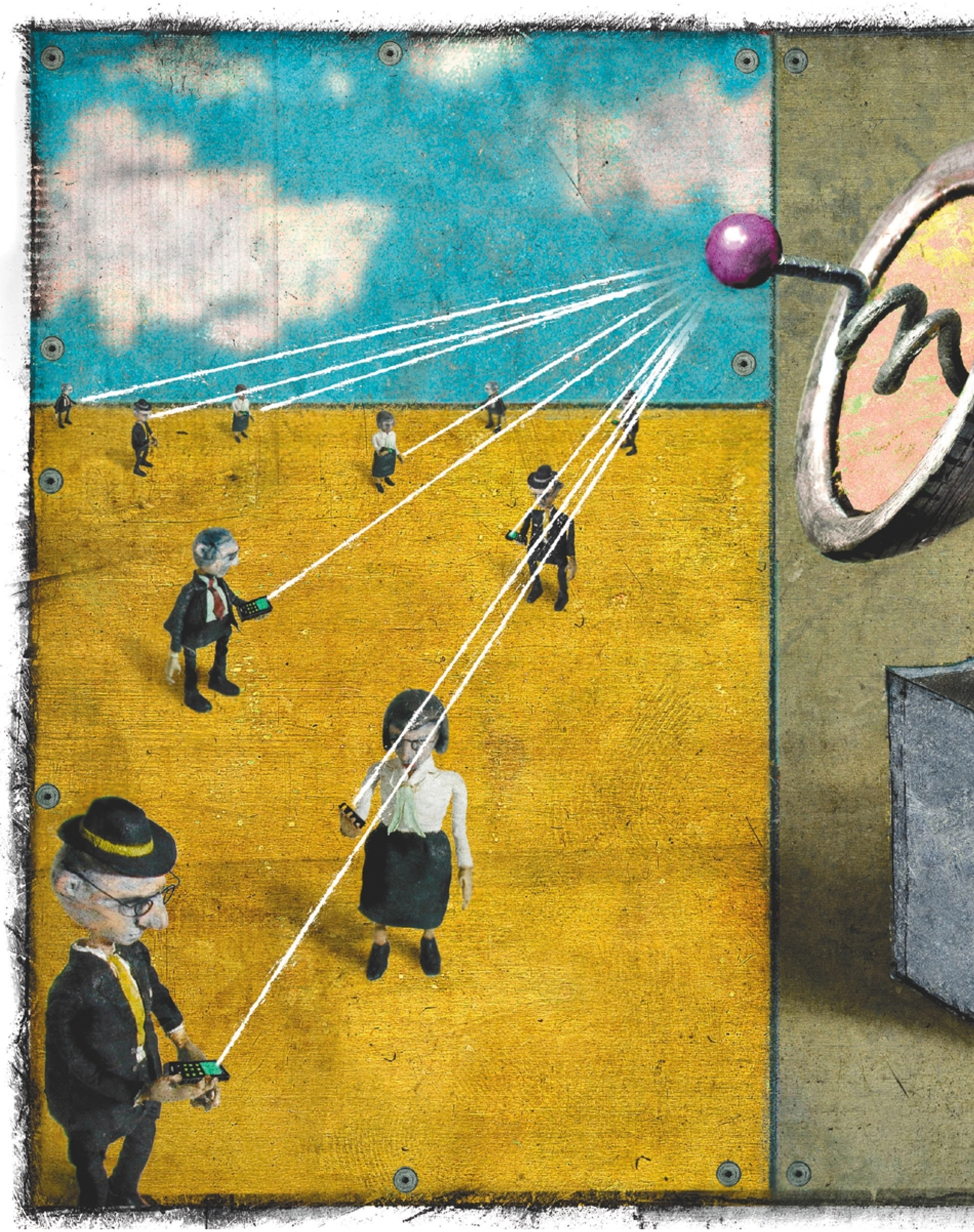


# Plotting a Better Wireless LANscape

## As WLANs ramp up and new standards emerge, IT managers brace themselves for challenges

LAN MANAGERS AND CIOs CAN breathe a little easier, now that solid security standards are available for WLANs. This summer, the IEEE released — and many vendors have already implemented — the 802.11i authentication and encryption standard, bolstered by the WPA2 (Wi-Fi Protected Access 2) interoperability certification from the Wi-Fi Alliance industry group.

