

Implementing a Network Improvement Action Plan

Kim Todd
User Consultant
Client Computing
Northwest Missouri State Univ.
Maryville, MO 64468
660-562-1434
kdt@mail.nwmissouri.edu

Dr. Jon Rickman
Vice-President
Information Systems
Northwest Missouri State Univ.
Maryville, MO 64468
660-562-1134
rickman@mail.nwmissouri.edu

Tabatha Verbick
User Consultant
Client Computing
Northwest Missouri State Univ.
Maryville, MO 64468
660-562-1434
tab@mail.nwmissouri.edu

ABSTRACT

Firewall failures and the recent onslaught of computer viruses and worms, such as *Klez*, *loveletter*, *SoBig*, and *BadBoy*, increased network traffic and ever-growing network abuse, propelled security awareness at Northwest Missouri State University to a higher level and increased the need for finding and implementing effective solutions.

Northwest's *Information Systems Department* was able to build awareness of computer security issues, decrease network abuse, institute significant enhancements to the network and better ensure network reliability, through the implementation of a multiple step network action plan. This plan included the adoption of new policies and procedures, new student staff positions and equipment upgrades.

Categories and Subject Descriptors

- K.6.1 [Management of Computing and Information Systems]: Project and People Management
- K.6.2 [Management of Computing and Information Systems]: Installation Management
- K.6.4 [Management of Computing and Information Systems]: System Management
- K.6.5 [Management of Computing and Information Systems]: Security and Protection
- B.8.0 [Performance and Reliability]: General
- C.4 [Computer Systems Organization]: Performance of Systems
- C.5.0 [Computer System Implementation]: General
- C.5.5 [Computer System Implementation]: Servers
- K.3.0 [Computers and Education]: General
- K.4.1 [Computers and Society]: Public Policy Issues
- K.4.3 [Computers and Society]: Organizational Impacts

General Terms

Management, Security, Human Factors, Performance, Reliability

Keywords: Network Management, Customer Service, Communication, Network Stability.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS '04, October 10-13, 2004, Baltimore, Maryland, USA.
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

1. INTRODUCTION

Network reliability issues in spring 2003 at Northwest Missouri State University heightened the need to critically examine the campus network, specifically its firewall, which had proven inadequate to meet the demands placed upon it. Furthermore, concerns over continuous network traffic increases and a rise in network-based applications, as well as the prospect of attacks by new viruses and abuse by hackers, prompted the Information Systems Department to study how to improve network reliability. However, the investigation had to be conducted swiftly, because there was only a narrow window of opportunity for any upgrading due to the fast-approaching 2003 fall trimester. Consequently, any improvement plan needed to be developed and implemented in a two and a half month time frame, including the overall design deployment, the ordering of hardware and/or software, the hiring of additional staff and the evaluation of the action plan.

Following a two-week study, the Vice President of Information Systems approached the university's Board of Regents with a plan to deal with the multiple threats to the campus network's stability. The Board of Regents agreed to add one dollar to the campus technology fee, which is charged per credit hour, to fund any new hardware, software, staff and procedures that might be required. It was hoped that the Information Systems plan would resolve the many problems that had prevented effective usage of the network by campus users.

The 40-step network action plan was nearly complete in August 2003 when the university was hit with the equivalent of an Internet bombshell. If not for the action plan, the *Blaster* virus would have done just what its name implied and blasted Northwest's local area network and its World Wide Web (WWW) connection into a state of shutdown. However, with most of the network action plan completed, an acceptable level of service was maintained.

2. HISTORICAL PERSPECTIVE

Northwest Missouri State University implemented the first public university comprehensive networked campus in 1987 as an effort to better prepare its faculty, staff and more than 6,000 students for the emerging information-driven society. Northwest's Electronic Campus program provides networked computing stations in every residence hall room and faculty and administrative office.

In 1997, Northwest began issuing a personal notebook computer to all of its faculty members and added electronic classrooms with audio and video projection systems. In addition, Northwest upgraded the Electronic Campus by providing a networked personal computer in every residence hall room and all offices.

In the Fall 2005 trimester, as part of that on-going commitment to the Electronic Campus program, Information Systems will be providing university-owned notebook computers to every student living in campus housing.

One of the original key features of Northwest Missouri State University's Electronic Campus program was that every client station was networked. The campus's network connection to the world started at 56 kbps in the late seventies to support remote job batch entry computing and was increased to 1.5 Mbps in the early nineties to support WWW and email. The Missouri Research and Educational Network (MOREnet) provided Northwest with a 20 Mbps Internet connection in the late nineties. Currently, MOREnet provides the university with a 30 Mbps connection.

