CAMPUS NETWORKS

Wireless LANs in Higher Education

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 LAN technology.

BROCADE

Wireless networking delivers value for both users and network administrators in higher-education institutions. For students and faculty—a particularly mobile group of technology enthusiasts—wireless networking enhances productivity and flexibility. With the industry's broadest wired and wireless networking portfolio and a long history of delivering business-critical connectivity solutions, Brocade® offers all the components necessary to deploy a wireless campus. These include multifunction 802.11n Access Points (APs), a wide range of highly available and scalable wireless controllers acting as the nerve center of the Wireless LAN (WLAN), and the industry's leading wireless Intrusion Protection System (IPS).

BENEFITS OF WIRELESS TECHNOLOGY IN HIGHER EDUCATION

On college campuses worldwide, all stakeholders are well served by the deployment of a pervasive, unified access networking solution that includes both wired and wireless capabilities.

Students and Faculty

Students and faculty alike benefit from the advantages of a unified wired and wireless networking solution. Key advantages include:

- **Flexibility:** With anytime, anywhere access to resources, students can conduct schoolwork using wired and wireless clients in indoor and outdoor settings—the campus quad, cafeteria, student center, library, and many other places around the campus. Similarly, wireless networking enables instructors to deliver lessons outside the classroom, such as lab exercises in field settings.
- **E-learning:** Instructors can complement classroom instruction with online activities using advanced applications such as video streaming and Video on Demand (VoD) to create a more integrated learning experience.
- **Communication:** By providing campus-wide access to communications tools such as e-mail and online group discussion boards, wireless networking facilitates team-building across multiple disciplines.

Institutions

Institutions benefit from a unified wired and wireless network in the following ways:

- **Revenue:** A unified access network presents potential revenue-generating opportunities. For example, universities could charge visitors for wireless Internet access. Also, universities that might 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 the most desirable students and faculty.
- **Innovation:** By fostering a more collaborative and creative learning environment, wireless technologies enable the university to better support its academic mission and research objectives.

IT Organizations

The IT organization benefits from a unified wired and wireless network in the following ways:

- **Scalability:** With the increasing use of consumer Wi-Fi products, students and faculty expect ubiquitous high-speed Internet access all over the campus. A unified access network enables IT staff to quickly meet these demands across a large geographic area for the widest range of wireless and wired devices.
- **Flexibility:** Wireless networking can provide access in locations where wiring is impossible (for example, older buildings with historic value or asbestos concerns) or where access is needed only for temporary use, such as events facilities.
- **Lower cost:** Campus-wide cabling for Ethernet can be a costly and time-consuming exercise. In contrast, wireless networks can be installed much more quickly and at a fraction of the cost. The deployment of wireless and wired networking where appropriate—and seamless integration across both methods—reduces operational overhead associated with adds, moves, and changes.

CHALLENGES FOR WIRELESS DEPLOYMENT IN HIGHER EDUCATION

As universities migrate from a "hotspot" model to campus-wide deployments and as the perception of wireless changes from a "nice-to-have" to a transformational technology, administrators will likely face significant challenges with wireless technology, as described in the following sections.

Dense User Environments throughout the Campus

In wireless networks, users contend for access to a shared medium. As the number of active users increases, performance typically degrades due to increased collision rates among users seeking access. This poses a serious challenge for universities 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, universities often deploy wireless Access Points (APs) at a closer spacing.

However, this can cause co-channel interference, especially for 802.11b or 802.11g deployments, where only three non-overlapping channels are available. APs are placed closer together to take advantage of higher data rates, increasing the speed at which clients transmit data. However, AP Radio Frequency (RF) propagation does not stop at the desired data rate. 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 wide areas. Wireless LAN (WLAN) deployments are typically phased in over time, necessitating ongoing changes to the network design. The wireless deployment might also be modified as user density increases or as new applications are deployed. These changes to the WLAN design are extremely complicated to plan, with potential ripple effects on the existing deployment due to the limited number of non-overlapping channels available. While APs 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 potentially 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 requires different access policies to maintain appropriate security levels for different network resources. Moreover, universities have little control over end-user devices, making it very difficult to implement and manage security mechanisms that require client software.

