Feature Article:

In-Building Wireless Networks

By Mitchell Shnier

Many productivity-enhancing tools depend on wireless data communications. In the past, wireless data communications within buildings has been proprietary with no interoperability.

That is, the methods used were developed by each vendor for use with their own products, and these would not work with other vendors' products. Each vendor's products would have a relatively small installed base (providing low economies of scale) so the cost would be relatively high. Since vendors each used their own, unique, communication methods, switching to a different vendor's products usually required installing their entire system. Some users perceived that vendors therefore did not need to provide the best possible price, performance or service, since it would be very expensive for a user to switch their entire system to a different vendor's.

This situation — which was good for the vendors, but bad for users — changed in 1989 with the release of the beginning of a family of standards for wireless local area networks (WLANs), developed by Institute of Electrical and Electronics Engineers. IEEE 802.11 defined operation at 1 and 2 Mbits/s, and became somewhat popular. But the later adoption of 802.11b which defined 5.5 and 11 Mbits/s operation became extremely popular, as laptop users didn't have to compromise on throughput to go wireless.

While these standards are more than 600 pages long, actually using the technology is not very difficult — and better than that, this is a technology that works, can be used all over the world, and is very low cost. This, along with the iSeries' (and most every other computing device's) support for Ethernet and TCP/IP means that users have much greater flexibility in choosing products for their wireless applications. Rather than buying a complete "turn-key" system, where a vendor does everything for you (and charges accordingly), users can now do some of the planning, vendor selection, and configuration themselves, and gain valuable knowledge for later trouble-shooting and system expansion.

One extremely valuable aspect of 802.11 is that it can be used for many applications simultaneously, multiplying the benefit of its installation. For example, many organizations are now providing 802.11 coverage in their warehouses to provide communications for the following:

- real-time access to their AS/400s by wireless bar code scanners
- cordless telephones which can also receive text messages
- pocket PCs and other handheld personal digital assistants (PDAs)
- laptop and tablet PCs

In addition to the benefits of these many uses, deploying 802.11 in warehouses (as compared to an office area) is usually relatively inexpensive since running the cabling to the Access Points is easy (no ceilings or walls), and fewer Access Points are required (since there are fewer obstructions to the signal).

In this article, I will present some of the issues and configuration requirements involved in implementing an 802.11 wireless network to provide coverage to portable devices in a warehouse.

The Standards

As mentioned above, the standards are huge, but for this discussion we can pay attention to just a few key characteristics of them:

The basic 802.11 standard defines operation at 1 Mbit/s and 2 Mbits/s in the 2.4 GHz frequency band. The 802.11b standard defines 5.5 and 11 Mbits/s operation in the same 2.4 GHz band. The 802.11a standard defines operation up to 54 Mbits/s in the 5.8 GHz band. The 5.8 GHz band has the advantage that more channels are available, and there are fewer interfering devices in that band. However to provide connectivity for both 802.11a and 802.11b devices (some organizations will need to support both types of stations) would require two radios, substantially increasing the cost of such dual-band Access Points.

A proposed new standard, called 802.11g, is also to provide speeds up to 54 Mbits/s, but in the same 2.4 GHz band as 802.11 and 802.11b uses. This means that an 802.11g Access Point could easily provide connectivity for 802.11 and 802.11b stations as well. However, microwave ovens, many cordless telephones and other 802.11b WLANs all use the 2.4 GHz frequency band, so while this is a lower-cost expansion path, it provides less scalability in throughput.

The Network

Figure 1 shows a typical network. An Ethernet LAN is used to provide connectivity for an AS/400, PCs, terminals, another server, and a firewall for connectivity to the Internet. To provide 802.11 coverage as well, an *Access Point* is used. This is the term used for the magic device that provides wireless coverage, and creates a *wireless local area network* (WLAN). An Access Point requires power (discussed below), a LAN connection, and an antenna. As shown, some Access Points have two antennas, as this *space diversity* provides better protection against dead spots in coverage.

