Secure Wireless Networking at Simon Fraser University

Originally conceived to address capacity, our WLAN ultimately solved many other problems

By **Worth Johnson**

With the growing affordability of laptop computers, wireless access points, and network interface cards, it's not surprising that so many universities have recently installed wireless networks. Students and professors are mobile, and wireless networking is a powerful technology for delivering services to these users.

At Simon Fraser University, our interest in wireless networking goes back further than the past few years, however, having developed from concerns about capacity rather than mobility. Simon Fraser University is an interdisciplinary university located in Burnaby, British Columbia. Our university community includes nearly 25,000 students (of whom 17,000 are FTEs), faculty, and staff. Our interest in wireless networking increased dramatically in the mid-1990s. Computers were becoming increasingly important in research and instruction, and increased use meant we needed more computers, which meant more space. In 1994, one of our IT directors wrote a research paper warning that the university was going to have to build a new building—our biggest yet—simply to house the computers and computer carrels that students were going to need by 2005.

Going Wireless

This was not an option. An alternative was to enable students to bring their own computers to campus. By 1994, there was a huge growth in the popularity of portable personal computing devices such as personal digital assistants (PDAs) and enhanced function cell phones. We began asking ourselves, "If we're going to provide network services for a constantly changing pool of mobile computers, what technologies are likely to work?"

The university was already familiar with wireless computing: we had begun testing a proprietary, point-to-point wireless system in 1991. Now the pace and the scope of our testing increased. Between 1994 and 2001, we experimented with various proprietary systems. We grew concerned, however, about the costs and support headaches of implementing these systems on a broad scale. For example, one of them would have required us to keep track of the MAC address (a unique hardware address) of every computing system that students brought on campus—a daunting task, given the number of students, each with one or more computing systems. Also, we were not entirely satisfied with the quality of the support we received from the manufacturers.

The 802.11b Standard

During these years, standards bodies, universities, and computer companies contributed to the development of wireless technology, leading to the ratification of the IEEE 802.11 wireless net-

working standard in 1997 and the ratification of the 802.11b ("Wi-Fi") standard in 1999. These standards gave manufacturers a common blueprint for developing wireless technology. Wireless devices proliferated, prices fell, and many universities began deploying pilot projects, usually based on 802.11b.

In a typical 802.11b installation, a radio transmitter (an access point) is installed in the area where you want to provide wireless access for users. The access point is typically connected to a router on the traditional wired network. The access point functions as a doorway for wireless users, giving them access to the rest of the wired network. To communicate with the access point, a laptop needs a network interface card, a small radio transmitter about the size of a credit card. The network interface card communicates with the access point, creating a channel of radio waves between the laptop and the wired network. As long as the laptop remains within the coverage zone of the access point, the user has access to the network.

Because a single access point serves as a network connection for multiple users, universities can dramatically lower their wiring costs by going wireless where mobility has high benefits. Wireless has not yet been proven to be a replacement for wiring of permanent offices, however. Installing a single 802.11b access point eliminates the need for running cables for as many as 25 network ports. Adding access points and moving them to accommodate changing network needs are relatively simple tasks. With multiple manufacturers building 802.11b-compliant access points, universities now have the opportunity to buy the most affordable access point that meets their needs.

The 802.11b standard has two serious drawbacks, however. First, security in 802.11b installations is minimal. The 802.11b security standard, WEP (Wired Equivalent Protection), can easily be hacked. Networking experts have issued numerous warnings to 802.11b users, pointing out that WEP does little to prevent malicious users from gaining network access, spoofing networking devices, tampering with network traffic, and perpetrating a long list of destructive acts. WEP's crude "shared secret" mechanism for authenticating users is much less secure than the authentication systems most universities have in place for their wired networks. Not surprisingly, security quickly becomes a major concern for most organizations deploying 802.11b networks. As described below, it became our concern as well.

The second drawback to 802.11b is its poor support for campus-wide roaming. The 802.11b standard provides no mechanism for managing the network sessions of users roaming from one coverage zone to another if the zones are on different subnets. Although mobility is an attractive feature of wireless computing, 802.11b enables users to roam only in limited areas.

The Wish-List Approach

Because of the cost, manageability, and scalability issues, it became clear that our network would be based on the 802.11b standard rather than on any of the proprietary technologies that we had tested. By 2001, we had reached the conclusion that many universities are reaching now: that we would deploy a standards-based 802.11b wireless network. Despite its security and mobility shortcomings, 802.11b still represented a big step forward for wireless networking.

