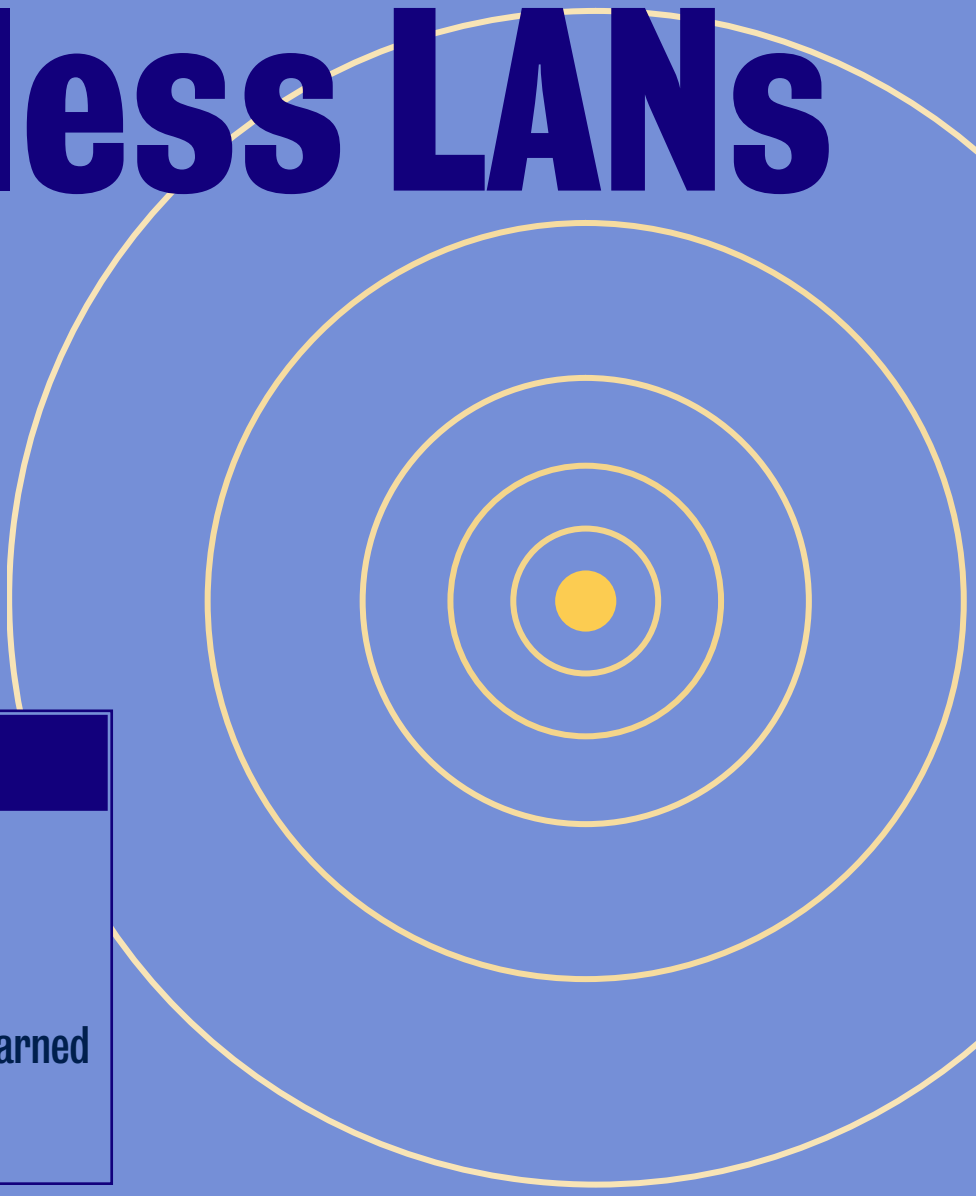
SPECIAL REPORT

A guide to Wireless LANs



Contents

Sponsored Exclusively By:

intel

Produced By:

NetworkWorld

www.nwfusion.com

Wi-Fi world

What if wireless Ethernet becomes as ubiquitous as cell service?