3. THE IMPETUS FOR CHANGE

One of the major challenges facing the Information Systems Department today is to provide a reliable Internet connection for academic and administrative services. Many of these services have recently been out-sourced to off-campus providers, such as the automated online library services and the digital periodical databases. The support of web enhancements to nearly every course was out-sourced by way of *eCompanion* at the following URL: <http://www.northwestonline.org>. The support of totally online web courses and degree programs was also entirely out-sourced to *eCollege.com*. Consequently, with the normal Internet activities, including web browsing and email, little bandwidth remained for "recreational" computing, such as, but not limited to, instant messaging, game consoles and file sharing.

Another challenge facing Information Systems was a direct result of the Electronic Campus program. As stated earlier in this paper, the program provided networked computers in every residence hall room and campus office. Because of this control over the computing equipment on campus, Information Systems had always maintained a high level of management over the majority of the software installed on computers operating on the Northwest network. Thus, computers had standardized software that included anti-virus software.

Because of homogeneous equipment and software, Northwest had for a long period of time enjoyed a relatively problem-free and reliable local area network and Internet connection. However, with the arrival of the new millennium and the rapid rise in personal computer ownership, students began to bring their own computing equipment onto campus with greater frequency. Some of the personally owned equipment brought to campus by students included wireless access points used to provide campus network access to their off-campus friends. Unfortunately, because of Information Systems' long history of only having to deal with university-owned computing equipment and software, there were very few policies and procedures in place to manage personally owned computers in the residence halls. Consequently, much of the action plan developed in 2003 was devoted to solving the problems of unmanaged personally owned computers.

In the academic year 2002-2003, increased network traffic and network configuration problems led to a very unreliable Internet connection. There was also network abuse, such as spyware, but the extent was unknown. Additional load on the firewall was also being generated by poorly designed instant messaging systems. The

firewall was failing regularly, which negatively impacted the university's academic and administrative computing activities. The most frustrating problem visible to everyone was that the firewall would "lock up." When this occurred, it became impossible to use most campus web and email applications.

From the onset of these problems, the firewall vendor was constantly involved. The vendor was confident that tuning or configuration changes to the firewall would correct the situation. They continually defended their product rather than focusing on supporting Northwest's users.

By late in the spring of 2003, the firewall failures were occurring every few hours. Most users would lose their Internet connection and then the firewall would have to be restarted. These failures were catastrophic when students were trying to complete online examinations. Some students were in tears and others would rail at the staff, while still other more aggressive users would demand that the entire network administration staff be fired. Information Systems received a flood of negative campus comment cards.

The lack of communication to users about what was specifically causing the firewall failures was the most common source of complaint. The communication issues were also frustrating for Information Systems as a whole, particularly the Client Computing branch of the department, which had the responsibility of dealing with campus users on a daily basis.

After weeks of these minimal communications, the network administrative staff was unable to resolve the problem, even though they were working constantly and in concert with the highest-level support staff provided by the firewall's vendor. Because the vendor was unable to fix their software, a second firewall vendor was brought onto campus. Like its predecessor, this new system also failed to handle the load. The second firewall vendor's software development team even tried experimental patches in an effort to prevent disconnections. Because of this inability solve the firewall failures, users were offered little in the way of explanation as to what was going on. The situation deteriorated to such an extent that during the last week of the spring trimester the university administration had to publicly announce that special arrangements would be made for any student unable to complete Internet-related course requirements.

4. NETWORK RELIABILITY IMPROVEMENT STRATEGY

In May of 2003, the Information Systems Department presented to Northwest's Board of Regents a set of seven known facts about the network and three specific questions. By addressing these facts and questions, the Information Systems Department would be able to develop a set of comprehensive network action steps. The facts presented at that meeting were:

1. Firewalls from two major vendors, which were configured to block music-sharing systems, had not been able to handle the load of the entire campus.
2. Most music being shared was an infringement of copyright and went against published campus policy.
3. The MOREnet connection bandwidth needed to be increased if music sharing was not managed.

4. Additional staff members would be needed to handle legal problems if music sharing was not managed.
5. Northwest did not have the tools necessary to control or stop music sharing inside the campus firewall.
6. Traffic management challenges would only increase with new features for Internet applications being steadily developed by large providers such as Microsoft and AOL.
7. Traffic management challenges would only increase as more academic and administrative application servers were moved off-campus.

