Mobilizing the Digital Classroom in Higher Education

Abstract

Higher education institutions are challenged to attract top talent in a highly competitive field. On the other hand, they must control the ongoing costs of daily administration, lecture delivery and basic research. Adding to these challenges is the exponential rise in the numbers of wireless users and multimedia applications accessing the campus network.

The demand for bandwidth is driven by an evolving and interactive classroom environment, in which technology is changing the way students learn and teachers teach. Today's highly mobile users expect ubiquitous wireless access across the far-flung campus. Because wireless is a shared-access technology, security planning must consider controls that include user identity as well as device location.

This white paper describes how higher education institutions can leverage Wireless LAN (WLAN) technologies for a networking solution that saves money and enhances productivity. It describes key challenges, along with best-practices resolutions, for deploying WLANs across the higher education campus.

Make Your Network Mobile

Overview: Why a Wire-Free Campus?

WLAN technology offers an ideal solution for higher education organizations seeking to expand anytime, anywhere connectivity across the campus. Wireless installation alleviates the need to disrupt solid walls or expose hazardous materials. It precludes the hours of labor needed to physically run LAN cabling through building walls or underground conduit. Additionally, with tablet devices such as the iPad™ and smartphones, end user devices no longer include Ethernet connectivity as an option.

802.11n WLANs use Multiple-Input, Multiple-Output (MIMO) antenna arrays and two frequency bands (2.4 GHz and 5 GHz) to transmit wireless signals up to six times faster than the older 802.11a/b/g technologies. The 5 GHz spectrum has an added advantage of less cross-channel interference, which is particularly useful in densely clustered deployments such as a 500-seat lecture hall or 400-room dormitory. Wire-speed like throughputs of up to 300 Mbps per access point mean high-quality streaming video and Voice-over-Wireless LAN (VoWLAN) are here-today facts, not future science fiction.

IT departments at academic institutions face several challenges for wireless deployment including:

- Selecting WLAN solutions and vendors
- Lifecycle management
- Interoperability of disparate client devices
- Managing churn of client devices
- Continued support of legacy systems
- RF site planning and survey
- Indoor and outdoor coverage
- Access for high-bandwidth applications
- Network security and access control
- RF and network troubleshooting
- Managing upgrades

