DOCUMENT RESUME

ED 468 621 EF 006 210

AUTHOR	Nair, Prakash
TITLE	The Role of Wireless Computing Technology in the Design of Schools.
INSTITUTION	National Clearinghouse for Educational Facilities, Washington, DC.
SPONS AGENCY	Office of Educational Research and Improvement (ED), Washington, DC.
PUB DATE	2002-10-00
NOTE	14p.
AVAILABLE FROM	National Clearinghouse for Educational Facilities, 1090 Vermont Ave., N.W., Suite 700, Washington, DC 20005-4905. Tel: 888-552-0624 (Toll Free). For full text: http://www.edfacilities.org/ pubs.
PUB TYPE	Reports - Descriptive (141)
EDRS PRICE	EDRS Price MF01/PC01 Plus Postage.
DESCRIPTORS	Computer Security; *Computer Uses in Education; Costs; Educational Facilities Design; Elementary Secondary Education; Local Area Networks; Standards; Technology Integration
IDENTIFIERS	Bandwidth; Laptop Computers; Network Protocols; *Wireless Technology

ABSTRACT

This document discusses integrating computers logically and affordably into a school building's infrastructure through the use of wireless technology. It begins by discussing why wireless networks using mobile computers are preferable to desktop machines in each classoom. It then explains the features of a wireless local area network (WLAN) and its common standards. The next section provides an update on advances, developments, and concerns in seven key areas: bandwidth, interference, system design and layout, security, network administration, occupant health, and vandalism. The documents then addresses the impact of WLANs on learning and on the future of school design, and issues of costs and equitable access. Appendices contain a comparison of wireless standards, a discussion of Bluetooth and 3G, and information on one-to-one computing. (Contains 12 references and a glossary of terms.) (EV)

The Role of Wireless Computing Technology in the Design of Schools

Prakash Nair, RA

October 2002

The National Clearinghouse for Educational Facilities

Full text available at:

http://www.edfacilities.org/pubs

The Role of Wireless Computing Technology in the Design of Schools

National Clearinghouse for Educational Facilities

Prakash Nair, RA
October 2002

Quinns Beach Primary School in Western Australia is a simple, unassuming campus. Room designs maximize opportunities for students to mix and collaborate. Spaces connect directly to outdoor learning and play areas that are usable throughout the year. Students of various ages work on projects in groups, creating a quiet buzz of activity. It is common to see older students mentoring younger ones. Teachers move around to the students and groups rather than being rooted to a lecturing spot.

Wireless laptops are a mainstay in this school, letting students compute from nearly anywhere inside or outside the building. To support their project work, students often access the Internet. They can print their work wirelessly on one of several high-speed printers located throughout the small campus. Electrical outlets are plentiful for times when laptop batteries grow weak. Students with a need to move large files or use applications that move large amounts of data across the network, such as video editing or CAD (computer-aided design), can access desktop computers hardwired to the school's local area network (LAN). These desktop computers constitute about thirty percent of the school's computers.

In this school, technology compliments the idea that learning is something personal that cannot be mass-produced, and that computers help students build the confidence, curiosity, autonomy, and skill to pave their own unique learning paths. Information technology—which reflects and supports an economy based on knowledge and requires workers skillful in using "knowledge tools"—is an integral part of this learning environment. Best of all for the school's administrators and the community, the Quinns Beach technology design was affordable enough to become reality.

Quinns Beach and schools in the United States, such as Rye Country Day School in Rye, New York, exemplify an approach being taken by many school districts to integrate computers logically and affordably into a school building's infrastructure. With laptops and other smaller devices quickly overtaking desktop computers in popularity, wireless networking's promise to provide ubiquitous computing anywhere, anytime for these portable devices is hard to ignore.

Why Wireless Computing?

The local area networks that bring computers alive in school buildings by providing connectivity between users and the Internet are sprouting wireless segments at an increasing rate, and for good reasons. Foremost among these are the freedom and simplicity of working without wires. In older school facilities or portable classrooms, wireless offers a quick way—sometimes the only practical way—to get students computing.

Author and educator Jamie McKenzie summarizes in the journal *From Now On* why wireless networks utilizing mobile computers are preferable to the still-prevalent practice of putting desktop machines in each classroom (McKenzie 2001):

Ease of movement. Untethered laptops can be moved anywhere in the building and require no special furniture.

Relaxed fit. Laptops are easier to accommodate within existing classrooms because of their small size.

Strategic deployment. Laptop computers can be deployed on rolling carts where they are needed most, creating one-to-one learning opportunities that traditional methods of placing hardwired computers throughout a school do not provide.

Flexibility. Laptops can be used within existing rooms and can be configured to fit the teacher's preference and the nature of the learning experience, whether it is team, group, or individual. Wireless laptops place no additional demands on furniture or space.

