

**Special Report**

# Wireless LAN Advances: A Concise Assessment

Sponsored By:



This Special Advertising Section Produced By:

**NetworkWorld**  
[www.nwfusion.com](http://www.nwfusion.com)

*Once a luxury, wireless is rapidly becoming a business necessity, an enabler that keeps mobile employees productive and customer-facing employees connected and up to the minute. But, and there is a bit "BUT"...as with any emerging technology there are lessons to learn, technologies to fine tune and advances all the while, meaning we have to relearn the lessons, fine tune the technology, etc.*

*This special report on wireless is a snap shot in time, examining how companies are putting the technology to work, the critical developments in wireless security, and the emergence of a whole new class of wireless LAN switch products that promise to redress many of the short comings of first generation wireless LAN solutions.*

## Table of Contents

<b>Mobile grows up</b> .....	<b>3</b>
IT execs are loading enterprise business applications onto those cool little gadgets.	
<b>WPA plugs holes in WEP</b> .....	<b>6</b>
New wireless security standard could drive hot spot, academic installations.	
<b>A switch in time</b> .....	<b>8</b>
Wireless LAN switches could drive 802.11 rollouts to the next level.	

## Mobile grows up

*IT execs are loading enterprise business applications onto those cool little gadgets.*

BY STEVE ULFELDER  
NETWORK WORLD, 10/27/03

Matt Norce has watched mobile computing evolve.

Four years ago, Norce, network administrator at J.C. Ehrlich, a Reading, Pa., pest-control company with 42 offices in five states, began giving mobile workers PDAs from HP.

He used synchronization software from Extended Systems to load appointment information and driving directions on the devices. But the 120 exterminators in the pilot project quickly asked for more functionality. People start out with basic [personal information management] applications. Then they see the potential of the software and they want to do enterprise apps too.

As a result, the pest-control company has added CRM and e-mail to its mobile arsenal. Working with Weidenhammer Systems, a Reading development firm, J.C. Ehrlich's team built a CRM application specifically for PDAs, avoiding many of the headaches that businesses face when they try to squeeze an enterprise application onto mobile devices.

The pilot program is being extended to all of J.C. Ehrlich's exterminators. On the hardware side, the HPs were replaced a while back with NEC MobilePros, "which are still our No. 1 unit," Norce says. And the company is rolling out newer NEC models that run Microsoft's Pocket PC operating system.

According to Gartner, 55% of large companies plan to move their pilot mobile applications into production this year. The primary reason is competitive pressure; with customers and trading partners growing more demanding about speed and quality of service, large businesses need to get useful data out to their mobile workers.

But only 25% of mobile application deployments will succeed this year, according to Gartner. The research firm says "social factors" - such as the introduction of wireless technology to workers who aren't ready for it - and bad architectural choices will be the major problems.

The good news is that mobile applications have matured enough so that a body of best practices has taken hold. Tips

from analysts and businesses can help you learn from other IT organizations' pain.

### Find third-party help

Pitney Bowes rethought its mobility program when the Stamford, Conn., mail and document-management giant undertook a sweeping reorganization. A division of the company had equipped its field service agents with handheld devices long ago. But "it was a proprietary system designed to look inward," says Ralph Nichols, Pitney Bowes' service program manager for document-messaging technologies. The system had other flaws too; it was a batch system relying on data that might be up to two weeks old, and most input and output was in code rather than text, "so until you intimately knew the codes, the information in the machine didn't have a lot of value," he adds.

The primary product sold and serviced by Nichols' division is Console Inserter, which is used by corporations with high mailing volumes to insert documents such as credit-card statements and utility bills in envelopes. A console inserter is a complex machine with many mechanical, electronic and software components.

Two years ago, Pitney Bowes standardized on Siebel Systems as its CRM and field-service application provider. But Siebel lacked wireless capability. For that, Pitney Bowes turned to Antenna Software, which offers a product called Antenna A3 for Siebel Field Service.

Antenna calls its underlying system A3 Mobile Foundation. The XML-based system supports diverse networks and carriers (including Code Division Multiple Access, General Packet Radio Service and two-way paging) and optimizes data transport accordingly, the company says. When Pitney Bowes technicians are out of network reach, the system stores their data input, then forwards it when they regain network access.

### Futureproof your investment

Vendors of enterprise software and handheld devices are trying to make it easier to mobilize industrial-strength applications. Some are using a partner strategy, such as Siebel's with Antenna. But some analysts believe that in the next two years, most chores now handled by wireless application gateway companies will be folded into enterprise applications.