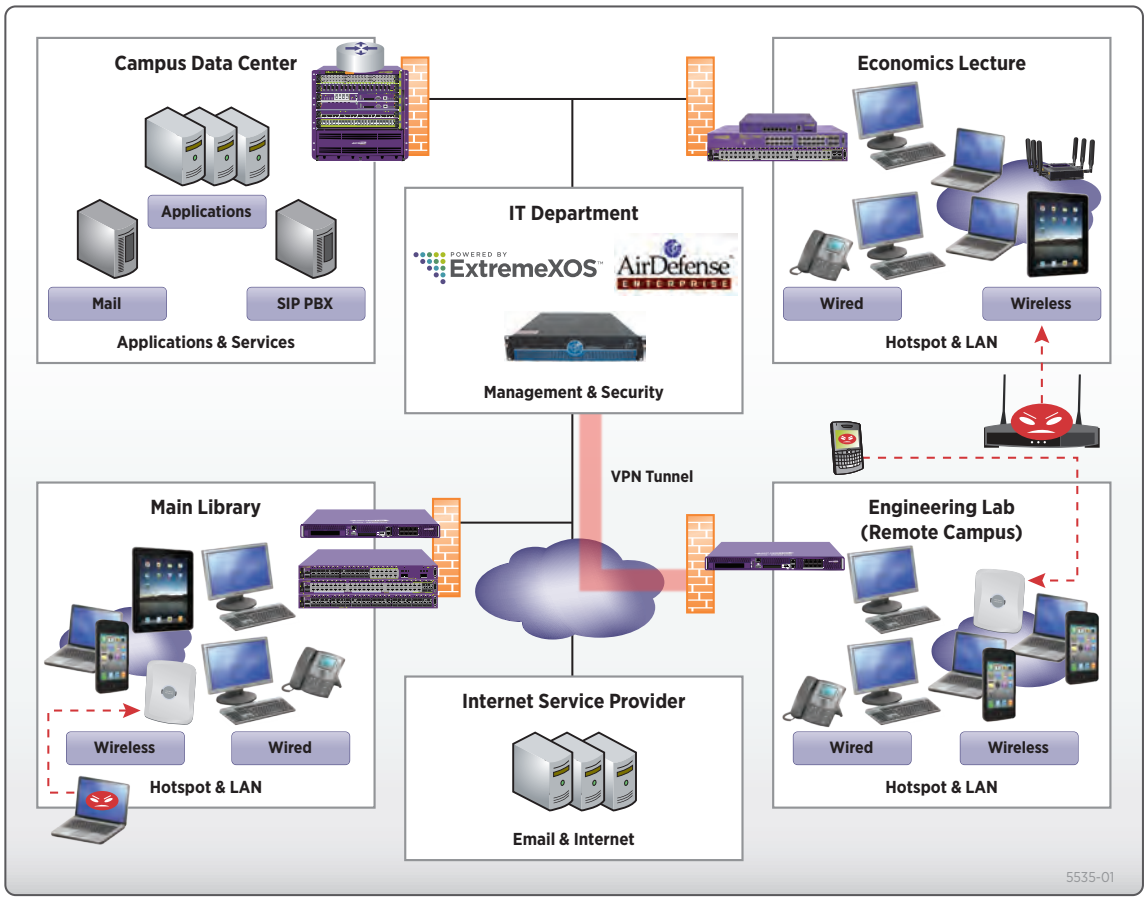

Figure 1: 802.11n extends connectivity across the extended campus with sufficient throughput for voice, video and graphics.

Extreme Networks® WLAN solutions offer some of the most advanced 802.11n technologies available, along with "smart enterprise network" features that can help improve the availability, reliability, coverage, manageability and security of wired and wireless campus LANs. Optimized for the ExtremeXOS® operating system, our high-performance, high-availability wireless architecture offers an ideal edge solution for delivering virtualized and/or cloud-based services, including video-on-demand, e-learning apps and student portals.

The following sections address the primary issues that higher education institutions should consider when planning a wireless installation:

- Achieving high-performance connectivity
- Ensuring scalability and reliability
- Enforcing campus-wide security
- Streamlining deployment and management

Achieving High-Performance Connectivity

While higher education institutions can deliver e-learning across the campus using either wired or wireless networks, mobile users rely on wireless access to deliver rich, streaming media and academic resources. With e-learning capabilities, students want the option to take their class work anywhere across a large campus and even to offsite locations. Students and faculty alike need technologies that help them to be more productive in classrooms and labs. They demand high-speed, free-roaming connectivity that supports new, powerful mobile devices. With the increasing adoption of devices like tablets and smartphones, this access must work both indoors and outdoors. And these user demands keep increasing, as applications become more sophisticated and demand more bandwidth.

The classroom environment requires consistent wireless access to high densities of students. The WLAN must be capable of handling hundreds of simultaneous association requests from client devices without bogging down the network and creating unacceptable delays. In an e-learning environment, ensuring fair access to wireless bandwidth is important as well. The challenge here is more than simply providing network access, it is providing each user with the optimal bandwidth for their e-learning experience.

Solution: Multimedia Bandwidth and QoS

Extreme Networks WLAN solutions deliver high-speed wireless connectivity across a campus with seamless mobility across indoor and outdoor locales. Summit® WM3000 series controllers and Altitude® Access Points (APs) deliver throughputs up to 300 Mbps per access point, and include features designed to boost signal transmissions across roaming RF zones and within dense deployments.

In the dense classroom setting, a grid of APs within a lecture hall can help balance client loads based on client count or bandwidth. Dual-band channels help reduce interference in crowded wireless zones, such as lecture halls, teaching labs, library study rooms and dormitories. High-power, concurrent dual-radio, 11n APs deliver high-performance wireless access for e-learning, along with the ability to support multiple, simultaneous unicast multimedia streams. High-availability controller features—such as Gigagbit Ethernet ports, self-aware fault-detection, automated-failover and support for redundant arrays—work with minimal administrative intervention to relieve traffic congestion and provide 24/7 availability.

802.11e Quality of Service (QoS), Wi-Fi Multimedia (WMM), Unscheduled Automatic Power Save Delivery (UAPSD), SIP Call Admission Control and Self-Monitoring at Run Time Radio Frequency (SMART RF) help ensure trouble-free delivery of time-sensitive and large files. IP PBX telephony, autoCAD graphics and multimedia streams are delivered to wireless handsets and mobile notebooks without skipping a beat, or dropping a packet.

Extreme Networks WLAN solutions allow network administrators to rate limit upstream and downstream traffic per user, helping ensure fair access to shared bandwidth. These rate limits can be tailored to prevent a user group, session or application from hogging a disproportionate amount of shared bandwidth. Using role-based access control, designated users such as graduate students and research faculty can be allotted a greater proportion of bandwidth over administrative staff or guests. Or certain applications such as online gaming may be rate-limited, giving traffic priority to academic services.