Yet, as they deploy broader WLANs as part of the overall corporate network, IT managers will face other issues — for which standards are still in development or have not yet even been started, notes Warren Wilson, an analyst at Summit Strategies. "Now the top problem is making it work robustly and reliably," says Paul Congdon, chief architect of ProCurve networking products at Hewlett-Packard.

These issues fall into four categories: quality of service, WLAN management, roaming, and interoperability with other wireless technologies.

### Quality of Service

As WLANs are more broadly deployed, traffic management will become an issue. APs can typically handle a dozen or so connections at a time, and the burst-traffic nature of data traffic means that most enterprises will handle that traffic easily, especially if their APs can offload traffic to one another during peak demand. "Most users aren't saturating the bandwidth," says Harry Simpson, vice president of sales and marketing at wireless management tools provider Roving Planet.

Bob O'Hara, vice president of systems engineering at wireless hardware provider Airespace, also sees increasing uptake in the warehousing and hospitality industries leading to potential saturation. "Health care is the exception because they have lots of other applications in use," he says.

Bandwidth saturation could be problematic for all enterprises in two areas. One is in high-traffic zones, where throngs of users might suddenly appear, such as at hotspots, requiring both prioritization and handoff to other APs. The other is in organizations that deploy VoIP on the WLAN for mobile workers, such as within a corporate campus or to allow follow-me-anywhere IP-based telephony systems that permit both wired and wireless access.

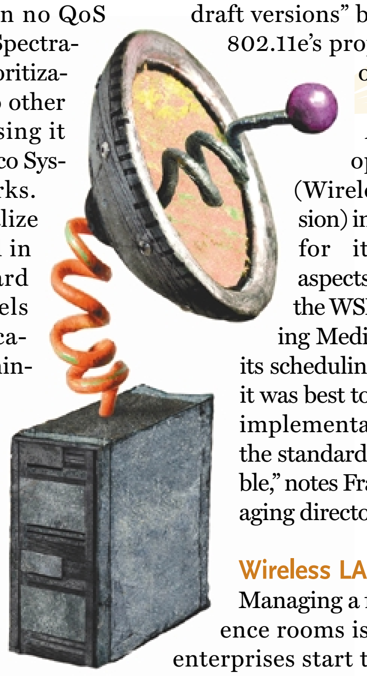
Because 802.11 wireless networks are contention-based, the first packets to arrive get the APs' attention. For streamed

BY GALEN GRUMAN | ILLUSTRATION BY RICHARD BORGE

> “The switch vendors are reluctant to make it easy to provide the same capabilities to other vendors.”
>
> **— Harry Simpson, Roving Planet**

data such as voice, this contention causes dropouts. Fortunately, “wireless VoIP handsets haven’t gotten there yet,” Summit Strategies’ Wilson notes. Roving Planet’s Simpson concurs, adding that voice over wireless is not high on the list of most enterprises’ needs.

Because there has been no QoS standard, VoIP provider SpectraLink has made its own prioritization protocols available to other vendors; among those using it are Chantry Networks, Cisco Systems, and Meru Networks. The IEEE expects to finalize its 802.11e QoS standard in spring 2005. The standard will set four priority levels each for users and applications so that network administrators can prioritize both user classes and application types, such as data, voice, and streaming media. It also will standardize power settings and traffic scheduling to help APs optimize radio range and bandwidth usage based on traffic patterns.



For most data applications, “the prioritization of 802.11e running on 802.11b networks is sufficient,” Airespace’s O’Hara says. For voice traffic, however, 802.11e is a minimum requirement, so O’Hara recommends enterprises use a 802.11a network for voice because it provides four times as many channels for carrying traffic than 802.11b does. If the Federal Communications Commission succeeds in its efforts to allocate 12 more channels to 802.11a, that would make 802.11a even more compelling for voice traffic.

