COSN'S
EMERGING
TECHNOLOGIES
SERIES

a guide to WIRELESS LANs IN K-12 SCHOOLS

CoSN
ADVANCING K-12 TECHNOLOGY LEADERSHIP
WWW.COSN.ORG

COSN'S
EMERGING
TECHNOLOGIES
SERIES

a guide to WIRELESS LANs

IN K-12 SCHOOLS

Consortium for School Networking
1710 Rhode Island Ave., NW Suite 900
Washington, DC 20036-3007
www.cosn.org
October 2003

Acknowledgements

A Guide to Wireless LANs in K-12 Schools was written by CoSN's Emerging Technologies Committee under the direction of report co-managers Gene Broderson and Darrell Walery. It was edited by Judy Salpeter with art direction by Glenn Hennessey. CoSN would like to thank sponsors Editorial Projects in Education—Publisher of *Education Week*, Plato, and SpectraLink for their generous support.

EMERGING TECHNOLOGIES COMMITTEE MEMBERS

Committee Chairs

Steve Rappaport
Executive Committee Chair
Consultant

Guy Harris
Co-chair Exploration Subcommittee
Market Development Manager
Texas Instruments, Inc.

Jennifer House
Co-chair Exploration Subcommittee
Principal
KCH Strategies

Kathryn Walsh
Co-chair Exploration Subcommittee
BBP

George Laskaris
Co-chair Implementation Subcommittee
Executive Director
New Jersey Higher Education Network

Karen Greenwood
Co-chair Implementation Subcommittee
Owner/Consultant
Nimble Press

Darrell Walery
Co-chair Implementation Subcommittee
Director of Technology
Consolidated High School
District 230, IL

Gene Broderson
Co-chair Dissemination Subcommittee
Director of Education
Corporation for Public Broadcasting

Marianne Pack
Co-chair Dissemination Subcommittee
Director, California Technology
Assistance Project – Region 6
Stanislaus County Office of Education

Tom Rolfes
Co-chair Dissemination Subcommittee
Education IT Manager
Nebraska CIO/NITC

Other Members of the Executive Committee

Jeff Dyson
Strategic Alliances Manager
SpectraLink Corporation

Jim Hirsch
Assoc Superintendent for Technology
Plano ISD, TX

Keith Krueger
CEO
Consortium for School Networking

Irene Spero
Vice President
Consortium for School Networking

Exploration Subcommittee Members

Robert Agoglia
Technology, Staff Developer
Community School District 20, NY

Dean Bergman
Administrator, Educational Technology
Nebraska Department of Education

Marla Davenport
Director, Learning and Technology
TIES

Tracy DuBay
Educational Technology Program
Western Michigan University

William Heidenreich
Director of Technology
Bellmore-Merrick Central HS District, NY

Joseph Micheller
Exec Dir of Curr, Instruction, Staff Dev
Cleveland Heights –
University Heights City Schools, OH

Kenneth Reed
Dir of Instruct Tech Servs & Resources
ACPS Burke

Ray Rose
Vice President
Concord Consortium

Bill Swift
Marketing Programs
3Com Corporation

John Watson
President
Eyecues Education Systems

Pat Whitney
President
Maximum Performance Partners

Implementation Subcommittee Members

Claudia Anderson
President
Audio Enhancement

Jayaram Balachnader
Chief Technology Officer
bigchalk.com, Incorporated

Michael Bowling
Director of Technology
Middletown/Monroe City Schools, OH

Dwight Christie
Director - MIS
Salina Public Schools, KS

Linda DeGrand
Section Chief, Distance Learning Sys
NC Department of Public Instruction

Carol Kaunzner
Technology Director
Fort Huachuca Accommodation
Schools, UT

Mignon Plyler
Director of Technology
Sherman ISD, TX

Thomas Shessler
Consultant - Instructional Technology
Hamilton County Educational Service
Center, OH

Susan Sullivan
Educational Technology Specialist
New Jersey Department of Education

SallyAnn Zoll
President/COO
LearnStar, Inc.

Dissemination Subcommittee Members

Mary Baker
Manager, Emerging Technology
School Board of Broward County, FL

Lynette Guastaferro
Director of Distance Learning
Teaching Matters, Inc.

Amanda Kenyon
Content Specialist
MINDS

Chee Pung Loy
Education Development Manager
Intel Americas, Inc.

John Merli
Director, Communications
Funds for Learning

Eric Nicklas
Program Manager
Missouri Research and Education
Network

Matthew Norton
Natl Sales Supportt Coordinator
Cox Business Services

Henry Pollock
Director of Professional Development
Miami Museum of Science

Bookie Shillcut
Technology Publisher
Peter Li Education Group

Gwen Solomon
Co-Director
TechLearning.com

Meegan White
Community Partnerships Coordinator
Assn of American Public TV Stations

Alan Wibbels
Technology Director
Educational Service Unit 10-Nebraska

Steve Zsiray
Assoc Supt of Inst Technology
Cache County School District, UT

Table of Contents

a guide to WIRELESS LANs IN K-12 SCHOOLS

Wireless local area networks (WLANs) have been around for some time, but only recently have the costs and benefits met at the magical point that propels a new technology into the mainstream. New standards, faster speeds, and decreasing costs are combining to make wireless networking an ever-more appealing solution for school campus connectivity needs.

This report from the Emerging Technologies Committee of the Consortium for School Networking (CoSN) examines the implementation of wireless LAN technologies in K-12 schools and identifies challenges, options and lessons learned. Some of the critical issues addressed in the pages that follow include: standards and compatibility, planning and implementation, security, and total cost of ownership (TCO). The goal is to provide a practical road map for CTOs, CIOs, school administrators, technology coordinators and others charged with planning for wireless implementation. It should be noted that the use of handheld devices—and the wireless connectivity associated with them—will not be the focus of this report but will be addressed in a future publication.

Why Wireless?

Ask any analyst about new technologies that are seeing rapid adoption in schools and wireless technologies will undoubtedly be near the top of the list. Here are some of the most compelling reasons schools give for purchasing wireless LANs.

MOBILITY: A wireless LAN (WLAN) makes it possible to roam virtually anywhere in a building or campus and still stay connected. With the growing popularity of laptops, notebooks, and PDAs—as well as newer devices such as tablet PCs and wireless Voice Over IP (VoIP) telephone devices—such mobility is increasingly important. Examples of education programs that involve mobile computing include: students carrying their own laptop computers from class to class and school to home; teachers and administrators keeping track of daily routines using laptops or PDAs; student researchers gathering data electronically from beyond the classroom walls; and mobile computer labs available to classrooms on an as-needed basis. With a WLAN, users of these mobile devices can upload or download tools and

assignments from the school network or access the Internet without needing to stop, locate an Ethernet connection and plug in. In addition to computing applications, the same wireless LAN can also support mobile telephones, keeping teachers and administrators in touch throughout the school facility without any airtime or usage charges.

