EDUCATION WEEK

VOL. 26, No. 9 • October 25, 2006 | American Education's Newspaper of Record | © 2006 Editorial Projects in Education | $3

FOCUS ON: BUSINESS & TECHNOLOGY

Technology Upgrades Prompt Schools to Go Wireless

High-speed networks utilize education software better, experts say

BY RHEA R. BORJA

As educational software and web sites become increasingly rich in multimedia, and more schools adopt one-to-one laptop computer initiatives, districts are turning to high-speed wireless networks to make better use of that software and bandwidth-heavy interactive Web sites.

Students and educators want the "bigger pipes" the newer wireless networks provide, which is one reason why both K-12 and higher education are in the forefront of this technology trend, according to experts such as Rachna Ahlawat. She is a research director with the Gartner Group, a Stamford, Conn.-based firm specializing in information technology research.

The new networks can handle the plethora of wireless devices, such as personal digital assistants and Voice over Internet Protocol phones—telephones that convert analog audio signals to digital data, then transmit that over the Internet—that educators now use, Ms. Ahlawat said.

"Education is one of the biggest [markets] for wireless right now," she said.

The percentage of public schools using wireless systems has increased fourfold between 2001 and 2005, according to a report by Market Data Retrieval, a Shelton, Conn.-based education data-research firm. In 2001, 10 percent of public schools reported using wireless networks. In 2005, more than 45 percent had such networks. However, the report did not differentiate between older and newer versions of wireless networks.

Districts adopt wireless networks to achieve blanket Internet coverage throughout a school or campus, or because it's cheaper and easier than retrofitting older or very large buildings for wired access, according to the mdr report. Many states with the highest percentages of wireless-networked schools are heavily rural, such as North Dakota and Kansas, with 63.3 percent and 62.7 percent of districts, respectively, with such technology.

In addition, more than 78 percent of districts in Maine, which has a statewide one-to-one laptop initiative, have wireless networks. Many districts in Alaska (60 percent) and Hawaii (65.5 percent) have also deployed wireless networks.

Addressing Security

Technology companies such as Meru Networks Inc., a Sunnyvale, Calif.-based company that makes the newest version of wireless networks, has seen interest from school districts nationwide skyrocket.

Over the past year and a half, K-12 requests for proposals have risen from 10 percent to about 50 percent of the rfps the company receives from its education customers, according to Ihab Abu-Hakima, the company's president and chief executive officer.

"It is the increasing trend toward using wireless pervasively," he said. "Not just for convenience, but as the primary mode of connectivity."

The newer generations of wireless systems give districts more security and flexibility than the older ones, say some district technology directors.

New York's Rush-Henrietta district has had a wireless network since 1999. But it had some security problems, said Thomson M. Thomas, the director of computer services for the 6,000-student district in suburban Rochester.

One school, for instance, is located near an apartment building, and many of the building's residents had their own wireless networks. As a consequence, the school computers at times would automatically log on to the residents' networks instead of the school's. When that happened, teachers and students could not access the district's online learning services or even print documents.

Plus, Mr. Thomas said, the older wireless system had limited power using the old 802.11b local area network standard developed in 1999. Its access points covered only two classrooms, which typically had two to four computers each. The high school also has mobile carts of laptops that can be wheeled to any classroom.

"If you put too many more [computers] in there, the bandwidth was so limited that you were limiting what students can do," Mr. Thomas said.

The Rush-Henrietta district hired Meru Networks last school year to upgrade its wireless system to solve that problem. The new network has a centralized security system and is more powerful. Mr. Thomas said that was an important step for a district that aims to place a laptop computer in the hands of its 500 teachers by the end of the school year.

"If we're going to make [technology use] an expectation, then there needs to be the support and infrastructure to achieve that," he said. "Make things as simple as possible so there isn't that barrier."

Students in Maryland's 26,400-student Charles County school district outside Washington often had to wait for five to 10 minutes to boot up their laptops, according to B.J. Devkota, the district's chief information officer. That's because only a few students could log on simultaneously, or they'd overwhelm the district's wireless system.

The district upgraded the system during the 2005-06 school year. The new wireless system, created and installed by San Jose, Calif.-based Cisco Systems Inc., gives the district the flexibility to connect both its older buildings and its newer ones.

Older vs. Newer Wireless Networks

OLDER NETWORKS

▶ **Security:** Access points, communications hubs that receive and transmit data, are more susceptible to "denial of service" security risks.

▶ **Management:** Sometimes separate networks are re-quired for more bandwidth-heavy applications, such as converging data, voice, and streaming video. Also, access points lack sophisticated automated intelligence, so they are labor-intensive to maintain and upgrade.

▶ **Coverage:** Access points must operate below max-imum power and must be carefully placed in a classroom to avoid radio interference and coverage gaps. Also, access points can handle only 10 to 15 users at a time, so high-density areas such as auditoriums require more access points. Consequently, more planning is required to avoid interference.

▶ **Compatibility:** Older systems do not work well with different wireless cards. In particular, using both 802.11a and 802.11b/g wireless standards degrades performance.

NEWER NETWORKS

▶ **Security:** More sophisticated technologies for access points prevent many "denial of service" security attacks.

▶ **Management:** Many of the newer networks support more complex and sophisticated applications, such as converging voice, data, and video with high quality and definition. Also, access points can be centrally managed and upgraded.

▶ **Coverage:** Some newer systems allow access points to operate at full power, providing overlapping coverage. That means the network still works if the power in one access point fails. Some newer networks, moreover, can handle 100 users per access point.

▶ **Compatibility:** Some newer systems can work well with a mix of 802.11a and 802.11b/g wireless standards.

SOURCE: Meru Networks Inc.

Reprinted with permission from Education Week, Vol. XXVI, Issue 9, October 25, 2006, by The Reprint Dept., 800-259-0470.

EDITORIAL & BUSINESS OFFICES:
Suite 100, 6935 Arlington Road
Bethesda, MD 20814
(301) 280-3100
FAX Editorial (301) 280-3200
FAX Business (301) 280-3250

Education Week is published 44 times per year by Editorial Projects in Education Inc. Subscriptions: U.S.: $79.94 for 44 issues. Subscriptions: Canada: $135.94 for 44 issues.