Cleanliness. Elimination of cables and wires means that twenty-five or even thirty laptops can be accommodated in a room without creating clutter.

Low profile. Unlike desktops, behind whose large monitors students may be hidden, laptops have low profiles and allow teachers and students to make important eye contact.

Convenience. Wireless laptops' ability to be readily available when needed and easily stowed when not makes them more likely to be used. There is almost no setup time for wireless laptops. They can be up and running without students needing to find and connect or disconnect a wire (as would be required for hardwired network access) and without students needing to move to a fixed computer workstation. This is a huge advantage and another way in which the technology itself becomes subordinate to the task of learning.

Simplicity. The simplicity, comfort, and reliability of wireless laptops means that teachers and students can focus on learning, not on hardware. This helps technology attain the use that has been hoped for but not often realized because of technical difficulties or inconvenience.

What Is a WLAN?

A wireless local area network (WLAN) is actually nothing more than an invisible extension of the visible hardwired network most schools already have. The wireless links in a wireless network are made possible by two key sets of components: access points and wireless network adapters. Access points are radio transceivers operating on one or more frequencies and acting like satellites to send, receive, and manage information from all the computers and devices in the network. Wireless network adapters are radio transceivers housed within each computer that establish communications with the access points. Signals from an access point can travel roughly 800 feet outdoors and considerably further with add-on antennas. Their efficacy indoors varies depending on obstructions, the number of users, and the industry standard they are based on.

Standards Shape Performance

WLAN performance has been shaped by a family of standards under the 802.11 designation developed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE). Interoperability between products is verified by the Wireless Ethernet Compatibility Alliance, which grants the use of its Wi-Fi (wireless fidelity) logo to products that pass its tests. The IEEE 802.11b standard, a mainstay of WLAN development since 1999, and the soon-to-be-ratified 802.11g standard (see Appendix One for a comparative analysis), permit access points to transmit over one of three specific channels or frequencies. This means that, within a given zone, up to three access points can be installed, each transmitting on a different channel, with the wireless network adapters inside computers constantly sampling the three channels and locking onto the one offering the best performance. With the IEEE 802.11a standard, which offers advanced capabilities over the 802.11b standard (despite its "a" designation), access points can be set to operate on one of eight discreet channels, with up to eight access points deployed in a coverage area or zone, such as an auditorium, where many users might be accessing the network. This is important because, as with wired networks, the bandwidth available in a given area is shared—that is, the more users "drawing" from a specific access point in a given area, the slower the wireless connection. Adding additional access points to a given area increases the bandwidth available and the performance for users.

Wireless Evolution in Schools

Wireless computing's potential to revolutionize technology access in schools became evident soon after the first edition of IEEE 802.11 was published in 1997. Writing for *Schoolhouse Journal* about the technology's potential, architect and facilities planner Ed Kirkbride noted, "Wireless laptop computers reduce the need for and costs of technology cabling and additional electrical power and wiring, and they reduce the disturbance to existing construction as well as the environmental hazards and costs for remediation of asbestos and lead paint" (Kirkbride 1999). Wireless technology enables every school, new or old, to provide networked computing.

Despite its promise, the early adoption of wireless networking was not widespread. Concerns included high costs, bandwidth, interference, security, safety, reliability, and longevity. This next section provides an update of advances, developments, and concerns in seven key wireless areas:

Bandwidth. As discovered by the millions of home users who have migrated from 56 kb/s modems to broadband DSL or cable connections, higher bandwidth means less waiting while your computer accesses information from somewhere else.

When wireless networking was first introduced into schools, the 1 or 2 Mb/s data transmission rate that the first iteration of the IEEE 802.11 standard offered was a limiting factor. The available bandwidth of an access point, analogous to water in a pipe, could be diluted beyond ideal quantities, particularly when users simultaneously browsed websites, opened large files, or worked with multimedia applications. That problem was lessened with the IEEE 802.11b standard, which delivered about 7 Mb/s of a promised 11 Mb/s transmission rate to a single user. Remember that this is shared bandwidth; the more users that are connected and actively using the system, the less bandwidth available to each user.

According to Charles Bartel, director of computing services at Carnegie Mellon University and a pioneer of campus-wide wireless implementations, the typical user seems to be satisfied with a network speed of about 1.5 Mb/s, which is about the speed offered by a T1 line. Bartel believes that this speed can be achieved with about one wireless access point per classroom using a network based on the 802.11b technology (CMU.edu 2000). The adequacy of this speed is predicated upon the kind of staggered access that enables workers in large offices to share a single T1 line without experiencing bandwidth logjams—because users are performing different tasks at different times. In schools, bandwidth logjams with wireless systems can similarly be mitigated when computers are used in conjunction with individualized instruction, where students perform different tasks at different times and rarely access large files simultaneously from the school network or Internet. Even with staggered access, Quinns Beach and other schools with the 802.11b technology have discovered that higher bandwidth activities like transmitting large files and viewing full-motion video from a DVD player can overtax their systems. Newer standards, such as the 54 Mb/s system created by the IEEE 802.11a and draft 802.11g standards, are helping to meet demand for increased bandwidth.