The time had come to move from testing to deployment. Aware of both the benefits and the risks of 802.11b technology, we developed a detailed wish list for our new network.

- *Ease of access for students.* We wanted to make it easy for students to bring computers to campus and connect to the network from locations where students congregate. Access points should be positioned in common student areas, such as the open seating areas and the library.
- *Campus ID.* Like many campuses, we assign each student, faculty member, and staff member a unique ID that grants access to the university network. We wanted to extend this authentication system seamlessly to the wireless network.
- *A universal Web-based login interface.* To minimize our support workload, we wanted students to be able to access the network through the same interface at home and on campus. Given the ease of use of Web portals, we wanted to have a Web login interface using the campus-wide authentication system already in place.
- *Ease of use for faculty.* To encourage faculty to make the most of their own computers, we wanted to make it easy for them to connect to the network

from various locations. Faculty will only take advantage of new online teaching tools if their overall online experience is positive. We wanted to eliminate configuration hassles, allowing faculty to trust their computers rather than fear them.

- *Improved wireless security.* We wanted a security system that overcame the security shortcomings of WEP. We wanted to prevent unauthorized users from accessing the network, spoofing authorized users, tampering with network traffic, and so on.
- *User-specific access rights.* We wanted to be able to enforce access rights based on user ID and group ID. Most 802.11b systems treat all users alike. Once authenticated, all users gain equal access to the network. By contrast, we wanted to control the access of users once they were logged in. Students and faculty should be able to access the network, but students should not necessarily have access to all the resources available to faculty and staff. A student roaming with a laptop should not be able to access the network subnet supporting applications such as university payroll systems, for example. And graduate students or teaching assistants might require broader privileges than undergraduate students.
- *Support for all standard IP devices.* We wanted to support all standards-based computers and PDAs, including PCs, Apple operating systems, PocketPCs, Palm Pilots, and so on. We wanted students to be able to buy the systems that made the most sense for them, and we wanted to be able to support newer, smaller, more lightweight devices when they appeared on the market.
- *Accounting and logging.* We wanted an accounting system that would enable us to monitor network usage, identify trends, and troubleshoot problems.

Selecting a WLAN Management Solution

We began evaluating wireless network management systems that would make 802.11b more secure and manageable. After reviewing a number of choices, in mid-2001 we selected the Vernier Networks System from Vernier Networks in Mountain View, California. The Vernier Networks System uses a two-tier network architecture to provide centralized control and monitoring of a wireless network, while scaling to support large numbers of access points in large numbers of locations.

The Vernier Networks WLAN management system consists of two types of components. A central Control Server integrates with our campus authentication system and allows our campus ID system to be applied to the wireless network. The Control Server also includes the Rights Manager, a Web-based application that allows our IT organization to define the access rights granted to specific users and specific user groups. The Rights Manager lets us define rights for a default guest account as well, enabling campus visitors to receive limited network access.

With the Rights Manager, we can establish role-based access controls that tailor network privileges to a person's role on campus. Access rights can be based on time and location, as well. For example, if we wanted to, we could define access rights that permitted only graduate students to access the business school library after 5:00 p.m. We're not ready yet to enact policies quite this precise, but it's nice to know that our network already supports this capability.

The other WLAN management component is the Access Manager. Each Access Manager manages network traffic flowing through a collection of access points limited only by the total throughput of the network segment to which the Access Manager uplinks. The Access Manager includes a traffic inspection engine that operates at Layer 3 in the network protocol stack. This layer sits above the basic connection layer of 802.11b. By working at this higher layer, the Access Manager can recognize important features—such as the source, destination, and time—of each network packet. It uses this information to enforce the access rights defined by the Control Server.

Our system provides security oversight missing from generic 802.11b installations. Because the WLAN management system tracks the login sessions of all users, it can detect and block sessions in which hackers are trying to spoof MAC addresses or insert data packets into traffic streams. Traffic from unauthorized users is blocked once it travels from the access point to the Access Manager; it never reaches the rest of the network. Traffic from authorized users is managed, based on the access rights defined for the traffic's user.

Another benefit of our implementation is that it overcomes 802.11b's shortcomings in the area of mobility. Because the WLAN management system is aware of each user's location and privileges, it can automatically tunnel connections across the network, preserving the login session of a user as she roams from one coverage zone to another. For example, a student can walk from one end of our campus to another along a major traffic corridor and stay connected to the network the whole way. The student's connection will be tunneled from one coverage zone to the next automatically. The student does not have to log in or log out; she simply continues working.

