The Need to Improve Remote Access to Online Library Resources: Filling the Ga...
Denise Troll Covey
Portal : Libraries and the Academy; Oct 2003; 3, 4; Social Science Module
pg. 577

The Need to Improve Remote Access to Online Library Resources: Filling the Gap Between Commercial Vendor and Academic User Practice

Denise Troll Covey

abstract: Research reveals that academic libraries are not meeting user needs and expectations for easy access to online library resources. Remote users are particularly dissatisfied. Survey results indicate that the technologies currently deployed to support off-campus users are inadequate and problematic for both users and libraries. A new approach is required to improve service quality. The Internet2 Shibboleth software offers a viable alternative.

Access to the Internet has precipitated new information-seeking behaviors and expectations. To provide quality customer service, libraries must support these behaviors and meet these expectations. The situation is particularly challenging for academic libraries. Fulfilling their mission to support teaching, learning, and research is now tied to their support of these new information-seeking behaviors and expectations. Several recent studies show that students and faculty go online first when they need information. If they use the library, they often use it remotely, from outside of a physical library facility. They inextricably link good customer service with convenient, easy access to information and easy-to-use online tools and resources. The results of these studies indicate significant gaps between user needs and expectations and what libraries are providing. The results also indicate that these gaps are in high priority areas for users, which makes them high priority areas for academic libraries, strategic to providing quality customer service. The following bullets, extracted from seven studies conducted 2001–2002, illustrate the crisis libraries are reaching in customer service.

portal: Libraries and the Academy, Vol. 3, No. 4 (2003), pp. 577–599. Copyright © 2003 by The Johns Hopkins University Press, Baltimore, MD 21218.

- *Self-sufficiency is the academic work paradigm.* For academic knowledge workers, self-sufficiency or personal control hinges on easy access to information. Roughly 90 percent of the students and faculty who participated in a survey of the scholarly information landscape, sponsored by the Council on Library and Information Resources (CLIR) and conducted by Outsell Inc., indicate that ease of access is their second most important information need, topped only by the need for quality resources. However, fewer than half of the students and faculty in the survey indicate that libraries are adequately meeting their need for easy access. Participants in the survey rated ease of access to information and having sufficient training to use the tools and resources available as their third most significant problems.[1]
- *The Internet is changing perception and use of the library.* The Outsell study revealed that though students and faculty trust the library more than the Internet, they turn to a popular Internet search engine like Google to satisfy their daily information needs. Approximately 80 percent of the students and faculty who participated in the study said that the Internet has changed their use of the library, and over a third said they use the library less now than they did two years ago. A study conducted under the auspices of the Pew Internet and American Life Project revealed that 73 percent of graduate and undergraduate students use the Internet more than the library; only 9 percent said they use the library more than the Internet when they need information.[2] Roughly 80 percent of the college students who participated in a survey conducted by the Online Computer Library Center (OCLC) said they use the library fewer than three hours per week. Four out of five students in the study said they sometimes use the library for web access, but only one in five prefers this access point.[3] The OCLC study and a study conducted as part of the Evaluation of the Distributed National Electronic Resource (EDNER) Project show students turning to an Internet search engine first when they need information.[4] In the OCLC study, 40 percent of the students indicated that they use an Internet search engine for every class assignment, while only 11 percent said they use the library web site for every class assignment. Though over a third of the students in the OCLC study felt the range of information available on the web is inadequate, most (96 percent) of them believe that the information they find on the web is good enough for class assignments. In contrast, an analysis conducted by Steve Lawrence and Lee Giles in 1999 revealed that only about 6 percent of the web sites indexed by popular web search engines like Google was appropriate for academic use.[5] Even if the percentage has increased in the past few years, the fact that almost half (46 percent) of the students in the OCLC study believe that other sites have better information than the library web site is reason for concern.
- *College students expect convenience.* They associate convenience with easy access to information and easy-to-use online tools and resources. Students in the OCLC study perceive the difficulty of navigating and searching the library web site and online resources as barriers to library use. Their number one recommendation for libraries is to make it easier to access and use library resources. Results from both the Pew and the EDNER studies indicate that students use the Internet

more than the library because it is easier to find resources using the Internet. Current college students acquired their information-seeking habit of using Internet search engines in high school, and they see no need to change their habit because they can successfully find adequate information using Internet search engines.

- *Remote access to online resources is very important.* Over half (54 percent) of the students and faculty in the Outsell study said they access library resources from their residence. The percentage is higher (68 percent) for undergraduate students. According to the Pew study, 69 percent of undergraduates live off campus and 59 percent of them use their home computer more than computers at school. According to the OCLC study, 90 percent of students access the web from their home computer, and 78 percent prefer remote access. Over 40 percent reported having high-speed access from home via cable modem, T1/T3 line, ISDN, or ADSL/DSL. They perceive vendor licensing restrictions and password requirements as barriers to easy remote access to library resources.
- *User assessments of library service quality reveal significant problems.* The ARL LibQUAL+ survey results from spring 2002 indicate problems in the areas of access to information and personal control. Speed and convenience are key characteristics in both areas. In terms of access to information, users want convenient business hours and timely document delivery and interlibrary loan. In terms of personal control, users want easy, convenient, remote access and easy-to-use tools and web sites that enable them to find the information they need without assistance. They also want libraries to provide state-of-the-art equipment. While libraries are meeting minimum needs in these areas, the gaps between what we are providing and what users really want is significant.
- *Students and faculty perceive technology as critical to student success.* Results of a study sponsored by McGraw-Hill Ryerson in 2002 indicate that most faculty (83 percent) rate new technology among the three key factors in student success, just behind course preparation and faculty training and development.[6] Approximately 77 percent of the U.S. faculty participating in the study cited computer technology as the most important and effective resource for students, ahead of the library. Only 56 percent of the participants even mentioned the library as a valuable resource for student success, positioning the library on a par with tutoring. The results of the study suggest that while content is critical to meeting faculty objectives for student success, the library might not provide the most up-to-date materials. The Internet appears to have the edge on currency. A somewhat parallel pilot study of student perception of learning success, conducted by Dieter Schönwetter, indicates that they too, like faculty, believe technology to be critical.[7] When asked what the library could do to enhance their success, 46 percent of the students responded provide more technology, 30 percent said provide more assistance, but only 24 percent requested more materials. When asked what their institution could do to enhance their success, 26 percent responded provide greater exposure to technology. When asked what their professors could do to enhance their success, 32 percent responded provide greater exposure to technology. When asked what textbook publishers could do to enhance their success, 55 percent of the students mentioned online access or

CD ROMs. When asked in general what would enhance their success at learning, 43 percent responded greater exposure to technology, 31 percent responded simply more technology, while only 26 percent mentioned academic courses.

