Wireless LANs in Higher Education

Universities and colleges are among the most aggressive adopters of Wi-Fi technology. The trend toward more collaborative and open learning environments, fueled by the explosive adoption of mobile devices among students and faculty, makes higher education campuses fertile ground for wireless LANs.

Benefits of Wireless in Higher Education

Wireless delivers value for network users and the institution in general as well as network administrators. For students and faculty—a particularly mobile set of technology enthusiasts—wireless networking delivers productivity and convenience. For the IT staff, wireless represents a comprehensive broadband network solution that can be deployed without the hefty price tag or administrative overhead of traditional wired LANs.

Students & Faculty

- **Flexibility**: With anytime, anywhere access to resources, students can conduct schoolwork in unconventional settings—the campus quad, cafeteria, student center, library and many other places around the campus. Similarly, wireless enables instructors to deliver lessons outside of the classroom, such as lab exercises in outdoor settings.
- **E-learning**: Instructors can complement classroom instruction with on-line activities to create an integrated learning experience.
- **Communication**: By providing easy access to communications tools such as e-mail and on-line group discussion boards, wireless facilitates team building across multiple disciplines.

Institution

- **Revenue**: Wi-Fi presents potential revenue-generating opportunities. For example, universities could charge visitors for wireless Internet access. Also, colleges that may have once charged for long distance phone services, but have seen such opportunities evaporate in recent years, might consider introducing wireless VoIP services to students.
- **Competitiveness**: Today's students are more technologically savvy than ever. Wireless access throughout campus and student living areas helps academic institutions compete for students and faculty.
- **Innovation**: By fostering a more collaborative and creative learning environment, Wi-Fi enables the university to better support its academic mission and research objectives.

IT Organization

- **Scalability**: With the increasing awareness of consumer Wi-Fi products, students and faculty expect ubiquitous Internet access on campus. Wi-Fi enables the IT staff to quickly meet these demands across a large geographic area.
- **Flexibility**: Wireless can provide network access to locations where wiring is impossible (e.g., older buildings with historic value or asbestos concerns) or where access is only needed for temporary use, such as events facilities.
- **Lower cost**: Cabling for Ethernet can be a costly and time-consuming exercise. In comparison, wireless can be installed much more quickly and at a fraction of the cost. Moreover, wireless can virtually eliminate the operational overhead associated with adds, moves, and changes to the campus network.

Wireless Challenges in Higher Education

As universities migrate from hotspot to campus-wide deployments, and the perception of wireless changes from a “nice-to-have” to a transformational technology, network administrators will experience significant growing pains. The campus environment presents unique challenges for Wi-Fi technology, including:

Dense User Environments throughout the Campus

In Wi-Fi networks, clients contend for access to a shared medium. As the number of active users increases, performance typically degrades due to increased collision rates among clients seeking access. This poses a serious challenge for the university with a number of locations where the user population is dense, such as classrooms, libraries, labs, dormitories, and other common areas. To address higher density areas, access points are typically placed at a closer spacing. However, this creates co-channel interference especially for 802.11b or 802.11g deployments, where only three non-overlapping channels are available. Access points are placed closer together to take advantage of higher data rates, increasing the speed at which clients transmit data. However, access point RF propagation does not stop at the desired data rate.[1] This means that even careful planning to avoid adjacent APs having the same channel will not avoid the problem of co-channel interference.

Expansive Campus with Dynamic User Requirements

University campuses are typically large sites, consisting of dozens of buildings sprawled across hundreds of acres. Wireless LAN deployments are typically phased in over time, necessitating on going changes to the network design. The wireless deployment may also be modified as higher user densities are experienced, or new applications are deployed. These changes to the wireless LAN design are extremely complicated to plan, with potential ripple effects on the existing deployment, due to the limited number of non-overlapping channels available.

[1] While an access point can be set to limit data transmissions at only the highest data rates, specific 802.11 control information will continue to be sent at the lowest data rates, thus propagating over long ranges and causing significant co-channel interference.

One Network, Numerous Security Profiles

University network users include many different groups, including students, faculty, staff, visiting researchers and community users. Each group will require different access policies to maintain appropriate security levels for different network resources. Moreover, the university has little control over end user devices, making it very difficult to implement and manage security mechanisms that require client software.

Technology-savvy Users with Appetite for Advanced Applications

Students and faculty are quick to embrace new technologies for convenience and “just because.” While many enterprise organizations begin to adopt wireless for basic Internet access, university users will experiment with advanced applications such as wireless VOIP, which demands higher levels of quality of service to ensure reliable network performance along with less disruptive handoffs between APs as users move across the campus.

