

BRADFORD CAMPUS MANAGER

Case Study

Industry Higher Education

Binghamton University

Binghamton, Endicott, and Johnson City, NY

Binghamton University is located in the Town of Vestal, just one mile beyond the Binghamton city limits in the Southern Tier of Upstate New York. Binghamton, Endicott, and Johnson City ("the Triple Cities")--along with suburban Vestal--make up Greater Binghamton offering a sophisticated cultural life, lively spectator sports and accessible outdoor recreation.

Customer

Binghamton University serves a community of about 14,000 full and part-time students and 2500 employees. The college supports more than 6,500 registered system users including wired/wireless laptop, mobile, and PC, Linux and Macintosh system users.



Problem

Through a targeted, remediation-capable network access control solution, the automated facility to enforce security at every point where a user interfaces the network both physically and logically; a solution resulting in greater uptime, less downtime while enhancing and maintaining the "infrastructural integrity" of the University campus at large

Solution

Binghamton University selected Campus Manager from Bradford Networks, an appliance based solution that manages, secures, and controls all devices accessing the network while enforcing network authentication and registration policies. This includes identifying, localizing and tracking network clients quickly, connection-based security scanning and isolating 'at risk' users and devices in a Quarantine area.



BRADFORDnetworks
Maximizing Network Security

The Customer

- 14,000 students
- 500 faculty

Binghamton University, one of the four University centers in the State University of New York (SUNY) system, is located in the town of Vestal, just one mile beyond the Binghamton city limits in the Southern Tier of Upstate New York. Binghamton, Endicott, and Johnson City ("the Triple Cities")—along with suburban Vestal—make up Greater Binghamton offering a sophisticated cultural life, lively spectator sports and accessible outdoor recreation. U.S. News & World Report has ranked Binghamton among its top 50 public universities in the nation for eight years in a row.



Official enrollment exceeds 14,000 including underclass and graduate students. This includes 1,100 international students representing 87 countries. Of the more than 500 full time faculty, 93% hold a PhD. Founded in the liberal arts, the University's programs lead to bachelor's, master's and doctoral degrees including selected professional and graduate programs.

The Problem

- Registration
- Security
- Usage Policy

The venerable chestnut "always be prepared" can be applied almost universally to any professional, even personal setting. The context itself might change, of course, but the reason for doing so almost never does.

Joe Roth, Network Support Technician for Binghamton University, always believed that his crackerjack Computer Services group had crafted an IT framework that had been architected to support the most demanding needs of incoming freshman and campus faculty alike.



"The network had been designed with scalability in mind," observed Roth. "Our network needs to be able to scale in order to support the current and future population at the University. This includes providing one port per bed in the residence halls and the ability to add bandwidth to the closet if needed. In fact, we took the approach of standardizing on equipment to ensure that we would be able to meet our future technology needs. The by-product of standardization, of course, is that it gives us the ability to provide support for almost any piece of computer equipment to which a student might want to connect."

This "one-size fits all" framework extends even to the University's Residential Network (ResNet).

"We made sure to standardize on one switch vendor in the dorms, and we have also replicated essentially the same setup in each wiring closet. This means that there are no surprises in the network setup when visiting a wiring closet to work on a trouble call."

Roth added, "In the ResNet, we have a clear separation between our core, distribution, and access layers, having standardized on a switch model in each. Our original configuration was based on the same switch model at the distribution and access layers."

Roth's department is responsible for the campus network, VPN, firewalls, security, and anti-virus. It also handles the Microsoft server environments, desktop support, and departmental project support. However, prior to Campus Manager from Bradford Networks being deployed, user registration did not exist on campus and policies were enforced manually. When an infraction did occur, tracing it involved manually tracking down the MAC address and shutting down a port.



The Problem

- Registration
- Security
- Usage Policy

"The challenge with securing a network like ours is introducing security at every point where a user interfaces the network both physically and logically," said Roth. "Something like an authentication system that can operate on a per port basis is ideal, but then the challenge becomes policing traffic to and from the users' machine to make sure that they're secure and that our network and systems are free from anything they might bring in."

The same framework that maintained the integrity of the campus network now required, said Roth, the development and enforcement of a network-wide access control policy.

