A CAMPUS TECHNOLOGY
CUSTOM WHITE PAPER

www.campus-technology.com

NONSTOP WIRELESS

Securing WiFi Networks in Higher Education

Two institutions provide a blueprint for successfully deploying a secure, high-performance WiFi network on their campuses.

Table of Contents

Executive Summary

For years in the corporate world, networking gurus have spoken of something called “always-on enterprises.” These are businesses that require connectivity 24/7, enterprises in which users must be able to access their WiFi all the time. For these entities, reliable wireless connectivity is an irreplaceable aspect of the network, something as important as a dial tone on the telephone system.

Now, this networking philosophy is becoming prevalent in higher education, as well.

Students are used to constant connectivity—they come to campus with their own personal laptops and expect to be able to connect to the Internet whenever they want, from wherever they want. When these users don’t get their way, they go out and set up their own access points, a reality that causes nightmares for IT managers charged with keeping the campus network safe. To combat this phenomenon, academic technologists are being forced to make sure their campus wireless connectivity boasts top-quality performance, stellar security, easy-to-use management, and omnipresent reliability.

Everywhere, anytime and reliable WiFi access has become mission-critical to the overall health of higher education institutions. Without it, wireless is just another way to connect to the Web.

Sponsored by:

TRAPEZE NETWORKS
A BELDEN BRAND

In this paper, we look first at the challenges of WiFi in higher education and what schools must consider when planning their deployments. We then examine Trapeze Network's NonStop Wireless solution and see how two campuses are using this technology to meet the WiFi demands of their students, faculty and staff.

The unique challenges of WiFi in higher education

Personal laptops are now mandatory at practically every college and university in the US and Europe, strengthening the position of higher education as the fastest adopter of wireless LANs worldwide. Higher education as an industry also leads the demand for higher data rates offered by 802.11n access points**.** Because of the prolific use of laptops, PDAs and other WiFi devices, WiFi coverage is needed everywhere, including outdoors. Put simply, it has become the number one networking and telecommunications priority of the new millennium.

With this in mind, most academic technologists consider three main aspects of mastering WiFi in higher education:

Easy Deployment and Management

Managing large multi-site wireless networks spanning hundreds of acres is no trivial task. That's why most network administrators take a great deal of care to thoroughly evaluate the management tools they will use to plan, configure, deploy and monitor wireless networks. The right management tools can dramatically affect the price and performance of the initial implementation and minimize the time it takes to maintain the network and troubleshoot issues as they arise.

Performance and Scalability

When a school regularly has hundreds of students all opening their laptops in the same auditorium at the same time, that institution needs much more than high-performance; it needs intelligent traffic management to balance loads and ensure identity-based access profiles can be both enforced and honored.

Mission-Critical Availability

With thousands of students practically living on the Internet every day, reliability is crucial—not just access-level reliability, but system-level reliability. This kind of foolproof system is needed to prevent a catastrophic meltdown of services if one critical WLAN controller should fail.

Beyond these three aspects of wireless in higher education, technologists also must grapple with the challenges of serving large pools of intelligent users. With university wireless, these technologists often see people trying to break the rules by installing and operating their own access points. How do these IT gurus stop people abusing the bandwidth? How do they stop people abusing the network as a whole? A manageable, scalable WiFi solution can help.

NonStop Wireless from Trapeze Networks

The NonStop Wireless solution from Trapeze Networks comprises access points, controllers, a lot of management and security capabilities and locations, and of course, the systems software, which is the "secret sauce" that makes it all work. Whether it's nurses getting voice and messaging while on the move, or retail staff doing price checks and inventory management from anywhere in the store, or a teacher being able to deliver classes outdoors, almost every industry has highly mobile workers that can benefit from uninterrupted connectivity anywhere.

The growing dependence on wireless for primary connectivity places new demands on the WLAN infrastructure: demands for a secure, high performance, highly reliable and easy-to-manage wireless network. The Smart Mobile architecture from Trapeze Networks ensures mission-critical mobility while delivering uninterrupted campus-wide network access, even in failure conditions.

Trapeze solves related processing problems with local switching, by letting the access points do a lot of the work of forwarding traffic.