A single Access Point can provide connectivity to as many *stations* as you're likely to have (most can handle hundreds of simultaneous connections), but additional Access Points will be required to provide:

- more throughput in a given area (this is rarely needed)
- radio coverage for a larger area (this is very common)

Generally, an Access Point has a range of hundreds of feet. It can be over a thousand feet outdoors with no obstructions and an antenna mounted

high off the ground. And it can be tens of feet indoors with walls and office furniture as obstructions, and especially with some miniature wireless adapters commonly used on PDAs.

Site Survey

For any wireless network, it is important to have a site survey performed to ensure adequate signal quality in the areas which require it. This should be done using equipment which can not only verify the signal strength, but also check for interfering noise. Companies such as Berkeley Varitronics (www.bvsystems.com) sell such equipment for US$1,200 to $4,300, which is expensive enough, and is used seldom enough, that for new installations, companies usually have others do the site survey and recommend the number and location of the Access Points.

A site survey should also check for other issues, such as:

- source of power for the Access Points
- unusual mounting requirements (aesthetic requirements, security against theft, building code requirements)
- checking LAN cable distances and connection points
- temperature extremes

Access Points

A key decision when implementing a wireless LAN is the choice of Access Points. For less than $200 each, office supply stores sell Access Points from companies such as Linksys Group and D-Link Systems. However, there are many requirements other than the basic functionality that are important, for example:

- support for prioritization of specific types of traffic; this is important if the wireless network may be used to support wireless telephones
- support for virtual LANs (VLANs), which is important for both prioritization of traffic, as well as isolating certain types of traffic for security purposes
- maximum power output, some Access Points have a lower transmit power than others, and therefore less range
- encryption support, most Access Points support the basic standardized types of encryption, but these have been found to be inadequate for some applications
- support for additional radios, as new versions of 802.11 become available, some installations may need to simultaneously support more than one standard, and it may be desirable to have a common enclosure to house multiple radios, sharing some components such as power supply and LAN connection
- management and diagnostics are important issues when many Access Points are installed, and being able to view and change parameters for more than one Access Point at a time, and to easily update firmware is important
- choice of antenna is important for special situations (such as mounting on an external wall, or a point-to-point, rather than omni-directional coverage pattern), and consumer Access Points generally don't offer this
- mounting options, including clips for T-bar suspended ceilings, options for open-web steel joists, and having security holes to ensure Access Points in public places are not stolen are important for many commercial environments
- transmit power control is important in some situations where it is desired to transmit at a lower power to reduce range (to keep people outside your building from trying to access your network) or to increase the number of Access Points that can use a frequency in a given area (to increase the number of simultaneous users)
- extended temperature range, for operation both below and above normal office temperatures

Commercial-grade Access Points from companies such as Cisco and 3Com can cost as much as $2,000 each.

In addition, there are other devices called wireless Bridges and wireless Gateways which can provide other capabilities, such as connecting two LANs together, or sharing a single IP address between multiple devices.

The selection of Access Points therefore requires a careful analysis of the requirements.

