

WIRELESS

Enabling Enterprise Wi-Fi

Lisa Phifer

Security and management concerns persist, but it's probably only a matter of time before the technology becomes ubiquitous.

The 802.11 Wi-Fi market is booming, but enterprise adoption still trails SOHO uptake. According to market research from the Dell'Oro Group, residential players Cisco Linksys and D-Link led the overall Wi-Fi market last year, dominating third-place Cisco Aironet, the Cisco division that manufactures the best-selling enterprise offering.

Most analysts expect enterprise adoption to accelerate, and soon. Infonetics Research predicts that enterprise WLAN purchases will top \$1.7 billion by 2006, more than doubling the \$702 million consumer wireless LAN (WLAN) market.

Enterprise sales to date actually reflect widespread but extremely shallow Wi-Fi deployment. For example, a December 2003 Webtorials poll showed that 53 percent of enterprises have already deployed WLANs. However, only about one-third of those early adopters now support more than 100 users.

Clearly, many enterprises are still dabbling in Wi-Fi, delivering limited wireless services to small target areas or workgroups. What will it take for these companies to pull the trigger on Wi-Fi deployment, rolling out 802.11 on a broader scale?

Why Wi-Fi?

For starters, enterprises must see tangible return-on-investment (ROI) from Wi-Fi deployment. Some companies are not yet convinced that wireless is necessary in the workplace. Research by International Data Corp. (IDC) conducted in March indicated that 38 percent of enterprises surveyed did not perceive a real need or business value in WLAN deployment. Lack of business justification also placed second in deployment barriers identified by a poll of NetWorld+Interop 2004 attendees, conducted by the show's organiz-

er, MediaLive International (which also owns BCR).

Before dismissing these enterprises as behind-the-curve or short-sighted, consider this: Wi-Fi just might not be required by everyone, *everywhere*.

In fact, vertical markets where Wi-Fi now enjoys significant deployment have applied wireless to specific use cases: point of sale systems in retail establishments; inventory tracking in warehouses; patient data access in health care facilities; and Internet access on college campuses.

Enterprise Wi-Fi deployment may follow suit. According to Sage Research, the most common enterprise wireless users last year were highly-mobile employees like field service and sales. This year, enterprise Wi-Fi is spreading gradually to marketing, operations and other departments.

Few companies would (or should) consider ripping out existing infrastructure for wholesale replacement by wireless. Instead, most will pursue selective Wi-Fi deployment in places where they'll get the biggest bang for their buck. For example:

Executive Summary

Wi-Fi is one of the hottest technologies in enterprise networking, but actual adoption has not been as pervasive as one might believe. A number of issues have combined to make IT managers cautious about rolling out Wi-Fi ubiquitously.

Many are still concerned about security, and even where security is implemented, such implementation can be highly complex. Tools are still being developed to assist enterprises in large-scale deployment, management and monitoring of Wi-Fi systems.

Companies must also tackle the issue of how to scale Wi-Fi networks from today's broad-but-shallow deployments to corporate campuses where wireless access is ubiquitous. Standards are continuing to evolve in these and other areas, creating a moving target for investment in Wi-Fi hardware and software.

The bottom line: wireless LAN deployment may not yet be simple, but a wide variety of products and techniques is available today or will be available by the end of this year to address the concerns that trouble most IT administrators □

Lisa Phifer is vice president of Core Competence, Inc., a network security consulting firm based in Chester Springs, PA.

As WLANs get larger, they become more difficult to configure, monitor and tune

■ **LAN Extension:** According to polls, increased productivity is the top motivation for deploying Wi-Fi in the workplace. To let workers reach intranet systems and data when away from their desks, coverage is often provided in conference rooms, cafeterias and other “hotspots” where employees congregate. But providing ubiquitous coverage throughout the campus is more expensive and challenging, and the incremental value may be less clear.

■ **Temporary Access:** An oft-cited Wi-Fi benefit is its ability to facilitate moves, adds and changes. According to Webtorials, a wired Ethernet drop runs about \$150. WLAN adapter prices have fallen below \$50. Providing network access to a contractor or visitor can be accomplished faster and cheaper with wireless. New workspaces can be created rapidly in any open area, using wireless for network access, edge-to-core backhaul or both.