"Historically, we could not enforce a policy that required a student to protect their machine from viruses and other malicious activity. The best that we could do was to suggest that a student load anti-virus software and keep up-to-date on their patches. The only time that we could absolutely ensure that they were installed was when we visited the machine to repair it," conceded Roth.

Network downtime due to the resulting worm traffic was becoming a real issue on campus. Without a pre-existing system for registering users and handling remediation, the effect of viruses and worms on the network became the virtual equivalent of dominos spread out over the floor lined up mere inches from one another. With the proper push or catalyst (e.g. worm), the dominos (or user machines) would teeter, begin falling against one another and threaten to bring the entire network down.

"The main challenges that we faced before the implementation of CM were the exponentially increasing numbers of calls regarding viruses and spyware. The main virus threat was internal with infected machines attacking other unpatched machines as they connected to the campus network," said Mike Hizny, Assistant Director of Networking. "This resulted in continuous network instability and constant efforts by our residence hall consultants to try to fix machines and keep the dorm networks running. Our full-time network group was spending countless nights tracking down and trying to eliminate infected machines that kept taking network segments down. The public image of an unstable network far outweighed the labor costs and number of calls we received."



The Network

- Cisco switches
- DELL & IBM Servers
- Windows Servers
- Oracle & SQL
- Active Directory

The campus network consists of a mix of DELL and IBM servers with hardware platform support for both PC (Intel-based) and Macintosh, and all popular operating systems including Windows, MAC OS, Linux, and Unix. The Windows 2000 and 2003 Servers are joined in the campus data center by an array of Sun hardware and Linux Servers. On the backend of the network, the University employs Oracle and SQL databases and uses Active Directory 2000 and 2003 for authentication. Binghamton has standardized on a Cisco-based switch fabric. The number of users Roth and his team support exceeds 10,000, with 6,500 in the ResNet and 3,500 others, including faculty and staff.

The Solution

Roth and his team began their search in earnest for a solution that would authenticate users connected to the network while verifying that the machine connected to it had valid anti-virus software and was up to date with patches. The solution also had to offer the ability to have each person connecting onto the network agree to the campus Acceptable Use Policy. Additionally the solution needed to offer a light, administrative "footprint."

The Solution

- Out-of-band Control
- Non-persistent agent
- Worm/Virus Detection

In Hizny's opinion there were several features that set Bradford's solution apart from all other vendors. "We liked that Bradford's solution supported out of band control and included an ability to inspect and update user machines without actually creating administrative accounts on them. We like to take a hands-off approach to students' machines and felt that we would have a large liability if we installed an administrative account on each machine in order to remediate them. The non-persistent agent control allowed us to inspect, confirm, and modify the computer settings and then exit gracefully with no remnants. Another consideration was the number of control boxes that were needed by each solution. The Bradford solution required 2 control boxes and the nearest competing solution required five. Ultimately, we felt that it was the best-of-breed solution and that the implementation and learning curve gave us the best, and most timely, competitive edge for a summer installation and fall rollout."



The performance of the system has been great. We register around 6,500 – 6,800 students in the first few days of a semester and the system handles the load with little performance degradation.



Integrating Virus Intervention Strategies Using the Combined Capabilities of Campus Manager and PacketShaper

Detecting viruses on the network, as Roth soon learned, was one thing. Stopping them altogether quite another.

"During the first semester we deployed Campus Manager and got everyone through registration, then at that point we started looking at how much further we could go with it; what we could do in order to mitigate certain problems on the network."

One of the biggest problems, Roth admits, was the amount of worms and viruses that trafficked the network on a regular basis. While they were no longer bringing the network to its collective knees, locating infected machines and placing them in quarantine was still an issue.

"We already had a system that was custom written in house, which used Packeteer's PacketShaper™ to detect worm or virus traffic. The remediation didn't actually remove them from the network or halt virus traffic. It just gave users a web page when they tried bringing up their browser that said, 'You've Been Quarantined.' While that alerted users that there was a problem, it didn't really stop the problem from happening in the first place and it didn't quarantine them at all."

Roth turned to Bradford and the company's PacketShaper integration solution.



