

White Paper |

Education



Lessons in Wireless for K-12 Schools

Don Reckles

ARUBA[®]
ARUBA
networks

Introduction—The Growing Need for the Network

Primary and secondary (K-12) educational institutions are increasingly turning to computer technology to improve the quality of education and the overall effectiveness of the school environment for teachers, administrators, students and their parents. There has been a swift proliferation of computers in K-12 schools. In 2004, public schools had roughly one computer for every four students, up from 1:14 in 1994, and 95% of schools were connected to the Internet, up from 50% in 1995.

The increased use of computer technology has enabled new educational tools and methods, higher productivity and improved communications. However, the reach of the computer network has limited the utility of computers and educational applications.

The networks in most schools are unable to satisfy today's requirements. The necessary sharing of resources and the mobile nature of students, teachers and administrators make the network requirements even more challenging. Many classrooms cannot even accommodate a mobile cart—a 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. In schools that allow students to bring in their own computers, there is a battle for the limited number of network connections.

It would seem the problem could be easily addressed with a wireless LAN (WLAN). A WLAN can liberate students, teachers and administrators from the wire, thereby increasing use of current computer-based educational tools, making possible new applications and technology, and providing ubiquitous all-time access to network-based resources.

However, that answer is not as simple as it seems. While a widely deployed WLAN resolves the question of access, schools' IT directors and network administrators must pay careful attention to deployment cost, investment protection, network management and security.

First generation 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, management and investment protection of wireless network equipment, schools can roll out a pervasive wireless network 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 secure WLANs for K-12 schools.

The Unique Challenges of the K-12 WLAN

Schools face unique challenges because of their budget constraints, security environment and varied constituencies affected when implementing a wireless network. Some forward thinking WLAN solutions are ideally suited to address these considerations.

Financial Considerations

Schools, particularly public schools, face greater financial pressures than most enterprises. There is an enormous need to use every dollar efficiently and effectively, and to ensure that capital purchases have a long, productive life. This financial pressure requires that WLAN deployment costs be kept low, that the existing infrastructure be leveraged, and that the investment protected for years to come.

Lowering cost and easing deployment

First- and second-generation wireless access points (APs) had complex functionality built directly into them. These “fat” APs were expensive. As a result, organizations deployed as few as possible and designed the network for maximum coverage per AP, not maximum performance. This required a costly survey of the RF environment during the planning process. In addition, each fat AP had to be configured individually, which was expensive and time consuming.

Today, most large WLAN implementations use a centralized architecture. This network design moves the intelligence from the access points to a centralized WLAN switch or mobility controller. The controller, usually located at a data center or central equipment room, provides all the essential network services and security. The controller is connected to a network of “thin” APs that self-install out of the box.

The thin AP is designed to be inexpensive, allowing organizations to deploy them more densely for better coverage and performance. Some controllers are able to maintain full awareness of all APs and monitor their RF environments. In turn, the controller is able to continuously optimize coverage by automatically calibrating and adjusting the power and channel of each AP.

The combination of a dense deployment and automatic AP calibration eliminates the need for the site survey and allows schools to install a wireless mobility network easily and at a low cost.

Leveraging existing infrastructure

Because fat APs are expensive and contain critical network security information, they must be protected and are typically installed in the plenum space of a building to prevent theft. Even some APs that might be considered thin store encryption keys and other security information locally, requiring that they be similarly protected. Deployment in the plenum space usually requires new cabling, which is expensive, time consuming and intrusive.

However, some centralized WLAN solutions eliminate the need for a separate cable infrastructure by storing all security information in the mobility controller rather than the AP. Therefore, these APs can be

connected to any existing wall jack anywhere in a school, leveraging the existing wired infrastructure, simplifying network upgrades and sparing, and reducing the cost of network installation. Additionally, many APs support 802.3af Power-over-Ethernet; they draw their power over the network connection and do not need a separate AC source.

Future-proofing your investment

Perhaps most important among schools' financial considerations is investment protection—the need to ensure that products purchased today will be in service for many years to come. Because financial resources are tight, uncertain, and bond-oriented, schools need solutions that can address their current needs and be easily and cost-effectively enhanced to support future requirements.

Centralized WLAN networks offer greater scalability than a network of distributed fat APs. Schools may want to consider a mobility controller that can scale to support hundreds of APs. That way, the same mobility controller installed today to support a pilot or small network can be used tomorrow to support the entire school, a growing student body and new deployment areas.

Scaling the network is simple; adding access for a classroom can be achieved by plugging a low-cost thin access point into an existing network port. Some mobility controllers can even work with 3rd party APs, protecting any investment schools have made towards a WLAN solution. Furthermore, some WLAN systems offer optional, modular mobility applications, allowing network administrators to add more sophisticated and specialized functionality if and when they need it.

School networks must be able to move forward with advances in technology, devices and applications while providing compatibility for legacy devices. This investment protection is particularly important with a newer technology such as wireless where standards are still evolving. For this reason, schools should seek out WLAN solutions that feature a programmable architecture and a process that allows all networked controllers and APs to be upgraded from a single, central location.

Ease of Management

A school's network must be easy to manage. This is particularly important since 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.