BY JOANIE WEXLER

Gwenn fires up her laptop at the breakfast table and, through the wireless Wi-Fi Ethernet link in her house, logs on to the corporate VPN to check her e-mail before leaving for the airport. She'll get coffee at Starbucks, which has a public Wi-Fi service, and she figures she can run the numbers her boss is asking for and send them from there.

At the airport she logs on one last time before boarding the plane, downloads the PowerPoint slides she'll need for her presentation and double-checks the timing for the videoconference she intends to include in the presentation once she has a Wi-Fi link set up at the conference center in San Jose.

Welcome to the Wi-Fi reality waiting around the corner. Wireless LAN services are popping up in so-called "hot spots" across the country — airports, hotels, restaurants, cafés and convention centers.

There are already a few thousand Wi-Fi-enabled locations worldwide, says Amy Cravens, an industry analyst at Cahners In-Stat. That's enough to whet user's appetites, but the number "won't really take off until most corporate environments have wireless LANs," she says.

However, the industry faces some serious issues that may stymie ubiquitous service, including:

*Fragmentation among wireless LAN services. The services today are offered primarily by little-known wireless ISPs such as AirPath, Concourse Communications, Surf and Sip, and Wayport.

*Lack of roaming agreements. The wireless ISPs only offer islands of wireless LAN connectivity.

*Unproven business models. After Wi-Fi enabling several hundred Starbucks locations and other properties, MobileStar Network filed for bankruptcy late last year and sold its assets to VoiceStream. It is unclear how partners in Wi-Fi services can make money.

"The state of the hot-spot supply chain is a nightmare right now," says Ian Keene, vice president and chief analyst in the telecom practice at Gartner. "The business model was straightforward until last year. Then the property owners woke up and wanted control — and a share of the revenue."

Nonetheless, there is a Wi-Fi ground swell that is hard to mistake.

Wi-Fi drivers

As wireless LANs grow within corporations, the desire to extend support follows naturally. Cahners estimates that the number of 802.11-based access points shipped each year will nearly triple from 1.2 million in 2001 to 3.5 million in 2005. The firm expects yearly 802.11 network interface card (NIC) shipments to jump from 6.3 million last year to 19.4 million in 2005.

In fact, most of the major notebook computer makers ship products today with embedded 802.11 NICs. Combine that with the fact that Microsoft has embedded Wi-Fi capabilities into Windows XP and it is clear that, like it or not, there is a Wi-Fi user base growing up around you.

The XP operating system automatically searches for a Wi-Fi access point and, if it finds one, asks the user if he would like to use the service. "We had users signing up for our service before it was even announced," says Tim Barrett, vice president of AirPath.

Wi-Fi support can indeed draw business. Mark Hedley, CTO at hotelier Wyndham International, based in Dallas, says his company is "most certainly taking conference business away from other hotels" thanks to the 802.11 connectivity in 148 of its properties.

Wireless provider Wayport ate the up-front capital costs, Hedley says. "You won't likely see much more of that in the wake of the dot-com demise. At the time, everyone expected a 20% consumption rate, but it's actually been more like 2% to 4%."

Unified roaming

The biggest challenge for users now is lack of unified roaming. Users must subscribe to individual wireless ISPs in each area they frequent, making it not only inconvenient but also difficult for the corporate network group to track usage and billing.

The industry is trying to standardize a settlement process through which carriers would sort out who gets paid when a customer roams from one service area to another.

In the meantime, aggregators and clearinghouses are stepping in. They partner with multiple wireless LAN service providers, aggregate the players' networks to create a merged footprint and put a common brand on the services.

Wireless ISP aggregator Boingo, which launched its services in January, is "partnering with every Wi-Fi [wireless] ISP we can find to build out our network," says Christian Gunning, director of product management. "It is cost-prohibitive for a single carrier to be ubiquitous. But having a patchwork of [Wi-Fi] locations and different ways to authenticate themselves and log on is confusing and difficult for users."

Longtime IP remote-access players iPass and Gric — which aggregate and broker worldwide dial-up IP services — also have begun expanding their services to include wireless LAN offerings.

And where are the traditional carriers, ISPs and mobile network operators in all this? They're remaining mum, for the most part.

Even VoiceStream, the company that purchased MobileStar's assets, will only say that the 500 Starbucks stores and American Airlines Admirals Clubs that MobileStar serves remain connected — for now. A spokeswoman says it is too early to predict where VoiceStream will take its public Wi-Fi business next.

