

# Network Design Manual

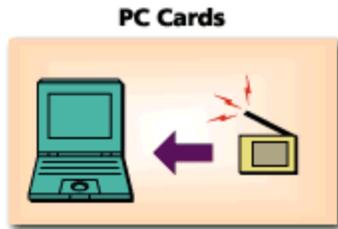
## Planning and Implementing Wireless LANS

By Peter Rysavy Wireless communications allows us to live and work in ways never before possible, offering us flexibility, mobility and a link to our environment that is almost magical. Anybody that uses cordless or cellular phones, pagers, TV remote controls, keyless car entry, or garage door openers will readily agree. While telecommunications and computer networking have vastly increased our options on how and what we communicate, they have physically constrained us by leashing us with a physical wire to the network. But wireless communications brings us back to a form of communications that is inherently natural to us. As creatures we do not like to be physically constrained. Human speech itself, despite its limited range, is wireless.

### The First Bit

Wireless communications today span a wide range of different technologies, including cellular, Personal Communications Service (PCS), satellite, infrared, wireless data WANs, specialized mobile radio, and wireless LANs. A previous online chapter, [Wide Area Wireless WANs](#), discussed wireless wide area networks, including cellular, PCS, CDPD, RAM Mobile Data, ARDIS, Metricom Ricochet, paging and satellite communications. In this chapter we shorten our sights to concentrate on local area networks.

Wireless LAN technology today is relatively mature, though its adoption has not always met vendors' expectations. Nevertheless, wireless LANs are becoming commonplace in applications such as health care, trading floors, supermarkets, transportation and warehousing and are increasingly being used in office environments. Meanwhile the number of vendors keeps increasing, the technology keeps getting better and less expensive, and with the recently completed IEEE 802.11 standard, interoperability between vendors is becoming less of an issue. Moreover, convenient form factors such as PC Cards are becoming common. You may be surprised at how easy wireless LANs are to use and deploy, and how cost effective they are compared to wired LANs, which have many indirect and hidden costs associated with installation and reconfigurations.



Wireless LAN hardware costs more than wired LAN hardware and throughput is usually slower. But the technology allows us to set up networks in hard-to-wire places such as historic buildings or in temporary circumstances such as at trade shows and to support technology workers who need to be mobile. Many wireless LAN vendors also offer products that can bridge networks together as an alternative to leased line connections (though that is not our focus here).

Wireless LANs are fundamentally different from their wide area cousins. They differ in performance, usage, type of spectrum and in their connection with existing networks. Explaining why is one of our first topics as we examine the types of wireless LANs. We then drill into the various aspects of how wireless LANs work so you understand how to purchase and deploy them. We explain how to configure network software and applications, we discuss future trends in the industry, and we end with a useful table of vendor information. Our table of contents is:

- [Types of Wireless LANs](#)
- [Understanding Wireless LANs](#)
- [Making Network Software and Applications Work](#)
- [Propagating Into the Future](#)
- [Vendor Information](#)

## Types of Wireless LANs

It might seem obvious that the key differentiating factor between wireless LANs and wireless WANs is that they operate in a local area, but local operation has many significant and not necessarily obvious consequences. First and foremost, wireless LANs operate at much higher speeds, ranging from 1 Mbps to 20 Mbps compared to wireless WANs, which today range from 4 Kbps to 30 Kbps. Higher speeds are possible because that band of the spectrum is shared by a much smaller number of users. Whereas a cellular base station can serve a radius of over 10 kilometers (six miles), a wireless LAN access point typically serves a maximum radius of about a hundred meters. Due to the shorter distances involved in wireless LANs, radio signals experience less interference and distortion from the environment, thus reducing the amount of error control required. Users are also stationary or moving at walking speeds, while wide area networks support users moving at highway speeds where signals are subject to a form of interference known as Rayleigh fading. Another factor is that smaller distances result in much better signal-to-noise ratios. All these factors in combination allow much higher throughputs.

