HIGHER EDUCATION **HOW-TO GUIDE**

4 KEY TIPS FOR UPGRADING TO AN 802.11N WLAN

WHY YOUR CAMPUS NEEDS AN 802.11N WLAN

Laptops, smartphones, and tablets are the devices of choice for the highly mobile “digital natives” found on every higher education campus. To handle the increased demand for anywhere, anytime access and bandwidth-heavy mobile applications, colleges and universities are investing in their Wireless LANs (WLANs) so students, staff, and faculty can push larger files and stream applications across the airwaves. As a result, wireless networking has evolved to the point that WLANs are now peers to wired networks in providing high-performance, robust, and secure connectivity to growing populations of students.

Enter 802.11n, the most recent, ratified IEEE standard for wireless networking, which enables a six-fold increase in data rates over earlier standards (802.11a/b/g), as well as increased reliability. When running optimally, 802.11n networks can reach speeds up to 300 Mbps, whereas WLANs based on older standards peak at 54 Mbps. That’s a huge boost in performance that enables universities and colleges to both meet the demands of their user community and protect confidential data as required under regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA).

BROCADE

4 KEY TIPS FOR UPGRADING TO AN 802.11N WLAN

Most institutions of higher education have investments in existing 802.11a/b/g devices and are being overwhelmed by the increased use of mobile devices and applications. As a result, campus IT departments are upgrading to 802.11n WLANs to support more users, cover a wider territory, and manage bandwidth-intensive applications. Their key goal is to elevate the trust level of the WLAN to that of the wired network, and ultimately create a unified wired and wireless network.

CAUSE FOR ATTENTION

Upgrading to an 802.11n WLAN provides universities and colleges with higher performance, additional range, and increased bandwidth. To make the move to an 802.11n WLAN and attain these benefits, you will need to consider the cost of new equipment (both capital and operational for maintenance and support), management complexity (especially if upgrading introduces a multivendor environment), and the impact on the wired network.

Since 802.11n WLANs are much faster and have higher throughput rates, legacy networking equipment may not have the capacity to handle the additional traffic load. When your WLAN becomes faster and more powerful by a magnitude of three or more, the performance of your wired network will suffer as the WAN and Internet gateways become overwhelmed by additional traffic.

Additionally, second-generation WLANs have a centralized hub and spoke architecture, which in 802.11n networking places more burden on the wired network to handle the increased flow of traffic between the controllers and the Access Points (APs). The result is network congestion, latency, reliability problems, scalability limitations, and slower speeds.

Just how much legacy hardware you will need to replace to prevent these performance and reliability issues will vary depending on your environment. Facility design is critical with wireless networks, as campuses can have many sources of radio interference and attenuation (caused by physical obstructions). Make sure to do an exhaustive analysis of your building's construction—down to stairwells, atriums, and pillars—to prevent lack of coverage.

It's also imperative to examine Radio Frequency (RF) considerations when determining which APs to deploy and where. In older 802.11a/b/g networks, data travels in a single, direct path from the user device to the AP. 802.11n networks operate via Multiple Input, Multiple Output (MIMO) technology, which means data can travel over multiple paths that reflect off walls and other objects. MIMO helps enable the higher speeds in 802.11n, but it also may render the placement of legacy APs unsuitable. Without thorough planning and simulations, you might not know until you turn on an AP and use it exclusively for 802.11n whether it is optimally placed. If it is not, performance might not be any better than the existing network. Fixing these problems later on can be time-consuming and expensive, as the movement of one AP can have a ripple effect across many network devices.

4 KEY TIPS FOR UPGRADING TO AN 802.11N WLAN

You might be able to eliminate wholesale wired infrastructure upgrades by deploying a few, targeted technologies on campus. Adaptive APs, for instance, can bridge traffic at the edge of the network locally, instead of routing data (which can include large multimedia files) to the controller at the center of the network and back. By doing so, universities can avoid major core network upgrades needed to manage edge traffic while preventing network performance issues. (Individual infrastructure plans for higher education environments can vary, depending on requirements and budgets.)

