10
Effective Practices and Lessons Learned

This report provides baseline information on current and anticipated higher education networking technology and practices, drawn from ECAR’s online survey of 517 higher education institutions and in-depth interviews with 19 IT executives and managers at 13 EDUCAUSE member institutions. Chapters 4 through 8 follow the report’s navigational diagram, describing the campus network; external connectivity; networking practices, organization, leadership, and management; and emerging technologies and converged services. Chapter 9 examines success factors. The sidebar summarizes ECAR’s research findings about institutions that feel their institution has a higher-quality network infrastructure—one that is secure, fault tolerant, and optimally designed to meet future needs.1

This chapter presents relevant lessons learned and effective practices synthesized from ECAR’s research on IT networking in higher education. Some may be recognizable from other ECAR research studies; others are inherent to networking. They all, however, underscore the importance of maintaining a core portfolio of good IT practices to effectively serve the institution at large.

Which Institutions Report a Higher-Quality Network Infrastructure?
Institutions that…
◆ consider the network to be a strategic resource
◆ have a primary network goal to provide leading-edge network performance and services
◆ do not consider inadequate funding a barrier to the delivery of networking services
◆ have formal policies and procedures that cover networking issues and are comprehensive, enforced consistently, and regularly updated
◆ provide more redundancy measures for the institution’s central network
◆ have a disaster recovery plan for the institution’s data networking capabilities

"Soft" Practices Complement Technical Strategies
ECAR noted in its report Information Technology Security: Governance, Strategy, and Practice2 the importance of both sophisticated technologies and human and cultural factors of campus life in creating a secure institutional IT environment. We observe a similar trend in this ECAR research on IT networking. A
higher-quality network infrastructure is usually associated with technical characteristics such as adaptability, fault tolerance, reliability, scalability, and security. Yet one of the more interesting findings is the role that nontechnical factors play in creating a higher-quality network infrastructure. Both survey results and interviews show that although technology is indeed important in network design and management, the network is also contextually shaped and constrained by factors like senior leadership attitudes, funding resources, and institutional mission. ECAR’s research highlights several practices that focus on IT networking’s “softer,” or nontechnical, side.

**Cultivate Senior Leadership Awareness**

We noted in Chapter 9 that institutions where the network is considered strategic rate the quality of their network infrastructure higher. “It is important to build trust with leadership,” explains Joanne Kossuth, CIO, Franklin W. Olin College of Engineering. “Our senior administration never questions whether the IT department did due diligence to the nth degree and tested alternatives during the network design process. In fact, when our trustees read that VoIP is gaining popularity or networks are now converged, they remark what a great idea we had.”

Given senior leadership’s varying proclivities for technology, the recognition of networking’s strategic implications might not be initially straightforward. Interviews revealed different approaches to ensure that senior leadership understands the institutional network’s intricacies—and importance. Ron Stauss, vice chancellor, information technology and telecommunications, North Harris Montgomery Community College District, stresses the importance of an IT leader’s participation in the president’s or chancellor’s cabinet, serving as an on-the-spot networking advocate and educator: “If the IT leader is not present at the cabinet meetings, you must rely on someone who doesn’t fully understand IT (it’s not their job) to present the network initiative. If a question arises, it is typically tabled until those questions can be answered. If I’m present, I can respond to any inquiries, and it makes a remarkable difference.”

Olin College’s Joanne Kossuth takes a more formal approach, providing such educational opportunities as show-and-tell sessions for college constituencies, including senior administrators, to tour network facilities such as wiring closets, server rooms, and the network core. These opportunities help end users better understand exactly what makes the network tick. “Before actually seeing the facilities, our end-user constituencies, including administrators, understood the network based on either their own user experience or on PowerPoint presentations,” she explains. “The people that took advantage of the tours now have the added experience of the ‘wow’ factor. The visual effect of the number of cables and amount of equipment gets across the complexity of the network and helps them understand that it is not just about pushing a button.”

