FEATURE

Break Free With Wireless LANs

October 29, 2001, Network Computing
By Peter Rysavy

Wireless LAN use has reached critical mass, with offices, universities and homes, as well as public areas, such as airports, hotels and restaurants, getting in on the act. Some nonprofit organizations are even attempting to blanket entire metropolitan areas with free Internet access. All major notebook manufacturers offer wireless as an integrated option, and with PC vendors it's a standard check-box item. This acceptance comes because WLAN technology has reached a level of utility, stability, awareness, pricing and acceptance that makes it a powerful and straightforward networking option.

Cellular technology has long tantalized us with the potential of anywhere, anytime data access, but we see the broad deployment of WLAN access points ultimately delivering on this promise. Worried about throughput? If 11 Mbps isn't fast enough for you, 22 Mbps, 54 Mbps and even higher speeds will soon be available at little extra cost.

As attractive as the WLAN option is, however, IT managers must confront complex issues. One is how to deploy a network today that can be upgraded easily in the future. Another is security. A firewall costing thousands of dollars can be completely compromised by a single incorrectly configured access point, even when that access point is behind a brick wall. WLANs could also fall victim to their own success as multiple network standards, including Bluetooth, start to interfere with one another. There are also IP addressing issues, and locating access points across subnets makes it impossible to roam from one location to another without mobility middleware.

The good news is that solutions exist for most of these problems, and forthcoming standards will address many of today's limitations. WLAN technology is good today and will only get better, but to be successful in using it, you must carefully navigate through an evolving landscape.

Market Trends

There's no doubt that the WLAN market is booming. Worldwide sales of WLAN equipment increased by 80 percent last year, to more than $1 billion, and will approach $3.2 billion by the end of 2005, according to analysis firm IDC. Traditionally, WLANs have seen greatest acceptance in vertical markets, such as health care, inventory control and warehousing, where companies could justify high equipment and integration costs because the applications provide a clear ROI (return on investment). But in the past year, use has expanded into horizontal markets, including mainstream businesses, homes and educational environments.

Among mainstream enterprises, high-tech companies and those with lots of laptop users are leading the charge to wireless. For example, Microsoft has more than 2,000 access points serving upward of 10,000 WLAN users. Companies are deploying access points in meeting rooms, cafeterias and classrooms. Small companies are finding the technology cost-effective because they can set up shop in one location, often low-rent digs without network cabling, then easily move the

network into new offices as the company expands. Home users are getting into the act as well, sharing peripherals and broadband Internet connections--sometimes with their neighbors.

An increasing number of public WLANs are at airport gates and lounges, hotel meeting rooms, convention centers, and shopping malls, with MobileStar Network Corp. and Wayport the current market leaders in providing this access. What's exciting for users is being able to use the same notebook or PDA and wireless adapter at work, at home and while traveling.

Although build-outs are at an early stage, many market analysts argue that WLAN technology is better suited for public broadband connections in hot-spot zones, such as airports, than is current 3G (third-generation) cellular technology, which is still years away from widespread deployment. Lower infrastructure outlays and the use of unlicensed spectrum mean WLANs can deliver data at less than a tenth of the cost of cellular-based networks. The question for cellular operators is whether to embrace WLAN technology or try to compete against it.

Some European cellular providers, including Sonera Corp., of Finland, and Telia, of Sweden, offer WLAN service as an option to their mobile subscribers, but North American operators are as yet undecided. Why, you ask, would operators spend tens of billions of dollars to deploy 3G cellular networks when current cellular technology in combination with WLANs provides most of the same benefits at a fraction of the cost? The simple answer is that WLAN technology is not now on most operators' master plans, and it will not be added without a considerable amount of technical work, not to mention a readjustment of market vision.

WLAN products themselves are increasingly attractive. First, prices have come down dramatically over the past year, with PC Card formats finally breaking the magic $100 price barrier. Compare this with $500 per card several years ago. Access points used to cost $1,500, but now SOHO (small office/home office) gateways that integrate router functionality and firewalls can be had for as little as $200. Of course, you get what you pay for, and if you want an access point with roaming support, enhanced security features, good range and management functions, you will pay more.

Another important attraction of today's products is interoperability. Thanks to the efforts of the Wireless Ethernet Compatibility Alliance and its WiFi (Wireless Fidelity) certification, most cards will work with most access points, though mixing and matching access points from multiple vendors to support effective inter-access-point communication will require a forthcoming new standard (for a rundown of standards, see "Wireless LAN Standards," below).

