

## in a nutshell...

### Industry

Education

### About Flagler College

Flagler College is a private, four-year liberal arts college for 2,000 students, located in St. Augustine, Florida

### Network Environment

100 Mbps Ethernet network spanning more than ten buildings with 2,300 users; 100 Macintosh and 400 Windows PC network.

### The Challenge

Network slowdowns resulting from a combination of virus traffic from dormitories and UDP traffic from one user's computer.

### The Solution

Using EtherPeek, the IT team immediately identified the specific traffic type causing the problems and the sources. They reconfigured some network devices to reject the virus traffic and normal performance returned. For the UDP traffic, they removed the student's laptop from the network within 45 minutes of discovering the problem.

## College Runs a Lean Response Team with EtherPeek

---

With a staff of four managing some 2300 users on a 100Mbps Ethernet network that spans more than ten different buildings, Joe Provenza knows that it takes the best network management tools to maintain high efficiency and rapid response. That's why he relies on the EtherPeek product family from WildPackets for his network fault analysis and troubleshooting needs.

Provenza is Technology Services Director at Flagler College, a private liberal arts college located in St. Augustine, Florida. After Provenza came on the job in 2000, the college decided to upgrade its network significantly, moving to an all-Cisco network from a hodgepodge of products, and more importantly, opening up the campus network to student traffic from dormitories. "We run a more buttoned-down network than many colleges," he says, "so bringing dorm room traffic onto the network represented a major change for us."

To prepare for the upgraded network, Provenza and his team searched for a powerful network monitoring and troubleshooting tool that would allow them to spot and quickly repair any new performance or security issues. After rejecting other products as being unreasonably expensive, Provenza acted on a tip from the CIO of another university to check out EtherPeek. "From the beginning, our experience with EtherPeek has been a positive one," Provenza says. "Even without any training, we were able to use it almost immediately to find and analyze problems."

While the team quickly made EtherPeek a standard part of its network maintenance toolkit for issues like printing problems, the first major test of the product's effectiveness came in the fall of 2002, when the college added dormitory traffic to its network. "Almost the moment we turned up the dormitory connections, our network began to slow down," Provenza says. While dorm traffic was the likely cause, the IT team needed to identify the specific traffic type in order to deal with it.

“We started up EtherPeek and almost immediately we could see that the problem was a huge volume of virus traffic coming from the student dorms,” says Provenza. “Within minutes, we reconfigured some network devices to reject the virus traffic, and performance came back up to normal.”

More recently, the IT staff recognized a slowdown in Internet traffic and initially thought that its intrusion detection equipment was at fault. Upon examining the traffic with EtherPeek, however, the team immediately saw that the excess traffic was UDP packets, and that they were all coming from one student’s computer. EtherPeek enabled fast action: “We were on site removing the student’s laptop from the network within 45 minutes of

discovering the problem,” says Provenza, “Without EtherPeek, we probably would have been at that problem all day and into the next, because it’s a needle in a haystack unless you’ve got something that lets you look at live traffic on the network.”

“It’s very impressive, what we’ve been able to do with EtherPeek when we’ve needed it... It’s been invaluable in the few real emergencies we’ve had here.”

Joe Provenza

In another instance, EtherPeek actually helped

Provenza’s team show a manufacturer how to upgrade its product. The college had deployed a device to aggregate T1 traffic from three different providers, but soon after deployment, the device was bogging down. By capturing trace files and sending them to the manufacturer’s engineering team, Provenza helped the manufacturer to recognize the issue: because the device wasn’t designed for untrusted networks, the manufacturer needed to revise its feature set in order to make the product useful for a relatively “open” environment like a university. Once the design changes were made, the product worked flawlessly.

“It’s very impressive, what we’ve been able to do with EtherPeek when we’ve needed it,” says Provenza. “It’s been invaluable in the few real emergencies we’ve had here.”

EtherPeek’s award-winning interface and its ability to analyze live traffic during capture were key elements that enabled such rapid responses, but these features have also proven themselves for daily maintenance and relatively minor issues. When integrating the college’s 100-system Macintosh network into Microsoft Active Directory, for example, the authentication process was unexpectedly taking a long time. By analyzing the transactions with EtherPeek, the team realized that the authentication traffic was taking a different route than they had anticipated. After capturing trace files and working through them with technicians at Apple, they were soon able to improve authentication performance.



### About WildPackets

Since 1990, WildPackets has been advancing the science of network fault analysis. From the desktop to the datacenter; wireless LANs to Gigabit backbones, local segments to distributed, WildPackets products enable IT organizations to quickly find and fix problems affecting network services. WildPackets products are sold in over 60 countries through a broad network of channel and strategic partners. Over 5,000 customers across all industrial sectors deploy WildPackets products, including Agilent, Cisco Systems, Comcast, EDS, Microsoft, Siemens AG, Unisys, Motorola and Deutsche Bank.

### WildPackets Academy

WildPackets Academy offers comprehensive network analysis instruction, meeting the professional requirements of network managers at all levels. All course offerings are available in public venues and as customizable on-site programs. For complete course outlines and schedules, visit [www.wildpackets.com/academy](http://www.wildpackets.com/academy)

With licenses for EtherPeek on both Windows and Macintosh platforms, Provenza feels he has everything he needs to maintain network uptime and performance without increasing his head count. "We run a small staff here," he says. "Most schools our size have a lot more people on the IT staff. Thanks to advanced tools like EtherPeek, we can handle a lot of work quickly and keep our costs down."

### WildPackets, Inc.

1340 Treat Blvd., Suite 500  
Walnut Creek, CA 94597  
[www.wildpackets.com](http://www.wildpackets.com)