■ **Voice over Wi-Fi:** Polls suggest that somewhere between 20 and 30 percent of companies hope to save money by running voice over WLAN (VoWLAN). Voice over IP (VOIP) promises to displace traditional enterprise telephony by leveraging existing IP networks to carry voice, video, and data services, and Wi-Fi extends VOIP services to in-building mobile handsets. Indeed, VoWLAN may be the carrot used to justify ubiquitous Wi-Fi deployment, since spotty coverage is a deal-breaker for telephony—it must be all or nothing.

■ **Traveler Access:** Enterprise Wi-Fi usage isn't limited to in-house WLANs. Public Wi-Fi “hotspots” are readily available at many airports, hotels, business centers, cafes and other venues frequented by business travelers. Even companies with limited on-premises deployment may support road warriors by paying for Wi-Fi adapters and services and hotspot security measures. Here again, the corporate payback is increased productivity when travelers turn down-time into work-time.

Beating The Barriers

Michelle McLean, director of product marketing for Trapeze Networks, is seeing more horizontal deployment by enterprise customers this year. “Employees are going to [install WLANs] for IT if they [the IT staff] don't get on the ball,” said McLean. “Are the floodgates opening? I don't think we're there yet. But this will be the year when issues are finally solved and companies start asking about the benefits.”

However, even when the benefits are clear, the road to reaping those rewards may not be. Early Wi-Fi adopters encountered both expected benefits and unexpected barriers.

Wireless insecurity is (still) the top concern. Wi-Fi Protected Access (WPA) greatly diminished WEP cracking threats last year. Nonetheless, a recent Fortress Technologies poll found that

63 percent of CIOs and technology managers still do not believe 802.11 devices can provide adequate security. A recent Network Computing poll indicates that security *complexity* has now become the primary WLAN deployment barrier.

As WLANs get larger, they become more difficult to configure, monitor, and tune. Performance and management barriers placed second and fourth, respectively, in Webtorials' “2004 WLAN State of the Market” survey. Enterprises have spent more than a decade refining wired network infrastructure; we shouldn't expect WLANs to require less. Enterprise-class management systems and tools must be adapted and extended to address the unique challenges posed by wireless.

Uncertainty over standards may be stopping some companies from purchasing Wi-Fi products in volume. Advances like 802.11g and 802.11i have improved speed and security, but require new hardware. Retiring a few trial access points (APs) is one thing; replacing an enterprise-wide AP rollout is quite another. Until the standards wheel stops spinning, how can you be sure that what you buy today won't gather dust tomorrow? Enterprises need equipment that's field-upgradeable, to protect their investment.

Fortunately, new standards and emerging technologies for scalable enterprise WLAN security, performance and management are now dissolving the barriers.

Tightening WLAN Security

According to the Wi-Fi Alliance, more than 400 products now support Wi-Fi Protected Access, and WPA is required in all Wi-Fi certified products. WPA mitigates vulnerabilities associated with Wired Equivalent Privacy (WEP), the broken encryption used in earlier products. WPA uses RC4 with temporal keys (TKIP) and message integrity checks (MIC) to prevent data forgery, insertion, and “WEP cracking” over the air (see *BCR*, May 2003, pp. 42–46).

This June, the IEEE ratified the long-awaited 802.11i, a new standard for Robust Security Networks (RSNs) that use 802.11a, b, or g radios. The Wi-Fi Alliance expects to begin certifying 802.11i products in September of this year under the brand “WPA2.” As the name suggests, WPA2 is a superset of WPA. It adds a stronger, more computationally efficient alternative for confidentiality and integrity: the Advanced Encryption Standard (AES), used with the CCM protocol (CCMP) defined by RFC 3610 (Table 1).

