

**The Response of University IT Departments to Peer-to-Peer File Sharing
Technologies**

Prepared by

Jason G. Caudill

PhD Student in Instructional Technology

The University of Tennessee, Knoxville

A 535 Claxton Addition

Knoxville, TN 37996-3456

Abstract

As peer-to-peer (P2P) networking applications exploded in popularity one of the groups most immediately and significantly impacted was the university campus. Population demographics, hardware availability, and broadband network access combined to create large communities of P2P application users. This use was responsible for massive increases in bandwidth usage and a related loss of network availability. Network administrators and other university officials face a challenge in how to best approach the problem and ensure that campus networks are available for legitimate academic use. Implemented solutions and possible future paths will be detailed and examined in relation to the policy environment.

One of the most serious network management issues to develop for campus administrators in recent years is that of peer-to-peer (P2P) networking. From bandwidth to security to issues of usability the control of P2P networking on a campus is essential to stable operations. As bandwidth use increases, service failures can occur for users on the network. Security issues threaten everyone connected to the network, and in public lab environments, it is critical to weigh increased user security against decreased user functionality.

Security Threats

Because of the potential of service failures, many universities are taking steps to address P2P applications on their campuses. As early as 2000, universities were taking steps to block P2P access over their networks. Vanderbilt University established a policy on March 28, 2000 to block outgoing Napster traffic from 8AM to midnight on weekdays. This step was taken because, according to Vanderbilt's Academic Computing and Information Services, "Despite aggressive increases in bandwidth, Vanderbilt's connection to the Internet continually approaches maximum capacity. To allow teaching, learning and research to continue without hindrance, measures need to be taken to alleviate this problem" (Vanderbilt University, 2002). In the fall semester of 2001, Penn State University established bandwidth quotas for residence hall students that automatically monitored usage and issued warnings to students exceeding their limits. Much like Vanderbilt, Penn State expressed their need for such a system. "Heavy downloads by individuals using software such as Napster and MP3.com were making it increasingly difficult for University users to access and effectively use the Internet to

support their class work and research efforts, according to Gary Augustson, vice provost for information technology. ‘Uninterrupted network access is extremely critical for Penn State to carry out its mission today,’ Augustson said. ‘The need to ensure that this critical resource is available to support legitimate academic interests prompted the University's immediate response to the issue’” (Penn State Intercom, 2001). Radford University simply limits the percentage of bandwidth available to P2P applications through on-campus connections. Out of a total of 55 megabits of bandwidth available to the university in 2002, no more than 10 megabits may be used at any time for P2P applications (Oakes, E., 2002). Obviously, there are a variety of responses to deal with the bandwidth problem, but just as obvious is the importance of addressing the problem. In conjunction with the bandwidth problems, there are also concerns about virus transmission over these networks.

Because P2P networks open individual computer systems to other users searching, downloading, and uploading files to and from those systems there is considerable risk of malicious users utilizing the data transfer for the purpose of virus transmission. This risk is considerable for individual users, but is compounded when the infected files have the potential to be transferred to multiple other users across a university, national, or even international network of P2P users. Along with the interruption of bandwidth, the risk of security violations has been recognized by university information technology departments and many of them are taking steps to address the problem. The University of Winnipeg has identified several different security concerns based on P2P networking through their own observations. First of all, there have been documented instances of file sharing programs automatically installing

spyware, which is a type of program that monitors and reports user activity such as the files they access. Also, users themselves are contributing to the security problem by inadvertently sharing data on their systems that does not need to be accessible to external users. Examples of this found in University of Winnipeg experimentation include Windows system files and even entire hard drives (University of Winnipeg, no date). Saint Louis University identified that Brilliant Digital Entertainment's software will allow Brilliant to basically commandeer your computer's unused processing power to help with other companies' complicated computing tasks. The primary objection of the university to this technology is that individual users are "authorizing use of a resource that you do not own – the University's bandwidth – for commercial use. This is a violation of University policy" (The Inside Guide to Saint Louis University, 2002.) For many reasons, P2P networks are a threat to user and university security. While there are few alternatives to protect users from these security threats short of termination of access, education of users, with Saint Louis University's site as an example, can help to inform users of how best to protect themselves.