No matter the transport used, voice quality could still be compromised because 802.11e can’t change the contention-based approach of 802.11 networks, notes Phil Belanger, vice president of marketing at hotspot deployer BelAir Networks. “But it will be better,” he says, adding that “a lot of vendors are ready to go with the draft versions” because several of 802.11e’s proposals are all but officially agreed on.

So the Wi-Fi Alliance has developed the WME (Wireless Media Extension) interim certification for its prioritization aspects and is developing the WSM (Wi-Fi Scheduling Media) certification for its scheduling aspects. “We felt it was best to work on a shared implementation for a part of the standard that was very stable,” notes Frank Hanzlik, managing director of the alliance.

## Wireless LAN Management

Managing a few APs in conference rooms is not hard, but as enterprises start to deploy dozens, updating them with authentication keys, firmware upgrades, and policies might become a difficult IT challenge.

Enterprise-class APs permit remote updating via software tools, accessing the APs’ settings typically through MIBs (management information blocks), which are capability specifications called through SNMP and are widely used for wired routers, gateways, and switches. Wireless devices, however, have additional configurations related to managing the radio strength for which there are no standard MIBs.

“The original philosophy [for 802.11] was to put the power in the end nodes, à la Ethernet, but this has put an additional burden on the task of doing handoff because more control is needed by the intermediate devices that don’t have that control,” HP’s Congdon says.

To deal with this issue, today’s enterprises must standardize their wireless APs, gateways, switches, and routers from one vendor and rely on that vendor’s proprietary management tools or use a solution from a third-party tool provider — such as Airespace, AirMagnet, AirWave, Aruba, Cognio, Legra Systems, Roving Planet, Trapeze Networks, or Wavelink — that manages multiple vendors’ hardware. Congdon says that the use of switches for AP coordination can also help make WLAN management less of a burden until appropriate standards are developed.

The IETF is developing the CAPWAP (Control and Provisioning of Wireless Access Points) taxonomy to describe the interfaces and protocols used by various WLAN management devices and to delineate their advantages and disadvantages. The goal is to create a common understanding of these mechanisms so that vendors and IT managers can deploy the appropriate ones. The IETF is also coordinating this taxonomy with the IEEE 802 network interconnections standards, including 802.11.

Although wireless management devices use SNMP MIBs to manage hardware, standards for wireless-specific MIBs would be useful for measuring utilization, managing RF output power, and switching channels, BelAir’s Belanger says.

“Standards are needed for the generation of the information,” adds Jack Winters, chief scientist at antenna maker Motia. “How you use it is up to you.” There’s also a need to get settings, policies, and parameters from the client, which now “doesn’t contribute any information to the access point to help manage the RF signals," says Martin Brewer, senior product manager at wireless management tools provider Wavelink.

Debate exists as to how far standards should extend. "The switch vendors are reluctant to make it easy to provide the same capabilities to other vendors," Roving Planet's Simpson says. Summit Strategies' Wilson agrees that as long as the wireless hardware is SNMP-aware, third-party LAN management software vendors' offerings will be capable of handling hardware feature differences. As switches gain wider use, enterprises may start using lightweight APs, which are managed in groups by controllers in a hierarchy of nodes and branches.

This situation reduces the complexity and cost of APs but can lead to reduced interoperability among vendors' hardware, Airespace's O'Hara notes. "That is ripe for standardization," he says, noting that the IETF has developed a draft for such a standard, which would discourage the use of proprietary, single-vendor lightweight hardware.

How would wireless back-haul connections be managed? Today, wireless APs are linked to one another and to switches and routers through the wired LAN, so management-related back-haul data is carried through the higher-capacity, more-secure LAN. (User traffic is also routed to the back-haul wired LAN at these connections.) In many environments, however, connecting APs via wires is difficult or expensive. To address that problem, the IEEE is developing 802.11s, which would manage wireless back-haul connections and create what are called mesh networks so that not every AP would need a direct connection to the wired LAN. The trick, says Motia's Winters, "is to figure out how not to interfere with the clients' traffic."