Two years ago, TKIP was launched as an interim solution for legacy equipment, improving security while AES standards progressed for next-generation hardware. But over the past year, many WPA products have incorporated both TKIP and draft AES. Therefore, APs purchased recently—particularly enterprise APs from vendors like Cisco, Trapeze Networks and Airespace—will be field-upgradeable to WPA2. PC cards using recent

TABLE 1 Comparing WEP, WPA And WPA2

	WEP	WPA	WPA2
Confidentiality	RC4 with WEP 24-bit IV 40/104-bit Key	RC4 with TKIP 48-bit IV 128-bit Key	AES-CCMP 48-bit IV 128-bit Key
Integrity	CRC	Michael 64-bit Key	CBC-MAC 128-bit Key
Authentication	Optional Shared Key	PSK (Personal) 802.1X (Enterprise)	PSK (Personal) 802.1X (Enterprise)
Dynamic Key Delivery	None	EAP-based	EAP-based
Pre-Authentication and Key Caching	No	No	Yes
BSS Support Infrastructure Mode	Yes	Yes	Yes
IBSS Support Ad Hoc Mode	Yes	No	Yes
Standard Completed	1999 Part of 802.11	October 2002 Snapshot of 802.11i	June 2004 Final 802.11i
Certified Products	March 2000	April 2003	Sept 2004 (projected)

“Existing solutions to security and authentication are more complicated than the problem itself”

chipsets (e.g., Atheros) may also be firmware-upgradeable. However, laptops with embedded 802.11b (e.g., Centrino) are still likely to require new hardware for WPA2.

In short, we can now stop waiting for 802.11i and strong link layer security. Equipment purchased in late 2004 and beyond should include robust, efficient airlink confidentiality and integrity, suitable for enterprise use. Features to assist with WEP-WPA-WPA2 transition, like multiple SSIDs and VLAN support, are also becoming common in enterprise-class APs.

Controlling Network Access

Data protection is just one piece of the puzzle. Preventing unauthorized network use is another piece, and one that's proven harder to solve.

WPA (and soon, WPA2) are provided in two forms: WPA-Personal and WPA-Enterprise. WPA-Personal uses a group passphrase (pre-shared key) to authorize WLAN access. Group passwords are simple and satisfactory for SOHO use, but most businesses require stronger individual user authentication. WPA-Enterprise uses 802.1X Port Access Control to provide the level of individual user authentication and authorization required in corporate networks.

However, 802.1X is no slam dunk to deploy. It requires infrastructure (RADIUS), client software (called Supplicants), and complex configuration. Supported authentication methods depend upon the Extensible Authentication Protocol (EAP) used with 802.1X. Since the 802.11i standard doesn't mandate one EAP type, that choice is left to each enterprise.

A year ago, vendors seemed to be converging on one or two EAP types capable of meeting most enterprise needs. Supplicants supporting EAP-

Transport Layer Security (TLS) and Protected EAP (PEAP) were embedded in new operating systems and Wi-Fi adapters to simplify administration. Ubiquitous 802.1X support appeared to be falling into place.

But today, there's still a tangle of inter-dependencies among EAP types, servers, databases and supplicants—it can be complicated to select exactly the right combination, given your operating system, interface card and access points. EAP-TLS hasn't caught fire, PEAP has diverged into two incompatible Supplicants, and new EAP types have been proposed for faster cross-network roaming. EAP types must stabilize and implementations must converge before enterprise 802.1X deployment can become widespread.

New products and services have emerged to fill this gap, finding innovative ways to strengthen business WLAN security with reduced complexity. Approaches include:

■ **Adopt An Alternative:** According to Tony Fascenda, CEO of KoolSpan, a WLAN security vendor. “Existing solutions to security and authentication are more complicated than the problem itself.” Fascenda believes enterprises need more effective and intuitive solutions. KoolSpan sells SecurEdge, a hardware lock-and-key system that provides transparent bridge-mode AES link layer protection.

Similarly, Fortress Technologies sells Air-Fortress, a Federal Information Processing Standard (FIPS)-certified link layer solution that combines gateway hardware and client software. Products like these employ simple but strong alternatives to 802.1X, like USB smart cards (KoolSpan) and tri-level symmetric keys (Fortress).