Ensuring Scalability and Reliability

Scalability and reliability are essential to support mission-critical applications and resources. The wireless infrastructure should be expandable, capable of responding to increases in user population and additions of new sites without requiring a forklift upgrade. Service uptime is critical as well because downtime impacts user productivity and adds to operational costs. System reliability is another critical factor that should be evaluated very carefully as part of lifecycle management analyses.

Solution: Flexible Installation and Configuration

Implementing an Extreme Networks WLAN solution can help provide superior savings in cost and time. Summit WM3000 series controllers, Altitude APs and Motorola AirDefense Security Platform (ADSP)* wireless management suite are backwards-compatible with 802.11a/b/g-compliant systems, to streamline network integration and speed up configuration.

For maximum installation flexibility, Altitude APs come in versions for indoor or outdoor use, with external or internal antennas. Choose thin APs for the most cost-effective wireless deployments. Or install adaptive APs to configure as a bridge or mesh, or to terminate an IPSec VPN tunnel. All Altitude APs are encased in tamper-proof housing and come with built-in mounting brackets. They are 802.3af Power over Ethernet (PoE)-compliant, eliminating the need to locate them near wall outlets or install separate power supplies.

Summit WM3000 series controllers automatically scan the WLAN discovering, licensing and configuring new APs for nearly plug-and-play ease of installation. The SMART RF feature automatically configures and calibrates Altitude APs to run at top efficiency by detecting radio channels, power levels, interference, coverage holes, unauthorized access and link failures—all without requiring manual intervention. The controllers can supply low-voltage PoE to wired network appliances, without requiring a separate power injector. This can mean less clutter in the wiring closet and more savings on utility bills, not to mention less carbon into the atmosphere.

*Future availability. Appliance models 1252, 3652 and 4250 sold separately.

Solution: SMART RF, Mesh and Clustering

The SMART RF feature is designed to simplify initial RF configuration, reducing the time and cost of new deployments. For new installations, SMART RF scans the RF environment and determines the best channel for transmitting power configurations to each managed radio. SMART RF also provides ongoing RF optimization and self-healing functions, helping improve the performance and management of existing deployments. RF environments are dynamic and change over time. SMART RF periodically performs recalibration helping keep the WLAN operating at optimal levels.

Extreme Networks WLAN solutions are highly scalable. The APs support fully redundant mesh configurations, which help extend connectivity into locations where running wired Ethernet is not an option. Each Summit WM3000 series controller can manage over 1,000 access points.

For dense deployments that demand extreme levels of availability, resilience and response times, Summit WM3000 series controllers can be configured as a cluster that supports load balancing, AP steering, auto-failover, aggregate throughput and cluster management. Clustering multiple controllers boosts wireless network performance in several ways. Controller N+1 redundancy with active-active load sharing helps eliminate a single point of failure, with each controller acting as both a sensor and failover system for other controllers in the group. Aggregate load-balancing allows the cluster to adapt easily to rapidly changing traffic loads, helping eliminate “hairpin” traffic congestion at the network edge.

Smart License Sharing is a unique scheme to share access point capacity licenses across a cluster and enables group redundancy without the need for a dedicated backup controller. Within the cluster, increasing aggregate capacity and throughput can be as simple as adding a zero access point license controller.

Enforcing Campus-Wide Security

IT staff must ensure that network and data integrity is not compromised by campus-wide wireless access. Access for various classes of users, including open Internet access for guests, can pose obstacles to the goal of securing the network from unauthorized or rogue users. Along with the challenge of providing diverse levels of access permissions, higher education campuses face high user turnovers every year and typically include pockets of legacy devices and unauthorized installations.

Add up all of these factors and it is easy to picture how the on-campus computing environment becomes riddled with exploitable vulnerabilities. For example, open Ethernet ports could be exploited by plugging in an unauthorized or a rogue AP. The rogue AP could be used by a hacker to gain unauthorized, anonymous backdoor access into an internal database containing sensitive information.

IT staff needs to assure that the user/device authentication and data encryption schemes are bulletproof. The WLAN solution must be able to detect rogue activity in the airwaves and in real time, locate and mitigate potential threats before a network is breached.

Solution: Multi-Layered Security

Extreme Networks WLANs are designed to create multiple layers of security, across wireless and wired segments of the campus network. Many of these security features work automatically or with minimal intervention, and can be configured to send network alerts prompting further administrative action as needed.