"I consulted Bradford about their integrated Campus Manager/PacketShaper solution and at the time I learned they were only using it for usage policy management, chatting, and file sharing. We, however, saw the Bradford example for using PacketShaper to control things such as instant messenger traffic and we thought, 'What if we could take this example, modify it, and apply it to worm traffic on the network?' I contacted Bradford about it and with their help set up a trial run."

The Solution

- Music, Movie Download Detection
- RIAA, MPAA Enforcement

As Roth describes it, PacketShaper detects something is occurring—a worm or virus—then passes that IP address of the offending machine to Campus Manager; CM can track that down to a specific port, and then Roth and his team can act based on that.

“It was literally tested and deployed the same day, and the results were phenomenal. Within one day we had already taken significant steps towards cleaning up our ResNet. Campus Manager is really about control management, knowing where every client is connected and being able to manage them based on that,” said Roth.

And the benefits of that integration, according to Roth, are moving forward.

“We have already purchased another Campus Manager system for use on the faculty/staff side of the network,” said Roth. “We plan on using the PacketShaper integration and eventually moving toward verification of faculty and staff PCs. We are also working on integration with another IDS box we have purchased so that we can take advantage of more advanced anomaly detection.”



File-Sharing and Copyright Enforcement Using Campus Manager

A recent phenomenon that Roth and his team did not originally anticipate—the file sharing of copyrighted material—also required an enforcement solution and once again, Roth has relied on Campus Manager from Bradford Networks to serve as the “virtual buffer” between users determined to infringe on copyrighted materials through a few strategic clicks of a mouse on the ResNet.

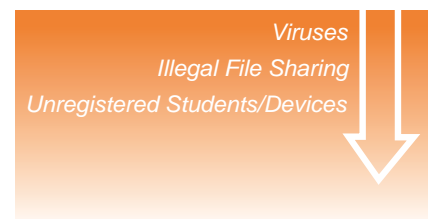
As Cindy Kester, Assistant Director of Academic Computing explained, within Campus Manager there are generally two reasons why users are disabled: the detection of a virus or worm, or reports she receives from RIAA (The Recording Industry Association of America) and the MPAA (Motion Picture Association of America) that users on campus have been found sharing files illegally. Generally, the files identified are music, movies, software, games, and TV shows.

“Originally, once we received the report, we shut a person’s port off,” said Kester. “They would then start up their computer and they wouldn’t get any response and they would be left guessing what was going on. They would think it was a technical problem and would call the help desk.”

Prior to Campus Manager, identifying whom the offending file-sharing student was in a specific location proved difficult and time-consuming. When Kester or an administrator received the report they would ask the operations team to find out who was using the IP address used to download the file. Often however, there were two residents—sometimes three—in the offending dorm room. Accumulating that level of information would sometime take a half-day or more of time. Then, an administrator would have to physically look up the phone number for the room and the email address of all the residents in an effort to try and contact them. About half the time the operations team would reach someone, explain the problem and the offending party would sign the paperwork agreeing to stop serving copyrighted material. If that didn’t happen within a week to 10 days, however, the designated operations person would disable the dataline so that no computer could connect to the campus network from a port in that room. It was a technical problem and would call the help desk.”



MAXIMIZING NETWORK SECURITY



The Benefits

- Copyright Infringement
- User Isolation & Notification

The results using this methodology, however, proved mixed. “Sometimes this would prompt the student to get in touch with us and sometimes the student would contact a residence hall consultant to troubleshoot the connectivity problem. Other times the student would plug into a different port and continue working,” said Kester.

“With Campus Manager, rather than shutting off the client’s port, we can modify the client’s record so that when they open their web browser they get a message that says, ‘You’ve been disabled, because...your machines is infected with a worm or due to an RIAA infraction,’ and so on. Campus Manager expedites things so they’re calling the help desk to say, ‘I can’t get connected because I have an RIAA infraction.’ This direct messaging expedites things so much that it easily eliminates three other levels of support this call would go through trying to figure out what was going on.”

From a technical standpoint, when Kester and her team receive a copyright infringement report, an administrator can enter the IP address in Campus Manager and find out the user ID of the person who registered the computer, that person’s name and location on campus, and the MAC addresses of all computers registered with that user ID. A code is then entered that disables all the devices that show up in the queue for that person. As a result, the only web page those computers will go to is a page informing them there has been a copyright infringement and they have to see the ResNet team to discuss the incident. Once the incident has been resolved, the code is removed and devices are again enabled using Campus Manager.

