

802.1X AUTHENTICATION FOR WIRED NETWORKS

2005 COMPUTERWORLD HONORS CASE STUDY

EDUCATION & ACADEMIA

IN ORDER TO ENHANCE NETWORK SECURITY AND PROVIDE THE CAPABILITY OF PERMITTING ACCESS TO NETWORK RESOURCES BASED ON AN INDIVIDUAL'S AFFILIATION WITH THE UNIVERSITY, 802.1X-BASED NETWORK AUTHENTICATION WAS IMPLEMENTED FOR THE UNIVERSITY'S CAMPUS RESIDENCE HALLS IN SEPTEMBER 2004. [20055369]



Robert Carrigan,
Chairman of the Chairmen's Committee

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

Dan Morrow,
Chief Historian

SUMMARY

In order to enhance network security and provide the capability of permitting access to network resources based on an individual's affiliation with the University, 802.1x-based network authentication was implemented for the University's Pittsburgh Campus residence halls in September 2004. 802.1x authentication will ultimately be deployed for all wired network ports at the University.

APPLICATION

The University of Pittsburgh is ranked among the nation's top public universities and regarded as one of the world's leading research institutions. The University serves 32,000 students on its five campuses located across western Pennsylvania. The main campus is located in Pittsburgh.

The University's network, "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. These devices include computer servers and workstations, as well as 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 (such as the University of Pittsburgh Medical Center and the Pittsburgh Supercomputing Center), research networks such as Internet2 Abilene Network and National LambdaRail.

Historically, the University's 30,000 wired network ports, when active, have been open to any user with access to a University IP address. The demand for network service in large, open access areas, residence halls, and shared spaces have driven the need to provide authenticated network access in some form. Authenticated access will address three key needs: to improve IP address allocation and management through dynamic assignment, improve network security by associating network utilization with specific users at the port level, and provide the infrastructure for usage based billing services. Early attempts to provide authenticated network access have proven to be problematic. For example, the University currently utilizes Bluesocket® appliances for wireless network authentication. These have proven to be highly effective for wireless implementations within departments and other small areas, but the device is not currently sufficiently scalable to permit deployment for large wired network segments.

The University previously addressed the specific need to authenticate access to its residence hall network using the PPPoE protocol. With this implementation, two Cisco 7500 switches were used to authenticate nearly 6,000 users at the Pittsburgh campus. While PPPoE proved to be an effective, easily supported solution, it also proved to have scalability issues that prevent deployment across the entire network.

More recently, 802.1x has come to the fore as a network authentication solution. Originally designed to provide network authentication for wireless services, the University quickly recognized the applicability to wired installations as software publishers began to incorporate supplicant software routines into new releases of their operating systems and as network switch manufacturers began to provide support for the protocol into their switches and network equipment.

Computing Services and Systems Development (CSSD) elected to pilot 802.1x authentication in the Pittsburgh campus residence halls in part because of the need to provide a better authentication solution than PPPoE and because of a separate plan to replace all of the network switches supporting these buildings with newer equipment. Following development efforts that occurred over the summer of 2004, the authentication system was introduced to resident students beginning in August of that year in time for the start of the fall academic term.

Based on the successes of this project, plans are now under development to implement 802.1x authentication for all wired network ports at the University of Pittsburgh.

BENEFITS

802.1x has proven to be effective in addressing the need to provide authenticated network access for the following reasons:

- Traffic bottlenecks that can be a problem with PPPoE authentication are eliminated. 802.1x authentication is handled by the first network switch encountered when a user connects to the network while all network traffic must pass through one or more separate concentrators with PPPoE.
- 802.1x provides improved security in open areas and shared spaces. All users must have University computer account into order to authenticate to any wired port on the network.
- 802.1x provides the ability to introduce roles-based access to networked services. For example, guest users could be granted access only to the Internet while students, faculty, and staff have access to the entire network.
- Any authorized user can connect to the network from any wired port without the need to reconfigure IP address and gateway settings each time a computing device is moved to a new location.
- All users will connect to the network using a common interface.
- Most new operating system versions provide native support for 802.1x, eliminating the need to install a separate client add-on package.

IMPORTANCE

The University's 802.1x implementation takes full advantage of technologies from Cisco, Microsoft Corporation and Meetinghouse, Inc. Port-level authentication requests are handled by the closest network switch to the user. The switch queries the Microsoft Internet Access Server to authenticate the user. The IAS queries the University's Central Directory Service to determine the access privileges that have been granted to the user.

802.1x technology is being widely adopted in the form of new switch equipment that provides support for the protocol without upgrade or modification. Microsoft's Internet Access Server (RADIUS authentication server) was selected because of its feature set and compatibility with the Central Directory Service. The Meetinghouse 802.1x software client was chosen because of its multi-platform, multi-version operating system support. Although newer operating systems natively support 802.1x, CSSD decided to distribute the Meetinghouse client to ensure that all users connect using a common interface.

The importance of this technology exceeds network authentication significantly. Historically, administrative departments have been charged a flat rate monthly network access fee "electronic dialtone charge". In response to complaints that users who connect to the network infrequently pay the same rate as high-bandwidth users, the University has elected to convert to a usage-based billing model. Under this scenario, a monthly fee would be charged based on the volume of traffic generated by the user. Because 802.1x associates individual users directly with ports, the technology will ensure that users are billed according to actual network usage no matter which port they may use at any one time.

ORIGINALITY

The University of Pittsburgh is at the leading edge in adapting 802.1x network authentication technology to a wired network infrastructure. As a result, the University provided valuable data to all three companies involved in the project in order to refine their hardware and software offerings to support use in conjunction with wired network infrastructure. Because the University was among the very first to implement the 802.1x authentication protocol for wired networks, the project team had no body of experience in other schools or corporate settings from which to draw.

SUCCESS

The University considers its pilot implementation of 802.1x to be highly successful. The system was fully implemented for the Pittsburgh Campus Residence Halls in time for students to arrive for the start of the fall term. The client software is sufficiently easy to configure that a single-page handout was all that students needed to successfully connect to the network. Most users were able to connect with no additional assistance from CSSD support staff.

One of the chief successes of the pilot program was in the willingness of the vendors involved with the project to work both with the University and with each other to resolve problems that arose quickly and effectively. Each of the vendors proved to be highly motivated to resolve issues and make code revisions and bug fixes as quickly as possible.

DIFFICULTY

As the University was one of the first schools or companies anywhere to adopt 802.1x authentication for wired network service, the project team quickly discovered that there is very little information available on how to accomplish this successfully. Timing issues with requests and acknowledgements in the user authentication process had to be resolved. Further, some problems were encountered with the Cisco switches, Microsoft IAS Server, and Meetinghouse software client that all had to be resolved before the system could be completed.

In addition, some problems involving a low number of users were encountered after students began attempting to connect. All of these problems were ultimately determined to be software-related.