



Updates, issues and opinions – what's the **buzz** on campuses around the country?

Find out today: blogs.universitybusiness.com



UB web seminar series **Archive Now Available FREE**

STREAMLINING STUDENT SERVICES



The Magazine for College and University Administrators

FEATURES

Rethinking Wireless

by: *Matt Villano*

As wireless LANs grow on campuses across North America, academic technologists strategize for the challenges of the future



Remember when the only network on college and university campuses was the wired one? When schools like yours invested millions in fixed Ethernet ports? When "network security" meant betting the house on the hope that outsiders wouldn't sneak onto campus and plug in? Those days aren't all that far behind us; even the pioneers in the wireless space didn't ditch their wires much before the current 802.11b wireless standards were ratified in 2001.

Why Wireless

The academic wireless Local Area Network (LAN) has come a long way since then. Though few schools have advanced beyond expanding the networks they bought back in 2001, hundreds of schools across North America now have some form of wireless capability, and hundreds more consider it every day. The price of hardware necessary for wireless has dropped considerably, with access points ranging from \$150 to \$500 apiece, and network adapter cards as low as

\$60. Last—but certainly not least—with the impending arrival of new wireless standards 802.11a and 802.11g, wireless technology will get faster and more secure, making even the harshest skeptics curious.

"Wireless is here, and it's here to stay," says Ron Yanosky, senior analyst with the Higher Education Technology Strategies Group at Gartner, Inc., in Stamford, CT (www.gartner.com). "When you consider that the modern college student is mobile most of the time, investing in a wireless LAN for your campus simply makes sense; you're investing in the technology that suits your users best." Still, as Yanosky points out, you can't just grow a multiple access-point wireless network overnight; the process takes time, planning, and careful execution. Experts and academic technologists all over North America agree that perhaps the three most critical steps in building a wireless LAN are designing the network, managing it, and securing it. After that, of course, the rest is up to you.

Designing your Network

One of the biggest challenges in laying out a wireless LAN lies in designing the layout of the access points and ensuring that adequate coverage is provided throughout the service area. Since every access point has a range of roughly 800 feet in an open environment, the name of the game is stationing your access

Buena Vista University
LOCATION: Storm Lake, IA POPULATION: 1,300 students WIRELESS SOLUTION: In 2001,



[View UB Magazine online](#)



Keeping It Green

Sustainability
University Business
June 2009

Get your staff on the same 'page'
Have them subscribe today!

UB Daily

points to maximize coverage and minimize cost. While trial-and-error layouts frequently do the job, academic technologists agree that the most efficient designs are based on hard measurements, and not rule of thumb.

Of course, the coverage equation isn't as simple as plopping a new access point every few hundred feet. Because the coverage area of each access point is so small, terrain is not as much of a propagation issue as the layout and construction of buildings on campus. Wireless signals transmit perfectly through wood, plaster, and glass, but metal, brick or concrete walls have proven to be significant barriers. Compounding this problem is what experts refer to as the "contention-oriented" nature of the 802.11b wireless protocol: If one access point is too close to another, it will "defer"—that is, the point with the stronger signal will knock the weaker point offline, creating interference that impairs capacity and slows the network down.

"This technology is incredible when it's applied correctly, but there's so much working against it that many people actually hinder their own network coverage with poor planning," says Chuck Bartel, director of networks at **Carnegie Mellon University**, and project director of the school's wireless network (dubbed "Wireless Andrew"). To maximize coverage, Bartel suggests that technologists base network design on exhaustive signal-strength measurements, even utilizing an aid as sophisticated as SitePlanner from Austin, TX-based Wireless Valley (www.wirelessvalley.com) or AirMagnet, a diagnostic from the Mountain View, CA, company with the same name (www.airmagnet.com).