The WLAN management system provides the Web portal interface we were looking for, combined with the user-specific access rights we considered ideal. When a wireless user tries to access our network, he is presented with a Web login page that resembles login pages used on the wired part of our network. The user enters a user name (his unique university ID) and a password. The WLAN management system verifies this information through our central authentication system, Radius, and then grants the user whatever access rights we have assigned through the Rights Manager.

The WLAN management system also addresses the security problems in WEP. We can extend the authentication system we use on our dial-up network to our wireless network, so we do not have to rely on WEP's "shared secret" approach to authentication. WEP's inherent assumption that the access point contains the database of approved users is not scalable, nor does it support roaming. In addition, our system automatically detects security problems, such as duplicate network addresses and network abnormalities, and supports traffic encryption standards such as IPsec, L2TP, and PPTP, should we want to increase our security further.

Faced with the prospect of helping thousands of users configure their computers for the wireless network, the IT organization has come to appreciate another feature of our WLAN management system. Using technology developed through many years of research, the system automatically detects configuration problems in computers and dynamically adapts the network to provide connectivity. An authorized user whose computer is misconfigured can nonetheless gain access to the network because the system adjusts to accommodate that user. Every time the system does this, our IT organization is spared a support call. This capability, which would benefit a university of any size, is essential for manageably growing our network on campus.

Heightened security concerns and requirements in the aftermath of the September 11, 2001, attacks demand raising the base level of security on the Internet, and all colleges and universities, including those in Canada, will have to participate in this effort. Some institutions began 802.11 wireless implementations without architecting robust authentication and authorization services. Today, however, installing and maintaining a wireless network that does not include a solid authentication and authorization management system imbedded into the architecture would not likely be seen as acceptable network "citizenship." At Simon Fraser University, we feel confident that our system will provide at least the minimum security required in today's world.

Table 1 summarizes the features we looked for in a WLAN management system and explains the importance of those features to a university.

Table 1

Key Features for a University's WLAN Management System

Feature	Benefits for a University
Support for all IP-standard devices	■ Enables the university to deploy whichever access points it finds most cost effective ■ Enables students, faculty, and staff to use the computing devices they like best ■ Ensures compatibility with new 802.11 standards, such as 802.11a
User-specific and group-specific access rights	■ Enables the university to enforce focused security policies
Integration with existing authentication systems	■ Enables the university to use the same authentication systems for both wired and wireless access
Web portal interface	■ Provides an intuitive, easy-to-use login interface ■ Provides an interface that universities can use for both wired and wireless access
Support for roaming across subnets (wide-area mobility)	■ Enables users to roam about large areas without continually logging out and logging in ■ Overcomes 802.11b's limited support for mobility
Anti-MAC address spoofing	■ Prevents hackers from gaining access to the network by spoofing the hardware address of an authenticated user's computer
Support for IPsec and VPN encryption	■ Provides maximum security for encrypting wireless traffic, overcoming the weak encryption of 802.11b's WEP technology
Service management for misconfigured users	■ Dramatically lowers the support workload for IT teams deploying wireless networks
Scalable architecture	■ Scales to support larger networks; for example, deploying an Access Manager in a building newly configured with access points brings that building's wireless coverage zones into the campus-wide WLAN system ■ Supports multi-building and multi-campus deployments, while providing centralized monitoring and control
Layer 3 intelligence	■ Enables new security and service applications based on user ID, time, and location

