Conclusions

On the basis of the online survey results, numerous IT and user interviews, and case study discussions, EDUCAUSE and IDC conclude that wireless networking is becoming an integral component of IT infrastructure for institutions of higher education. Half of all higher education institutions operate at least a limited wireless network, and most others—all but 8 percent—are planning for wireless. Most institutions that have implemented wireless networks are expanding them.

As wireless networking gains popularity on campuses, several key trends have emerged. Wireless is a supplemental, not substitutional, network for the wired infrastructure at higher education institutions. It provides an additional means for students, faculty, and staff to access the institution’s network. Its convenience, more than its capability, drives its adoption. In fact, wireless is bringing network access to more places—libraries, classrooms, common areas, and hard-to-wire locations—but users must be careful how they use it. Limited bandwidth means that data-intensive applications or simultaneous access by too many users may severely degrade wireless network performance. As a result, the wired infrastructure will continue to be the primary campus network. Institutions plan to implement new technologies (IEEE 802.11a, 802.11g) that will expand bandwidth to provide better performance and help meet the demands of a growing number of users.

Wireless is one of the most successful IT implementations. More than 90 percent of higher education institutions surveyed reported that their wireless networks met or exceeded expectations. Students and faculty incorporate wireless access into their day-to-day activities on campus for both academic and personal endeavors—conducting online research and checking e-mail, for example. The institutional staff, in many cases, is not as involved because many work from an assigned workplace that already contains a data port for wired network access. The key challenge for wireless is the classroom application—training faculty to adapt their pedagogy and instructing them to incorporate online teaching elements so that they can realize the full potential of wireless technology.

Conversations with IT administrators and users consistently illustrated the ease and enthusiasm with which students adopt wireless technology. The technology fulfills students’ expectations for instant information. A stroll around the case study campuses found
students huddled around wireless laptops, collaborating on projects. Some institutions seed wireless adoption through the library, implementing initial pilots and/or establishing laptop checkout programs for students.

While desktops are still the primary computing device in higher education, anecdotal evidence suggests that laptops are gaining popularity among both students and faculty. Laptops are the primary device used to access the wireless network. Some administrators, however, are looking beyond the laptop to the widespread use of lighter and less expensive PDAs and handheld PCs to expand the uses and adoption of wireless networking on campus.

Some administrators worry that the lack of universal student access to laptops may promote different educational experiences for those who can and do access the wireless network and those who cannot or do not. For example, how do laptop haves and have-nots collaborate on common projects? Institutions have addressed this in several ways:

- laptop checkout programs for students at libraries or student common areas,
- carts of laptops that faculty reserve in advance for classroom or lab applications, and
- mandatory laptop requirements for students in academic programs, particularly professional graduate programs in business, law, engineering, and medicine.

Wireless also has raised support issues for both students and faculty. IT departments must deploy extra resources to handle the surge in user help requests (installing drivers, for example) when the wireless network initially goes online. More daunting are the support issues that institutions face as faculty adapt course curriculums to facilitate online teaching elements and learn to operate the new classroom technology confidently. Some institutions have created specific programs and departments to address this issue.

Wireless is viewed by some institutions as a competitive differentiator. As prospective students’ technology demands become more sophisticated, wireless is becoming increasingly a “checklist” item. This is especially true in professional schools—business, law, medicine, and engineering—where wireless-equipped laptop computers are increasingly mandatory. Wireless not only facilitates the academic process but also enhances students’ preparation for their postgraduate careers.

Examining the survey results reveals that research universities led the wireless adoption curve. Many implemented their first wireless network more than three years ago, most likely using pilot implementations to test the technology’s capabilities, then expanding to other parts of the academic community. In the past two years, master’s and baccalaureate institutions have broadly adopted wireless. Associate’s institutions have begun to implement wireless too, although adoption lags in this segment.

Cost is a double-edged sword. Installation costs typically are relatively low: The reported median amount spent or budgeted is $50,000, and the median cost per student is only $50. Many institutions, employing the qualitative measure of positive user feedback, feel their return on investment is successful. Maintaining the networks over the long term, however, can be a challenge, because a wireless network represents a parallel infrastructure to support. While this enables IT departments to piggyback on current staff for operation, maintenance, and support functions, most are planning to implement new technologies, which will require some capital funding. Unfortunately, most IT departments have no long-term
funding strategies or cost recovery plans for their wireless networks, and many institutions are grappling with this issue.

Wireless installation is a challenging, complex process because there are so many variables—building architecture, construction material, room design, and room capacity—that impact access point and antenna placement. Many institutions implement a pilot application initially to learn about wireless technology characteristics. Others hire value-added resellers to assist in the process. And because it is easy for individual departments and colleges to install their own wireless networks, many institutions centralize wireless planning, operation, and policy within their IT departments to avoid interference and incompatibility problems.

Security presents a dilemma. Wireless technology’s radio transmission medium expands network access for authorized users throughout the campus, but it also creates the potential for security breaches and poaching of institutional resources by unauthorized users. Fortunately, no institution reported any significant problems—yet. Still, no easy solution exists today for the potential problems. Some institutions, especially doctoral ones and those with large enrollments, regard wired equivalency privacy (WEP) as ineffective and non-scalable. Instead, they turn to solutions like virtual private networks (VPNs), but this is costly and inefficient. Some institutions stress user education, outlining the potential security risks that wireless networking poses to users. A relatively large number of institutions (particularly AA and BA) have no encryption/authentication tools in place. Effective and efficient solutions (Advanced Encryption Standard use in VPNs, IEEE 802.1x/EAP) are coming, but they are a year or two away.

Different institution types exhibit different intentions about adopting newer wireless technologies. Perhaps because they have greater experience or financial resources, many research universities plan to adopt IEEE 802.11a in the next two years; other segments appear to be more reticent or divided over standards.