**Ensure Ample Network Investment**

Alan Bjornsen, writing in *American School & University*, says, “Laying the groundwork for a fast, efficient information technology system is not as complicated as it first seems. The most important thing is simple and straightforward; if there is only a dollar to spend, spend it on the infrastructure. Once the school is on a solid foundation, it can run an application to solve virtually any problem and meet virtually any educational or administrative need.” In Chapter 9, ECAR research also shows that those institutions that feel they are not experiencing inadequate funding would rate their network infrastructure as stronger, especially for the optimal design of
desktop connectivity and for the fault tolerance of the network.

Interviewees discussed ways to ensure adequate investment in their networks. Olin’s Joanne Kossuth leverages her relationships with vendors. “We believe that a partnership is a two-way street,” she explains. “Some institutions define partnership as getting their 50 percent discount. Olin, however, volunteered up front to serve as vendor reference sites, hosting user groups, providing live equipment demonstrations for potential customers, and encouraging our students to participate in focus groups about future product development. If my annual budget falls a little short, my vendors and I work together to create a package to ensure that Olin continues to be properly equipped to serve as the best reference site for them.”

Gavin Leach, associate vice president for finance and planning, Northern Michigan University (NMU), tries “to buy everything so it is reusable. As new technology becomes available, we can move the older equipment to lower-priority areas. As a result we have been able to put dollars into networking each year in a way so that we always remain current or slightly ahead of the curve with our technology.” Joe Aulino, vice president and CIO, Marist College, goes one step further by “looking at ways to leverage the infrastructure to generate revenue by providing some value-added or new services.”

**Align the Institution and Its Network**

Networking’s higher education origins may lie in research and academic pockets, but the advent of the Internet, administration systems, and course management systems enabled the network to extend its reach throughout the institution. When the network and institution become more interwoven, “an understanding of the institution’s big picture is very important,” advises Mike Fitzgerald, senior data network engineer, Brandeis University. “You don’t want to do networking by the seat of your pants.” IT leaders increasingly must consider both technical and institutional factors in network planning. ECAR’s research bears this out: we found that Carnegie class, student enrollment, and network size can impact campus network profiles. For example, doctoral institutions report higher bandwidth, higher-speed transmission standards, and more wireless access. Use of single-mode fiber and remote access rises as student enrollment rises. Bandwidth from the commodity Internet rises as the number of devices rises. The presence of student resident halls promotes greater concerns about P2P file sharing.

Our qualitative interviews also highlighted different IT activities and attitudes based on primary network goal. Network managers at leading-edge institutions typically have to future-proof the network to meet an extensive and diverse set of needs; deploy emerging technologies; and support innovative research. ECAR’s research noted that institutions whose primary network goal is to provide leading-edge network performance and services to the institution rate the quality of their network infrastructure—design of the backbone, desktop connectivity, and wireless networks, as well as network security and fault tolerance—higher than other institutions. For example, Steve Updegrove, senior director, information technology services at The Pennsylvania State University, describes his institutional infrastructure as one that contains “advanced, integrated telecommunications and networking services, which have been critical to the overall accomplishments of those within the university.”

In contrast, self-described “cost minimizers” have different aims. “We manage our network core cost-effectively and pragmatically,” explains Jose Valdes, associate director for telecommunications, Colorado State University. “We believe in being ‘early
Phil Trivilino, manager of network infrastructure at St. Lawrence University, concurs: “We don’t offer Internet2 connectivity here. There is limited demand for it because we are a liberal arts college. When we reviewed our Internet connectivity contracts, we chose our local broadband service provider because it offered a more competitive price package than our local Internet2 provider.”

The IT leader must understand the overarching institutional characteristics and act accordingly. The different activities we find at leading-edge and cost-minimizer institutions are neither right nor wrong; they are appropriate to achieve the institutional network goal.

