



NETWORKWORLD

October 23, 2006



The quandary of managing the wired with the wireless network

Unified management of wired and wireless networks is the ideal -- and a long way off.

By Ann Bednarz

Faculty at the University of Moncton have a new way of keeping in touch with colleagues and students when they're roaming around campus: Wi-Fi phones that use the school's wireless network. The university, which is in Canada's New Brunswick province, had planned an IP telephony rollout after upgrading its wired network last summer. Adding a campuswide wireless LAN and using it to carry voice traffic was not part of the plan - it just seemed to fall in place, says Jocelyn Nadeau, IT director at the Edmundston campus.

"With the infrastructure we had, deploying wireless at the same time we deployed voice over IP just made sense," Nadeau says. For example, the upgrade included Power over Ethernet, so getting electricity to the wireless access points was simple. "We took a big project and made it bigger. But it all worked well."

New! Watch this Network World Webcast - Cellular Data and Convergence: Mobility Reaching the Red Zone

Voice over Wi-Fi is among a handful of emerging applications that industry watchers say is helping to propel wireless from a conference-room convenience to a more pervasive, mission-critical technology for today's business environments (see "VoIP, the killer enterprise wireless app"). As that happens, enterprises are becoming more aware of the challenges of managing wireless components.

"Wireless still really has a long way to go in terms of manageability and predictable behavior," says Paul DeBeasi, a senior analyst at the Burton Group. "There are rules for how you design and deploy a regular wired network, and if you follow the cookie-cutter rules, you'll have a stable, reliable, high-performance network. It's not like that with wireless."

The complexity of WLAN management

A wireless network's susceptibility to environmental conditions contributes to the complexity of managing it. To deal with the physical elements, enterprises often deploy dedicated tools, such as modeling and simulation software or radio frequency (RF) monitoring wares. (See related story on the various wireless standards.)

In addition, wireless network managers need operational software, which typically comes from their WLAN infrastructure vendor, to tackle such tasks as managing encryption keys, provisioning user access and keeping firmware up to date. On top of that an enterprise might run an overlay service, such as wireless intrusion prevention.

This all can add up to a sea of consoles - and that's just for the wireless side. Still elusive is the ability to manage wired and wireless networks from the same console, using the same techniques.

Configuration of wireless infrastructure and devices ultimately should be wrapped into larger network and systems management frameworks, says Rachna Ahlawat, a research director at Gartner. Vendors such as CA, HP and IBM have made progress letting their respective management platforms import data from WLAN management software, but that work has been more for the purposes of reporting than for taking management action. "They've just started scratching the surface," Ahlawat says.

Still, the tools available to help network executives manage WLANs are better than they used to be. In particular, vendors have shifted from autonomous access points to controller-based architectures that allow centralized management and configuration.

John Turner remembers when his team had to service access points individually. "If we wanted to change [a service set identifier] or update the code or add something, we had to go out and touch each of the access points individually," says Turner, who is director for networks and systems at Brandeis University in Waltham, Mass.

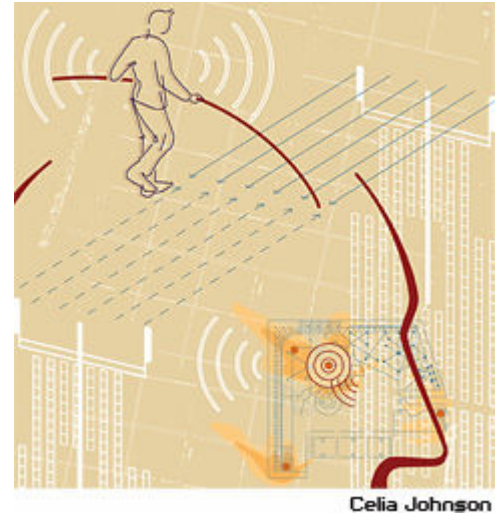
"I only have two people who do network management, for the wired and the wireless. When we had a dozen access points it wasn't so bad, when it was two dozen it was OK, but when it hit 36 it was ridiculous."

