



E D U C A U S E

CORE DATA SERVICE



2002 Summary Report

Brian L. Hawkins, Julia A. Rudy, and Joshua W. Madsen



EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. Membership is open to institutions of higher education, corporations serving the higher education information technology market, and other related associations and organizations. Resources include professional development activities; print and electronic publications, including books, monographs, and the magazines *EDUCAUSE Quarterly* and *EDUCAUSE Review*; strategic policy advocacy; teaching and learning initiatives; applied research; special interest collaboration communities; awards for leadership and exemplary practices; and extensive online information services. The current membership comprises nearly 1,900 colleges, universities, and education organizations, including 200 corporations. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C.; www.educause.edu, e-mail info@educause.edu.

© Copyright 2003 EDUCAUSE

All rights reserved. No part of this monograph may be reproduced in any form without permission in writing from EDUCAUSE.

Art direction by Joseph Daigle, Studio Productions

Networking and Security

The fourth section of the core data survey focused on networking, methods of remote access, bandwidth shaping, videoconferencing capabilities on campus, deployment of new technologies, and practices related to network security.

Network Speed and Shaping

The core data survey requested data about the bandwidth available from a campus to the commodity Internet and to high-speed networks. Table 4-1 shows the distinct patterns that characterize bandwidth availability to the Internet by Carnegie groups for responding institutions, with the greatest access reported (not surprisingly) by doctoral institutions and the least by AA and BA institutions.

Looking at access to high-speed networks,

Table 4-2 shows that the greatest access was reported by doctoral institutions, most likely due to the large data sets, visualization, and other applications needed by faculty at such institutions for their academic work. About three-fourths of the AA, BA, and MA institutions responding to our survey provide no access whatsoever to such networks.

Shaping bandwidth refers to adjusting parameters on the campus Internet connection to limit use through various means, such as type of connection, location of connection, direction of traffic, time of day, or other specific characteristics. A campus may choose to shape bandwidth to ensure that the downloading of large files does not interfere with the basic operational needs of the campus and that the bandwidth is available when faculty and students need it for their academic work.

Table 4-1
Total Bandwidth Available to the Commodity Internet from Campus

	All	DR	MA	BA	AA	Other
0 Mbps	0.5%	0.0%	1.2%	0.8%	0.0%	0.0%
More than 0–4.5 Mbps	28.5%	1.5%	27.2%	43.6%	48.3%	29.2%
4.6–12 Mbps	20.9%	3.0%	25.4%	36.8%	25.8%	11.5%
12.1–44 Mbps	16.4%	15.7%	18.3%	9.0%	12.4%	28.1%
45–89 Mbps	15.1%	31.3%	15.4%	8.3%	6.7%	9.4%
90–154 Mbps	5.8%	11.9%	3.6%	0.8%	5.6%	8.3%
155–299 Mbps	7.2%	20.9%	6.5%	0.8%	1.1%	4.2%
300–999 Mbps	2.3%	8.2%	1.2%	0.0%	0.0%	1.0%
1,000 Mbps or more	3.2%	7.5%	1.2%	0.0%	0.0%	8.3%

Table 4-2
Total Bandwidth Available to High Performance Networks from Campus

	All	DR	MA	BA	AA	Other
0 Mbps	56.8%	11.9%	71.6%	82.7%	74.2%	41.7%
More than 0–4.5 Mbps	4.8%	0.0%	5.9%	5.3%	10.1%	4.2%
4.6–12 Mbps	4.0%	2.2%	1.8%	5.3%	6.7%	6.3%
12.1–44 Mbps	3.9%	1.5%	3.6%	0.0%	3.4%	13.5%
45–89 Mbps	8.9%	22.4%	7.1%	6.0%	2.2%	3.1%
90–154 Mbps	2.9%	6.7%	2.4%	0.0%	3.4%	2.1%
155–299 Mbps	8.2%	28.4%	5.3%	0.8%	0.0%	3.1%
300–999 Mbps	4.7%	17.9%	1.2%	0.0%	0.0%	3.1%
1,000 Mbps or more	5.8%	9.0%	1.2%	0.0%	0.0%	22.9%

