# Mobile Security

## Roll out a wireless LAN solution to keep your network and students secure.

It didn't take long for Bret Krebeck to verify the integrity of the security of Rock Valley College's wireless local area network (WLAN). While launching a countermeasure to mitigate rogue access, the system administrator inadvertently hindered work within a WLAN class by blocking students' wireless access within the lab.

"I forgot that they had class," he acknowledges. "The countermeasure I took automatically rendered the access point unusable."

Within a matter of minutes, Krebeck was able to fix the predicament on the fly, thanks to the versatility of the community college's 3Com WLAN Manager, a solution deployed at the Rockford, Ill., campus last year.

"It allows you to determine where and how you launch countermeasures," Krebeck explains. "I could just tweak it back so it wasn't operating in the lab."

With wireless access spanning 90 percent of the college's physical campus — which encompasses five separate sites — the need for a robust security solution was imperative to the success of Rock Valley's wireless initiative. The college is among a growing number of schools and universities relying on WLANs to deliver a broader range of services to both students and faculty. Yet with this benefit comes a host of threats that must be impeded with reliable authentication and policy-based user access safeguards, as well as tools that thwart viruses and other types of malicious code from infiltrating a network through a student's notebook or mobile device. Since administrators have little control over these devices, systems must be in place to filter out harmful programming or attachments and, in some instances, deny network access completely.

Rock Valley found all the protection it needed in the 3Com WLAN Manager, which works with the college's four WX1200 wireless switches, each of which can accommodate up to 12 managed access points (MAPs). The solution enables simple and accurate operation of the college's entire WLAN by keeping administrators aware of all air space activities including detecting and locating rogue access points, ad-hoc networks or other radio frequency (RF) interferers.

"We didn't want students putting up their own access points or even an employee sticking one into an office, as that is a major security breach," says Krebeck, who lauds the 3Com solution's rogue detection and identification capability. "And even more, we didn't want to have to walk around and find them," he adds.

For further protection, the 3Com WLAN Manager automatically adjusts MAP power to eliminate coverage gaps and optimize RF performance, as well as manages, secures and tracks on a per-user or per-group basis to all services on the wireless network. Improved user group authenticated access control, consistently enforced roaming policies and monitored bandwidth usage are additional features that give Krebeck peace of mind when it comes to the security of Rock Valley's WLAN.

"We have a management console that allows us to see the status of all access points, push updates and reboot remotely," he explains of the software tool.

The scalability of the solution is another reason the system administrator selected the 3Com product, which allows supplemental wireless switches and MAPs to be easily added at any time. "We needed a way to grow our network," Krebeck explains, noting that the college still has some room for expansion, with 32 of 36 MAPs currently being utilized. "This gives us the versatility to add switches and access points as we need them."

### Students Go Wireless

That need may present itself shortly, as the college is preparing to grant student access to the WLAN in the spring. "We had to wait because students didn't have individual user names and passwords until [recently]," Krebeck says, noting that faculty and administrators have been accessing the college's WLAN for more than a year.

As an increasing number of Rock Valley students began to inquire about wireless access, the school recognized its desire to stay ahead of the curve, and provided them with their own

Bret Krebeck
System Administrator
Rock Valley College
Rockford, Ill.

identification and passwords.

"It was important to us to roll this out before it was needed," says Krebeck, who attributes the somewhat relaxed implementation pace to the school's robust wired network, which already provides a significant number of walk-up workstations for students through more than 2,500 wired switch ports.

"We felt it was the right time to provide students with wireless access, although right now, it is more for convenience," he acknowledges. "We've been telling them that it's coming, and now they are chomping at the bit for it," adds Krebeck, who anticipates that wireless usage on campus will double once student access is granted.

Rock Valley College has further bolstered its network security with the implementation of a TippingPoint intrusion prevention system (IPS), an appliance that blocks malicious and unwanted network traffic, while allowing legitimate traffic to pass through unimpeded. With digital vaccines that protect against emerging threats and bandwidth capabilities that stop rogue applications such as peer-to-peer and instant messaging from infiltrating the network, the TippingPoint IPS eliminates the need for costly ad-hoc patching while delivering the highest level of security.

"We had viruses, spyware and adware creeping in through our firewall," Krebeck recalls, noting that the college experienced some significant network outages as a result. "We have a great firewall, but it's just not equipped to block these sorts of attacks," he concedes. "This product gives us gateway security and adds another layer to our perimeter security."

Even more, the TippingPoint solution has increased the uptime and availability of Rock Valley's network since it was installed. "We have not undergone a virus attack that impacted the network," Krebeck reports. "That is very significant for us."

The purchase of a second TippingPoint appliance — which features two additional segments for protection — has afforded additional benefits to the college. With one of those segments dedicated to remote access and VPN users, Rock Valley College is able to provide its remote employees with Internet and RVC resources without leaving itself vulnerable to any threats.

"It protects us from them and them from us," Krebeck explains. "We can control to a great degree what we have on the laptops and desktops at Rock Valley, but there is no guarantee as to what sort of desktop prevention [these users] have [at home]."

To increase its security even further, the college is now preparing to roll out another feature of its TippingPoint IPS, Quarantine, which prevents infected devices from harming neighboring systems and provides a rich set of actions in response. "What's very attractive to us is that it does not require the client to be run on a workstation, which is a lot of work and just not as desirable," says Krebeck. "This solution is very exciting for us."

Rock Valley also has plans to pilot mobile PDA (personal digital assistant) connectivity through the WLAN next year.

Throughout Rock Valley's implementation of the multiple layers of its network security solution, CDW•G has provided significant support, Krebeck notes. From tapping the knowledge of CDW•G's product experts, to enjoying attractive pricing, to relying on quick shipments of orders, the college has benefited greatly from its partnership.

"CDW•G helped me determine which WLAN solution to purchase while staying within my budget," Krebeck reveals. "They have also provided us access to their team of product experts, who have shown me exactly how I would benefit (from a particular solution)." Furthermore, the system administrator notes, "I can order with confidence and in almost all cases, CDW•G has the best price."