AirMagnet is precisely the tool Todd Grappone used to design a wireless network up the road at the **Stanford University School of Medicine** in Palo Alto. When Grappone, associate director of Development for Stanford's Information Resources and Technology department, set out at the end of 2001 to build the School of Medicine's wireless network, an AirMagnet signal search revealed dozens of wireless access points on and around campus that students had set up themselves. To maximize coverage and performance, Grappone says he spent months taking over the "rogue," or independent, points. (The school took over support, and under the new wireless system provided free access to owners of the rogue points.) Thanks to these efforts, he adds, today it's rare that students access the wireless LAN at speeds less than 5 or 6 mbps. Of course, if the network-capacity needs of Stanford School of Medicine students change, Grappone will be ready to tweak his network design. Already, the wireless computing guru says that to meet growing demand in certain areas, he has repositioned a handful of access points from scarcely used meeting rooms to more popular lounges on and around campus. According to Yanosky, experts refer to this degree of responsiveness to student usage patterns as the "sidewalk paradigm."

"When many schools build a new academic building, they don't put in sidewalks until they get a sense of where the students tend to walk," Yanosky explains. "You can apply exactly the same principle to wireless—one of the most attractive elements about the technology is that it's more dynamic than anything in the past." Yanosky says that using the sidewalk paradigm is one of the most important ways to make sure a wireless network is designed to meet coverage and capacity requirements consistently.

Managing your Network

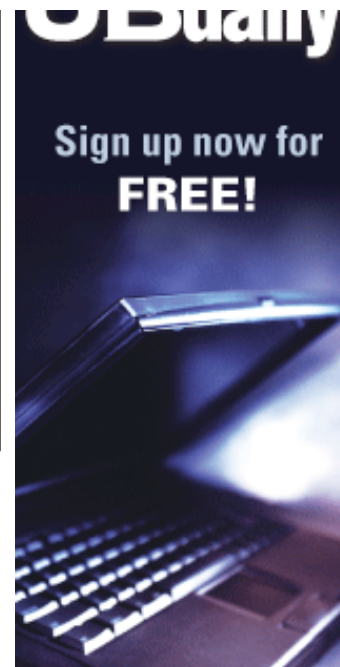
Physically changing the location of access points as user needs dictate is one way to manage your wireless network; other methods can be far less taxing on an IT staff. At the **University of Maryland** in College Park, for example, senior network engineer Leah Goldman keeps watch over the school's wireless network from the comfort of her own desk, thanks to LAN management software Mobile Manager from Wave-link Corp, in Kirkland, WA (www.wave-link.com). Goldman says she uses this program to generate bandwidth reports, view traffic for particular access points, and run statistical analyses for weak links in the system. The result? A LAN uptime of nearly 98 percent.

And at **Buena Vista University** in Storm Lake, IA, technologists achieve even better results with a different set of products (uptime at BVU is 99.5 percent). There, Managing Director of Information Services Ken Clipperton employs a piece of software from Basking Ridge, NJ-based Avaya Inc. (www.avaya.com) called CajunView, designed specifically for the school's Cajun network switches. Clipperton says he uses this tool to run many of the same

BVU ripped out its wired network and dumped \$380,000 into a wireless alternative, including 1,300 Gateway 450L laptop computers that the school configured and distributed to students to use on the new system.

UNEXPECTED ADVANTAGE: While no more than 700 students used the wired network, all 1,300 students use the wireless network in one form or another.

LESSON LEARNED: If you build it, they will come. Now, according to IS Managing Director Ken Clipperton, technologists only hope they can keep up with demand.



Carnegie Mellon University

LOCATION: Pittsburgh, PA
POPULATION: 5,600 students
WIRELESS SOLUTION: Started as a research network in 1994 to support the school's wireless research initiative, 'Wireless Andrew' now operates at the traditional 802.11b standard and boasts some of the most sophisticated management and security technologies in the business.

UNEXPECTED ADVANTAGE: Students can connect to the LAN literally anywhere on the school's main two-square-mile campus—something even network designers didn't think would be possible. No other campus of this size has such complete coverage.

LESSON LEARNED: Perfection takes time: Wireless Andrew was almost 10 years in the making, and today it ranks as one of the best.

diagnostics that Goldman can run, and adds that it also enables him to reboot every point on the network with a software upgrade, almost instantaneously.