When Brandeis decided 18 months ago to blanket its 100-building campus with wireless access - a project requiring the deployment of more than 800 access points - Turner knew manageability had to be a top priority. The university chose Aruba Networks' gear.

Aruba espouses the idea of thin access points, managed by centralized controllers. The architecture lets Turner's team manage the wireless network from one location.

"We've done software upgrades on the Aruba system, we've made SSID changes, we've done a lot of different things here and there. It's a no-brainer. The access points are just the delivery mechanism. There isn't anything we have to do to them other than make sure they're plugged in," Turner says.

WLAN infrastructure vendors, such as Aruba, Cisco and Trapeze Networks, have done a good job of bolstering the management features in their product sets - but each vendor's software is designed to manage only its own infrastructure products, Ahlawat says. For heterogeneous environments, such vendors as AirWave Wireless and Wavelink offer specialized wireless network management software that lets enterprises manage several different



makes of infrastructure products. "But there still isn't any vendor that can give me a solution for common wired and wireless. The vendors haven't made this a priority," she says.

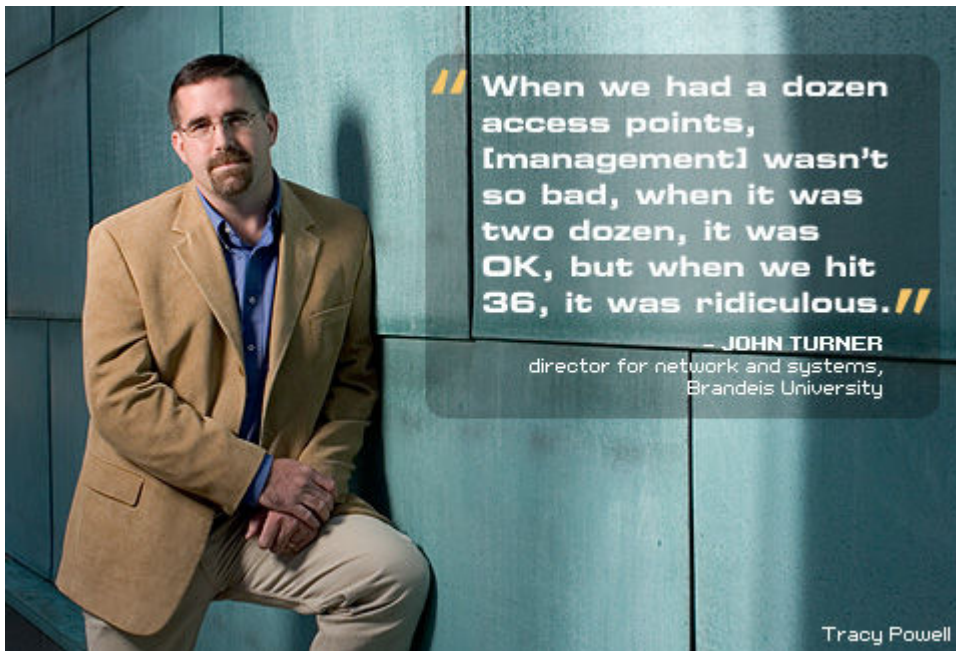
WLAN management as art

If there's one reason management hasn't gotten a ton of attention from vendors and IT staff, it would be security. That issue traditionally has dominated wireless considerations, but as enterprises, vendors and service providers have become adept at addressing wireless security, priorities are beginning to shift. "As companies start to think about using wireless LANs in less casual deployments, for things like voice and location detection of tagged items, they're more concerned about reliability. It's an interesting shift in the last year," says Ellen Daley, a vice president at Forrester Research.