**Networking Technology Practices**

“Soft” elements contribute to a higher-quality network infrastructure, but effective technical practices are clearly important as well. ECAR’s research reveals network-related practices and lessons learned in several areas, including infrastructure planning, convergence, mobility, external connectivity, and reliability.

**The Network Is Never Done**

Balancing network supply and demand can be a tricky proposition. As writer Anne Donker observes, “CIOs assume the network will always be there, until they find it doesn’t meet their new applications requirements. Then they remember that infrastructure matters, too.” IT leaders find maintaining a network infrastructure to be a very fluid process because they must constantly meet evolving user demands.

IT departments typically keep abreast of the current user demand and implement accordingly. A prime example is wireless technology. The *ECAR Study of Students and Information Technology: Convenience, Connection, and Control* notes rising student ownership of mobile devices. Marist College’s Joe Aulino also observes, “Students will have invested money in wireless technology and come to college with an expectation that wireless will be available.” Unsurprisingly, institutions are responding accordingly. Chapter 4 notes that wireless network access continues to rise, especially in areas that are not as hardwired, like indoor public spaces (dining halls, lounges, and lobbies), classroom seats, and outdoor spaces.

Other IT leaders, like Olin’s Joanne Kossuth, go a step further by conducting external environmental scans to anticipate future networking needs. When she plans, she researches the current network capabilities that math and science high schools—Olin student recruitment venues—provide their students. Kossuth explains, “Students will come to our college expecting us to do one better.”

In Chapter 9, ECAR research noted varying levels of agreement that the network supports staff, faculty, and student needs. Some institutions, however, use service-level agreements (SLAs) to help them understand the usage and value of their service offerings to their customer base. Jon Saperia, co-chair of the IETF SNMP Configuration Working Group, comments, “If it is worth the expense to deploy a new network service, it’s worth the expense to know if the service is supporting the business goals that drove its deployment.”

Not all needs, however, can be calculated. Unlike the corporate world, which typically builds its network to support specific needs,
higher education thrives on discovery and experimentation. The network can’t grind to a halt when a professor plugs in a new supercomputer or adds video conferencing to a course curriculum. IT departments, therefore, must try to build ahead of the user demand curve. Anna Tomecka, associate CIO and director of information technology services, Brandeis University, explains, “We know the faculty will want new services, but we don’t know what it will be—most likely video. So we continue to upgrade our network, waiting for this outburst of activity that we expect any day, any week.” St. Lawrence’s Phil Trivilino also looks ahead “to providing Gigabit Ethernet to the desktop in support of emerging arts technology as well as the new science complex that is currently under construction.”

Consider Organizational as Well as Network Convergence

Technology issues naturally arise when institutions converge their network, but this also gives IT departments an opportunity to rethink and redesign their IT organizations. “A big mistake some make is to equate telecom convergence with VoIP,” explains Indiana University’s Brian D. Voss. “The latter is just a subset (and one might argue a small one) of the former. Converge your organizations, converge your WAN links, and converge your cost/funding models!”

Voss describes organizational convergence’s benefits for IU. “When we streamlined the infrastructure and systems portion of the function, our new infrastructure and systems division was much more compact and focused. We could effectively lead it with a single senior manager. Our user services—now completely integrated from a user and organization perspective—are much more tightly integrated, closely matching the use of information technology by the community, and thus presenting a single, coordinated service interface to the users (that is, call one place for help or service for all IT areas). Within the technology division, we are now more tightly focused.”

When data and telecommunications staff members converge into a single unit, the entire IT organization benefits from the cross-pollination of their expertise. The Meta Group’s vice president, Elizabeth Ussher, observed that “a converged staff creates its own culture and will consider a variety of resolutions to a business problem, regardless of incumbent technology vendor.… As a result, converged staffs tend to be more business-solutions-oriented and regard technology as a tool to accomplish this. Cross-training has increased, but mostly this is done in house.”