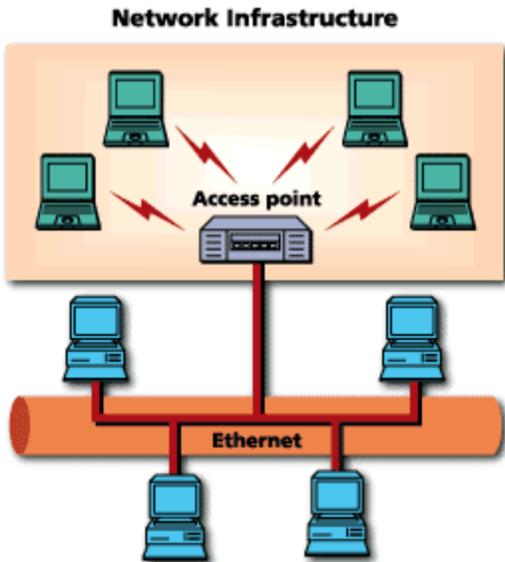
The higher throughput of wireless LANs has the virtue of allowing you to use existing network operating systems and applications (e.g., file and printer sharing, database access) compared to the modem-like applications for wireless WANs. And unlike wireless WANs, which are mostly operated by public carriers with usage fees, you get to buy and operate your own network. This gives you control of the whole network, but leaves you responsible for its proper installation and functioning. Fortunately, wireless LAN technology is well past its infancy and is ready to meld into your organization as a reliable subsystem. And the radio bands used by nearly all wireless LANs let you deploy networks without obtaining a license.

In this section, we delve into the different topologies available: spread spectrum, which is the most common RF technology used today (the two types of spread spectrum include direct sequence and frequency hopping); a low-power, narrowband approach that enables higher speeds; HiperLAN, which is a European standard; and infrared approaches.

### *Topologies*

The term wireless is actually somewhat misleading, since most wireless LANs interconnect with wired networks. The bulk of the distance between a wireless node and another node may well be over wires or fiber. Nevertheless, it is possible to build a network that is completely wireless. In such an instance, the physical size of the network is determined by the maximum reliable propagation range of the radio signals. Networks such as these are referred to as ad hoc networks, and are well suited for temporary situations such as meetings, conferences and sporting events.

It is more likely that you will install what is called an infrastructure network, where your wireless LAN connects to an existing wired LAN. In this instance you will need an access point that effectively bridges wireless LAN traffic onto your LAN. This function may be handled by software in a workstation that houses both a wireless card and a wired (e.g., Ethernet) card. But most wireless LAN vendors recommend dedicated hardware called an access point for this function. The access point can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



### *Spread Spectrum*

Most wireless LANs today use spread spectrum technology, not because spread spectrum is the best radio technology for wireless LANs but more as a result of FCC rules (Federal Code of Regulations 15.247) that allow for unlicensed operation in a number of radio bands, including 902 to 928 MHz, 2.400 to 2.483 GHz and 5.725 to 5.85 GHz. These are the industrial, scientific and medical (ISM) bands where unlicensed users are "secondary users" of the band and must not interfere with licensed primary users. Fortunately such interference has not been an issue because wireless nodes are restricted to 1 watt of power for transmissions and because the nature of spread spectrum is that it appears as noise to all but intended receivers.

Nevertheless, as a user of wireless LAN technology you need to be aware that primary users of the spectrum are not restricted to 1 W of transmission and could potentially interfere with your network. Moreover, companies are finding more and more use for the ISM bands, including wireless speakers and cordless telephones. The Metricom Ricochet network for instance, uses the 900-MHz ISM band. Will you experience interference problems using spread spectrum? Probably not, but you may want to think twice before using wireless LANs for mission-critical or life-and-death applications.

In today's market, the 900-MHz ISM band best serves consumer products, while the 2.4-GHz band best serves midrange performing wireless LANs (1 to 3 Mbps) and the 5.7-GHz band best serves higher-performance wireless LANs (5 to 10 Mbps). The 2.4-GHz band has the advantage of being available for unlicensed use in some European countries and Japan, and is the band where most new wireless LAN products operate today. As to coverage, spread spectrum usually operates over a typical range of about 100 meters and coverage areas ranging from 5,000 to 25,000 square meters (50,000 to 250,000 square feet).

