



December 2003

Wireless Networking at the University of Pittsburgh

Jinx P. Walton, Director
Computing Services and Systems Development
University of Pittsburgh
728 Cathedral of Learning
Pittsburgh, PA 15260
Telephone: 412 624-6100
E-Mail: jpw@pitt.edu

Founded in 1787 as a small, private school in a log cabin near the confluence of Pittsburgh's three rivers, the University of Pittsburgh has developed into a system consisting of its main campus, located Pittsburgh's Oakland section, and four regional campuses located throughout western Pennsylvania. The University's 9,600 employees, including 3,800 faculty members, serve more than 32,000 students through the programs of 18 undergraduate, graduate, and professional schools. Computing Services and Systems Development, the University's central IT organization, is committed to delivering reliable, current information technology resources in support of the University's dual teaching and research missions.

Wireless Networking Pilot

The demand for wireless network access at the University of Pittsburgh has increased dramatically over the past several years. In recognition of the need for increased network access and to keep pace with rapidly evolving wireless network technology, the University launched a pilot project in 2001 that involved several selected classrooms and a heavily used student area. The purpose of the pilot was to fully test the implementation of wireless networking technology prior to full-scale production deployment.

The pilot program resulted in the decision to base initial wireless service on the IEEE 802.11b standard using equipment that could easily be reconfigured to operate under newer standards such as 802.11a or 802.11g as support for these were reliably incorporated into commercially-available equipment. Also, the decision was made to standardize on the Enterasys RoamAbout R2 wireless access point. Although PPPoE was used as the authentication and authorization gateway during the pilot because it was already implemented for network user authentication on wired ports in the University's student residence halls, the decision was made not to use PPPoE in conjunction with wireless service due to its lack of scalability and the need for users to install and client software in order to connect to the network. We anticipated that wireless users would have laptops and handheld computers that they would need to connect to other wired and wireless networks. The need to use client software to access the University's wireless network was likely to create unnecessary support issues as these users moved from place to place.

Security, Authentication, and Authorization Using Bluesocket and the Central Directory Service

The inherent insecurity of wireless communication requires careful attention to security resulting in an early decision to implement 128-bit Wired Equivalent Protocol (WEP) and the requirement that all users authenticate to the wireless network using their assigned University computer account usernames and passwords. Access to sensitive data including financial systems, student records, and research data is prohibited over the wireless network.

In addition to the security provisions, the planned deployment of the production wireless network called for roles-based authorization of users in specific areas. Students, for example, are permitted to connect to the wireless network in public areas and classrooms. Faculty and staff may be permitted to connect within their own schools or departments, but not in others. The University's Central Directory System (CDS) includes information on all individuals affiliated with the University. CDS provides the cornerstone for the University's authentication systems. Because the role of each individual is maintained within CDS, the infrastructure for wireless user authorization was already in place.

In order to utilize the capabilities of CDS to authenticate and authorize users and to ensure that sensitive data are kept off limits, it was necessary to identify an appropriate wireless authentication gateway. Bluesocket was selected following an extensive evaluation of available commercial solutions and custom-developed applications in use at other colleges and universities based on its flexibility, ease of configuration and administration, security, and reporting features.

A major advantage of Bluesocket for our wireless implementation is that only a web browser, not client software, to access the customizable user login screen. It is completely compatible with the University's LDAP authentication service and provides the ability to restrict or allow access based upon the user's role within CDS. Bluesocket is compatible with all of the popular operating systems (Windows, Windows CE, Linux, and Macintosh) and supports multiple security protocols including IPsec, Point-to-Point Tunneling Protocol (PPTP), and Advanced Encryption Standard (AES). Bluesocket allows for roaming, even when using IPsec. Automatic failover is also supported. Management and configuration is Web-based, straightforward, and secure. Finally, Bluesocket supports RADIUS user accounting allowing the University to keep user access logs by using the RADIUS accounting services already in place.

Wireless PittNet

Authenticated wireless network access is available to students in various high-traffic locations on the Pittsburgh campus, including study areas in several academic buildings, the main library, and the student union lounge. Outdoor wireless access is available in selected areas. Faculty and students can connect to the wireless network in designated classrooms and University departments have the option to implement wireless network access in administrative offices.

The University's central IT organization is responsible for the design, installation and management of the wireless network. Site surveys are conducted to determine the optimum number of wireless access points needed to support the space configuration and the anticipated number of end user devices to be served.

Site surveys include consultation with the department to understand its planned use of wireless technology, monitoring of existing radio frequency signals for interference, measurement and evaluation of signal strength, and delivery of a report that describes the proposed layout of the wireless network.

Bluesocket WG-2000 gateways are used to authenticate and authorize users in student areas. WG-1000 gateways are used in departments and classrooms. The University supports four wireless network interface cards: Cisco Aironet 340/350 cards, the Orinoco Gold card, the Enterasys RoamAbout, and the Apple AirPort card. All cards must be Wi-Fi compliant and support 128 bit WEP encryption.

The Future Direction of Wireless PittNet

The University's goal is to offer secure, reliable wireless network service for the benefit of the University community. The University will continue to meet or exceed industry standards for security and performance to ensure that this goal is met. Bluesocket wireless gateways provide the most flexible, secure, reliable, and manageable solution identified to date and will continue to be deployed within the University's wireless network for some time to come.