Aerohive NETWORKS

white paper

Schools Graduate to Enterprise-class Wi-Fi

How K-12 (primary and secondary) educational institutions can benefit by advancing a grade in their wireless LAN strategies and investments.

Table of Contents

Executive Summary

On-line multimedia and interactive educational applications are invading the classroom and prompting schools to take a fresh look at what's possible with the latest in wireless LAN (WLAN) technology. This paper examines how schools can apply 802.11n enterprise-class Wi-Fi technology in ways that pay while overcoming such traditional challenges as shrinking budgets, high network management costs, and nagging performance and reliability troubles.

Introduction: Wi-Fi Earns High Marks in the Classroom

Primary and secondary schools are motivated to find enterprise-grade wireless networks. One reason is the rise of popular online learning applications that involve multimedia experiences and interactive sessions – activities that require very high-speed networks.

For example, Pender County Schools in Burgaw, North Carolina, uses the bandwidth-hungry World of Warcraft video game as a teaching tool. And Pender County teachers have been known to post recordings of middle-school students reciting self-composed poetry to YouTube, where student peers can critique the performances. All this activity means, "There's lots of video coming over our network," says Landon Scism, the district's chief technology officer.

With his observation, Scism describes what many primary and secondary schools are experiencing worldwide.

To conserve costs, it's a common practice for schools to shuttle laptops between classrooms on mobile carts for special online lessons rather than building expensive computer rooms or buying a computer for each student. Schools with even slimmer budgets have simply adopted the university-computing model by asking students to bring their own laptops or other mobile devices to school to use for coursework.

The mobile nature of these laptops on wheels and student-owned computers makes using over-the-air broadband networks for delivering student access more practical than hard-wiring Ethernet connections all over the school. Moreover, a perfect storm of trends and events is now allowing schools to install professional-grade wireless networks that have the robust management and automated features needed to meet schools' network growth and reliability requirements.

Consider the following developments, for example:

- Industry **standards** for IEEE 802.11n WLANs, which offer Ethernet-like throughput, are now firmly in place. Standards eliminate the risk of near-term product obsolescence and the potential for interoperability problems among client devices and WLAN access points (APs).

- Centralized configuration, **management**, and security across the entire WLAN are now available to meet the requirements of multiple-AP deployments and even multiple-site deployments at negligible additional costs.
- The latest 802.11n systems on the market are available for about the same **price** as earlier 802.11g WLANs, but transmit data six to eight times faster than the older WLANs.
- Newer WLAN architectures strike just the right balance of distributed functions and centralized control to support affordable and manageable system **scalability** going forward.

These developments, combined with schools' need to accommodate the mobile nature of computers and high-speed multimedia network streams, are the key drivers behind a resurgence of interest in deploying Wi-Fi of a higher caliber in primary and secondary educational environments. A closer look at these developments follows.

Standards: Let's Hear it for 802.11n

High-speed 802.11n standards were ratified in late 2009, delivering nearly a six-fold increase in data connect speeds per radio compared to older Wi-Fi networks. Each 802.11n radio in an AP that is built on chipsets made by Atheros Communications (which supplies silicon to most of the WLAN industry) supports data connect rates of 300Mbps and actual throughput of about 120Mbps to 170Mbps if operating in the 5GHz band. The variation in throughput is attributable to differences in vendor implementation, a school building's physical environment, the nature of the application at hand, the number of concurrent users, and other factors.

As a result of the new standards-based, high-speed 802.11n products, many more laptops, netbooks, smart phones, and tablet computers can simultaneously use the network than was possible with earlier 802.11g networks, which offered just 54Mbps connect rates and about 22Mbps of actual throughput. In addition, the greater capacity of 802.11n networks better supports the streaming media types of applications that instructors increasingly use as teaching tools.

Many schools, then, are examining the 802.11n version of Wi-Fi as a primary learning venue, and one that delivers the mobility and throughput users need without the excessive cost of cabling every student device. They are also finding that wireless connectivity contributes to parent-teacher communication and school safety in ways that will be mentioned later.

Management in the 21st Century Schoolhouse

Because high-speed wireless networking is becoming fundamental to learning and communications experiences, schools today, then, really require an "enterprise-class" network: one that's able to support mission-critical applications with sophisticated manageability, security, and reliability attributes. These features tend to be scarce or altogether absent in most of the standalone, consumer-grade wireless APs that many schools have installed in the past because of their low sticker costs.

The older APs also tend to be more limited and inconsistent in how many simultaneous users they can support.

For example, at Churchtown School in Southport, England, teachers use laptops to control smartboards in the classroom and to access Web-based academic applications such as KnowledgeBox. Laptops stored on three laptop trolleys are wheeled around to classrooms.