## Wireless Standards Snapshot

MOST WIRELESS STANDARDS COME FROM THE IEEE, WHOSE 802.11 CATEGORY covers more than a dozen standards for specific wireless areas, but the IETF, Wi-Fi Alliance, and WiMax industry group also develop related standards.

### TRANSPORT

**802.11a, 802.11b, 802.11g:** All are IEEE standards for the transmission of wireless signals providing maximum throughput of 54Mbps in the 5GHz band, 11Mbps in the 2.4GHz band, and 54Mbps in the 2.4GHz band, respectively. All are in use.

**Wi-Fi:** The Wi-Fi Alliance's Wi-Fi designation certifies interoperability among 802.11a/b/g devices because each standard has optional components that if not implemented would still technically fulfill the IEEE standards but might not permit interaction with other vendors' devices.

**802.11n:** This new IEEE standards effort seeks to develop 100Mbps maximum throughput, most likely in the 5GHz band and through the simultaneous use of multiple channels. The standard is slated for completion in 2007.

**802.16d, 802.16e:** Both are IEEE efforts to standardize wide-area, high-speed wireless zones. 802.16d is oriented to fixed-wireless deployments, whereas the forthcoming 802.16e standard will permit mobile use, such as in trains or cars. There are so many permitted variations in each standard that the 802.16 label will likely need subcategories to clarify specific products' range, bandwidth, or support for mobile users.

**WiMax:** An effort by the WiMax Forum industry group, this is an evolving certification for 802.16 interoperability standards, similar to the Wi-Fi Alliance's efforts for 802.11.

### SECURITY

**802.1x:** This venerable IEEE authentication standard is used by the 802.11 standards.

**802.11i:** Recently approved by the IEEE, this encryption standard replaces the vulnerable static-key WEP standard. It allows for dynamic shared encryption keys.

**WPA2:** The Wi-Fi Alliance's WPA2 standard assures interoperability among 802.11i-based devices. (WPA1 was an interim standard issued before the final 802.11i standard, to keep vendors from straying from the draft 802.11i standard.)

### MANAGEMENT, ROAMING, AND QOS

**802.11e:** An IEEE effort to be completed in summer 2005, it defines prioritization levels and provides basic levels of QoS for data, voice, and video traffic.

**WME, WSM:** The interim Wireless Media Extensions and Wi-Fi Scheduled Media standards from the Wi-Fi Alliance are based on the draft 802.11e. They're meant to ensure interoperability and consistent deployment across different vendors' pre-standard products. WME is available now, whereas WSM is expected in spring 2005.

**802.11f:** This IEEE standard defines communication between APs for layer 2 roaming, but it does not support roaming across different WLAN segments.

**802.11r:** This is an IEEE effort to standardize handoff for fast roaming among APs, including authentication keys, to allow fast roaming that will support voice over wireless in addition to data over wireless. It would also address roaming across segments. The standard is slated to be complete by 2006.

**802.11s:** Yet another IEEE effort, this standard is designed to wirelessly connect APs for back-haul communication and mesh networking. The standard is expected to be complete by 2006.

**CAPWAP:** Standardizing the taxonomy of mechanisms for the control and programming of wireless APs is the goal of this recently completed IETF effort. The acronym stands for Control and Provisioning of Wireless Access Points.

**LWAPP:** An in-progress IETF effort, the Light Weight Access Point Protocol governs how lightweight APs communicate with WLAN system devices and with the controllers that manage the lightweight APs. — *G.G.*

"Interoperability ... is not an issue right now. We don't even have the hardware yet."

— Jeff Orr, Proxim

### Roaming Among Networks

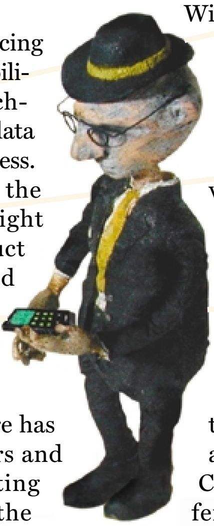
Although the 802.11f standard — already part of most 802.11-based hardware — enables roaming among APs on the same network segment, 802.11 roaming often breaks down as users move across network segments, especially for voice traffic, says Abhijit Choudhury, director of ASIC architecture at chipmaker SiNett. (For data connections, the client can usually get away with using DHCP to get a new IP address with no noticeable downtime, notes Ben Guderian, director of industry relations at SpectraLink.) Also, the reauthentication effort during roaming can interrupt connections that are streamed, especially VoIP.