Keep Mobility Strategies Open

Wireless and mobility “create networking requirements that must address when students, faculty, and staff are not necessarily in one fixed place anymore with anywhere/anytime access,” describes John P. Campbell, associate vice president of teaching learning technologies, Purdue University. Interviewees offer relevant thoughts and strategies.

Determine Which Devices to Integrate

Mobility has resulted in new means—such as laptops, cell phones, and PDAs—for users to access the network. IT departments have to determine which devices to integrate into the network, and this is no simple task. Varying device types may have dissimilar hardware, operating systems, and software issues, multiplying user support requirements. Network modifications may be required for various mobile devices to effectively use the network. Elazar Harel at the University of California, San Diego (UCSD), explains, “You need to design applications to understand the screen sizes on the various devices. Something that displays on a computer with its reasonably sized screen won’t show up on a cell phone...
screen.” Both requirements could strain network staff resources.

**Focus on Security**

Wireless also adds another dimension to security issues. “It is a challenge to provide security on the network, with PCs, Macs, UNIX, and pocket PCs. Now we must add cameras and phones,” Harel explains. “How do you keep them all secure?” Some institutions, like St. Lawrence University, have implemented VLANs, “which gives us the flexibility as well as granular control over what people can do on the network,” Trivilino says. “We have four different VLANs, but only the guest VLAN is different, offering only Internet access.” Harel foresees the “eventuality of single sign-on because users will carry so many devices, there will have to be a better solution than everyone carrying several passwords and login IDs with them.” He envisions the cell phone as the future “smart card,” whereby the network sends the device a one-time password in real time, thus eliminating the need for static passwords. “You will have a mechanism to get your token via the phone and be able to sign in to different applications and services.”

**Consider Personal Privacy**

Wireless technology provides new means to penetrate personal privacy: GPS tracks user location, camera phones take unauthorized photos, people eavesdrop illicitly on cell-phone conversations. IT leaders must be cognizant of potential privacy backlash issues. Limited technical options exist, but institutions could proactively create relevant incident handling procedures to minimize institutional damage in the event of a crisis.

**Explore External Connectivity Opportunities**

Today’s institutions are increasingly reaching out to one another through external research and educational networks, creating extended educational communities. One driver of external networks is the current glut of dark, or unused, fiber optic cable. The telecommunications industry’s collapse has lowered prices, making it economically feasible for more institutions to build their own external high-speed networks rather than lease lines from the local carrier. “If you are going to lease a line, and there happens to be dark fiber for sale at an advantageous price, then it makes sense to own the line,” states Marist’s Joe Aulino.

**Collapsing Geographic Barriers**

External networks offer several possible benefits for institutions to explore. “IT networking helps to collapse geographic barriers,” states Garret Yoshimi, manager of telecommunications, University of Hawaii. “The locations of the University of Hawaii System (including 10 campuses on six islands) can connect with our global community of stakeholders and customers and effectively participate at the forefront of global research activities.” Even colleges and universities not as geographically isolated as the University of Hawaii are turning to external networks like Internet2, National LambdaRail, and regional optical networks to conduct multi-institutional research, hold cross-institutional classes, and in some cases co-manage administrative services.

**Leveraging Resources**

Multiple institutions can leverage resources and funds to solve common problems via external networks. For example, the 5C Consortium in central Massachusetts is building a fiber ring to provide high-speed bandwidth access to its members. Marist’s Joe Aulino envisions “multiple small institutions eventually banding together to monitor networks centrally to make it more affordable for all.” Multi-institutional wireless networks enable locally proximate institutions to tackle the previously discussed mobility issues together.
Reaching Out to the Community

External networks provide a new means of community outreach as colleges and universities offer their network resources to the community. NMU’s Gavin Leach noticed that, “as wireless access expanded on campus and the use of it took off, it started bleeding off campus. Students noticed this and began to automatically test for off-campus access. NMU approached the city to try to move the wireless network out to our 6,000-plus commuter students throughout the city. The city saw great value in this and has been very supportive of our efforts to push the network technology and high speed outward, not only to help our students, faculty, and staff, but in the long run to enhance the local community and the economy in the area.” Olin College is trying to financially justify bringing high-bandwidth capability to its hometown of Needham, Massachusetts, to enhance the town’s student educational experiences and facilitate interactivity among the townspeople via the town Web site.