To get the most out of your migration to high-performance wireless technology, consider the following four tips. With careful planning, you can have a successful upgrade that maximizes the benefits of next-generation wireless technology.

TIP 1: SAVE WITH PROFESSIONAL SERVICES

Most college campuses have limited staff, so you might want to consider augmenting your technology team with WLAN professional services to help facilitate the planning and implementation process. Such services can help managers map requirements and understand network demands, recommend optimal design and routing paths, and maximize the use of existing legacy hardware. The deployment planning phase can help prevent the common oversubscription of equipment due to guesswork; the more ports and switches you install, the more opportunities for something to break, which increases complexity and costs.

WLAN-focused professional services experts typically analyze CAD drawings of a facility (to consider walls, shelves, lighting, and so on) and then model the environment. The result is a map of your organization's RF coverage based on predicted AP locations and user profiles.

These services also allow you to design against budget parameters. For instance, to stay within budget, you might be able to design for partial coverage in some locations on campus while maintaining wall-to-wall coverage in the classrooms and administration buildings.

TIP 2: MANAGE 802.11N CENTRALLY

Universities typically have multiple campuses and need to troubleshoot their WLANs remotely. Campus environments also have highly mobile student populations that must be re-authenticated as they move from classroom to library to cafeteria. A critical consideration during preparation is how to best manage and support your new WLAN.

Fundamentally, managing the policy and security of WLANs can be challenging, especially if the user interfaces among vendors are inconsistent. WLANs are also more difficult to troubleshoot due to the elusive nature of radio interference and the issue of attenuation (disruption from physical obstructions). Although you might not want to replace legacy equipment unless absolutely necessary because of cost or contractual issues, you might find that the best equipment for 802.11n will come from an alternate vendor.

One way to reduce complexity is to install a centralized management system, which allows you to create a network and security policy once and have the system do the translation, configuration, and communications to the different WLANs. This system also allows managers to remotely troubleshoot the entire network through a single tool and interface. This means that network managers no longer have to log into multiple vendor systems and correlate all of the information to configure the network or resolve a problem—which is a huge time saver. In addition, these systems have layers of functionality, including the ability to identify and classify possible sources of interference, deploy sensors to monitor airwaves 24×7, and obtain historical and real-time analysis of events.

The goal of a centralized network management system is to make it easy to manage the network from a single integrated dashboard while protecting the network from vulnerabilities and reducing costly support calls. This translates into better security, performance, and reliability, and lower overall costs. A centralized network management system also allows a fluid transition to an 802.11n WLAN by providing interoperability, an open systems architecture, and multiplatform support. Because such a system is also easy to use, it can minimize reliance on the highest level of support (level III) technicians by enabling first-level support staff to resolve issues without extensive manual troubleshooting or assistance from senior experts.

TIP 3: UPGRADE THE WIRED NETWORK TO GIGABIT ETHERNET

Budgets are always tight, but advanced technology is becoming a recruitment tool at many universities and colleges. Students, parents, and faculty place a high priority on the types of technology available when they are evaluating a college or university. When the WLAN can scale to meet the demands of ever-increasing mobile applications, online collaboration requirements, and virtual learning environments, administrators can leverage the technology to attract more students and retain faculty.

By making smart investments in your wired networks, you will have the highest-performing wireless networks available. Since the transmit data rates of the 802.11n standard have increased significantly, for the first time it is possible for a wireless network to routinely outperform a 100-BaseT network. That's why before you upgrade your WLAN you need to understand how the increased throughput of 802.11n will affect your end-to-end network performance.

With this knowledge comes the need to intelligently upgrade the wired network infrastructure to support Gigabit Ethernet (GbE) and 10 GbE on backhaul connections for 802.11n WLANs. To eliminate potential slowdowns across campus, ensure that your wired network edge is fast enough to support the new wireless speeds. Doing so will help you avoid network bottlenecks at the connection and uplink points.