“Campus Manager has made the process easier, more efficient, and saves many man-hours,” said Kester who credits CM for resolving these kinds of incidents in a shorter time and with fewer resources needed, including those individuals within operations—who, generally speaking, are not involved in the investigation of most cases—and residence hall consultants who are never called on now to troubleshoot a connectivity problem that is attributed to a copyright infringement report.

“Campus Manager has been a win-win solution for us. We can use the report to trace individuals rather than to rooms that often have more than one individual and more than one computer,” said Kester. “And, of course, the custom web pages from Campus Manager take the guess work out of the process; now the student knows what the problem is and can get it resolved sooner.”



Expanding Campus Manager Campus Wide

Formerly, Campus Manager supported only Binghamton’s student ResNet. For incoming Fall 2006 students, however, Roth and his team decided to make it available campus wide.

“The positive impact and success of our Campus Manager deployment in the ResNet showed that it would be a useful tool to have running campus wide. The acceptance of the process by our on campus students gave us the confidence to begin expanding the validation process campus wide,” said Roth.

According to Roth an ability to increase visibility into users – who they are and how they are connected – are among the chief reasons for this expansion.

“The ability to dead-end (disable) infected users or users who are in violation of policies was a desirable feature to have campus wide,” said Roth. “We were also interested in gaining insight into our access layer and who was connected to it. We also liked the idea of verifying a host before they were connected to the network and we wanted to see this process used on a campus wide basis. We are already reaping the benefits of the client management portion of the system. Searching for a MAC or IP address on campus has never been easier.”

The Benefits

In addition to giving Roth and his team the ability to record statistics such as operating systems that help them plan towards future purchases and training support the expansion has also paid dividends in time to Roth and the rest of his IT staff.

"The product is frequently used by our IT staff to locate hardware on the network, determine where a host might be connected, where a multi-access point may be, things of that sort. It certainly makes managing the network a much easier task," said Roth.

Campus Manager's ability to scale and to provide reliable service also played a part in Roth's decision to migrate the solution campus-wide.

"After connecting nearly 6500 students to our first system successfully we felt extremely confident that the hardware would be able to handle the numbers of faculty and staff that are present on campus. We did acquire a second set of hardware for the task, but scalability was never as much a concern as reliability. When implementing any piece of hardware on an enterprise network reliability is always a concern, however, that is where the quality of support comes into play. Knowing that a knowledgeable technical support staff is backing the product helps put the issue to rest," stated Roth.

For Roth Bradford as a brand and as an organization continues to meet and often exceed his expectations. "Bradford is not only willing to supply a quality product, but they are also always willing to admit that it can do more," offered Roth. "When it comes to networking an endless combination of brands, models and configurations are available, and when it comes to computing you have to expect almost anything to be on the users PC. To maintain a product that deals with these kinds of conditions you have to be prepared to change the system at any point in time – Bradford has stepped up to this challenge and has met it (and continues to meet it)."

He added, "The network and computing technology implemented at EDU's is constantly changing, if you keep a product that claims to secure and manage it at a standstill for too long it becomes obsolete. Our network isn't going to be the same this semester as it was last semester, our students will be using different software and we will be researching a different technology, whether it be wired or wireless, our NAC solution will have to keep up, Bradford has proven that they can maintain stride."

Even now, in Fall 2006, plans are underway to include Campus Manager in Binghamton's migration to a fully integrated wireless environment.

"This semester, for example, we expanded CM to our public areas, which include podiums in classrooms and lecture halls, study lounges, study areas in the library, etc. It also began servicing our dorm-wide wireless deployment," confirms Roth. "We are looking into expanding it to faculty & staff offices and campus-wide wireless. We have already set up a guest access solution using CM, but we are looking at improving and streamlining it."



Additional Benefits

Campus Manager from Bradford Networks, said Roth, has effectively insinuated itself not only into upgrading the performance and user accountability associated with the University's ResNet, but it's also paid off in dividends both on a day-to-day as well as long-term basis.