"Today, there are a lot of small vendors" in the gateway business, says Nick Jones, an analyst with Gartner. "Most will not survive in the long term. The functionality will get sucked into

## Special Report

larger apps. Oracle, IBM's WebSphere, SAP, Microsoft - they've all got some [wireless] functionality already, and that trend will continue, with wireless application gateways becoming part of the larger portal server software."

Hardware vendors have gotten in on the act as well. In June, Research In Motion (RIM) updated the development environment for its popular BlackBerry devices, adding extensions making it easier to integrate CRM and other enterprise applications with BlackBerry's existing functionality.

Dave Werezak, vice president of marketing at RIM, says that when customers seek to mobilize software, "We work with Siebel, or SAP, and so on, and depending on the nature of the app, help establish the connectivity on the server side."

### Pick the right app

Dennis Gaughan, an analyst at AMR Research, says corporate mobile deployments have tended to fizzle because they lack a persuasive business case. "This stuff is not for the faint of heart, so the application should offer significant return on investment," he says. "The problem is, most companies pick e-mail as their first [mobile] app, and it's hard to develop a business case for that. So people deploy wireless e-mail to a select group of executives - and that's where it stays."

According to an AMR report, "83% of companies report that their first mobile project - and often their last - is wireless e-mail access, which they choose . . . because it is an unambiguous application that is already widely adopted."

Despite this allure, e-mail usually turns out to be useless as a test bed for other mobile applications, says Gaughan, who co-authored the report. The cost is high (\$40 per month per user at some large businesses) and its benefits are almost impossible to quantify - not exactly a convincing formula for a pilot project.

You're most likely to show positive results (and persuade senior management that mobility is a worthwhile investment) if you select applications that directly affect your ability to serve customers, AMR found. This is why salesforce automation and field service are both popular choices.

In the first year, Pitney Bowes equipped its field service engineers with handhelds running a Siebel/Antenna application - inventory in the field dropped 15% and the number of expensive emergency orders to the company's central distribution center dropped 90%, Pitney Bowes' Nichols says.

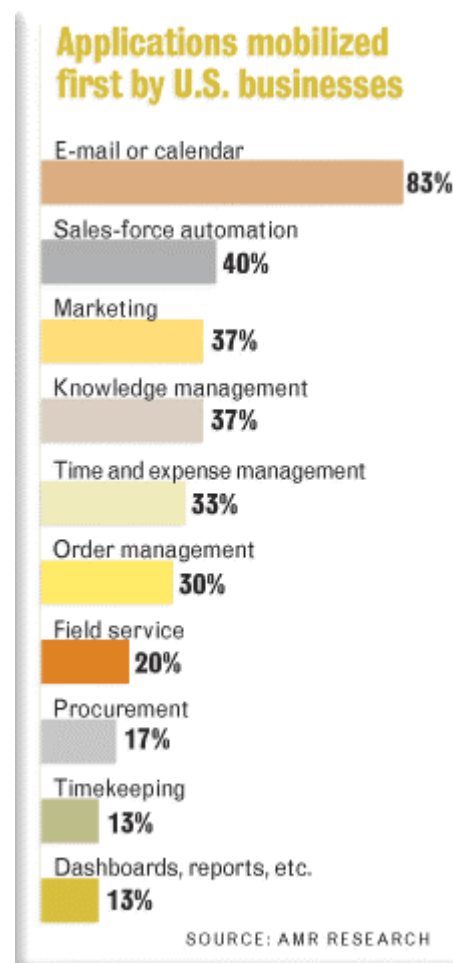
And according to J.C. Ehrlich's Norce, that company's technicians have significantly increased their number of daily appointments. These are the kinds of returns that persuade business executives to keep investing in mobilization.

### Be wary of wireless

Mobile applications that can be synched up with company servers a few times each day - perhaps even once a day - might work perfectly well (and are almost sure to cost significantly less). But companies tend to fall in love with the idea of real-time communication, and thus commit themselves to wireless without analyzing whether employees need the technology. This can lead to fiscal disaster.

According to Gaughan, one company interviewed by AMR had so much trouble implementing its wireless network that the cost of its mobile project eventually doubled initial forecasts. The problems revolved around ensuring network availability and security/authentication. Another company went through three different handheld devices, unable to find one that matched mobile workers' needs.

True, real-time communication - that is, a wireless network with automatic background synchronization - is expensive and complex. While AMR says this solution might be needed for global logistics and transportation workers, it might be overkill for other employees. For example, delivery drivers whose routes vary little probably



## Special Report

would need only a daily cradle-based synchronization.