Technology-Savvy Users with an Appetite for Advanced Applications

Students and faculty are quick to embrace new technologies for convenience and "just because." While many organizations are just beginning to adopt wireless networking for basic Internet access, university users want access to advanced applications such as wireless Voice over IP (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 BROCADE WLAN TECHNOLOGY FOR HIGHER EDUCATION

While some vendors have created WLAN switch architectures, they have focused 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 to meet the requirements of large-scale, dynamic environments. The key challenge is managing contention, interference, and Quality of Service (QoS) in dense Wi-Fi environments with both data and voice clients. The Brocade Mobility family of enterprise wireless products delivers all the required elements for larger WLAN deployments and also future-proofs the network for wireline voice quality over WLANs by:

- Providing a multilayer security approach
- Eliminating channel planning and co-channel interference problems
- Integrating easily with existing network infrastructure
- Providing a scalable solution set suitable for both large, sprawling college campuses as well as smaller, more compact facilities

To meet these objectives, the Brocade Mobility family leverages the performance, security, and reliability features of the new IEEE 802.11n standard, as described in the following sections.

Introduction of the 802.11n Standard

With the introduction of 802.11n, the field of WLANs is undergoing a paradigm shift as phenomenal as the beginning of WLANs themselves. The extraordinary data rates that the final 802.11n standard will support will ultimately solidify the realization of wireless and wired networking as peer campus networking options. Rich multimedia applications will be seamlessly streamed to every point in a facility, demonstrating much higher performance than is possible with legacy 802.11a/b/g technologies.

Historically, some universities have avoided ubiquitous wireless deployments, mainly because network administrators had concerns about network security, performance, and reliability. As a result, they deployed WLANs grudgingly and cautiously. Traditionally, these concerns were valid. Ten years ago, WLAN encryption standards were weak, data rates were slow, and wireless APs and routers were relatively difficult to manage and maintain. Today, however, technological advances have rendered those problems obsolete. In fact, today's WLANs can be as secure, as reliable, and just as fast as wired networks.

Higher Performance

The original 802.11 WLAN standard (ratified in 1997) offered maximum data transfer rates of only 2 Megabits per second (Mbps), which was sufficient for basic data transfers, but not nearly fast enough for video.

Wireless data rates have come a long way since then. 802.11n uses Multiple Input/Multiple Output (MIMO) technology, which can simultaneously transmit three data streams. 802.11n is very fast, offering throughput rates up to 248 Mbps in a clean environment and approximately 150 Mbps in real-world conditions—more than sufficient for high-bandwidth audio and video applications. Data also travels a long way with 802.11n—approximately 230 feet (70 meters) indoors and 820 feet (250 meters) outdoors.

Tighter Security

In the past, the security mechanisms available for WLANs were insufficient for the privacy needs of college campuses. An encryption protocol known as Wired Equivalent Privacy (WEP) received a great deal of bad publicity in 2001 when cryptography experts exposed its vulnerabilities. But just as Wi-Fi speed has come a long way, so has Wi-Fi security. Today, it's safe to say that a good Wi-Fi network can be as secure as a wired network because of the availability of a range of mechanisms for protecting a WLAN.

Wi-Fi Protected Access (WPA2), based on the IEEE 802.11i security standard, uses algorithms built on the Advanced Encryption Standard (AES). As the name suggests, it provides highly advanced key encryption. In addition, modern Wireless Intrusion Protection Systems (WIPS) enable administrators to automatically detect and locate rogue devices, prevent intrusions to a WLAN, and protect the network against Denial-of-Service (DoS) attacks. Various techniques such as "geofencing" enable administrators to provide access based on the location of wireless devices, adding physical security to wireless access.

Greater Reliability

In the past, a corporate WLAN typically included a series of autonomous APs scattered throughout an office or building. Finding an effective radio signal was often a matter of trial and error. Since there was no central management, administrators often would not know whether an AP had failed until a user complained.