■ **Off-Load Administration:** Companies that

**WLAN
misconfiguration
will be the culprit
in 70 percent of
successful
attacks**

don't want to create an 802.1X infrastructure can pay someone else to do it. For example, Wireless Security Corp. offers an Internet-based 802.1X managed authentication service. Interlink recently announced LucidLink, which is turnkey 802.1X software that automates security configuration on all three pieces (client, AP, server). Products like these can be used by larger companies, but are really focused on SMBs that lack the infrastructure and expertise to handle 802.1X.

■ **Extend Your VPN:** Many companies already use VPNs for remote access. Leveraging those VPNs to secure WLAN access sounds sensible; re-using existing infrastructure should reduce total cost of operation.

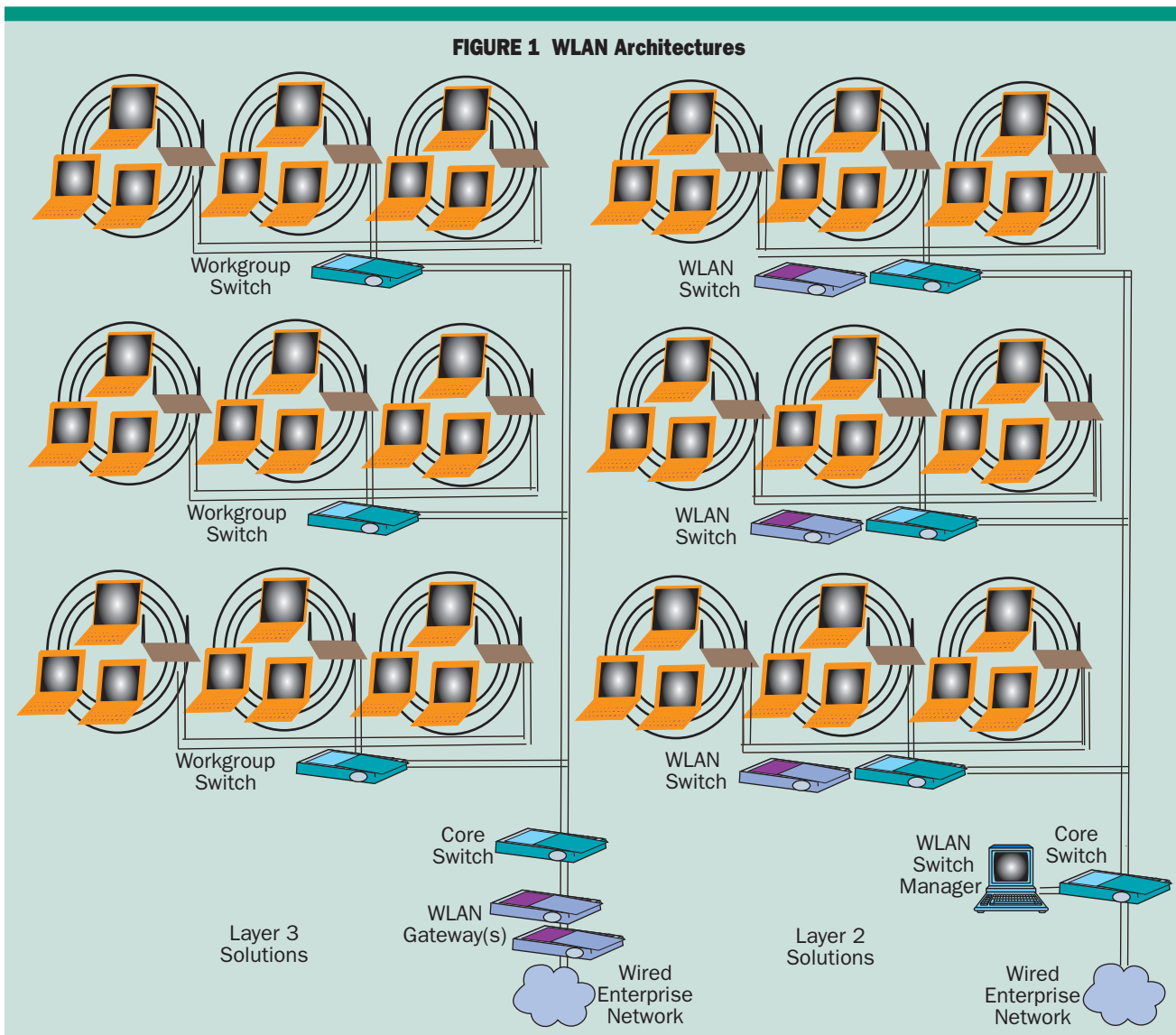
Unfortunately, Wi-Fi devices roam, and even brief loss of signal wreaks havoc on VPN tunnels. To make tunneling over Wi-Fi reliable, many WLAN vendors now support subnet roaming. For example, Trapeze's Mobility System provides session persistence when a user roams to an AP in the same or different subnet. All