Another crucial driver in this market, and one that gets little mention, is the matter of applications. By applications, we mean not only the NOS, such as Novell NetWare or NetBEUI, but also end-user applications, like Lotus Notes or Microsoft Exchange. When you must deliver applications to a cell phone, slow speeds, high network latency and high usage costs demand that you carefully configure your application or use wireless middleware or the services of a wireless ASP (application service provider). This often means you have to rebuild your application specifically for wireless. But with WLANs, thanks to high speeds and low usage costs, companies can use nearly all their existing networking applications without making any changes. The elusive killer application for wireless networks might just be any application.

There are some caveats, though. If you want to take advantage of public WLAN

service to access a private intranet, you should consider VPN software to protect your communications from eavesdroppers. And if you want to maintain an IP address across subnets or keep sessions alive as you drop in and out of coverage in an extended area, you will need the assistance of wireless middleware from the likes of NetMotion Wireless. But these are minor complications compared with the benefits of mobile broadband.

WIRELESS LAN STANDARDS

Standard	Status	What it defines
IEEE 802.11	Completed 1997	Original WLAN standard. Supports 1 Mbps to 2 Mbps.
IEEE 802.11a	Completed 1999	High-speed WLAN standard for 5-GHz band. Supports 54 Mbps.
IEEE 802.11b	Completed 1999	Current dominant WLAN standard. Supports 11 Mbps.
HiperLAN2	Completed 2000	Competing high-speed WLAN standard for 5-GHz band. Supports 54 Mbps.46
IEEE 802.1x	Completed 2001	Comprehensive security framework for all IEEE networks, including Ethernet and wireless.
IEEE 802.11g	Expected 2001	Alternate high-speed WLAN standard for 2.4-GHz band. Supports 20+ Mbps.
IEEE 802.11i	Expected 2001	Wireless-specific security functions that operate in combination with IEEE 802.1x.
IEEE 802.11e	Expected 2001	QoS mechanisms that support all the IEEE WLAN radio interfaces.
IEEE 802.11f	In process	Defines communication between access points.
IEEE 802.11h	In process	Defines spectrum-management techniques for 802.11a.
WISPR	Expected 2001	Wireless ISP Roaming. Recommendations by the Wireless Ethernet Compatibility Alliance on how to support roaming across multiple public WLAN networks.

One new application that could end up being a major driver for high-speed WLANs is video in homes. Today, digital set-top boxes are needed at each television where you want reception--an expensive proposition. A less costly approach is to have one box that receives the digital cable or digital satellite signal, and a WLAN that shunts multiple video streams to televisions throughout the house. This will be possible with new WLAN standards that provide the necessary speeds and QoS.

The market has also overwhelmingly accepted one wireless standard: IEEE 802.11b. At 11 Mbps, IEEE 802.11b provides sufficient speed for most applications, even though actual throughput is only about 6 Mbps, and a busy 802.11b network degrades much faster than wired Ethernet because of a less efficient medium-access protocol. IEEE 802.11b is making serious inroads to the home environment as well, so the fate of the home-oriented HomeRF (Home Radio Frequency) specification has become quite uncertain, especially with one of HomeRF's major initial backers, Intel, defecting to IEEE 802.11b.

However, you should watch standards development most closely. IEEE 802.11b launched the industry, but widespread usage has exposed security flaws that are addressed only by vendor-specific solutions. Keeping track of these developments and designing a network with which you can easily migrate to improved technology is the crux of WLAN deployment today.

Technology and Standards Developments

Vendors and standards groups are advancing WLAN technology on three broad fronts: higher speeds, improved security and QoS. In an ideal world, one new standard would encompass these improvements. When a vendor's products support these improvements, you could just upgrade its equipment, and everything would be backward compatible. But this world does not exist, and advancements will occur in stages.

With respect to speed, there are exciting new developments. The IEEE 802.11a standard (which was started before the IEEE 802.11b standard) specifies a new physical layer that runs at a raw data rate of 54 Mbps. Although maximum user throughput is likely to be 25 Mbps to 30 Mbps, this is still a fivefold increase over IEEE 802.11b--almost like going to Fast Ethernet from conventional Ethernet.

IEEE 802.11a uses an advanced radio technique called OFDM (Orthogonal Frequency Division Multiplexing). Instead of sending data bits sequentially at a very high data rate, OFDM sends multiple data streams in parallel over separate radio carrier signals. This results in a more robust radio signal that makes high bandwidth communications practical. In fact, many next-generation wireless systems, including fixed and mobile wide-area systems, are based on OFDM.