To date, Trapeze has installed NonStopWireless at some of the world's largest institutions. For example, Cardiff University in the United Kingdom is the largest wireless network in higher ed: 65 buildings and 33 square miles of footprint. That's a Trapeze network. Other institutions in the US have deployed NonStop Wireless to meet their WiFi needs; the University of Minnesota is in the process of deploying 9,000 802.11n access points over a 1,200-acre site.

With most WLAN solutions, configuring N:1 redundancy is complex and when a crisis happens, hundreds of users still get disconnected. Trapeze's controller virtualization approach is different: It delivers non-stop availability even at a session level, promises hitless failover with zero downtime, and requires no maintenance to keep track of ongoing adds, moves and changes. In particular, the offering excels in four areas: performance, security, management and reliability.

Performance

Unlike other WLAN systems that rely solely on centralized forwarding at the WLAN controller, the Trapeze Smart Mobile architecture also allows distributed forwarding at the access point to offload WLAN controllers and optimize traffic flows for latency sensitive applications such as voice. Trapeze also has implemented many other innovations to maximize bandwidth availability, and control utilization.

What's more, Quality of Service (QoS) profiles and bandwidth limits can be set on a per-SSID or per user basis giving granular control over which applications get most bandwidth and priority treatment. Patent-pending Band Steering features also transparently cause 802.11a-capable devices to use the 5 gigahertz band, recovering 30 to 40 percent more usable capacity, without requiring any client or network configuration changes.

Trapeze is also unique in enabling automatic client load-balancing across multiple access points, even between access points managed by different controllers.

Security

Since 2002 Trapeze has played a lead role in the standards bodies and has been among the first to implement new standards that relate to security and voice service enablement. Trapeze continues its leadership today, as the elected chair of IEEE 802.11 Task Group, as well as the chair of two other WiFi Alliance Task Groups covering Network Management and Security.

Trapeze provides the highest levels of security for both voice and data including the WPA/WPA2 standards and all WMM subsets, and is one of the few WLAN vendors with a validated FIPS 140-2 certified solution. Trapeze also offers enhanced WIDS/WIPS protection, to prevent even the most determined hackers, and with SmartPass 7.0, enables up-to-the-second dynamic adjustment of users' access privileges based on their location, time and date, traffic, and more.

Easy-to-Use Management

With its unique three-dimensional predictive planning capabilities, Trapeze Networks simplifies WLAN deployment. In fact, Trapeze's planning takes into consideration both environmental conditions and WLAN capacity requirements, in order to compute the optimum placement and configuration of access points for best price and performance.

Trapeze Networks offers advanced WLAN management capabilities with RingMaster, the management platform that makes it easy for network managers to plan, deploy, configure and monitor every aspect of their multi-site networks completely remotely, all from a single console.

High Reliability

High-availability demands system-level resilience, not just device-level resilience. With the latest evolution of its Smart Mobile architecture, Trapeze Networks delivers non-stop availability with hitless failover.

The traditional approach to redundancy is to have a fully-loaded, fully-configured device ready to back up any other device which may fail. But many-to-one redundancy is inefficient, as 99 percent of the time, the backup device sits idle. Trapeze's approach is different; think of it as controller virtualization.

Under the Trapeze strategy, a group of controllers is configured as a Virtual Controller Cluster that allows each controller to act as a backup for any other. This unique many-to-many redundancy approach keeps all devices in service, so you know they work. It also eliminates the need for expensive backup devices that rarely get used, and makes full use of access point licenses spread over multiple controllers. But much more important is the unmatched reliability benefits of hitless failover for active sessions.

Because WLAN controller failure no longer has any impact on user sessions, this capability allows instant capacity scaling, and unscheduled in-service upgrades, all with zero downtime.

Importance of Location Tracking

Location can be a huge component in delivering a different type of security over a wireless network. This is why, earlier in 2009, Trapeze Networks acquired Newbury Networks. With the technology subsumed through this acquisition, Trapeze now has the ability to offer conventional access control with radius servers, but also can control access to a customer's wireless network based upon location. The technology can be used in a number of ways: either to lock users out or to change the types of services that are available to people depending on where they are.