Shell Pipeline, a subsidiary of Shell Oil Products, went through this decision-making process. Over the past three years, Shell Pipeline undertook an implementation of SAP's ERP system. Initially, the SAP didn't affect Shell Pipeline's field technicians; they continued to mail paper forms to headquarters, where the data was keyed in. This process was inefficient, and the data was spotty and old by the time it made its way into the database.

For a time, Shell Pipeline asked the field technicians to become proficient SAP users; they printed out their work orders at the beginning of the week, and manually entered data into SAP at the end of the week. While this improved the quality of the data, it cut into the field technicians' critical "wrench time." It also created an unhappy workforce; technicians had to work through more than 20 SAP screens to complete each report, and according to a Shell spokesman, they made no secret of their unhappiness with the system.

Shell decided to outfit the techs with handhelds and create applications that would let them enter work-order, inspection and status updates while in the field, and transmit the data to the SAP system.

The company first looked at wireless products for real-time communication, but decided public networks wouldn't support such an ambitious project, especially because the technicians are frequently in rural areas of California and Louisiana, where wireless simply won't work.

Shell settled on offline application access and cradle synchronization instead, using Telispark's mWorkManager and mInspect applications, as well as Symbol Technologies 8100 handheld devices - at the time, the only devices that were rugged enough for the company's needs. Telispark enables two-way communication between field technicians and SAP.

When technicians cradle their Symbol 8100s and transmit back to headquarters, data first goes through the Telispark server, then into the SAP system, updating records as needed. Next, information downloads from SAP, through the Telispark server and out to the field. Shell says the company built special firewalls and devoted massive attention to security protocols at the Telispark-SAP connection point.

J.C. Ehrlich is moving toward wireless, Norce says, but the company has become comfortable with using cradles. Technicians' devices run software that generates a text file and multiple database files. Through either a cradle or a wireless connection, the techs send their day's information to the company's AS/400, which splits the data and routes it to the appropriate application or database.

During the business day, customer service reps set up technicians' appointments for the next day. At night, that data is downloaded to handhelds.

### Don't overlook training

Training is a vital part of any mobile project because users often are reluctant to alter their work processes, and might resent the new technology. Shell Pipeline overcame this hurdle by selecting 40 volunteers (out of 300 technicians) to become "super users." The volunteers were trained on the Symbol handheld and the Telispark applications, then they trained their peers. Shell Pipeline says this peer training led to rapid acceptance of the mobile devices, though there are still a few diehards who want to write on the back of an envelope.

The company estimates it's cut down on field technicians' paperwork by 80%; saved the workers up to three hours per

**More going mobile**  
A recent survey by AMR  
Research found that  
**one-third**  
of enterprise employees can be  
classified as mobile.

Large Scale WLAN  
Connectivity.  
Taking The Wireless  
World Beyond Access.

**Chantry**  
NETWORKS

[Chantry Networks](http://www.ChantryNetworks.com)

## Special Report

week of paperwork prep time; and slashed six to eight hours of data-entry time per technician per week.

Once Pitney Bowes settled on Siebel and Antenna, the integration was “no different than anything else,” Nichols says. The non-technical facets of integration were more challenging, he adds. “We got the end-user community involved in explaining the world they live in. [IT] project team members went out to walk in users’ shoes for a day, and we had a lot of workshop sessions to talk about functionality.”

Gartner’s Jones says that steady technological improvements have pushed other challenges to the fore among companies considering mobile applications. For example, “Before mobility, [field service] engineers would come to a regional office in the morning to fill out forms, pick up new forms and chat around the coffee machine.” Equipping those engineers with wireless devices eliminates the need to visit that office daily, which would appear to be a good thing.

However, Jones says studies indicate that “the way field-service engineers learn to fix things is not to read manuals or bulletins - but to talk to each other at the coffee machine. Take that away and you’ve broken what sociologists call ‘the community of practice.’”

As mobile computing technology matures, you can expect these “soft” challenges to gain prominence. In a way, that’s good news - many of the technology challenges are now manageable, if you proceed cautiously.

*Ulfelder is a freelance technology and business writer in Southborough, Mass. He can be reached at sulfelder@charter.net.*

## WPA plugs holes in WEP

*New wireless security standard could drive hot spot, academic installations.*

**BY JIM GEIER**  
**NETWORK WORLD, 03/31/03**

The wireless LAN industry’s first crack at security - 802.11 Wired Equivalent Privacy - has been discredited and rightly so. WEP is so easy to break that it’s like having a plastic lock on your office door.