Mobility Exchanges within a Mobility Domain share identities and session state to keep users authenticated and VPN tunnels connected when devices roam.

Improving Manageability

Gartner predicts that WLAN mis-configuration will be the culprit in 70 percent of successful WLAN attacks. As enterprise Wi-Fi usage grows, IT departments will require automated, centralized management to reduce error and manage large networks cost-effectively.

"If you're looking at thousands of devices, you're not going to go out and touch all those devices to apply policies," said Eric Hermelee, VP of marketing at Wavelink, which has been selling wireless management software since 1992. "The challenges were different then: [products were] proprietary, less mature, less fast, less robust." Today, companies like Gap and Barnes & Noble use Wavelink's Mobile Manager to manage 802.11 networks with thousands of APs.



Hermelee slices WLAN management into configuration, monitoring, security, and maintenance. "Security tends to be the catalyst for defining and enforcing consistent policies throughout the network because of some type of mandate," he said. "Not far behind is configuration. IT doesn't want to staff up a new group to manually manage the WLAN extension of their existing network. The next order of business [is] how well is [the WLAN] doing?" Automated maintenance is then needed to keep up with new firmware and drivers.

Enterprise-class WLAN management tools have emerged from a variety of sources.

Companies like Wavelink, Perfigo and Airwave offer third-party WLAN management solutions. Third parties typically use agent software on stations and AP administration interfaces to provide overlay management that's Wi-Fi aware but station/AP vendor-neutral. For example, Wavelink Mobile Manager uses data extracted from APs, switch and router tables, and Wavelink's Avalanche client.

Traditional management players like Hewlett-Packard, IBM and CA are also moving to integrate WLAN management. For example, Trapeze's WLAN Mobility System has an HP OpenView plug-in for centralized control and monitoring. But tools like Trapeze's RingMaster are still needed for Wi-Fi-specific tasks like site survey, capacity calculation and coverage verification. Wavelink also has an OpenView plug-in for Mobile Manager. "We're just starting to see customers that try to tie these [element and network managers] together," said Eric Hermelee.

Enterprise-class AP vendors like Cisco and Proxim have long provided SNMP interfaces for element management. Over the past year, WLAN switches have gone farther (Figure 1). Companies like Airespace, Aruba and Trapeze now sell distributed systems composed of APs, L2 switches or L3 gateways, and management servers. These components are tightly coupled, so planning, configuration and monitoring tasks are more easily automated. For example, Trapeze's RingMaster allocates channels and calculates power settings, generating configuration files pushed to all Mobility Points (APs).

In fact, WLAN switches have generated industry debate on the appropriate placement and distribution of management and data path functions. "Fat APs" push management processing to the network edge, while "thin APs" depend on tightly-coupled WLAN switches to configure and monitor them. This "fat/thin" dividing line, which was never entirely precise, has been further blurred by Cisco's recent entry into the WLAN switch market.

The vendor's Structured Wireless Aware Network (SWAN) framework bundles Cisco's Aironet, CiscoWorks WLAN Solution Engine (WLSE), Cisco Access Control Server (ACS) and

Cisco Catalyst products into an architecture that treats Wi-Fi as an extension of the overall network. SWAN does include some WLAN-specific features—for example, aggregate radio management and rogue AP detection. But overall, SWAN adds bits and pieces of Wi-Fi awareness to existing Cisco network infrastructure, rather than creating a separate WLAN with its own management tools.