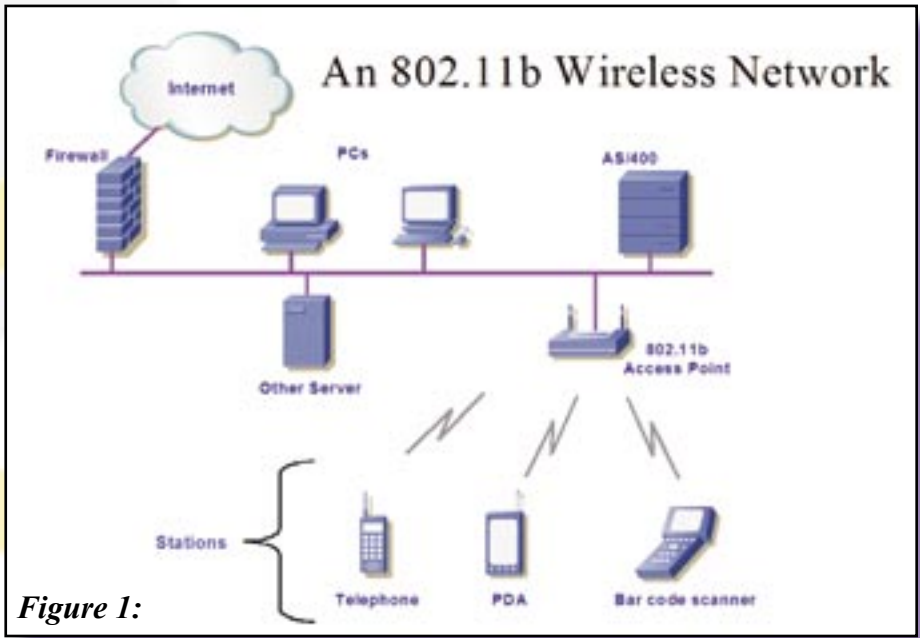


Figure 1:

Configuration

As with most networking devices, there are some crucial parameters that must be configured before they can be used.

While I've spelled out the acronyms below, thankfully, there's no need to understand where these terms came from. The basic parameters which need to be set are as follows:

Ad-hoc or **Infrastructure** mode (also called IBSS — Independent Basic Service Set, and ESS — Extended Service Set, respectively). In Ad-hoc mode, the stations (the mobile devices) directly communicate with each other, just as any two PCs on an Ethernet can directly exchange frames. Normally however, WLANs use Infrastructure mode, where all stations *associate* (that is, connect to) the nearest Access Point, and the Access Point then handles all communications with other stations and with other devices on the LAN.

BSSID (Basic Service Set Identification) — this is the name of the network, and is up to 32 case-sensitive characters. All devices that need to directly communicate with each other must have matching BSSIDs. So every client device (bar code scanner, PDA, laptop computer, and so on) and every Access Point must have their BSSID set to the exact same string.

Channel needs to be set only on Access Points (the stations in Infrastructure mode automatically find what channel the Access Point with the matching BSSID is set to). In North America, channels 1 through 11 can be used. As shown in **Figure 2**, adjacent channels overlap, and the only channels which completely don't interfere with each other are channels 1, 6, and 11. Therefore, it is best to only use channels 1, 6, and 11. And when the coverage areas of adjacent Access Points overlap, it is best to set those Access Points to different channels.

Encryption type and key also needs to be set the same on all communicating devices. 802.11 includes a type of encryption called Wired Equivalent Privacy (WEP), as the intent was to provide a level of security for the packets being sent through the air equivalent to the security you get for the packets on your own internal wired LAN To configure WEP, there are three choices for the type of encryption:

- none, where anyone can snoop your packets as if they were plugged into your LAN
- 40-bit (also called 64-bit, due to an additional 24-bit value that is also used in the encryption process) encryption. In this case, you also need to set a 5-byte shared secret encryption key.
- 104-bit (also called 128-bit, again, due to the additional 24-bit value) encryption. In this case, you need to set a 13-byte shared secret encryption key.

The encryption keys themselves are usually entered as hexadecimal digits. So a 40-bit encryption key is 5 bytes, and is entered as 10 hexadecimal digits, such as **FA5E4321CA**. People don't like remembering 10-digit sequences like that, so most vendors allow you to enter something called a *passphrase*, which is a longer sequence of words or digits, such as *iSeries is my series 4ever*, or something else which you can remember. This passphrase is then run through an algorithm to generate the 10-digit hexadecimal key. The problem is that each vendor uses a different algorithm to generate the 10-digit hexadecimal key from the passphrase, so using the passphrase method only simplifies things if all your equipment is from the same vendor.

The characteristic that the encryption keys are "shared and secret" is important — and a problem. *Shared* means that both the sender and receiver of an encrypted message use the same key. That is, all the Access Points and all the stations on the WLAN must be configured with the same key. *Secret* means that the key must not be known to outsiders, as the encryption key is the only thing keeping someone parked outside your building with a laptop PC and a WLAN adapter from being able to watch all your traffic as if they had plugged their PC directly into your LAN.

So if a visiting vendor wants to demonstrate their wireless product on your WLAN (that is, their product needs to be temporarily configured with your encryption key), or an employee that knows your encryption key leaves the company, then you need get to every Access Point and every station and reprogram a new key. And while you are doing this, the network won't be very usable. And if there are problems, such as forgetting how to get at this configuration parameter which is buried in some menu scheme you don't use very often, then you have a bigger headache.

