

NETWORK OPERATIONS CENTER DESIGN AND IMPLEMENTATION

2005 COMPUTERWORLD HONORS CASE STUDY

EDUCATION & ACADEMIA

A UNIVERSITY NETWORK OPERATIONS CENTER PREVENTS MOST SERVICE DISRUPTIONS BY PROVIDING AROUND-THE-CLOCK PROACTIVE MONITORING OF THE UNIVERSITY'S NETWORK AND ENTERPRISE APPLICATIONS AND SERVICES. THE NOC PROVIDES THE CAPABILITY FOR EFFECTIVE SERVICE-BASED MONITORING BY CLEARLY IDENTIFYING SERVICES AND THEIR RELATED INFRASTRUCTURE AND THE EFFECT OF PROBLEMS WITH THESE SERVICES ON THE GOALS AND ASPIRATIONS OF THE UNIVERSITY COMMUNITY. [20055411]



Robert Carrigan,
Chairman of the Chairmen's Committee

Ron Milton,
Vice-Chairman of the Chairmen's
Committee

Dan Morrow,
Chief Historian

SUMMARY

To meet the ever-increasing challenges of maintaining a stable, reliable, technology environment for its students, faculty, and staff, the University of Pittsburgh has established a state-of-the-art operations center. The Network Operations Center prevents most service disruptions by providing around-the-clock proactive monitoring of the University's network (PittNet) and enterprise applications and services. The NOC provides the capability for effective service-based monitoring by clearly identifying services and their related infrastructure and the effect of problems with these services on the goals and aspirations of the University community.

APPLICATION

The University of Pittsburgh, with its main campus in Pittsburgh and four regional campuses located throughout western Pennsylvania, is one of the nation's top public universities and regarded as one of the world's leading research institutions. The University's 32,000 students and nearly 12,000 faculty and staff, along with visiting scholars and researchers from over 100 countries, depend upon the University's world-class network "PittNet" for their daily teaching and learning, research, and business activity.

At the heart of PittNet is a multi-switch gigabit network backbone that joins hundreds of local Ethernets into a large, geographically-distributed network supporting over 100,000 networked devices and more than 60,000 users. These devices include file servers and workstations, along with laboratory data acquisition tools, critical computer-based medical equipment, and facility control systems. PittNet also provides access to networked University resources through a variety of connections, including the Internet, wide area network links to collaborating institutions including the University of Pittsburgh Medical Center (UPMC) and the Pittsburgh Supercomputing Center (PSC) and research networks including the Internet 2 Abilene network and National Lambda Rail.

Over the past 20 years, network service has evolved from being a research tool accessed by a relatively small number of faculty and students to the technological backbone of the entire university. Today the network ties together the individual applications and services that support the entire enterprise of teaching and learning. Additionally, University business functions are severely hindered without stable, reliable, and high-performance network resources.

Utilization of network-based resources includes the expectation from the University community that these services will be available at any time from any location. For some time it has no longer been possible to endure extended outages due to failure, configuration issues, or unusually high loads on network equipment or on the servers or software application programs that provide the services on which the University community so heavily depends. Expectations and valid requirements continue to grow with today's need for constant access, with the result that even short outages can reflect negatively on the University and on technology departments.

Prior to the implementation of a network operations center, the support model was reactive in nature.

A computer operator or, frequently, a user noticed that an application, system, or network segment was unavailable and contacted the Help Desk. The Help Desk analyst would then notify a systems analyst or network engineer who would then troubleshoot and resolve the problem. Although the University's Help Desk has provided around-the-clock coverage since 1998, the unit had neither the tools nor expertise to troubleshoot and resolve critical outages. In addition to being too frequent, outages occurring outside University business hours took too long to resolve because staff needed to be called in to first isolate and then resolve the problem.