Although WEP can keep casual snoopers from accessing a wireless LAN, companies need and can do much better.

Effective wireless LAN security solutions, such as Cisco’s Lightweight Extensible Authentication Protocol (LEAP), have been in use over the past year, but they provide limited interoperability. In most cases, client radio cards and access points must be from the same vendor, something that doesn’t fare very well in public hot spots and many companies that don’t enforce a standard desktop.

Late last year, the Wireless Fidelity (Wi-Fi) Alliance announced Wi-Fi Protected Access (WPA), a standards-based security mechanism that eliminates most 802.11 security issues.

### WPA basics

WPA is based on the current state of the 802.11i standard, which is still under development. Ratification by the IEEE isn’t expected until late this year. The Wi-Fi Alliance, realizing that the long wait is stalling the market, launched WPA, which is expected in vendor products this spring.

One advantage of WPA is that it enables the implementation of open wireless LAN security in public areas and universities. These hot spots and academic sites haven’t been able to use basic WEP.

A key flaw in WEP is that its encryption keys are static rather than dynamic. That means to update the keys, an IT staffer has to visit each machine, which isn’t feasible in an academic setting or even possible in a hot spot. The alternative is to leave the keys unchanged, which makes you vulnerable to hackers.

These public sites haven’t been able to use the stronger proprietary mechanisms, such as LEAP, because of the interoperability issue.

But WPA provides effective key distribution and enables use across the often different vendor radio cards.

To ensure that WPA is taken seriously, the Wi-Fi Alliance has mandated that by year-end the security mechanism will be required for all new Wi-Fi certifications. It’s likely that WPA also will become the default out-of-the-box configuration, which would help the majority of small office/ home office (SOHO) users. Older products will not need to comply, but vendors surely will supply applicable upgrades.

### How WPA works

WPA includes both the Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms, which together provide dynamic key encryption and mutual authentication for mobile

## Special Report

clients. WPA thwarts hackers by periodically generating a unique encryption key for each client.

TKIP introduces new algorithms to WEP, which includes extended 48-bit initialization vectors and associated sequencing rules, per-packet key construction, key derivation and distribution function, and a message integrity code (referred to as “Michael”).

In companies, WPA can interface with an authentication server, such as Remote Authentication Dial-In User Service, using 802.1x with EAP. The authentication server is a storehouse for user credentials. This function enables effective authentication control and integration into existing information systems.

WPA implementations in SOHOs, however, don't require an authentication server because of the ability to operate in “pre-shared key mode.” Similar to WEP, a client's pre-shared key (often called a “pass phrase”) must match the one stored in the access point. An access point uses the pass phrase for authentication. If the phrase matches, the client is given access to the wired side of the access point.

WPA fixes all known problems with WEP, except denial-of-service (DoS) attacks.

Potential DoS attacks are a significant risk for any application where loss of wireless LAN access affects life, profits or reputation. A hacker easily can bring down a WPA-protected network by sending at least two packets using the wrong key each second.

When this occurs, the access point assumes that a hacker is trying to gain access to the network. The access point shuts off all connections for 1 minute to avoid the possible compromise of resources on the network. Thus, a continuous string of unauthorized data can keep the network from operating indefinitely, which means you should have a back-up process ready for critical applications.

### Implementation considerations

WPA is primarily a solution for legacy equipment because you can install WPA via simple software upgrades to your Wi-Fi-certified access points. This enables effective security among clients having different radio cards, assuming the radio cards also implement WPA. Access points that implement WPA will support a mixed environment of client devices, ones implementing WPA and others that don't.

WPA will maintain forward compatibility with the 802.11i standard. The eventual 802.11i standard will include Advanced Encryption Standard (AES) as an option, which is stronger than RC4. But an issue is that AES will likely require the replacement of a legacy access point because of the need for higher performing processors. As a result, 802.11i will be targeted for new equipment.

### Evolution of wireless LAN security

WEP goes the way of the dodo bird, WPA emerges as missing link to 802.11i

Name	Wired Equivalent Privacy	Wi-Fi Protected Access	802.11i or Wi-Fi Protected Access Version 2
Acronym	WEP	WPA	WPA2
A.K.A.	Won't Even Protect	Will Protect Alright	Will prove airtight
Features	Weak encryption keys based on RC4 algorithm (typically 40-bit keys).  Static keys that make easy targets for hackers	Same underlying RC4-based encryption as WEP  TKIP (temporal key integrity protocol) added so that keys are rotated and encryption is strengthened.	Strong AES encryption based on Rijndael algorithm (128, 192 or 256 bit key sizes).  Adds two strong authentication features: wireless robust authentication protocol or WRAP; counter with cipher block chaining message authentication code protocol or CCMP.
Life span	1997-2003	2003-2004	2004-??????