"It has streamlined our operations in a few ways," concluded Roth. "One is that it provides an interface between Computing Services and our ResNet users before they start their computing experience on campus. We can deliver important messages and verify their computers before they start using the network for other reasons. We basically get to interact with them and their PC without having to visit every student, and we can change this interaction at a central management point and deliver it to 6,800 students instantly."

The Benefits

- Self Remediation
- Bandwidth Control

He added, "It has also streamlined how we handle our users' experience on the network. We now have a way to automatically remediate/disable users when either an infraction occurs or if we detect some anomaly sourced from their PC. One example of this is the Packetshaper integration. Our Packetshaper handles how we distribute bandwidth to our ResNet, and it is already analyzing the traffic coming to and from the dorms. The integration between the Packetshaper and Campus Manager simply leverages what both systems are already capable of, and means that we don't have to deploy another hardware device or piece of software to do our IDS detection; we use what was already there inspecting the traffic and managing our students connections. Another example along the same lines is the ability to deliver a custom webpage based on why a student has been placed in remediation or disabled. This has replaced our original system of actually shutting off the student's port. "

Campus Manager's ability to look up a device by its MAC or IP address and find out what port it's connected to provides Roth and his team with additional visibility into the network that heretofore they didn't have. This allows the IT and operations group to provide better, more targeted support to other departments connected to the network.

According to Hizny, the reason for deploying Campus Manager in the first place was to ensure a seamless, even transparent, registration process.

"We really wanted to make the registration process quick, efficient, and complete so that it did not impact the users trying to connect and go," said Hizny. "Being a research campus, it is really hard to measure the cost of lost productivity and business associated with a network outage. Any outage puts a stop to data communication, email, and research, which truly impacts the image of the University."

Roth is also proud to cite applications for Campus Manager beyond registration. "The manager for our meal card system (BUC\$) oversees about 80 serial servers for things such as vending machines and cash registers. We have recently begun moving all of these to their own subnet and VLAN, and Campus Manager has helped provide a method for tracking these and verifying their location to ensure that we are switching the correct ports. When we began doing this he did not have locations for quite a few of the servers, and we were able to easily track them down via MAC through Campus Manager, which saved us a lot of time."

Roth has also been impressed with Bradford Networks level of interest and support in helping him meet his performance requirements.

"Bradford has been extremely responsive to integrating with outside vendors. Whenever we need new vendor support added, it simply takes a phone call or an email and they begin working on the problem. That kind of support gives them an edge and is almost unprecedented in the market today."

He added, "Campus Manager has helped take the guesswork out of where some data ports terminate on the network. This has resulted in a more secure/controlled environment and enables us to provide a positive networking experience to the entire campus. We can provide a better level of service to our students when their machines are infected and we experience less downtime due to network anomalies."

And in terms of planning ahead for every possible circumstance, Roth uses a familiar analogy: "The Campus Manager system has essentially become like a Swiss army knife on our network, and new tools and uses seem to show up within the system almost monthly."

“

The ease of administration and customization of the system is a great benefit. Managing the system takes very little time and is intuitive. We are able to easily customize the web-pages and features of the system and Bradford provides great support for custom configurations.

”

The Benefits

Benefits Gained From BRADFORD CAMPUS MANAGER

Integrated Campus Manager and PacketShaper solution detects the presence of viruses and worms, identifies the IP address of the offending machine, and enables IT personnel to effectively shut traffic off to and from the affected ResNet port.

Identifying incidents of illegal file sharing that results in copyright infringement can now be traced to an individual's IP or MAC address. Offenders are notified through a custom web page why their port has been "shut off."

Streamlines student registration by enabling a common, virtual interface between Computing Services and ResNet users, facilitating the delivery of important messages, verifying the state of student machines before they access the network, and achieving all of it virtually, without having to interact with individual PCs or visit each student.

Takes the guesswork out of locating where selected data ports terminate on the network, resulting in a more secure environment, a positive networking experience for the entire campus, and less downtime due to network anomalies.

Effectively reduces the number of operations and computing personnel required to assist students experiencing network access or connectivity failures.

Contains, limits, and mitigates the number, incidence, and extent of virus contaminated machines, ensuring internal service level agreements continue to be met.