But word on the street is the big-name traditional carriers — including the likes of AT&T, WorldCom and Sprint — have something up their sleeves.

Wireless LAN equipment supplier Cisco says all the major carriers are looking at delivering wireless ISP services.

"We haven't announced formal relationships with any, but we are working with them all," says Kristine Stewart, director of market development in Cisco's worldwide marketing group.

That's one hint that, before you know it, your company's user population will be chanting for Wi-Fi support.

Wexler, a writer in Campbell, Calif., is author of Network World's "Wireless in the Enterprise" e-newsletter — joanie@jwexler.com.

Wi-Fi guide

A practical guide to deploying wireless Ethernet

BY JOHN COX

Wi-Fi wireless LANs are deceptively easy to install. In fact, you might already have some.

"Users are installing these on their own," says Guy Denton, executive principal with IBM's Global Center of Competency. "We do security audits and find numerous wireless access points that the company knows nothing about."

The simplicity, however, masks an array of critical issues. "We often get called into projects after the fact," when clients run into unexpected problems, says Joe Musgrave, vice president with Signa Services, a wireless LAN consulting company in Erlanger, Ky. Users who aren't getting the bandwidth they expected, for example, might add more access points only to see bandwidth plummet.

Rolling out Wi-Fi LANs — products that meet interoperability tests spelled out by the Wireless Ethernet Compatibility Association — requires careful planning, a thorough security analysis, in-depth network design, and knowledge of products and evolving standards.

Easy? Well, not if you want to do it right.

Initial requirements

Presuming there is a call to add wireless support — workers that want to bring laptops to conference rooms, the cafeteria or other offices, for example — a good place to start is your local wired network, says E.J. von Schaumburg, CEO of InvisiNet, a wireless LAN installer. By examining your wired network you will see traffic patterns and bandwidth demand typical of the user population. After all, the wireless network will be an extension of the existing network.

Based on this review, you can start to estimate what throughput, coverage and security you'll need for a given set of applications, Musgrave says.

These considerations, in turn, guide planners through the process of evaluating different wireless interface cards and access points.

The expertise to handle such evaluations varies widely. At BMW Group, which has 200 802.11b Wi-Fi access points at plants in Munich, the IT staff handles the process with help from equipment vendors and some outside support staff, says Daniel Lange, IT strategist with BMW.

Currently, the decision to go wireless, he says, is made on a case-by-case basis, weighing business needs at a given site against criteria such as security and costs. Later this year BMW will formalize a process that will help business users evaluate the need for wireless before they formulate their IT requests, Lange says. In particular, the process will help users assess the emerging 802.11a technology, which supports a maximum speed of 54M bit/sec.

To help users through the Wi-Fi needs assessment phase, Signa has created a seven-page preproject information sheet covering details such as the size of the facility, building construction mate-

rials and number of users. "We often hear from IT managers, 'I never thought about those things,'" Musgrave says.

One thing often overlooked is that wireless LANs require wiring: Wired Ethernet jacks may have to be installed so access points can be attached to the corporate LAN. And electrical power outlets may be needed for the access points, though some vendors offer the option of powering the access devices over Category 5 cable.

Wireless everywhere?

While wireless offers obvious utility in warehouses and other wide-open spaces, there is disagreement about whether wireless LANs are suitable for general office environments.

At BMW, such deployments are discouraged because of the limited 802.11b bandwidth, about 5M to 6M bit/sec, and because of security concerns. "We do not consider 802.11b to be a drop-in replacement for wired infrastructure," Lange says. Some corporations limit wireless to conference rooms or other semipublic areas, relying on the wired net for day-to-day use.

But Federal Express is deploying wireless throughout two campuses at headquarters in Memphis, treating it as an extension of the corporate net.

FedEx workers have come to expect the convenience of wireless access, according to Ken Pasley, directory of wireless development at the company. If a group gathers for a meeting in one location that doesn't have wireless coverage, they'll move until they find it, he says.

One potential gotcha: Because of the limited bandwidth, Pasley says you have to watch out for large file downloads, such as CAD/CAM drawings. "You'd have to look at those closely," he says. But Signa's Musgrave says that even at 5M bit/sec, wireless LANs can support a range of business applications, including enterprise resource planning and PowerPoint.