The vendors and service providers have addressed the science of security well, Ahlawat says. The pieces are available, enterprises just need to put it all together, she says. That's not the case with management, however. "Management is more of an art. You don't even know what the different pieces are, and how you put together your network management is going to be very company-specific," she says.

For WLAN management, the University of Moncton is turning to HP, which designed and implemented the school's Cisco-based wireless network. With the wireless infrastructure in place, Nadeau says now he's on the lookout for management efficiencies. "We're trying to look at solutions that would allow us to manage everything from a single point," he says.

One area on Nadeau's radar is access control. Today the university uses an open source wireless authentication client, SecureW2, to manage wireless access. The setup, however, requires students to bring in their laptops so IT can install and configure the client software. "If that load turns out to be as big as we think it will be, we will need to look at another solution," he says. "That's the next phase in our wireless project."



Looking ahead, analysts expect WLAN infrastructure vendors will continue to bolster their built-in management capabilities and begin to eliminate the need for third-party overlay services. For example, vendors are getting better at RF monitoring, Burton Group's DeBeasi says.

"There are separate companies selling devices to allow you to monitor what's happening on your wireless network on a physical layer, but they're not integrated into the management tools. Over the next two or three years . . . companies like Cisco and Aruba will be integrating those capabilities right into an access point," he says.

Tighter integration will reduce the number of consoles and increase functionality. For example, network managers should be able to take action automatically in response to environmental conditions, such as interference or an oversubscribed access point. "If you monitor in an integrated way, and you see a problem you can then use expert intelligence built into your controller to tell the access point, 'Do this.' If you have an overlay network, you can't take any action without involving a human being," DeBeasi says.

Bo Mendenhall, principal information-security architect at the University of Utah Health Sciences Center (UUHSC), has seen the beginning of such improvements. The Salt Lake City institution, an AirDefense customer of almost four years, depends on the vendor's sensor-based security software to monitor its wireless landscape and detect rogue access points and suspicious traffic.

Four years ago, wireless access-point vendors weren't offering that kind of functionality. Lately that's been changing, Mendenhall says. For example, UUHSC is almost done upgrading its WLAN infrastructure with Aruba products, which include air monitors that perform functions similar to those of the AirDefense sensors. Mendenhall isn't ready to give up his AirDefense products but admits their functionality overlaps some with the Aruba systems. "But Aruba doesn't have the level of granularity that AirDefense gives us," Mendenhall says. "If we need more in-depth, forensic-type information, or more long-term trending information, we still look to AirDefense."

Mendenhall says he can envision the two vendors' functionality continuing to converge, but it could take a year or two. In the meantime, using the two systems in tandem lets UUHSC validate information. "If we see something in Aruba, we can go back into AirDefense and see if we see the same type of traffic pattern or attack. There are benefits to having both systems."

On the management front, the Aruba gear fits Mendenhall's desire for centralized WLAN handling. "I wanted one console for someone to be in on a daily basis, regularly looking for the operational as well as the security problems," Mendenhall says. One of the benefits is that all the logs are in one place, which makes it easier to troubleshoot problems, he says. With Aruba's centralized console, it takes just 1.25 full-time employees to manage UUHSC's wireless network, which has 500 access points and air monitors, he says.

Greatness to follow integration

Things eventually will get even better in terms of management for enterprises, experts say.

The elements are expected to come together, because it makes sense that they do, says Craig Mathias, principal at the Farpoint Group. "There's roughly 90% commonality between what goes on in a wired network and what goes on in a wireless network," he says. "It doesn't make sense to have two different directory services, two different security systems. Everything can be put in one place and centrally managed."

Enterprises will wind up with a single hierarchy of management tools that govern wired and wireless -even mobile devices - and those tools will be driven by policies, he predicts. "You'll say, 'This specific user has the following capabilities and this level of priority.' The network then just implements the policy."

Brandeis' Turner, for one, looks forward to that day: "I would love to have the same visibility into our wired network that we do into our wireless network."