



# **NETWORKWORLD**

**October 9, 2006**

## **The Wi-Fi divide**

***WLANs find a home in tiled work areas, but deployment lags in carpeted office environments.***

**By Susan Breidenbach**

The wireless wave has swept through colleges, hospitals, factory floors, retailers, downtowns, hot spots and the home, but it's still just lapping at the edges of traditional enterprise office environments. As the original 802.11 standard approaches its 10th birthday, concerns about wireless security and management overhead keep the technology's popularity in highly mobile "tile niches" from spilling over into enterprise "carpeted areas" and industries.

Carpeted-area wireless LAN (WLAN) deployments continue to face some significant roadblocks. Most of the employees who occupy these areas work at desks, and few have laptops. The low penetration of laptops replacing traditional office desktops is an inherent limitation and many companies continue to see them - and Wi-Fi - more as a convenience than a business necessity. The risks continue to outweigh the benefits by a significant margin.

To check the Wi-Fi pulse of the industry, Network World recently touched base with nine companies in various stages of WLAN adoption, ranging from no-wireless policies to aggressive rollouts.

One Wi-Fi skeptic is Blue Cross of Idaho, a representative of the carpet-heavy insurance industry. Most employees work at desks with wired access, and very few have laptop computers. Except for one mobile training area, a strict no-wireless policy is enforced by Network Chemistry's RFprotect monitoring technology.

"We wouldn't shy away from wireless if we identified a real business need for it, but we just haven't seen one on the campus," says Jan Marshall, manager of technical and network services for the Blue Cross/Blue Shield franchise. "The amount of manpower required to keep a wired network secure and working is much less," he adds.

### **Security still a concern**

Nevertheless, security continues to hold back deployments. In a recent Gartner survey, 98% of enterprise IT professionals said WLAN security was a major concern, and 60% said it was not adequate.

Financial institutions in particular are reluctant to deploy wireless. Some avoid WLANs completely, and others deploy the technology only to accommodate guests.

Prudential Financial is "cautiously optimistic" about WLAN security, says Jim White, vice president of information systems. The company is testing the wireless waters with a 200-user pilot begun earlier this year. Before that, concerns about security and shared-media performance had kept wireless out of the company.

"This year, speed, reliability and - at least, theoretically - security have improved," White says, referring to ratification of the 802.11i wireless standard and the integration of authentication and Active Directory in Windows XP Service Pack 2. "We're using [Wi-Fi Protected Access] and WPA2 encryption, plus the direct tie into Active Directory gives us additional controls over the environment."

Similarly, Turner Construction Co. had WLAN security concerns that kept a no-wireless policy in place until the middle of last year. Company laptops were shipped from the factory with the embedded wireless technology disabled at the BIOS level. Users could enable it for hot-spot access to the Internet outside the company, but wireless access to the private enterprise network was not allowed.

"But then a lot of technologies fell in place at about the same time," recalls Mason Brown, senior network security engineer for Turner. "The WPA encryption and 802.1X authentication looked like strong security, plus Windows XP Service Pack 2 introduced seamless authentication with Active Directory." He also cites the advent of lightweight access points.

"In short, the server side and the wireless hardware side came together, and we could provide a seamless and secure wireless experience for users," he says. Turner put together policies and let its 46 branch offices know that wireless was available, and 11 offices have implemented WLANs throughout their facilities.

Ironically, the paradigm shift toward thin access points with centralized management that began about a year and a half ago initially slowed WLAN deployment. While replacing intelligent, distributed access points with this more centralized architecture enables better security, management and scalability, customers were baffled initially as vendors did an about-face and started singing a different tune.

"It took users a while to understand the benefits of the centralized architecture," say Aaron Vance, senior analyst with Synergy Research. "Now they see how it is more conducive to large-scale rollouts that will have tangible business benefits to them. You can now scale up to tens of thousands of access points, which would have been operationally impossible in the distributed scenario."

One WLAN early adopter, the University of Utah Health Sciences Center (UUHSC), has seen the benefits of the thin-access-point architecture. The medical center cut its wireless teeth on the old 802.11 frequency-hopping technology and evolved its infrastructure with the standard, gradually seeing specialized medical devices and mobile carts starting to communicate over the WLAN. And UUHSC is eyeing the emerging 802.11n standard, which would let bandwidth-intensive devices, such as portable X-ray machines, transmit images over the WLAN.