Centralizing Management and Control

School RF environments are in a continuous state of flux. Among other factors, schools are often located in residential communities, surrounded by homes with their own wireless networks. These nearby networks can cause interference and other performance issues for the school's network. Centralized WLAN solutions that continuously monitor the RF environment, detect interference and automatically adjust AP settings go a long way to eliminating these problems and easing the management burden. Additionally, to maximize coverage and uptime, some solutions automatically detect AP overload or

failure and adjust the power of other nearby APs to fill the gap. This centralized and automated management enables schools to administer and maintain a mobility network with minimal resources.

In cases where network administrators must intervene, they will want to do so from a centralized management console, and may even need to remotely capture a packet or flow. Some solutions include a centralized management console providing color-coded “heat maps” that display real time status of the environment and extensive network, device and user information for easy troubleshooting.

Reducing VLANs

VLANs (virtual LANs) are a large contributor to management complexity in wireless networks. VLAN were originally designed to contain broadcast traffic, to avoid flooding the network infrastructure with unnecessary messages and to separate management and data traffic on wired networks.

Legacy wireless LANs used VLANs as a method of keeping wireless traffic separated from the wired traffic. This was effective in small networks, but quickly became too complex and became unmanageable in larger networks. Implementation of WLANs began to require extensive reconfiguration of the wired network, and in some cases, necessitated replacement of wired network equipment.

Thin APs communicate with controllers across IP networks and require no reconfiguration or additional VLANs to the existing network whatsoever. Schools should look for wireless solutions that carry all traffic through encrypted IP tunnels over the existing network, with all services centrally provisioned by the mobility controller. In that way, any place an IP network exists, a secure wireless network can also easily exist.

Security

Schools have extensive network and user security requirements, many of which are unique to schools. Wireless networks introduce special concerns and considerations including who is allowed onto the network, controlling where they can go, and preventing intruders.

Authenticating Users and Better Support for Network-Based Boots

By default, wireless is shared and open. To protect its networks and accommodate its varied constituents, schools need tight control over who is allowed onto the wireless network. Nearly all wireless solutions provide one or more levels of encryption and authentication. However, most require client software on every computer and device. This additional work can paralyze a limited IT staff, especially given the mix of older computers and operating systems often found in schools.

To solve this dilemma, many schools use web-based authentication, also called captive portal. With captive portal, users must enter their username and password on a web page before they are permitted to connect to the network.

However, captive portal creates a challenge for schools that use network-based boot scenarios. Network-based boots, which are used extensively with MacOS 9 and 10, centralize configuration information and data, and require clients to load from a server. But very few captive portal implementations allow custom protocols and datastreams to work prior to network login. To avoid this dilemma, school IT departments should identify captive portal solutions that allow the administrator to specify customized firewall access policies.

Controlling Access

Schools have many constituents including students, teachers, administrators and guests. These constituents have different access needs and rights. Once on the network, users' rights—where they can go and what they can do—need to be managed and controlled. In some cases, devices must be prevented from talking to one another to thwart the spread of malware, such as viruses and worms.

A centralized controller with an integrated policy enforcement firewall allows network managers to create and apply unique roles. The policies might be based on a combination of parameters such as user, group, application, time of day and location.

For example, students can be given access to the school's server-based educational applications all day, but access to the Internet only after school hours; a teacher can be permitted to access school policy information and instructional materials; and a school counselor can be permitted to see all student records from within the administrative office.

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

Protecting Against Network Intrusion

For schools, the security threat is not only from outside the school, but from the students themselves. Wireless networks in schools often serve the brightest and most talented hackers. Students are technology savvy and they have the time and motivation to demonstrate their technology prowess.

To eliminate these threats, a mobility solution must provide comprehensive wireless intrusion detection and prevention. It must protect against most types of intrusions including probing and network discovery, denial of service attacks, surveillance, impersonation, client intrusion and network intrusion.

To be most effective, the system must be able to automatically detect an unknown AP and determine whether it is valid, interfering (i.e., detected, but not connected to the wired network), or rogue (i.e., detected and connected to the wired network). If the AP is interfering, the mobility system should alert the IT manager and prevent wireless clients from associating with it. If the AP is rogue, the mobility system should disable it, alert the IT manager, and identify where it is connected so it can be removed. Similarly, the system should also be able to detect and classify all wireless client devices in the environment and disable invalid clients.

Summary

Schools have a growing need for and reliance on network-based resources and technologies. Increasingly, they need to make these resources and technologies accessible to more people, more often in more places. This trend will continue. Wireless mobility networks address networking needs more easily and cost effectively than wired networks.

Schools should consider only WLAN solutions that address the specific needs of primary and secondary schools today, and allow for:

- An easy, cost-effective implementation that leverages the existing wired network and provides superior scalability and investment protection
- A less complex network with centralized management and control, requiring less time and fewer personnel resources to operate
- Advanced future-proof network security, including authentication, access control and intrusion protection, providing integrity for the air, the network, the users and the data.

About Aruba Networks

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks 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>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. All rights reserved. Specifications are subject to change without notice.

WP_EDK12_US_071217



1322 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
<http://www.arubanetworks.com>