## Special Report

### Is WPA an interim step or a long-lasting solution?

WPA can provide excellent security. The demand for compliance from the Wi-Fi Alliance assures users of plug-and-play security that has been a real roadblock to wireless LAN proliferation.

Customers should implement WPA through upgrades to existing equipment and should insist on it in new equipment. Because of new hardware requirements of 802.11i, WPA will likely be a security solution that lasts until you move to the next generation of hardware.

*Geier provides independent consulting services to companies developing and deploying wireless network solutions. He is the author of the book, Wireless LANs. He can be reached at jimgeier@wireless-nets.com.*

### A switch in time

*Wireless LAN switches could drive 802.11 rollouts to the next level.*

**BY NANCY GOHRING**  
**NETWORK WORLD, 05/19/03**

The wireless LAN switch is emerging as the missing piece that will let wireless networks scale beyond the small workgroup to full-blown enterprise implementations.

Until now, WLANs consisted of a client connecting to access points crammed full of security, management and other intelligence required to control the wireless portion of the network. The problem is that managing multiple access points was an unwieldy prospect for enterprise deployments that could include hundreds or thousands of access points.

Furthermore, installing access points has been a headache. Many companies hire consultants to conduct site surveys and radio frequency planning to determine the best place for access points. That's expensive. Also, WLANs initially offered such poor security that some IT managers have outright banned them in their offices.

It all adds up to lots of interest and lots of pilot projects, but not very many enterprisewide rollouts. "Right now, it's really been mainly trial deployments," says Russ Craig, research director for Aberdeen Group.

An array of point products have hit the market over the past couple of years aimed at solving these problems. But that means if IT departments need more than one of those prod-

ucts to solve multiple problems, they have to become system integrators, something few departments have the budget or manpower to do.

Enter the WLAN switch. "The conclusion a bunch of folks came up with is that you make the access point a less intelligent device, and you enable a switch or a router to communicate with all the access points," Craig says. "That way you can manage them remotely and configure them from a central panel." Most new products also deliver power over Ethernet to the switches instead of requiring AC power.

Combined, these features will enable less expensive and easier deployments, which could provide a huge boost to the WLAN market. "The uptake is going to be significant," Craig says.

The term switch is a bit of a misnomer, because while the WLAN switch offers similar management and control functions as a wireline switch, it doesn't do so on a port-by-port basis and it doesn't provide dedicated bandwidth to an end user. An exact parallel essentially would require dedicating a single blast of wireless coverage per user. Until that happens, the term switch will have to suffice for the current generation of product.

Start-ups and old timers in the networking and wireless worlds are flocking to the wireless switching market. The list includes AireSpace, Aruba Wireless Networks, Chantry Networks, Legra Systems, Nortel, Proxim, Symbol Technologies, Trapeze Networks and Vivato. Although each aims to solve the



**Wireless Wizards**  
Got a wireless LAN question or problem?  
Ask our Wireless Wizards at  
[wireless\\_wizards@nwfusion.com](mailto:wireless_wizards@nwfusion.com)

[Network World](#)

## Special Report

same set of problems, they do so slightly differently, and while all but Vivato dumb down their access points, they do so to different degrees.

### Dumbing down

"We're trying to drive the commoditization curve down so an access point becomes as cheap and mindless as an Ethernet port on your wall so you can put them wherever you need them," says David Callisch, marketing director for Aruba. Aruba's access point is light but not totally empty - it does air monitoring to watch for rogue access points.

Trapeze also doesn't completely strip all intelligence from the access point. "From a control and management aspect, we have a thin [access point]," says George Prodan, vice president of marketing for Trapeze. But Trapeze access points handle packet processing functions such as encryption/decryption and quality of service.