The University's strategic plan for information technology, "An Information Technology Foundation for the 21st Century" recognized the need for the development and implementation of a network

operations center:

“Central to the success of the University's technology initiatives is the implementation of a 24-hour, seven-day network operations center (NOC) from which the status of the entire data and voice network, along with the status and performance of central services and systems, can be visually displayed through the use of advanced monitoring systems and technologies. The NOC will include staff capable of interpreting and responding to network and system status information. The NOC will be tightly integrated with the existing Technology Help Desk service to facilitate flow of user problem reports and availability of timely communication to the University community.

PittNet and central University systems and services are presently monitored on a 24-hour basis, but the monitoring systems in place have varying degrees of capability and operate independently of each other. Implementation of the NOC will centralize responsibility for monitoring and responding to network and system performance issues and ensure a consistent level of access to the information that is generated by them.”

Implementation of a network operations center in a university environment requires careful consideration of the structure of the network, the purposes for which it is used, and similarly, the number and types of servers and applications used to provide the wide array of networked services that are not only presently in place, but planned for the future. The University maintains a wide variety of enterprise applications supporting teaching, research, and business efforts. Among these are its newly-developed student administrative information system; central IMAP e-mail service, Central Directory, purchasing, human resources, and payroll systems, academic UNIX and VMS timesharing services, enterprise Web and portal services, storage area networks, data backup systems, and many others. A wide range of operating systems, database architectures, and an extensive range of server and workstation application software packages are supported within the University environment. The complexity of the University's environment had caused earlier attempts to implement network monitoring software alone to have poor results.

In order to ensure that this expensive undertaking would meet with success, University Computing Services and Systems Development (CSSD) engaged the expertise of Callisma, Inc., a wholly owned subsidiary of SBC Communications Inc., to lead the NOC design and implementation effort.

Preliminary design work began during the early fall of 2003 with an assessment of the University's network, telecommunications, and application infrastructure. Following acceptance of the first phase, the industry standard OSI Network Management Model for fault, configuration, accounting, performance, and security (FCAPS) was selected as the basis for development of new processes for monitoring, classification, diagnosis, resolution, and management of faults in applications, services, and the network. The assessment included a thorough review of the University's existing Help Desk, change management, and other relevant processes. This assessment was a critical prerequisite to the evaluation and selection of a “manager of managers” (MOM) tool. The MOM tool consolidates and logically presents information captured from the network, applications, and services. It also provides workflow automation to enhance the response of NOC personnel. The University's MOM is custom-designed to present information from the point of view of the services affected in order to ensure appropriate impact analysis and prioritization of response.

A staffing model was developed early in the NOC planning process with four types of positions established: monitors, network engineers, application and server engineers, and network management system (NMS) engineers. Monitors review faults detected by the manager of managers (MOM) and problem reports referred by the Help Desk. Whenever possible, monitors resolve the fault or problem utilizing the troubleshooting and other tools available to them. Problems or faults that cannot be resolved by the monitors are referred either to network engineers or to system engineers depending on the nature of the issue. The network and system engineers are experienced in troubleshooting and resolving complex network and application or server issues. Network management system engineers are responsible for development and maintenance of the MOM and all other management tools utilized by the NOC.

Physical space plans were developed and construction began concurrently with the development of the NOC architecture, staffing model, and plans for integration with Help Desk and change management processes. During the civil unrest of the 1970's the University moved critical information technology systems to a remote location removed from the main Pittsburgh campus. Originally constructed as a computer center with a machine room to house the University's administrative mainframe computer and provide office space for support and operations staff, the location proved ideal for locating the NOC in proximity to servers supporting enterprise applications and for locating the NOC and the Help Desk in adjacent space. Renovations began in the spring of 2004 and were completed in early July.

BENEFITS

The chief goal of the Network Operations Center is to proactively identify and resolve problems that lead to critical outages before such outages occur --- and whenever possible, before any user is aware

that there a problem has occurred. Because the NOC views the University environment from a service perspective rather than solely on individual components, the staff has an immediate view of what will be affected when a fault occurs and can take timely and appropriate steps to prevent users from being affected.