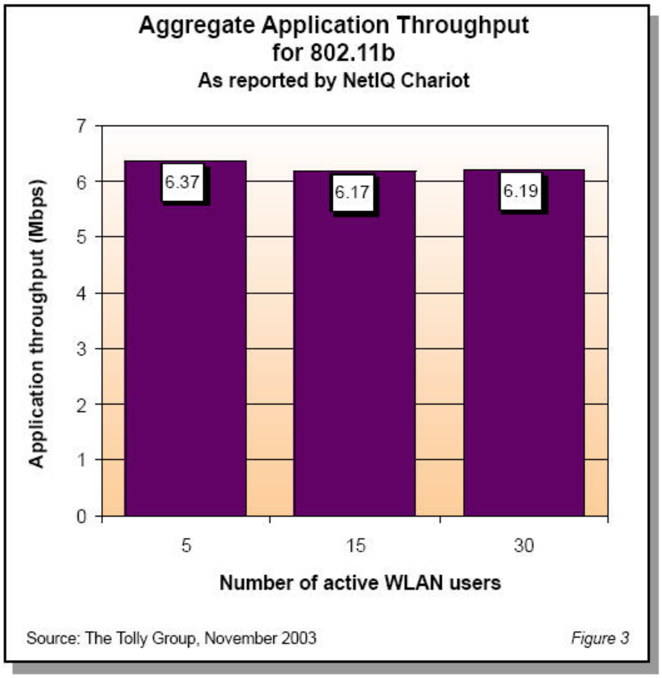
Benefits of Foundry Wireless LAN Technology for Education

While others have created WLAN switch architectures, they focus primarily on ease of deployment and central management of AP configuration parameters. Solving this problem is both important and necessary, but it is not enough. The key challenge is managing contention, interference and Quality of Service in a dense Wi-Fi environment with both data and voice clients. Foundry has done just that with its IronPoint Mobility Series.

Designed for High Density

Switch-like Performance on a Wireless Network

Foundry Wireless LANs employ Over-the-Air QoS that deterministically schedules client transmissions. This significantly mitigates client collisions, allowing high densities of clients to receive switch-like performance on the wireless network. For larger areas where multiple access points are used, Foundry WLAN architecture uses coordinated APs to manage co-channel interference and collisions from clients in other cells. The combination of Over-the-Air QoS and global coordination of APs results in unparalleled performance for even the largest networks in the world.



Source: The Tolly Group, November 2003

Figure 3

Eliminate 802.11g Performance Penalties –True Dual Speed Connectivity

In 802.11b/g mode, most wireless LANs penalize the faster 802.11g clients due to having to take much more time to transmit to the slower 802.11b clients. The Foundry IronPoint Mobility Series uniquely solves this problem with dual speed mode. Dual speed mode is the default for Foundry Access Points and is based on fair time on the channel, not fair access for 802.11b and 802.11g clients. In this mode, 802.11g clients perform up to five times faster than in standard wireless LAN systems.

The First True Converged Wireless LAN Network for Voice and Data

The Foundry IronPoint Mobility Series is a purpose-built converged voice and data network solution. Addressing head on voice application sensitivity to delay, jitter and latency, Foundry reduces or eliminates the wireless LAN impact on these factors. By building on the system's ability to control channel activity with its Over-the-Air QoS the IronPoint Mobility Series dynamically recognizes when a VoIP call is initiated and reserves bandwidth over the air for the call resulting in unparalleled call quality and connection reliability.

It is important to note that while IEEE is introducing 802.11e to solve some of the quality of service issues, this standard does not address several important areas. Foundry uses 802.11e and builds upon it to provide a much more robust system. 802.11e only delivers downstream Quality of Service performance. This means that client communications upstream to the Access Point are not managed and contention is likely in a dense environment. Foundry's patented call flow intelligence determines which streams are voice applications and automatically manages quality of service in both directions.

Additionally, 802.11e does not provide Quality of Service on a per application basis. This means that if a laptop is simultaneously running a soft phone for a voice over Wi-Fi call as well as checking email, the device receives the high priority assigned to it, not just the voice over Wi-Fi application. This situation worsens contention. Foundry's Quality of Service capability is on a per-application basis, not per-device, so each application receives the correct QoS settings.