In addition, you will achieve investment protection because your WLAN is able to accommodate the demands of students, faculty, and staff, as well as the influx of new mobile devices and applications. And as new, more powerful smartphones, tablets, and other mobile devices enter the market, your scalable 802.11n WLAN will be able to easily support them both inside and outside the classroom.

TIP 4: ADD LAYERS OF NETWORK SECURITY

Institutions of higher education are prime targets for security breaches. They house volumes of confidential financial, health, and other personal information about students, alumni, donors, faculty, and staff. Unfortunately, malicious hackers often see these environments as easy targets. With mobile devices accessing the network from all across the campus, a WLAN without multiple layers of security can serve as an open door to a devastating security breach. In the past, the security mechanisms available for WLANs were insufficient for the privacy needs of college campuses. But just as wireless speed has come a long way, so has wireless security.

Today, several security mechanisms exist to help WLANs achieve the same level of security as wired networks. For example, Wi-Fi Protected Access (WPA2), based on the IEEE 802.11i security standard, uses algorithms built on the Advanced Encryption Standard (AES) to provide highly-advanced key encryption. In addition, modern Wireless Intrusion Protection Systems (WIPS) enable administrators to automatically detect and locate rogue devices, prevent intrusions to WLANs, and protect networks against Denial-of-Service (DoS) attacks. Some of these systems will automatically shut down intruders without requiring any IT staff intervention. Various techniques such as “geofencing” enable administrators to provide access based on the location of wireless devices, adding physical security to wireless access.

Using intrusion protection tools along with multiple layers of security not only reduces security worries among IT staff and management, but might also prevent the theft of confidential university information.

MAKE YOUR NETWORK THE NETWORK OF THE FUTURE

Looking ahead, supporting a highly mobile population is sure to become even more complex. Sophisticated online applications such as video streaming, distance learning, and digital educational material will soon be standard, and an advanced wireless network that can deliver these new capabilities to users will be a must-have for every college and university.

Success ultimately depends upon cost-effectively designing, managing, and optimizing your new network to enable the high-bandwidth applications that 802.11n is designed to handle. Wireless networks can have the same level of reliability, performance, and security as the wired network. With proper planning and a well-crafted strategy, moving to an 802.11n network can be well worth the effort.

Network experts agree that by replacing older 802.11a/b/g wireless APs and clients throughout your environment with 802.11n access points and clients can provide students,

faculty, and staff with a higher quality experience, with improvements in signal-to-noise ratio, and better, faster connections—especially for voice and video learning applications.

READY TO GO?

While these four planning tips can help you prepare your transition to an 802.11n WLAN, planning and migration can be a time-consuming task. Fortunately, Brocade has the services and tools to assist network planners in this process. Brocade can help you build an effective WLAN infrastructure based on the innovative Brocade® Mobility family of solutions.

And finally, remember this: once you commit to using advanced 802.11n wireless technology, you 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 wired and wireless networking equipment. With the industry's broadest wired and wireless networking portfolio and a long history of delivering business-critical connectivity, Brocade offers all the solutions and technology necessary to deploy a reliable wireless infrastructure.

4 KEY TIPS FOR UPGRADING TO AN 802.11N WLAN

BROCADE RESOURCES

- Brocade Higher Education Web page: www.brocade.com/highereducation
- Higher Education Resource Center: www.brocade.com/highered
- Brocade Mobility WLAN Solutions: www.brocade.com/mobility

BROCADE MOBILITY WLAN SOLUTIONS

Brocade offers a comprehensive portfolio of products and services for 802.11n WLANs.

The Brocade Mobility solution is a third-generation 802.11n network solution that includes 802.11n migration planning, wireless infrastructure, multivendor management, security and compliance, troubleshooting, and spectrum and forensic analysis.

This distributed, intelligent infrastructure can help institutions of higher education to:

- *Extend legacy equipment for investment protection*
- *Increase security by integrating protection into APs*
- *Reduce the number of controllers needed in the WLAN*
- *Minimize downtime through sophisticated traffic routing across the campus*
- *Provide ease of management and significant network administrator time savings*
- *Attract students and retain faculty*

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

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