- *College students follow the path of least cognitive resistance.* According to the EDNER study, efficiency, or the amount of time and effort required to find information, appears to matter more to students than the relevance of the information found. A research report published by the Library and Information Commission suggests that user satisfaction is multi-dimensional, occurring within a framework of expectations comprised of the information-seeking task, the functionality of the retrieval system used, the assistance provided, the user's own abilities and immediate goals, and (finally) the information retrieved. Efficiency and the user's experience of interacting with the retrieval system—in short, the ease and speed of finding information—can be equally as important in satisfying the user as the utility or appropriateness of the information found. Low expectations will be highly satisfied with low precision results.[8]

Libraries are taking steps to address the issues raised in these studies, to close the gaps and improve customer service. For example, they are redesigning their web sites to improve navigation, endeavoring to reduce turn-around times in services like interlibrary loan and e-reserves, empowering users with direct-borrowing tools and tracking mechanisms, and marketing their resources or packaging and pushing them through portals to targeted user groups. Libraries are doing what they can to remove barriers and facilitate convenient, easy access to and use of quality resources. However, they can't do it alone. For example, libraries cannot provide users with the ease and convenience they have come to expect, based on their experience with popular Internet search engines, without the cooperation and initiative of the commercial vendors from whom they license online resources. Supporting remote access—a high priority need and expectation for academic library users—is a case in point.

Libraries are doing what they can to remove barriers and facilitate convenient, easy access to and use of quality resources.

Users want free and unfettered access to information from anywhere, anytime. Commercial vendors must charge a fee for and restrict access to the value-added bundling of electronic library resources and delivery systems they provide. Vendors are restricting access by institutional IP address, so libraries tediously track ranges of campus IP addresses and report them to vendors whenever new licenses are signed or new ranges are added. But many institution-affiliated users want to access electronic library resources from computers that do not have an institutional IP address. Libraries are providing proxy servers or virtual private networks to fill this gap between vendor and user practice.

A proxy server is a server technology that sits between a client application, like a web browser, and a real server that delivers content or services to users. The proxy server intercepts transactions between users and real servers. In the current context, users of computers without an institutional IP address must login to the proxy server using their institutional ID and password. Thereafter, their requests go through the proxy server, which has an institutional IP address that real servers can recognize as authorized to receive commercially licensed content. The proxy server then relays the information to the users of computers without an institutional IP address.[9] The user login to the proxy server accomplishes the task of authentication, verifying to the institution that the user is affiliated with the institution. The proxy server accomplishes the task of access control, verifying to the remote server or vendor that the user is authorized by institutional affiliation to receive the licensed content or service.

A virtual private network (VPN) is similar to a proxy server in the sense that it accommodates the needs of users who are legitimately authorized to use institutionally licensed resources, but who do not meet the current access-control requirement of commercial vendors, i.e., a computer with an institutional IP address. A VPN is an on-demand, private network that uses the Internet to connect users with remote servers. Unlike a proxy server, which users simply need to login to via a web page, VPN requires users to register their computer with the VPN service and to configure their computer to use the VPN. After these tasks are completed, use of the VPN is similar to use of the proxy server. Users initiate a VPN session by starting the software and logging in with their institutional ID and password. Thereafter their requests go through the VPN, which temporarily assigns an institutional IP address to their transactions so that remote servers can recognize their requests as authorized to receive commercially licensed content. The information is relayed over the VPN to authorized users of computers without an institutional IP address.[10]

Though proxy server and VPN technologies assign an institutional IP address to user transactions, they are problematic and no doubt implicated in user assessments of library service quality. For example, use of cable modems, DSL, and Internet Service Providers like America Online (AOL) is common among remote users of the library—and a frequent source of remote user access problems through proxy servers and virtual private networks.

Access restriction is not the only way in which vendors disappoint libraries and contribute to a reduction in service quality. Many vendor products are not easy to use. Some vendors offer substantial training for librarians and staff, no doubt expecting them to train their library users. Unfortunately many users don't come into the library, and even if they do, they want to be able to use the library's electronic resources with ease, which is to say, without substantial training. Some vendor products require downloading of desktop clients, a task difficult if not impossible for remote users. Vendors have not integrated OPAC and campus authentication systems, which frustrates users by requiring them to remember different IDs and passwords to review what books they have checked out or what fines they owe, rather than enabling them to use their regular campus IDs and passwords. Despite years of tedious lobbying and standards development, many content and integrated library management system vendors still do not provide libraries with meaningful, comparable usage statistics that would enable careful assessments of the use and cost-effectiveness of the electronic resources and systems that increasingly strain library budgets.

Meanwhile, increasingly savvy users are spoofing institutional IP addresses and implementing open-access proxy servers that circumvent the IP-address restrictions that vendors put in place. The recent online theft of journal articles from the JSTOR database was reported in the *Chronicle of Higher Education*.[11] The thieves found and exploited open proxy servers on college and university campuses and apparently attempted to download the entire collection of scholarly journals in JSTOR. When JSTOR took steps to prevent further downloads, the culprits worked around them, ultimately stealing about 50,000 articles before outside consultants helped JSTOR stop the downloads. The *Chronicle's* reporting of the JSTOR incident raised the issue of potentially more serious breaches, like the unauthorized downloading of confidential medical records, but did not raise the issue of campus liability. However, given the ambiguity under the Digital Millennium Copyright Act of whether institutions of higher education are Internet Service Providers (ISPs), academic libraries and their parent institutions should be concerned. The IP-addresses and locations of compromised or infiltrated open proxy servers can be identified, and the institution could be held accountable by the vendor and/or the government.

The IP-Address Restriction Survey

Prior to the publication of the research studies cited above and the JSTOR theft, the painful experience of running a proxy server at Carnegie Mellon and discussions with colleagues at conferences across the country led me to question both the adequacy and the real and hidden costs of the technologies libraries are using to fill the gap between vendor and user practice in accessing online resources. Conversations with colleagues led me to believe that dissatisfaction was widespread among library users and staff. The various problems and frustrations encountered with proxy servers and virtual private networks appeared to me to be commonly shared, but none of us seemed to know what these technologies were really costing our libraries to run in terms of dollars squeezed from already strained or diminishing budgets or other kinds of hardships. When I asked my colleagues whether a survey would be beneficial to identify and quantify the problems and costs associated with current technologies deployed to provide authorized users of computers without an institutional IP address with access to IP-address restricted resources, the answer was a resounding "yes." Librarians and library technologists agreed that a better understanding of the current situation broadly shared with libraries and information providers could illustrate the difficulties inherent in current implementations and help motivate the move to more appropriate and manageable authentication and authorization technology.

Given this encouragement, I decided to conduct a survey of academic libraries to assess the impact of their efforts to fill the gap between vendor and user practice. Hoping to increase the response rate, I asked Deanna Marcum, President of the Council on Library Information Resources (CLIR), to endorse the research. She graciously agreed to provide a cover letter to accompany the survey. Through my interactions with colleagues in the Digital Library Federation (DLF) and CLIR, I engaged Peter Brantley of the Internet 2 Shibboleth project and Dale Flecker, then acting technical program director of the DLF, to help me compose the survey questions.