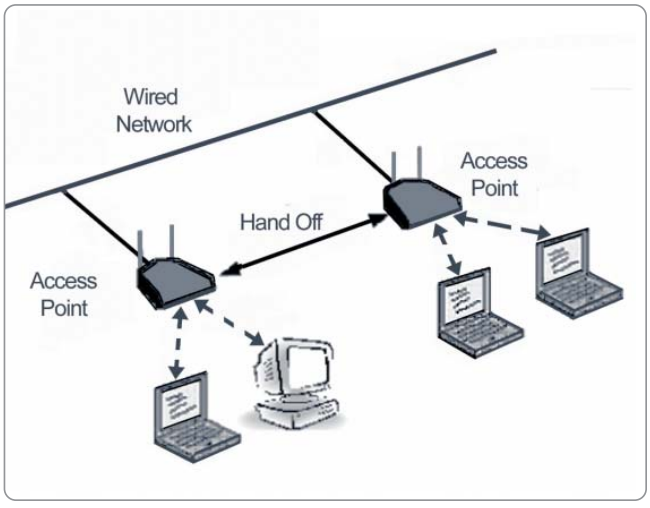
FLEXIBILITY: With ever-changing populations, resources and needs, schools rarely have the luxury of installing computer networks and leaving them unchanged. Many districts deal annually with expansions, renovations, portable classroom structures and other physical changes to their facilities. Wireless technology can play a significant role by extending the wired infrastructure to allow devices, people and entire classrooms to be moved without having to add or re-run cable. Within individual classrooms, wireless LANs provide flexibility as well—making it easy to pull together an ad hoc lab of laptop computers, for example, or add new desktop computers and printers to the mix without having to drill new holes or run hard-wire drops to each hardware device.

SAVINGS: Hard wiring school buildings can be staggeringly expensive, especially since the majority of older buildings were not designed with cable runs in mind. Eliminating the need to wire and rewire—especially in those facilities with hard-to-access walls—can result in a tremendous financial savings for schools. Phasing out hard-wired labs in favor of mobile wireless laptop labs can also save space and money in overcrowded schools. While the cost of purchasing and maintaining wireless networks and devices should not be dismissed as inconsequential (see the section on TCO later in this report), many districts find that, in the end, wireless LANs save them money.

EXPANDABILITY: When adding wireless technology, existing networks do not need to be abandoned. On the contrary, most wireless LANs are used as add-ons to wired networks; wireless access point devices are located in strategic locations to connect mobile devices or hard-to-wire classrooms to the existing network. In this way, districts expand their options without losing their initial investment in infrastructure.

Components of a Wireless LAN

The main elements of a WLAN are access points and computers equipped with wireless network cards or receiving stations. The access point is the wireless equivalent of a LAN hub. It receives, buffers, and transmits data between the wireless LAN and the wired network, supporting a group of wireless user devices.



An access point is typically connected to the wired network through a standard Ethernet cable, and

communicates with wireless devices by means of an antenna. The access point transmits to and receives signals from devices such as laptops, PDAs or other computing devices that have been equipped with wireless network interface cards (NICs) that are able to communicate by radio wave rather than a physical cable.

The access point, or the antenna connected to it, is generally mounted high on a wall or on the ceiling, providing network access to any enabled device that enters the area. Under the right conditions a single access point can serve several rooms. Sometimes the access point moves with a mobile lab as part of the cart configuration. Rooms in which the mobile cart is to be used must have at least one network drop to which the access point can be attached when in use.

Access points have official ranges from under 20 meters to 500 meters, although it is important to note that typically observed ranges are invariably much lower than the official maximum. A single access point can typically serve 15 to 25 computers, although the numbers vary greatly depending on the technology, configuration and use. Like the cells in a cellular phone network, multiple access points can support hand-off from one access point to another as the user moves from area to area.

Internet access is addressed by means of a router, which provides the connections from wireless and wired devices to the school's broadband Internet connection, such as a T-1 or DSL line. In addition, it is possible to connect wireless LANs on different parts of a campus to one another via wide-area wireless devices.

Understanding the Standards

Implementing wireless networks requires a working knowledge and understanding of emerging wireless standards. Given how quickly the standards for wireless technology are being updated, it's little wonder that many people are confused. As one sage said, "The best thing about standards is that there are so many of them."

For schools interested in implementing WLAN technology in 2003 and 2004, the options that are most important to understand are the three current versions of the 802.11 standard set by the Institute of Electrical and Electronics Engineers (IEEE). Devices complying with the 802.11 standards are also known as "Wi-Fi" (for Wireless Fidelity). The four basic factors that distinguish the standards from one another are: frequency, speed, range, and number of non-overlapping channels. Compatibility issues are also a factor in comparing options.

If you have already implemented wireless technology in your district, you are probably working with the earliest version of the 802.11 standard: 802.11b. It is relatively inexpensive and has been the most widely accepted standard in wireless networking to date. Officially offering speeds up to 11 megabits per second (Mbps), 802.11b is what is built into most existing laptop wireless NICs and is the current standard in cafés, airports and other places where public wireless access is so popular. It operates in the 2.4 GHz radio band, which actually means that it occupies approximately 30 MHz of the frequency spectrum—with its first channel operating at 2.412 GHz, second at 2.417 GHz, and so on. For practical purposes, it offers three channels (channels 1, 6, and 11 for the

Wireless Standard Summary

	802.11b	802.11a	802.11g
RADIO FREQUENCY	2.4 GHz	5.8 GHz	2.4 GHz
LINK SPEED			
Maximum	11 Mbps	54 Mbps	54 Mbps
Typical performance	4-5 Mbps	20 Mbps	20 Mbps
DISTANCE COVERAGE			
Inside	300-500 feet	100-164 feet	300-500 feet
Outside	1,500 feet	100-164 feet	1,500 feet
NON-OVERLAPPING CHANNELS	3	12	3
STRENGTHS	-Older and less expensive than **a** or **g** -Most products already on the market use **b** -Wider range than **a**	-Considerably faster than **b** -More channels -Using the less common 5 GHz frequency results in less interference	-Considerably faster than **b** -Backward compatibility with the widely-adopted **b** gives it a major edge over **a** -As it gains momentum, it is becoming considerably less expensive than **a**
WEAKNESSES	-Fewer channels and lower speed mean limited bandwidth -2.4 GHz is more common frequency, which can result in interference	-Expensive -Not compatible with **b** or **g** -Shorter range than **b** or **g**	-Since it is so new, devices that use it are just beginning to appear -More expensive than **b** -2.4 GHz can result in interference

GHz = Gigahertz
Mbps = Millions of bits per second

U.S.) that can be used without interference from adjacent, "overlapping" channel frequencies.

A more recent standard, 802.11a, delivers better performance and support for denser networks. It operates in the 5 GHz radio band, a less crowded frequency than the 2.4 GHz band, which is used by home cordless phones, microwaves and other devices. Offering a maximum link rate of 54 Mbps, 802.11a allows better support for video and multimedia applications and places wireless networking speeds more in line with the fast Ethernet speeds (100 Mbps) commonly available through wired networks. In addition to the faster link rate, the 802.11a standard specifies up to 12 non-overlapping radio channels. This—and the fact that the 5 GHz frequency is not widely used—results in better protection against possible interference.

But every silver lining has at least one cloud.

A down side to 802.11a is that it has half the range of 802.11b, requiring twice as many access points. In addition, the newer standard has a more difficult time penetrating walls, which makes it less desirable for interior applications involving mobile devices and roaming access. Another serious concern is that 802.11a does not work with existing 802.11b devices. Since 802.11b is so common—and can be expected to be around for a long time—the incompatibility factor has prevented many consumers and manufacturers from jumping on board. This, in turn, has kept the prices on new 802.11a products quite high.

While a number of companies have promised access points that support both 11a and 11b standards, it is likely that 802.11a will be superseded by the newest wireless standard: 802.11g. Approved by the IEEE in June, 2003, 802.11g operates in the same 2.4 GHz radio band as 802.11b but has speeds equivalent to 802.11a. A big plus for 802.11g is that it offers backward compatibility with the original 802.11b standard. Although prices for 802.11g products will be higher than the older 802.11b options, they are generally less expensive than 802.11a—and expected to drop as the new standard gains popularity.

Deciding When and Where to Jump In

Of course, nothing in the world of technology stands still and there are plenty of committees at work defining even faster, more robust wireless standards. These include 802.11n, a still-undefined standard meant to operate at speeds in excess of 100 Mbps, and Ultra Wideband (UWB) an even faster standard that will use numerous channels, rather than a narrow band, and is expected to offer speeds approaching 1 gigabit per second.