In the world of higher education, officials can manipulate this technology to make sure students are paying attention during class. For example, say a school has 200 people entering an audito-

rium at one time. Based upon their location, administrators can literally lock down the users from doing anything else except browsing a number of pre-approved Web sites. They can't use Instant Messenger. They can't text. They can't do anything except visit the Web site that the lecturer is using in his or her notes.

This development not only benefits those faculty members who are trying to teach a class, but it also helps students who might otherwise procrastinate and not focus on the subject at hand.

Case study: Ohlone College

Ohlone College, a small two-year school in northern California, has experienced the benefits of nonstop wireless first-hand. The institution has two main campuses—one in Fremont and the other in nearby Newark. It serves roughly 8,500 full-time equivalent students, and has 465 part- and full-time faculty members, as well as a staff of about 235. All told, the school has spread 135 access points across both campuses. In the summer of 2009, the college broke ground on a new student services building in Fremont.

Historically speaking, the geography of the Ohlone campuses presented a huge challenge for reliable wireless. First, the campus is located on the side of a hill, making the distribution of wireless signals throughout campus challenging, even with an ample number of access points. Secondly, particularly on the Fremont campus, square footage was a problem, as well. This campus measures 234 acres—a huge footprint for a two-year school. Together, these problems combined for spotty service and a host of associated problems.

According to CTO Bruce Griffin, this prompted the drive for a better wireless solution across the board.

The Objective

Before evaluating wireless LANs and deploying a system, Griffin and his team needed to understand the impact of mobility on the network infrastructure, applications and users. While the school's user community was enthusiastic about wireless, the IT staff was initially concerned about security and manageability, particularly client support. Supporting thousands of faculty and student demands required seamless integration between wired and wireless networks, strong security, and ease of wireless LAN management and client support.

When Griffin first arrived on campus in December 2007, the institution took a "systems" approach to wireless; technologists looked at the technical aspects of the equipment but really weren't viewing it as a service they provided to our end-users. In his words, they focused more on hardware and software than the actual impact wireless made on the learning community.

"There were some profound conflicts that were arising as a result," he says. In particular: Ohlone had two separate wireless networks; an open one for students and a secure network for administrators and other employees.

The double networks spawned other problems. First, users openly questioned which network they needed to access in order to utilize specific resources. Furthermore, spotty coverage led to campus-wide uncertainty about the location and status of wireless access points.

"We'd see a lot of meeting time that was spent with people asking, 'Is wireless up?'" Griffin remembers.

Users attempted to stabilize spotty coverage by setting up rogue access points of their own. Among the existing networks, there were other issues. The unsecured, campus-sponsored network frequently was victimized by hack attacks, viruses and malware outbreaks. The secured campus-sponsored network had difficulties as well; though it relied on a widely available certificate, the certificate had serious compatibility issues with Apple computers, and when users couldn't get the certificate to work, many of them just started using the open network.

"From my perspective as the guy in charge of running this stuff, it was frustrating to say the least," Griffin says, looking back.

Change on the horizon

In early 2008, plans for the new student services building on the Fremont campus jumpstarted the effort to revitalize the wireless network at Ohlone. Griffin and his counterparts sat down and started thinking about some of the features they would want from a new network. On their list:

- Ability to use wireless phones over the wireless LAN.
- Improved coverage.
- Wireless access for visitors.
- Future-proofing for changes to come with 802.11n.
- Seamless integration between wired and wireless coverage.

With this list in hand, a team of technologists set out to review a number of different wireless products. After a lengthy review, team members settled on NonStop Wireless from Trapeze Networks. According to Griffin, the team selected Trapeze for a number of reasons:

- The NonStop Wireless technology played nicely with Juniper Networks, which was the vendor behind Ohlone's wired network.
- Trapeze already was on campus; much of the pre-existing wireless technology had come from this vendor.
- Pre-existing Trapeze mounting brackets for access points meant the school did not need to invest in new mounts.
- Trapeze presence on campus also meant Griffin and his team did not have to retrain their staff.

Implementation

Ohlone technologists made the final decision on opting for Trapeze toward the end of 2008; implementation began immediately. The school initially deployed the Trapeze wireless LAN Mobility System in Hyman Hall, which is home to the largest concentration of computers on campus as well as the math and English departments.