The survey and cover letter were sent as an email enclosure to 128 library directors at small, mid-sized, and large institutions in June 2002. Respondents were instructed to route the survey to the people at their institution who could answer the questions and to return the completed survey by the end of July. They could return the completed survey as an email enclosure, via regular U.S. mail, or fax. Seven of the surveys bounced back because the email address was incorrect. Two library directors responded that their institution did not provide a service that enabled authorized users working without an institution-affiliated IP address to access IP-address restricted resources. One responded that a partner institution provided this service for them and that the partner institution would complete the survey. The overall response rate for the survey was 58 percent. The response rate for completed surveys was 55 percent (71 completed surveys). Data from completed surveys were coded and analyzed using Statistical Package for the Social Sciences (SPSS). Of those responding, 46 percent identified themselves as liberal arts colleges, 43 percent as universities (30 percent as private universities, 13 percent as public universities), and 6 percent as an "other" type of institution.

Proxy Server and Virtual Private Network Implementations

Almost all (94 percent) of the institutions that responded provide a proxy server service. All of the private and public universities and most of the liberal arts colleges (85 percent) and other institutions (75 percent) run a proxy server. Of the 67 proxy server implementations:

- Almost half (45 percent) were implemented by the library
- Over a third (36 percent) were implemented by their institution's central computing organization
- 17 percent were implemented through a collaboration of the library and central computing
- 2 percent were outsourced

Some (12 percent) of the respondents did not specify the proxy server software used at their institution. The others named eleven different proxy server softwares. Ezproxy was the most popular, with at least 37 percent of the implementations. The second most popular software was Squid, with at least 11 percent of the implementations. Few sites reported developing their own proxy server or using the other software products mentioned.

In contrast, only 30 percent of the responding institutions were running or testing a virtual private network (VPN) service at the time the survey was conducted. A third of the private and public universities were operating or testing a VPN. Only 18 percent of the liberal arts colleges were operating or testing a VPN. Most (75 percent) of the "other" institutions were operating or testing a VPN. Sixteen production implementations were reported, with five institutions just beginning to implement or in the process of testing VPN:

- Most (85 percent) were implemented by the institution's central computing organization
- The rest (15 percent) were implemented by libraries in partnership with central computing
- None were implemented by libraries alone

Many (38 percent) of the respondents did not specify the VPN software used at their institution. The others named five different VPN technologies. Cisco was the most popular, with at least 43 percent of the implementations. The other products named were mentioned by only one institution.

Almost one-fourth (24 percent) of the institutions responding were running both a proxy server and a VPN at the time the survey was conducted. Though the survey did not ask how long the institution had been operating each of these services, the written comments strongly suggest that the proxy servers had been in operation for a long time and that the VPNs were more recent. Several sites stated explicitly that the VPN was new. No one commented that the proxy server was new. Though only a few institutions commented that they had implemented or were implementing VPN as a potential solution to their proxy server problems, the sheer number of sites (17) running or planning to run both services suggests some dissatisfaction with the proxy server and hope that VPN will be an improvement.

Problem Frequencies

The survey results indicate that proxy servers are more problematic than VPN implementations. However, the VPN results reported here should be interpreted cautiously because only a small number of institutions (23 percent) responding to the survey were running production VPNs. A few others were just beginning to test VPN. Furthermore, respondents throughout the survey appeared to know much less about their VPN service than they did their proxy server service, probably because the libraries were much less involved in implementing and maintaining VPN and because the VPN implementations were more recent. Libraries responding to the survey clearly had less experience and expertise with VPN than with proxy server technology.

Almost half (47 percent) of the libraries with VPN service did not know how frequently problems occurred. Of those who did report problem frequency, 7 percent reported daily or weekly problems and 20 percent reported monthly problems. In contrast, very few respondents (5 percent) indicated that they didn't know the frequency of problems with their proxy server. Though 38 percent reported that there were seldom problems with their proxy server, almost half (47 percent) of the respondents said there were daily or weekly problems with their proxy server. Another 11 percent reported monthly problems with their proxy server. Regardless of how long the services have been in operation, both proxy server and VPN service are sometimes problematic, and dealing with proxy server problems appears to be routine in many libraries. See figure 1.

Problems Types and Sources

Survey respondents reported a variety of problems with their proxy server or VPN. The problems they identified with the services are similar, though the frequency with which they reported the different types of problems varies somewhat with the technology. See figure 2 and table 1.

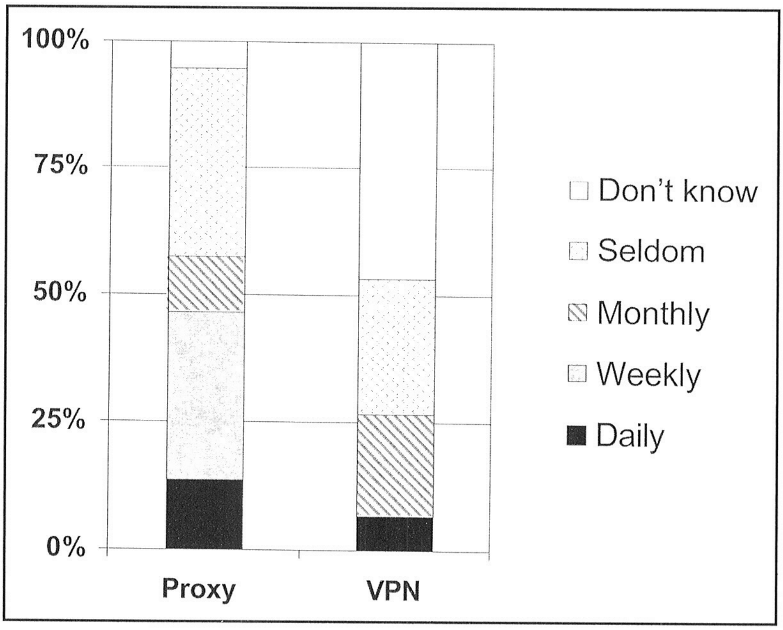

Figure 1. The frequency of problems with proxy servers and VPNs.

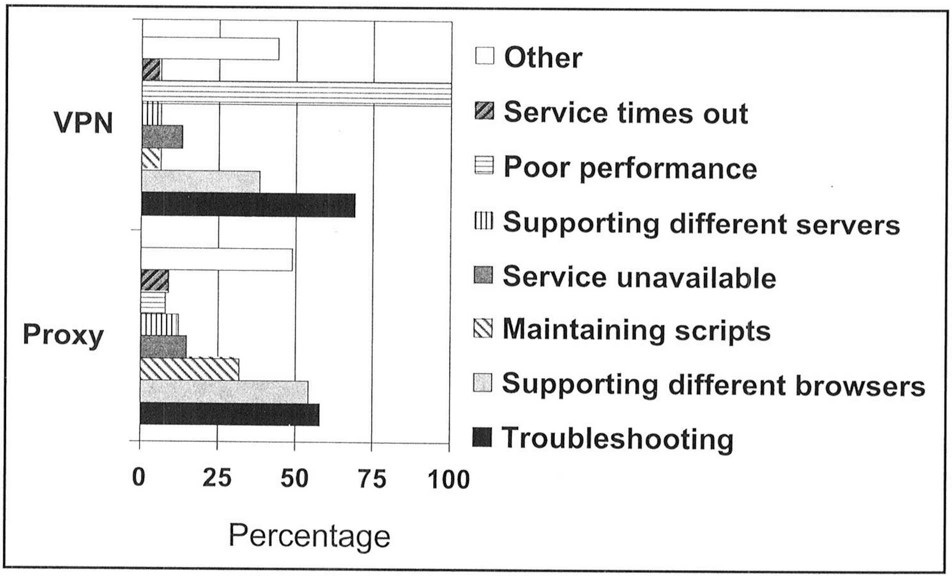

Figure 2. Percentage of respondents reporting different types of problems with proxy servers and VPNs.