In addition, the radio can dynamically employ different modulation methods based on the quality and strength of the radio signal, resulting in extremely high throughput at shorter ranges and lower but reliable communications at higher ranges. And whereas IEEE 802.11b uses the increasingly congested 2.4-GHz radio band, IEEE 802.11a operates in the less congested 5-GHz unlicensed band, which has more than three times the available spectrum (300 MHz vs. 80 MHz). However, there is no long-term protection against interference in the 5-GHz band either.

Atheros Communications has been aggressively developing and promoting the benefits of 802.11a technology. Atheros shipped chipsets this summer, and we expect a raft of WLAN products using these chips to appear by year's end. With aggressive pricing on these chipsets, building an 802.11a product should cost no more than making an 802.11b device. So why not just wait for 802.11a?

The answer is complex. First, there is the question of range. The laws of physics dictate that the range of free-space radio communications decreases with higher frequencies, but indoor propagation differs from free space because of absorption and reflections. Moreover, power transmit levels and the type of modulation used also affect range. The result is that it is hard to accurately predict in advance the range of any particular radio technology.

According to Mobilian Corp., a manufacturer of both IEEE 802.11b and IEEE 802.11a components, up to four times as many access points are needed to cover an area with 802.11a than an area with 802.11b. However, recent "real-world" testing by Atheros in office environments indicates otherwise. Atheros claims that, as long as you place access points in close proximity, about 60 to 80 feet from one another, you can readily overlay an 802.11a network on an 802.11b network. For the full 54-Mbps speed of 802.11a, range is restricted to about 50 feet; at 100 feet, throughput drops to 36 Mbps; and at 200 feet, 6 Mbps. Keep in mind that actual user throughput is about half of these link rates.

Although throughput drops off with range, according to Atheros and other vendors, it remains higher with 802.11a than with 802.11b. However, until 802.11a products are available and more testing is done and publicized, laying an 802.11a network over an

802.11b network will remain a complicated issue and will likely not be just a matter of swapping a radio card in a dual-slot access point. Fortunately, being able to power access points using their Ethernet connections does ease the redeployment burden.

There is another issue, though: backward compatibility. While 802.11a and 802.11b employ different radio bands, many initial network cards will support only 802.11a. Dual-mode cards will also become available but will cost more for some time because separate chips are required. With 802.11b so widely entrenched, initial 802.11a deployments will constitute small islands of coverage, making the upgrade hard to justify for many users.

Entrenched 802.11b vendors also are not rushing out with 802.11a products, and many of the initial 802.11a vendors are secondary players looking to gain market footing. Still, higher speeds are inevitable, for the increased bandwidth support not only offers higher throughput but supports a larger number of users, something that will quickly become an issue as the popularity of the technology increases.

IEEE 802.11a is not the only high-speed option, either. The European Telecommunications Standards Institute, or ETSI, has developed a family of high-speed wireless standards, with HiperLAN2 a direct competitor to 802.11a. HiperLAN2 uses the same physical layer as 802.11a, including OFDM and operation in the 5-GHz band, but it differs at upper layers. Whereas 802.11a is based on CSMA (carrier sense multiple access), HiperLAN2 centrally coordinates access, dynamically assigning time slots to individual mobile stations. This deterministic approach (analogous to token ring) is more complicated but provides for QoS--currently missing in 802.11a--and makes HiperLAN2 a more seamless extension of ATM networks.

For IP-based applications, however, the two standards offer comparable capabilities. So will we have to live with two standards? Perhaps, but IEEE 802.11a has greater momentum, with more companies developing components and with end-user products closer on the horizon. And, as we'll see in a moment, QoS is coming to 802.11 networks as well. Another factor is regulations: European regulations governing interference management favor HiperLAN, but standards work under way by the IEEE (802.11h) will address this as well.

To complicate matters further, the IEEE is developing another high-speed standard, 802.11g, which has a peak rate of more than 20 Mbps. This standard will likely use OFDM. Although not directly backward compatible with 802.11b, 802.11g does operate in the same radio band as 802.11b, and vendors will be able to offer cards that support 802.11b and 802.11g, possibly simplifying network upgrades. But if 802.11a products start rolling out, 802.11g could be too little, too late.