Spread spectrum was developed by the U.S. military as a robust radio technology that is both difficult to jam and to eavesdrop on. It works by spreading a signal that would normally occupy a

certain amount of spectrum over a much broader amount of spectrum. There are two forms of spread spectrum: frequency hopping and direct sequence. Both are allowed by FCC rules.

In frequency hopping, the signal dwells momentarily on one frequency, then hops to another, then another in a pseudorandom sequence that eventually repeats itself. A receiver must hop at exactly the same time to exactly the right frequency to be able to receive the signal. FCC rules require that the band be divided into a certain number of frequencies and that the hopper must use a certain number of these frequencies.

Direct sequence is very different. Each "one" in the binary data is converted to a sequence of predetermined ones and zeroes and each "zero" is converted to the inverted sequence. The binary data in the sequences are referred to as chips, and the ratio of chips to original bits is referred to as the spreading ratio, or gain, of the system. FCC rules require a minimum spreading ratio or gain.

Some wireless LANs are based on frequency hopping, some on direct sequence. Direct sequence allows higher throughputs, although such designs may cost more and use more power. There is almost a holy war about which type of spread spectrum is better, though mobile designs today tend to use frequency hopping. You should choose your network based on features and price, and not on which spread spectrum technology it uses.

### *Low-Power Narrowband*

An alternative approach to spread spectrum that some wireless LAN vendors are using is to transmit narrowband signals at low-power levels, a method allowed by FCC CFR 15.249 rules. By transmitting at low-power levels, vendors do not have to use spread spectrum, which gives them the ability operate at higher data rates. RadioLAN's product uses this approach and operates at 10 Mbps in the 5.8-GHz band with 50 milliwatts (mW) of peak transmission power. The price of this higher performance is a reduced transmission range of about 30 meters (100 feet) in an office environment.

### *HiperLAN*

HiperLAN, an abbreviation for Higher Performance Radio LAN, is a wireless technology standard developed by the European Telecommunications Standards Institute. It boasts very impressive capabilities, including a data rate of about 24 Mbps using a channel width of 23.5 MHz. In Europe, spectrum is available in the 5.15 to 5.3 GHz range, allowing for five separate channels. This type of throughput readily supports multimedia applications. Unfortunately, no commercial products are yet available. But the technology is under consideration for new spectrum in the United States in the 5-GHz band as part of the U.S. Unlicensed National Information Infrastructure band.

### *Infrared LANs*

An alternative approach to radio-based wireless LANs is infrared communications. Infrared networking uses electromagnetic radiation with wavelengths of 820 to 890 nanometers,

corresponding to a frequency of about 350,000 GHz. The advantages of IR include no need for licenses, no safety issues, huge potential capacity and good control of interference. IR does not penetrate walls, so infrared LANs must be contained in a room. Note that IR LANs generally do not operate in outdoor areas where there is sunlight. IR transmitters and receivers can be designed either for directional use or for diffuse use, where signals bounce off walls and other objects to reach the receiver. In fact, IR is specified as one of the physical layer options in the new IEEE 802.11 standard.

Though it is a promising technology, there are relatively few IR LAN products available today. But one type of infrared technology that has been broadly deployed is the use of IR for short point-to-point connections following standards specified by the Infrared Data Association.

### *Infrared Data Association (IRDA)*

The Infrared Data Association is a consortium of vendors that has defined low-cost IR communications characterized by:

- Directional point-to-point communications of up to one meter
- 115-Kbps and 4-Mbps connectivity
- Walk-up ad hoc connectivity for LAN access, printer access, and portable computer to portable computer communications

Many laptops today include IRDA ports, though devices such as LAN access points and printers with IR capability are not yet very common. The IRDA estimates some 60 million IRDA ports in the market.

### *Unlicensed PCS*

When allocating spectrums for Personal Communications Service, the FCC included some bands for what is called unlicensed PCS: 1910 to 1920 MHz and 2390 to 2400 MHz were reserved for data and 1920 to 1930 MHz for voice. Unfortunately, restrictions on the use of this spectrum have limited its usefulness for wireless data to the extent that no product offerings are yet available.

