from room to room and watch as statistics regarding bandwidth, signal strength, and signal-to-noise ratio are displayed graphically on your monitor.

The RoamAbout site survey tool, like other similar tools, helps you better understand the relationship between clients and access points. Armed with this understanding, you can determine where you need additional access points to achieve optimal data transmission rates.

For more information about Enterasys' RoamAbout tool, see "Enterasys Provides Wireless Connectivity to BrainShare Network" on p. 20.

CENRALIZED MANAGEMENT

After you have installed access points, how do you manage them? If you experimented with WLAN systems two or three years ago, you may be surprised (and somewhat relieved) to learn that most WLAN systems today allow you to centrally manage access points.

Most vendors, including Enterasys, Cisco, BreezeCom, IBM, 3Com, and Proxim support Simple Network Management Protocol (SNMP), thereby enabling you to configure and manage your access points from a central location. In addition, many vendors, including 3Com, Dell, Ericsson, and Proxim, offer web-based management interfaces. Consequently, you can configure and manage access points via your browser.

Finally, some vendors offer additional software that you can plug in to a management platform that you are already using. For example, 3Com offers a solution that you can plug in to HP's OpenView, allowing limited management of your WLAN system.

As for the wireless clients, you can configure and manage those in the same way you configure and manage any other client on your network. Furthermore, most vendors' products are compatible with NDS. (For a list of these vendors, visit www.ncmag.com.) As a result, you can control wireless users' access to the network in the same way you manage wired users' access to the network.

Perhaps Nogee best sums up the bottom line on setting up and managing WLAN systems. WLANs "used to be difficult to set up and administer," Nogee says, "but things are definitely improving there."

DO WLANS PLAY NICELY WITH WIRED AND OTHER WIRELESS PRODUCTS?

In other words, you have nothing to worry about in terms of 802.11b products playing nicely with wired products. However, do 802.11b products coexist peacefully with other wireless products? Basically, yes. However, any device that operates within the 2.4 GHz frequency range potentially can interfere with the signals between 802.11b access points and clients.

One heavily publicized (and probably overstated) cause for concern is Bluetooth, a wireless personal area network (WAPAN) technology. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) technology and operates in the 2.4 GHz band at a rate of up to 2 Mbps over a range of up to 33 feet. (For more information about FHSS, see "What Is a WLAN?" on p. 12.)

Although members of the press have
been known to present Bluetooth as a WLAN technology, 802.11b vendors and industry analysts are quick to set the record straight: Bluetooth has neither the range nor the performance capabilities to be a viable WLAN technology.

As a WLAN technology, Bluetooth enables you to connect a few devices using radio frequencies and forming a small wireless network, sometimes called a picocell. For example, Bluetooth eliminates the need for keyboard, mouse, projector, printer, and scanner cabling. Bluetooth also enables laptops, mobile phones, and personal digital assistants (PDAs) to talk to one another without the need for cables or the tedium of infrared beaming.

With the exception of the brouhaha over Y2K, the press has never made so much ado over what might happen. In this case, what might happen is that Bluetooth devices and 802.11b devices might interfere with one another when operating within close proximity.

For now, the problem is mostly theoretical because few shipping products include Bluetooth chips. Nevertheless, the two technologies operate (or rather, will operate) within the same frequency range, and Bluetooth is likely to crop up in corporate environments where 802.11b is already running. When that day arrives, you can expect a degree of mutual interference. But what degree of interference and with what results?

Drewry of 3Com admits that Bluetooth devices and 802.11b devices operating “in close proximity (that is, a few inches) can interfere with one another.” Drewry adds, however, that the interference will not cause “dramatic effects” on the performance of either technology. Both wireless technologies, Drewry explains, “are designed to reliably handle interference from each other as well as other technologies in this band.”

In most cases, Drewry summarizes, the interference between Bluetooth and 802.11b systems will disrupt the systems’ signals (and thus degrade performance), but the interference won’t halt the systems’ signals.

As discussed in the main text of this article, wireless LAN (WLAN) technology enables clients equipped with compatible WLAN cards to communicate wirelessly with each other and with a wired LAN. WLAN technology also enables you to bridge that formidable gap between LANs.

For example, the Novell Corporate Events Team used a wireless LAN bridge to complete connections for the Novell Connecting Points (NCP) network the team set up for COMDEX/Fall ’99. The team bought two Proxim Stratum 100 microwave towers from UrJet Internet. Together, the team and representatives from UrJet Internet anchored the towers to the roofs of the Las Vegas Convention Center (LVCC) and the Venetian Resort in the days before the event.