Table 1

Percentage of respondents reporting different types of problems with proxy servers and VPNs.

	Proxy server	VPN
Troubleshooting	58%	69%
Supporting different web browsers	54%	38%
Maintaining scripts to work with different vendor products	32%	6%
Service unavailable	15%	13%
Supporting different web servers	12%	6%
Poor performance	8%	100%
Service times out	9%	6%
Other problems	49%	44%

Over half of the institutions running a proxy server or VPN reported troubleshooting—identifying what and where the difficulty is—as a problem. Over half of the institutions running a proxy server also reported supporting different web browsers as a problem. Supporting different web browsers appears to be somewhat less of a problem with VPN. Almost a third of the institutions running a proxy server reported script maintenance as a problem. Comments from several institutions lamented the fact that vendors don't forewarn them when they change their software, apparently oblivious to the fact that their changes break library proxy servers and disrupt remote user access to their products. All of the sites running a VPN reported poor performance as a problem. Evidently once users login to VPN, they use it for all of their online work, not just to access IP-address restricted resources. This puts a tremendous load on the VPN, which slows network performance.

Over half of the institutions running a proxy server also reported supporting different web browsers as a problem.

Over 40 percent of the institutions running either a proxy server or VPN reported miscellaneous other problems, including user errors, configuration problems, and problems with firewalls, Internet Service Providers (ISPs), and marketing. Of particular note is that 13 percent of the VPN institutions reported problems with ISPs while only 2 percent of the proxy server sites reported problems with ISPs.

Though again the VPN data must be interpreted cautiously, the similarity between proxy server and VPN problems is disconcerting. Several institutions commented that they had implemented or were implementing VPN as a hoped-for solution to their proxy server problems. The survey results suggest that the result could be the same problems, though with less frequency, and a decline in performance—but with the burden of maintenance and support shifting from the libraries to the central computing organization. Such a shift could mean user education and training in new procedures for reporting problems, which in turn could increase the dissatisfaction of already dissatisfied remote users.

The survey also asked respondents to identify the three vendors or e-resources that presented the most frequent problems with their proxy server or VPN, and the three that presented the most difficult problems to solve. Respondents named fifty-five different products. ISI Web of Science, Elsevier ScienceDirect, and Bell and Howell's ProQuest were reported as the source of the most frequent problems. ISI Web of Science, LexisNexis, and IEEE e-resources were reported as presenting the most difficult problems to solve, followed closely by netLibrary and ProQuest.

Regardless of what the problem is, service to users remains disrupted until the problem is identified, localized, and solved. Given the increasing number of licensed electronic resources using IP-address access restriction and user preferences for remote use of online resources, the collective experience of remote users might well be that remote access to library resources is unreliable. Studies of service quality suggest that reliability is the most important characteristic of service quality.[12] The unreliability of remote access to online library resources could be a big contributor to user dissatisfaction with the ease and convenience of access to library resources and to their turning to Internet search engines and other web sites for information.

Problem Reporting

Almost half (46 percent) of the survey respondents indicated that the procedure for reporting proxy server and VPN problems was well organized at their institution. Another 44 percent said that it was somewhat organized. A few (7 percent), however, described problem reporting as downright haphazard at their institution. Disorganization appears to be more of a problem at universities than colleges, perhaps because of their size and having multiple library locations at one institution. Approximately 10 percent of the private universities and 8 percent of the public universities reported haphazard organization of problem reporting.

Over 70 percent of the institutions indicated that proxy server and VPN problems were discovered through email or phone calls from users or librarians. Users tend to report problems using email slightly more often than the telephone. In contrast, librarians use the telephone to report problems more than twice as often as they use email. Approximately 14 percent of the institutions indicated that they also discover problems through telephone calls from other help desks on campus that are located in departments, colleges, or their institution's central computing organization. Only 10 percent of the institutions indicated that an automatic message from the proxy server or VPN alerted technical staff when there was a problem.

Most institutions (72 percent) reported that the time varied between problem occurrence and when the technical staff responsible for fixing the problem learned about it. The time lag could be a day or more. Only 13 percent of the respondents said the technicians routinely found out about a proxy server or VPN problem within hours of the problem occurrence. Only one institution felt confident enough to report that technicians were alerted to problems within minutes of their occurrence. Given the time it takes to identify, locate, and fix problems, the lag time between problem occurrence and when the technicians learn about them and are free to turn their attention to them can only exacerbate user frustration and confirm their perception that remote access to online library resources is unreliable.

Time Spent Dealing with Proxy Server and VPN Problems

The survey asked three different questions to try to get a sense of the effort invested in proxy server and VPN maintenance and support. One question asked how much of the libraries' help desk time is spent on proxy server and VPN problems. Another asked respondents to estimate how much time library technical staff and non-technical staff spend dealing with proxy server and VPN problems. The third asked how much time librarians and staff spend explaining the proxy server and VPN to users.

- *Help Desk Time.* Most libraries (76 percent) reported that little of their help desk time is spent dealing with proxy server or VPN problems. Only 15 percent said that 20 percent to 40 percent of their help desk time is spent on these kinds of problems. However, a few sites (4 percent) reported spending as much as 70 percent to 90 percent of their help desk time on proxy server problems. No site reported this much time invested in dealing with VPN problems at the help desk. The survey did not ask the operating hours per week of the library help desk.
- *Library Technical and Non-Technical Staff Time.* Most libraries (approximately 70–75 percent) estimated that their technical and non-technical staffs each spend one day or less per month dealing with proxy server or VPN problems. However, of the institutions running a proxy server, 25 percent reported that their technical staff spends one to three days per month and another 3 percent said their technical staff spends more than three days per month dealing with proxy server problems. Librarians and other non-technical staff invest a comparable amount of time. Almost 20 percent of the proxy server sites indicated that their librarians and other non-technical staff spend one to three days per month, and 5 percent said that their non-technical staff spends more than three days per month dealing with proxy server problems. Even sites running the most popular proxy server, Ezproxy, reported routinely investing entire workdays per month dealing with proxy server problems.

  Surprisingly, given that central computing organizations manage most of the VPN implementations, a third of the libraries reported that their technical and non-technical staffs spend one to three days per month on VPN problems. Perhaps this is because the implementations are relatively new or just underway. No VPN site reported library staff spending more than three days per month on VPN problems. However, even sites running the most popular VPN, Cisco, reported routinely investing time in resolving VPN problems.
- *Time Explaining to Users.* When asked how much time librarians and staff spend explaining the proxy server or VPN to users, most institutions (73 percent)

reported fewer than five hours per month. Another 14 percent reported spending one to three full workdays per month. Roughly 10 percent said they spend more than three workdays per month explaining the proxy server or VPN to their users. Universities appear to spend more time explaining these technologies to users than colleges, perhaps because they have more users, a more complex or decentralized computing infrastructure, or run both a proxy server and VPN. Almost twice as many private universities as public universities reported that they spend more than three days a month explaining the proxy server or VPN to their users. See figure 3.