Meeting New Requirements

IT departments may find that external connectivity breeds new requirements as well as benefits. For example, those institutions opting to build their own external networks become de facto carriers, requiring new skill sets to ensure the miles of fiber cables are properly lit and operational. However, Dan Updegrove at The University of Texas, Austin, notes that “the biggest benefit from external connectivity may not be the state-of-the-art network. What we’ve got are universities talking to each other in a shared governance environment. For the first time in Texas, we’ve got a nonprofit structure in which academic medical centers and nonmedical universities, public and private, urban and rural institutions from across the state are all at the same table. That’s exciting.”

Balance Network Openness and Security Requirements

ECAR published a full study dedicated to IT security in higher education in 2003,10 so security was not a primary focus of this study. Yet security concerns bubbled up throughout this research. Spero P. Bowman, CIO and associate vice president for academic resources and planning at California State University, Northridge, summarizes the situation: “The whole security issue is the biggest and most costly challenge, requiring more and more attention, resources, and compliance.”

One issue is higher education’s propensity to innovate in network environments—innovation that promotes the early adoption of new technologies, often before universally adopted standards emerge. “The problem with security is that we can’t implement a solution for our faculty members, students, and staff without the rest of the world doing it also,” states UCSD’s Elazar Harel. “When we implement new networking devices, we keep up with the technology and vendors. We choose the technology we think will be successful. It is a gamble sometimes, but we are pretty successful.”

Another security dilemma is higher education’s traditionally open culture. The network continues to support more administrative and academic functions, making confidential information more accessible. In addition, as the network edge expands, so does the security threat. The data modem pool once represented the last mile to campus, but now faculty, students, and staff access the university network remotely, putting the university at risk because it becomes unclear where the network user is located and where his or her device has been. “You have to provide secure access, limited to your faculty, staff, students, and people you want on your network,” summarizes NMU’s Gavin Leach.
Consequently, institutions and IT departments must constantly grapple with how “closed” to make their network through security measures. Some institutions have a naturally closed environment. Larry W. Bryant at the U.S. Air Force Academy reports, “We’re lucky in that we operate on an active-duty military base that follows DoD security regulations for both wired and wireless networks, which protects us from the outside. In addition, all users have Norton antivirus on their machine. We also push the latest patches for students and staff to ensure everyone is compliant with all the latest patches.” But at other institutions, if security activities go too far, it may promote discomfort among faculty, students, and staff.

One solution is the creation of formal network policies. As Indiana University’s Mark Bruhn noted in ECAR’s IT security study, “Several security commentators have expressed concern that IT security can be inimical to academic freedom, but we believe this depends on the policy driving the institution, not the tools themselves. Indeed, IT security can support academic freedom by ensuring ready and timely access to information by authorized users. This is a major reason for having a comprehensive IT security policy; it can embed the academy’s most important values into an area that some might find otherwise problematic.” ECAR research notes, too, that institutions possessing formal networking policies and procedures that are comprehensive, regularly updated, and enforced consistently will more likely rate the quality of their network infrastructure higher. Involving institutional constituencies in policy creation ensures that their academic freedom concerns are addressed as well as providing a forum for the IT department to learn about users’ networking requirements.

The 24 x 7 Network Needs Around-the-Clock Reliability

The network’s ever-growing complexity and importance raise the significance of 24 x 7 reliability. “With every passing year, the university’s business operations, instructional programs, research programs, and outreach programs are more dependent upon the rock-solid reliability of the network,” UT Austin’s Dan Updegrove succinctly states. “Yet we add more 24 x 7 services to a data network that really isn’t architected as a 24 x 7 infrastructure.” Unsurprisingly, ECAR research shows that institutions that implement redundancy measures consider their backbone network to be optimally designed and, especially, that the network is more fault tolerant.