As with every new proposal, there is plenty of political wrangling around these and other emerging standards, and even the winners are not likely to be producing usable products for a few years. With today's wireless technologies already meeting many educational needs, few advisors would recommend waiting around for tomorrow's breakthroughs. But being aware of trends and predictions allows K-12 decision-makers to adopt wisely.

Here are some suggestions from educational leaders and industry pundits with experience implementing wireless networks:

- For schools just getting going with wireless, jumping straight to the newer, faster products is worth considering, although price concerns might make it preferable to combine some old with the new. With the backwards compatibility of 802.11g or dual cards, for example, it is possible to continue to invest in inexpensive 802.11b devices for most uses while upgrading to a or g for applications involving video or other high-bandwidth needs.
- If you have already implemented the 802.11b standard and have no pressing need for higher bandwidth applications, then you can afford to wait and see which of the new standards best fits your needs and budgets.
- Given the comparative strengths of the two newest 802.11 standards, a number of schools are considering 802.11a for external connections between buildings while moving to 802.11g for high-speed, internal connectivity.
- To minimize compatibility issues, look for products

that are "Wi-Fi certified." The Wi-Fi Alliance is a nonprofit organization formed in 1999 to certify interoperability of 802.11b products and to promote Wi-Fi as the global, wireless LAN standard across all market segments. The Wi-Fi Alliance has instituted a test suite that defines how member products are tested to certify that they are interoperable with other Wi-Fi certified products. With the advent of backwards-compatible standards, Wi-Fi certification will be extended to the newer, faster products as well.

- A number of companies now promise dual or multiple-standard access points and NICs. Investing in a large number of dual band (or "combo") PC cards and desktop NICs today can be prohibitively expensive, but adding new access points that support both standards is worth considering if you are hoping to tap into the best of both worlds. Or you can set up separate access points—each supporting its own standard—and link them together with inexpensive switches.
- Wireless is not the best solution in every situation. Wired networks are still faster than even the best wireless options available today, making them better for multimedia and video conferencing. When cable has already been run and mobility is not an issue, you may want to stick with—and add on to—your existing wired network. In only rare situations will a school or district want to go entirely wireless.

Designing the Wireless Network

Careful planning is essential before you begin implementing WLAN technology in your school or district. Unless you have professional IT staff members well trained in wired and wireless network implementations, you might want to contract with an outside consultant experienced in deploying wireless networks and conducting professional site surveys. Whatever choice you make about this, you will find that there are several key steps involved in planning for WLAN implementation. They include:

DETERMINING THE SCOPE

A scope document is frequently used to define the performance specification for a site—including the desired applications of wireless and the number and type of devices to be used. The scope might involve mobile laptop labs, wireless laptops and/or wireless telephones for teachers, or a network to support one-to-one student-to-computer ratios. Performance specifications go on to define what the wireless infrastructure must be able to do. For example, you might specify that each classroom in area A should be able to support up to 25 laptops simultaneously with a maximum of 50 laptops connecting to and using the Internet. The scope document must account for the expected use over a period of time, not just the current semester. It is important to determine the scope within the context of the school's curriculum goals, technology plan, expected purchases, professional development needs, and even after-school programs or outdoor use. The plan also should account for anticipated changes in environmental conditions such as remodeling and expansion.

PLANNING THE LAYOUT

Once the scope of the implementation has been determined, it is necessary to design the layout of access points to maximize coverage and minimize cost. This generally involves a professional site survey to determine the number of access points needed and their placement. Most wireless vendors will conduct a site survey as part of the bidding process, although many school districts opt to hire an independent consultant to offer a vendor-neutral plan.

As part of the process, professional surveyors use sophisticated signal-strength measurement instruments to map out a comprehensive plan for deployment of access points. Factors in the analysis and design include the number of simultaneous users, their location and activities, the architectural plan of the school and the building materials used. Because the access devices use radio frequencies, they can go through plaster and wood quite easily but brick, concrete, cinderblock, or metal walls can significantly reduce propagation coverage and create dead zones requiring additional access points. In addition, access points that are too close together create interference that can impair the performance of the network.

Maximum coverage needed and total devices available must be balanced to create the most cost-effective layout. For example, designing an implementation that allows all students to connect at all times may be overkill if your school only has two mobile labs with 16 devices per lab. With a maximum of 32 computers in use at any time, you can probably meet your needs with 2 or 3 access points. At the same time, you will want to have a plan in place for extra access points to be added as additional users and connections enter the picture.

In addition to location, you will need to decide if you will use fixed or mobile access points or some combination. When the goal is to provide coverage to multiple classrooms or to allow mobile device users to roam freely in a school building, the solution generally involves fixed access points mounted in the ceiling or on the wall. Schools that are using wireless carts to create mobile computer labs have a choice between installing fixed access points in all the classrooms that will share the lab or opting for a mobile access point that travels with the cart and gets plugged into the network once in place. The mobile option can minimize the number of access points that need to be installed but it does require network drops in key places and adds an extra setup item for teachers who are preparing to use the lab.

SELECTING WIRELESS DEVICES

Access points and wireless mobile devices vary in price and features. Finding publications or organizations that you trust to compare and evaluate the options is always wise. In addition, the following factors should be prioritized to determine the best fit for your district's budget and implementation needs.

- **Manageability:** Since management tools and options vary in their sophistication, consider what sorts of control your network administrators will want to have over the system—and how much time they are willing to devote. More features mean more options, but options are only of value if managers plan to use them.
- **Scalability:** Do the devices fit into your long-term wireless strategy? How easy is to add new access

points or expand the WLAN in other ways? Are there upgrade paths for supporting the newest standards as they are announced?

- **Support:** What kind of technical support and warranties are provided by the manufacturer? Are driver and firmware updates readily available and easily distributable? Does this company have a reputation for stability and longevity in the technology market? A stable company will more likely provide support and upgrades for their products well into the future —a feature that is very important in this rapidly-changing field.
- **Dependability and Performance:** What have others found out about the dependability and performance of a particular WLAN setup? Online newsgroups and trusted publications are two places to find candid reviews of products.
- **Compatibility:** Look for Wi-Fi certified devices. Even then, there can still be compatibility issues with equipment from different vendors. Using the same vendor for wireless NIC cards and access points is often recommended for large installations. You should also make sure that these devices are compatible with the platform or operating system you are using.

EVALUATING AND PLANNING FOR EXPANSION

The planning process does not stop once you have purchased and installed your first wireless networks. Many districts are choosing to phase in their wireless installations gradually, piloting them in one school or department to analyze the feasibility of expansion. Careful monitoring of usage patterns, unexpected problems and costs, and user opinion is essential to determining next steps.

Understanding the Security Risks

One of the most widely-held concerns about wireless networking is the security challenge it presents. In addition to securing equipment from tampering and theft—a natural concern given the portability of laptops and mobile access points—education leaders need to think about securing the district's data and infrastructure from hackers and unauthorized use.

Since wireless technology was originally designed for military use, security issues have always been a consideration. The IEEE task group that specified the 802.11 standard incorporated three security measures that it hoped would provide a level of privacy similar to ordinary wired networks. These include:

- **Wireless Equivalent Privacy (WEP),** which uses encryption keys, or codes, to match the client device with the access point.
- **Service Set Identifier (SSID),** a password that enables access to the WLAN.
- **Media Access Control (MAC),** authentication protection that restricts access to computers on a list created for each access point on the WLAN.

