

As seen on campustechnology.com

Network Security

The Air Gap: Isolating the Wireless Network To Secure Campus Data

By Dian Schaffhauser - 07/24/09

The concept of an "air gap" in computing refers to the idea of isolating a computer installation to make it extraordinarily secure--so much so that it could almost be considered a closed system. While [Lewis University](#) isn't taking the design to that extreme, CTO John Dalby still uses the term to describe how he has set up the Romeoville, IL campus' wireless network to be separated from its wired counterpart. The air gap has provided a level of security, he said, "that I needed to keep my student and staff information away from hackers and anybody who wanders onto campus and gets on this wireless network." The result: Nobody has yet hacked into the university's student information systems; nor has the campus reported any instances of identity theft since going live with its first wireless network in 2003.

A Revamp of the Original Wireless Network

That first network had a wireless infrastructure designed by system integration firm Fiber in the Sky and built with [Proxim Wireless](#) hardware. The initial deployment encompassed an indoor wireless network, and a later expansion announced in 2006 added an outdoor mesh network.

In a mesh network, nodes provide WiFi access to users while connecting to each other to share bandwidth, identify the fastest routes around the network, and enable redundancy in the event of equipment failure.

So, when [Scientel Wireless](#) purchased Fiber in the Sky in 2008, Scientel Executive Vice President Nelson Santos requested a meeting with Dalby simply to get a sense from the CTO about how this key account was doing. He heard an earful. "John had some real issues with the existing network," Santos recalled.

"Although we started getting wireless service to students and faculty, we found it wasn't as reliable as we needed to really be worthwhile," explained Dalby.

First, the wireless network was limited to specific academic buildings. Second, it was unreliable. The university relies on a [Blackboard](#) application for course management, including the ability to issue online tests. But frequently, students would get halfway through a test, and the network would go down.

"These tests are timed, and you'd be typing the answers when your connection would go down," said Richard Conley, a graduate student and help desk specialist at Lewis. "You'd be locked out of the test and have to make calls to try to get the test reset. It was just very inconvenient to be kicked off the Internet when you were actively using it."

Users stopped relying on the wireless network. In that first meeting Santos assured Dalby that one of his company's goals would be for the campus community to start trusting the network "so it becomes part of everyone's daily life."

He brought in a team of engineers to collect data and quickly found that although there were plenty of devices around campus, their placement was haphazard. "We saw indoor technology being used outdoors and modified, which presented some issues," recalled Santos.

Plus, the initial deployment didn't take into account the kinds of interference that are, in some cases, unique to Lewis' campus. That includes older buildings with thick walls, others with all metal walls. It includes a radar system in use at Lewis University Airport, which is right next door to the 380 acres owned by the campus. Next to that is a National Oceanic and Atmospheric Administration (NOAA) weather system for the state of Illinois. Within three miles is a Doppler radar system used by a Chicago television station. The campus sits next to a river used to bring barges from the Mississippi River to Lake Michigan. Those barges are monitored via radar.

"I'm not sure the people who put the initial [wireless] system in had enough [radio frequency] experience or took into account all of those interference things," concluded Dalby. "So that became the challenge that Nelson and his engineering staff and deployment staff had to overcome."

Santos' crew used a spectrum analyzer to evaluate not only what was in band, but also what was in adjacent channels. "There's a lot of leakage from certain systems," he said. "The common mistake with integrators is that they focus on the main infrastructure, which has lots of power and big antennas. It has the margin to overcome a lot of these factors. But where people fail is in figuring out what's going on at the user level. The user is using a notebook or iPhone or something small. They don't have big antennas and lots of power. It's the opposite."

Interference--including the kind generated from having too much wireless hardware operating--isn't an uncommon source of wireless network problems, Santos said. "Customers get serious about wireless, and they don't understand why their system isn't working. We go and look. They have so many devices, they're creating an environment that's almost inoperable. As you add more devices, you create a ton of interference--self inflicted."

Wireless Network, Take 2

Rather than reworking the configuration of the existing equipment, Lewis U followed Scientel's recommendation that it rebuild the network from the ground up. "The effort to get the existing network to work would have proven more time intensive and without giving any confidence that we'd be better off," said Santos.

He doesn't mention that although Scientel works with equipment from [Motorola](#), [Alcatel-Lucent](#), and [Cisco](#) and considers itself "vendor-agnostic," Proxim wasn't one of its primary technology partners.

In addition, by this time Dalby had a different perspective on how the wireless network should operate in its reincarnation. "We didn't get enough information from our users the first time. I

missed a few things that were requirements." Those needs included wireless-anywhere on the 140-acre campus, including the ability to do computing outdoors, for example, on the campus green.