## **Understanding Wireless LANs**

Before you deploy wireless LANs, it helps to understand how they work. Wireless LANs operate in almost the same way as wired LANs, using the same networking protocols and supporting the most of the same applications. But they have some fundamental differences:

- While they use the same networking protocols, they use specialized physical and datalink protocols;
- They integrate into existing networks through access points which provide a bridging function;
- They let you stay connected as you roam from one coverage area to another;
- They have unique security considerations;

- They have specific interoperability requirements;
- They require different hardware;
- They offer performance that differs from wired LANs.

We will study each of these topics in detail, as well as the IEEE 802.11 standard, how to go about deploying a wireless LAN, and the use of unlicensed wireless links to bridge networks together.

### *Physical and Link Layers*

In looking at a typical wireless LAN protocol stack diagram, we see that from the network layer up, wireless LANs use the same protocol stack as wired LANs. But what about at the lower layers?

At the physical layer, the wireless network interface card takes frames of data from the link layer, scrambles the data in a predetermined way, then uses the modified data stream to modulate a radio carrier signal. At the link layer, a key function is to control access to the medium. Unlike Ethernet networks, which are carrier-sense-multiple-access with *collision detect* (CSMA/CD), most wireless LANs are carriers-sense-multiple-access with *collision avoidance* (CSMA/CA). Once a node starts sending data, it cannot detect whether another station is also transmitting and so senders rely on a positive acknowledgment from the receiver to indicate that no interference occurred during the transmission. This makes wireless LANs less efficient than wired LANs under heavy loading. You should test your network under typical loading conditions.

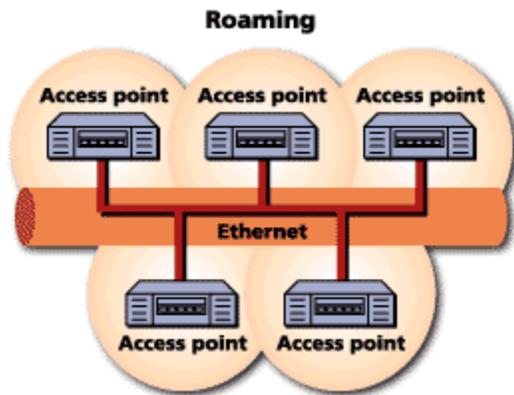
### *Integration With Existing Networks*

While you can operate a wireless LAN as a standalone network, chances are you will want to connect it to your wired infrastructure. This is easily accomplished by using a wireless access point, a small device that bridges wireless traffic to your network. The wireless LAN then appears as one network segment in your overall network. Today you usually need to purchase the access point from the same vendor as the wireless NIC, though with standards such as IEEE 802.11 and industry interoperability initiatives such as the Wireless LAN Interoperability Forum, you will have increasing options to combine equipment from different vendors. Most access points bridge wireless LANs into Ethernet networks, but Token-Ring options are often available as well.

### *Roaming*

In many wireless LAN applications, you would like users to maintain a continuous connection as they roam from one physical area to another. In doing so, they may well move from the coverage of one access point to another. Nearly all wireless LAN vendors support this kind of roaming through a process by which the mobile nodes automatically register with the new access point. What you will need to consider in your network planning is how your infrastructure network is divided into subnets. If one access point is on one subnet and another access point is on another subnet, traffic will have to cross a router, something that most wireless LAN vendors currently do not support. The two possible solutions are:

- Connect all access points back to one subnet, which might require extra cabling.
- Use Mobile IP your network protocol is IP, as we discuss further below.



Sine the IEEE 802.11 standard does not address roaming, you may need to purchase equipment from one vendor if your users need to roam from one access point to another.

### *Security*

The thought of radio waves propagating in all directions from your network may concern you. Fortunately most wireless LANs provide a number of effective security measures. First of all, spread spectrum radio signals are inherently difficult to decipher without knowing the exact hopping sequences or direct sequence codes used. This at least keeps honest people honest. To protect you against truly determined intruders, most wireless LAN products also offer optional encryption mechanisms. Also, the IEEE 802.11 standard specifies optional security called "Wired Equivalent Privacy," whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN. The standard also specifies optional authentication measures.