Furthermore, 802.11e does not address the critical issue of handoff between APs or indirect sources of interference from hidden nodes or co-channel interference. Handoff can take up to several seconds, which will impair the quality of the voice call. Contention from hidden nodes causes additional delay and transmission errors, which will impact voice quality. Co-channel interference – the impact of multiple access points being heard by each other – will also add noise to the environment, causing quality issues. Foundry's Cellular WLAN Architecture coordinates APs and creates a Virtual Cell to eliminate handoffs and manage intercell contention. With Virtual Cell technology, multiple APs appear as a single AP to the voice client so no handoff or re-authentication is needed as the client roams. Client access to the medium is deterministically scheduled so that voice clients reach the network in a consistent, regular basis. These methods allow Foundry to deliver a five-fold increase in density of voice calls over any other WLAN solution.

Virtual Cell Technology Eliminates Channel Planning

A university's high density of clients, unique building topologies with multiple enclosed classrooms and long hallways, and older construction create a challenging environment for wireless LAN deployment. Other wireless LAN solutions require complex channel planning in an attempt to mitigate co-channel interference, which can add significantly to installation time and cost. Foundry greatly simplifies this process with Virtual Cell technology, which eliminates co- and cross-channel interference. With the worry of co-channel interference removed, Foundry access points are simply placed in the best positions to ensure complete coverage. Complex 3-dimensional site surveys to ensure that access points on the floor above or below are on different channels become a thing of the past and the network is up and operating more efficiently in less time.

Comprehensive and Flexible Security Framework

With so many mobile users entering and leaving the campus and the widely reported security issues, university network administrators are rightfully concerned about wireless LAN security. Fortunately, standards and product advances are facilitating secure wireless networking. The Foundry IronPoint Mobility Series supports advanced encryption and mutual client and network authentication using WPA. In addition, Foundry Access Points support up to 64 separate SSIDs each with a different security configuration. Each SSID can be mapped to a specific VLAN port, providing enhanced security by restricting network resources based on user type and application.

In addition, for guests on campus, the Foundry IronPoint Mobility Series supports a Captive Portal. Any guest that opens their browser will automatically be redirected to a secure SLL-based login page before being granted access to the Internet. This allows the university to audit use and provides an authentication method that universally works without requiring configuration of the wireless security settings to match that of the university network.

The Foundry IronPoint Mobility Series proactively searches and prevents rogue access points. By scanning all 2.4 and 5 GHz channels, the Foundry IronPoint Mobility Series can identify unknown and unauthorized access points, alerting IT administrators. Clients attempting to associate with a rogue access point can be automatically blocked, preventing all access to the university network. The rogue detection capabilities are integrated with the system to provide simultaneous on-going monitoring and client service, thereby eliminating tradeoffs between security vulnerability and service to clients.

Foundry Networks: Higher Performance Mobile Computing

By effectively managing channel access and eliminating AP co-channel interference, the Foundry IronPoint Mobility Series delivers unparalleled value and performance for the wireless campus, featuring:

— *Full-rate 802.11G even in mixed 802.11B/G environments*

— *Simplified deployment with lower installation and configuration costs*

— *Lower total cost of ownership*

— *5X voice calls by providing the QoS required of real-time application*

— *5X the number of active users (100 as opposed to 25 – 30) with switch-like performance in the dense environments typical of universities*

— *Loss-less handoff to allow students and faculty to roam without interruption*

— *A centralized architecture for deploying, managing and operating the wireless infrastructure across the campus*

— *A robust set of built-in authentication, encryption, and RF monitoring mechanisms to prevent network security breaches*

Conclusion

University campuses have been pioneers in deploying wireless LAN technology, driven by the large mobile population and a natural tendency towards innovation. While more and more higher education institutions are making the case for pervasive Wi-Fi coverage on campus, providing such coverage presents several technical challenges that are costly, difficult, or impossible to overcome with traditional WLAN system designs created to support small or hotspot deployments. Foundry's Wireless LAN System is the only Wi-Fi solution built from the ground up to serve high densities of users and provide high quality of service for today's robust applications such as voice. Foundry also greatly simplifies wireless LAN deployment for large university campuses with the Virtual Cell Technology which facilitates gradual migration towards pervasive coverage without time-consuming channel planning. The System also delivers basic capabilities expected by university IT administrators, including seamless roaming across subnets and comprehensive security policies that can be tailored to different user communities. Foundry allows universities to deploy pervasive wireless LAN networks confidently and cost-effectively.

Foundry Networks, Inc.

Headquarters

2100 Gold Street

P.O. Box 649100

San Jose, CA 95164-9100

U.S. and Canada Toll-free: (888) TURBOLAN

Direct telephone: +1 408.586.1700

Fax: +1 408.586.1900

Email: info@foundrynet.com

Web: http://www.foundrynet.com