

<http://www.thejournal.com/magazine/vault/A4742A.cfm>

University of Florida Rolls Out Wireless Gateways for Secure Network Access, Control

How can network administrators provide secure wireless access to a vast user population scattered over a large area while keeping costs and complexity in check? This is a problem many university administrators and technology coordinators face, including those at the University of Florida, which has wireless networking deployment headaches that most enterprise network administrators will never have to face - starting with its size.

The University of Florida's main campus in Gainesville houses about 900 buildings spread across more than 2,000 acres. Last fall, there were more than 48,000 students supported by nearly 12,000 faculty and staff. And according to Matt Grover, the university's senior network engineer, the University of Florida had more than 20,000 distinct wireless devices. The administration's main problems centered on authenticating network users without causing excessive delays or significant additional network traffic. However, they knew that their solution would need to be easily deployed, reliable and affordable.

Homegrown Solution

The first solution the university applied was homegrown - an extension of the system that network managers created to authenticate users on the wired network. According to Grover, the university had a gateway based on a Linux router that was authenticated via the campus ID; the topology was VLAN (virtual LAN) aggregation behind core POPs. While the solution served the purpose of authentication, there were growing problems. "The hardware on the existing solution was aging, there were support issues, and the person who wrote the system had left the university," says Grover. "There were also slaving issues that made it decentralized, and the security group didn't have control over every piece of the infrastructure." With growing concerns about finding the necessary replacement parts and the ability to patch the software as required, network administrators at the University of Florida decided to begin the process of looking for a replacement.

The process of looking at possible replacements for the homegrown system began with the basics of authentication and security, but stretched to include a critical local issue: the ability for an authorized user to proxy a guest user into the system. This additional capability is unusual but necessary in an academic environment - where components from embedded controllers to game consoles might have a legitimate need to access the network but no way to pass through the normal authentication process. With the criteria in place, the review process began and quickly encompassed systems from a variety of vendors. According to Grover, it was Bluesocket's early response to the authentication proxy issue that set them apart from the competition.

"The one feature that was absolutely crucial was the proxy capability," says Grover. "Users needed it for conference phones, TiVo-like systems, PlayStations and other nontraditional UI (user interface) devices. Bluesocket wrote the feature into a unit the way we wanted before we ever bought the first box. That demonstrated a level of support and commitment that we were absolutely looking for."

Other vendors were unable to meet this requirement with the speed shown by Bluesocket. Also, the Bluesocket devices could be deployed as a drop-in replacement for the existing solution, so the University of Florida decided to move its wireless authentication to a Bluesocket platform in October.

Wireless Gateways

Initial rollout plans called for 10 Bluesocket Wireless Gateways (www.bluesocket.com) to be deployed, so the university's networking team began rolling out the Wireless Gateways one at a time. According to Grover, the network administrators have been so pleased with the level of control offered by the Bluesocket solution that they are exploring the flexibility provided by Bluesocket's approach to authentication and user groups. He says that the flexible options in user-group support offer potential solutions to some of the more difficult problems seen with wireless networking. "We're looking at the possibilities of giving users different roles and levels of quality to make applications like VoIP over wireless feasible," Grover explains.

However, the rollout, like most technology deployments, has not been without certain challenges. At the University of Florida, these have included questions about the best way to structure reports, as well as concerns over link aggregation and scaling with the particular user patterns seen in student populations. But when issues have come up, solutions have been found, according to Grover - referring back to the initial experience of custom code as an indicator of Bluesocket's willingness to work with the university to solve problems.

One of the pleasant side effects of the Bluesocket deployment has been its affordability when compared to other commercial solutions. "Even without the custom feature implementation, the Bluesocket solution was cheaper," says Grover. "All the candidate products were expensive, but Bluesocket offered better features and customization for the money."

Grover says that the university's administration is looking forward to the completion of basic rollout so that they can begin exploring features of the Bluesocket system that are, so far, unused. "The systems have a ton of features we're not using right now - we're deploying the boxes as authentication gateways," he says. "We're just beginning to look at the quality-of-service features and gateway services to contain users infected with viruses and worms." From Grover's point of view, the potential for wireless at the University of Florida looks bright and secure.

###