What is not yet clear is what vendors will do to facilitate the upgrading of access points to higher speeds. Those with modular radios (such as PC Card format) will be easier to upgrade than those with integrated radios. For example, dual-slot access points from Enterasys Networks and Intermec Technologies Corp. will support 802.11a and 802.11b simultaneously, though the potential difference in range remains an issue. An alternative approach will be to lay an 802.11a (or 802.11g) network over an 802.11b network and have the two operate independently. This may be simpler but won't be the most efficient tactic in terms of infrastructure. If you expect to consider this approach in the future, make sure you run two Ethernet ports to each access-point location today.

Stay Safe

Although speed gets everybody's attention, it is actually new security features that may bring us greater peace of mind. The current IEEE 802.11 security method, called WEP (Wired Equivalent Privacy), employs either 40-bit or 128-bit encryption using the RC4 algorithm. Unfortunately, WEP has serious security holes and relies on manual key distribution.

To address these shortcomings, the IEEE is developing a new security architecture, specified by IEEE 802.1x, that can be applied to all IEEE access networks, including wireless (at any speed) and wired networks. This architecture provides a framework for authentication, encryption, message integrity and key distribution, and is designed to work in conjunction with existing security standards, such as EAP (Extensible Authentication Protocol) and RADIUS (Remote Access Dial-in User Service).

Another new standard, IEEE 802.11i, specifies how security is specifically implemented in wireless networks, including 802.11b and 802.11a. With solid backing by key players, such as Cisco Systems and Microsoft, and standards close to completion, expect products to start supporting these new security standards as early as next year.

Microsoft Windows XP, for example, supports 802.1x and EAP. One result: A single user logon can be used for both the wireless and the infrastructure networks. Taking advantage of these new wireless security features will mean more integration work, but this is far better than the current approach of no security at all. Of course, these security standards are only now approaching completion; it may be some time before vendors support them, and there is the big question of interoperability.

The final major push is QoS, with yet another standard, IEEE 802.11e. This standard provides for both asynchronous data traffic and data traffic that is time controlled, such as voice or video. It also allows each traffic stream to employ different policies. For example, a video stream that is time sensitive could employ forward error correction instead of packet retransmission. IEEE 802.11e--for QoS--in conjunction with IEEE 802.11a--for speed--will match HiperLAN2's capabilities.

QoS is an essential capability for voice and video support, but these mechanisms will need to be integrated with QoS mechanisms in infrastructure networks at large, and this will take some time. So while exciting, it may be years before applications in corporate environments can truly take advantage of this capability. Home use of integrated voice/video/data networks will happen much faster. However, there is no reason to wait for these more exotic features: Today's products offer more than sufficient capabilities for many applications. And as long as you put some hard questions to your vendors about their upgrade paths, you can safely deploy a network that you can enhance as needed over time.

Executive Summary

Wireless LANs

Want to be a hero? Remember those users who just yesterday were bitching and moaning that you deleted their MP3 files from the server? What would they say about always-on wireless Internet access, not just at the office but when they telecommute? At the very least, you'll never again get stiffed when it's time to pay for lunch.

Although the payoffs are alluring, building a WLAN (wireless LAN) is still a formidable task, even in a controlled environment. Will it be fast enough? How about QoS (Quality of Service)? Should you go with 802.11b, hold out for speedier 802.11a, or mix and match? Can users roam without their sessions dropping? What about hackers sitting in your parking lot sifting through Ethernet packets? Don't fret. We walk you through the history and current state of WLAN technology, lay out the standards currently on the table and offer tips to build a WLAN that will serve you well today and in the future.

Once employees get a taste of wireless, they'll want it everywhere. We recommend you take a proactive approach and select a wireless gateway for your telecommuting users. That way you'll be able to standardize on a device that will best suit your company's security, throughput and configuration needs, and will let you offer helpdesk support. To help you make an informed purchasing decision, we gathered 11 devices from 10 vendors for our largest head-to-head review of SOHO (small office/home office) wireless gateways, defined as products that integrate NAT (Network Address Translation) routing capabilities with wireless access points. Some also offer 10/100 Ethernet switching and a parallel port for sharing peripherals. How much for all this? Retail pricing hovers around $300, but street pricing is more like $200. That's dirt cheap for the benefits provided. In fact, we gave MaxGate's UGate 3300 Cable/xDSL device our Best Value award. This inexpensive gateway finished a close second overall to Nexland's WaveBase, our Editor's Choice.

Finally, we address the state of MMDS, or multipoint multichannel distribution system. Also known as wireless DSL, MMDS is a broadband wireless technology that has the potential to bring broadband access to users outside DSL coverage areas--a single MMDS hub can serve a radius of up to 35 miles, compared with 18,000 feet from the central office for DSL. The only drawback is the availability of spectrum.