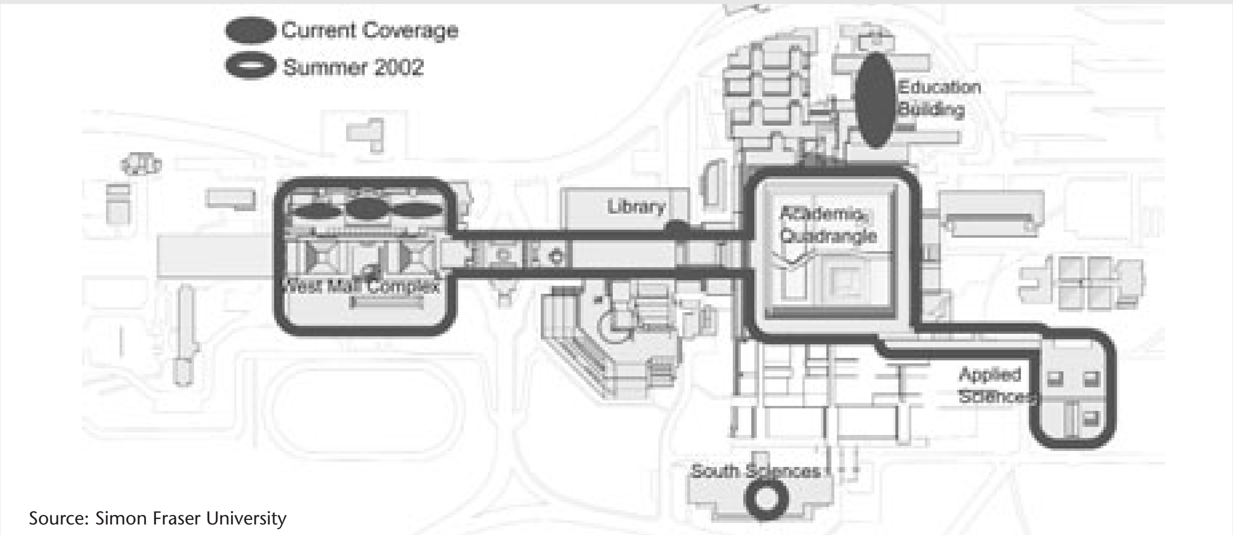
Deploying the Network and Spreading the Word

In August 2001, after experimenting with proprietary systems, we deployed our new 802.11b network managed by the Vernier Networks System. Over the summer of 2002, we extended the network to provide coverage in more buildings and along two traffic and study corridors across campus. Our 802.11b network now includes access points in the Faculty of Education building, the Applied Sciences building, in study areas, and in other interior and exterior areas on campus. (See Figure 1.) We have also installed 10 access points on the university's downtown campus and another 30 access points on its Surrey campus. Access Managers at these locations connect to the WLAN management system at our main campus, giving us centralized control over all our wireless locations.

To promote the use of the network, the campus store now sells network interface cards, and the university Web site featured a news story about the network and

Figure 1

Wireless Coverage at Simon Fraser University



Source: Simon Fraser University

the availability of network cards. In preparation for the rollout of the network, our campus computer store held a contest for the student community to name the network. Advertising was put into the student paper, and prizes were given for the name chosen and a runner-up.

Providing a Seamless Computing Environment for Students

Meeting our original goal, the wireless network enables students to bring their own computers to campus, where they can connect easily to the network without worrying about cables or plugs. Faculty, staff, and students use the same account and password combination whether they are dialing in or using the wireless network on campus. Faculty and staff moving from one office or teaching space to another never need to change their laptops' configurations.

Whether their devices are wired or wireless, students now access the network through the WLAN management system's sign-on page. Pleased with the login experience and integrated authentication of the WLAN management system, the university is using the WLAN management system for "triple A"—authentication, authorization, and accounting—on both its wireless and wired networks.

Enthusiastic Responses Across Departments

The new wireless network, with its secure login and support for roaming, has been well received. The Faculty of Education, for example, uses it for weekend professional development workshops in which teachers separate into working groups and spread out across the whole Education building. In good summer weather the groups meet outside on decks and grassy lawn areas. The department has 35 wireless laptops to loan out for workshops and for use by instructors.

Another user community that has responded enthusiastically to the network is students working in the library with their laptops. One area in the library has small rooms where people can meet to collaborate. Typically these rooms are booked solid. Some of the best feedback we have received comes from students accessing the wireless network from those rooms. They can now collaborate online, and they are pleased with how well everything works.

Also pleased are the university's faculty in the business school and applied sciences, whose departments are located at opposite ends of the campus and whose deans provided matching funds for the wireless deployment. Their goal was to provide coverage zones throughout their buildings. Our goal in the IT department was to create a corridor running the length of campus so that someone could walk from one departmental office to the other without losing network access. The university's recent expansion of its network meets this goal. The major traffic corridors on campus are covered by the 802.11b network, making the network widely accessible and thereby encouraging its use.

We now authenticate an average of almost 800 unique individuals per week on the network with 2,200 wireless connections. These users account for 45 gigabytes of network traffic across our campus backbone per week. What's important is that they are not lining up to use our 400 drop-in lab seats, and, more importantly, they are doing their computing work when and where it is convenient for them.