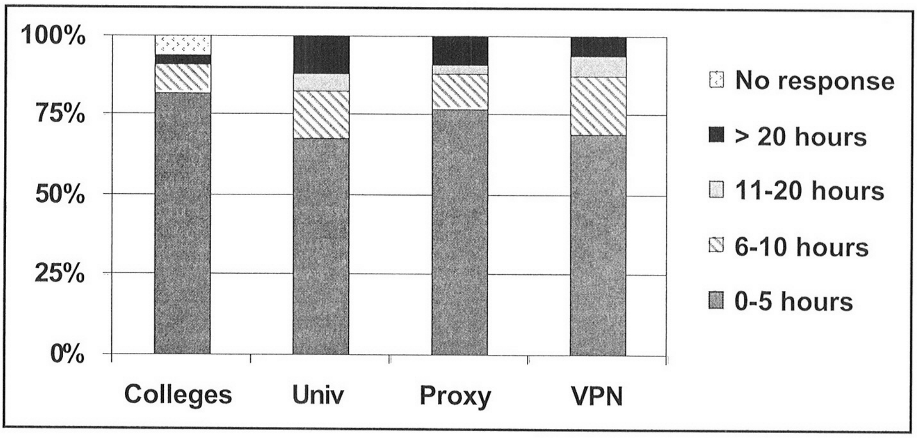

Figure 3. Time spent explaining the proxy server or VPN to users.

The survey results suggest that VPN requires about as much time to explain as a proxy server. See table 2. The newness of many VPN implementations could understandably drive up the time needed to explain VPN to users and staff unfamiliar with the technology. Nevertheless, the fact that proxy servers that have been in operation for a long while continue to take about as much time as a new service is puzzling, given that significantly less than half of a campus population turns over in any given year.

Table 2

Time explaining to users.

	0-2 hours	3-5 hours	6-10 hours	11-20 hours	>20 hours
Proxy server sites	51%	24%	10%	3%	9%
VPN sites	35%	29%	18%	6%	6%

One has to wonder how many users actually take the time to report problems they encounter or to ask for clarification or training. The results of the study conducted by OCLC, noted earlier in this article, indicate that most college students (61 percent) turn first to their friends or classmates when they need assistance. Roughly a third (36 percent) consult their professors or teaching assistants. Only one in five (21 percent) asks a librarian when they need help using the web. Given the undergraduate preference for using popular Internet search engines and their inclination to follow the path of least cognitive resistance, it's easy to imagine them quickly turning to Google if and when they encounter problems in remote access to online library resources. If this is indeed the case and these users instead turned to librarians to learn about or resolve their problems with proxy servers and VPNs, the time investment of non-technical library staff would no doubt be considerably greater than reported in the current survey results.

Library Staff Costs

Over half (55 percent) of the survey respondents estimated that they spend less than $5000 per year on proxy server or VPN maintenance and support. Twenty percent said they spend more than $5000 per year, with 13 percent estimating expenditures over $10,000 and 6 percent estimating expenditures over $15,000. Ironically given the investment of library staff time noted above, 13 percent of the institutions reported no staff costs. See figure 4. University libraries appear to spend more on these services than colleges, but this could simply be because they are larger and have larger budgets. The survey did not gather comparative data about the expenditure for these services per student or faculty FTE. For reasons unknown, the survey responses indicate that VPNs cost libraries more than proxy servers.

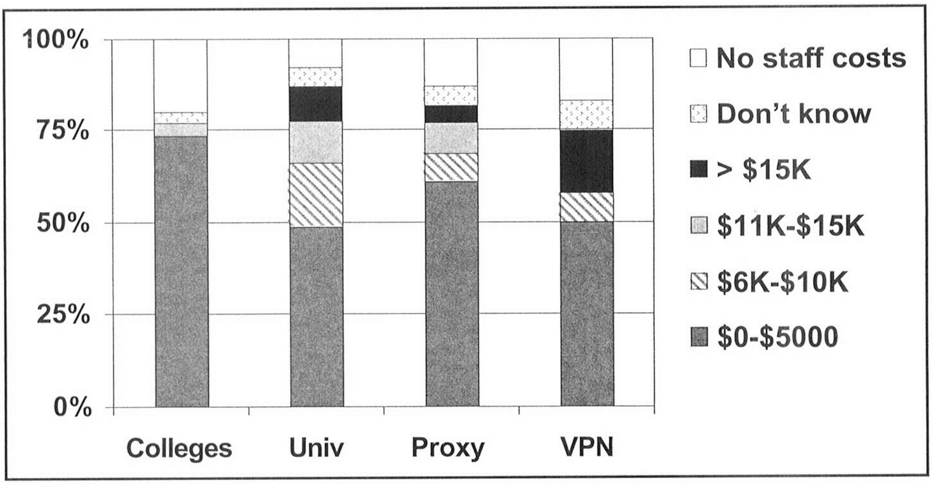

Figure 4. Library expenditures for supporting and maintaining proxy servers and VPNs.

Negative Impacts

Most of the survey respondents (60 percent to 75 percent) reported that proxy server and VPN problems lower user satisfaction and service quality. Approximately a third reported that proxy server and VPN problems cause significant delays in other library projects. Many sites (approximately 20 percent to 30 percent) also indicated that proxy server and VPN problems adversely affect the allocation of library resources and, to a lesser extent, lower the morale of library staff. Despite the frequency of problems or the time and money invested in communicating and fixing the problems, a few respondents (7 percent) said that their proxy server had no negative impact. Written comments about "other" negative impacts described user frustration and delays in their work caused by desktop browser or other configuration problems. See figure 5 and table 3.

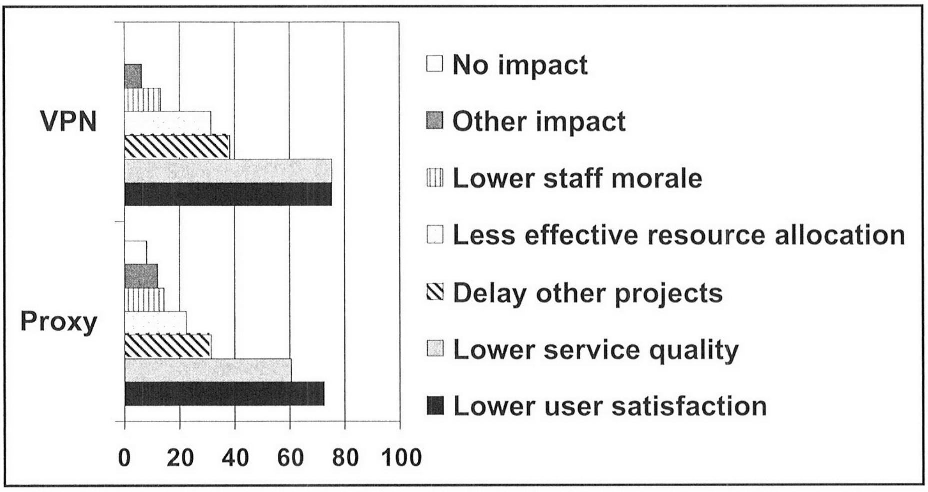

Figure 5. Percentage of institutions reporting negative impacts from proxy server and VPN technologies.