FedEx started using wireless LANs five years ago, mainly in package sorting and aircraft maintenance areas. With the shift from those early proprietary LANs to 802.11b, which doubled bandwidth to 11M bit/sec, the company saw a 30% jump in productivity at the package sorting centers, Pasley says.

Security

Although security often comes up later in network design, it has to be considered early with wireless because of the inherent vulnerabilities. Wireless LANs are, by definition, not secure: Data is broadcast through the air and is hard to contain. The original encryption scheme for 802.11, called Wired Equivalent Privacy (WEP), is known to have several inherent weaknesses.

Given that, wireless security is a blend of art and science. "You should know what the vulnerabilities are and do what you can within reason to mitigate them," says Dennis Moule, information systems manager for carrier software vendor CoManage. "You make reasonable, sensible precautions to minimize risks. . . . And keep current with the emerging risks and how these might affect the equation."

Depending on the requirements, security can range from turning on the basic WEP encryption to full-blown authentication and encryption via VPNs tied into RADIUS servers. One Canadian integrator reports that many of his wireless customers say their data has almost no value to anyone outside the company, so security is not a priority for them.

But that's a deliberate decision. Many users don't seem to realize that the default security level for most wireless LAN equipment is zero. "I've been doing research on companies that have wireless nets and it appears the majority don't turn on [WEP] encryption, leaving their nets completely open," says Vincent Gullotta, head network engineer for LANocracy, a wireless LAN installer.

"We assume that there is no security, that the wireless access point is an open, public Ethernet jack," says Christopher Hertel, network design engineer with the University of Minnesota's office of IT. The university treats the wireless LAN as if it were a public Internet, putting a firewall between the LAN and the wired net, and using a campus VPN and authentication via an X.500 directory.

This configuration is increasingly common, but it comes with a number of trade-offs. Administration becomes more complicated, requiring the distribution and updates of VPN client software to thousands of devices. There may be a lack of VPN clients for some operating systems. You have to build a separate wired infrastructure linking access points on the other side of the firewall. And destination addresses are limited to the VPN gate servers.

A related but obscure issue is that most employees with wireless laptops don't realize their wireless cards remain active, even if they're not using the VPN. It's possible for an attacker to use that active link to jump a worker's laptop and infect it with a virus or other malicious code, which is transmitted to the corporate network via the VPN when the worker logs on.

For its part, CoManage uses basic security steps: 128-bit WEP encryption, obscure network names, a clear prohibition on hooking up access points without talking to the IS department and periodic efforts to crack its own net using programs such as WEP Crack, Airsnort and Netstumbler. Moule plans to use the improved WEP Plus when his vendor upgrades access points and network interface card (NIC) software. At some point, as attacks become more common, CoManage will adopt a firewall/VPN model.

Site survey

The actual LAN design — how many access points are placed — draws on all this data and research, and hinges on several factors: the type of materials used in building construction and furnishings, the number of users in a given area and whether that number changes, and the throughput those users need. The larger the deployment and the more demanding the applications, the more complicated the equation becomes.

Signa uses a blend of off-the-shelf programs, such as AutoCAD and Visio, with their own list of wireless parameters when they reach the design phase. They enter data on the site dimensions, wall materials and other variables, and create a three-dimensional model showing an initial placement for the access points. But this model is always augmented with an on-site survey.

Most corporations don't have the expertise of Signa's designers. However, they can use handheld spectrum analyzers to detect radio interference and the same laptop applications many wireless LAN vendors offer for the site survey. You plug in an access point, then walk around with a wireless laptop and the programs show signal strength and throughput at different locations and different distances.

If you're doing this design work yourself, watch out for a common mistake: using one brand of interface card and access point for the initial design, then a different brand in the final deployment. Doing so can lead to surprises stemming from different radio-frequency propagation characteristics, which leads to dead spots and lower bandwidth.

One consideration sometimes overlooked is aesthetics: do you want the access points to be visible or hidden behind ceiling tiles? And then there's the basketball factor: FedEx had to raise the access points in its sorting bays higher off the ground because college-age part-timers were leaping up and slapping at them to practice slam-dunks.