In light of the evident growing need for network reliability, it is surprising that 40 percent of ECAR survey respondents indicate that they have no disaster recovery plan for data networking at their campus. “The constantly changing network environment is reliability’s biggest challenge,” states NMU’s Gavin Leach. “It’s an ongoing challenge as we are constantly pushed to upgrade and move to new technologies, which in turn impacts our ability to keep up with it. We have to support the network both from our end by keeping it operational as well as from the user end by providing support.”

ECAR research, however, notes that institutions that maintain disaster recovery plans characterize the quality of their network infrastructure more positively. Indeed, former mayor of New York Rudy Giuliani advises, “When planning for disaster recovery, plan well and plan hard.” Some institutions are following his advice by conducting preemptive planning and monitoring to augment redundancy efforts. “We spend many hours
troubleshooting problems because we know problems are going to occur,” states Mary Jane Heider, director of academic computing at Genesee Community College. “It is ‘when’ it breaks down, not ‘if’ it will break down.” Chris Piety, assistant director of network services, Middle Tennessee State University, determines network benchmarks. “Our department knows what is normal by monitoring our network with products that graph our network statistics,” he explains. “We also have a network management station that monitors every piece of equipment on the network. So if something goes down, we can be proactive, not reactive.”

Look Outside Higher Education

ECAR’s IT alignment study observed IT leaders’ reluctance to conduct environmental scans outside higher education when conducting IT planning. Higher education’s prominent role in networking’s evolution may encourage similar thinking as well. Networking boundaries, however, continue to encompass more and more devices, prompting forward-looking IT leaders to broaden their technical horizons into areas not typically associated with higher education.

A case in point is embedded technology. Retailers like Wal-Mart use radio frequency identification (RFID) technology for inventory control; pharmaceutical manufacturers plan to “chip” bottles of prescription drugs to prevent theft and counterfeiting. Eventually, embedded technology will find its way onto college and university campuses, perhaps in library books, student ID cards, or even the students themselves. This in turn will open a host of new integration, support, and security issues for IT leaders to face, which in some ways bear a general resemblance to the wireless concerns faced today. The cycle of adoption begins yet again. The innovative IT leader will be prepared.

Endnotes

1. ECAR’s networking survey asked respondents to give their opinions (strongly disagree, disagree, neutral, agree, strongly agree) to the following statements about the design, security, and reliability of their campus network: (a) My institution’s central network backbone is optimally designed to meet our needs for the foreseeable future. (b) My institution’s desktop connectivity is optimally designed to meet our needs for the foreseeable future. (c) My institution’s wireless connectivity is optimally designed to meet our needs for the foreseeable future. (d) My institution’s network is secure. (e) My institution’s network is fault tolerant.


4. ECAR’s networking survey asked respondents to select one of four statements describing their institution’s goal for the network on the basis of four report descriptors. The descriptors are, Cost Minimizer: Provide reliable performance and services at the lowest possible cost; Requirements-Based: Provide appropriate levels of performance and services to different users, based upon their need; High Speed for All: Provide high-speed networking to the entire institution; Leading Edge: Provide leading-edge network performance and services to the institution.


6. R. Kvavik et al., ECAR Study of Students and Information Technology, 2004: Convenience, Connection, and Control (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Study, Vol. 5, 2004). The study found that 82 percent of freshmen and seniors at 13 participating higher education institutions own cellular phones, 46.8 percent own laptops, and 11.9 percent own PDAs.


9. The 5C Consortium consists of Amherst College, Hampshire College, Mount Holyoke College, Smith College, and the University of Massachusetts, Amherst.


11. Ibid., pp. 70–71.