The original wireless LAN covered all classrooms, labs and offices in Hyman Hall, and supported up to 400 users across 45,000 square feet. The WLAN also includes switches in the building's server room and several access points mounted on walls and ceilings. By the summer of 2009, this network had been expanded to the entire Fremont and Newark campuses. School technologists had replaced every access point on campus—a total of 135.

In addition, technologists had installed more than two dozen access points in the new student services building on the Fremont campus—all of which were working before the building was even formally open.

To maximize usability, Ohlone also opted for SmartPass, proprietary Trapeze software that enables control over guest access to wireless networks. One of the functions of SmartPass is to give customers dynamic types of authorization. With it, Ohlone academic technologists can tweak security policy on the fly; if a user starts abusing bandwidth and downloading streaming video continuously, the technology empowers network administrators to cut off the user completely. SmartPass gives Ohlone administrators the ability to dynamically change people's authorization attributes. Not only does this technology provide guests with access to the wireless network, but

Griffin says it also will reduce some of the administrative issues which he and his colleagues have in IT.

"It should enable us to give them a better service-level out at the edge, where they're actually dealing with the individuals who come onto campus," he says. He adds that the school is looking to eliminate its old certificate method sometime in 2010.

Overcoming Obstacles

No technology implementation is without its pitfalls, and Ohlone's experience with its new wireless network was no exception. Griffin says the biggest obstacle associated with the effort was communicating information about the upgrade to students and other users; he said Ohlone tackled this with regular email blasts informing them of the change.

Another obstacle: the new student services building. Until Ohlone gets people into the building, using the new wireless network in a live environment, campus technologists really won't be able to determine the best placement for the new access points.

"Placement [of access points] and the corresponding performance is a key aspect of delivering a reliable wireless service," he says. "It's impossible to get things 100 percent right on these buildings and we want to make sure we're receptive to areas where we can improve early and move forward."

In the immediate future, Griffin says he and his colleagues must fine-tune their access points, and continue to tweak access-point placement. One advantage: stronger technology overall. When the college upgraded to NonStop Wireless, it bought access points with stronger radios, meaning it ultimately will need fewer access points to cover the same square footage. Griffin says this has yielded between a half-dozen and a dozen spare access points that technologists can use to expand coverage.

Another plan for the near future: detecting and eliminating rogue access points, which mysteriously continue to plague the campus network.

So far, Griffin and his colleagues are very happy with the effort. Rogue access points are down, and users have enjoyed seamless integration between Ohlone College's wired and wireless networks.

With the new Trapeze system, users also keep their wired VLANs and subnets, access control lists, authentications, roaming policies and history, location tracking and bandwidth usage based on their individual identities. These unique credentials stay with each user as they move from wired to wireless and back again. Traffic isolation therefore is maintained among VLANs across the wired and wireless networks. Faculty and staff traffic remains separated from student traffic—and thus secure—no matter what.

Down the Road

Farther down the road, technologists at Ohlone College have their sights set on much larger issues. First and foremost on this list is the 802.11n protocol, which already is being adopted by a number of corporate environments. Griffin says Ohlone is testing an 802.11n connection in a number of spots on campus already.

“It’s an amazing improvement to what people have had before,” he says of the faster and more efficient protocol. “It opens up the ability to perform a number of tasks on wireless that we weren't able to do previously.”

One of these tasks is videoconferencing; with a brand new videoconferencing center on the Newark campus, the new technology should facilitate the wireless distribution of videoconferencing within the year. Griffin notes that faculty members hope to leverage this feature to increase the number of distance education classes. Staff members also hope to utilize it to hold “meetings” in real time with users all over the area.

Future-proofing also is in the works. Though the 802.11n wireless protocol is still relatively new, Griffin says that by preparing for these standards, Ohlone can start to move away and phase out all 802.11b connections on campus—a move that should make the overall network even faster.

“This should really boost performance on the N side of the access points,” he predicts. “It’s all part and parcel of an improved wireless service.”