But a classroom with 15 trolley laptops and a teacher laptop was pushing the practical limit of the consumer-grade APs that the school had installed, says the school's network and infrastructure manager. The situation necessitated an upgrade to an enterprise-class system able to support 45 or more client devices per AP concurrently.

Educational environments are not unlike enterprise business environments as they continue to experience an increased reliance on mobile network access in this manner. As such, individual schools and entire school districts require growing numbers of APs and an affordable, efficient way to provision, configure, manage, and secure them – the same attributes that the business world demands from its networks.

Another case in point: Harrisonburg City Public Schools in Virginia changed to an enterprise-class system when 40 of its consumer-grade APs failed within a brief period of time. When they rebooted, the APs automatically reverted to their factory default configurations, which meant that security features were disabled. That left the network suddenly vulnerable to would-be intruders.

The lack of inherent reliability and security in this class of device provided the impetus for the Harrisonburg school district to upgrade to an enterprise-class system with automated and centralized policy-setting, configuration, and management features.

The Harrisonburg district isn't alone in its preference to deploy 802.11n APs across a number of school buildings and its desire to provision and manage them in ways that:

1. Don't involve costly physical visits to each AP by allowing provisioning and management from a central location; and,

2. Enable all the APs to be provisioned, managed, secured, and troubleshot consistently so IT support staff only have to learn one system.

Consider The Madeira School, an all-girls boarding and day school in McLean, Virginia, as another example. It started out with two simple APs several years ago, which grew organically to a 30-AP network.

That became unmanageable when Madeira's director of technology wanted to temporarily change network access policies in the dorms during a holiday. Doing so would have entailed individually reconfiguring 15 APs and then reconfiguring them yet again to return to the usual daytime policy.

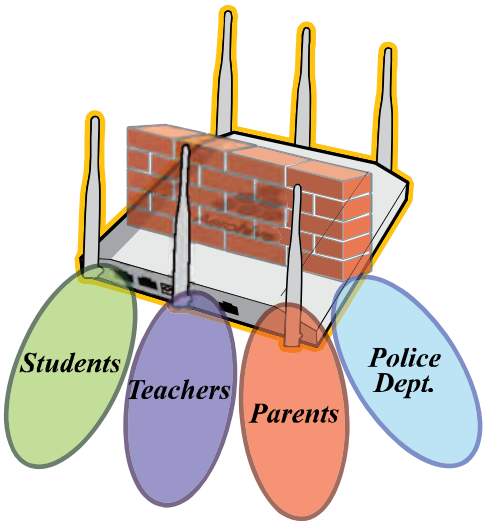
This process wasn't an option with the school's short turnaround time and small staff. Eventually, Madeira invested in a system with a centralized and automated policy engine that can push out policies to multiple APs over the air, giving IT staff the flexibility to create, change, and reinstate policies as warranted.

Another challenge facing many schools: What of the Parent-Teacher Association (PTA) meetings that might require network reconfiguration for giving parents guest Internet

access at the school? Using an enterprise-class Wi-Fi system, IT support staff can add an extra service set identifier (SSID) that allows guests to connect to the public Internet or to school resources that are intended for public access through the WLAN. But the separate SSID keeps them partitioned from seeing any confidential data.

The Framingham Public School District, for instance, has created several separate SSIDs in its 440,000 square-foot high school. On one WLAN infrastructure foundation, the district has, in effect, created separate, partitioned WLANs for internal student applications, faculty, guests, and even the local police department. The police have access to all the district's IP surveillance video cameras across all buildings and campuses as part of a program aimed at bolstering school safety (see diagram).

Keeping User Groups Separate and Secure



The multiple-SSID support can also come in handy during sporting events and other occasional or temporary school activities where limited access by users other than students or school employees might be desirable.

The Price is Right (But Do Your Homework)

It goes without saying that with limited IT staffs and budgets, schools also need networks with an affordable price tag. The good news is that it's finally possible to get enterprise-class attributes all in one affordable package.

One reason is simply that the WLAN industry has matured, and, as mentioned, 802.11n interoperability standards are firmly in place. This has allowed prices to drop in step with volume production, resulting in 802.11n price points falling to about the same as older 802.11g products.

Another affordability factor is that government subsidy programs such as the U.S. Federal E-rate program continue to allow eligible schools to receive steep discounts on networking equipment and services.

Other strides relate to the emergence of simpler architectures that eliminate many of the components and licensing costs that have been associated with many enterprise-class WLAN systems in the past. These trends are described below.

Buyer Beware: Differences in Pricing Models

An important point to consider when comparing prices is the pricing model of the WLAN vendor: what are all the components for which the vendor will charge you? Pricing elements frequently are inconsistent from vendor to vendor, which makes apples-to-apples comparisons challenging. In general, the simpler the pricing model, the easier it is to determine the ultimate price tag of your initial installation and what it will cost to make incremental additions to the network in the future.