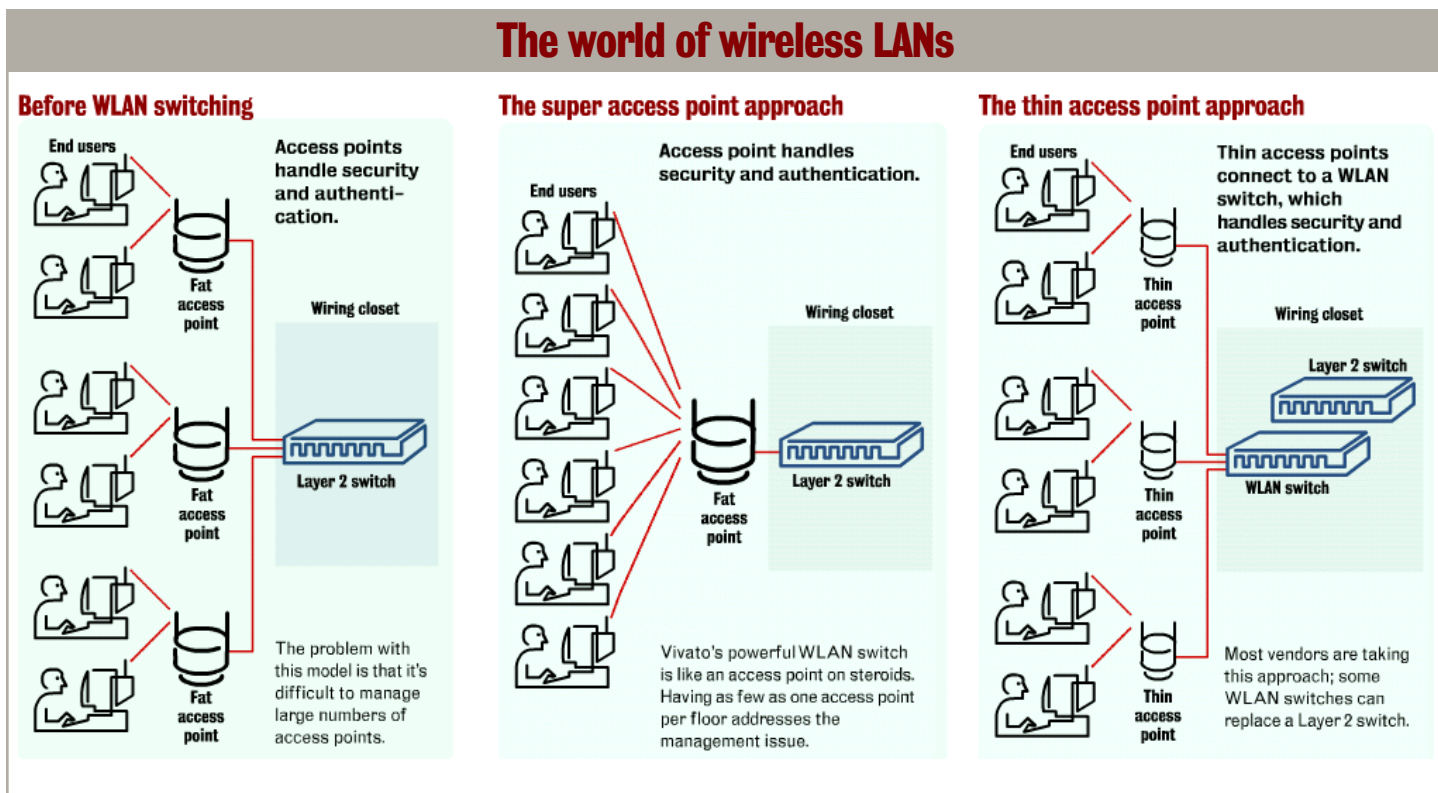
Symbol offers some of the most stripped down access points on the market, comprised of power over Ethernet capability, an omni-directional antenna and the 802.11b radio.

Vendors also are differentiating themselves by the degree to which they upset existing systems. The ideal solution integrates the WLAN with existing wired networks so companies can continue to take advantage of previous investments. All the vendors support that philosophy, but they ask for some level of upheaval. At the very least, they push customers to use their access points to get the best performance.

### Standing out

With so many start-ups attacking the same market, the pressure to stand out from the crowd is intense. Aruba says it hopes its flexible architecture will attract customers. Users will have the option of placing the Aruba switch in the wiring closet with existing Layer 2 switches or centralizing the switch in the data center.

Where the WLAN switch sits might be a crucial selling point for many customers. Sarah Kim, an analyst for The Yankee Group, says that asking customers to replace an existing switch will be a tough sell. "There's no way anyone in this market will go to a prospective customer and say, 'Take this out of your closet,'" she says.



## Special Report

But Proxim does just that. Proxim's Maestro switch will replace an existing Layer 2 switch, handling wired and wireless switching in a single box. "Maestro is truly an Ethernet switch," says Georgeanne Benesch, vice president of product management at Proxim. "What we've done is added functionality to a switch to enhance it for wireless."