Case study: Kean University

A new deployment of NonStop Wireless also has transformed the computing environment at Kean University, the third-largest four-year state institution in New Jersey. The university, located in Union, N.J., has roughly 13,000 full-time students and sits on roughly 150-plus acres.

Across that landscape sit roughly 40 buildings; until recently, the school's wireless deployment consisted of indoor coverage only.

As part of a new, centrally managed wireless network, Kean has paved the way for a total conversion to 802.11n, the forthcoming wireless standard that is faster and more secure than its predecessors. Joe Marinello, the institution's director of IT, says the effort has revolutionized computing across the board.

The Objective

According Marinello, Kean's original goal with wireless was simple: to deliver wireless to every nook and cranny of campus, indoors and out. Marinello says the need arose from a preponderance of mobile computing devices on campus—students, faculty members and other users connecting without wires whenever possible.

Perhaps nowhere was this switch more evident than in the residence halls, where students had both wired and wireless connections. Following an 802.11a, b and g wireless deployment of 800 access points between 2005 and 2007, Kean officials saw the use of the wired network dropping pretty much day by day, month by month, semester by semester. Marinello says it got to a point where 85 to 90 percent of our residence hall users were relying on wireless connectivity exclusively.

"We saw the writing on the wall that this was where we would have to take the campus network in order to support the changing needs of our users," he says. "We had to give them what they wanted."

With so many users embracing wireless, Kean officials decided they wanted to expand the campus wireless network in such a way that prepared it for 802.11n wireless down the road. The expansion progressed on two fronts: more indoor coverage and new outdoor coverage. To manage both of these high-demand wireless zones, Kean officials sought a contiguous, enterprise-class solution they could monitor centrally.

After considering solutions from a number of different vendors, Marinello and his colleagues settled on NonStop Wireless from Trapeze.

Implementation

The decision was essentially an expansion of a pre-existing Trapeze deployment. Earlier this decade, when Kean had added the 800 access points, the university deployed an OEM of the Trapeze product through Nortel Networks, who at the time was providing the school's wired switch gear.

This time around, however, after Kean decided on for NonStop Wireless, Marinello and his colleagues opted to eliminate the middleman and buy direct through Trapeze.

Trapeze came in and updated the school's older access points with new firmware that made the devices capable of being controlled by the single-management platform. At the same time, Kean worked with Trapeze technicians to install new APs. Because both older and newer devices fit in the same mounting brackets, Kean did not have to spend extra money on new brackets for the new devices.

Expansion of the indoor wireless network was first—Kean standardized on Trapeze MP-432s. To determine where to place new APs in existing buildings, Marinello and his colleagues used RingMaster software from Trapeze. When it came time to figure out where to place the devices in new buildings, the Kean team sat down with Trapeze engineers to review architectural blueprints and CAD files to determine the best spots.

"We couldn't physically site survey these buildings because many of them were in the process of being built," Marinello says. "Trapeze took our architectural drawings, put them through their software, predicted coverage areas and generated coverage maps from those predictions."

With the indoor network squared away, next came the development of the outdoor network, powered by Trapeze MP-632As.

Kean officials approached this as a physical site survey and it took about a week. As part of this process, Trapeze experts sectioned off the campus into different areas and went around with Radio Frequency (RF) testing equipment to measure signals in every spot. From this, Trapeze came up with a comprehensive plan that would disperse about 70 radios to cover all of the university's outdoor needs.

In terms of cost, Kean spent roughly $400,000 to cover the entire outdoor campus, including athletic fields and common areas. On the indoor side, the bill ran about another $200,000. Marinello says that the largest cost of the indoor deployment was to replace all of the older access points. He estimates that to retouch the old devices cost $1,000 per device.

Overcoming Obstacles

While the Kean upgrade to centrally managed NonStop Wireless was relatively uneventful, the university did experience a few minor hiccups as they upgraded and expanded their wireless coverage.

One of the biggest issues Kean came across was the physical deployment itself. Because the institution has been around for most of the last century, it has buildings that range in age from brand new to nearly 100 years old. Marinello says that in some cases, the simple process of taking the new APs and finding places to put them proved to be an incredible challenge.