Table 4-3
Methods and Use of Bandwidth Shaping

	All	DR	MA	BA	AA	Other
Only track bandwidth utilization	29.3%	17.2%	29.6%	12.0%	52.8%	47.9%
Shape by time of day	24.2%	20.1%	31.4%	39.1%	5.6%	13.5%
Shape by location on campus	39.1%	65.7%	43.8%	44.4%	5.6%	17.7%
Shape by type of traffic	60.4%	72.4%	74.0%	76.7%	15.7%	38.5%
Shape by direction	40.3%	56.0%	41.4%	57.1%	9.0%	21.9%
Do not track or shape	9.8%	2.2%	4.1%	9.8%	30.3%	11.5%

As seen in Table 4-3, about 10% of all campuses report not shaping bandwidth at all, but this level is elevated by the high percentage of associate’s colleges (nearly one-third) reporting no bandwidth shaping practices. More than half of these colleges also reported only tracking use without any other shaping strategies. The most popular strategy is shaping by the type of network traffic, with AA institutions nonetheless using this strategy far less than doctoral, masters, or baccalaureate institutions.

The second most common strategy is shaping by direction on the Internet, that is, filtering to differentiate between data and traffic that flow from the campus to the Internet versus from the Internet to the campus. Doctoral and baccalaureate institutions use this strategy to the greatest extent. Shaping bandwidth by location (for example, shaping only for res-

idence halls) is the next most common approach, with doctoral and baccalaureate campuses doing this the most and associate’s colleges the least. The next most frequently reported strategy is shaping by the time of day, which is used most by baccalaureate school respondents.

Remote and Wireless Access

Providing remote access to the Internet and to campus networks is critical to serving faculty and students who live off campus. The survey asked about six commonly used methods of providing such access to four constituencies: faculty, students, staff, and alumni. Providing access to faculty via an internal modem pool, the strategy employed by more than 60% of all responding campuses, is the most common method employed. Internal modem pool access, however, is differentially employed for

Table 4-4
Level of Remote Access Provided via an Internal Modem Pool to Various Constituencies

	All	DR	MA	BA	AA	Other
Faculty	61.5%	80.6%	57.4%	63.9%	44.9%	54.2%
Students	45.9%	73.9%	46.2%	44.4%	15.7%	36.5%
Staff	64.4%	80.6%	61.5%	66.2%	49.4%	58.3%
Alumni	6.9%	7.5%	6.5%	9.0%	3.4%	7.3%
Not provided	34.1%	17.9%	37.9%	31.6%	49.4%	39.6%

Table 4-5
Number of Campus Sites from Which Interactive Videoconferencing Can Be Initiated

	All	DR	MA	BA	AA	Other
0	28.3%	9.0%	26.6%	48.9%	30.3%	28.1%
1	15.0%	6.0%	16.6%	24.8%	10.1%	15.6%
2	12.1%	6.7%	13.0%	13.5%	20.2%	8.3%
3	9.2%	6.7%	9.5%	3.8%	16.9%	12.5%
4-5	10.6%	14.9%	13.6%	3.8%	10.1%	9.4%
6-10	12.7%	20.1%	14.2%	4.5%	9.0%	14.6%
11-20	6.9%	17.2%	5.9%	0.8%	1.1%	8.3%
More than 20	5.2%	19.4%	0.6%	0.0%	2.2%	3.1%

various constituencies, as shown in Table 4-4, with the greatest access provided to faculty and staff and significantly less to students. Only about 7% of respondents make such access available to alumni.

Only about 5% of campuses reported providing access by an outsourced modem pool, and there are no differences in the frequency of such offerings across types of campuses. Approximately 20% provide access via ISPs with an institutionally arranged discount, while only about 10% of campuses provide subsidized ISP accounts.

The growth of wireless network access on campuses is striking. The core data survey captured detailed data (far too great to include in this summary report) about the extent of penetration of wireless into seven areas of the campus: classrooms, libraries, open spaces, research facilities, administrative offices, public laboratories, and residence halls. In general, there is wide variation as to the level of deployment of wireless across these categories and across the Carnegie groups. Overall, the

highest level of penetration is found in libraries, with a third of all campuses having three-quarters to 100% of their libraries providing wireless access. Doctoral institutions have incorporated wireless technology into classrooms and public spaces to a greater extent than other Carnegie classes. Wireless access is least available in residence halls and research facilities overall.