The site survey is essential for dealing with one of the most confusing design issues: 802.11b access points have a maximum of three nonoverlapping channels for users. Too many access points, haphazardly placed, will overlap these channels and users will see a serious drop in performance because of contention for the channel. Proper channel configuration can let you stack three access points atop each other giving users maximum available bandwidth.

The just-emerging 802.11a products have eight indoor channels and four more for outdoors, which means that more access points can be packed into the same area, to support more users at higher bandwidth — and, for now, at a higher cost compared with 802.11b LANs.

In theory, the higher bandwidth of 11a means the radios cover less distance, so two to four times more 11a access points will be needed to cover the same area as with 11b. But this will vary greatly by site.

From B to A?

Most corporations seem to be going with 802.11b installations while planning to pilot 802.11a down the road. FedEx is sticking with 802.11b, with no plans to use 802.11a or 802.11g. The latter boosts 802.11b speeds to nearly 54M bit/sec but uses the same radio frequency band as 802.11b — 2.4 GHz.

One popular configuration that's emerging is using 802.11b to create blanket site coverage at a maximum usable bandwidth of 4.5M to 6M byte/sec, with an eye to using 802.11a products to create higher-bandwidth "hot spots" for select users or applications. Some vendors offer access points with two card slots so customers can add 802.11a when needed. One company, Symbol Technologies, will let customers snap on 802.11a access points to existing 802.11b products, so the former can use the power and network management features of the "host" access point.

There's no shortage of vendors for wireless access points and NICs. They range from inexpensive 802.11b products that require minimal configuration and offer limited opportunity for customization, to premium-priced "enterprise-class" devices. Enterprise access points, for example, may have metal covers, special seals for harsh environments, network management software, an advanced Web-based user interface for administrators, a range of specialized software and a battery of proprietary features. These vendor-exclusive features might include support of higher bandwidths using proprietary techniques that the IEEE standard does not cover.

These "vendor exclusives" can frustrate interoperability. But experts and experienced users agree that a number of other factors can also render systems incompatible. One is software: drivers available for one brand of network cards may not work with another brand of access points. Or a given may not vendor support the drivers you need.

This stew of variables is so complex that Signa's designers have created a chart that details the different features and performance characteristics of access points and interface cards. In

some locations, a specialized antenna may be needed to "shape" and direct the radio transmission. In that case, the access point must be able to accept an external antenna.

The equipment criteria are established by blending data from phase 1, the initial requirements process, and phase 2, the site survey.

"You have to distinguish between what are features of the [802.11b] standard for interoperability and what are vendor proprietary 'standards,'" says Tiberio Massaro, Signa's professional services marketing manager. Then, network executives can make decisions knowing the trade-offs.

Deployment

It's a relief that most users and integrators agree that deployment of a properly surveyed and designed wireless LAN is pretty straightforward.

Experts recommend staging the equipment first — create the network names and identification databases, load the net information into the access points, burn in the IP addresses and test everything.

You know where the access points are going, and what interface cards are being installed in which clients. It's a matter of pulling the needed cables for the access points, possibly adding some power outlets and attaching the access points.

But details remain. If you have outdoor units, these need to be properly enclosed and grounded. LANocracy's Gullotta recommends always following the manufacturer's instructions. "For whatever reason, I've found that wireless LAN installations go much more smoothly if you follow these exactly," he says.

One of the final steps is to test the installed LAN thoroughly, at all levels, checking security policies, throughput and coverage.

There will be ongoing adjustments. FedEx employees piled equipment around one access point and network performance dropped. New shelving, new walls and shifts in inventory all can affect FedEx's throughput.

When an access point "hangs," for whatever reason, and simply stops working, it can create a more serious, hidden problem, IBM's Denton cautions. To get the device working again, you can shut off power and then turn it back on, or do a reset.

"But a reset clears out the security protocols," Denton says. "It can make a secure access point totally insecure, and no one will know the difference unless they specifically check."

User training must take into account everything from these serious security issues to the more mundane idea of teaching people that moving their wireless clients a foot or two might improve throughput drastically.

Such is the state of Wi-Fi: As easy as it is to get a wireless network up and running, doing it right takes as much upfront planning and more ongoing diligence than your traditional wired networks.