The University's network and its academic and administrative systems include components such as leased communications lines and outsourced services outside the direct control of CSSD. In addition, factors such as problems with electrical power distribution and facilities construction that may occur that make it impossible to prevent outages. The NOC provides the capability of observing faults resulting from these kinds of issues that permit a much more rapid escalation to the appropriate service provider and constant monitoring to ensure that the provider resolves the problem promptly. In the event that an outage occurs that is the responsibility of CSSD, the immediate availability of expert staff around the clock results in much shorter resolution times than were ever before possible.

IMPORTANCE

Network operations centers have long been a corporate standard for telecommunication service providers and other large business operations. Although other higher education institutions claim to have network operations center services, these are often limited to monitoring the individual elements of a communications network rather than the full set of data and voice services, enterprise academic, e-mail, and financial applications and end-to-end services included in the University's implementation. The University of Pittsburgh is among the first academic institutions to successfully implement a leading-edge, full-scale, integrated information technology operations center.

The immediate success of the University's NOC is directly tied to Callisma's architecture of the management technology solution and their careful selection of Micromuse Netcool to serve as its manager of managers (MOM). In order to achieve the greatest degree of interoperability with monitoring agents, reporting tools, and a web interface, the University implemented a full suite of Netcool modules. Netcool has the ability to integrate information from other applications including the Ciscoworks tool, in place to manage the high concentration of Cisco network equipment in the University's installed base, and MRTG, a freeware application used to analyze network traffic patterns, within which the University has developed significant reporting capability. Monitoring and reporting are part of the functionality that the NOC provides: the NOC is expected to resolve application and service faults using the MOM.

The key to quickly determining the degree to which server, network, or application faults have an effect on the usability of a service lies with the asset database that has been incorporated into the NOC suite of tools. This database was custom-designed for this implementation. Asset discovery is done weekly following the weekly system maintenance period to ensure that the database reflects the true state of the installed plant. When a fault is detected by the system, it is correlated to the asset database which groups assets by services so that NOC engineers immediately know which services, and subsequently which users, are affected by the problem.

The NOC itself incorporates a state-of-the-art command center design utilizing NER console stations, a Christie Systems rear-projection video cube wall with eight panels, and ancillary 40" LCD video display screens. The Netcool Webtop interface provides numerous high-level and detail displays showing the current status of the network resources, applications, and services, detailed fault status information, current news and weather information, and much more.

The NOC is physically located adjacent to the University's enterprise machine room providing NOC monitors and engineers the ability to virtually and physically monitor enterprise applications and servers, the facility's electrical power feeds, HVAC system status, and the status of other infrastructure systems. The technology in use provides the University's 24-hour help desk with timely information on system status so that help desk analysts can knowledgeably assist end users. The Remedy call center management system in use throughout the help desk and central IT organization is tightly integrated with the NOC's MOM allowing problem tickets to be automatically generated as faults occur. In order to prevent the NOC staff from bombardment with fault alarms generated by multiple systems when problems occur, the event correlation and "de-duplication" capabilities of the system ensure that the system reports only the faults related to the underlying cause of the failure.

ORIGINALITY

Network operations centers have long been a corporate standard for telecommunication service providers and other large business operations. Although other higher education institutions claim to have network operations center services, these are often limited to monitoring the individual elements of a communications network rather than the full set of data and voice services, enterprise academic, e-mail, and financial applications and end-to-end services included in the University's implementation. The University of Pittsburgh is among the first academic institutions to successfully implement a

leading-edge, full-scale, integrated information technology operations center.

The immediate success of the University's NOC is directly tied to Callisma's architecture of the management technology solution and their careful selection of Micromuse Netcool to serve as its manager of managers (MOM). In order to achieve the greatest degree of interoperability with monitoring agents, reporting tools, and a web interface, the University implemented a full suite of Netcool modules. Netcool has the ability to integrate information from other applications including the Ciscoworks tool, in place to manage the high concentration of Cisco network equipment in the University's installed base, and MRTG, a freeware application used to analyze network traffic patterns, within which the University has developed significant reporting capability. Monitoring and reporting are part of the functionality that the NOC provides: the NOC is expected to resolve application and service faults using the MOM.