"Last year we were bringing a new medical education building online, and we took a fresh look at how we were doing wireless," says Bo Mendenhall, manager of information security at UUHSC. The medical center decided on a thin-access-point switched solution from Aruba Networks and has replaced 90% of its fat access points. Aruba's built-in monitoring capabilities are used to help secure the WLAN, augmented by AirDefense technology in critical areas.

While the medical center's clinical areas are completely covered with WLAN access, deployment in the administrative offices is still quite low. The original driver for the WLAN was the mobility requirements of healthcare professionals, but such an imperative is lacking on the administrative side.

BNSF Railway is another WLAN early adopter that has a carpeted/noncarpeted divide - though in BNSF's case, it is more an indoor/outdoor divide. The vast majority of the Fort Worth, Texas-based railroad's 1200 access points are outside, where they provide access to maintenance and intermodal yards.

The intermodal yards handle containers that are transported by ocean vessel, rail or truck. The trucks moving these containers around were originally equipped with a proprietary 900MHz wireless system, but they were replaced about five years ago with 802.11b, which was subsequently supplanted by 802.11g. Like UUHSC, BNSF picked Aruba WLAN technology because of its security features.

"At first, we didn't think security issues could do that much damage," says Frederick Gratke, director of technology for BNSF. "But we gradually realized there were people who could be malicious for no particular reason. We now pay a lot of attention to security and developing standards, and are pushing certificates to users for authentication."

However, it is the lack of a business case, rather than security fears, that keeps WLAN deployment somewhat limited in the railroad's office areas. Cafeterias, break rooms and other common meeting areas are covered, but a lot of the cubicles and offices are not.

### **ROI considerations**

This same carpeted/noncarpeted divide is manifested to some extent in enterprises as diverse as entertainment-focused West Edmonton Mall (WEM) and defense contractors Lockheed Martin and Textron. Billed as the world's largest entertainment and shopping center, the West Edmonton Mall covers the equivalent of 48 city blocks in Edmonton, Alberta, and includes 800 shops, 100 restaurants, a hotel and nine major entertainment attractions. Guests are provided with an uncommon 21st-century experience, and wireless connectivity is a part of it.

Having a huge facility to cover, WEM eschewed WLAN technology until thin access points with centralized management started to emerge about three years ago. The company settled on a WLAN infrastructure from Chantry (now part of Siemens' HiPath portfolio) and began a phased rollout.

"We started with hospitality first, because that was the lowest-hanging fruit," says Joe Schuldhaus, the mall's vice president of IT. "Management wanted to see some payback. We lit up the hotel, the conference center and all of the hotel assets, including the food courts in the mall."

Guests can purchase wireless Internet access, and the mall's shops can piggyback on the wireless infrastructure. The network also is being leveraged to automate some of the mall's operational facilities, collecting feeds from the security cameras and enabling the maintenance staff to interact with the HVAC systems remotely.

WEM, which is using AirTight's SpectraGuard technology to monitor for rogue activity, is "not keeping wireless out of anywhere deliberately," Schuldhaus says. While the focus is elsewhere, access points are being deployed in back-office environments, including some remote offices and executives' homes. "We can manage them remotely and keep full ownership of the security," he says. "Employees just power up their laptops and see everything as if they were here in the main facility."

As defense contractors, Lockheed Martin and Textron must run somewhat tighter network ships. The federal 8100.2 NIST standard regulates wireless deployments, and areas doing classified work can have no wireless communications.

"We're right on the cusp, with wireless about to take off across the enterprise," says Jasyn Voshell, senior IT auditor for Textron. WLANs cover about 20% of Textron, with deployments split fairly equally between carpeted and noncarpeted areas. But going forward, the emphasis will be more one-sided.

"We will probably focus on the manufacturing areas first, because that's where most of the measurable ROI is. People in manufacturing have to be mobile, and having cables all over the floors is dangerous. In the carpeted office spaces, wireless is more just a convenience for the conference rooms."

Textron's access points are deployed in a DMZ, where they connect to a VPN switch, and laptops are equipped with software that protects them against a variety of wireless threats and keeps track of where they go when they are off the campus. A wireless intrusion-detection system (IDS) keeps an eye on what happens on campus.

"When we put the IDS system in, it was amazing to see how many rogue [access points] we had out there," Voshell says. "We didn't expect that."

Textron is a multi-industry manufacturing conglomerate that derives about a quarter of its revenue from defense work. The much more heavily defense-focused Lockheed Martin is a bit more circumspect about its WLAN deployments and plans. Rollouts have favored the noncarpeted areas, says senior systems analyst Ben Halpert, but the company is in the process of defining a comprehensive mobility strategy.