Videoconferencing Capabilities

Videoconferencing capabilities were reported by all campus types, but about one-fourth of all responding campuses do not have a single site (not including desktop videoconferencing) from which interactive conferences can be initiated, with that being true for nearly half of the BA institutions. In addition, the level of penetration varied immensely by Carnegie class, as seen in Table 4-5. Doctoral institutions have the greatest availability of these facilities, with about 20% of universities in this category having more than 20 such sites.

In addition to central sites for videoconfer-

**Table 4-6
Number of Desktops That Can Deploy Desktop Videoconferencing**

	All	DR	MA	BA	AA	Other
0	42.0%	9.0%	45.6%	66.9%	50.6%	39.6%
1-5	13.4%	4.5%	17.2%	15.0%	20.2%	10.4%
6-10	8.5%	8.2%	9.5%	6.0%	13.5%	6.3%
11-25	8.7%	11.2%	10.7%	4.5%	5.6%	10.4%
26-100	10.6%	25.4%	5.3%	3.0%	2.2%	17.7%
101-1,000	9.0%	15.7%	7.1%	4.5%	7.9%	10.4%
More than 1,000	7.7%	26.1%	4.7%	0.0%	0.0%	5.2%

**Table 4-7
Status of Voice-over-IP Technology**

	All	DR	MA	BA	AA	Other
Deployed	13.2%	17.2%	10.1%	7.5%	16.9%	17.7%
Piloting	18.7%	41.0%	13.0%	6.8%	9.0%	22.9%
In progress	4.7%	3.7%	4.7%	1.5%	11.2%	4.2%
Considering	40.6%	32.1%	46.2%	48.1%	31.5%	40.6%
Not planned	22.9%	6.0%	26.0%	36.1%	31.5%	14.6%

**Table 4-8
Status of Video-over-IP Technology**

	All	DR	MA	BA	AA	Other
Deployed	29.8%	56.0%	24.9%	12.0%	34.8%	21.9%
Piloting	10.6%	17.2%	7.1%	6.8%	7.9%	15.6%
In progress	9.3%	11.9%	9.5%	5.3%	7.9%	12.5%
Considering	31.7%	10.4%	41.4%	37.6%	34.8%	33.3%
Not planned	18.5%	4.5%	17.2%	38.3%	14.6%	16.7%

encing, respondents were asked about the number of desktops that could deploy videoconferencing. The same pattern was found as with central sites, with doctoral institutions having the most such capability, followed by “Other” and MA institutions. More than a quarter of the doctoral institutions have over a thousand machines with this capability. As seen in Table 4-6, two-thirds of BA schools do not have a single machine with such capability.

Deployment of New Technologies

The core data survey explored the level of deployment of seven new technologies that

are currently hot topics of conversation within the higher education IT community. Data for these technologies are presented in Tables 4-7 through 4-13.

As shown in Table 4-7, voice-over-IP (VoIP) technology is being fully deployed at about 13% of campuses, with the highest level in doctoral institutions and the lowest in baccalaureate institutions. Nearly 23% of all responding campuses reported no plans for this technology, with this being especially the case for baccalaureate and AA institutions and least so for doctoral campuses.

Video-over-IP technology is employed to a

**Table 4-9
Status of PKI Technology**

	All	DR	MA	BA	AA	Other
Deployed	12.1%	10.4%	12.4%	9.8%	20.2%	9.4%
Piloting	4.8%	11.9%	3.6%	1.5%	1.1%	5.2%
In progress	6.3%	9.7%	4.1%	3.8%	9.0%	6.3%
Considering	36.6%	51.5%	37.3%	28.6%	16.9%	43.8%
Not planned	40.3%	16.4%	42.6%	56.4%	52.8%	35.4%

**Table 4-10
Status of LDAP Technology**

	All	DR	MA	BA	AA	Other
Deployed	53.9%	75.4%	47.3%	40.6%	51.7%	56.3%
Piloting	5.0%	4.5%	6.5%	3.0%	4.5%	6.3%
In progress	15.5%	14.9%	17.8%	14.3%	12.4%	16.7%
Considering	14.2%	4.5%	18.3%	20.3%	13.5%	12.5%
Not planned	11.4%	0.7%	10.1%	21.8%	18.0%	8.3%