From a technological standpoint, wireless networks won't likely supplant the speed advantage of wired Ethernet networks; moreover, high-performance desktop computers operating on wired networks for specialized applications such as CAD and video editing still will be needed. But more and more applications in schools can and will happen wirelessly, and wireless networks will flourish, particularly hybrid systems that utilize wired backbones offering a mixture of wired and wireless segments.

Interference. With wireless products crowding the 2.4 GHz frequency on which they operate, WLAN technologies operating under the IEEE 802.11b and draft 802.11g standards will have to cope with interference. Wireless signals will not penetrate through metals and other materials that reflect or absorb them, such as objects with a high water content. Even people can affect transmission rates. According to Howard Strauss, technology coordinator for the Corporation for Research and Educational Networking (CREN) Tech Talk series, "To a microwave oven, cordless phone or wireless LAN, you are very close to being just a five- or six-foot mobile column of water, absorbing radiation that was intended for cooking or communication" (CREN.net 2000). The net effect of interference is not that data is lost but that the system slows down. Interference can be minimized by the careful siting and installation of access points and, in the case of new construction, the design of the building itself.

System design and layout. To create a wireless-friendly building or campus requires collaboration between WLAN designers and architects early in the planning and design process. The number of wireless devices greatly affects system design, layout, and cost, with larger systems presenting many more challenges. "The best approach," Bartel (2000) advises,

> is to predetermine spaces that will have a large number of users, such as large group instruction areas and libraries, that could benefit from additional access points. You also must determine the areas, such as offices, that need to have fail-safe service and might better utilize hardwired connections. Budget constraints may dictate that there be areas where a best-effort coverage is acceptable.

Bartel suggests that the best design will come from a site survey that includes deploying access points through an interactive process of sample testing, rough layout testing, mapping the layout on paper with color-coded coverage patterns, then retesting to find the best compromise between coverage and capacity. Testing is done with an RF (radio frequency) test unit during normal hours to include potential "interferers" as part of the testing process. A fully occupied space will test differently than one that is empty or being tested at times other than normal hours. Designing a good WLAN requires a little "art" along with science and often a bit of tweaking after the initial installation to get optimum results.

Access points must be carefully located so that users who go beyond the range of one access point will be switched automatically to the next without encountering dead zones where signals are too weak. Dead zones can also occur because of the presence of metals or competing signals from devices such as microwave ovens, although microwave ovens built to newer specifications no longer pose a problem.

By providing an adequate number of strategically placed access points, a good design can reduce significant bandwidth loss caused by too many people online or by people venturing too far from an access point or getting too close to more than one access point broadcasting on the same channel.

Security. Since wireless signals use radio waves, there is always the danger that unauthorized users can tap into a wireless system more easily than a wired one. But reports of security problems from schools using WLAN technology are not widespread, and today's wireless standards offer greater security than earlier versions.

Present wireless security technology, also called wired equivalent privacy (WEP), offers two levels of encryption: 40 bit and 128 bit, with 128-bit encryption recommended for applications where greater security is needed. The trade-off is that higher encryption levels slow down the system, though not to the point where today's high-speed systems lose significant functionality. The objective of WEP is to provide security similar to wired networks. Of course, wired networks have their own security vulnerabilities. For example, in many schools, it is easy to walk into a public space and connect a laptop to a jack with no questions asked.

Encrypting signals that traverse the wireless link itself is just one of several layers of security that a school may provide for its computer networks. Other appropriate security methods, such as password authentication, firewalls, and virtual private network solutions, can greatly reduce security risks for users and for WLAN-based resources (Nair 2001).

Network administration. Network administrators will find WLAN networks harder to operate, manage, and secure on a daily basis than wired networks because user mobility means that there is less predictability about which parts of the network will be more loaded than others at given times. Jeff Spain, network administrator at Cincinnati Country Day School, notes that one problem he has with wireless is that he cannot apply quality of service controls (QOS) to the wireless access point. QOS in a hardwired network lets users make changes on the fly to optimize performance and get instant feedback from users' computers—something that wireless networks do not yet allow.

Occupant health. Studies about potential WLAN health risks do not find a compelling danger posed by the electromagnetic radiation from WLAN equipment. The Wireless Networking Industry's Information Source summarizes the issue (WLANA 2000), noting:

> The interpretation of more than four decades of research in this area has led to a scientific consensus on the safety of exposure to radio-frequency electromagnetic fields. This consensus is reflected in the recommendations and standards developed by committees such as the National Council on Radiation Protection and Measurements Scientific Committee 53, IEEE Standards Coordinating Committee 28, International Radiation Protection Association/International Non-Ionizing Radiation Committee, and National Radiological Protection Board. Manufacturers of wireless networking products design them to operate within the guidelines of these standards and recommendations and, therefore, [the products] are considered safe.