Unfortunately all of these methods have proven to be far weaker than intended—allowing "eavesdroppers" and hackers fairly easy access. Dr. Jane Bloomquist, Quality Assurance Manager for the Chicago Public Schools talks about urban schools

that have been "warchalked" by hackers who mark the Tsunami symbol on buildings and sidewalks outside wireless school sites to indicate free access. In fact, an entire community of hackers (or "whackers" as they're often called in the wireless world) is actively engaged in exchanging information on wireless "freeloading" opportunities using Web sites such as netstumbler.com.

While this sort of whacking usually focuses on gaining free access to the Internet, Bloomquist and others worry that the same security holes can be used to access confidential student information, alter records, or inflict malicious damage of other sorts on school LANs. Clearly this could be disastrous for a school district.

With security topping the list of wireless concerns for users in the business and government sectors as well, the IEEE 802.11 task group is hard at work on specifications for a new security standard to be called 802.11i. The enhancements will include an entirely new privacy algorithm and provisions for enhanced authentication. The goal was for 802.11i to be finalized by the end of 2003 with products incorporating it by early 2004, although it is not clear whether this timeline will be met.

In the meantime, however, incremental improvements have been made along the way. Most notably:

- **WEP encryption schemes** have improved over the years, moving from the original 64-bit scheme (also known as"40-bit" because it uses a 40-bit key and 24 bits of system-generated data) to cards that offer a choice of 64-bit, 128-bit or, more recently, 256-bit encryption.
- **802.11X,** an authentication protocol, has been incorporated into many Wi-Fi wireless devices since early 2002. It employs dynamic keys instead of the static keys used in WEP and has improved authentication procedures.
- **Wi-Fi Protected Access (WPA),** a subset of the 802.11i developing standard, has recently been certified by the Wi-Fi Alliance for use in new products. It changes the way keys are derived, rotates them more often for security, and adds a message-integrity-check function to prevent packet forgeries.

Choosing Your Solutions

Since virtually all of the security approaches described here come at a cost, an important starting point is to develop an overall security strategy based on an evaluation of your risks. How is the wireless network being used? What is the risk to your district if the data on the network are accessed? What happens if unauthorized users start connecting through your access points? What types of unauthorized uses present the greatest threat?

With these concerns in mind, you are ready to consider the precautions suggested here:

- **Use the features already offered by your wireless system.** According to many experts, the biggest threat to the security of any wireless LAN is the failure to use the optional protection mechanisms that are built in. For example, a surprisingly high number of users fail to turn on WEP encryption.
- **Set a unique SSID.** Every system comes with a simple default SSID that is widely known to potential hackers. (Cisco Aironet's identifying

"tsunami" SSID, for example, led to the popular war tag described earlier.) Configuring the wireless LAN with a unique system ID—one that does not identify the school, district or location—is an important start. You might consider turning off the broadcasting option that has the access point automatically send its SSID information out to devices on the system, although the down side to disabling the broadcast is that each user will need to know the SSID and enter it manually.

- **Change WEP keys periodically.** In smaller wireless systems, with a limited number of wireless devices and management tools that help automate the process, it can be feasible—and wise—to change WEP encryption keys as often as once a week. Even if the size of your system makes such frequent changes unworkable, consider changing the keys on occasion to decrease the ease of hacking.
- **Set the highest level of encryption your system can comfortably accommodate.** If you have the option of 128-bit or even 256-bit encryption and the information on your network is sensitive, it might makes sense to employ the higher-bit encryption. Bear in mind, however, that all the devices within a particular WLAN need to be set to the same level and that each new level can have a negative impact on system speed.
- **Use the security features of your operating system and basic applications.** It should go without saying, but it is probably wise to remind everybody involved to password-protect any files, documents and folders that contain sensitive data.
- **Keep your instructional and administrative domains as separate as possible.** For many districts this means limiting wireless communications to instructional applications and Internet searches and not allowing any wireless access to student records or other sensitive data. Naturally, this is impossible in districts where an important component of the wireless program involves teachers or administrators using wireless laptops as their main computing device. In those cases, additional methods need to be employed to protect the administrative portion of the network.
- **Implement firewalls.** For starters, you will want a hardware-based firewall to protect the main administrative network. Many districts are also considering implementing software firewalls at lower levels—possibly all the way down to the individual computers.
- **Consider installing a Virtual Private Network (VPN) to encrypt data exchanged between wireless devices and the server.** While firewalls are designed to prevent unauthorized users from accessing data residing on your server, VPN systems protect information as it travels between two points—in this case, between the school or district server and wireless computers. Essentially a VPN creates a "virtual tunnel" to carry the encrypted data. This requires installing additional software on your server, but the VPN client is already included in many desktop/laptop operating systems.
- **Power down your wireless access points when they are not in use.** This process can be automated using management tools with timers set to turn access points off when they are not needed.

As the wireless industry attempts to arrive at a standardized solution to users' security fears, system administrators have a variety of options. Clearly each of these involves tradeoffs. Not only do the newest devices require a financial

investment, upgraded protection schemes have the potential to gobble up a great deal of administrative time as network managers focus on ensuring that every device on the WLAN continues to employ and recognize the same passwords, ids, encryption schemes and more.

There are also tradeoffs between security and performance, with additional levels of encryption or authentication generally taking up bandwidth and slowing down performance. Finally, there is the issue of standardization. Whether you are incorporating a higher level of encryption or a new authentication protocol, all the devices on a particular WLAN need to be capable of—and set to make use of—the same controls or else communication breaks down.

It is likely that, as the most blatant WLAN security vulnerabilities become a thing of the past, schools will find themselves investing in the newest solutions while migrating the "older" WLAN devices to particularly non-vulnerable uses. In the meantime, each district must weigh its options and chart a path consistent with its overall security policies and concerns.

Managing the Network

As many of the schools profiled in the appendix on pages 18 to 22 will attest, the deployment of wireless technology involves a considerable amount of work on the part of technology coordinators, network managers and support staff. While one or two access points are relatively easy to install, the challenges escalate quickly when a school considers a more comprehensive wireless solution. New management tasks range from the security monitoring described above to maintaining and scheduling the use of mobile labs.

In the first few years of a wireless adoption—especially with industry standards changing every several months—one can expect to spend time troubleshooting. As Steve Zsiray, associate superintendent for curriculum and instructional services in Cache County, Utah, puts it, "Our goal is provide a seamless solution but it takes a while to get there." In the meantime, he counts on "teachers who are pioneers and willing to put up with problems, and frustrations," as well as on "great technicians who like to read and experiment."

Examples of the sorts of glitches Zsiray and others have reported in their first years of implementation:

- **Recognition and login problems:** As laptop users move from one part of a campus to another, the process of attaching to the wireless network can sometimes be buggy—either because there are too many users in that segment of the WLAN or because the access point and wireless card somehow fail to recognize one another.
- **Speed issues:** Even the fastest WLAN today is slower than the wired networks teachers and students are used to. Unless educators have realistic expectations and limit their wireless uses to lower-bandwidth ones, they are likely to be frustrated—especially with 802.11b solutions. In addition, some schools have found that login delays or retransmission to correct bit errors slow things down more than anticipated.
- **Compatibility issues with upgrades:** As already mentioned, upgrading to newer standards—for performance or security reasons

—can result in a mixture of older and newer devices that might not be able to communicate with one another. Even when an upgrade can be made to older equipment, the system sometimes lacks the power to perform well—leading users to consider having to replace currently installed devices.

- **Access point adjustments:** In spite of careful planning, some sites find themselves having to rethink the placement of access points to avoid dead spaces. On the other hand, access points located too close to one another can be confused by the wireless computing device and freeze up.
- **Network reliability:** The inherent nature of wireless communications, with all of its flexibility, also entails a vulnerability to loss of signal, RF interference and other complexities requiring additional user support.
- **Inappropriate uses:** An example of "wireless gone bad," shared by Karl Yeutter of Kearney Public Schools, is illegal music swapping by students using the school's wireless access points. The students were bringing mobile devices to school with music downloaded from peer-to-peer services on the Internet and swapping them wirelessly with peers at school.

