Implementing Proactive Network Management Solutions in the Residence Halls

Param Bedi
Chief Information Officer
Arcadia University
450 S. Easton Road
Glenside, PA 19038
215-572-4019
bedi@arcadia.edu

About Arcadia University

Arcadia University, founded in 1853, is a private, coeducational comprehensive university in suburban Philadelphia offering undergraduate and graduate study to more than 3,400 students annually. The Arcadia University Center for Education Abroad, ranked second in the country and recognized by U.S. News and World Report for its outstanding programs, is one of the largest campus-based international study programs in the United States, serving an additional 2,000 students each year from nearly 300 American colleges and universities. U.S. News also ranks the University among the top colleges and universities in the North and Barron's has named Arcadia a "best buy" for the past 12 years.

Residence Halls Network

There are about 1,100 students in the 10 residence halls and apartment complexes. The residence hall students connect to the campus network, while the students living in the apartment complexes use the Comcast high speed network for their computing needs. The residence hall students have a dedicated 5 mb connection to the internet. This internet connection is independent of the connection for faculty and staff.

Arcadia University's ResNet was not working to its full potential. We did not have any registration process in place, and lacked the policies and organization needed to run an effective ResNet. The network was constantly being overwhelmed with viruses which created performance issues for the students. All problems had to be fixed manually, which consumed much valuable time.

How Campus Manager Helped Arcadia University

Arcadia University needed a solution to enforce both the ResNet policy and security. The ResNet was overwhelmed with viruses like blaster which caused a lot of problems. All these problems had to be fixed manually which consumed much valuable time.

Campus Manager brings a policy and security solutions for Arcadia University's ResNet

- Enforce the ResNet policies
- Enhance the ResNet securities
- Gain control of the network
- Prevent virus propagation
- Reduce the ResNet downtime

What is Campus Manager

Not a gateway or single point of failure. If Campus Manger fails, network traffic will not stop. The network will be left in whatever configuration it was in at the time Campus Manager stopped working.

Not a turn-key solution. This is not a solution that you plug in and walk away from. Campus Manager is a product the IT Staff must customize to their network in order to get the fullest potential from the solution.

A way to detect rogue DHCP servers, locate and manage vulnerable computers, and enforce network policies.

No client software on the user's computer

How Campus Manager Works

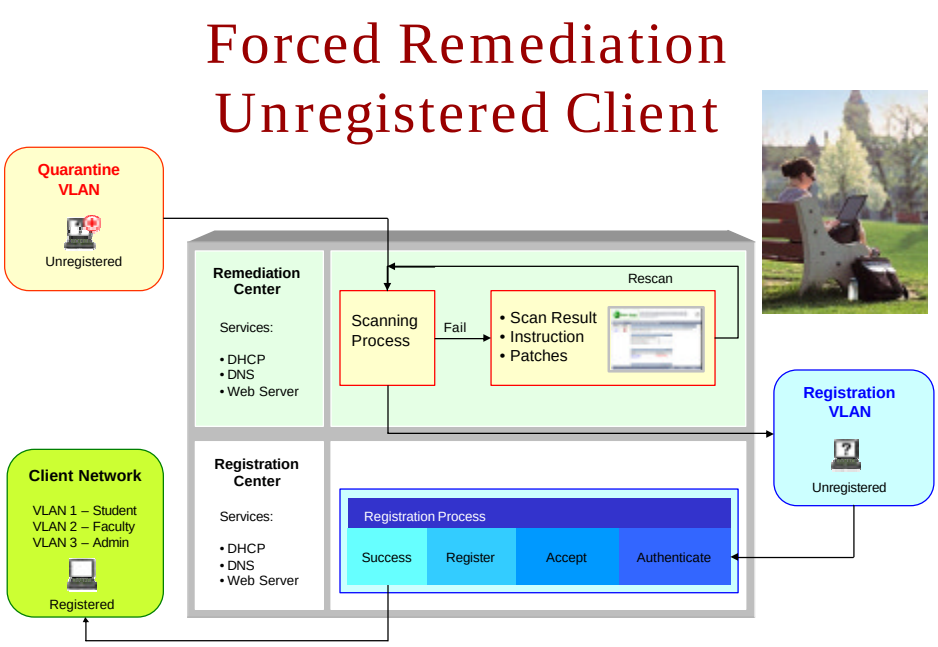
Campus Manager sits passively on the network attached to a core device.

When a new device tries to gain access to the network a link up/down trap is sent to Campus Manager.

Campus Manager reads the user's MAC address to authenticate the user's MAC with Campus Manager's own database.

If the user's MAC is recognized and is considered healthy, the user is allowed access. If the user's MAC is not-recognized or is considered vulnerable, the user must go through the registration and / or remediation processes.

Campus Manager can authenticate with your database using LDAP.



Campus Manager Remediation Center (CMRC)

The CMRC offers a variety of Nessus Scans (www.nessus.org) to check user's computers for vulnerabilities.

Nessus is an open source program with over 2000 scans. Scans are customizable, and custom scans are constantly being added to Nessus's national scan database.

Administrators have the option of choosing which Nessus scans best fit the requirements of their environment.

When a user fails a Nessus Scan in forced Remediation, the user is not allowed any further into the registration process until all the failed scans have been addressed

A web-page will alert the users to their vulnerabilities, provided them with ways to fix themselves, and a 'rescan' link is presented in order to ensure all vulnerabilities have been fixed

Client Assessment Tool (CAT)

Client Assessment Tool (CAT) is an ActiveX application that inspects Microsoft Windows PCs. Run from any web server, the application executes on the client PC and enforces your security and network policies. Designed to work in harmony with BSi's Campus Manager.

CAT provides the option to check for several versions of Anti-Virus software.

CAT provides the option to ensure your clients are running the latest version of Windows Critical Updates and Service Packs.

CAT allows the option to import any registry change into the Windows client. For example, you can import the ability to ignore SP2 critical updates for XP users, turn off DNS caching in Internet Explorer or force updates from a local SUS server. CAT also provides the option to install an administrator level account on the client system.

Detects and removes XP-Home bridging.

Detects and enforces Spyware Protection Program.

Alarms

Email IT Staff

Email offending client

Disable / Re-enable client

Disable / Re-enable port

Mark as "At Risk" and switch to Quarantine VLAN

Conclusion

Campus Manager gives the IT staff the tools they need to proactively manage the ResNet.

With the help of CAT and the CMRC, a Campus Manager solution will help ensure users gaining access to your network are checked for multiple vulnerabilities which would cause numerous problems to the well-being of your ResNet.

Not only does Campus Manager monitor network health, it makes your network healthy. A healthy network has very high up-time, high performance, and involves less time to troubleshoot.

Campus Manager helps ensure the learning process at a higher education institution are not interrupted or disturbed because of computer networking issues.