Technology consultant Keith Lightbody suggests that it is important to consider the level of radiation in the school environment, given that students are in school for about 12,000 hours of their lives. Electromagnetic radiation is emitted by many familiar devices, including computers, cordless phones, microwave ovens, and fax machines. For purposes of comparison, Lightbody provides the following chart that ranks radio emissions from WLAN systems and other devices encountered in daily life:

Radio Emissions Comparison Chart

Wireless access point	30 mW
Mobile (cellular)	600 mW
Mobile (cellular) phone car kit	3,000 mW

(mW = milliwatt, one thousandth of a watt)

In a study conducted at Quinns Beach Primary School and Seven Oaks Senior College, in Perth, Western Australia, Lightbody noted that the wireless networking equipment used in these schools has radiation levels 400 times lower than the limit specified in Australian standards.

Vandalism. With schools' increased expenditures for high-technology equipment and infrastructure, the potential for vandalism requires careful consideration. As aptly reported in *Education Week,* "These days, a single case of vandalism can carry an especially hefty price tag—thanks to increased presence of computers, telecommunications devices, broadcasting and recording equipment, and other expensive technology on school campuses (Bowman 2002)." The extent to which a WLAN system is susceptible to vandalism depends on how it is deployed. The most common type of installation in schools is the rolling cart, where the wireless access point is contained within the cart, and safety depends on how securely the cart is stored after hours. Another typical installation is an add-on system, where wireless transceivers or access points are plugged into existing network connections to extend the reach of the wired network. These add-on systems are vulnerable to vandalism because the access points are often placed in visible locations, as are other devices such as extender antennas, which literally extend the reach and strength of signals to and from an access point. Such devices can be easily detached and stolen, and building owners are beginning to enclose them in protective cages to prevent loss. A third common type of wireless installation is the integrated system, where the wireless infrastructure is installed when the building is constructed—though such an integrated approach is also possible in retrofit situations. In these cases, access points can be hidden from view within ceiling plenums and connected to invisible extender antennas integrated into the ceiling systems. At least one manufacturer (Armstrong Industries) now offers wireless extender antennas disguised to look like ceiling tiles. Under this scheme, no part of the wireless infrastructure is visible to building users.

WLANs offer some advantages that reduce the possibility of vandalism while improving functionality. For example, schools can install brackets that permit the easy installation and removal of data projectors. This is more realistic for projectors that come wireless-ready, because wireless projectors reduce the time and expense of setup and takedown and can be installed anywhere. The improved functionality derives from the fact that students and staff can easily "beam" their signals from untethered laptops to data projectors via the WLAN. This not only speeds up connection time but also means that presenters can be located anywhere in the room and not be hostage to a location dictated by the reach of cables required to connect their laptop to the projector.

Impact of WLANs on Learning

Wireless computing is changing many traditional learning environments because of its reach and convenience. Higher education campuses, the earliest WLAN users, have documented WLAN's effects on student learning and behavior. As noted by Educause (2002), a nonprofit association dedicated to advancing higher education by promoting the intelligent use of information technology,

> Students entering higher education in the next few years may take for granted the idea of a wireless campus—a place [where] they may never have to worry about finding a phone jack or a data line to connect to the school's network. They will have the ability to use their laptops and handheld devices—whether to e-mail a paper, do library research, or participate in a class online discussion—anywhere on campus, without having to worry about physically plugging in their hardware.

Beth Blackwood, principal of the K–12 Presbyterian Ladies College in Perth, Western Australia, says WLAN technology has absolutely changed the way her teachers teach and her students learn:

> Prior to wireless, it was very difficult to access information online. Each classroom was networked, but at best we could only daisy-chain a few laptops at a time from the connection. It is now possible for 600 students to access e-mail and the Internet across the campus. Since wireless networking, there has been a proliferation of teachers designing digital curriculums—using links, the intranet, and the Internet—and seeking to have queries and assignments e-mailed to them.

When asked if students connected to the network or Internet from locations other than their classroom, Blackwood replied,

> The students access the network across the campus. It is not unusual to see the girls using their laptops on the grounds after school while they are waiting to be picked up by their parents. They utilize the laptops in the boardinghouse, at sports for recording trials and scores, and at recess and lunchtimes. None of this was possible before wireless. We have a student who lives directly across the street from the school. I often see her sitting on the sidewalk outside her house with her iBook® on a weekend or early evening—the sidewalk is close enough to access our wireless network.