**Table 4-11
Status of Biometric Technology**

	All	DR	MA	BA	AA	Other
Deployed	1.1%	4.5%	0.6%	0.0%	0.0%	0.0%
Piloting	2.9%	5.2%	4.1%	0.0%	2.2%	2.1%
In progress	1.4%	1.5%	1.8%	0.8%	2.2%	1.0%
Considering	16.1%	25.4%	14.8%	11.3%	12.4%	15.6%
Not planned	78.4%	63.4%	78.7%	88.0%	83.1%	81.3%

**Table 4-12
Status of Smart Card Technology**

	All	DR	MA	BA	AA	Other
Deployed	15.8%	24.6%	18.3%	12.8%	3.4%	14.6%
Piloting	2.6%	4.5%	2.4%	1.5%	0.0%	4.2%
In progress	4.8%	3.0%	4.7%	5.3%	4.5%	7.3%
Considering	34.9%	29.9%	38.5%	32.3%	34.8%	39.6%
Not planned	41.9%	38.1%	36.1%	48.1%	57.3%	34.4%

much higher extent than voice over IP, as shown in Table 4-8. About 30% of all campuses reported using this technology, but, again, this is most true for doctoral institutions and least true for baccalaureate institutions. AA

schools are second highest in reporting using this advanced technology, probably in large part due to their innovative use of technology in teaching and learning.

The use of public key infrastructure (PKI) is

**Table 4-13
Status of Web Services Technology**

	All	DR	MA	BA	AA	Other
Deployed	57.2%	77.6%	60.4%	44.4%	50.6%	46.9%
Piloting	2.9%	3.0%	3.0%	1.5%	1.1%	6.3%
In progress	12.9%	6.7%	14.8%	19.5%	11.2%	10.4%
Considering	17.1%	12.7%	14.2%	15.8%	19.1%	28.1%
Not planned	10.0%	0.0%	7.7%	18.8%	18.0%	8.3%

**Table 4-14
Characteristics of Firewalls on Campus**

	All	DR	MA	BA	AA	Other
Firewall at external Internet connection	77.6%	50.7%	83.4%	86.5%	91.0%	80.2%
Firewalls around certain high-security servers or networks	48.6%	75.4%	45.0%	31.6%	33.7%	55.2%
Firewalls deployed by or on behalf of individual departments	26.7%	67.2%	17.8%	7.5%	6.7%	31.3%
Requirement that all clients use personal firewalls	0.5%	1.5%	0.6%	0.0%	0.0%	0.0%
No firewalls	4.7%	4.5%	4.7%	6.8%	3.4%	3.1%

interesting to note, as this technology may well be critical in the deployment of campus security policies and practices. As seen in Table 4-9, deployment of PKI is still in the early stages of diffusion, despite the amount of campus discussion and numbers of conference presentations on this topic. As one would expect, doctoral institutions are furthest along with this deployment, but second are AA institutions, although a large percentage of campuses in this Carnegie class indicate that they are not planning such an implementation. It will be interesting to watch the trend line on this technology when next year's core data are released.

One indicator of the potential trend line for PKI is the current level of deployment of Light Directory Application Protocol, or LDAP. Such a directory is essential for the authentication and authorization efforts required in PKI, and

over half of all campuses currently have LDAP deployed, as shown in Table 4-10. There are significant differences with this technology deployment, with more than 75% of doctoral institutions having LDAP deployed, while only 40% of baccalaureate institutions have deployed this technology.

There is virtually no deployment of biometric technology, which includes use of fingerprints, retinal scans, or other physiological means of user identification for security purposes. About 80% of all responding campuses are not even planning for this technology (see Table 4-11).

