White Paper |

Education

Connect Every K-12 Laptop... Wirelessly, Effortlessly, Securely

Brad Noblet | BN Consulting | Former CIO, Dartmouth College

ARUBA® networks

Overview

The increased use of laptop computers in K-12 schools has created a unique opportunity to dramatically improve the quality of teaching and learning. The integration of audio, video and graphics animation, coupled with interactivity, has enabled new teaching paradigms that expand the learning opportunities for all students. In addition, the Internet and other communications networks have opened access to a plethora of information never before available, taking students well beyond their classroom resources. Every laptop now includes Wi-Fi connectivity, which when used in conjunction with next-generation wireless access infrastructure from Aruba Networks, can deliver secure, high-speed network access to every latop at a price that enables ubiquitous deployment of this new, effective teaching tool.

Introduction—The Growing Need for the Network

Primary and secondary (K-12) educational institutions are turning to computers and software applications to improve the learning environment for teachers, administrators, students, and their parents. A growing number of public schools strive to provide one computer for every student. Computer technology has enabled new educational tools and methods, increased productivity, and improved communications. The utility of both computers and educational applications is a function of access to the networks on which these tools depend—limitations to network access prevent the realization of their full potential.

Modern teaching styles and learning applications put more emphasis on multi-media and interactivity, dramatically increasing network capacity and performance demands. The shared nature of resources and the mobile nature of students, teachers, and administrators make the network requirements even more challenging. Unfortunately the networks used in most schools cannot meet the challenge. Many classrooms cannot accommodate a mobile cart entailing the temporary installation of five or ten networked computers for a special lesson or activity. Adding computer labs and PC-equipped work areas requires intrusive infrastructure installations and expensive upgrades. The problems are worse in schools that allow students to bring in their own computers because of contention for the limited number of network connections.

This problem should be easily addressed with a wireless LAN (WLAN), however, the solution is a bit more complicated. The right WLAN can liberate students, teachers and administrators from the mobility and flexibility limitations of a wired network, fostering the use of computer-based educational tools and delivering ubiquitous always-available access to network-based resources. To obtain the right WLAN requires that school IT directors and network administrators pay careful attention to deployment costs, investment protection, network management, and security.

Early WLAN technology had a host of issues that made broad implementation expensive and risky, but a new generation of technology has solved these problems. With advances in the security, performance, management, and investment protection of wireless network equipment, schools can roll out pervasive wireless networks today and gain economic and technological benefits that will pay back many times over.

This paper discusses the specific needs, challenges, and solutions associated with implementing WLANs that are best-suited for K-12 schools.

The Unique Wireless Networking Challenges of the K-12 WLAN

Schools face unique wireless networking challenges because of their mobile populations, performance requirements, budget constraints, and security needs. Some forward-thinking WLAN companies have addressed these challenges and theirs are the solutions that K-12 schools should consider. Among the issues to be addressed are:

- **Mobility and performance considerations**: The advent of new multi-media, interactive teaching, and learning applications has dramatically increased demands for network capacity and performance. Additionally, the desire to make the best use of computing resources and classrooms has increased the need for portable computers with untethered network connections that can be used wherever and whenever needed.

- **Performance and deployment**: Early wireless Access Points (APs) worked on a stand-alone basis, and their complex functionality made them expensive. As a result, organizations deployed as few as possible and designed the network for maximum coverage rather than maximum performance. These APs required a costly RF environment survey prior to installation, and once installed, had to be configured individually, an expensive and time consuming proposition.

- **Financial considerations**: Schools, particularly public schools, face tremendous financial pressures. Every dollar must be used efficiently and effectively, and capital purchases must be long-lived. This financial pressure requires that WLAN deployment costs be kept low, the existing infrastructure leveraged as much as possible, and the investment protected for years to come.

- **Security considerations**: The open nature of RF communications means that WLANs must meet a very high standard before they can be considered secure. Access control must be coupled with the secure transport of information. Given the diverse constituency served by school's WLAN, security must be flexible enough to be tailored for individual users.

These issues can be addressed using a centralized mobility network in which the intelligence is moved from the access points to a centralized mobility controller. In such an architecture the mobility controller, usually located at a data center or central equipment room, provides all of the essential network services. The controller is connected to a network of "thin" access points, so named because they rely on the controller to manage them. The thin AP design is very cost effective and designed to be inexpensive to install, thereby enabling schools to deploy them more densely for better coverage and performance. Utilizing the mobility controller's central intelligence to assess and then optimize AP configuration and coverage eliminates the need for a costly site survey, and allows schools to install a wireless mobility network easily and economically.

A centralized architecture also permits network capacity to be intelligently allocated across all APs within a geographic region, maximizing the offered performance to meet the demands of new, multi-media and interactive applications. Since the mobility controller is fully aware of all APs, as well as the RF environment, it continuously optimizes coverage by automatically calibrating and adjusting the power, channel, and AP used for each session.