In addition to these facts, the following questions had not been resolved:

1. Should instant video messaging be blocked or managed?
2. Were firewall failures caused by an extensive number of active sessions, complex blocking rules, excessive traffic, data broadcasts or attacks from on campus?
3. Could music sharing be controlled on the campus local area network?

After meeting with the Board of Regents, an investigation was launched to determine what needed to be done to address these questions. The first step of the investigation began by contacting other universities in Missouri to determine what they were experiencing and what solutions they had come up with to resolve similar problems. Teleconferences were also held with MOREnet representatives and two additional firewall providers.

During May of 2003, meetings with the university administration took place to discuss policy enforcement issues. It became clear that the administration did not want an overly aggressive search policy for inappropriate user behavior, which did not drastically impact the stability of the Northwest network. Networking consultants were also brought in to examine Northwest's situation; we also brought in an engineer from *Enterasys*, the vendor for most of the networking equipment on campus. There were also meetings with representatives from Sprint Network Management Services to explore new and more reliable network configurations. Additionally, Network Instruments conducted a network management system demonstration.

Once a thorough exploration of the situation was concluded, a network improvement plan was submitted to the Board of Regents, which gave approval to proceed with the proposed action plan in early June 2003. Shortly thereafter, a public campus forum was held to discuss the action plan with the campus community.

These discussions, while challenging, were extremely beneficial in reopening the doors of communication and helped to improve relations between the campus community and Information Systems. This communication proved to be critical to the success of the action plan.

5. CONSENSUS, CHANGES & COST

The consensus of multiple vendors and several network administrators was that Northwest needed a powerful new hardware-based firewall that could handle network address translation and a very robust set of filtering rules. It was thought that the filtering rules, which had blocked most of the peer-to-peer file sharing through the firewall, might also need to be streamlined or simplified.

The second refinement recommended by the majority of the vendors was to install a router on the inside of the firewall to reduce the load created by broadcast messages coming from the campus local area network. In addition, many agreed it would also be helpful to segment the flat campus network into subnets, which would assist in locating and isolating abusive users.

The third recommendation was to add a packet flow control device, or a packet shaper, to manage the use of all types of Internet traffic. The packet shaper would be especially helpful in giving more priority to academic and administrative network tasks, which could be identified by packet signatures rather than by port numbers.

With these recommendations in mind, key Information Systems staff visited a campus site using a Cisco PIX firewall. The PIX firewall was selected and ordered because of its very high capacity and hardware based, not software based, processing of network address translation. On July 15, 2003, the PIX firewall was installed.

All of the above equipment recommendations were implemented in a matter of two months. The rapid reconfiguration was difficult, but the network was only out of service for one extended weekend and then several Saturdays during the summer.

The cost of the new equipment for the Internet interface upgrade was approximately \$44,000. The firewall, with a fail-over unit, accounted for about \$16,000. The packet shaper accounted for about \$17,000. Nine thousand dollars for new routing/switching equipment completed the new connection to a faster Internet service of 30 Mbps.

In the end, over \$250,000 was spent completing the local area network upgrade from shared to managed switched/routed Ethernet. As with any major upgrade, the ongoing maintenance costs increased by about 10% per year of the initial expenditure. It should be noted that the action plan expanded the final stage of a 3-year network upgrade plan. The network will be expanded again in fall 2004 to accommodate wireless hot spots on campus for notebook computers.

5.1 NEW POLICIES & DISCIPLINARY PROCESS

In an effort to address abuse of the network and to make students, faculty and staff more aware of the importance of network stability, the Information Systems Department worked to strengthen and revamp policies that governed network usage.

The Information Systems Department studied policies from other colleges and universities. Many of the policies discovered at these institutions were incorporated into Northwest's policies.

Several new sections were added to the campus Computer User's Guide, the most important of which was Network Stability Assurance. The Network Stability Assurance section was an attempt by the Information Systems Department to articulate in detail what was and was not allowed on the Northwest network. The section also publicly affirmed the department's commitment to provide consistent and reliable network services to campus users.

As previously mentioned, personal computers and equipment on the Northwest network were causing many issues with network stability. As a result, the computing policies were revised to include mandatory registration of personal equipment connected

to the Northwest network. The registration of personal equipment aided Information Systems in tracking down computers that were causing problems on the network, whether it was a misconfiguration or a virus.

Furthermore, a comprehensive disciplinary section was added. Several meetings were held with representatives from Student Affairs, the Human Resources Office and Student Senate to define the regulations and the penalties for non-compliance. More importantly, these meetings helped generate and reaffirm each area's commitment to preserve due process within the disciplinary procedures.