"I'd be exaggerating if I said we have physically touched more than five of our [150] access points in the last 30 months," he boasts. "We hardly ever even stress about it; with performance like ours, the wireless network essentially becomes out of sight and out of mind." Still, BVU is a unique case. When the school built its wireless network in the beginning of 2001, it eliminated its wired network altogether, and purchased a Gateway 450L laptop computer for each of its 1,300 students. This, of course, is yet another way Clipperton manages his network: By controlling the hardware and software students use to access the network, Clipperton can keep closer tabs on how students use the network once they're on it. To maintain consistent performance, for instance, BVU technologists have programmed the school-sponsored laptops to refuse any applications that will eat away bandwidth from the LAN. As a result, the "eBVyou" network rarely performs under 10 mbps.

Information technology experts at the **University of South Dakota** in Vermillion tried a similar approach, only on a much smaller scale. There, CIO Roberta Amber supplemented the wired network by spearheading a recent effort to put 1,300 Palm PDAs into the hands of all first-year undergraduates, as well as first-year law and medical school students. With the help of EthIR LAN and EthIR Star infrared wireless connectivity adapters from Clarinet Systems of Milpitas, CA (www.clarinetsys.com), these students can use their PDAs to access certain parts of the network that school officials and network administrators have deemed acceptable.

"The technology is being used by faculty, administrators, and students to share information, collaborate, and communicate more effectively," university President James Abbott says of the program. "We can also load the devices with a host of applications, from financial calendars to reference books, word processors, and more."

Securing your Network

With wireless LANs like the ones at BVU and USD—those in which a school provides the hardware necessary to access the network—security is only a concern when the hardware falls into the wrong hands. At other schools, however—schools that make their wireless LANs available to anyone with a network adapter card—security is of paramount importance. Experts like Gartner's Yanosky say, at the very basic level, a wireless network must require users to authenticate themselves. As such, standard authentication software comes in a variety of flavors, and can even be written by a skilled system programmer.

Many schools with large wireless networks boast software that forces users to authenticate their identities the moment the network detects them. At Carnegie Mellon, for example, a homegrown program requires individuals to submit their user name and password every time they attempt to access the LAN, to ensure that they are, in fact, affiliated with the school. At the University of Maryland, a similar system from Mountain View, CA-based Vernier Networks (www.verniernetworks.com) requires authentication, then tracks every spot each user roams on the network. If a security breach occurs, network administrators can track down offending parties quickly and painlessly.

"If something goes awry, we can pinpoint where on campus someone is, down to a few dozen feet," says UM's Goldman. "We're not using this data to track individual students across campus, but if we had to, we could."

More advanced wireless networks include other security features designed to make it even harder to access critical information on the LAN. At **McGill University** in Montreal, Director of Network and Communications Services Gary Bernstein has divided the LAN into a series of virtual private networks (VPNs), each of which restricts authenticated user access based upon characteristics the user previously has registered with the school. Under this system, McGill essentially has three levels of access—public, semi-public, and private. In public places like the library, any authenticated user can log on. In semi-public places such as a meeting room, or private places such as the student records office, only authenticated users with certain privileges can access the network. In what is perhaps the pinnacle of wireless security, some schools recently have added 128- and 256-bit encryption to their wireless LANs, coding both the data that users submit (personal information, credit card numbers, etc.), and the data that the network sends back. At BVU, for instance, every time the school requires a user to submit his or her Social Security number inside a Web application, the wireless network automatically generates the application in a secure sockets layer (SSL) or a hypertext transport protocol secure (HTTPS) page. And at the **University of Pennsylvania's** Wharton School, Melissa Muth is director of Core Systems and Networking, and also runs a proprietary financial database called Wharton Research Data Service, or WRDS. Muth says she has abandoned Telnet and now funnels U Penn wireless users through the

University of Maryland

LOCATION: College Park, MD
POPULATION: 34,800 students
WIRELESS SOLUTION: In the middle of 2002, UM received a grant to place 100 access points in heavily trafficked areas of campus to begin a wireless network. Since then, technologists have added a number of points to department offices, expanding the network by as much as 20 percent.
UNEXPECTED ADVANTAGE: Because technologists charge departments for access points and installation, the school's IT department actually has been able to make money off the wireless LAN.
LESSON LEARNED: Wireless can be a moneymaker!

encrypted Secure SHell (SSH) software from SSH Communications Security, Inc., in Palo Alto (www.ssh.com).