Today, the best WLANs are very reliable. They are managed from a central wireless controller, with a graphical interface that shows the location and performance of every AP and user on the network. This enables administrators to identify potential problems and make proactive adjustments to prevent actual problems.

Today's corporate WLANs are extremely resilient and, in many cases, self-healing. If one AP fails, a neighboring AP assumes the workload. If the central wireless controller loses power, a redundant controller takes over its workload.

When running in conjunction with a high-speed Gigabit Ethernet (GbE) wired network, wireless APs can keep going (and take over) when a wired switch fails. Thanks to the advent of mesh networks, APs can communicate with each other without the switch. Similarly, APs can take over when a WAN link fails, enabling continued communication (and business uptime) within offices and facilities.

A SEAMLESSLY INTEGRATED WIRED/WIRELESS CAMPUS

In committing to advanced 802.11n wireless technology, administrators must ensure that every piece of the WLAN is both reliable and compatible with the other pieces of the network. The best way to ensure compatibility is to find an equipment provider offering a broad range of networking solutions (see Figure 1).

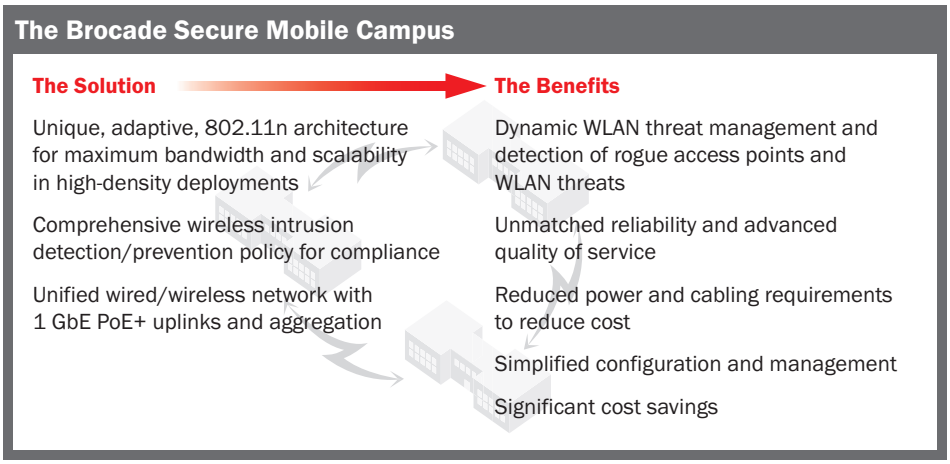

Figure 1.
Key benefits of a secure Brocade mobile campus.

With the industry's broadest wired and wireless networking portfolio and a long history of delivering business-critical connectivity, Brocade offers all the products necessary to deploy a wireless infrastructure. The Brocade Mobility family (see Figure 2) supports the latest draft of the 802.11n standard, providing leading-edge capabilities for a wide range of business benefits. This family includes:

- Brocade Mobility RFS6000 Controller
- Brocade Mobility RFS7000 Controller
- Brocade Mobility 5181 Access Point
- Brocade Mobility 7131 Access Point

Figure 2.
The Brocade Mobility family provides a comprehensive suite of wireless solutions.

Wireless Controllers

Brocade offers wireless controllers acting as the nerve center of the WLAN. A large enterprise-level switch, the Brocade Mobility RFS7000 Controller supports 802.11n. The smaller Brocade Mobility RFS6000 Controller extends 802.11n capabilities to midsized deployments.

The Mobility RFS6000 provides failover capabilities, helping to ensure high availability and reliability. It also offers comprehensive support for voice services on the WLAN, enabling advanced voice applications such as push-to-talk for both indoor and outdoor deployments. Furthermore, it includes an ExpressCard Slot expansion port, which enables a wireless WAN backhaul connection—supporting current and next-generation WAN technologies such as EVDO, HSDPA, and WiMax—and providing network resiliency for remote and branch offices in the event of wired backhaul failure.