Library Staff Satisfaction

Most institutions (64 percent) running a proxy server indicated that they are always or usually satisfied with the service. Almost a third (32 percent) are less pleased with the service, and some (5 percent) are routinely dissatisfied with their proxy server. In contrast, no VPN sites expressed routine dissatisfaction with the service, perhaps because the libraries are not responsible for fixing the problems or because optimism about a new service prevails while the kinks are being worked out. See figure 6.

The level of staff satisfaction with their proxy server is bewildering, given that most proxy server sites reported a routine investment of time and money in providing a service that continues to have daily or weekly problems that lower user satisfaction and service quality. The connection between problem frequency and staff satisfaction is unclear. For example, 46 percent of the institutions running Ezproxy reported daily or

Table 3

Percentage of institutions reporting negative impacts from proxy servers and VPNs.

	Proxy server	VPN
Lower user satisfaction	72%	75%
Lower service quality	60%	75%
Delays in other projects	31%	38%
Less effective allocation of resources	22%	31%
Lower staff morale	14%	13%
Other negative impacts	12%	6%
No negative impacts	8%	0%

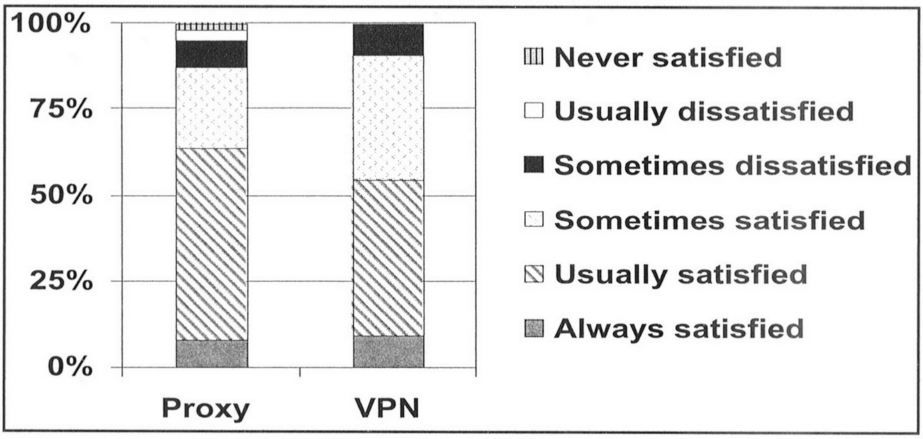

Figure 6. Library staff satisfaction with proxy servers and VPNs.

weekly problems with their proxy server, but 88 percent of them indicated that they were always or usually satisfied with their proxy server. Several respondents commented that though proxy server problems were frequent, most were easy to solve and the disruptions they caused were minor—comments that don't seem to match the survey data on the negative impacts of the proxy server on users and library operations. Another explanation could be that the library staff who answered the survey question about staff satisfaction were not the staff responsible for troubleshooting and fixing the problems or the staff who calculated the time and money invested in the service.

Motivations to Change to a New Technology

In descending order of importance, survey respondents confirmed the following as critical path requirements for changing to a new technology:

- Confidence that the new technology will be an improvement (77 percent)
- Many vendors adopt the new technology (56 percent)
- Time to implement the technology (52 percent)
- A rapid and transparent transition path to the new technology (49 percent)
- Money to implement the technology (49 percent)
- Documentation on how to implement the technology (42 percent)
- Personnel to implement the technology (42 percent)
- Technical training to implement the technology (32 percent)
- Personnel to train users to use the technology (28 percent)

Some respondents commented that *all* vendors must adopt the new technology before their library would adopt a new technology. Others commented that the new technology must be so easy to use that no user training will be required. Ideally the new technology will not require users to configure their computer or their web browser, and it must integrate with existing campus authentication and authorization services. Additional comments indicate that the new technology must be simple, stable, robust, and at least as easy for users to use and technicians to implement and maintain as current proxy server or VPN software. The approval of central computing organizations and library users were also mentioned as important conditions for migrating to a new technology. Several respondents explained that they were currently in the process of implementing a new technology—either changing proxy server software or testing VPN—so another new technology was unlikely to capture their interest or enthusiasm. Despite the costs incurred or the negative impacts of currently deployed technologies on library users and resources, with the exception of those already engaged in transitioning to a new technology, comments indicated that the respondents' level of dissatisfaction with their current proxy server or VPN was insufficient to motivate change.

Conclusions

From the perspective of library operations and staffing, if we consider that a dependable service requires 10 percent of a person's time to support and maintain, the survey results suggest that most proxy server and VPN implementations are dependable. From the users' perspective, however, this appears not to be the case. Evidence from the research reports bulleted at the beginning of this article clearly indicates that libraries are not meeting user needs and expectations for easy, convenient access to information. Admittedly, problems with proxy servers and VPNs alone do not account for user dissatisfaction. Difficulties encountered trying to navigate library web sites and to use online library resources (once they are discovered and accessed) in effect encourage users to turn to Internet search engines to satisfy their daily information needs. But the increasing likelihood that library users or potential users are off campus, and their reported preference for remote access to information, bring proxy server and VPN problems into the foreground. From the users' perspective, at best these technologies are a barrier to access; at worst they are unreliable. If the ultimate goal is use of quality resources by the academic community—use of the resources that libraries pay so dearly for—there is reason for concern, particularly with undergraduate students. Much work remains to be done to lead these students to quality resources, chief among which is finding a more reliable technology to support remote access. Recapping the data here will highlight the urgency of the problem:

- 68 percent to 90 percent (Outsell and OCLC studies respectively) of undergraduates access information from their residence.
- Undergraduate students spend 47 percent of their study time in their residence, 34 percent in the library (Outsell).
- 69 percent of undergraduate students live off campus, and 59 percent of them use their home computer more than computers at school (Pew study).
- 78 percent of undergraduates prefer remote access (OCLC).
- 73 percent use the Internet more than the library (Pew). They turn to an Internet search engine first when they need information (OCLC and EDNER studies).
- 96 percent of undergraduates believe the information they find using Internet search engines is good enough for class assignments (OCLC).
- 46 percent believe that other sites have better information than the library web site (OCLC).
- 46 percent believe that the technology provided by the library is far more critical to their academic success than the content provided (Dieter Schönwetter).
- To undergraduate students, the amount of time and effort required to find information is more important that the relevance of the information found (EDNER).