Still, Proxim says it thinks it has the lead on competitors because Maestro builds on the experience of Proxim's first-generation product, Harmony. Three years ago it started shipping Harmony, which centralized WLAN systems, but wasn't a full switch.

Each vendor has a heavy focus on security, offering solutions to address security at all layers. They all support 802.11 standard security mechanisms including Wi-Fi Protected Access and 802.1X, and multiple virtual LANs.

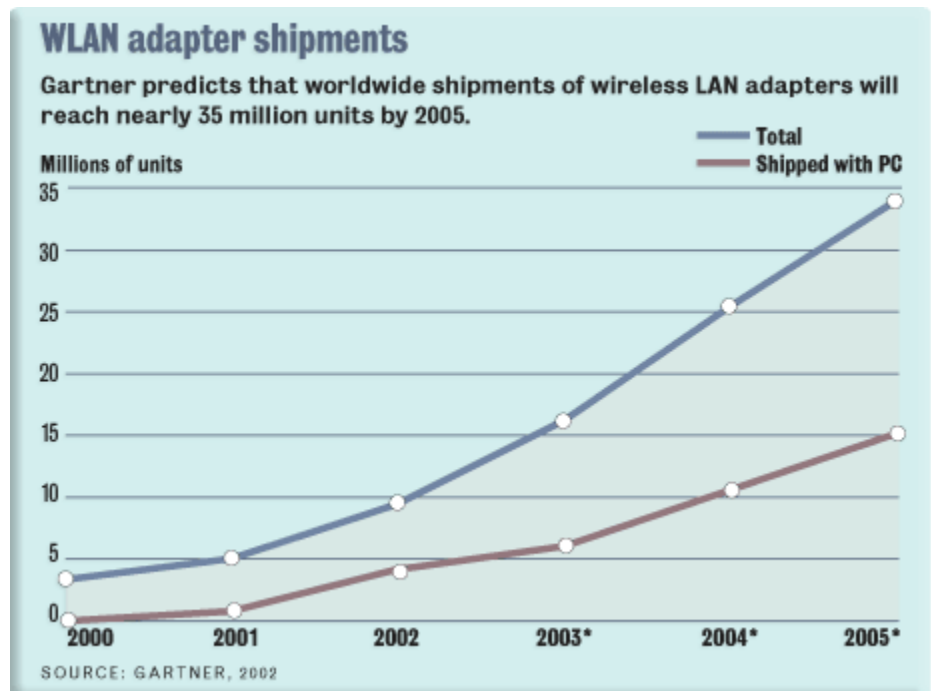
Trapeze is unique in that it doesn't support VPNs because it says the setup and tear down time is too long to allow quick enough handoffs to support voice services. Instead, Trapeze offers a variety of techniques that can encrypt transmissions over the air because the encryption happens at the access point. "It's much more powerful than a VPN termination in the switch, which leaves the rest of the connection in the clear," Prodan says. "Our wireless solution is more secure than the wired" network at most corporations, he says.

### Outing rogues

The way each company handles rogue access points also is worth looking at closely. Aruba's access points scan the air so that the switch can see illegal associations. The switch can send a message to a nearby authorized access point, which disconnects the client associating with the rogue access point.

Symbol's client devices look for unauthorized transmissions over the air, reporting that data back to the access points. "We make cooperation a whole solution, not just in the infrastructure," says Ray Martino, vice president and general manager at Symbol.

AirFlow's approach to rogue access points is unique because of the way it handles media access control (MAC) addresses. In a typical WLAN network, each access point has its own MAC that associates with the user's client. In an AirFlow network, the client associates with a single MAC that sits in the switch. The



