

## New NAC at Oregon CC Delivers at All Levels

Community colleges have changed over the years. Back in the day, students came and went. They spent a few hours on campus and then left to go on to do other things – they went home, they went to work, they just went somewhere else.

That's was then.

Now, students are spending more time on campus and it doesn't matter if they are part of Generation Y or not. Our students run the gamut from straight out of high school to professionals polishing their skills to seniors trying something new.

One thing they have in common is that they all have portable computing devices – everything from laptops and iPads to smart devices like Droids and iPhones. And they want to be connected at all times. Our students are plugged in and they expect to be able to use any device they bring with them.

Southwestern Oregon Community College is unique in the sense that our student demographic includes a campus residential housing population. These apartments are thought of as homes and our network needs to accommodate all the home-like devices that may not typically be present on a community college campus – such as Skype capability and a variety of gaming devices.

A few years ago, we didn't give as much

consideration to these types of devices on the SOCC network and whether or not they met the safe computing practices of our IT security policies. We needed to address the growing issue of personally owned (i.e., unmanaged) devices accessing our network along with a growing demand for wireless access campus-wide. For us it was fundamental that we get a handle on what was happening on our network.

Originally, we looked to the promise of network access control (NAC) to provide the tools to help us run the college IT operations. The several different NAC methods proposed by vendors fell into two camps: switch manipulation and appliance-based.

We selected Lockdown Networks and the switch manipulation method to take control of Layer 2 switching infrastructure. However, with limited staff resources this method was burdensome and time-consuming. After only a few months, it was obvious that we needed a differ-



BY  
ROCKY LAVOIE

ASSISTANT DIRECTOR OF  
INFORMATION SERVICES  
SOUTHWESTERN OREGON  
COMMUNITY COLLEGE

**We needed to address the growing number of personally-owned devices accessing our network.**

ent strategy.

We stepped back to re-evaluate our network and security requirements and to identify what we really wanted to accomplish. What did we need? What did we want? How would it make SOCC a better college?

Our basic issues and requirements had not changed. We still needed to be able to identify who and what

was on the network. We still needed to enforce our IT security policies. And we still needed to provide students and faculty with reliable network access.

What we wanted now was to be able to do it quickly, easily, and without a lot of hassle for our relatively small team. We also wanted a NAC solution that would work with an ever-expanding universe of new computing devices without having to start over with each new product wave.

All of our students, including commuters and resident students, needed access to the same services from any location. Our residents

also have access to shared drives and storage areas on the SAN; making it especially important that their malware protection is current.

An increase in the number of students registering for both on-campus and distance learning classes also meant that the volume of access and bandwidth requirements would increase. Whatever we chose would need to be able to handle the volume.

The SOCC network infrastructure is complex; we're essentially the network for a small city. We're using a Cisco hub and spoke layout with a 6509 at the distribution layer and 4500 Cisco switches at the edge. Whatever NAC solution we selected would need to be able to integrate without having to upgrade the entire network.

The Safe•Connect NAC solution from Impulse Point fulfilled all of these requirements. The product is software-appliance based and operates at Layer 3 without any Layer 2 switch manipulation. The system operates in an out-of-line network fashion and it is highly scalable, so we're able to handle everyone at one time – even if we should happen to double or triple the number of users accessing the network. This means that during peak times, such as registration and back-to-school, we don't have to worry about the network crashing. The entire campus

See *Oregon*, pg. 10, col. 1

### Safe•Connect Network Access Control

Visit [www.SimplifyNAC.com](http://www.SimplifyNAC.com)

### Oregon, from page 9, col. 4

now has wireless capability and Safe•Connect works equally as well whether the student is connecting wirelessly from the library, dorms, or from home.

Peer-to-peer file sharing also used to be a problem for us and like many college campuses; we've had our brushes with RIAA (Recording Industry Association of America) violations. Safe•Connect allowed us to "slam the door" on illegal file sharing and students are better educated about what they can and cannot do on the network.

One benefit to selecting Safe•Connect was the product's track record of being able to identify new devices and provide that information in a relatively short time frame. When the

iPad was first introduced, it was fingerprinted for us and we were able to recognize it and provide access to our students within 24 hours.

Safe•Connect is provided as a managed service, so whenever new devices come out, or anti-virus or operating system version upgrades are announced, we automatically receive them. We don't have to remember to search for them and that makes us more efficient.

A new device type connecting to the network doesn't shake us up the way it used to do. We know that when a new device hits the market, we'll be able to provide our students with prompt access while ensuring the security of our network. ▲