



Rutgers University

A Bluesocket wireless system meets the challenge of providing secure and reliable wireless access to multiple departments and buildings spread out across the 1200-plus acres of this noted university. The system not only provides wireless access to a diverse collection of faculty and students, but provides a way to monitor bandwidth and limit extensive file-sharing among tens of thousands of academic users.

Chartered in 1766, Rutgers University is the eighth oldest college in the country. It consists of 29 degree-granting schools, with more than half offering graduate-level programs in subjects ranging from accounting and business administration to nursing and law. The university boasts a total for more than 51,400 students and close to 2,600 teachers – all of whom now benefit from a Bluesocket wireless network.

BLUESOCKET DEPLOYMENT AT RUTGERS UNIVERSITY

- Wireless network consisting of 24 Bluesocket gateways (Series 1000, 1100, 2100)
- 802.11b/g technology in 27 buildings (35 total planned in 2005)
- Gateways installed in single location with wireless access via remote bridges
- Support for more than 51,400 students, 2600-plus faculty across 1200-plus acres
- Custom bandwidth quota system based on Bluesocket syslog reporting
- Outside wireless provided via directional antennae
- System promotes collaboration and creative idea-sharing

Rutgers, The State University of New Jersey

Situated in three different locations across nearly the entire state of New Jersey, Rutgers University is one of the most impressive and prestigious colleges in the U.S. However, for all its stature and academic credentials, Rutgers didn't take its first steps into wireless computing until early 2002. In selecting a wireless system, Rutgers looked for a network that was secure, easy to manage, and would provide maximum flexibility and scalability to its diverse student and faculty population.

The Challenge for Rutgers University

Rutgers' wireless journey began in early 2002 with nearly six months of research of current wireless solutions and products. After considering several possibilities and measuring them against the college's requirements, it was decided to install an 'all-in-one' centralized management solution since the university's limited budget for wireless couldn't support using expensive, intelligent wireless access points (APs) in the volume needed for such a large-scale deployment.

"There was absolutely no operating budget, so trying to grow the network the way it needed to be was virtually impossible," says

Ken LeCompte, a systems programmer and administrator with Rutgers University Computing Services (RUCS), who was selected to lead the university's charge into wireless and is now one of two people who operates and manages the RUWireless project for Campus Computing Services.

One of the biggest challenges for Rutgers was selecting and installing a system that would eventually serve many departments and buildings that are spread out across a wide geographic area. This meant that each building must operate as an independent wireless network.

Security was also a major concern right from the beginning, especially since the network would be used by a highly creative and potentially curious student population that might view any weak link in a wireless network as a challenge. RUCS administrators decided to encrypt wireless traffic, although encrypting communications at the access point level would have been a Herculean task with such a large and diverse user population. The only other option was to encrypt communications at the gateway level by forcing wireless traffic back through a secure virtual private network (VPN). The problem, however, was that most of the vendors offering VPN based

“The Bluesocket system was just more polished, and the company was the first to market with a solution that worked.”

Ken LeCompte
Programmer/Administrator
Manager of Wireless at Rutgers University

solutions charged a considerable license fee per client, or didn't yet have a workable solution.

“This drove us to do something a little different,” says LeCompte, which was to consider Bluesocket, Inc. and a competitor as a wireless gateway provider, since they were the only two vendors offering VPN support that did not require client licensing. Bluesocket quickly surfaced as the preferred vendor because its user interface was far easier to manage than the competing system. “The Bluesocket system was just more polished, and the company was the first to market with a solution that worked,” recalls LeCompte.

At present, Rutgers' RUWireless serves 27 different buildings, including seven libraries, and consists of 23 Bluesocket Series WG1000 and WG1100 gateways and one Model WG2100 that was acquired as a beta system for testing purposes. Plans are to wireless-enable a total of 35 buildings across the campus by the middle of this year.

The Bluesocket Solution

In early deployments, it was not unusual for a department to have a Bluesocket gateway with only a couple of access points installed, since each operated as an independent wireless network. This proved to be a very expensive solution and a dramatic under-utilization of the Bluesocket equipment, however. As a solution, the RUWireless team developed a tunneling bridge technology that eliminates the need for installing a gateway in a department and tunnels all wireless traffic back to a centralized 'farm' of Bluesocket gateways.

The tunneling bridge technology significantly reduces the overall cost of implementing wireless, and adds an element of fail-safe protection since wireless traffic can easily be shifted from one gateway to another, or to a group of gateways dedicated as system backups.

Coupling the Bluesocket wireless solution with the tunneling bridge technology has also proven useful in authenticating wired ports. This was a significant task since these ports had to be available, if needed, for roughly 15,000 events and meetings per year, says Doug McCrea, assistant director of IT at Rutgers and one of the schools' first wireless 'customers'.

Another challenge Rutgers faced as it expanded its wireless network was to develop a reliable method to monitor wireless bandwidth usage, especially by students who might be tempted to engage in too much file sharing. The RUWireless team did this by developing a quota program that relied on the built-in capability of the Bluesocket system to monitor quality of service and generate highly granular logs of system activity. These syslogs are pumped out every 30 minutes or so, and then input to a SQL database table. The data in the table is compared to a sliding seven-day limit on total bandwidth of 2.5 gigabytes. Once users exceed this limit, they are automatically locked out of the wireless network until that seven-day sliding window expires.

Down the road, the college hopes to expand its wireless network to include outside areas where students and faculty congregate. For now, the university has 'lit up' some areas where students and faculty congregate by using directional antennas that project wireless access into those spots.



For more information, visit our Website at www.bluesocket.com

Or call:

United States

+1.866.633.3358 (toll free)
+1.781.328.0888 (Massachusetts)

Europe

+44 (0) 1483.549.814 (UK)

Asia/Australia

+65 6582.3881 (Singapore)
+64 9 489.9000 (Australia/New Zealand)