The final, and for network administrators, most disturbing aspect of file sharing security threats is that of a denial of service attack. A denial of service attack is a malicious computer worm that generates large amounts of network traffic with the intent of crippling the network by overwhelming the network's bandwidth. Because there is such a high volume of traffic via P2P networks as a part of their normal operation, it can be relatively easy for a well-constructed attack to be hidden in that traffic (Wagner, A., no date). Once a virus enters a network it can be extremely difficult to control and remove. Early in the fall semester of 2003 the University of Tennessee suffered severe

service interruptions because of the worm attacks that spread internationally infecting Windows machines. After a period of time, the network services department actually had to deny service to some ports, thus denying the users internet access, because their machines had not been cleared of the virus and were posing a continuing threat to the network at large. Given the time and resources it requires to fight and defeat an infection of this type, it is obvious why organizations want to do their best to remove the possibility of an application actively opening the door for such a virus to enter a network.

Policy Implementation

Given the expansive and complicated policy landscape involved in university network administration and the use of P2P technology by students many different factors impact the possible implementation of new policy. Of particular interest are the belief systems behind the policy, organizational structure, implementation and evaluation of the policy, how and if the institution will be improved, and perhaps key to this policy in particular, the question of who will reap the benefits.

The beliefs involved in securing P2P technology are varied and conflicting. Students and other users of file sharing believe they have a right to access entertainment without paying what they consider to be exorbitant prices, and also that once they have acquired music, it is theirs to do with as they please, in particular theirs to post and share with friends and other people via the internet.

Directly related to the beliefs of the students is how the beliefs of institutions of higher education impact the policy. Like every organization, colleges and universities have a vested interest in the efficient operation of their processes. As discussed earlier, file sharing often slows university networks and impedes students and others from

accessing necessary resources such as e-mail and online research materials. For this reason, universities would like to see P2P networking at least reduced, if not eliminated. At the same time, however, institutions have an interest in seeing their students safe and protected. This safety includes a student's privacy, which could easily be violated through improperly shared folders. Given these constraints, universities are understandably concerned about exactly where their rights begin and end with respect to controlling what students do online. While there have been no 1st Amendment arguments posted against institutions for limiting network access to certain services, they may very well be coming, and if they do, yet another concern will be added to compound the belief systems underlying university policy.

In implementing a policy regarding P2P networking, there are some very useful advantages and some unusual limitations on universities. As the question largely concerns file-sharing traffic over an institution's own network a university has the advantage of controlling the physical infrastructure and technical controls over the medium in question. At the same time, given the legitimate uses of P2P technology for the exchange of information for research purposes and other applications, a blanket elimination of P2P access would be detrimental to the institution and its students, as well as to its administration and faculty. Additionally, any implementation beyond a local level would be very difficult due to the vast differences that may be found between campuses in what kind of hardware and software is being used to operate the institution's network. Beyond that, sometimes even a single campus can have multiple networks operating different hardware and backed by different types of server software. Because of this, any policy will have to be based on broad definitions of what will or will not be

allowed rather than specific prescriptions for how to implement the enforcement of those restrictions.

Having established the structure of the organization in which the policy must be implemented the means of actually implementing and evaluating the policy must follow. Of primary importance will be establishing who has the authority to mandate the change. Many organizations face the problem of divisions trying to do what they want to do and hoping to escape the notice of top management who established the policy. In technology, however, the scope of the problem expands exponentially. Because of the highly specialized nature of the field and the rapid and constant change it endures, managers are often unable to observe for themselves how things are being done, if in fact they are being done at all. Cases exist of low-level administrators operating their own file-sharing servers on university systems with no knowledge of management. Given this situation, it is imperative that when the policy is implemented there are people with both the authority and the knowledge to ensure that the implementation is executed appropriately.

Once implemented, there is the added problem of evaluation. The key difficulty is the question of how do you evaluate the absence of something? Given perfect execution of a policy eliminating P2P networking on a campus, no files would be uploaded or downloaded via the institution's network. The problem is if the policy countered existing methods of file sharing, how will it become apparent that people have successfully circumvented the controls with technology not necessarily addressed by the initial policy implementation? Answering this technical problem will be essential to effective evaluation of policy.

Closely related to evaluation of the policy is the question of whether or not an institution will be improved by establishing a policy that limits or eliminates illegal file sharing over the university's network. Presumably, the increased availability of bandwidth to users of the network will be an improvement to the system. Coupled closely with the improvements, however, is the underlying threat that in order to control the P2P networking and increase bandwidth availability it will be necessary to monitor network usage. There are certainly issues of privacy which are beyond the scope of this paper involved in monitoring internet usage and network activity of students, but what is almost certain is that students, and faculty perhaps more so, will object to and resent the oversight. Such unrest is certainly not good for an organization. Generally, in the study of industrial-organizational psychology, it is recognized that disgruntled group members are less productive, and over time can even be less healthy than satisfied members of the same group structure. The question then becomes what the scope of the possible damage is as opposed to the benefit of a P2P policy.