Analyzing Total Cost of Ownership

As with any technology, the costs of going wireless involve more than an initial investment in equipment. When school districts ignore the questions of Total Cost of Ownership (TCO) over the lifetime of the technology, they risk unforeseen expenses and complications.

The chart on this page takes a quick look at some of the TCO factors to be considered in the first stages of wireless implementation. Since costs will vary significantly depending on your region, physical plan and technological needs, these prices should be used only for preliminary estimates; you will want to adjust them for your own circumstances based on a site survey and bids from potential vendors.

Wireless TCO Overview

COMPONENT	ESTIMATED COSTS
Access Points	-$238 to $638 each
Wiring (to connect the access points to the wired network)	-$100-$200 per drop
Wireless Cards	-$47 to $121 each
Installation Services	-30 to 35% of the equipment cost
Security Solutions	-$0 to $12,000 (varies greatly)
Carts (with power outlets)	-$550 to $1500
New computing devices	-Laptops: $1200 to $2000 each -PDAs: $100-$600 each -IP wireless phones: $500-$800 each
Access Point Management	-Basic management generally provided by manufacturer but additional management features are offered by third parties at varying costs.
Training	-$100-$175 per hour
Monitoring software (to detect interference)	-$0-$8,000

Here is an explanation of some of the costs in the chart on page 13:

- **Installation Costs:** Installation costs can be calculated in many different ways. As a general rule, installation adds about 30 to 35 percent to the total of all hardware and software costs, although a more complex installation could add up to 40 percent. Wiring costs listed above include installation.
- **Security Costs:** Security solutions range from the software and firmware included with the cards and access points to third party hardware. As an example, adding a hardware VPN (virtual private network) to your network can range in price from $5000 to over $10,000.
- **Access Point Management:** A number of excellent WLAN management software products allow a trained network administrator to monitor traffic, generate bandwidth reports, run diagnostics on access points, produce statistical analyses for weak links in the system, and remotely install software upgrades from a central location. If the access point does not come with suitable management software, third party software products may be needed. Products for larger installations are priced per access point and others can be purchased as single software solutions to run on laptops.
- **Technical Training:** Although you should expect the initial installation to include training for local technical support staff, we have indicated how much it is likely to cost if priced separately. Training sessions at the time of installation assures that technicians will be aware of how to manage and troubleshoot the exact equipment you have installed with the exact configuration.

Ongoing Costs

In addition to the initial implementation costs shown in the chart on page 13, wireless technology—like any new technology—involves ongoing costs that need to be factored into your budget. They include:

SUPPORT STAFF

Cost estimates need to include the human resources necessary to implement and manage the WLAN. As we have already addressed, the human resource demands related to managing wireless traffic, dealing with passwords and security issues, scheduling and maintaining wireless carts, and generally troubleshooting the new technology can be significant.

ONGOING TECHNICAL TRAINING

After the initial installation of a wireless network, technology coordinators and local support staff are likely to need additional training in areas such as:

- Emerging standards and specifications
- Network security risks, vulnerabilities and strategies for remediation
- LAN management and network monitoring software
- Bandwidth requirements of applications running on the wireless LAN

PROFESSIONAL DEVELOPMENT

Other than offering an initial introduction, the schools surveyed for this report did not find a great need to instruct their teachers in the technological details of wireless; when everything was working, they found the new technology quite seamless and intuitive. However, many of the education leaders we spoke with did say that the increasing use of wireless and mobile technologies was translating

into a need to offer professional development sessions on new applications and management techniques. While this shift in a school's professional development needs is hard to quantify—and might replace or complement rather than be offered in addition to other professional development sessions—it is worth considering as a possible cost.

MAINTENANCE

For maintenance issues that cannot be resolved in-house, some districts purchase a service contract from an outside vendor. These are typically "time and materials" contracts and cost between $100 to $175 per hour. Most vendors will discount rates when you purchase blocks of time.

UPGRADES AND EXPANSION

With wireless standards still in flux, the physical life of a product might be longer than its useful life. Whenever possible, purchase licenses for firmware and software upgrades. Phasing in wireless LANs with an eye to expanding and upgrading each year is a wise approach. Even with the best of planning, you can anticipate that you will discover gaps in coverage so budget for some additional access points to be added as the network is brought online.

ELECTRICAL

Both the access devices and the wireless computing devices have electrical needs. Laptop batteries typically need to be recharged every two hours and replaced after about two years. A number of schools are discovering that wireless cards drain battery power more quickly than expected, resulting in higher electrical/consumable costs.

THEFT PREVENTION

As laptop programs become more widespread, many schools worry about loss and theft. With wireless networks catching on at home, some sites report that students have stolen access points within their reach. Additional costs may include replacement for access points and extra physical security to lock down units.

UNANTICIPATED COSTS

While it is impossible to predict what they will be, you can assume that some surprise costs may arise from the implementation of wireless LANs. One district had worker's compensation claims from injuries associated with pushing the heavy carts; they addressed working conditions by locating carts closer to the classrooms where they are used and installing larger wheels on the carts. Other districts have reported a need to replace cordless phones and other devices that interfered with the wireless LAN's connection.

Wired vs Wireless: Which Costs More?

As one gets a handle on the total cost of ownership for WLANs, it is easier to address an important question that many technology planners are asking: How do the costs of a wireless solution compare to what you would be spending if you expanded your wired network? The answer will vary, depending on the site and the reasons for going wireless, but here are the major factors involved:

- **Wiring Costs:** Studies have shown that a wireless installation, as compared to running wire to network or add telephones within an existing structure, can be as little 1/6 the price. Especially

in older buildings, hard-to-reach places, or districts with rapidly-expanding needs, mobile wireless solutions can save a considerable amount of money.

- **Space Resources:** A significant space savings is reported by schools using mobile, wireless labs and laptop computers in place of dedicated hard-wired computer labs; in such settings, the more efficient sharing of computers and the decreased need to dedicate valuable space to fixed computer labs can reduce costs considerably. Karl Yeutter of the Kearney Public Schools in Nebraska explains that, "We haven't estimated the value of freed-up room space but we know that it is substantial in terms of cost per square foot of new construction."
- **Price of Computers:** On the other side of equation, the increasing use of wireless laptops for mobile computing can result in higher costs since, on average, laptops cost approximately 30 percent more than comparable desktop models. Laptop computers also tend to have a shorter life span and higher total cost of ownership than desktop PCs due to such factors as limited battery life. In the case of mobile labs, on-task time can be compromised by the need to distribute, power-up, power-down and collect shared laptops each time they are used. Not all wireless implementations rely on laptops, of course, but for the many districts that are embracing wireless networking to support one-to-one laptop programs or mobile labs, these extra hardware costs must be factored in.
- **Indirect Costs:** Reliability issues and support needs must also be factored into the equation. In settings where slower wireless connectivity causes less efficient use of the network or the wireless network requires excessive maintenance and upgrades, these costs have to be weighed against the convenience of easy, 24-hour network access for the mobile user.

On average, districts seem to be finding that wireless and wired networking are fairly comparable in price, which means the implementation decisions come down to goals and needs. As Dennis McIntyre of Westside Community Schools in Nebraska puts it, "There isn't an easy way to compare the costs of wireless to a similar wired solution. Wireless implementation brings a whole different set of user opportunities that would not even be possible in a wired solution."