Educators like Blackwood are seeing the liberating power of the wireless network, understanding how it represents a culture change. As author Terian Tyre notes, "WLAN technology also uniquely enables ad-hoc networks. These may be quickly set up in standalone, peer-to-peer mode, with or without a connection to the school or district LAN. Teacher training, student workgroups, PTA nights, science fairs, and board meetings, to name just a few examples, could all benefit from such on-the-fly connectivity."

WLAN and Future Learning Places

Though some believe WLANs are more an add-on technology than a factor necessary for the conceptualization and design of school facilities, it is easy to envision WLANs in a variety of roles. WLAN technology offers great flexibility and functionality in retrofit situations as well as an excellent complement to learner-centered design features that some schools are adopting. A few examples include (Nair 2002):

Learning studios. Multipurpose learning studios, where different children can engage in different tasks in various activity zones or areas, would benefit greatly from a WLAN. Unlike a scheme requiring each computer to be tethered to a network with wires, the wireless approach is unobtrusive, complementing the idea of personalized learning.

Kivas, atriums, and "learning streets" instead of corridors. The value of these kinds of informal places that stimulate social interaction and learning is greatly enhanced by the ready accessibility to the world of information that mobile students can attain via a WLAN.

Resource areas. WLAN technology can readily deliver the resources that help maximize the utility of the school library, media center, cafeteria, and fitness center as learning areas that students can use as they see fit—not on some predetermined schedule as may be required in a computer laboratory. With WLAN technology, all of these areas and others can easily serve as formal and informal learning laboratories.

Unfettered access. Wireless technology will be an important part of the student and teacher empowering process. Once students get used to the idea of ubiquitous access to the Internet, the school intranet, and to each other from any location in the school, it is more likely that they will want to continue such access outside school. Having their own portable computing devices will help foster that kind of anytime, anywhere learning, which can continue at home, where students and teachers can talk to each other by e-mail as well as by audio and video chat sessions.

Living, not static, architecture. Wherever maximum flexibility for change is desired, which includes having the ability to rearrange spaces, move walls, as well as furniture and equipment to create a variety of teaching environments, WLAN technology provides the maximum amount of flexibility from the perspective of electronic communications and student access to information.

Costs and Equitable Access

According to Scott Carlson (2000), "The technology is good for the bottom line. Wireless technology often is less expensive than standard wire-and-wall-jack installation. In older buildings, wireless access may cost only a fifth of what an institution would spend on standard hookups." In some cases, universities have actually equipped desktop computers with wireless access because of its convenience at a reasonable cost. The computers can be rolled out into lobbies and common areas and be used for student registrations and other temporary tasks requiring network access. While K–12 needs are somewhat different, there is no question that wired systems that try to create the ubiquitous computing environment permitted by wireless technology will be substantially more expensive.

One benefit of wireless that often goes unnoticed is its ability to connect portable classrooms with the school network and the Internet. By beaming signals wirelessly to these temporary units, schools save the cost of wiring these buildings. Many school districts have chosen to leave their portables unwired, creating a situation of technology haves and have-nots. By extending both network and Internet connections to the portables by wireless means, schools can ensure that equitable technology access is available to all. Thousands of portable classrooms can benefit in this manner.

Wireless in the Future

In the future, more schools will be designed with the understanding that learning does not begin or end within the classroom. Wireless devices are but one means of freeing teaching and learning from the confines of the classroom and making education truly an anywhere, anytime enterprise.

The question for educators contemplating investments in technology is not so much whether wireless is a good option but how to make it an effective tool in the creation of student-centered learning environments. This means thinking about ways in which to integrate wireless solutions into the overall scheme of learning.

Today, wireless systems no longer are experimental or risky. In fact, a well-designed wireless network represents a good measure of "future proofing" a facility. It allows the next generation of handheld devices, tablet computers, high-powered laptops, data projectors, printers, scanners, video cameras, and various other WLAN-compliant devices to connect to the network and each other while giving administrators, teachers, and students a greater measure of freedom and flexibility. In this fast-changing technological world, wireless systems will play an increasingly vital role.

Glossary of Terms

LAN. Local area network. A communications network of computers or other electronic equipment in a local area such as a school or office.

MAN. Metropolitan area network. A communications network designed for a city or town that is larger than a local area network but smaller than a wide area network.

WAN. Wide area network. A communications network utilizing devices such as telephone lines, satellite dishes, antennas, and microwaves to span a larger geographic area than can be covered by a local or metropolitan area network.

WLAN. Wireless local area network. The extension of a wired LAN (see *LAN*) through radio transmissions to permit mobile users to connect their laptop computers or other wireless-enabled digital devices to a LAN.

WWAN. Wireless wide area network. A wide area network that uses wireless radio signals to connect two or more LANs located within different buildings.

kb/s. Kilobits (one thousand bits) per second.

Mb/s. Megabits (one million bits) per second; one thousand times faster than a kb/s.