The key to quickly determining the degree to which server, network, or application faults have an effect on the usability of a service lies with the asset database that has been incorporated into the NOC suite of tools. This database was custom-designed for this implementation. Asset discovery is done weekly following the weekly system maintenance period to ensure that the database reflects the true state of the installed plant. When a fault is detected by the system, it is correlated to the asset database which groups assets by services so that NOC engineers immediately know which services, and subsequently which users, are affected by the problem.

The NOC itself incorporates a state-of-the-art command center design utilizing NER console stations, a Christie Systems rear-projection video cube wall with eight panels, and ancillary 40" LCD video display screens. The Netcool Webtop interface provides numerous high-level and detail displays showing the current status of the network resources, applications, and services, detailed fault status information, current news and weather information, and much more.

The NOC is physically located adjacent to the University's enterprise machine room providing NOC monitors and engineers the ability to virtually and physically monitor enterprise applications and servers, the facility's electrical power feeds, HVAC system status, and the status of other infrastructure systems. The technology in use provides the University's 24-hour help desk with timely information on system status so that help desk analysts can knowledgeably assist end users. The Remedy call center management system in use throughout the help desk and central IT organization is tightly integrated with the NOC's MOM allowing problem tickets to be automatically generated as faults occur. In order to prevent the NOC staff from bombardment with fault alarms generated by multiple systems when problems occur, the event correlation and "de-duplication" capabilities of the system ensure that the system reports only the faults related to the underlying cause of the failure.

SUCCESS

The implementation of the NOC has been successful virtually from its inception. Development of a NOC was a key component in the University's strategic plan for information technology that was first published in May 2000. The careful attention to planning, which included extensive pre-planning and a three-phase design and implementation project plan ensured that the software, systems, and personnel selected would be able to successfully monitor, troubleshoot, and resolve problems beginning with the first day of operation.

The University's decision to engage Callisma, Inc., an experienced consulting partner, very early in the project was critical to this success. With its extensive experience in NOC design and implementation projects and its ability to develop a clear view of the University's environment and requirements, Callisma was able to work with University personnel quickly and effectively towards documenting and refining processes. Callisma also contributed its expertise to the development of the NOC staffing structure and design of the actual NOC facility. In large part due to this partnership, the University was able to complete the planning, design, and implementation of the NOC within nine months.

The success of the NOC's implementation is observable both by direct and indirect measures. The most notable measure is the 60% decrease in "critical" problem reports to the Technology Help Desk. Prior to implementation, most problem reports defined as critical involved service outages observable by end users. Post-implementation, shows reduced numbers of critical problem reports that are now generated by the NOC monitors based on observed faults before the Help Desk receives a problem report from an end user. Indirectly, the 24-hour real-time monitoring capabilities have led to situations in which the NOC staff observe faults caused by electrical power failures or problems with leased lines and provide the first report to the appropriate University unit or outside vendor. Initial design work began in October 2003 and early NOC operations began in June 2004, indicating that all activity was successfully completed on a highly accelerated schedule.

DIFFICULTY

The development of the network operations center involved several levels of difficulty. First, it was necessary to select the software tools and agents capable of inventorying and monitoring the University's highly complex network infrastructure. Second, tools and agents capable of monitoring the wide array of hardware platforms, operating systems, and database architectures in use needed to be identified and selected. Third, the workflow involved in identifying, reporting, troubleshooting, and resolving observed or reported faults needed to be completed. An additional level of complexity involved reviewing the staffing within the existing development and network engineering groups in order to reassign some experienced staff resources to the NOC. Additional job positions needed to be created and filled. Concurrently, space renovations needed to be completed, and the monitoring tools and "Manager of Managers" software installed and configured.