While faculty and graduate students are more likely than undergraduates to turn to library resources rather than an Internet search engine to find information for their academic work, they too work remotely, from off campus. According to the Outsell study, 50 percent of graduate students and 39 percent of faculty work at home. Graduate students report that 26 percent of their academic work is done at home. Faculty report that 11 percent of their work is done at home. These users also encounter the problems—experience the unreliability—reported in the current survey of proxy server and VPN technologies. Recent focus groups with students and faculty at Carnegie Mellon indicate that the unreliability of the proxy server is their primary problem and the source of their dissatisfaction with (remote) access to library resources. Some of them reported that they were so frustrated with using the proxy server that they "gave up on it."[13] Clearly current technologies designed and implemented to support remote access are not enabling users to be as self-sufficient as they want to be.

The bottom line is that a seemingly dependable service, from the library perspective, is not a quality service from the user perspective. The current survey suggests that, though proxy server and VPN technologies are routinely problematic and disruptive, libraries are sufficiently satisfied to stay the course. What is required to overcome the inertia of maintaining the status quo is a widely adopted technology proven to be easy to implement, integrate, maintain, and use. The situation appears to be a "catch 22," a chicken-and-egg problem, a tautology: libraries won't adopt a new technology unless or until it's widely adopted. Libraries take their lead from vendors. They implement technologies that match what their preferred vendors have in place to ensure user access to needed electronic resources. Vendors take their lead from libraries. They implement technologies that match what's in place in their current or potential customer base of libraries. We appear to be stalled, complacent, unmoved, and unmovable.

Our users are not stalled or complacent. The technologies libraries have deployed to fill the gap between vendor and user practice do not meet their needs and expectations. The overall LibQUAL+ scores from spring 2002 indicate that we are not providing our users with easy, convenient—which increasingly means remote—access to electronic library resources. Just as libraries need to contain costs, so do library users. They have accounts with different ISPs and use different technologies to connect to the Internet based on what's affordable and available in their area. They expect these technologies to enable remote access to library resources.

If academic librarians are genuinely as concerned as we claim to be about customer service in the support of research and education, how can we be complacent? If we are aware that most undergraduate students and many of our faculty and graduate students prefer online information and do much of their academic work off campus, if we know that the technologies they use for Internet connectivity (for example, cable modems, DSL, ISPs) do not interact well with proxy servers and VPNs, if we are truly concerned about undergraduate student use of resources on the surface web and their preference for easy-to-find rather than appropriate and relevant information, how can we be sufficiently satisfied and insufficiently motivated to change what we're doing? How can we be satisfied with annually allocating human and financial resources to a service that users aren't satisfied with and that causes delays in other library projects, presumably projects that will serve our users? Surely services that frustrate users and don't reliably support their priorities and preferences warrant our serious attention.

Next Steps

Where do we go from here? There are technologies emerging that are easier to use and provide more robust security than proxy servers and VPNs. Some vendors and academic libraries have experimented with Public Key Infrastructure (PKI). PKI is a combination of software, encryption technologies, and services that protect the security of Internet communications and transactions. PKI integrates public key cryptography, digital certificates, and certificate authorities to confidently validate (authenticate) the identity of Internet users and servers, authorize and control access to Internet resources and services, and both ensure the privacy and verify the integrity of the messages or documents "signed" by the certificate. Here's how it works: Upon request, a Certificate Authority (CA) provides a user with an encrypted digital certificate containing the user's public key and identity information. The CA's public key is publicly available. A service or content provider who receives an encrypted request uses the CA's public key to decrypt the user's digital certificate, which is attached to the request. Obtaining the user's public key and identity information from the certificate, the service or content provider can then send the user an encrypted message or document that only that user can decrypt. No user IDs or passwords are needed to accomplish the secure transaction.[14] Though the solution seems straightforward, after several years in the marketplace, PKI technology has not been widely tried and adopted in the academic community. One reason might be because digital certificates are tied to particular hardware devices. Academic users are likely to use different computers—including computers in libraries and other public computing facilities where their digital certificate will not reside. Another reason could be the cost of implementing PKI. For example, Dartmouth College invested $50,000 to implement PKI just to authenticate digital signatures for electronic payroll authorization. They expect campus-wide expansion of PKI, including using it as a substitute for IP address checking to control access to licensed library resources, to cost as much as $500,000.[15]

A more recent potential solution to the problem of providing secure access to restricted resources and filling the gap between vendor and user practice is Shibboleth. Shibboleth offers a comprehensive, flexible, affordable, easy to use and implement architecture, technology, and policy structure for authenticating users and controlling access to Internet resources and services. Shibboleth is an Internet2 project developing and testing software to support cross-domain or inter-organizational web authentication and access control. The beauty of Shibboleth, from the users' and academic institutions' perspective, is that it uses the campus's local authentication system to verify the identity of users: no need to remember different user IDs or passwords or worry about the IP address of the computer. From the content providers' perspective, Shibboleth provides secure access and keeps access control in their hands. The academic institution authenticates the user. The content provider determines whether that user gets access to their resources and services.[16]

A more recent potential solution to the problem of providing secure access to restricted resources and filling the gap between vendor and user practice is Shibboleth.

Shibboleth provides a general solution to the problem of authentication and authorization by not requiring the exchange of any specific credentials about the user. These remain negotiable. For example, academic libraries can negotiate with commercial vendors to provide access to all of their students, faculty, and staff; the credentials that Shibboleth will provide to the vendor need only verify that the person is currently a member of the campus community. Alternatively, a professor can restrict access to course materials to only students in her class, in which case the credentials that Shibboleth will provide will verify that the person is currently a student in that particular class. Shibboleth enables different attributes about the user to be released to different content providers based on negotiated access control policies.

What does Shibboleth require? Campus computing organizations need to adopt an enterprise-wide approach to authentication, directory, and web-based services, and they need to implement a component of Shibboleth that integrates with these services. Vendors and other content providers need to implement a component of Shibboleth that queries the campus authentication service to ensure that users are affiliated with the institution. Integration with the campus directory service will enable institutions to provide content providers with more information about their users than just their institutional affiliation, for example, their status as faculty or student or their registration in a particular course. This information will help content providers assess usage patterns and develop information resources and services better suited to their user communities.

Academic institutions need to have campus-wide authentication, directory, and single sign-on service to use Shibboleth effectively. To assess the technical readiness—not the motivational readiness—of campuses to implement Shibboleth, the final questions in the survey I conducted asked whether the institution had or was implementing a Lightweight Directory Application Protocol (LDAP) or a Single Sign On (SSO) system. (The survey assumed that academic institutions had some kind of authentication service like Kerberos.)

In the context of Shibboleth, LDAP is needed to provide the attributes for policing access control. LDAP began as a standard, open protocol or access method for applications to "talk" to directories. It later expanded to include the hierarchical directory structure and service itself. An LDAP directory is a repository of user and group information. Each user or group has an entry in the directory, with associated attributes.[17] For example, a user entry might include the user's name, email address, status, department, etc. A group entry might include the names and contact information for all the members of the group. Authentication services contact the LDAP service to get user or group information needed for access control or other security purposes.[18] Although not yet widely implemented, LDAP eventually should make it possible for almost any application running on virtually any computer platform to obtain directory information.[19]

Single Sign On (SSO) service is an authentication process that enables users to enter their user ID and password once to get access to multiple web-based applications or resources rather than having to enter their ID and password every time they change applications or resources.[20] Though not technically required for Shibboleth, neither users nor content providers will see Shibboleth as progress over IP address restriction if people have to authenticate every time they want to access a restricted web application or resource.