Gb/s. Gigabits (one billion bits) per second; one million times faster than a kb/s.

access point. An antenna that transmits and receives signals over the airwaves and thereby serves as the interface between a wired network and wireless LAN adapters installed in laptop computers or other wireless devices (see definition for *wireless network adapters*).

backbone. The principal or main transmission line in a network that carries data gathered from smaller wires or cables that interconnect with it.

bandwidth. The amount of data that can pass along a communications channel in a given time period.

bit. A unit of information that has the value 0 or 1; short for binary digit.

byte. A unit of information comprising eight bits, generally used to signify a letter of the alphabet.

CAD. Computer-aided design. A hardware and software system that permits its users to automate the development of design representations, drawings, and related documents. CAD systems require high-definition monitors, powerful processors, and other special equipment.

encryption. Use of code to obscure communications. The numbers, such as 128- or 40-bit encryption, refer to the size of the key used to encrypt the message. Encryption with a 128-bit key requires many times more computer power to decipher than encryption with a 40-bit key.

Ethernet. A popular apparatus for enabling communications between two or more computers over a communications cable. Ethernet supports data transfer rates of 10 Mb/s. Fast Ethernet, a newer version, supports transfer rates of 100 Mb/s. Evolving 10 Gigabit Ethernet systems support transfer rates of 10,000 Mb/s. Faster systems are being developed.

fiber optic cable. A thin strand of very pure glass covered in plastic developed to supercede the use of copper cable for transmitting great quantities of information encoded as pulses of laser light.

firewall. A security plan intended to prevent unauthorized users from accessing a computer network.

GHz. A unit of electromagnetic wave frequency equal to one thousand million hertz (1,000,000,000 Hz). The gigahertz is used as an indicator of the frequency of ultra-high-frequency microwave signals.

hardwire. To connect (computer components, for example) by electrical wires or cables.

IEEE. Institute of Electrical and Electronic Engineers, Inc., an international standards organization.

interoperability. The harmonious working together of different types of computer hardware and software.

PDA. Personal digital assistant. A handheld computer that can upload and download information from a desktop computer and other devices. Some PDAs have wireless capability and also can access the Internet.

T1. A leased telephone connection popular with businesses and schools for connecting to the Internet. Provides data transmission rates of 1.544 million bits per second (1.5 Mb/s).

virtual private network. A private network that uses the Internet to connect remote sites or users while utilizing advanced security techniques to create secure communications.

WEP. Wired equivalent privacy, a data privacy mechanism for wireless networks described in the IEEE 802.11 standards. Its purpose is to simulate in wireless networks the same security features of a wired network.

wireless network. The extension of a LAN or WAN without wiring so that devices equipped with wireless network adapters can communicate with the wired network via the airwaves.

wireless network adapters. Electronic devices in laptop computers, notebook computers, and handheld devices that give users the ability to move freely within a campus or building environment while maintaining an uninterrupted connection to a network (also see *access point*).

Appendix One

Wireless Standards: A Comparative Analysis

Standard	Bandwidth	Advantages	Disadvantages	Comments
IEEE 802.11 (1997)	1 Mb/s to 2 Mb/s	This standard is effectively obsolete, but it paved the way for the standards that followed.	Bandwidth limitations did not allow widespread use in schools.	Early wireless adapters for computers were expensive; security was a problem.
802.11b (1999)	5 Mb/s to 11 Mb/s	Provides sufficient bandwidth to satisfy a majority of applications in schools. Improved security. Products available from multiple vendors. Interoperability assurance between products offered by Wireless Ethernet Compatability Alliance. Can be less expensive than wired systems, particularly for older or historic buildings. Good outside range (about 800 feet); permits campus-wide installations. Transmissions automatically switch among one of three channels.	Potential interference from other products such as microwaves, cordless phones, and Bluetooth devices that operate on the unlicensed 2.4 GHz frequency band. Effective bandwidth is usually only 7 Mb/s, not sufficient for bandwidth-hungry applications such as video conferencing and DVD transmissions. Effectiveness is reduced in densely populated areas that have hundreds of users, such as school auditoriums.	802.11b is a widely accepted standard that most schools are satisfied with both for indoor and campus-wide applications.