As shown in Table 4-12, the deployment of smart cards is most prevalent at doctoral institutions and reported least by AA institutions. The overall level of penetration is less than one might have expected, with only about 16% of all responding institutions reporting

**Table 4-15
Practices Regarding Security-Related Software Patches and Updates**

	All	DR	MA	BA	AA	Other
All critical systems expeditiously patched or updated	82.1%	76.9%	84.0%	79.7%	86.5%	85.4%
Some critical systems expeditiously patched or updated	15.9%	17.2%	16.0%	18.0%	11.2%	15.6%
Computers connected to network have security holes fixed	47.3%	44.8%	47.9%	36.1%	68.5%	45.8%
Proactive scans in critical systems	56.0%	70.9%	53.3%	48.1%	48.3%	58.3%
Proactive scans in computers connected to network	31.7%	44.0%	27.8%	18.0%	29.2%	42.7%
Security system includes intrusion detection system	38.5%	59.0%	43.2%	18.0%	23.6%	43.8%

deployment of smart card technology and more than 40% reporting it is not planned.

The final emerging technology analyzed is the use of Web services as a set of tools and building blocks for system development. As shown in Table 4-13, with over half of all campuses deploying Web services, this is the most commonly adopted of the seven technologies examined. It is worth noting that not a single doctoral campus reported not planning to use Web services.

Security

The final area of analysis is security, including the processes being used to secure campuses from disruptions of service, incursions, and other security breaches. Perhaps the most common type of security protection being used by responding campuses is a firewall. Experience has shown that a single firewall is not adequate to provide security, however, as many of the individuals who provide a threat to security are students and personnel who work and operate within the environment protected by the firewall. Table 4-14 shows various strategies currently being employed and their relative fre-

quency within each of the Carnegie groupings.

Overall, fewer than 5% of all campuses have no firewalls, with the most common strategy for all responding institutions being the deployment of a firewall at the external Internet connection. This is true for a very large percentage of all campuses other than doctoral institutions, which more often reported deploying firewalls around high-security servers and by or for individual departments. There was virtually no use of or requirement for personal firewalls irrespective of Carnegie group.

Table 4-15 shows the patterns and use of software patches and other practices to ensure security on campus. Far and away the most common practice is to expeditiously patch or update critical systems, with this being reported by about 82% of all campuses and no differences found between Carnegie groups. The second most common practice is conducting scans of the network on critical systems, with this occurring for more than half of all campuses and somewhat more frequently at doctoral institutions. Fixing the security of machines connected to the network is the next most common strategy, with nearly half of all

**Table 4-16
Security Policy Advisory Participants**

	All	DR	MA	BA	AA	Other
IT Policy/Security Officer	58.6%	76.1%	52.7%	39.8%	61.8%	67.7%
Central IT Organization	93.9%	98.5%	95.9%	91.7%	89.9%	90.6%
Auditor	39.9%	64.9%	39.1%	21.1%	27.0%	44.8%
General Counsel	49.6%	85.8%	49.1%	27.1%	36.0%	43.8%
Board of Trustees	11.3%	15.7%	13.0%	9.8%	9.0%	6.3%
Chief Financial Officer	42.7%	47.0%	49.7%	36.8%	40.4%	34.4%
Chief Academic Officer	46.7%	55.2%	55.6%	39.8%	42.7%	32.3%
President's Cabinet	54.1%	52.2%	66.3%	45.9%	66.3%	35.4%
Campus Task Force	31.4%	53.0%	27.2%	20.3%	34.8%	20.8%
State Agency/System Office	18.8%	21.6%	26.6%	3.0%	38.2%	5.2%
No Policy Development	1.3%	0.0%	0.0%	3.0%	2.2%	2.1%

institutions reporting this practice. The use of security intrusion detection systems is the next most common approach, but this method is used far more at doctoral institutions and much less at baccalaureate and AA schools. The conducting of scans on individual computers on the network is the second least used method, with the selective patching of critical systems the least used approach.

Finally, respondents were asked to identify the participants in policy development related to security on campus. As shown in Table 4-16, the patterns of involvement and the breadth of participation in such policy efforts varied

dramatically across Carnegie types. In all cases, the central IT organization was the most common participant in such processes, with about 94% of all campuses checking this group and no differences between Carnegie classes. However, commonality of the policy-making process ends there. A significantly higher percentage of doctoral institutions than other types of schools reported involvement of the IT policy/security officer, the university counsel, the auditor, and a campus task force. Fewer baccalaureate institutions reported engaging any of these participants than any of the other types of schools.