For example, some suppliers' networks require costly WLAN controllers while others don't. The purpose of the controller varies from vendor to vendor but, generally, the controller is where most management and control functions take place. The controller-based design requires data streams to be directed through the controller in order to apply any WLAN services, such as security and quality-of-service priority treatment, to them. Some controller-based vendors also require all data traffic to be backhauled to the controller for process-intensive forwarding, as well, which can add more latency,cause performance bottlenecks, and create single points of failure if backup controllers aren't also installed – piling on more capital costs.

While the concept of having services and policies applied centrally is appealing, in practice, this architecture has grown problematic within a high-bandwidth 802.11n environment, including distributed school districts, simply because of the very large data loads that 802.11n can handle. From a cost perspective, the centralized data-forwarding vendors require more controller resources to maintain equivalent throughput support, and this usually results in greater capital outlay (see box, "Controller Resource Costs: Doing the Math").

As indicated, for the resiliency of a business-grade network, the controller-based networks often require schools to buy at least two controllers – one for production and one as a failover. N+1 or N+N controllers might be needed in larger installations. Because controllers are the costliest component of the network, this setup can quickly increase the cost of the overall solution, particularly when redundant controllers are deployed at multiple locations.

Controller Resource Costs: Doing the Math

Assume a 4Gbps backplane in a company's WLAN controller, which is typical. Then assume an installation of 802.11n dual-radio, dual-frequency APs, each capable of 225Mbps total through-put. The 225Mbps figure allows for 75Mbps in the 2.4GHz-band radio and 150Mbps in the 5GHz-band radio. The 5GHz frequency offers greater 802.11n throughput because of a capability called "channel bonding," which isn't practical in the 2.4GHz band.

Given that 4Gbps equals 4,000 Mbps, a 4Gbps controller backplane would support just 18 APs (4,000Mbps divided by 225Mbps per AP) sending full loads simultaneously. 4Gbps controller prices start at about US$13,000 list and can range to US$30,000. At least one vendor has an 8Gbps backplane on the market. It lists for about $22,500 when supporting 50 APs and costs nearly $40,000 to attach 100 APs to it. Add more controllers for more AP support and for redundancy, given that a WLAN controller can be a single point of failure, and you can see that the prices in centralized controller architectures add up rapidly.

Most enterprise WLAN vendors even have an additional management layer that sits above the WLAN controllers to "control the controllers." Such architectures involve still more costs in software fees (described in the next section) and complexity.

Other vendors such as Aerohive, by contrast, more efficiently handle all these functions in distributed APs with only the provisioning and management capabilities conveniently handled through a central management application. Unlike a controller, the management application is not essential to the ongoing operation of the network, which would continue to run if the application should fail. There are many benefits to this architecture; from a pricing perspective, for example, the only components you have to account for are the APs and either the one-time cost of a management system or an annual management "cloud" service fee.

Licensing Fee Gotchas

More subtle pricing discrepancies among vendors exist, too. Some vendors take a nickel-and-dime approach to pricing, in that they charge per-AP license fees for controller usage and often for some or all features that they build into their controllers or management systems. If you need multiple features across many APs, these fees can add up quickly, so it's best to ask about them in detail upfront.

To compare bottom-line pricing across vendors, take all the components you'll need from one vendor – including capital costs of APs, controllers, controller licenses, feature licenses, network management system licenses – and divide them by the number of APs for a per-AP price of the solution. That will give you an apples-to-apples price comparison.

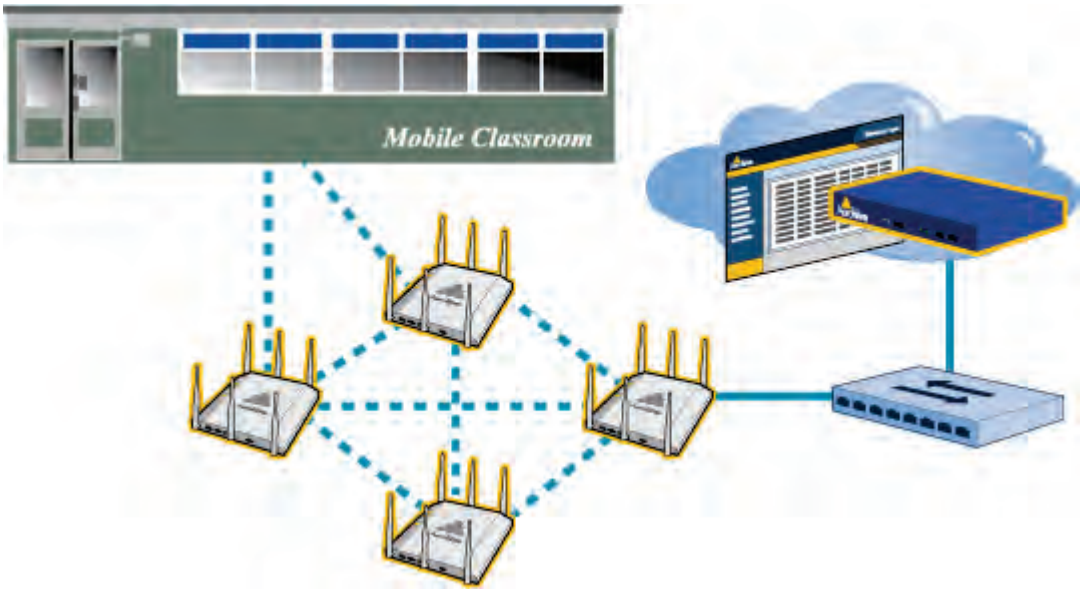
So You Want Scalability? Then Ditch that Controller