### *Interoperability*

Before the IEEE 802.11 specification, the only interoperability between wireless NICs and access points occurred when vendors worked cooperatively. One such effort is The Wireless LAN Interoperability Forum (WLIF), which was formed by a number of wireless LAN vendors to address interoperability issues. WLIF has published protocol specifications based on Proxim's airlink and also performs certification testing. A number of vendors are also working together to create what is called the Inter-Access Point Protocol (IAPP), which defines how access points communicate with each other.

Though IEEE 802.11 lends legitimacy to the industry, by itself it does not guarantee interoperability, since it only standardizes the physical and medium access control layers. The standard does not address issues of roaming or communications between access points which is required for handoffs. And vendors must still work with each other to ensure their IEEE 802.11 implementations interoperate. You should ask your potential vendors which products they work with, regardless of what standards they meet. Also, you should do your own verification testing if you plan on using products from multiple vendors.

## *Hardware*

Wireless LAN hardware typically comes in the following physical forms:

- PC Card, type 2 format, either with integral antenna which is becoming the norm or with tethered antenna/RF module.
- ISA Card with external antenna connected by cable.
- Handheld terminals with integrated radios for vertical market applications such as warehousing.
- Access points that are standalone devices about the size of a hardcover book.

Costs range from \$300 to \$800 for network cards, with access points costing \$1,500 or more. Wireless bridges that link wired LANs together range from \$2,000 to as high as \$10,000 per node depending on performance.

## *Performance*

The quoted throughputs of commercially available wireless LANs range from 1 Mbps to 10 Mbps. See the following table for examples of throughput:

| <b>TYPE OF WIRELESS LAN</b>   | <b>QUOTED DATA THROUGHPUT</b> |
|---|-------------------------------|
| IEEE 802.11 standard  | 1 Mbps or 2 Mbps              |
| Open Air Interface as specified by the Wireless LAN Interoperability Forum (based on Proxim frequency-hopping spread-spectrum technology) | 1.6 Mbps                      |
| WaveLAN (Lucent Technologies) and Aironet direct-sequence spread-spectrum products  | 2.0 Mbps                      |
| WinData   | 5.7 Mbps                      |
| RadioLAN  | 10 Mbps                       |
| HiperLAN standard (no commercial products)  | 24 Mbps                       |

You need to be careful with quoted throughputs since they represent best case throughputs. Wireless LANs experience higher error rates than wired LANs, resulting in retransmission of frames. Furthermore, as discussed above in [Physical and Link Layers](#), the collision avoidance mechanism is not as efficient as collision detection used in Ethernet, especially with a large number of users. Based on various tests, you can expect actual throughput for your application to be about half the quoted "over-the-air" throughput. Note also that there is a trade-off between throughput and distance. Higher data rates come at the expense of lower maximum distances for reliable operation, which is why many products offer a choice of throughput speeds.

## *The IEEE 802.11 Standard*

Finally released in 1997 after nearly seven years of development, the IEEE 802.11 standard specifies physical layer and medium access control (MAC) protocols. The MAC constitutes the lower half of the datalink layer in the OSI network model. 802.11 was designed so that to upper levels the network behaves like a standard wired network. To accomplish this the link layer engages in error correcting functions that are not usually employed at the link layer in wired LANs.

At the physical layer, 802.11 specifies use of the 2.4-GHz ISM band with both frequency-hopping and direct-sequence spread-spectrum at 1 Mbps with optional 2-Mbps throughput. Power can range from 10 mW to 1 watt. In trying to accommodate every possible variation in technology, the standard specifies an IR physical layer as well.

At the datalink layer, 802.11 specifies a MAC protocol based on carrier-sense-multiple-access with collision avoidance and an optional request-to-send and clear-to-send mechanism that allows longer uninterrupted transmissions. The standard also provides for optional time-bounded services such as voice and video communications by allowing access points to control communications using polling methods.

The 802.11 standard is an important milestone for the industry and will provide a degree of interoperability, but it is not essential that you use 802.11-compliant equipment for a number of reasons:

- You may be comfortable purchasing all your equipment from one vendor.
- Many vendors already provide interoperable equipment.
- 802.11 only specifies 1-Mbps and 2-Mbps throughput. You may need a wireless LAN that operates at higher speeds.