Monitoring More Effectively

Monitoring is one area where wireless and wired networks tend to require very different approaches and tools. Wireless network composition and usage is highly dynamic. Watching traffic from the wired side of authorized APs, while useful, is simply not enough.

More than 16 million laptops with embedded Wi-Fi were purchased by businesses in 2003. By next year, Wi-Fi will be standard in virtually every laptop sold. With Wi-Fi turning up everywhere, it can be hard to differentiate between visitors and malicious attackers. Companies with WLANs must stop visitors from accessing private resources, and prevent employees from connecting to neighbor or rogue APs.

Even in companies without WLANs, workers who use Wi-Fi at home can accidentally connect to unauthorized APs in or near the office. The only way to detect and prevent these problems is to watch what's happening over the air.

Today, WLAN monitoring tools fall largely into three categories:

- **Portable 802.11 traffic capture and analysis tools**, sold by companies like AirMagnet, Berkeley Varitronics, Network Instruments, Sniffer and WildPackets, are commonly used for tasks like site surveys, rogue AP spot-checking, as-needed intruder investigation or network troubleshooting.

- **Standalone wireless intrusion detection systems (WIDS)** are available from some of these same WLAN analyzer vendors, plus WIDS specialists like AirDefense, Network Chemistry and Newbury Networks. WIDS products use fixed-position sensors for 24/7 passive capture, feeding traffic summaries to a central server for storage, analysis, alerting and reporting.

- **Integrated WIDS** features are provided by many WLAN switch vendors, leveraging the existing communication path between paired APs and switches to detect the presence of rogues and other security and performance events.

Many companies will combine approaches—for example, using a WIDS for full-time network surveillance and a handheld WLAN analyzer for in-depth investigation of high-priority alerts. Products in all three categories are quickly growing in depth and sophistication to keep up with enterprise needs. For example:

—AirMagnet recently added mobile support for troubleshooting new EAP types, like Cisco's EAP-FAST.

The battle over "fat" vs. "thin" APs has further complicated the picture

Large networks also require more sophisticated tools for site surveying

—WildPackets recently added voice over IP (VOIP) analysis to AiroPeek NX to assist with VoWLAN deployments.

—Newbury Networks' Wi-Fi Watchdog provides location detection with an 802.1X-based feedback loop that enables/disables WLAN access based on physical location.

These are but a few of the many 802.11-specific monitoring tools that enterprises will come to expect and rely upon when deploying large-scale WLANs.

Planning For Performance

Security problems may be apparent in small trial deployments, but performance challenges do not surface until usage grows. Consider how APs installed in empty conference centers tend to work just fine until attendees arrive *en masse*.

Handheld WLAN analyzers can be used to conduct site surveys, recording signal and noise measurements at regular intervals throughout any area that requires Wi-Fi coverage. In smaller WLANs, a planner can use measurements to manually plan AP placement, channel allocation and power outputs to provide adequate coverage while avoiding cross-channel interference.

In larger networks, more sophisticated tools are required to assist with the site survey process, automatically generating coverage maps on floor plans, optimizing parameter settings, and supporting "what if" analysis. Products that can support these kinds of enterprise WLAN planning tasks include AirMagnet Surveyor, Berkeley Varitronics Systems Bird's Eye and Trapeze RingMaster.

According to Trapeze's Michelle McLean, RF management capabilities are essential. "Do you have a way to really visualize the air?," she asked. "A .JPG image [of your office] is not a floor plan." McLean argues that a floor plan must be tied to the physical environment, incorporating actual obstacles and their RF characteristics: "Larger deployments require the sophistication of spectrum management."

Pre-deployment site surveys are essential, but post-deployment change is certain to follow. Some WLAN switch systems can dynamically adjust output power to respond automatically to changing conditions, like AP failure or a sudden surge in demand. But McLean argues that dynamic power control is tough to perform effectively.

"You don't want power changes to be rapid," said McLean. "[That would be] like route flapping. You need a client feedback loop [like that under development in 802.11k, Radio Resource Measurement Enhancements] to do this right." Instead, Trapeze RingMaster provides one-click channel/power replanning to strike a balance between automation and IT control.