Cox is Senior Editor at Network World magazine covering Wireless. He can be reached at jcox@nww.com.

Wireless LAN lessons learned

Coping with everything from renegade users to interfering elevators.

BY DENISE DUBIE, APRIL JACOBS AND KATHLEEN OHLSON

Doctors and nurses at St. Luke's Episcopal Health System had to change the way — and even where — they dealt with patients to get the most out of their wireless LAN.

"At first, we couldn't figure out why all of a sudden a wireless device would lose its signal. Then we heard the transport elevator pass the floor, and it became very clear," says Gene Gretzer, project manager for access technology at the Houston hospital. After an IT stakeout of sorts, he discovered that metal beds on the elevator interrupted the connection between wireless laptops and the nearest access point.

Since widely deploying the hospital's wireless LAN, Gretzer says, users have begun to realize that computer problems sometimes have nothing to do with the computer. "It's not uncommon

to hear, 'Is someone using the microwave? My laptop stopped working,' " he says.

Getting around the physical hurdles of deploying a wireless LAN is just one concern a company must address when going wireless. Network managers also must learn which applications work well on the network and how to better secure the wireless network from potential intruders. More and more companies — particularly those in retail, healthcare, financial services and education — want to conduct business wire-free for easy access and mobility. Many, such as St. Luke's, have learned a few things along the way that have made their wireless deployments a business asset.

In Gretzer's case, as soon, he and his staff performed extensive site surveys, St. Luke's connectivity issues disappeared. And he says routine follow-ups ensure that no one puts, say, a wooden shelf in front of an access point.

For the most part, St. Luke's, staff uses wireless laptops to scan patient wristbands that are produced with a bar code when a patient is admitted to the hospital. All data regarding that patient is then accessible via the bar code. To avoid inputting a lot of information by hand, hospital staffers use laptops equipped with wireless network interface cards to scan the wristbands. Gretzer estimates staff productivity is up 15% to 20% because of the wireless scanning.

"The wireless system allows caregivers to spend more time with the patient and less time filling out paperwork," Gretzer says. "On the computing side, it's much faster and gives multiple people immediate access to patient records."

St. Luke's is careful to use applications that work well within a wireless LAN, Gretzer says. Bursty applications, such as e-mail, fit the bill because they allow immediate access to data but consume little bandwidth.

St. Luke's initially invested about $1 million to set up the wireless LAN and roll out 130 access points. The healthcare group is upgrading its Proxim 802.11 wireless LAN to a Cisco AiroNet 802.11b system. The 802.11b standard, also known as Wi-Fi, operates on the 2.4-GHz frequency and offers users speeds of 11M bit/sec, as opposed to the 1M to 2M bit/sec rate of an 802.11 wireless LAN. The upgrade will cost about $250,000, and the boost in speed will reduce the hospital's access points down to 80, while still providing the same service.

Another healthcare facility exploiting wireless technology is the University of Texas M.D. Anderson Cancer Center in Houston, which in March deployed Cisco 802.11b wireless LAN technology to 120 nurses, doctors, administrators and other employees. The 15-access-point wireless LAN will cost the center about $45,000, and there are plans to roll out wireless LAN access points to 67 more clinics in the next three years, says Jim Thompson, director of communications and computing.

While implementing the wireless LAN pilot, Thompson and his team encountered an unexpected volume of previously existing signal traffic.

"It turned out we had wireless [pockets] everywhere" because staffers bought their own antennas, Thompson says. Conducting a thorough site survey is important, he says. "You don't want to put an antenna where you have a meshed concrete wall — you can't get a signal out."

Guest services

Wireless LAN implementations in some types of businesses can face challenges that are not common in private companies. In the hospitality industry, wireless LAN deployments can become more difficult when offered as a public service to guests.

Aaron Ruggaber, director of purchasing for Penticton Lakeside Resort & Casino in British Columbia, installed a Lucent Orinoco wireless LAN in mid-2000 to give guests high-speed Internet access. Before implementing the wireless LAN, Ruggaber had to configure each guest's laptop to dial in to the resort's Internet setup.

"It was a very slow [process] and a pain in the butt," he says. "We weren't able to give the access we wanted to clients."