Some survey respondents indicated that they did not know whether their institution had or was implementing LDAP or SSO. A few respondents skipped these questions. Nevertheless, at least 80 percent of the institutions that completed the survey currently have or are implementing an LDAP directory, and at least 72 percent have or are implementing an SSO. Not surprisingly, more universities than colleges have or are implementing LDAP (94 percent compared with 67 percent) and SSO (85 percent compared with 61 percent). The news bodes well that much of the academic computing environment is technically ready for Shibboleth. What remains to be instigated is the motivational readiness, which depends in large part on the results of the Shibboleth beta test currently underway and what commercial vendors choose to do. Several commercial vendors and academic libraries are beta testing Shibboleth now. Four countries in Europe have expressed interest in testing Shibboleth at a national level.[21] A successful beta test will spread the word and hopefully instill the requisite confidence that Shibboleth is a significant improvement over proxy server and VPN technologies.

Users, campuses, and vendors have different, overlapping needs. Academic users want to be able to use any computer to do their work—a computer at their office, their home or residence, in the library, or some other campus computing facility. They want to login only once (per day per machine) using their campus user ID and password to get access to all restricted web-based resources and services that they are authorized to use. They don't want to have to install any software or configure their browser, their computer, or their network. Campuses, commercial vendors, and other information providers want good security, satisfied users, and useful data about their users. Shibboleth has the potential to satisfy all of these needs.

Shibboleth is relative easy and inexpensive for campuses and vendors to implement. The Shibboleth development team provides documentation and support. Users need no additional training once they are familiar with their campus's single sign-on system. The transition can be rapid and transparent if and only if both campuses and vendors take the step to implement their Shibboleth component. I urge librarians to learn more about Shibboleth, and to encourage their campus and their vendors to participate in the beta test. Let the vendors know that the IP-address restriction they currently provide is woefully inadequate to meet, not just the needs of libraries and library users, but their own needs for security and information about their users.

Denise Troll Covey is Associate Dean of University Libraries at Carnegie Mellon University; she may be contacted via email at: troll@andrew.cmu.edu.

Notes

1. Having enough time to do their work was their number one problem, followed by knowing what resources are available. Amy Friedlander, "Dimensions and Use of the Scholarly Information Environment: Introduction to a Data Set" (November 2002). Available: <http://www.clir.org/pubs/reports/pub110/contents.html> [September 15, 2003].
2. Steve Jones and Mary Madden, "The Internet Goes to College: How Students Are Living in the Future with Today's Technology," Pew Internet & American Life Project Report (September 15, 2002). Available: <http://www.pewinternet.org/reports/toc.asp?Report=71> [September 15, 2003].
3. OCLC White Paper on the Information Habits of College Students, "How Academic Librarians Can Influence Students' Web-Based Information Choices" (June 2002). Available: <http://www.oclc.org/services/brochures/informationhabits.pdf> [September 16, 2003].
4. "How students search: Information seeking and electronic resource use," EDNER [Formative Evaluation of the Distributed National Electronic Resource] Project, Issues Paper 8 (2002). Available: <http://www.cerlim.ac.uk/edner/ip/ip08.rtf> [September 15, 2003].
5. Steve Lawrence and Lee Giles, "Accessibility and Distribution of Information on the Web." *Nature* 400 (1999): 107–109. Summary available: <http://www.wwwmetrics.com> [September 15, 2003].
6. Campbell, Michner, and Lee, "Technology and Student Success in Higher Education: A Research Study on Faculty Perceptions of Technology and Student Success" (Toronto: McGraw-Hill Ryerson, Ltd., 2002). Order information for 4th edition (press release, June 10, 2003): <http://www.mcgrawhill.ca/highereducation/administrators/research.php> [September 15, 2003].
7. Dieter Schönwetter, "Student Perception of Learning Success with Technology" (University of Manitoba, 2002). Order information for 4th edition (press release, June 10, 2003): <http://

www.mcgrawhill.ca/highereducation/administrators/research.php> [September 15, 2003].

8. F. C. Johnson, J. R. Griffiths, and R. J. Hartley, "DEVISE: A framework for the evaluation of Internet search engines," Library and Information Commission Research Report 100 (2001). Available: <http://www.mmu.ac.uk/h-ss/cerlim/projects/devise/devise-report.pdf> [September 15, 2003].
9. Addison Ching, "Internet Access Control Using Proxy Servers," *The DataBus* 36, 1 (December 1995–January 1996). Available: <http://www.cedpa-k12.org/databus-issues/v36n1/proxy.html> [September 15, 2003].
10. Jeff Tyson, "How Virtual Private Networks Work," in *HowStuffWorks* (n.d.). Available: <http://computer.howstuffworks.com/vpn.htm> [September 15, 2003].
11. Dan Carnevale, "Security Lapses on Campuses Permit Theft From JSTOR Database," *The Chronicle of Higher Education* (December 12, 2002). Available: <http://chronicle.com/free/2002/12/2002121201t.htm> [September 15, 2003].
12. D. A. Nitecki, "Assessment of Service Quality in Academic Libraries: Focus on the Applicability of SERVQUAL," *Proceedings of the 2nd Northumbria International Conference on Performance Measurement in Libraries and Information Services* (Newcastle on Tyne, England: Department of Information and Library Management, University of Northumbria at Newcastle, 1998), 181–196.
13. Carole A. George, "A Study of Independent Access to Library Resources" (May 13, 2003). Available: <http://www.library.cmu.edu/Libraries/LibQualPersonalControl.pdf> [September 15, 2003].
14. "Understanding PKI." Available: <http://verisign.netscape.com/security/pki/understanding.html> [September 15, 2003]. See also <http://www.webopedia.com/TERM/D/digital_certificate.html> [September 15, 2003].
15. Tom Warger, "Get Real," *University Business*. Available: <http://www.universitybusiness.com/page.cfm?id=152> [September 15, 2003].
16. Phil Becker, "Shibboleth: Identity the Internet Way," *Digital Identity World* (August 5, 2002). Available: <http://www.digitalidworld.com/article.php?id=90> [September 15, 2003].
17. Alan Frank, "Lightweight Directory Access Protocol," *Network Magazine* (January 1, 1998). Available: <http://www.networkmagazine.com/article/NMG20000727S0003> [September 15, 2003].
18. "Lightweight Directory Access Protocol (LDAP) is a user registry in which authentication is performed using an LDAP binding." Available: <http://publib7b.boulder.ibm.com/wasinfo1/en/info/aes/ae/csec_ldap.html> [September 15, 2003].
19. See <http://www.webopedia.com/TERM/L/LDAP.html> [September 15, 2003].
20. See <http://www.webopedia.com/TERM/s/single_signon.html> [September 15, 2003].
21. Becker.