Introduction
The trend to digitize the classroom and provide students with access to vast array of learning tools online, drive the need for higher-speed, more reliable Wi-Fi networks in schools, colleges, and higher learning campuses. The use of computer technology has enabled new educational tools and methods, higher productivity and improved communications. However, the reach of the wired computer network has limited the utility of computers and educational applications.

With Inscape Data Corporation’s AirEther SB3000 Wi-Fi access and connectivity solutions, educational institutions gain consistent, reliable connectivity, wider coverage area, higher performance, lower maintenance, and secure wireless than any other Wi-Fi systems. Built for rugged environments, Inscape Data AirEther wireless access solutions securely connect more laptops, ipads, tablets, and smart-phones reliably and securely for our next generation of digital classrooms.

Challenges
In this day and age of increasing budget deficits, the education institutions are scrambling to meet the needs of students to provide quality education with the most cutting edge technology their budget can afford. Cutting cost on wireless LAN equipment would not be top of the list. Some forward thinking wireless LAN solutions are ideally suited to address these considerations.

Public educational institutions face even more 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.

Lower cost with Wi-Fi
Wi-Fi had been around since the early 1990s and enjoyed great measures through wireless technology advancement. The early generation Wi-Fi access points (APs) had complex functionality built directly into them. These loaded APs were costly. 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 loaded AP had to be configured individually, which was expensive and time consuming to deploy and maintain.

In these days, 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 strip down APs that self-install out of the box.
The so called “thin” AP is designed to be cost effective, 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. The wireless management software plays a crucial roll in lowering the overall maintain ace cost and increasing performance of the network.

**The use of existing infrastructure**

Whether deploying thing or loaded APs, considerations must be taken to deter theft and temperament. Loaded APs are costly 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.

In many cases, centralized wireless LAN 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 3 Lessons in Wireless for K-12 Schools Inscape Data Corporation 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.

**Simple to Maintain**

Every IT staff wants a network that is easy to manage. They have every right. A schoo’s network is no different. 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 wireless access point management solutions enable schools to administer and maintain a mobility network with minimal resources.

In routine occasions, 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 the display of real time status of the environment and extensive network, device and user information for easy troubleshooting.

Educational network utilizes VLAN to better manage the network. Reducing VLANs 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.

With a thin access point network, controllers across IP networks 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.

**Wireless Security**
Due to security requirement unique to each school, extensive network and user security requirements are in place. Wireless networks introduce special concerns and considerations including who is allowed onto the network, controlling where they can go, and preventing intruders and hackers.

IT department typically leave wireless networks open to simplify user authentication process and to provide better support for network-based services and shares. 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.

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.

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.

**Conclusion**

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, and advanced secure access, including authentication, access control and intrusion protection, providing integrity for the air, the network, the users and the data.