### *Deploying Wireless LANs*

Deploying a wireless LAN is relatively straightforward. At the wireless nodes you must install the wireless network card as well as the appropriate software drivers which your network protocol stacks use to access the wireless card. These drivers come with the card.

The difficult part is knowing where to install your access points. The first step is to define exactly where you want coverage, which requires a site survey. Wireless signals can penetrate walls, sometimes several walls, but how well they do so depends on how the building was constructed. You will need to verify that you have coverage where you want it. Different vendors provide different tools to do this, but one approach is to use two portable computers with wireless hardware operating on a point-to-point basis. Using diagnostic software provided by the vendor, you can determine a coverage area for a potential access point by keeping one portable computer fixed and moving around with the other. Check with your vendors as to what tools they provide and what approach they recommend for deploying their access points.

### *Bridging Networks With Unlicensed Wireless Links*

Wireless LAN technology is also used for bridging conventional wired networks together, which can be particularly useful if two sites have a line of sight with each other and the only wired bridging option involves monthly services charges to a telco or other network provider. Many wireless LAN vendors offer bridging products based on the same spread-spectrum technology as their wireless LANs. Using these is quite straightforward. First you need to determine whether to use omnidirectional antennas, effective to about 100 meters, or directed antennas for greater range. These directed antennas can easily cover distances of over a kilometer and with amplification (which is now allowed under recently relaxed FCC rules) can reach as far as 40 kilometers (25 miles).

Specified throughputs range from 1 Mbps to 10 Mbps, depending on the product offering and price. Actual throughput will be less. Testing of 10-Mbps bridges by Network Computing showed throughputs of just over 5 Mbps. After taking into account range and throughput, consider any other bridging requirements you may have, such as support for routing and for specific protocols.

## **Making Network Software and Applications Work**

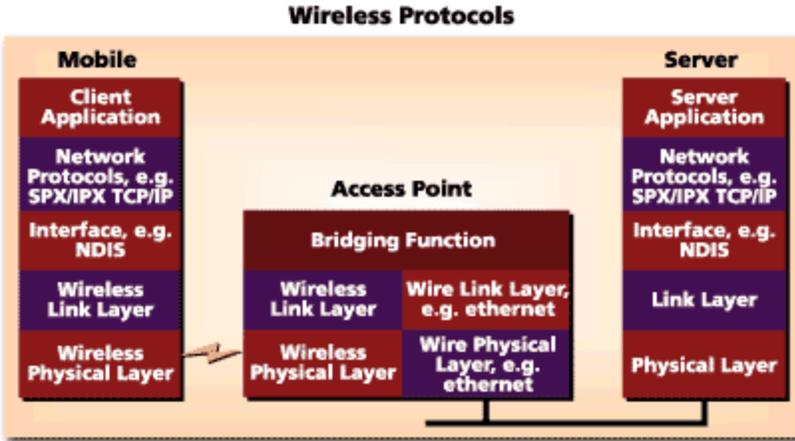
So we now know how wireless LANs work and how they interconnect with other networks. But what is involved in making network systems and applications work? Fortunately this is straightforward. In this section we look at the protocol stacks involved, where Mobile IP might make sense and how to configure applications for optimal performance.

### *Protocol Stacks*

We have already discussed how wireless LANs use physical and datalink layer protocols that are specialized for the finicky wireless environment. But from the network layer up, traditional networking protocols function with no modification required. This means that virtually all mainstream networking systems are supported, including:

- TCP/IP
- SPX/IPX (Novell)
- NetBEUI (Microsoft Windows for Workgroups, LAN Manager, Windows NT, Windows 95)
- LANtastic (Artisoft)
- Pathworks (DEC)

