

# Network keeps students mobile

University of Georgia project uses authentication servers for security.

**N**etworked computers have become as much a part of the university experience as desks and chalkboards, and wireless network access is one of the ways universities keep score of who is best serving the needs of faculty and students. In this environment, the University of

Georgia's PAWS Project (Personal Access Wireless/Walkup System) is a major step toward keeping UGA, with its 33,000 student body, at the forefront of major institutions of higher learning.

The PAWS Project began as a single-site experiment that has grown to encompass the majority of more than 420 access points scattered across the university's Athens, Ga., campus. As the project grew from experiment to deployed infrastructure, administrators realized that several key user interface and security considerations had become requirements.

Security was key, as administrators wanted to be sure that network users were legitimate students and faculty who could authenticate their log-in names against a central database. A consistent user interface was a secondary consideration, as administrators knew that they could not so inconvenience users that they sought ways to circumvent the secure installation.

UGA's enterprise information technology services staff undertook a rigorous review process, analyzing authentication systems from a variety of vendors, and from Georgia Tech. They decided that a Bluesocket system of multiple authentication

servers would best meet the combination of needs their users placed on the network.

The needs were diverse, since having a single source for authenticating both wired and wireless users in the new areas of deployment was important.

One location where wired authentication took place was in the press area at the university's Sanford Stadium, seating more than 86,520 people. A 24-port switch allows visiting journalists to connect to the Internet to file stories and upload digital photos, while authenticating to individual guest accounts presented by a Bluesocket appliance.

According to David Matthews-Morgan, associate director for network planning, the wired segment is a prelude to a larger network. "We've been in dialogue with the UGA Athletic Association for providing ubiquitous wireless for the stadium population in general," he says, explaining that UGA is contemplating joining the ranks of institutions providing network access to go with major sporting events. The stadium project, while high profile, is less likely to affect the students of the university than the large mixed-media network put in place at the Student Learning Center (SLC).

Matthews-Morgan explains that the size of the center makes it a hub for daily student computing. "The SLC is a 200,000-square-foot building with classrooms on the first two floors and PCs in an 'electronic library' on the third and fourth floors," he says. "There are about 500 PCs, along with a ubiquitous wireless cloud."

Matthews-Morgan adds that, in addition to the PCs and wireless access, there are hundreds of 10-BaseT Ethernet ports in the SLC to which students can connect laptop computers not equipped with wireless networking capabilities. Matthews-Morgan and the network staff wanted to maintain a consistent user experience when accessing the network, so all wired and wireless users are authenticated through a system of four Bluesocket WG-2100 Wireless Gateway appliances.

The network accessed by the students at UGA is notable for the diverse collection of hardware that forms its infrastructure. The primary vendor



University of Georgia's David Matthews-Morgan, associate director for network planning, has a lot on his hands keeping 33,000 students wirelessly happy.

Victor Cruz is a free-lance writer based in the Boston-area who writes on a variety of technology subjects. He can be reached at [vcruz@mediapr.net](mailto:vcruz@mediapr.net).

for wired networks on campus is Enterasys, but the university is far from a single-vendor environment, according to Matthews-Morgan.

**Matthews-Morgan points out that one of the key considerations for any authentication scheme was that it work across the wide variety of equipment in place on campus.**

“The Student Learning Center is built on Cisco equipment, and our core is Foundry, with some Foundry equipment in individual buildings,” he explains. “Extreme and Hewlett-Packard equipment is also in place at various locations, and many of the 420 wireless access points we know about are low-end products that don’t really meet our established standards.”

Matthews-Morgan points out that one of the key considerations for any authentication scheme was that it work across the wide variety of equipment in place on campus. He says that Bluesocket’s approach filled that requirement by fo-

cus on users and roles, rather than access points and ports, as the central mechanism for access control.

PAWS is not yet pervasive, and the university is pushing to make wireless network access available in many more locations on campus. A major focus is on lighting up large outdoor spaces on two busy portions of the campus, a project that was expected to be completed in April.

“We are lighting up a north campus green space of approximately 280 by 1,300 feet, and a south campus green space of approximately 200 by 2,100 feet,” Matthews-Morgan says. Moving consistent network security into green spaces and additional buildings has meant making changes to the original plans for Bluesocket deployment.

“When we first started deploying the gateways, we put them in individual buildings, but that began getting expensive, so we’re developing a new model,” Matthews-Morgan says. “Our network has 16 core locations, and we want to place these gateways there and tie groups of buildings together with some of the unused fiber connections we have in place. That will be how we implement the green space projects, where a single gateway will connect seven to nine buildings.”

Matthews-Morgan says security standards built into networking protocols are a long-range goal, but that the standards-based dream is a ways off. “Once we get everyone moved to 802.1x security, then a few years down the road we can transition the standard to wireless. I don’t know whether our current Bluesocket solution is forever, but I see it as our solution for years to come.” □



**7 New England Executive Park  
Burlington, MA 01803  
Toll Free: 866-633-3358  
info@bluesocket.com  
www.bluesocket.com**