802.11 Wireless Access Points

Brocade also offers a broad range of wireless APs for both indoor and outdoor deployments. The latest of these is the Brocade Mobility 7131 Access Point, which supports 802.11n. The unique design of the Mobility 7131 provides high-speed client access, mesh backhaul, and dedicated dual-band IPS functionality. The Mobility 7131 integrates a third radio in an expansion slot that can be field-upgraded to enable next-generation data and non-data applications such as WiMax and cellular backhauls.

Mesh Access Points

For many institutions, activities are not limited to the space bounded by four building walls—operations extend outdoors into remote and sometimes harsh environments. To mitigate wiring and to enable outdoor network connections, universities are deploying wireless mesh networks. In a wireless mesh network, the network dynamically routes packets from AP to AP to extend WLAN coverage to areas where Ethernet or fiber cabling is cost-prohibitive. Brocade Mobility 5181 and 7131 Access Points support these types of fast self-assembling and fast self-healing mesh capabilities.

Gigabit Ethernet to the Wired Network Edge

Because the transmit data rates of the 802.11n standard have increased significantly, it is now possible for wireless networks to routinely outperform 100-BaseT networks. The result is a need to intelligently upgrade wired network infrastructure to support 1 and 10 GbE on backhaul connections for 802.11n WLANs. Brocade FastIron® Series switches provide flexible and feature-rich Layer 2 and Layer 3 rack-mounted and modular 1 and 10 GbE switching solutions for building a high-performance and secure network edge. Upgradeable with high-density Power over Ethernet Plus (PoE+) capabilities, these switches also eliminate the need for an electrical outlet and dedicated UPS (power source) near 802.11n APs.

INDUSTRY-LEADING INTRUSTION DETECTION ACROSS WIRELESS/WIRED NETWORKS

As WLANs become a pervasive enterprise edge infrastructure in higher-education campus environments, the rogue AP problem has become much more complex. When thousands of neighboring APs are located near campus environments, simple rogue discovery is not enough to help administrators assess the risk level. Instead, administrators need a system that can provide automatic rogue management across both wireless and wired networks.

By automating the process of rogue discovery, analysis, threat assessment, and termination, the Motorola AirDefense® Intrusion Prevention System (IPS) for Brocade Mobility provides a comprehensive rogue detection solution that can scale to tens or hundreds of widely distributed sites. This solution offers important capabilities for enterprise WLANs:

- Robust security, including rogue elimination, intrusion detection, dynamic defenses, and forensic analysis
- Simplified wireless regulatory compliance, including flexible policy definition and 24×7 monitoring
- Cost-effective centralized troubleshooting, including remote troubleshooting, proactive monitoring, interference detection, LiveRF coverage, and historical analysis

Point-to-Point and Point-to-Multipoint Wireless Bridges

Most university campuses contain multiple buildings, and they require network connections between those buildings. The Brocade Mobility family is fully compatible with the industry-leading suite of Point-to-Point (PTP) and Point-to-Multipoint (PTM) wireless Ethernet bridges from Motorola, the strategic Brocade partner for wireless connectivity. These bridges provide highly reliable connections between buildings—even in high-interference or obstructed environments. Unlike competing solutions, the PTP bridges do not require a direct line of sight between nearby buildings.

CONCLUSION

Universities have been pioneers in deploying WLAN technology, driven by the large mobile user population and a natural tendency towards innovation. While more and more institutions of higher education are making the case for pervasive Wi-Fi coverage on campus, providing such coverage presents several technical challenges that are often costly, difficult, or impossible to overcome with traditional WLAN systems created to support small or hotspot deployments.

The introduction of 802.11n provides an opportunity for a holistic approach to upgrading the network edge, and Brocade Mobility solutions help maximize the value of this leading-edge technology. As a result, universities can significantly reduce Capital and Operational Expenses (CapEx/OpEx) and feel confident in the decision to deploy wireless technology as a mainstream campus networking option.

For more information about Brocade products, services, and solutions, visit www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

© 2010 Brocade Communications Systems, Inc. All Rights Reserved. 04/10 GA-WP-1424-01

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, and TurboIron are registered trademarks, and Brocade Assurance, DCFM, Extraordinary Networks, and Brocade NET Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

BROCADE