The result was a stable, 100 Mbps line-of-sight connection between the NCP Network Operations Center (NOC) in the LVCC and the remote NCP workstations in the Venetian Resort, the Sands Expo, and Convention Center. (For more information about NCP, see “Losing Weight at COMDEX With NetWare Cluster Services for NetWare 5,” Novell Connection, Mar. 2000, pp. 18–30. You can download this article from www.ncmag.com/past.)

The Proxim Stratum 100 towers look like flat-panel television screens and measure only 4.75 inches high by 13.5 inches wide x 10.25 inches deep (12.1 cm x 34.3 cm x 26.0 cm). (You can find photos of the Stratus 100 at www.proxim.com/products/stratum/photos.shtml.) Despite their small frames, the towers were physically challenging to anchor: The group had to carry the 23-pound (10.5 kg) towers and their 8-pound (3.6 kg) mount units to the rooftops. The group then anchored the towers by bolting them to cinder blocks—which were also hand-carried to the rooftops—and running guide wires from the towers to the blocks.

Although carrying the towers to the rooftops and anchoring them was physically difficult, establishing the line-of-sight connection between the towers was surprisingly simple. A member of the Novell Corporate Events Team explains that the group aimed the tower on the Venetian Resort at the tower on the LVCC, then aimed the LVCC tower back at the Venetian Resort tower, and that was that. The connection worked immediately.
Do 802.11b Devices Play Nicely With Other WLAN Devices?

Whether or not your company’s 802.11b system will interoperate with other WLAN systems depends on the frequency range and the spread-spectrum technology that the other WLAN system uses.

For example, 802.11b devices interoperate with many 802.11 devices, assuming the 802.11 devices use DSSS rather than FHSS, as some of these devices can. As you already know, the upcoming 802.11g products will also operate in the 2.4 GHz frequency range and will use DSSS, enabling them to work well with 802.11b devices. Although 802.11b devices will not interoperate with the upcoming 802.11a systems, 802.11b devices will be compatible with 802.11a systems. In other words, the two systems will not interfere with one another.

Before you get bogged down by these details, however, you should understand this much: Virtually all 802.11b devices are interoperable. The Wireless Ethernet Compatibility Alliance (WECA) stamps the Wi-Fi (for "wireless fidelity") seal of approval on all of the 802.11b devices that pass its interoperability tests. (For more information, visit www.weca.net.) Knowing that most 802.11b devices are Wi-Fi certified, you shouldn’t be surprised to learn that 802.11b devices are frequently called Wi-Fi devices. To date, approximately 80 companies support WECA, and more than 100 products are currently Wi-Fi certified, according to Murphy. (To view a list of certified products, visit www.wi-fi.com/certified_products.asp.)

The bottom line is this: You can lay your WLAN interoperability concerns to rest.

Are WLANS Secure Enough For Corporate Use?

Arguably the best answer to the question of whether WLANs are secure enough for corporate use is “Good question!” Vendors and analysts agree that security is one of network administrators’ primary concerns about WLAN technology. Most vendors and analysts also agree that your concern is warranted. However, vendors will say that your concern is warranted only to the extent that concern regarding security on any network—wired or wireless—is warranted. In other words, security (or rather the lack thereof) should always be a concern.

The primary point of contention pivots around the following question: Is the level of security available for wireless networks more, less than, or equal to the level of security available for wired networks?

Ask any WLAN vendor representative, and you’re likely to hear either that WLANs are every bit as secure as wired networks or that WLANs are actually more secure than wired networks. WLAN vendors base these claims on several points. For example, vendors may point out that the military was the first to use the spread-spectrum technology on which WLANs are based. During World War II, the military used spread-spectrum technology to secure radio communications. Vendors will also certainly point out that every Wi-Fi system supports what is called Wired Equivalent Privacy (WEP),

For more information, visit www.ncmag.com/advertise.html.
which—as its name clearly suggests—purportedly provides a level of security equal to that found on a wired network. (You can enable WEP at the client interface or at the access point.)

WEP uses a 40-bit key that is based on the RC4 algorithm to encrypt the data transmissions between wireless clients and access points. Some vendors exaggerate the length and, therefore, the strength of this key: By including the 24-bit initialization vector, these vendors claim the total key length is 64 bits. Don’t be fooled, however: 64-bit and 40-bit WEP provide identical levels of security.

To improve security, most WLAN vendors provide an extension to WEP. This extension allows for the use of 128-bit key lengths.

THE NEW BAD NEWS

What vendors don’t typically point out is that the military used a spread-spectrum technology based on FHSS rather than on DSSS. Of course, 802.11b devices are based on DSSS.

In addition, vendors will probably not volunteer that enabling WEP impacts performance: Your company’s WLAN will take about a 10 percent performance hit when you enable WEP.