The second iteration of the wireless network went in during the summer of 2008 using 802.11n wireless networking gear and software from Motorola. That included AP300, AP-5131, and AP-7131 indoor access points; an RFS6000 wireless switch; a MotoMesh Duo Two-Radio outdoor mesh network; Canopy 5.4 GHz unlicensed point-to-multipoint links; the One Point Wireless Suite for network management; and network design utilities LANPlanner and MeshPlanner.

The mesh network provides a level of redundancy that's important to the health of the network, said Dalby. If an access point goes bad, he explained, the others increase or change their power to cover the area. "It becomes a self-healing mesh. So we get higher service levels without having fully duplicated systems--all self-healing and all reporting back to the central switch that runs the network for us."

Another advantage of the mesh network approach is that since the access points pass data along to each other, not every single unit requires an Ethernet connection to the network. The only requirement is power.

As Santos explained, although there's no "meshing" standard--akin to WiFi's 802.11n--most vendors use one of two designs: spanning tree, where the access point follows a particular data communication path until it dies, and then it looks for another path; and dynamic, where the access points do load balancing, continually monitoring for multiple paths through the mesh and sending data along them. Motorola's meshing protocol is dynamic.

Scientel worked with Motorola engineers to create a layout that was compliant with dynamic frequency selection radar requirements while reducing radar-inflicted interference. The system integrator reduced the outdoor infrastructure by half and the indoor infrastructure by about a third. "Some may equate the reduction in infrastructure with a reduction in coverage. In fact, it isn't an exact correlation, said Santos. "It is really about proper RF planning. Our coverage actually increased not decreased with the reduction in units."

In fact, coverage is no longer limited to academic buildings; wireless is now considered pervasive on campus.

However, integration of the indoor and outdoor wireless isn't always a simple matter, particularly when it involves mobile operations. In fact, Scott French, a Motorola vice president in its emerging technologies and solutions division, called the Lewis deployment unique in that regard. "It's seamless--leveraging a variety of wireless broadband technologies all managed from one application suite, all with the same level of security. And that end-to-end wireless solution is a much more flexible platform to enable expansion, interoperability with other networks off campus, and sharing of data when they're ready to expand--as opposed to wireline, where, once you put it in, you're fixed."

"Now that we have reliable wireless access, I am using my PDA much more than before," said Ray Klump, an associate professor of mathematics and computer science. "I'm getting calls and e-mails and accessing the Internet wherever I happen to be. You'd be surprised how many students are instant messaging me for help, and now I can access and answer those questions from anywhere on campus."

Dalby said that in spite of the fact that he and the IT staff are still working to reverse the negative impressions of the former network, data shows adoption is growing. Usage has quadrupled. Concurrent usage has grown from a peak of 50 to a peak of about a thousand users--about a sixth of the total campus population. Also, Scientel, which has taken over management of the network infrastructure and provides help desk services for the university--has seen trouble tickets go down.

Maintaining the Air Gap

What didn't change in the redesign of the network was that focus on maintaining the air gap--keeping the wireless and wired networks separate. The wired network is where important university applications--including student information systems--are maintained. The wireless network provides access to the Web, where students, faculty, and staff can surf and access software-as-a-service, such as the Blackboard implementation.

From what Dalby's seen, the air gap idea hasn't pervaded higher ed IT. "Most [institutions] put their wireless on top of their wired," he said. "Then they have security issues up the wazoo."

This concept of the air gap serves several purposes. "We try to protect our wired network and student information as much as possible," Dalby said. "We limit the number of Internet ports open to the university. We filter what comes into the university on the wired network. Plus, of course, we put anti-spam and anti-virus heavily onto our network." If a user needs to gain access to the wired network through a wireless connection, he or she needs to use the virtual private network to tunnel in, which imposes its own access controls.

He's had complaints from some members of the faculty, who are concerned about the lack of academic freedom. His counterpoint: "We've provided faculty with wireless laptops, which they can use to get onto the wireless network. And we impose very few constraints about where they go and what they do. Therefore, they're academically free to do what they wish."

Lesson Learned: It's the Reliability

Now that the wireless network has stabilized and provides some headroom for growth, Dalby and the university are looking ahead. Currently, Lewis U has a deployment of three surveillance cameras on the network, all focused on the single entrance into the campus; but that may grow. A few of the campus police have laptops in security cars, which may expand. Dalby said his team is also considering outfitting facilities people with devices in order to be able to monitor and close out work tickets via the Web. Longer term, the campus may use its wireless network to control heating, air conditioning, and ventilation.

But through all of the plans for the future, Dalby won't forget the one lesson the wireless fiasco taught him: how important reliability was to users. "You always need to find a way to get double coverage,

triple coverage," he said. "Users are elephants. They don't forget. If you have one failure, you're going to have to do a good advertising campaign to get them back into the program."