Standard	Bandwidth	Advantages	Disadvantages	Comments
IEEE 802.11a (1999)	54 Mb/s	Supports the transmission of video, voice, and other large files. Transmissions in the 5 GHz band ensure lack of interference from a host of devices such as cordless phones that share the 2.4 GHz frequency. Works well in densely populated areas because eight-channel operability means more access points can be deployed within the same space than with an 802.11b system. In some configurations, bandwidth of up to 108 Mb/s may be achievable. Speed decreases with increased distance at a lesser rate than with 802.11b systems. This means, as a user gets farther from an access point, an 802.11a access point will still deliver up to 12 Mb/s, whereas the 802.11b system delivers just 2 Mb/s.	Not backward compatible with existing 802.11b systems. This means that schools significantly invested in 802.11b technology should think carefully before migrating to the 802.11a standard. However, there are indications that dual compatibility access points may soon be offered, effectively eliminating this disadvantage. Prices for 802.11a access points and peripherals will be higher in the short run. Effective range of 5 GHz systems is less than 2.4 GHz systems. This means more 802.11a access points will be needed to cover the same area than 802.11b access points. This is an issue that is more relevant to large campus settings. Lower range means that 802.11a systems will be more costly to install, though users will benefit from the higher bandwidth these systems offer. Most 802.11a access points do not permit the use of replacement antennas. Some of the frequencies used by 802.11a devices are not licensed for outdoor use.	In the long run, there seems little question that the newer, higher bandwidth 802.11a and draft 802.11g standards (see below) have many advantages over the older 802.11b standard. Dual-compatibility systems will also probably hasten the demise of 802.11b systems—particularly in the K–12 market, which is not already heavily invested in the older standard. It is hard to tell which of the two newer standards, 802.11a or 802.11g, will prevail in the long run or if they will coexist. In any event, it would appear that schools choosing either standard can avail themselves of the full benefits of high-speed mobile computing.

Appendix One (cont.)

Wireless Standards: A Comparative Analysis

Standard	Bandwidth	Advantages	Disadvantages	Comments
IEEE 802.11g (draft)	54 Mb/s	Essentially, this is similar to the 802.11b standard because it operates on the 2.4 GHz frequency band. All the advantages noted previously for the 802.11b standard apply. The 802.11g standard is backward compatible with the older 802.11b standard that many users are heavily invested in. This standard can compete more effectively with the 802.11a standard because it offers the same higher 54 Mb/s bandwidth. Offers greater range than the 802.11a standard, which means larger installations will be less expensive than for the 802.11a standard.	Not a standard yet. 802.11g products may require upgrades when the standard is released. Potential interference from other products such as microwaves, cordless phones, and Bluetooth devices that operate in the unlicensed 2.4 GHz band. Potential to increase bandwidth to 108 Mb/s (as with the 802.11a standard) has not been demonstrated.	See previous comments.

Appendix Two

Bluetooth and 3G: Competing Standards or WLAN Complements?

Wireless technology is now sufficiently mature that its use in schools is becoming common. The technology owes its development to the advance of standards that enable the marketplace to produce interoperable wireless products and equipment. As the following discussion about Bluetooth and 3G (third generation) illustrates, there are some areas of overlap between these standards and WLAN technology based on the IEEE 802.11 family of standards. All indications are that over the next several years, Bluetooth, 3G, and 802.11 standards will coexist. WLAN designs for schools should not be significantly affected by the emergence of Bluetooth and 3G.

What Is Bluetooth?
Essentially, Bluetooth is a cable replacement technology in the form of a standard specification that permits electronic devices such as camcorders, PDAs, and computers to establish a wireless link for convenient data exchange. A typical application would be to walk up to a printer and beam the document you want printed directly from your laptop. The Bluetooth standard is supported by the Bluetooth Special Interest Group, a trade association with more than 2,000 members, including IBM, Intel, Microsoft, and Nokia. Bluetooth-equipped devices transmit data to each other within a 30-foot distance at about 1 or 2 Mb/s utilizing the 2.4 GHz frequency band. This is the same band on which the IEEE 802.11b wireless systems operate, posing the potential for signals to interfere with each other, though technologies currently exist to minimize such interference.

Bluetooth devices also may beam signals to each other to create what is sometimes called a "personal area network," though such a network cannot offer the robust operations provided by networks based on the IEEE 802.11 family of standards. At the present time, schools should not do anything different when it comes to designing their IEEE 802.11 networks to accommodate Bluetooth technology. At some future date, when and if all computers and peripherals are Bluetooth-compatible, students may choose to access desktop computers or other devices such as printers and scanners directly from their laptops, PDAs, or cell-phones, rather than through a network based on one of the IEEE 802.11 standards.

What Is 3G?
3G is the technology that is going to bring high-bandwidth applications to your cell phone, PDA, and other wireless-enabled digital devices such as tablet computers. The advantage of 3G over the IEEE 802.11 standards and Bluetooth is that it will provide truly ubiquitous wireless access. This means that a 3G device will keep you in touch with the Internet and all your information anywhere you go, not just within a building or campus that is wired for WLAN. While still several years away from being fully implemented in the United States, 3G devices will eventually access data at the rate of about 2 or 3 Mb/s. The huge sums of money being invested in the development and rollout of 3G networks means that access will not be cheap, and users probably will try to access their information in other ways, such as by getting within the range of existing WLAN networks that are proliferating in schools, airports, and shopping centers. Despite competition from WLAN, 3G is expected to be adopted and accessed widely in the United States by 2006. In the meantime, the use of Internet-accessible phones and PDAs operating at lower bandwidths continues to grow exponentially. For schools contemplating wireless, 3G is not likely to be an important factor in the design scheme for at least the next several years. Yet because planning requires foresight, looking ahead at these technologies is a good idea.