Wireless LANs have become common in schools because they offer flexibility and mobility. They reduce the need to move and add network ports to accommodate the changing needs of a classroom or school. They reduce the clutter of cables in a classroom filled with computers. They allow students, teachers and administrators to learn, communicate and work electronically anywhere on a school campus. At the same time, security concerns, speed and interference problems, the high cost of mobile computers, and wireless management requirements all bring with them new challenges. Nevertheless, as standards develop and product prices continue to drop, wireless technology promises to shake off its growing pains and earn ever-greater respect as a flexible and powerful tool for learning and management.

RESOURCES FOR LEARNING MORE ABOUT WLANs

ORGANIZATIONS

IEEE Standards Association
standards.ieee.org
The IEEE (Eye-triple-E) site that keeps visitors informed about the progress of international standards' committees including those focusing on 802.11 standards

Wireless LAN Association
www.wlana.org
Trade association for WLAN industry offering updates on applications, standards, cost analyses and trends.

Wi-Fi Alliance
www.wifi.org
The official site of the Wi-Fi alliance with Q&A documents and information on Wi-Fi certified products.

ARTICLES AND PUBLICATIONS

Wireless Technology in Education: Moving from Pilots to Mainstream, 2002
www.peakgroup.net/wte.html
The Peak Group's extensive research report on educational uses of wireless networking, available in an education version that is free of charge.

The Wireless Networking Starter Kit
wireless-starter-kit.com
You can buy this practical book, published in late 2002 (with updates downloadable from the site) or view an excerpt, table of contents or index.

Cutting the Cord: Wireless Computing Comes of Age
www.cosn.org/initiatives/compendium.html
One of eight articles in the 2003 CoSN Compendium, published by the Consortium for School Networking.

eSchool News Special Report
www.eschoolnews.com/resources/reports/WirelessSpec403
A 2003 special report, sponsored by Gateway, on wireless networking in education.

Is Wireless Worth It?
www.techlearning.com/content/about/archives/volume23/may.html
Several related articles on wireless networking for K-12 schools from the May 2003 issue of *Technology & Learning* magazine.

The Wi-Fi Revolution
www.wired.com/wired/archive/11.05/unwired
A special report from *Wired* magazine on the wireless Internet.

Rethinking Wireless
www.universitybusiness.com/page.cfm?id=226
An April 2003 article from *University Business* magazine on the challenges of wireless networking on campus.

Some Schools Opt to Go Wireless
www.educationworld.com/a_admin/admin265.shtml
An April 2002 article on using wireless telephones in K-12 schools.

OTHER ONLINE RESOURCES

Wi-Fi Planet
www.wi-fiplanet.com
Formerly 802.11 planet, this is a general resource for information on wireless networking and standards.

Gartner, Inc.
www.gartner.com
Articles can be purchased from Gartner on a variety of technology topics including wireless security, TCO for K-12 education and other wireless technologies

NetworkWorldFusion
www.nwfusion.com/topics/wireless.html
Menu to a number of news articles from *Network World Magazine* and the NetworkWorldFusion Web site

Technological Insight
www.alliedtelesyn.com/allied/marketing/wireless/technological.htm
Helpful information about wireless security and standards

HP Wireless
www.hp.com/sbso/productivity/howto/wireless_lan/index.html
You can start with this "how to" on setting up wireless LANs or follow links to other HP articles on Wi-Fi

Mobile & Wireless Knowledge Center
www.computerworld.com/mobiletopics/mobile
Glossaries, news, explanatory articles and special reports on topics such as wireless hacking.

Palowireless
www.palowireless.com/i802_11
Palowireless' 802.11 Resource Center page, geared to wireless networking professionals, with links to news, forums, glossaries, tutorials and more.

Wireless ITtoolbox
wireless.ittoolbox.com
Industry news briefs, whitepapers, discussion groups and a variety of other technical resources related to wireless technology.

3Com
www.3com.com
The main menu points you to case studies and technical papers on topics such as 802.11 standards, VPNs and wireless security.

Cisco
www.cisco.com
You can search for background info and a wireless glossary in addition to information on Cisco wireless products.

Intel
www.intel.com/ebusiness/strategies/wireless/index.htm
An index page linking to a number of Intel's wireless articles that include definitions, implementation advice, and LAN security

Dell
www.dell.com/us/en/bsd/topics/segtopic_5_lma_truemobile.htm
Dell's Wireless Solutions page with links to glossaries, wireless FAQS, white papers, and product info.

Apple
www.apple.com/education/mobilecomputing
Case studies, product information and research about Apple Airport solutions.

SpectraLink
www.spectralink.com/solutions/education.html
Case studies, white papers, and product information on SpectraLink's wireless telephones in education environments.

Sun Microsystems
http://www.sun.com/mobility/enterprise/working_with_sun.html
including White Papers.
Additional information:
http://wwws.sun.com/software/solutions/mobility/index.html
Listing of resources around JAVA and J2EE in building wireless:
http://wireless.java.sun.com/enterprise/index.html
Classes on wireless
http://training.sun.com/US/catalog/wirelesstelco.html

MOREnet
www.more.net/technical/research/wireless/index.html

An online article, in the Technical Support section of Missouri's MOREnet Web site, focusing on the history, applications and challenges of going wireless.

APPENDIX: AT-A-GLANCE PROFILES OF 8 WIRELESS SITES

Kearney Public Schools, NE

Information Provided by: Karl Yeutter, IT Director *(kyeutter@kearneypublic.org)*

District Info: Located in central Nebraska, Kearney Public Schools comprises 12 schools with approximately 4,620 students and a rapidly-growing population.

Uses of Wireless: As one of the fastest growing communities in Nebraska, Kearney is committed to expanding its technology program while addressing space constraints. Using mobile wireless labs (with laptops on carts) in place of conventional hard-wired labs serves two purposes: it saves the district valuable space and allows the computers to be brought into classes such as shop or science where the need to access special equipment prevents teachers from taking their students off to the computer lab. As part of a pilot project, every teacher in Kearney's high school is receiving a wireless laptop for accessing the district's new PowerSchool management system as well as constructing lessons and teaching in wireless labs. School and district administrators also use laptop computers with wireless capabilities, allowing them the mobility needed to carry their computers with them when moving around campus (doing teacher evaluations, for example) or leaving their office for meetings at the central administration office. Some administrators use voice activation software built into Windows XP or from a 3rd party program such as IBM ViaVoice to dictate notes into their laptops.

Wireless Products:

-Students and teachers use Apple laptops with built in wireless

-Administrators use Gateway laptops with Belkin wireless cards

-Apple Airport access points are used with both the Apples and PCs

-RadioLan and Tsunami (Proxim) wide-area wireless solutions are being used to connect a number of campuses

Additional Information:

-The wireless programs are being phased in gradually. At first Kearney set up one access point for each mobile lab. Since then they have been tracking mobile lab usage data in order to create "hot zones" of roaming wireless coverage in areas that see the greatest mobile lab usage. The high school was selected as the pilot site for the teacher laptop project because it is a single building but the plan is to roll out to other schools later.

-There have been some problems with battery failures on the laptops.

-The district has found little need for training in the use of the pre-configured wireless computers but has had to develop guidelines to help teachers teach in wireless notebook labs. The challenges are different (e.g., protecting the machines, setting up the lab rather than having the lab set up when they arrive) than those in a wired lab. Media specialists or LAN managers have been able to handle the "checking out" of the labs to the teachers.

- To prevent theft, they have designed their own security carts and created a secure long-term storage area for cabinets when they are not in use. They have had no loss of wireless notebooks in the first year while, during the same time period, two desktops were stolen.

-Kearney has a state-of-the-art sports facilities and a nationally-known track team. They are looking into extending wireless access to the field to avoid the need for the messy Ethernet lines now used by a new digital photo finish system (for determining the winner of close races) established with help from the local university.