The basic issue for an organization administering computer labs open to use by the student body and other individuals affiliated with the institution is the sliding scale between improving security, in this case the inability to install and execute P2P applications, and usability, that being the flexibility of a computer system to allow users to install and execute custom applications or other features useful in the tasks they want to perform. Most of the examples below are taken from standard procedures at the University of Tennessee, Knoxville, but based on exchanges on information technology message boards many of the practices are representative of what is being done at comparable institutions across the country.

Computer Lab Controls

In public computer labs the controls placed on machines are largely a function of permission settings within the computer's operating system. As one example, many of the applications for P2P file sharing install by default to the C:/ drive, the main hard drive partition, of a computer. As part of the settings on a computer, it is possible to remove user control of the C:/ drive, meaning that they are unable to save information to it or install programs to that location. By doing this, it makes it impossible for many of the popular P2P applications to be installed on a computer. If the software can not be installed, then it obviously can not be used, and as a result files can not be illegally shared over the network the machine in question is connected to. Closely linked to this security feature is the option to designate a hard drive partition on the machine with permissions for a user to write and read data, but not execute programs. This allows a user to save files and access them at a later time but does not allow them to execute programs from that location. In labs on the University of Tennessee, Knoxville campus this partition is labeled as the D:/ drive. Doing this retains some measure of utility for the user, but also provides a second level of security against users installing unwanted programs on university computers. Also, many times the desktop environment is locked to prevent users from altering the system's appearance or executing programs from links they download or place on the desktop of the machine.

While it is difficult, there are methods to defeat these and other security measures placed on machines. In the case of many of the security settings detailed above, accounts designated as administrators do have access to the features that are not available to regular users. In the event that an administrator account is compromised or someone is

able to use security-cracking software to determine the administrator user name and password for a machine then that user will be able to install and execute applications on the machine. The reason the administrator accounts exist, and must exist, is the necessity for the employees responsible for the well-being of the machines to do work and at times install updates and requested software that require access to functions that are locked out for normal users. The problem, simply, is that if it is possible to design a security feature or piece of security software, it is possible to write another piece of software capable of defeating it

One of the reasons these methods for defeating security features exist is that while more security makes the job of a system administrator easier, it makes the user environment much less appealing. Many disciplines, with engineering being a prime example, make use of software packages that are available to anyone for free. Packages of this type are licensed as freeware whereby it is not only legal, but encouraged, for people to download and use the software at any time. If a class wants to utilize a piece of software like this, a student must use a personally owned computer to do it because it is not possible to install and execute the software from a lab machine. Basically, it is not possible to make a computer understand what is good software and what is bad software and have it allow installation of one but not the other. Also, many presentation and graphical programs look for additional features like fonts and templates in files that are located by default on the C:/ drive. Without permissions to write to the C:/ drive, users are unable to use additional features they may have downloaded from a legitimate website like the office page on Microsoft.com.

Non-Lab Computer Controls

Outside of the lab environment it becomes much more difficult to control what a person does with a computer on the university's network. Obviously, the information technology department of an institution cannot lock people out of having full control of their own computers. Because of this, there is no way to control what a person does or does not install on their own personal machine. For those machines connected to a network, however, it is possible to monitor bandwidth usage and network activity. The extent to which activity is monitored is a question that must be answered by each individual organization, but the monitoring process is possible and can be used to somewhat control file sharing activity. As a basic example, if a computer connected to a certain point in university student housing shows a spike of extremely high bandwidth usage, it may generate cause to examine the traffic through that port. If the traffic is identified as file sharing through a controlled application, the student can be warned, or in more extreme cases, the network connectivity of that port can be removed, thus eliminating the user's access to file sharing over the university's network. This is obviously a much less controlled and less effective method of control than what is possible on machines owned by the university, but it does give network administrators some level of supervision to control bandwidth waste and file sharing.

Further complicating the control of P2P technology on campus is the fact that while much of the traffic through these types of applications is for purposes of illegal trading of copyrighted works, there are also extensive legal, and even positive uses of the technology. Government and business uses are being developed for P2P networking technology, as are legitimate personal uses.