“Where should we put the APs? To what should we mount them? How are we going to get infrastructure to the APs to connect them?” he says. “We asked ourselves all of these questions and more to make sure we were going about things the right way.”

Another challenge: Managing user expectations. Marinello says that Kean users were so excited about the new wireless network that many of them hoped to abandon the wired network forever. To make sure the user base didn’t tax wireless bandwidth too dramatically, Kean technologists engaged in an aggressive campaign to inform users that certain tasks—downloading high-definition video, for instance—were better suited for the wired network, and should continue to be conducted there.

Down the Road

Once Kean rolls out wireless in a handful of new buildings on campus, the biggest plan for the university down the road is to migrate the entire wireless network to 802.11n. Switching over the indoor network is already underway as part of a pilot program with Trapeze Networks; migration on the outdoor network wasn’t expected to occur until early 2010.

Marinello says he and his colleagues have vowed not to market the new capabilities until both segments of the contiguous network are working perfectly.

Further down the road—perhaps in 2011 or 2012—Marinello says the university likely will look into deploying voice and other applications over the 802.11n wireless network. Already, members of the Kean IT staff have investigated replacing the handheld radio devices that are used to communicate on campus with VoIP units.

These same technologists also are focusing on developing applications that would deliver information about everything from class schedules to university history over the wireless network to user mobile devices.

“The goal is to take full advantage of our new network and make the computing environment here as robust as possible,” Marinello says. “We can do it all, thanks to Trapeze.”

Conclusion

The need for nonstop wireless has never been greater than it is on college and university campuses today. According to ABI Research, 99 percent of North American universities will have a WiFi network on their campus by the year 2013. The majority of these installations will include 802.11n.

Not surprisingly, student expectations top the list of factors driving these deployments. Today’s laptop-toting college students assume their institutions will deliver WiFi access campus-wide. For many, ubiquitous wireless is a criteria in choosing a college. "WiFi is expected as part of today's campus experience both from an educational perspective as well as from a social perspective. Students expect WiFi so that they can learn anytime and anywhere on campus as well as always be available for friends and family," said Stan Schatt, vice president and research director at ABI Research.

Universities also face demand for greater bandwidth as lecture halls begin to deliver multimedia content to large numbers of users. “Universities are breaking new ground by using video over WiFi in a number innovative ways,” Schatt explains. “This is driving the adoption of high speed 802.11n. Students in the near future (at least the diligent ones) will be just as likely to watch their favorite professor’s lectures on their laptops as they will be to view ‘America’s Next Top Model’.”

Clearly, a robust, reliable wireless network is critical to staying ahead of the curve in higher education. Choosing the right partner and solution is the key to building this environment. The right wireless solutions, like the ones featured in this paper, offers rock-solid security, dependability and performance with increased WiFi coverage and seamless integration to the wired network. It is easy to manage and can scale to accommodate user needs. Simply put, it delivers on the promise of next-generation wireless computing.

As users demand more from their computing environments, a scalable, easy-to-manage wireless network will become increasingly important. Successful institutions like Ohlone College and Kean University know this and are investing in tools that will better support learning and propel their students and network into the future.

About Us

Campus Technology

The only monthly publication focusing exclusively on the use of technology across all areas of higher education, Campus Technology provides in-depth coverage of specific technologies and their implementations, including wireless networks and mobile devices; enterprise resource planning; eLearning and course management systems; 'smart classroom' technologies; telecom, Web, and security solutions—all the important issues and trends for campus IT decision makers.

Targeting administrators, IT professionals and tech-savvy faculty, Campus Technology provides direction, analysis and detailed coverage of emerging technologies to assist technology leaders in their specific roles on campus. To learn more, visit www.campustechnology.com.

About Trapeze Networks

Trapeze Networks, a Belden brand, provides enterprise wireless LAN equipment and management software. Trapeze was the first company to introduce NonStop Wireless - delivering unmatched reliability to the enterprise wireless LAN and its solutions are optimized for companies requiring mobility and high bandwidth such as healthcare, education, and hospitality. Trapeze delivers Smart Mobile™ providing scalable wireless LANs for applications such as Voice over Wi-Fi, location services, and indoor/outdoor connectivity. To learn more, visit www.trapezenetworks.com.