Winning the Trust of Faculty

One obstacle to introducing technology to the teaching space is mistrust. Over the years, faculty have had to rely on classroom computing equipment that is sometimes unreliable. It's not unusual for this equipment to be moved from room to room many times and for its configuration to become inconsistent. Frustrated by their experience with this unreliable equipment, some faculty members have come to mistrust computers in the classroom altogether. They trust their own computers for research, but are wary of using computers for classroom instruction.

One of our objectives is to provide network services that enable faculty to bring their own computers to the classroom, where the network can automatically adapt itself to each computer's network configuration. This enables faculty to teach using the computers they know and trust.

Thanks to the WLAN management system, faculty can once again trust computers in the classroom. Consider a faculty member working in his office and calling up a Web site that he wants to discuss in the classroom. The laptop is plugged into the wired network and has been assigned a fixed IP address. Because the WLAN management system supports network address translation and can automatically translate addresses for one network (such as the office network) into addresses for another (such as a classroom network), the professor can unplug the laptop from the network port in his office, walk across campus to the classroom, plug in the laptop on a different network, and continue accessing the Web site in front of a room full of students. His laptop remains on the wireless network throughout his walk, so Web site access is constant. The automatic address translation enables the professor to access the material he wants without having to learn how to reconfigure the laptop for a new subnet. He can use his own laptop—a system he is already familiar with and trusts—rather than an unfamiliar classroom system that might not be configured correctly.

The faculty have responded enthusiastically to this new capability. They can trust the network now. In their view, everything just works. This lays the groundwork for the use of more computers in the classroom.

Taking Advantage of Layer 3 Intelligence

Now that the basic wireless network is in place, we hope to develop new software that will take advantage of the WLAN management system's Layer 3 intelligence to improve the accounting system used for the university's print services. Like many universities, we provide a central printing service for students. When a student submits a job to be printed, the university's printing software identifies the job by the system name of the computer the student is using. Now that students are bringing their own computers to campus, though, the university has no way of ensuring that every computer is uniquely named.

The WLAN management system's Layer 3 packet-inspection engine can identify the student ID associated with every packet traveling on the network, including packets headed for the printer. We are looking into developing software based on the WLAN management system that would embed the student's authentication ID in the print job, clearly labeling every print job with the ID of the student who sent it. This solution, which would provide a universal system for tracking print jobs submitted by wired or wireless computers, is not possible without Layer 3 technology.

Lessons Learned

With our growing community of wireless users, it looks as though we have avoided the computing bottleneck our colleague predicted in his paper back in 1994. We have also addressed other problems, such as the trust faculty place in technology in the teaching space.

Following is a summary of the lessons we learned developing and deploying our wireless network:

- Apply technology to address one issue (capacity) in ways that can bring benefits in many other areas (mobility, increased use of computers in the classroom, and so on.) By simplifying network access, wireless networks can increase the computing capacity on campus, while lowering wiring costs and enabling students and faculty to use computers they already know and trust.
- Take advantage of the low cost and widespread availability of 802.11b products, but look for solutions that will make 802.11b more secure and that will make supporting thousands of 802.11b users more practical. Investing in a wireless LAN management system such as the Vernier Networks System can overcome the security problems of WEP, provide easy-to-use controls for controlling network access, allow integration with disparate authentication systems, and provide a foundation for future networking applications.
- Once your network has Layer 3 intelligence and can distinguish users, locations, and time, you can control your computing resources more precisely and develop applications that would have been inconceivable a few years ago.
- To promote new technology, take advantage of campus news channels, such as Web sites and newspapers, and institutions such as campus stores.
- Take advantage of offers from individual departments to contribute to part of a bigger project. When the faculties of business and applied science offered to contribute funding to create a wireless corridor between their buildings, the entire university benefited.

Ready to Grow

With our wireless network and WLAN management system in place, we are prepared to scale our network and continue our exploration of wireless technologies. We can scale our network simply by deploying generic, affordable 802.11b access points and an occasional new Access Manager. We can continue managing our user accounts through our campus-wide ID system, as we did before we deployed our WLAN, but now we can add user-specific, time-specific, and location-specific policies.

Furthermore, with an IP-compliant WLAN management system that supports the latest 802.11 standards, such as 802.11q supporting VLAN tagging for wireless users (not to be confused with 802.11g, which is a speed upgrade to 22 Mbps), we are ready to take advantage of whatever new developments come along in 802.11 technology that might prove useful on our campus. *e*

Worth Johnson (wjohnson@sfu.ca) is Director of Operations and Technical Support at Simon Fraser University in Burnaby, British Columbia.