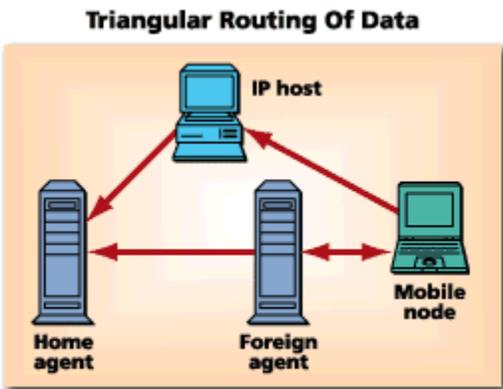
Actual protocols supported will depend on the specific vendor. The approach vendors take to support networking is the same as for wired LANs. When you purchase an Ethernet card, it comes with software drivers such as NDIS (Network Device Interface Specification from Microsoft) and ODI (Open Datalink Interface from Novell). The same applies to wireless cards. By installing the appropriate wireless driver, your network stack will not even know it is using a wireless connection, nor will your applications. However, mobility can sometimes complicate IP-based networking, so you may wish to look at Mobile IP.



*Mobile IP*

If your roaming wireless users sit down, turn on their portable computers, establish a wireless networking session, conduct their business, log off and then turn off their machines, mobility may not be an issue, especially if the users obtain IP addresses dynamically using Dynamic Host Control Protocol (DHCP).

But if IP network users keep their machines on, perhaps use handheld computers and wander from one area to another, they may ultimately connect with an access point that is connected to a different subnet. Because IP addresses by design refer to a particular subnet, IP traffic will not be able to find its way to the new location. This is where Mobile IP enters the picture. A recently completed Internet standard, RFC 2002, Mobile IP provides a mechanism by which hosts belong to a "home" network. When the host roams to a new network, it registers with its home agent. The home agent then intercepts traffic sent to the mobile node, encapsulates it in another IP packet, and forwards it to a foreign agent, a special node (installed in a workstation, router or a ccess point) which forwards the packets to the mobile node. Traffic originated by the mobile node can travel back directly and does not have to be sent via the home node, resulting in triangular routing of traffic.



*Application Configuration*

Almost any application that works over a wired LAN should work over a wireless LAN. The only thing you may want to do differently is to consider the size of applications and the speed of the network. If a user is operating on a 1-Mbps network and is loading a 5-Mbyte application from a file server, the application could take over a minute to load. It is usually better for users to have copies of frequently used applications, utilities and data files on their own hard drives rather than on file servers.

## **Propagating into the Future**

While we emphasize how to take advantage of wireless LANs today, it is worth noting some of the ongoing developments and what to expect over the next five years. This will give you a better idea of how wireless LANs might address your expanding needs, and whether you will be able to consider wireless LANs for other applications. There are a number of notable trends. One is that the performance of wireless LANs technology will keep increasing while costs will decrease. Another is that as wireless data usage grows, increasing amounts of spectrum will become available.

### *Higher Performance At Lower Cost*

Early wireless LANs of the late 1980s offered throughputs of about 250 Kbps. The next generation reached 1 Mbps and today rates of 10 Mbps are available, albeit with lower coverage range. While 1 Mbps to 2 Mbps can be considered the standard today (with some higher-speed exceptions), 10 Mbps will become standard over the next couple of years, especially as new technologies such as pulse position spread spectrum are deployed. Also, expect to soon start seeing HiperLAN products offering about 24 Mbps. And standards work is already under way with HiperLAN and a wireless version of ATM to extend speeds to 155 Mbps, though affordable products at such higher data rates probably will not be available for another five years.

Also, expect to see prices dropping, with 802.11 adapters falling as low as \$200 in a couple of years. At these prices, wireless LANs could start competing with wired LANs for typical worker connectivity, and could start propelling wireless LANs into horizontal markets.

### *New Spectrum Options*

Improvements in technology have allowed radio communications to take advantage of higher frequencies. Wireless LANs that originally operated at 900 MHz have migrated to the 2.4-GHz band. And now an increasing number of products are using the even higher 5.7-GHz ISM band. The possibility of cost-effective products at 5 GHz prompted the FCC in 1997 to allocate 300 MHz for a new band it is calling the Unlicensed National Information Infrastructure (UNII). As with the ISM bands, users can operate without a license, but to encourage innovation and free market forces the FCC is imposing virtually no restrictions on how this band is used except for transmission power levels.