Four-factor access control includes identity, role, location and device policy compliance via NAC. The Geofencing feature provides location-based access control to visitors, contractors, faculty and students. The latest authentication and encryption schemes, based on IEEE 802.11i/WPA2 standards, safeguard confidential wireless traffic from packet sniffers and spyware. Hotspot security features enable authenticated or open access to the Internet for visitors and guests. Wireless intrusion detection features help protect the network from unauthorized access. Altitude APs can be configured as channel-specific or dedicated scanners that will detect and block rogue APs, controllers, mobile devices and/or user sessions.

The built-in, stateful-inspection firewall secures all traffic—wired and wireless—as it is switched or routed through the Summit WM3000 series controller. Firewall policies can be configured to permit, deny or mark traffic flows based on criteria or rules, such as traffic stream, VLAN, switch port, user role and/or device identity, location and connection characteristics. This centralized control enables network administrators to secure IP and non-IP traffic flows, as well as detect attacks to the wireless network not typically visible to traditional, wired-firewall appliances.

The wired link between an access point and controller can be secured with the built-in IPSec VPN engine. This is especially useful for remote deployment of an access point across a WAN link that traverses Internet.

For more detailed analysis and compliance reporting, Advanced Wireless IPS is available with the Motorola ADSP. This comprehensive wireless security and management suite integrates another level of in-house security into the WLAN infrastructure. The WIDS/WIPS feature can detect over 200 types of network threats. Advanced forensics and vulnerability and spectrum analysis further protect the network from potential intrusions and attacks.

Streamlining Deployment and Management

Networking multiple buildings across a campus can be a daunting task, particularly considering the scarce IT resources available within an academic institution. The ideal WLAN solution should provide capabilities for easy deployment and administration. Centralized, real-time management is critical for monitoring the campus-wide network that includes remote sites, multiple user groups and disparate client devices. Expert tools for RF assessment and network troubleshooting enable administrators to proactively address potential problems and achieve maximum service uptimes.

Solution: Remote Monitoring and Troubleshooting

Summit WM3000 series controllers include management software that provides lifecycle management of wireless networks from planning to configuration, to deployment, to monitoring. The browser-based dashboard provides administrators with a single, centralized console for large deployments, simplifying management and providing consistent configuration across the network. It delivers real-time visibility into and control of a wireless infrastructure comprised of hundreds of APs and thousands of disparate client devices.

The built-in RF planning tool enables predictive analysis of wireless coverage and capacity across the site, for proper AP placement during initial deployment, as well as for ongoing capacity planning. The central management console provides real-time event and fault management, uniform viewing into the network, and security and network health/performance alerts. The configuration compliance auditing tool inspects the WLAN infrastructure and automatically corrects unsanctioned changes, helping ensure network integrity.

Historical logs of WLAN statistics and associations help administrators analyze long-term performance trending. The comprehensive reporting functionality provides regulatory compliance reports and enables the creation of customizable reports. Network assurance tools remotely troubleshoot user connectivity issues and resolve WLAN performance problems, and include expert help to assist administrators in understanding how network performance is being impacted and what actions are needed to remedy the issue. Built-in visualization tools speed up the chore of identifying a problem, locating possible resolutions and implementing the correct solution.

Motorola ADSP works like a virtual IT assistant to remotely monitor, configure and troubleshoot wireless environments across the entire campus, including remote locations. This comprehensive management platform facilitates WLAN set-up, monitoring and troubleshooting. IT administrators can use it to mass configure remote APs by creating one desired configuration setting and pushing it across the network to designated APs. Role-based Identity Management streamlines the chore of adding, tracking, authenticating, monitoring and removing thousands of users each year, as students matriculate in and graduate out.

Summary

Extreme Networks networking solutions more than meet the performance and mobility demands of leading-edge technology adopters in the higher education market. Easily scalable, highly secure and convergence-ready, our wired and wireless solutions can help higher-education organizations evolve from outmoded hardware and software, block security vulnerabilities, improve coverage and availability for users and prime the campus network for multimedia e-learning and online collaboration services.

Extreme Networks solutions are designed to deliver a "mobile enterprise network" capable of:

- seamless integration of legacy and next-generation systems
- proactive detection and containment of rogue devices and unauthorized logins
- centralized management of roaming users and remote devices
- adaptive provisioning for virtual network services
- auto-sensing/-adjusting power levels, traffic loads and service priorities
- identification of users across subnets, ports, devices and roles

Visit our Website to learn more about cost effectively achieving a "mobile enterprise LAN"—one that is device-agnostic, self-healing, service aware, centrally managed and high performing.

Make Your Network Mobile

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +65 6836 5437

Japan
Phone +81 3 5842 4011

www.extremenetworks.com