Guests have the option of receiving a wireless network PC card and client software that can be integrated into the laptop for wireless access. However, Ruggaber says resort guests have not embraced the wireless technology as he had expected. He also has encountered more obstacles than he anticipated deploying the equipment, and from vendors.

Ruggaber was told a wireless card installation would take about 10 minutes, but it actually averaged 35 to 40 minutes for each installation.

Venetian Hotel in Las Vegas also deployed a wireless LAN to let staff check in guests in the convention center or at the carport using handheld wireless devices that are equipped with belt printers, credit card swipers and key encoders. Chris Stacey, Internet marketing manager, says the hotel uses wireless devices because of the volume of guests who check in between Thursday and Sunday every week.

"We had mobile check-in stands where people could check in, but the handhelds are a lot easier because we can serve guests anywhere in the hotel," he says.

Wire-free FedEx

As with the hotels, convenience and efficiency are two reasons FedEx expanded its wireless deployment in the past five years. Currently in the process of rolling out upwards of 10,000 access points, the shipping giant upgraded from 802.11 to 802.11b about 18 months ago. Since implementing a wireless LAN five years ago, FedEx estimates staff productivity to be up 30%, which is easier to envision when you consider each package receives

an average of 12 scans during its travels. Not only does wireless offer mobility, it also has safety advantages.

"People scanning aren't tethered to anything and can work freely without getting caught up in any wires," says FedEx Director of Wireless Strategy Ken Pasley. FedEx plans to bring wireless technology to its fleet of wide-body planes to track packages and repair aircraft without a wired connection on the tarmac.

"We've dealt with airports for years, and they're fairly static, but with wireless we're finding different techniques to get access points out there," Pasley says. "Wireless is not mundane. This is an exciting business."

However, it's the "gee-whiz" aspect of today's wireless technologies that can bring down a wireless LAN, says Joe Baron, network architect at Prudential Financial in Newark, N.J. He says the thrill of easy, remote access makes employees want to tie their unauthorized PDAs and handhelds into the corporate wireless LAN.

"The biggest risk to deploying [wireless LANs] in the enterprise is the low-cost consumer gear that someone plugs in to the corporate net," Baron says.

Wireless security must extend to physical devices, as Earl Fischer discovered after deploying wireless LANs in each of Famous Footwear's more than 50 shoe stores. Fischer, vice president of information systems at the Madison, Wis., shoe retailer, says the Symbol SPT 1700 handhelds he designed for staffers to scan bar codes on shoes are often stolen. But because part of his wireless strategy is to "keep the devices as vanilla as possible" most thieves deposit the PDAs in nearby trash cans.

On the brighter side, Fischer says deploying wireless LANs reduced pricing errors by 75%.

With an access point per store, the handhelds tap back into the headquarters system via a VPN. Fischer strips down the Symbol devices to run only his proprietary applications that deal with inventory and pricing and keep each store updated weekly. He says keeping the devices simple lessens the learning curve for users.

"It's about adding convenience and efficiency that you wouldn't get with tethered devices," Fischer says, but adds that he doesn't worry about the people pocketing his devices eventually tapping into his corporate network. "If you plan properly, [wireless LANs] will help you do your business better, without putting that business any more at risk."

Dubie is a Staff Writer at Network World magazine covering Enterprise Applications. She can be reached at ddubie@nww.com.

Wi-Fi spies

New authentication and encryption techniques will protect wireless LANs from drive-by hackers.

BY JIM GEIER

By now, the stories of hackers driving around in cars, breaking into wireless LANs with off-the-shelf tools such as AirSnort or WEPcrack have become commonplace.

Wired Equivalent Privacy (WEP), the 802.11 standard for wireless security, has been discredited on a couple of counts:

* Weak encryption. To comply with federal encryption export rules that existed in 1997, the 802.11 standards group limited WEP key lengths to 40 bits. This provides a limited level of encryption that is relatively easy to compromise.

A hacker using a statistical analysis tool can crack a WEP key from a wireless LAN with typical levels of traffic in less than 24 hours.

* Static keys. Another problem is that WEP keys are common among the desktop cards and access points within the same wireless LAN, and they don't automatically change on a regular basis. To make matters worse, WEP has no key distribution method. Once you set up the keys for each user, they're difficult to change.