Legal Uses of P2P Networking

The U.S. government is working to utilize P2P networking to provide public access to governmentally compiled data (Vance, A., 2001). In addition to supplying data more quickly to the public, the system also enables the agencies participating in the program to more quickly exchange information with each other. A major advantage to the system is that instead of having to design, build, and then maintain a central server for information and the numerous workstation connections to that server, the P2P system allows regular desktop machines across the agencies to connect directly to each other with no need for a centralized data storage location. The developer of the software, NextPage, states that in addition to the government system, the software has been adopted by legal, banking, accounting, and insurance practices.

Beyond data exchange, business uses for P2P are growing. The technology has the ability to allow users to collaborate live time from different physical locations using instant messaging capabilities (Rutherford, E., 2000). Additionally, it is possible to use the same type of technology to share processing power between systems. Instead of investing new funds into more powerful computers for the purpose of processing large amounts of data, P2P can utilize unused processing power across a broad network of machines (Fox, P., 2001).

Finally, P2P uses are expanding outside of government and business applications to practical, legal, personal uses. The originators of Kazaa, one of the most widely used file sharing applications, have released a test version of new software called Skype. The program enables users to speak to each other over internet connections live time, much the same as a telephone conversation. While there are other applications, generally

termed telephony, which will allow users to perform the same operation, Skype utilizes P2P advances to make it possible for the program to be used in a variety of environments that are not accessible by other programs (Libbenga, J., 2003).

Considering the many factors involved in administration of networks with respect to P2P networking, it is clear how difficult it can be to manage a large, multi-user network. At the local level on campus at the University of Tennessee, there are many actions already underway to prevent illegal use of these applications. Even more extensive measures are possible, and the implications of both existing and future applications are being examined.

University of Tennessee Computer Practices

There are two different areas of concern for the information technology groups at the University of Tennessee; the computers in public laboratories and the privately owned machines connecting to the university network through on-campus housing. Measures being taken on each front will be examined, with lab machines being more locally controlled and private machines being administrated via network controls.

In computer labs maintained by the lab services group of the office of information technology, several layers of security exist to defeat file sharing. The permission settings on the machines have been discussed in an earlier section, and are a key component of defeating P2P technology. In addition to the permission settings, a security program called DeepFreeze is installed on all of the machines. DeepFreeze functions by recording an image of everything on the computer when it is installed. Any changes made by users are written to a virtual partition, which is deleted on restart, thus restoring the machine to its original state. A partition of the hard drive, the D:/ drive, is removed from

DeepFreeze to allow a safe place for users to save their documents, but as mentioned before, it is not possible to execute programs from that drive, so there is no need relating to P2P applications for files on the D:/ drive to be removed on restart. Also, DeepFreeze automatically restarts after one hour of idle time for the machine, so even if a user finds a machine in an unstaffed area to operate on, the machine will restart itself and delete any changes made after a one hour idle time, thus providing security for the machine even when lab services does not have a person available to restart the machines and reset DeepFreeze. In addition to security software, all lab machines require users to log in with a unique username and password. This not only helps to safeguard a user's privacy, but also provides a trail in the event a user successfully defeats other security measures and performs file-sharing work from a lab computer.

A key factor in enforcing network activity from personal machines located on campus is the section of the UT computing code, which specifies, "University IT resources are for use in conducting authorized University business. Using these resources for personal gain or illegal or obscene activities is prohibited" (Office of Information Technology, 2003). By monitoring bandwidth usage through university supplied network ports in on-campus student housing it is possible to identify excessive traffic and examine records of what material was contained in that traffic. If it becomes apparent that a student has been making use of file sharing technology on the university network, they are sent a warning and details of the university's acceptable use policy. In cases of repeat offenses or extreme abuse, a student's network connectivity can be removed. While this system is far from being as effective as the lab procedures, it does work to identify and remove the worst violators of the policy.

Security Measures and System Usability

For all of the current and possible future actions, the primary implication that is always considered is the usability of the system. The overall goal of the system and network administrators is to provide access to information technology resources for academic use. The security features implemented thus far in the labs have somewhat decreased the flexibility of the machines to be used for some applications requiring downloaded programs or plug-ins, but over the course of time the reduction in problems resulting from these security features more than outweighs any loss of utility. In the case of the limited network monitoring of residents' computers, the elimination of what are colloquially referred to as bandwidth hogs speeds up network access and increases utility for everyone on the network. Given these positive results, activities undertaken to this date appear to meet, if not exceed, all stated goals of the organization.

Moving beyond the local level, there are questions of what can be implemented on a national scale to combat the problem of file sharing and the related legal threat posed to universities and their students. There are definitely some actions that can be undertaken to combat the problem on a nation-wide scale from within the information technology departments of higher education institutions. It is important to remember, however, that all possible implementations of blanket policy must be tested against the physical limitations of such actions. Due to the very nature of the field, there are significant obstacles to standardization that may not be present in other fields of policy.