-"We haven't estimated the value of freed-up room space due to not needing wired labs," Yeutter says, "but we guess that it is substantial in terms of cost per square foot of new construction." On the other hand, he points out, notebook computers are more expensive, not only to buy but to support (in terms of batteries, upgrades, maintenance, and so on). Apple Airport was selected because it was reasonably priced. However, Yeutter is concerned that it has a shorter range than some of its competitors. "When you factor in the possibility of having to purchase more Airports vs fewer of another brand," he says, "the money is sometimes is in favor of Airport's competitors."

Clarke County School District, GA

Information Provided by: Dr. Ginger Jewell, Coordinator of Educational Technology *(jewellg@clarke.k12.ga.us)*

District Info: Small but densely populated, this metropolitan county serves 11,312 students K-12. The population is diverse with 27% below the poverty level but an overall per capita income that is above average for the state.

Uses of Wireless: One of the district's schools (Hilsman Middle) is part of a state pilot of eight middle schools chosen because of poor test scores and high poverty. Now in its second year, the pilot focuses on increased student achievement through the use of technology-integrated rich curriculum. More than 750 laptops with wireless access have been issued to the Hilsman students for one-to-one use. Each student is also provided Internet access at home. Wireless has been installed in all the other Clarke County schools with at least one mobile computer lab (with 22-26 laptops and a cart) per school and plans to expand as money permits. All teachers and administrators in the district have wireless laptops, although Jewell feels strongly that anything requiring access to sensitive data must continue to be handled through hard wired connections. Wireless technology is also used to connect desktop models in portable classrooms, where hard-wiring doesn't make sense.

Wireless Products:
-Gateway laptops (at grant school) and Compaq laptop (at other schools)

-Enterasis wireless is used with Gateway computers and Cisco with the others

-Compaq desktops with Microsft USB adapters are used for wireless connectivity in portables.

Additional Information:
-Professional development is emphasized—with 10 hours of a 50 hour required course focusing on wireless. The emphasis is not on hardware but on classroom management, utilizing management software and using wireless-enabled technology tools such as Discourse. "This is a huge issue," Jewell says, "and absolutely critical to appropriate use."

-Jewell reports that the wireless technology pushes the envelope with the large number of individual student logins and email accounts that can cause technical glitches. "It eats human resources as support is required to a much broader audience with highly different needs and uses."

-Clarke County is considering moving to 802.11g in future implementations but they are waiting for it to mature and be more universally acceptable. With cards needing to be replaced in order to carry 802.11g, the expense wouldn't be worth the gain on older equipment so this will be limited to future purchases.

-The move to laptops has increased the cost per PC by almost 30%. On the other hand the access points are cheaper to put in than additional cable drops and the district is finding the mobile labs "much more effective than standalone labs as teaching tools." Jewell anticipates the wireless trend continuing, with 1:1 computing the norm in a few years and "wireless clouds" covering large areas, making home access a non-issue.

Amarillo Independent School District, TX

Information Provided by: Gary L. Allen, Executive Director, Office of Technology *(gary.allen@amaisd.org)*

District info: This urban school district has 30,000 students, and a campus that is 60% Title 1.

Uses of Wireless: A variety of wireless solutions have been implemented including wireless carts with mobile access points, plugged into the classroom's wired LAN port when in use, and campus-wide roaming using wireless access points installed at the ceiling. The district also uses wireless for point-to-point (wide area) connectivity between the administration building and a support office and is extending the network via a wireless broadcast to remote buildings on a campus location (portable or gym).

Wireless Products:
-Apple Laptops with built-in wireless

-Dell Laptops (some built in and some with wireless cards)

-Cisco wireless access devices (some mobile on carts and some permanently mounted)

Additional Information
Amarillo ISD also uses Compaq Ipaq Pocket PCs with wireless connectivity.

Cache County School District, UT

Information Provided by: Stephen W. Zsiray, Jr., Associate Superintendent for Curriculum and Instructional Services *(steve.zsiray@cache.k12.ut.us)*

District Info: A rural school district, located in an agricultural valley in northern Utah, Cache County has 21 schools and 13,044 students, with 27% receiving free or reduced lunch and 10% qualifying for Title 1.

Uses of Wireless: Initial uses have focused primarily on technology training for teachers. To allow training at different sites with minimal set-up and start-up time, the district established a mobile lab of laptop computers. Stored in containers with wheels and a handle, the lab can be packed into a van and moved to any school site or to the district office—all of which are set up with

wireless connections. At the high schools, wireless computers are being used in a business lab and by the math department—for instruction, grading and attendance and teacher presentations. The intent is to experiment with the efficacy of the current wireless implementations and expand delivery to more students in coming years.

Wireless Products:
-Toshiba, Gateway and Apple laptops

-Windows laptops have Ornico wireless cards

-Apple Airport access points (used for Macs and PCs)

-Breezecom WAN products for external wireless

Additional Information:
-Staffing involves one trainer, one technician, and one director for mobile training lab and one technician (working with teachers) at each of the high schools wireless labs.

-There have been no difficulties mixing Windows PCs and the Apple Airport network, although the overall implementation has involved lots of troubleshooting.

- With cost a big consideration, Zsiray says that upgrading to faster wireless (802.11a or 802.11g) does not yet warrant the expense. Overall, it is not clear whether wireless is saving the district money but it offers new flexibility and opportunities.

- Zsiray credits pioneering teachers, skilled technicians and a helpful statewide network (the Utah Education Nework or UEN) with making the pilot a success.

Hampton City Schools, VA

Information Provided by: Georgianna Skinner, Coordinator of Technology. *(gskinner@sbo.hampton.k12.va.us)*

District Info: This is an urban district with 22,000 students, 35 schools, a large Title 1 population and eligibility for a 57% E-rate discount.

Uses of Wireless: Wireless laptops are being used to supplement the wired networking in all of Hampton's County's schools. "Instead of teachers taking their students to a lab, the lab comes to them." In addition, student laptop pilot projects are taking place in three schools. The entire faculty at three middle schools—along with select groups of students—are using wireless laptops throughout the day. At two high schools a wireless laptop program has been implemented with 9th grade students who are at risk of not passing state standards for graduation. In addition, any faculty member who works in more than one building is given a laptop to use instead of a desktop. As part of the laptop pilots, the district is working with Glencoe-McGraw/Hill to provide on-line textbooks and resources. Hampton County has long placed a heavy emphasis on technology, with close to a 3:1 student-to-computer ratio and teachers required to demonstrate technology proficiency in a number of ways. Professional development in the instructional uses of wireless labs is now part of the program.

Wireless Products:
- Apple iBook laptops

- Apple Airport access points

- All schools are set up for wireless access and all laptops have wireless capabilities.

Additional Information:
-The motto, according to Georgiana Skinner, is "more with less." The district has its own repair shop, network crew and telephone support staff . They believe in training people on site and pride themselves on supporting and rewarding technical staff for the work they do.

-Hampton City Schools have standardized on Apple OS because they believe it is easier to maintain, with on-site instructional staff/librarians able to do much of the troubleshooting.

-Skinner credits a supportive superintendent and school board for allowing them to try different approaches without a fear of making mistakes.

-They are exploring "point to point" wide area wireless with a pilot this fall.

-A grant from 3Com has allowed the district to add two new schools to the wireless program this year.

- In unusual circumstances a desktop model might be set up for wireless access but Skinner reports that it's generally been more efficient to hardwire the desktops.

