TECH WATCH

Creating Order Out of Chaos

As school districts rely more on wireless, some are finding management and protection a challenge.

Karen D. Schwartz

Jeff Roller is a calm guy, which is surprising, given his line of work. Roller manages more than 800 wireless access points (a number that promises to double in the next two years), serving 56 sites, for the Amarillo (Texas) Independent School District. That means making sure sites are secure, every computer connecting to the network complies with the district's policies and no unauthorized users get in.

Amarillo ISD's Jeff Roller can monitor wireless bandwidth and performance while dealing with rogue access points by using AirMagnet's WiFi Analyzer.
DOUG MERRIAM

The job could be a huge headache, given the complexity of wireless technology, the depth of technical acumen possessed by many of today's high school students and the determination of outsiders to get a piece of the school district's wireless action.

Roller, IT director in the Office of Technology, realized early on that managing a wireless network presented a different set of challenges from managing a wired network. Today, a comprehensive approach to wireless management gives him peace of mind despite the enormity of his task.

For the past five years, the school district has been using the AirMagnet WiFi Analyzer to monitor performance, conduct site surveys, ensure security and generally troubleshoot the network, its users and its access points.

"It became clear about five years ago when we decided to expand our wireless infrastructure across all campuses that we needed something comprehensive, because every campus is constructed differently," he explains.

The Growth of Wi-Fi

Amarillo, which already runs 802.11a, b and g, is aggressively adding 802.11n to its schools.

Lamar (Texas) Consolidated Independent School District is just starting down the wireless path, but its IT staff has the same goal — to make sure from day one that its wireless network is secure and managed efficiently. The 22,000-student district, located 35 miles southwest of Houston, also chose to go with the AirMagnet WiFi Analyzer as part of a massive project to outfit the entire district with wireless access.

"We're about to embark on a wireless overlay for our school district, and we need diagnostic and monitoring tools to manage what's coming onto the network and to be able to monitor how the system is working," says Network Administrator Vincent Lapetino.

What the Lamar and Amarillo districts are doing — making sure their wireless networks are managed comprehensively — is the only way to go, says Mark Tauschek, a senior research analyst at Info-Tech Research Group of London, Ontario.

Current Issue
Mar/Apr 2009
In With the Good — Out With the Bad
Uptime Rules of Thumb
A Data Center Turns Inward
TOC

“School districts in particular need a way to manage wireless networks from a single pane of glass for all locations, because they are so geographically dispersed,” he says. “And security is paramount in K–12, so a system that can constantly collect data and send it to a management console for quick analysis and action is very important.” Amarillo ISD is just one of hundreds of school districts in North America moving aggressively to wireless technology. According to ABI Research of Oyster Bay, N.Y., Wi-Fi usage in K–12 is expected to grow significantly in the next five years (see chart, right), driven by a move toward “anytime, anywhere” learning, as well as the need to adopt secure technologies such as wireless video surveillance.

And that means finding tools that manage the wireless environment as thoroughly as schools’ wired networks are managed, says Ed Zaiontz, chairman-elect of the Board of Directors for the Consortium for School Networking (CoSN) and executive director for information services at Round Rock (Texas) ISD.

“The types of safeguards that have been in place for physical networks now have to apply to wireless networks, like monitoring bandwidth and performance and dealing with rogue access points,” he says. “You want users to be able to connect only to approved access points, and you don’t want people from outside to be able to connect to your network without your knowing about it.”

For Amarillo, AirMagnet WiFi Analyzer does all of that and more. For example, Roller’s team uses it to conduct site surveys and spectrum and performance analysis to determine the best locations for wireless access points.

“We need to know what RF [radio frequency] fields we would be dealing with in each location — where the microwave in the cafeteria is that could cause interference, where other wireless signals in a residential neighborhood might cause interference, and where the optimum location of access points in each location should be,” Roller explains. “It helps us determine where we can best tune our signals to keep the public out of our network and keep the public’s networks out of our schools. Using these features, we can determine the best places to put access points to create a campuswide wireless infrastructure and guarantee that each classroom has connectivity.”

Preparing for the Future

If a school district plans to implement performance management and troubleshooting tools for wireless networks, the tools should definitely be compliant with 802.11n, an up-and-coming standard that will drastically improve wireless network speeds, CoSN’s Zaiontz says.

“Many school districts are migrating or planning to migrate to 802.11n, because it gives them the speed they need for more bandwidth-intensive applications, like video streaming, videoconferencing and online testing,” he says. “A tool like this that can handle 802.11n can go a long way toward ensuring that the wireless network doesn’t become overwhelmed.”

AirMagnet WiFi Analyzer does support 802.11n — and it’s a good thing, considering that Amarillo ISD is moving aggressively toward adopting the standard, as its budget allows. To get the best performance from 802.11n, the school district also has installed AirMagnet’s 802.11n wireless PC card.

“We needed something that would allow us to test 802.11n,” Roller says. “For example, if I know an application will require 18 megabits per second of throughput, I can simulate with AirMagnet to guarantee that we have 18Mb across all locations. And it will do the same when we get to applications that require 300Mb of throughput.”

One of WiFi Analyzer’s most important jobs for Amarillo is detecting rogue devices. And that goes for students as well as outsiders.

“If a student brings a laptop in — something they aren’t currently allowed to do — how do we know it has the antivirus or spyware protection that our policies require?” Roller asks. “With this tool, I know what devices are supposed to be on my network, and I can verify based on MAC [Media Access Control] that there is a rogue device, and based on the radio frequency, I can find it in a specific location.”

That feature will become even more important when the school district allows students to bring notebooks from home. When that time comes, “we can use AirMagnet to make sure they are compliant with our policy,” Roller says.

And Roller is confident the tool will easily be able to handle the doubling or tripling of access points that he expects as a result of state initiatives for online standardized testing.

“The only way we will have enough seats and machines in front of kids is by installing more wireless access points, but we know that with what we have, we can handle it,” he says.

Preparing for 802.11n

School districts, much like large companies with a dispersed workforce, are good candidates for faster, more reliable networks that can handle massive bandwidth.

Although the new 802.11n standard isn’t fully approved, it’s finished for all intents and purposes, and most major manufacturers have 802.11n products ready to go. It’s expected to be available by the third quarter of next year at the latest.

Once an organization has decided to go with 802.11n, the IT department must decide how best to manage it. Some tools are good for site surveys or planning, while others specialize in managing multiple environments or widely distributed geographical locations.

In some cases, it makes sense to go with a third-party tool, such as a wireless LAN assurance tool, which can verify that the network is actually accomplishing what you think it is doing. Third-party tools also are recommended for intrusion detection on wireless networks.

Implementing an 802.11n network also means shoring up the security infrastructure. For example, few wireless intrusion detection systems today detect 802.11n, because they were designed for 802.11a, b and g. That means organizations installing 802.11n must upgrade immediately to detect n-based networks so they can monitor for rogue access points and ad hoc networks.

Projected Growth* of K–12 Wi-Fi in North America

.50% - 2008

2% - 2009

5% - 2010

9% - 2011

14% - 2012

18% - 2013

**compound annual growth rate*