5.2 COMPUTING POLICIES/ETHICS WORKSHOP

As on any campus, the challenge is to serve the campus community with uninterrupted network services while at the same time "police" that community in an effort to restrict abusive recreational activities that put the network at risk. At Northwest, the Information Systems Department is responsible for providing all academic and administrative aspects of computing for faculty, staff, and students.

One of the main challenges for Information Systems was to communicate to incoming students the acceptable use policies on the campus network. Although Northwest provides PCs or notebooks in every residence hall room, students are increasingly bringing additional desktop computers and notebooks to campus, as well as gaming equipment such as X-Boxes. More troublesome, they also often bring along the attitude of "I've done this for years at home. Why can't I do it here?"

Prior to 2002, Northwest Missouri State University required all students to take a three-credit hour, general education course entitled *Using Computers 44-130*. Designed as an interactive, modular learning experience and conducted by the Computer Science/Information Systems Department (academic), the course introduced undergraduates to microcomputers and basic software packages. Additionally, it provided the means by which the Information Systems Department could communicate policies and ethics in a more comprehensive fashion to incoming students.

Freshmen and transfer students have typically been the most likely candidates to commit computer violations and abuse. *Using Computers* was especially helpful in imparting what were acceptable and not acceptable computing activities on the Northwest network. Although the *Using Computers* course was extremely valuable during its twelve years of implementation, concerns about not attracting transfer students caused the university's administration to reduce the number of general education requirements for graduation. The *Using Computers* course fell victim to this reduction. Without the *Using Computers* course, the Information Systems Department found it much more difficult to teach new students the specific policies concerning the Northwest network.

As a result, the Information Systems Department felt that a key step in its plan of action was to find a new avenue of communication with the freshmen. Therefore, the PERT (Peer Educator in Residence for Technology) program was initiated (presented in more detail in the next section). The PERT program offered a unique opportunity to use students as educators. In this role, they became the instrument used to help promote and enforce policy through the Computer Policies/Ethics Workshop.

Although, the workshop had been conceptualized prior to fall 2003, it had never been implemented. With the new commitment to addressing policy violations and the advent of the PERTs as facilitators, the workshop became an effective educational and disciplinary tool.

5.3 PERT & WEEKEND HELP DESK

Students helping students with technology is the premise behind the Information Systems Department's innovative PERT program. Established in Fall 2003 and implemented in Spring 2004, the PERT program was developed initially to deploy network policy awareness to new students living in the freshman campus residence halls. It quickly expanded to include other duties, such as personal computer configuration on the Northwest network.

Students who become PERTs gain valuable skills, hands-on technology experience, and are compensated with free room and board within a freshman residence hall. The response to the PERTs has been positive, particularly since they are on call for the residence halls on weekends for reporting network slowdowns or outages.

In addition to the PERT students and in an effort to improve communication between network users and Information Systems on the weekends, the department added additional Help Desk hours on Saturdays during the fall and spring trimesters. Information Systems Help Desk had already been available on Sundays for over twelve years.

6. RESULTS & CONCLUSION

The most significant result of the Northwest Network Action Plan is that since the new firewall and interface equipment were installed, the university has not experienced a single unscheduled down time for the local Internet connection. In addition, due to the new policies and the disciplinary process that were deployed, approximately 32 students were found in violation of campus computing policies. Of these, two were granted an appeal and 23 completed the Computing Policies/Ethics Workshop. The remaining 7 individuals will complete the disciplinary process at the beginning of the fall 2004 trimester.

When the Blaster virus started to hit networks across the nation hard in late summer 2003, the campus network had already been upgraded. Thus, Northwest was in a much better position to confront and handle the situation than in spring 2003. Although the campus did experience some slowdowns in random subnets, the network as a whole survived with little negative impact. The reliability of the Internet was excellent. It took months to find, clean up and patch all the infected PCs on campus, but the Northwest network continued to function at a very acceptable level. However, had the network and policy upgrades not been implemented, major widespread outages would have occurred. The Information Systems Network Improvement Plan, which was implemented in a whirlwind fashion, proved to be a success in achieving what it had set out to do – assure network stability, decrease network abuse and build awareness of computer security issues.

With the present financial constraints on education, it is difficult to keep current in application development, hardware upgrades and especially network management tools. But with the increasing demand for Internet resources, every campus must still continually evaluate its network management tools and policies in order to survive in today's dynamic and hostile environment.