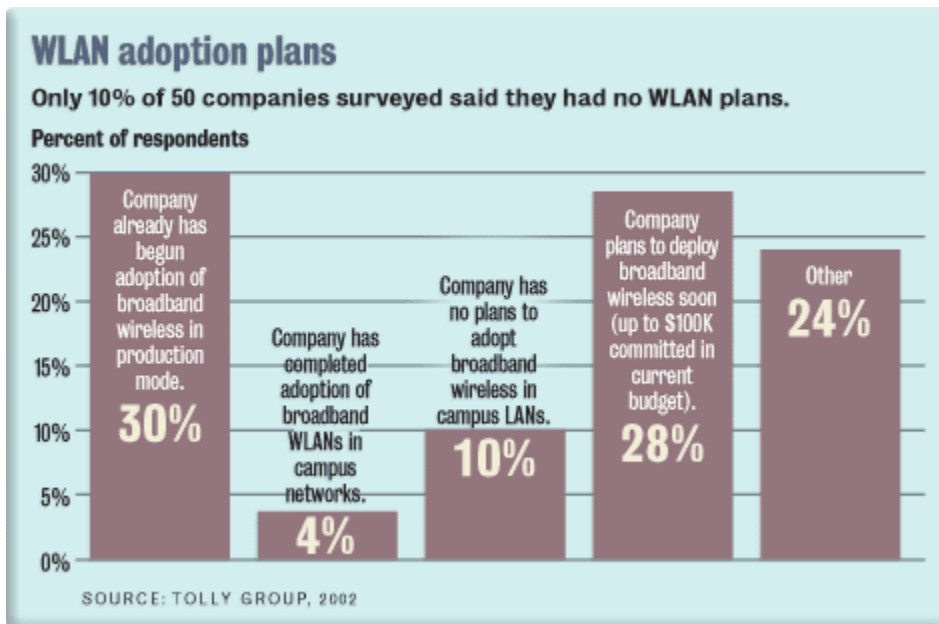
architecture makes roaming easy because reassociation isn't necessary when a user moves from one access point to the next because the MAC never changes. It also eliminates interference issues because each access point can operate on the same channel. "It's the networking effect as opposed to taking isolated environments and pulling them together," says President and CEO Robert Machlin.

Machlin says his competitors are providing a Band-Aid solution that connects isolated access points. Instead, Airflow redefines the shape of the network by centralizing the MAC function into the switch "so that the access points are nothing more than extension cords," he says.

One MAC address helps with security. Rogue access points can't connect to the network because they won't have the same MAC address as the rest of the WLAN network.

Customers could use different channels with AirFlow's solution, but they would do so to serve their own purposes. For example, they might want to tune the access points that serve one department to a different channel than the one next door.

AireSpace, which has deployed its platform at the Duke University Medical Center in Durham, N.C., and the University of California at Berkeley school of electrical engineering and computer science, focuses on ease of setup and operation, as well as security.



“We put a lot of energy into building a system that mediates the [radio frequency] environment automatically,” says Alan Cohen, vice president of marketing for AireSpace. The system includes tools for load balancing, interference management and dealing with rogue access points.

## Going outdoors

Vivato has created a buzz with an unusual approach that puts it in a category of its own. Vivato’s offering uses smart antenna technology to address the radio frequency shortcomings of current Wi-Fi systems. Instead of spewing radio signals out over 360 degrees, Vivato antennas focus three parallel narrow beams on clients that are using the connection. Because it focuses on narrow areas, power is concentrated and the beam can cover a greater distance than traditional access points. Even though the Vivato system complies with the 802.11 standard, the antenna can reach as far as 900 feet, replacing eight to 12 access points, Vivato’s Phil Belanger says.

Still, Vivato’s switches, which usually are located on each floor of an office building, must each be updated individually because all the intelligence is in the same box as the antenna and radio. Vivato has introduced an auxiliary product that ties each switch to a single management point.

Vivato also is unique in that it is selling an outdoor switch that can beam 802.11b signals over distances of up to 3,200 feet. This

switch could be used on a college campus, in a downtown area or even to blast wireless connectivity from one building to another without having to install access points inside.

The WLAN switch space isn’t just for start-ups, however. Nortel recently jumped in the game with a product it refers to as a security switch. Nortel’s main goal with the switch is to let customers administer one security policy that operates across wired and wireless networks.

“You can get to one security manager and define a policy and apply on all subsystems in a consistent and easy fashion,” says Atul Bhatnager, general manager for Nortel’s Ethernet switching business.

Another category of vendors makes hubs that they say can perform all the same functions as WLAN switches. Vernier Networks offers a hub connecting access points from any vendor. Bluesocket and ReefEdge fall into the same category. Bluesocket also has announced a “switch wireless gateway” that combines its existing gateway functionality with switching.

Each player in the WLAN switch space brings a slew of capabilities that each thinks will be most important to customers. But the introduction of products is really just an opening salvo. “WLAN is a relatively immature technology,” Symbol’s Martino notes. “The feature battle will go on forever.”

*Gohring is a freelance writer. She can be reached at nangohring@yahoo.com.*

© 2003 Network World, Inc. All rights reserved.



**Request Reprint**

[Request a reprint of this report.](#)