Another WLAN attribute important to many schools is the ability to scale themup or down, as needed, without costly licensing or equipment ramifications. Such scalability requires a move away from the centralized controllers described above where the core provisioning, network intelligence, management, and, often, data forwarding take place. Distributing all functions so that an AP can simply be added or subtracted, while the network automatically adjusts to the change, is necessary for meeting budget, for the reliability of the system, and for the sanity of the IT staff. The use of *mesh networking* is a big help on this score.

Temporary Connectivity Requirements

Mesh is a capability that allows two or more APs to communicate directly with one another, over the air, rather than requiring every AP to be cabled and powered separately to a LAN switch or other device. Mesh comes in particularly handy in organizations with temporary WLAN requirements, such as schools with portable classrooms or locations that are hard to reach with cabling (see diagram on next page).

Aerohive customer Wheaton Academy in West Chicago, Illinois, for example, has used mesh capabilities to install an AP high in the cupola of one of its buildings. Because APs simply discover one another and connect automatically, there's really nothing for the IT staff to do but install the AP and let the intelligence built into the system take it from there.



APs connect over the air in a fully meshed configuration. They discover one another, route around failures, and forward traffic to each other using the best path available. An AP can be added in a portable classroom or elsewhere and removed without any ramifications to the infrastructure.

Built-in Redundancy

The mesh capability also plays a large role in supporting business continuity and redundancy. This works in much the same way that IP routers operate in the Internet: if one AP should fail or be decommissioned, the others around it will adjust their power accordingly and direct traffic across an alternative route automatically. This is much more efficient – both from a functional and cost perspective – than investing in multiple expensive controllers that must fail over to one another if an AP connected to it should go offline.

"Why would I pay…thousands of dollars extra for a device [controller] that could deep-six my wireless network?" wonders Bob Vishanoff, Wheaton's director of information services.

Note that mesh support is one of the inconsistent pricing factors across vendors. Some vendors, like Aerohive, build into the fundamental architecture of the WLAN system. Others might charge thousands or even tens of thousands of dollars for mesh capabilities. Still others might not support it at all.

The Aerohive Advantage

Aerohive WLANs use self-organizing APs that require no network controllers or overlay networks. Instead, software in the APs allows them to discover one another as they are added or removed and adjust to the environment accordingly in a fashion Aerohive calls "cooperative control." The networks support enterprise-class network management and security without the cost, performance, and availability issues associated with controller deployments. Cooperative control eliminates the single point of failure, making the system more reliable. It also eliminates the bottleneck often associated with a controller-based system, providing increased performance.

The architecture strikes just the right balance of distributed and centralized capabilities. Data forwarding, WLAN security, and performance-enhancement services such as real-time packet prioritization are distributed out to the individual APs to minimize latency and to ensure that a failed WAN connection to a home location will not interrupt users already on the network.

The most important capability to be centralized – management – is handled from a single workstation, either in an appliance or in a service ("cloud") form factor. This enables IT staff to create a policy and push it out from one spot to any number of APs over the air, providing the flexibility to change policies back and forth as temporary locations or functions take place or new users groups need to join the network.

Pricing and scalability are very easily calculated with the Aerohive solution. You simply multiply the number of APs you need by the per-AP price, then add the cost of the management for that number of APs (your choice of a management appliance, a VMware virtual appliance for your private cloud or Aerohive's cloud-based management service). There are no feature licenses or redundant components to worry about – and thus, no surprises. At time of writing, a typical all-inclusive Aerohive 802.11n solution would cost approximately US$750/AP list price, before any education discounts.

To determine approximately how many APs are needed in your school and where to place them, use this free online Wi-Fi Planning Tool: www.aerohive.com/planner.

For more information about Aerohive's solutions, please visit: www.aerohive.com.

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

Corporate Headquarters
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters
Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252711901

WP1000106