An additional feature of the centralized approach is that security is more comprehensive, scaleable, and easier to manage when administered centrally. Off-loading security to the mobility controller benefits APs, too, by reducing their cost and complexity while boosting throughput capability..

Leveraging existing infrastructure

Access points that operate autonomously (so-called “thick” APs) and thin APs that store encryption keys locally contain vulnerable security information, and typically must be physically protected against tampering to ensure network integrity. For this reason, these APs are often installed in the protected plenum space of a building. Plenum mounting usually requires new plenum-rated cabling, which is expensive and time consuming to install.

Thin APs that do not store encryption keys locally rely instead on the mobility controller to centrally store security information. This allows the APs to be located anywhere without creating a security vulnerability. Most of these APs draw their power over the network connection (eliminating the need for a local AC power source) and can be connected to any existing wall jack anywhere in a school. Leveraging existing infrastructure in this way reduces the cost of network installation and simplifies network upgrades.

To further simplify installations, mesh networks were recently introduced that allow data in the network to hop wirelessly from AP to AP, eliminating the need for a local wired connection to the mesh APs. This capability allows a network to circumvent areas containing asbestos or cement walls, and span large open spaces or indoor areas in which it is not economical to install cabling.

Future-proofing your investment

Investment protection is among the most important financial considerations when selecting a WLAN. The objective is to ensure that products purchased today will meet the school’s requirements for years to come. Future-proofing can take many forms including allowing devices to be software-upgradable, modular hardware designs that can be upgraded piecemeal, and devices that can be repurposed as needed, e.g., APs that can be easily converted into mesh devices.

Properly designed centralized WLANs offer a high degree of scalability that goes from one to more than 500 APs. The same mobility controller installed today to support a pilot or small network can be used tomorrow to support an entire school or, in some cases, an entire district. Adding access for a classroom can be as simple as plugging a low-cost thin AP into an existing network port.

WLANs typically employ a modular software operating system and modular application engine driving the mobility controller. Network administrators can add more sophisticated and specialized functionality if and when needed, allowing the platform to adapt to changing needs over time.

School networks must be able to move in step with advances in technology, devices, and applications while remaining compatible with legacy devices. Backward compatibility is particularly important as newer technologies such as 802.11n high speed wireless are deployed. Migrating from old to new technology should not mandate the replacement of existing computers and teaching resources, but instead should gracefully support legacy devices.

Legacy support extends to network management, not just devices. As devices based on new technologies are added to a WLAN, they must be configured and managed. In some cases the devices will come from a new equipment supplier. Using a single multi-vendor network management platform that can manage all of the WLAN devices, old and new, will simplify technology transitions, lower equipment costs, and reduce staff training requirements.

Given the higher performance of next-generation 802.11n wireless, there are advantages to shifting telephony, CATV transport, HVAC control, and security camera services to the WLAN and off of the wired network. Once accomplished, these services could be easily and quick deployed and/or moved where needed without incurring wiring installation expenses. Given that these and other services are increasingly IP-based, they are readily amenable to being run on a single WLAN communications infrastructure. Today's mobility controllers have the capacity and performance to make wireless convergence possible, and can result in dramatic savings in service deployment costs and a commensurate reduction in the time to deploy.

Ease of Management

A school's network must be easy to manage because schools typically have limited IT personnel, with staff often pulling double-duty. For example, a computer instructor might also serve as on-site network administrator. The good news is that the WLAN learning curve is not steep. Color-coded coverage maps that display the real-time status of the WLAN complement self-configuring, self-optimizing networks to enable network managers to focus their attention on critical issues instead of learning about RF. In many cases, even troubleshooting is handled automatically—before a technician has time to address a problem, the network can heal itself.

Self-optimization is essential because the RF environment in schools is in a constant state of flux. For example, schools located in residential communities are exposed to RF signals from nearby home WLANs. Properly designed WLANs monitor the environment, detect interference, and automatically adjust AP settings to eliminate potential problems. Additionally, to maximize coverage and uptime, these systems automatically detect AP overload or failure, adjusting the power of other APs to fill the gap.

In cases where network administrators must intervene, they can do so from the mobility controller's management console. It is even possible to collect diagnostic data remotely, allowing a district to centralize and automate management from a commonly shared support center.

Reducing VLANs

Virtual LANs (VLANs) were originally designed to contain broadcast traffic and avoid flooding the network with unnecessary messages. They are also used to separate management and data traffic on wired networks. VLANs can be a major contributor to management complexity in WLANs. Legacy wireless LANs used VLANs as a way of keeping wireless traffic separated from wired traffic, a trick that was effective in small networks, but unmanageable in larger networks. In the latter case, the implementation of a WLAN often required extensive reconfiguration of the wired network, and in some cases, necessitated replacement of the wired network equipment.

The VLAN problem is solved with modern, properly designed WLANs. APs that communicate with mobility controllers across IP networks require no reconfiguration and no VLAN interface to the existing network. Wireless data and services are carried through encrypted IP tunnels over the existing network, with all services centrally provisioned by the mobility controller. In short, anywhere an IP network exists, a WLAN can exist, too.