The reauthentication issue becomes especially problematic with the new 802.11i security protocol or the use of RADIUS server authentication, both of which tend to take several hundred milliseconds. "Handoff for voice needs to be no more than 20 milliseconds," HP's Congdon says. So the 802.11r task group is studying faster algorithms and preauthentication to keep authentication time low. "If you have to go back to a RADIUS server every time you need to reauthenticate, there's no hope," Congdon says.

In the meantime, enterprises can use NAT and mobile IP, in which the "home" IP address is static and is redirected to the changing IP address as the device moves from one AP to another, notes Shrikant Sathe, SiNett's vice president of marketing.

Until 802.11r is complete, however, enterprises will need to use proprietary hardware from vendors such as SpectraLink to get fast roaming for applications such as VoIP, Sathe adds. IT managers should note that wireless VoIP systems use the insecure WEP (Wired Equivalent Privacy) encryption to keep authentication time under the 20-millisecond threshold, Airespace's O'Hara warns.

### Mobile Interoperability



The least pressing issue facing IT managers is interoperability with other wireless technologies, namely cellular data and 802.16 wide-area wireless. "Interoperability among the three is not an issue right now," says Jeff Orr, product manager for broadband wireless at equipment maker Proxim. "We don't even have the hardware yet."

The absence of hardware has not stopped some vendors and analysts from promoting 802.16 as just around the corner. Even Intel, the most aggressive 802.16 chipmaker, doesn't expect to have 802.16 chip sets ready for sale to laptop makers until mid-2006, notes Phil Solis, a wireless analyst at ABI Research. For fixed-wireless 802.16 deployments, Intel doesn't expect to see carrier trials until fall 2005, says Jim Johnson, vice president of the wireless networking group at Intel.

Interoperability with 802.16 should be the simplest to achieve, Orr notes, because it is Ethernet- and SNMP-based, as is 802.11, and will thus support the same security mechanisms and policies. "Policies need to be handled as a superset of what they do for the wireless LAN," he says.

Initial 802.16 deployments will be in fixed-wireless environments, based on the recently completed 802.16d standard popularly known as WiMax, for which the WiMax Alliance industry group plans to certify interoperability. Such 802.16d hardware will be used mainly as a substitute for cable modems and DSL service to connect desktops to the Internet, Wi-Fi Alliance's Hanzlik notes. By 2008, the mobile version of WiMax, based on the still-evolving 802.16e specification, should allow mobile deployments.

As WiMax gets off the ground, cellular data technology is already being deployed, with the GPRS and EDGE (Enhanced Data rates for Global Evolution) variations of the GSM technology used by carriers such as Cingular Wireless and T-Mobile and with the EvDO (evolution, data optimized) variation of the CDMA technology used by carriers such as Sprint and Verizon Wireless. Cellular and 802.11b are very different technologies at all levels, notes BelAir's Belanger, which makes handoff and billing difficult.

For example, authentication on cellular networks is typically handled by the use of embedded hardware IDs, whereas they are software-based under 802.11. Even more important are the business rules because cellular carriers would need to address roaming from their pay-as-you-go cell networks to largely free 802.11 networks as well as billing for use of private 802.11 hotspot networks such as those offered by Boingo Wireless, SBC, Sprint, and T-Mobile.

The Wi-Fi Alliance has a task group to explore 802.11b/cellular convergence, including billing and infrastructure issues, Hanzlik notes. Standards in this area could take years, Airespace's O'Hara says, adding, "I'm not sure there's been enough time looking at the problem to know what the standards might need to do."

*Galen Gruman is a San Francisco-based freelance writer.*