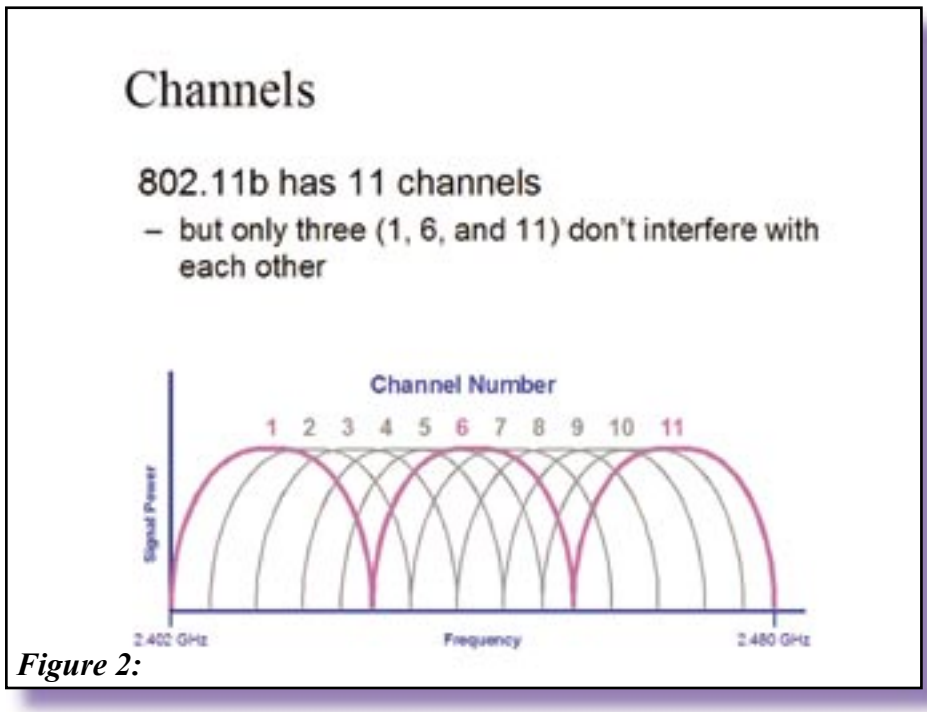


Figure 2:

So while WEP is great because it is standardized and interoperable (it works between different vendors equipment), it is a pain to maintain. But there's a worse problem than that.

Unfortunately, it turns out the way the encryption was implemented, it is quite easy to decrypt (that is, if you are smart enough, or look for programs called WEPCrack or Airsnort on the Internet, and can gather about a million packets before the encryption keys are changed). However:

- WEP is far better than nothing
- there are many additional very secure levels of encryption that can be implemented (such as VPNs)
- there are proprietary solutions (such as Cisco's LEAP, which is their implementation of Extensible Authentication Protocol, which is described in 802.1x)
- there are several standards in development (such as 802.1x, which implements Dynamic WEP, where the encryption keys are changed frequently and automatically, and 802.11i, in which a more secure type of encryption, called AES — Advanced Encryption Standard — is specified)

So the bottom line is, 802.11 can be as secure as you need, but like all security, there is some planning and work involved.