Adding Capacity

As enterprise WLANs grow, so will capacity demand. In the U.S., 802.11b and g are limited to

three non-overlapping channels. The new 802.11a offers up to 12 non-overlapping channels, depending upon indoor/outdoor environment. Spectrum reallocation may provide additional capacity by increasing the number of available channels, but many vendors are looking beyond these standards.

One possibility is to use available capacity more effectively by controlling quality of service (QOS). Like 802.11i, the IEEE 802.11e standard for QOS has progressed more slowly than most vendors had hoped. To address need for interoperable QOS controls before 802.11e reaches maturity, the Wi-Fi Alliance plans to certify a snapshot of 802.11e, branding the effort Wireless Media Extensions (WME).

WME lets Wi-Fi devices request high priority for some traffic—for example, giving VOIP priority over email. However, WME can't guarantee that any device will have priority over other devices. To let APs guarantee bandwidth to specific devices, the Wi-Fi Alliance expects to certify another QOS approach, Wi-Fi Scheduled Media (WSM), in mid-2005.

Another possibility is to increase data rates by changing the way channels are used. Like hubbed Ethernet, 802.11 channels are shared by all stations associated to a given AP. Despite the moniker, WLAN switches don't dedicate links to stations like Ethernet switches do. But new Multiple Input Multiple Output (MIMO) antennas can. MIMO takes advantage of an RF phenomenon called multipath, in which signals from a given source bounce off obstacles. APs can sample signals arriving from each device and choose the best path for communication. MIMO uses this technique to improve the performance experienced by each device without requiring additional channels (see *BCR*, May 2004, pp. 20–22).

Early MIMO products are expected to ship late this year; for example, Airespace expects to release its Intelligent RF Access Point (IRAP) in 3Q04. MIMO is one of several dozen proposals competing to become the foundation for 802.11n, the new high-speed (100–200 Mbps) WLAN standard to be developed by the IEEE. Another proposal, TGnSynch, seeks to increase capacity by using wider channels.

Enterprises can expect to see pre-802.11n products emerge from many sources over the next few years. The catch with any prestandard product is, of course, multivendor interoperability. In the WLAN arena, users must also watch out for interference between devices that use incompatible transmission techniques. Channel bonding by proprietary "turbo mode" extensions has proven to be a good example of the latter.

Conclusion

In this article, we've considered the benefits and challenges facing enterprises that roll out wireless devices based on 802.11 Wi-Fi. Wireless LAN deployment may not yet be simple, but a wide

variety of products and techniques is available today or will be available by the end of this year to address the concerns that trouble most IT administrators.

Ultimately, it may be inevitable that Wi-Fi will become ubiquitous within the enterprise. Wavelink's Hermelee argues that it is only a matter of timing and budget. "The technology is there from a performance, cost, and now security perspective," he said. "Tools are available to roll these Wi-Fi networks out in a secure, organized, and low cost manner—there are plenty of good reasons to do it, and the reasons not to do so are becoming less and less." □

Companies Mentioned In This Article

AirDefense (www.airdefense.net)

Airespace (www.airespace.com)

AirMagnet (www.airmagnet.com)

Airwave (www.airwave.com)

Aruba Networks (www.arubanetworks.com)

Atheros (www.atheros.com)

Berkeley Varitronics (www.bvsystems.com)

CA (www.ca.com)

Cisco (www.cisco.com)

D-Link (www.dlink.com)

Fortress Technologies
(www.fortresstech.com)

Hewlett-Packard (www.hp.com)

IBM (www.ibm.com)

Interlink Networks
(www.interlinknetworks.com)

KoolSpan (www.koolspan.com)

Network Chemistry
(www.networkchemistry.com)

Network Instruments
(www.networkinstruments.com)

Newbury Networks
(www.newburynetworks.com)

Perfigo (www.perfigo.com)

Proxim (www.proxim.com)

Sniffer (www.sniffer.com)

Trapeze Networks
(www.trapezenetworks.com)

Wavelink (www.wavelink.com)

Wi-Fi Alliance (www.wi-fi.org)

WildPackets (www.wildpackets.com)

Wireless Security Corp
(www.wirelesssecuritycorp.com)