The UNII band, which spans from 5.15 to 5.35 GHz and 5.725 to 5.825 MHz, is more than twice all the spectrum allocated for PCS, which itself has spawned a massive expansion of the cellular telephone industry. The UNII band will provide a home for HiperLAN (which in Europe

operates at similar frequencies) and for new wireless LAN technologies that will undoubtedly evolve to take advantage of this spectrum.

Developments like UNII are representative of the overall trend. Microwave communications can now easily operate at frequencies as high as 40 GHz. Expect to see wireless LANs keep moving up in frequency and expect to see licensing bodies keep allocating additional spectrums at higher frequencies as market demand increases.

## **Vendor Information**

This section lists principal wireless LAN vendors and gives contact information. Since the emphasis is on companies providing LAN-oriented products, the list does not include companies that sell only wireless bridges or wireless point-to-point modems. Most of the listed vendors sell wireless cards, generally in ISA and PC Card format, and wireless access points. Some also sell wireless products for bridging LANs together. Many are in the process of introducing IEEE 802.11-compliant products.

### **Aironet Wireless Communications** , Fairlawn, OH

<http://www.aironet.com>

800-394-7353

330-664-7900

Primary Technology: Frequency hopping and direct sequence spread spectrum at 1 and 2 Mbps

### **AMP** , Harrisburg, PA

<http://www.amp.com/networking>

800-835-7240

Primary Technology: Frequency hopping spread spectrum

### **Breeze Wireless Communications** , Carlsbad, CA

<http://www.breezecom.com>

760-431-9880

Primary Technology: Frequency hopping spread spectrum at 2 and 3 Mbps

### **C-SPEC Corp.** , Dayton, OH

<http://www.c-spec.com>

800-462-7732

937-439-2882

Primary Technology: Direct sequence spread spectrum at 2 Mbps

### **Digital Equipment Corp.** , Hampton, MA

<http://www.networks.digital.com>

800-344-4825

Primary Technology: Direct sequence and frequency hopping spread spectrum at 2 Mbps

### **Digital Ocean** , Lenexa, KS

<http://www.digitalocean.com>

800-345-3474

Primary Technology: Direct sequence spread spectrum at 2 Mbps

**JVC Professional Computer Products Division** , Cypress, CA

<http://www.jvcinfo.com>

714-816-6500

Primary Technology: Directed infrared at 10 Mbps

**Lucent Technologies** , Parsippany, NJ

<http://www.wavelan.com>

800-928-3526

937-445-5970

Primary Technology: Direct sequence spread spectrum at 2 Mbps

**NetWave** , Pleasanton, CA

<http://www.netwave-wireless.com>

800-638-9283

510-737-1600

Primary Technology: Frequency hopping spread spectrum at 1 and 2 Mbps

**Proxim** , Mountain View, CA

<http://www.proxim.com>

800-229-1630

415-960-1630

Primary Technology: Frequency hopping spread sequence at 1.6 Mbps

**RadioLAN** , Sunnyvale, CA

<http://www.radiolan.com>

408-524-2600

Primary Technology: Narrowband at 10 Mbps

**Raytheon** , Andover, MA

<http://www.raytheon.com>

508-470-9011

Primary Technology: Frequency hopping spread sequence at 2 Mbps

**Spectrix** , Evanston, IL

<http://www.spectrixcorp.com>

847-317-1770

Primary Technology: Diffuse infrared at 4 Mbps

**Symbol Technologies** , Holtsville, NY

<http://www.symbol.com>

800-722-6234

516-738-5200

Primary Technology: Frequency hopping spread spectrum at 1 Mbps

**Wave Access** , Natick, MA

<http://www.waveaccess.com>

508-653-3646

Primary Technology: Frequency hopping spread spectrum at 3.2 Mbps

**WinData, Littleton** , MA

<http://www.windata.com>

800-553-8008

Primary Technology: Direct sequence spread spectrum at 5.7 Mbps

A good source of additional information is an industry association called the [Wireless LAN Alliance](#) .

*Peter Rysavy is the president of Rysavy & Associates, a consulting firm that works with both companies developing new communications technologies and those adopting them.*