"No matter how you look at it, it is a security risk to have account passwords and proprietary information flying across the wireless network unencrypted," warns Muth. "When you don't have a firewall—and many schools don't—measures like these become necessary to ensure your wireless network is as safe as it possibly can be."

Planning for the Future

For technologists with wireless networks that are not as secure as those at McGill and Wharton, help is around the corner in the form of new wireless standards 802.11a and 802.11g. These standards will increase the operating speed of wireless LANs from 2.4 to 5.0 gigahertz, and will increase security features as well, often making encryption such as SSL and HTTPS commonplace on campuses around the world. Though the new standards won't come into effect before the beginning of the next school year, some institutions are anticipating the change already; at schools such as Carnegie Mellon and Buena Vista, technologists are readying their wireless networks to be "tri-mode," or compatible with all three 802.11 standards, by the beginning of 2004.

Meanwhile, technologists at other schools continue to explore bigger and better uses of wireless technology. At the **University of British Columbia** in Vancouver, for instance, IS technicians are gearing up to unveil a 2,000-access-point wireless network this summer, a network that should provide access to 6,400 students anywhere on the six square miles of campus. And at **Des Moines Area Community College** in Iowa, administrators already are touting an effort to cash in on 802.11a standards and add video and audio capabilities to the Compaq iPaq PDA devices that have accessed a wireless LAN since the beginning of 2002.

"Instead of reading about the signing of the Declaration of Independence, students will be able to see it on their little screens," says Executive Dean Anthony Paustian. "As we see it, the more fun we can make it, the harder students will work and the better they'll do."

Other schools are rolling out totally new wireless applications. At **American University** in Washington, DC, technologists are piloting geo-location software from Boston-based Newbury Networks (www.newburynetworks.com) that enables prospective students to take self-guided tours with nothing but a PDA. As the prospect walks around a particular building, a network adapter card in his PDA links to access points in and around that building, which pinpoints the student's exact location and feeds the device data accordingly. The application, dubbed LocaleServer, also is being used at **Dartmouth College** in Hanover, NH, where Director of Technical Services Brad Noblet says that some professors currently use it to poll student opinion during lectures, then use the real-time feedback to tailor the remainder of their talks.

Back at Gartner, analyst Ron Yanosky predicts this kind of geo-location software also will spawn another component of wireless technology: e-911. If products like LocaleServer enable colleges and universities to filter information to users based upon their location on campus, he asks, who's to say they wouldn't be able to pinpoint the location of a student in distress? Yanosky envisions a day in the not-too-distant future when students will be able to call for police by pushing special buttons on their laptops, and campus cops will be able to respond by pinpointing the location of any network user, within one to three feet. "The sky's the limit with wireless," he says. "The best part about it? It changes all the time."

Matt Villano is a freelance writer based in Seattle, and Moss Beach, CA.

McGill University

LOCATION: Montreal, Canada
POPULATION: 22,000
WIRELESS SOLUTION: McGill went wireless toward the end of 2001, and has expanded its network ever since. The network today contains almost 200 access points in 120 buildings across campus, and operates with a virtual private network (VPN) that restricts access based upon characteristics in a user profile.
UNEXPECTED ADVANTAGE: By restricting access through a VPN, McGill's network is among the most secure wireless LANs in North America.
LESSON LEARNED: You can never be too safe. School technologists are looking forward to 802.11g standards that will increase security even more.

Stanford University Medical School

LOCATION: Palo Alto, CA
POPULATION: 160 students
WIRELESS SOLUTION: In late 2001, Stanford School of Medicine technologists built a wireless network for student laptops in and around the one-square-mile campus. Last year, the school supplemented this network by expanding it to include Bluetooth-equipped PDA devices, which it also made available to all students.
UNEXPECTED ADVANTAGE: Students don't necessarily need their laptops to connect to the wireless LAN; they can connect with one of the school-funded PDAs.
LESSON LEARNED: Buying hardware doesn't necessarily guarantee use; more students use laptops than the school-funded PDAs.