Appendix Three

Toward One-to-One Computing

As the following chart shows, there has been an inexorable move toward having one computer for each student in the United States, called one-to-one computing. A more meaningful statistic, however, is the number of students per *multimedia computer,* which is a machine capable of accessing the Internet and performing the computer-resource-hungry applications that many curriculums demand. In this regard, as many as seven students still share one computer in K–12 schools around the country.

Year	Students Per Computer	Students Per Multimedia Computer
1992	18	
1993	16	
1994	14	
1995	12	
1996	10	
1997	7.3	21.2
1998	6.3	13.5
1999	5.7	9.8
2000	5	7.9
2001	4.2	6.9

Sources: Market Data Retrieval, Quality Education Data, and NoteSys, LLC [NoteSys ceased business operations.]

The goal of many educators is to have each student possess a multimedia-capable laptop computer so that, at any given time, *all* students in a selected location can be working on a laptop. Classrooms that have four or five fully multimedia computers do not make this possible.

References

Bowman, Darcia Harris. 2002. Vandals target school technology items. *Education Week* 21 (February 20), no. 23: 1, 11

Bartel, Charles. 2000. Carnegie Mellon University. Wireless Andrew—Frequently asked questions on deploying a wireless network (October 18). Retrieved 7/25/02 from *http://www.cmu.edu/computing/documentation/faq_wirels_tech/WireTechFAQ.html*

Carlson, Scott. 2000. Universities find wireless systems bring them convenience and savings. *The Chronicle of Higher Education* (October 11). Retrieved 7/25/02 from *http://chronicle.com/free/2000/10/2000101101t.htm*

Corporation for Research and Educational Networking (CREN). 2000. Implementing a campus wireless LAN: What are the realities? (October 19). Retrieved 7/25/02 from *http://www.cren.net/know/techtalk/trans/imp-lan_1.html*

Educause. 2002. The wireless campus. Retrieved 7/25/02 from *http://www.educause.edu/issues/wireless.html*

Kirkbride, Edward E. 1999. Smaller class size and wireless technology. *School House Journal. Urban Educational Facilities for the 21st Century* 2 (February), no. 1. Retrieved 7/25/02 from *http://designshare.com/UEF/UEF_3_99/UEF_3_99b.htm*

Lightbody, Keith. 2001. Wireless networking in schools (February). Retrieved 7/25/02 from *http://members.ozemail.com.au/~cumulus/wireless.htm*

Market Data Retrieval. 2001. Federal and state funding initiatives boost technology in K–12 public schools across the nation (November 5). Retrieved 7/25/02 from *http://www.schooldata.com/pr27.html.*

McKenzie, Jamie. 2001. The unwired classroom, wireless computers come of age. *From Now On, The Educational Technology Journal* (January). Retrieved 7/25/02 from *http://www.fno.org/jan01/wireless.html*

Nair, Prakash. 2002. But are they learning? *Education Week* (April 3, 2002). Retrieved 7/25/02 from *http://edweek.org/ew/newstory.cfm?slug=29nair.h21*

Nair, Prakash. 2001. Wireless wide area networks for school districts. Washington, D.C.: National Clearinghouse for Educational Facilities. Retrieved 7/25/02 from *http://www.edfacilities.org/pubs/wireless.pdf*

Wireless LAN Association (WLANA). 2000. Do wireless LANs pose a health risk to the consumer? Retrieved 7/25/02 from *http://www.wlana.org/learn/health.htm*

About the Author

Prakash Nair, RA, REFP, is an international school planning consultant and architect. He is president of Urban Educational Facilities for the 21st Century and principal of Prakash Nair Consulting. He can be reached at prakash@designshare.com.

Acknowledgements

The author thanks Keith Lightbody for his help and guidance with the preparation of this publication.

Additional Information

See the NCEF resource lists *Wired and Wireless Networks* and *Technology Integration* online at http://www.edfacilities.org/rl/

Reviewers

Ed Brzezowski, Eric Flack, Walter Horowitz, Glenn Meeks, Chuck Philips, Andrew Seybold.

Sponsorship and Copyright

Published by the National Clearinghouse for Educational Facilities (NCEF), an affiliate clearinghouse of the Educational Resources Information Center (ERIC) of the U.S. Department of Education.

Availability

NCEF publications are available at *http://www.edfacilities.org/pubs/* or by calling 888-552-0624 (toll-free) or 202-289-7800.

NOTICE

Reproduction Basis

- [ ] This document is covered by a signed "Reproduction Release (Blanket)" form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.

- [X] This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").