Poway Unified School District, CA

Information Provided by: Tracy Jones, Data Systems Supervisor *(tjones@sdcoe.k12.ca.us)*

District Info: Situated in suburban San Diego and throughout the city of Poway, PUSD operates 31 schools and serves 32,456 students

Uses of Wireless: Wireless laptops on carts are used by teachers in several schools, allowing for instant labs and making it possible for computing to happen at student desks rather than at tables lined up against the wall. Every

room has wired connections for high speed needs and for plugging in the mobile access points. Laptops are used as workstations for all the teachers in a new high school and for various functions such as P.E. Overall, Jones reports that the wireless computers give the teachers more flexibility and save the district money.

Wireless Products:
-Gateway laptops (60%)—with additional laptops being purchased from Gateway along with mobile lab carts

-Apple laptops (20%)

-Additional PC laptops from IBM, Toshiba and Earthwalk (20%)

-Cisco access points for PCs

Additional Information:
-They are looking into adopting 802.11g for increased speed. (802.11a was under consideration for a while but the newer standard seems to have won out.)

-Security is a concern. Two staff members attended a wireless security school. Although the school would like students to be able to bring laptops to and from schools, they do not want to leave access on all night. (Right now they use timers to turn the access points off and on.)

-Jones emphasizes the importance of developing an implementation plan and offering training for everybody.

-Future plans involve using wireless carts for on-site staff training instead of having staff members travel to an available computer lab.

Henry County Public Schools, VA

Information Provided by: Janet Copenhaver, Director of Technology *(janet@henry.k12.va.us)*

District Info: Henry County Public Schools is a rural school division with 8,600 students. Ten of the 12 elementary schools are full Title I schools.

Uses of Wireless: Henry County has one of the highest unemployment rates in the state, having lost more than 9000 jobs in recent years due to off-shore moves. County government and school officials have come together to respond to the crisis with the best technological education possible. With a goal of providing flexible and "anywhere, anytime" learning, laptop programs have been implemented in all four middle and all four high schools. Classroom sets of wireless computers can be checked out by teachers and taken to their rooms to form an instant lab. This has been particularly helpful in older schools where it was impossible to add more computers labs; instead they decided to "take down the walls" and go wireless. All teachers in the middle and high schools have a wireless laptop as well as access to the wireless carts. In addition, a number of wireless desktop labs are in use—including middle-school keyboarding and vocational labs, elementary grade instructional labs with older Macs and administrative offices with multiple computers.

Wireless Products:
-Middle schools use Apple laptops with Airport wireless

-High schools use Gateway and MetroBook laptops with Lucent wireless access points

-Macintosh and Gateway desktop models at several schools are equipped with wireless network access.

Additional Information:
-Henry County Public Schools recently received a Rural Urgent Technology Grant of almost $500,000 to install a wireless wide area network using Tsunami radio equipment. Each school now has a direct line of site to one of seven towers which transmit from 35Mbps to 45Mbps with a 100MBPS backbone from the central office.

-The wireless network is also used at night for adult education to try to retrain the work force. There is a strong commitment to educate the population in the best technological environment possible.

Westside Community Schools, NE

Information Provided by: Dennis McIntyre, Director, Instructional Technology/Media *(dmcintyre@westside66.org)*

District Info: Westside is an independent school district in metropolitan Omaha serving 5,800 students with 13 schools PK-12.

Uses of Wireless: The first implementation of wireless in the district involved the high school, a recently renovated facility that uses a modular schedule with a mix of large groups, small groups, labs, and independent study. In the summer of 2000 the district committed to the PowerSchool web-based student information system to allow "just in time" information on student progress. The entire building was set up for wireless access, using 30 access points, and the high school teachers were issued laptops so they could input or report information on any student from anywhere in the building, as well as accessing files for instructional purposes. With the high school program serving as a model, a similar implementation followed at the middle school. Wireless lab carts are now being added to all of the elementary

buildings. In several of the locations, the carts will take the place of a desktop lab, saving space for other classroom demands resulting from increased enrollment due to a state choice (optional enrollment) program. Wireless is also being used to connect desktop models in portable classrooms and in math/computer science labs where wireless cards give teachers the flexibility to rearrange the room configuration for "people and instruction" needs rather than LAN outlets.

Wireless Products:

-Apple laptops and desktops

-Apple Airport hubs and access points

-Avaya hubs installed at a few "critical mass" locations

Additional Information:

-Most work has been done by internal staff—district and building– with some consultation support from Apple Engineers. The people involved in the installation and maintenance include a district network manager and a building technology coordinator for each of the secondary sites. Wireless implementations at the elementary level are overseen by the district network manager and are supported by an additional team of two technicians. Site surveys have all been done by internal staff.

- With technology a high priority, the district continues to look at potential applications that would allow staff and students to readily exchange files, interact, or collaborate. They are also exploring the potential of 802.11g, available in the Apple Airport Extreme Base Stations, but a major concern is the limited range of 802.11g. Every effort is being made to keep the infrastructure fully compatible and to reduce any variations that may complicate service or maintenance of the infrastructure.

-McIntyre reports that the Airport wireless system is transparent (and becoming more so with new implementations). Very little "separate" training has been necessary for staff members to be able to use the wireless laptops and carts. Any problems have been worked out by creating "location manager" settings on the machines.

-Security has not been a major issue to this point with no serious incidents that have raised levels of concern. The newest technical challenges have occurred as the students acquire their own personal wireless-capable laptops. New policies and procedures are being developed for managing the growing numbers of non- agency devices connecting to the network, with a goal of allowing these connections while maintaining reasonable security. There have also been some issues with the interactions of the wireless system and the overall infrastructure, which have created slow downs or crashes in the network system.

-In terms of TCO, McIntyre says the biggest surprises have been the "implementation mindset change" requiring significant professional and curriculum development in order to adapt to such things as the instructional use of the lab carts in the elementary sites.

About CoSN

MISSION CoSN's mission is to advance the K-12 education community's capacity to effectively use technology to improve learning through advocacy, policy and leadership development.

AUDIENCE Key technology leaders at the school district, state and national level.

GOALS

1. Leadership Development: CoSN engages in programs and activities that build effective leadership capacity of technology decision-makers at the national, state and local levels to ensure technology has a positive effect on learning.

2. Advocacy: CoSN maintains a strong and effective voice for national policy and implementation of technology use in education to serve all students.

3. Coalition Building: CoSN builds contexts for private and public sector interaction and foster partnerships to shape the future of technology use to improve access, equity and professional development.

4. Emerging Technology: CoSN provides a place and the means to track emerging technologies and develop insights and tools to use technology to address core educational challenges.

Further information about membership in CoSN is available at www.cosn.org.

MAJOR COSN INITIATIVES

Annual K-12 School Networking Conference, the premier national technology leadership conference.

CoSN's School District Chief Technology Officers (CTO) Council, professional development for district-level technology directors (CTOs).

Internet & Education Web Telecasts, 60-minute interactive professional development focusing on key issues.

Data-Driven Decision Making: Vision to Know and Do, an initiative to help educators use data effectively.

Taking Total Cost of Ownership (TCO) to the Classroom, a resource to provide school leaders with the tools to budget for technology.

Safeguarding the Wired Schoolhouse, guidance for school leaders on options for Internet safety in schools.

CoSN Compendium, a series of eight monographs exploring timely issues of importance to K-12 technology decision-makers.

Cyber Security for the Digital District, an initiative designed to provide education technology leaders and policy-makers with strategies and tools they can use to ensure the privacy of data and the safe operation of technology within their school systems.

SPONSORS

Editorial Projects In Education
Publisher of EDUCATION WEEK

PLATO LEARNING™

SpectraLink Wireless@work

Consortium for School Networking
1710 Rhode Island Ave., NW Suite 900
Washington, DC 20036-3007
www.cosn.org
November 2003