Security

Schools have extensive, and in some cases unique, network and user security requirements. By virtue of RF being an open medium, WLANs deserve special consideration with respect to network security, including the protection of network data, managing network access, and blocking hackers and other intruders.

Authenticating Users and Better Support for Network-Based Boots

By default, a wireless network is shared and open to eavesdropping. To protect its networks while still providing access to constituent users, schools must maintain tight control over access to the wireless network. Most wireless solutions provide one or more levels of encryption and authentication. However, to do so, many require that client software be loaded on every computer and device. This additional workload can paralyze a limited IT staff, especially given schools' typical mix of older computers and operating systems.

To solve this dilemma, many schools use Web-based authentication, also called a captive portal, that requires users to enter an authorized username and password on a Web page before network access is granted.

Captive portals create a challenge for schools that use network-based boot scenarios. Network-based boots, used extensively by Mac OS, centralize configuration information and data, requiring clients to load from a server. The issue is that very few captive portal implementations allow custom protocols and datastreams to work prior to network login. Instead most captive portals allow the administrator to specify customized firewall access policies.

Controlling Access

Schools have many constituents including students, teachers, administrators, and guests, each with different access needs. Network access must be sufficiently flexible to accommodate the needs of each group without adding complexity. Once allowed on a network, a user's rights determine where they can go and what they can do, so rights management is essential to any access control scheme.

The best solution is an integrated policy enforcement firewall that allows network managers to create and apply unique roles based on each user's access rights. The policies can be based on any combination of rights such as user, group, duration, time of day, and location. For example, students might be given access to the school's server-based educational applications all day, but access to the Internet only after school hours. Likewise, a teacher might be permitted to access school policy information and instructional materials, whereas a school counselor is permitted to see all student records from within the administrative office.

A granular user rights and role-based approach gives schools the level of access control they need to protect data, clients, and privacy.

Protecting Against Network Intrusion

The security threat comes not only from outside the school, but also from within. School WLANs often serve as the learning ground for the brightest, most talented hackers. Students today are technology savvy and they have the time and motivation to demonstrate their technological prowess.

To counter these threats, a WLAN must provide comprehensive wireless intrusion detection and prevention against probing and network discovery, denial of service attacks, surveillance, impersonation, client intrusion, network intrusion, and other similar types of attacks.

The first line of defense is continuous RF monitoring, automatically detecting all APs in the RF environment. If an unknown AP is detected, a classification engine should determine whether it is valid, interfering (detected but not connected to the wired network), or rogue (detected and connected to the wired network). Once an interfering AP is detected and classified, the IT manager should be alerted and wireless clients prevented from associating with it. If the AP is rogue, the network should disable it, alert the IT manager, and identify its location so it can be removed.

Summary

Schools have a growing need for network-based resources and technology that are accessible from anywhere within the school at any time. WLANs address this need more easily and cost-effectively than wired networks, and can do so securely and with minimal IT overhead.

Aruba Networks understands the networking requirement of K-12 schools, having implemented WLANs in more than 2,000 educational institutions. Aruba's mobility controllers, access points, mobility software, and AirWave® wireless management platform offer a future-proof architecture that addresses the specific needs of primary and secondary schools. Aruba's multi-purpose WLANs enhance classroom connectivity and district-wide mobility while ensuring the security on which users depend.

Aruba's mobility solutions deliver:

- Easy-to-use, cost-effective WLANs that leverage the existing infrastructure and provide superior scalability and investment protection;
- Centralized, multi-vendor network management and control, requiring less time and fewer personnel resources to operate;
- Future-proof network security featuring authentication, access control, and intrusion protection to ensure the integrity of the network for all constituents.

To learn more about the capabilities and benefits of Aruba's mobility solutions for K-12 schools, please visit http://www.arubanetworks.com/applications/education-k12.php.

About Aruba Networks

People move. Networks must follow. Aruba securely delivers networks to users, wherever they work or roam. Our unified mobility solutions include Wi-Fi networks, identity-based security, remote access and cellular services, and centralized multi-vendor network management to enable the Follow-Me Enterprise that moves in lock-step with users:

- Follow-Me Connectivity: Adaptive 802.11a/b/g/n Wi-Fi networks optimize themselves to ensure that users are always within reach of mission-critical information;
- Follow-Me Security: Identity-based security assigns access policies to users, enforcing those policies whenever and wherever a network is accessed;
- Follow-Me Applications: Remote access solutions and cellular network integration ensure uninterrupted access to applications as users move;
- Follow-Me Management: Multi-vendor network management provides a single point of control while managing both legacy and new wireless networks from both Aruba and its competitors.

The cost, convenience, and security benefits of our unified mobility solutions are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com.

WP_K12LAP_US_080603

1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
http://www.arubanetworks.com

WP_K12LAP_080603_US