Network managers are reluctant to update WEP keys because of the long, tedious process of going to each end user's device to make the changes. As a result, wireless LANs using WEP have rel-

atively weak keys banging around the network for days, weeks and even months.

The bottom line is that the current version of WEP is ineffective for protecting valuable information. Most applications need stronger, dynamic encryption and authentication mechanisms. Even if you don't think you need something stronger than WEP, you probably do.

Any wireless LAN that provides a potential path to valuable resources — even if those resources don't have anything to do with the intended wireless application — requires more security than what WEP offers.

Consider a hospital that deploys a wireless LAN to support mobile monitoring of a patient's heart rate and temperature. Because of the limited security requirements of that type of patient information, the hospital may decide that this application doesn't require encryption.

However, the wireless LAN offers a path through the network backbone to the hospital billing system. A hacker with a radio-equipped laptop sitting in a car in the hospital parking lot can easily traverse the network. This puts the hospital billing system in the hands of the hacker.

The obvious industries that require the strongest wireless security include banking and finance. In addition, the expected increase of public wireless LANs at airports, hotels and other public places will increase the potential for hackers to find ways into places on networks where they shouldn't go.

In response, companies such as Illuminet and TTS-Linx are developing public wireless LAN products that focus on strong security mechanisms that go well beyond the existing 802.11 WEP. In addition, the 802.11 working group, the Wireless Ethernet Compatibility Alliance, Wireless ISP Roaming and vendors are aggressively developing solutions to fill the wireless LAN security hole.

802.1X to the rescue

Windows XP and the majority of access point vendors support IEEE 802.1X, which is a standard defining the framework for port-based authentication and key distribution over both wired and wireless LANs.

Most people envision 802.1X as the primary enabler for wireless LAN security because it does a great job of dynamically allocating encryption keys.

Extensible Authentication Protocol (EAP) is the heart of 802.1X and facilitates the authentication process between an "authenticator" and a "supplicant" via an authentication server.

In the case of a wireless LAN, the supplicant is the client (802.11 network interface card) and the authenticator is the access point. The access point serves as the boundary between the protected and the unprotected parts of the network. Authentication servers approve and disapprove access, and they come in several varieties, such as Remote Authentication Dial-In User Service and Kerberos.

When an 802.1X client attempts to connect with an access point, the access point establishes a port that only lets EAP traffic through. The process continues, and the access point uses the client's identity for authentication with the authentication server.

If the authentication result is positive, the access point will enable other specific traffic (such as Dynamic Host Configuration Protocol, Post Office Protocol 3 and Simple Mail Transfer Protocol) from the client to flow through the access point to the protected side of the network. If the client logs off, the access point will disable the client's ports.

EAP alone doesn't define all the techniques for securing a wireless connection. The security solution also needs to implement an "authentication type," such the Lightweight Extensible Authentication Protocol (LEAP) or EAP Transport Layer Security (EAP-TLS).

Both of these methods include mutual authentication between client and access point. LEAP dynamically generates WEP keys within Cisco-based wireless LANs.

EAP-TLS is an authentication type that requires clients and access points to possess digital certificates, which enables the dynamic distribution of WEP keys over a secure connection. Windows XP supports EAP-TLS for wireless network authentication. Most wireless LAN vendors now support EAP-TLS as well.

An issue with these 802.1X products is that they still use WEP for encryption, which is based on relatively weak keys. However, at least 802.1X changes the keys often enough to minimize problems. Administrators can set up systems to change keys every hour, every 10 minutes or once each session.

802.11i also to the rescue

The IEEE 802.11i subgroup, also referred to as Task Group I (TGi), is developing an enhancement to the 802.11 Media Access Control Layer to incorporate 802.1X mechanisms.

TGi is working out the details, but the standard will specify the use of 802.1X and leave the choice of EAP authentication type to the implementer. The 802.11i upgrade will change keys frequently and strengthen the encryption process.

Thus, 802.11i will solve the two primary security problems with WEP: weak encryption and static keys.

The 802.11i standard should become available and integrated within products toward year-end or the beginning of next year.

Geier provides independent consulting services to companies developing and deploying wireless networks. He is the author of the book Wireless LANs and leads workshops on wireless LANs. He can be reached at jimgeier@wireless-nets.com.