To actively pursue changes, a national program to enact stricter security controls on computers on every campus of higher education could work in concert with improved education about the issue to further reduce illegal traffic. While UT and many other

campuses are working on a constant basis to improve security of their computer systems many other institutions are not. There are a variety of reasons, from lack of concern to simply a lack of available knowledge, but the end result of lax security procedures is almost always violated systems and illegal activity. To change this situation, a national policy, set by the government, would almost certainly be necessary. Given the financial troubles being faced in many states, any expansion of departments is unlikely to happen without significant encouragement in the form of law or government mandate. The legislation would by necessity have to be somewhat vague as to the method by which security was implemented, but it could very effectively frame the end result of the security efforts. By doing this, there would be reasonably uniform efforts nationwide to control the use of educational computer resources for illegal practices.

On the national scale, there are unique difficulties in setting standardized policy in information technology. While broadly worded legislation specifying that security measures should or must be implemented to prevent the piracy of copyrighted material over university networks, any more definition becomes very difficult. At the machine level, the two major operating systems are Windows and Mac. Each of these operating systems has its own software and unique functionality. Because of this, security software and features that work on one system will not necessarily work on another. At the network level, this is further complicated by a variety of different server software packages that may or may not be compatible with others. As a final complication, the Linux operating system is rapidly becoming more popular. This third system adds an entirely new dimension of complications to standardizing any policy. In order to

guarantee uniform security and anti-piracy policy, it will take not only legislation, but a concerted, concentrated effort by computer administrators at every institution.

Conclusion

The constant growth and change of technology makes not only establishing, but also maintaining, sufficient policy very difficult. In order to protect students, networks, and themselves, it is essential that institutions of higher education ensure that they stay educated about the legal and social environments of not only P2P file sharing, but also the new technologies for illegal copyright violations that will inevitably develop.

Bibliography

- Fox, P. 2001. Potential Uses Help Brighten Future of P2P. *Computerworld.com*. Retrieved 10/4/03 from <http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,58004,00.html>.
- Libbenga, J. 2003. After Filesharing: P2P Telephony. *The Register*. Retrieved 10/5/03 from <http://www.theregister.co.uk/content/5/32616.html>.
- Oakes, E. 2002. RU Slowing Down RU's Network?. *Radford University*. Retrieved 9/30/03 from <http://www.radford.edu/~acadcomp/NetworkSpeeds/Bandwidth.html>.
- Rutherford, E. 2000. The P2P Report. *Knowledge Management Research Center*. Retrieved 10/4/03 from http://www.cio.com/research/knowledge/edit/p2p_content.html#company.
- Vance, A. 2001. US Government Uses P2P to Share Data. *itworld.com*. Retrieved 9/27/03 from <http://www.itworld.com/Net/3409/IDG010420p2p/>.
- Wagner, A. no date. P2P Systems as Attack Platform for Distributed Denial-of-Service. *Computer Engineering and Networking Laboratory, ETH Zurich*. Retrieved 10/2/03 from <http://kisogawa.ethz.ch:8080/teaching/ss03/SPA/talks/intro/ges.pdf>.
- Wagner, A. no date. P2P Systems as Attack Platform for Distributed Denial-of-Service. *Computer Engineering and Networking Laboratory, ETH Zurich*. Retrieved 10/2/03 from <http://kisogawa.ethz.ch:8080/teaching/ss03/SPA/talks/intro/ges.pdf>.
2002. Download Could Steal University Bandwidth. *Inside Guide to Saint Louis University, The*. Retrieved 9/30/03 from <http://www.slu.edu/readstory/newslink/1101>.
2003. Acceptable Computing Use Policy. *Office of Information Technology*. Retrieved 10/5/03 from <http://oit.utk.edu/itp/>.
2001. Automated System to Manage University's Bandwidth. *Penn State Intercom*. Retrieved 9/30/03 from http://www.psu.edu/ur/archives/intercom_2001/Nov29/bandwidth.html.
- no date. P2P Software the Reality of Cool. *University of Winnipeg, The*. Retrieved 9/30/03 from <http://www.uwinnipeg.ca/web/faculty/admin/tsc/security/p2p.html>.
2000. Napster and University Bandwidth. *Vanderbilt University*. Retrieved 9/30/03 from <http://www.vanderbilt.edu/resnet/napster.html>.