Finally, vendors may casually mention that the 128-bit extensions to WEP are based on proprietary solutions. This problem may be significant: Although Wi-Fi systems’ 40-bit WEP encryption schemes are guaranteed to be interoperable, the 128-bit schemes are not. That said, Enterasys’ Murphy claims that most 128-bit encryption schemes are, in fact, interoperable and further claims that WCCA will be testing this presumed interoperability beginning this year.

With the publication of studies on WLAN security conducted by the University of California at Berkeley (UC-Berkeley) and the University of Maryland (UMD) Department of Computer Science, concerns over WLAN security have risen to an all-time high. In the February 2, 2001 paper titled “Intercepting Mobile Communications: The Insecurity of 802.11b,” UC-Berkeley researchers report that by using admittedly sophisticated techniques, they were able to overwhelm WEP on 802.11b...
systems. More specifically, the U.C.-Berkeley researchers claim to have discovered security flaws that enabled them to eavesdrop on transmissions, intercept messages, alter the network, and build systems that allow them to pull passwords from thin air. (You can download a draft of this paper from www.isaac.cs.berkeley.edu/isaac/wep-faq.html.)

The March 30 U M D study, “Your 802.11 Wireless Network Has No Clothes,” further solidified the idea that 802.11b W L A N s are riddled with security flaws. The U M D researchers claim to have found security flaws that enabled them to easily sniff 802.11b network names, discover shared secrets, and thus gain unauthorized access to the network. The U M D researchers were also able to sniff MAC addresses and use these authorized addresses to masquerade as valid users. (You can download this study from www.cs.umd.edu/~waa/wireless.pdf.)

THE OLD GOOD NEWS

In response to this news, W L A N vendors are likely to point out that W EP was never intended to provide high security—just a level of security equal to that of a wired network. Furthermore, according to Proxim’s Chroust, the IEE, has been working on resolving many of the reported security flaws in the new 802.11e specification, which is expected to be finalized sometime next year. In addition, the 802.11x committee is working to improve authentication protocols on both wired and wireless networks.

However, you don’t need to wait for solutions based on 802.11e to secure W L A N s today. Vendors and analysts agree that the wise approach to security—on both wireless and wired LANs—is a layered approach. That is, you shouldn’t use only W EP to secure your W L A N ; You should also use other encryption solutions, including the 128-bit W EP extensions some providers include with their products.

The bottom line is this: Given enough time, the right equipment, and the know-how, someone could break into your company’s W L A N —just as they could break into your company’s wired LAN. To protect your company’s W L A N (and LAN), you need added layers of security.

READY OR NOT

A letter reading about many of the issues affecting W L A N s—such as performance, cost, management, interoperability, and security concerns—you are now better prepared to face the original question: Is the time right for corporations to go wireless?

You shouldn’t use only W EP to secure your WLAN; You should also use other encryption solutions, including the 128-bit WEP extensions some providers include with their products.

With 802.11b Standard, Franklin includes a product report card of sorts. In this report card, the reviewers rate the products in several categories, including performance, flexibility, ease-of-use, integration, and enterprise readiness. All five products scored As and Bs in all categories—including enterprise readiness.

W L A N vendors, of course, are not surprised by the current nor expected success of the W L A N market. In fact, ask a W L A N vendor whether or not the time is right for corporations to go wireless, and the answer you get will be so short and sweet that you’ll probably feel stupid for asking. “Certainly” the time is right, says Enterasys’ Murphy. “Has been for over a year.”

Gartner’s Dulaney, however, is not convinced the time is right for corporations to go wireless. “I’m not sure if [W L A N technology] is right for corporate offices,” says Dulaney. “But it’s certainly right for some offices—home offices, remote offices, small offices—and anywhere that cabling is costly and impractical.”

Whether you like it or not, however, W L A N solutions are permeating your corporate borders. “Like many previous emerging technologies,” 3Com’s Drewry points out, “departmental buyers and people in the operation side of the business are deploying W L A N s to solve real-world problems today—whether it be to address hard-to-wire areas, to provide simple connectivity to visiting salespeople, or to engender more productive meetings in conference rooms by delivering real-time information access.”

If Drewry is right, the answer to the question of whether the time is right for your corporation to go wireless may be a moot point. Sooner or later, W L A N systems will be part of your corporate network environment, whether you like it or not.

Thus, the better question to pose is this: How can I get the most from the W L A N devices and systems that will inevitably make their way into my company’s network? To this question, Drewry offers reasonable advice: You and others in your IT department should “champion the technology to ensure proper design, configuration, management, and security of W L A N systems.”

Linda Kennard works for Niche Associates, an agency that specializes in writing and editing technical documents.