"Lockheed Martin has seen increasing interest in extending wireless coverage into the carpeted areas and is working on a means to close the gap," Halpert says.

### **Don't knock convenience**

This gap can be virtually nonexistent in some companies. While many dismiss convenience as mere luxury, others regard it as a sufficient reason to embrace Wi-Fi technology wholeheartedly - even throughout the back offices. The fast-food industry, for example, is basically in the convenience business, and wireless fits easily into the corporate culture.

"We started looking at WLANs five or six years ago, and it caught on very quickly," says Gary Tomanich, a senior network analyst for a major fast-food chain. "The wireless culture just exploded, and it got to the point where no one wanted a desktop computer anymore."

In the midst of this unfettered enthusiasm, rogue access points started to proliferate as employees brought in their own devices. "For us, functionality trumped security, and that kind of came back to bite us," Tomanich says. "We brought in a third party to do a wireless audit, and the results were quite shocking."

A detailed remediation plan sent the fast-food chain looking at WLAN security products, and it now uses AirTight's SpectraGuard technology to ensure proper coverage and keep an eye on the airwaves. The SpectraGuard site planner tool let Tomanich's headquarters-based team deploy Wi-Fi networks securely in 33 regional sites, without having to visit them.

"There's no reason to be afraid of wireless," he says. "It's just that a lot of companies rolled it out without a lot of thought about standards and policies."

### **Implementation inhibitors**

Any type of wireless rollout - from cavalier to painstakingly planned - is not an option in many carpeted areas. According to Forrester, laptops make up 22% of the installed base of enterprise computers, and they still represent a minority of new purchases. The manufacturing sector, a WLAN early adopter, shows the highest preference for laptops, but they still account for just 32% of its new acquisitions. The average for all sectors is 25%, a number that doesn't present much of a case for ubiquitous WLAN deployment.

Mobility has long been touted as a big productivity booster, and 44% of respondents to the Gartner survey say increasing productivity was the primary reason to implement WLANs. However, such productivity is difficult to quantify and isn't proving to be a compelling reason to extend WLANs throughout carpeted areas. When push comes to shove, they are still seen as a convenience.

Another obstacle may be the shifting sands of 802.11 transmission standards. Frequency-hopping gave way to 802.11b, followed by 802.11a and 802.11g, and now the industry awaits 802.11n.

"A number of our no-wireless customers are waiting for 802.11n, which means they won't be deploying WLANs until late next year or even early 2008," says Dennis Tsu, vice president of marketing for AirTight. The Wi-Fi Alliance recently announced plans to begin interoperability testing soon of the pre-802.11n products flooding the market. These devices are gaining traction mainly with consumers.

Security issues also affect the carpeted areas more severely, partly because the reward variable in the risk/reward equation isn't as big, and partly because carpeted-area users are basically in control of WLAN security. While the handheld devices used in noncarpeted areas are preconfigured, carpeted-area users are equipped with laptops that can be configured as rogue access points.

In fact, unless they are using wireless monitoring technology for detection and enforcement, enterprises that think they have no wireless actually do. Employees pick up inexpensive access points at the local computer store, or configure their laptops to function as peer access points.

And companies can't watch for such rogue wireless activities unless they install wireless technology; some solutions require an actual WLAN. As this exposure to wireless gradually makes enterprises more comfortable with wireless networking, they gain confidence in their ability to manage and control a wireless environment, and start using the technology to implement WLANs rather than keep them out.

"It allows us to enforce whatever policy we choose, whether it is no wireless or part wireless or wireless almost everywhere," Blue Cross of Idaho's Marshall says about Network Chemistry's RFprotect.

Once companies do take the wireless plunge, their priorities and concerns quickly shift. According to the Gartner study, management becomes the bigger issue. "If you haven't deployed, you are worried about security," says Gartner research director Rachna Ahlawat. If you have deployed, you know that security isn't the problem - it's the management."

The IT professionals we interviewed agree. With no standards for WLAN management, they advise keeping things simple by sticking to access points from a single vendor. Otherwise, the risks are likely to outweigh the rewards in carpeted-area deployments.

Don't be surprised if getting into wireless increases the security of your wired network. "You can have a very insecure wired network as well," West Edmonton Mall's Schuldhaus says. "Wireless forces companies to be more vigilant about the overall security of their network infrastructures and more aware of the issues."