Power

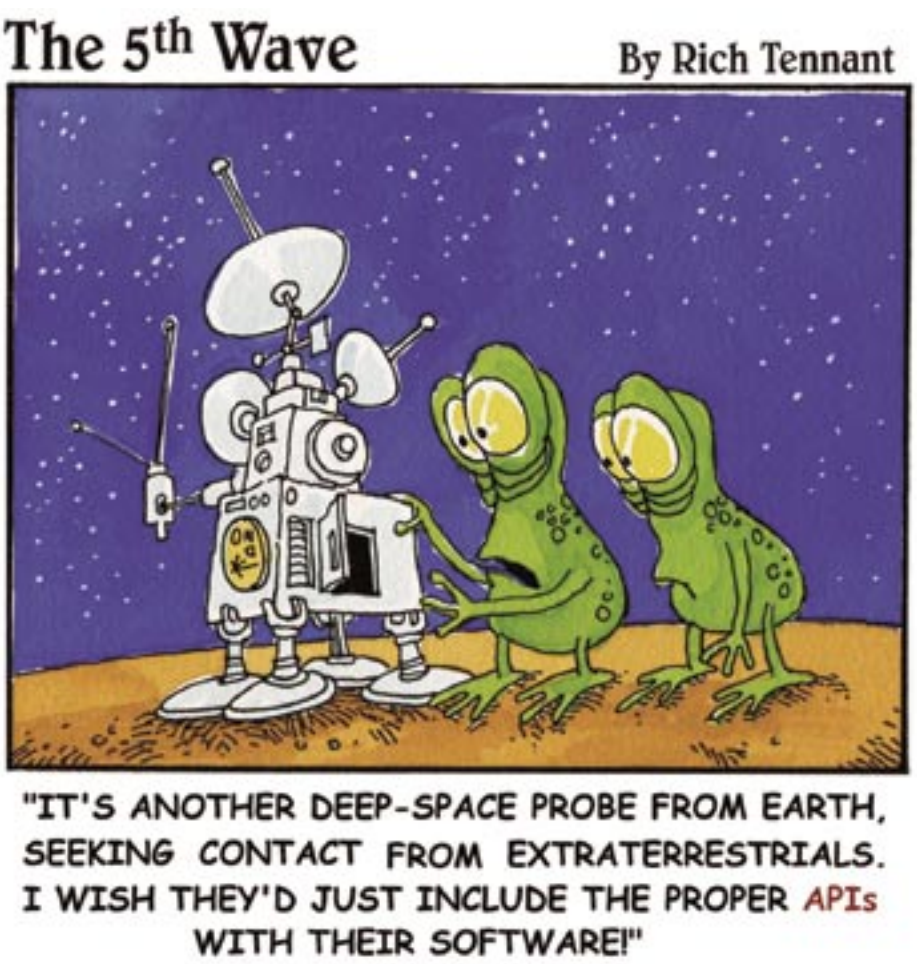
Access Points require power, often simply from the typical power cube transformer that plugs directly into a wall socket. Providing such a wall socket, or a long extension cord to one, for an Access Point mounted at the ceiling in the middle of your warehouse is a problem. The solution to this is called Power over Ethernet, where power is supplied to the Access Point either over an unused pair of wires in a standard 4-pair Ethernet cable (Ethernet itself typically uses only two pairs), or a fancier scheme that puts the power on the same pairs as are used for the data. Some important issues are therefore:

- which pairs are used
- what voltage is used, and
- how does the power get put onto those pairs.

For the first two issues, many vendors have come up with their own proprietary answers — for example, Cisco Systems has theirs, and Symbol Technologies has a different way of doing it. But these schemes will soon be replaced by a new standard to be called 802.3af, which is expected to be widely supported. It is expected to use 48 volts (this higher voltage means a lower current can be used to deliver the same power, which means power can be provided over a greater cable length) on the same pairs as are used for the data. Traditionally, the power has been put onto the cable using an external box, sometimes called a power injector, which is connected in-line with the Ethernet cable. Partially driven by the same concern (that is, needing to power devices connected to an Ethernet LAN) for VoIP (Voice over IP) desk telephones, the cleaner way of doing this is for the Ethernet switch connecting the Access Point to the LAN to supply and put the power onto the cable, and there are already products on the market that do just this.

Conclusion

A wireless LAN based on IEEE 802.11b is a low-cost way to provide connectivity for productivity-enhancing mobile devices in warehouses, offices and elsewhere. As with most technologies, there is new terminology to learn, and problems to avoid, I hope this article will be helpful to you in evaluating, implementing, or expanding your own wireless LAN. TUG



Mitchell Shnier *is president of Lance Communications, which is a developer of wireless bar coding equipment and 5250 communication software, and provides wireless and data communications consulting services. He can be reached at 416-222-1430 and MShnier@LanceCom.com.*