

in a nutshell...

Industry
Medical Education

Network Environment

An extensive, tightly integrated switched Gigabit Ethernet network links Cornell Weill Medical College to New York Presbyterian Hospital, Memorial Sloan-Kettering Cancer Center, the Hospital for Special Surgery, and Rockefeller University. Three overlapping ISPs link Cornell Weill Medical College to the outside world. At peak hours, network traffic consists of roughly 10,000 internal logical addresses, and runs 30–40 MBits/sec.

The Challenge

Weill Medical College needed to have immediate visibility to large volumes of network data at any moment. Its complex, multi-faceted infrastructure required comprehensive monitoring and analysis to be performed daily. In addition to monitoring and reporting, the college needed a versatile security tool.

The Solution

OmniPeek has been employed for troubleshooting, monitoring, analyzing and securing this large, dispersed enterprise network.

Cornell University Weill Medical College Utilizes OmniPeek

Increasing Network Complexity at a Multi-Site Medical Center

Today's enterprise networks are more complex than ever. In the digital age, it's hard to find a medium or large organization that doesn't use intranets, extranets, remote access, and other high-end technologies to increase efficiency and effectiveness. Networks are no longer small entities that can be easily managed, monitored, and secured. The more an organization becomes dependent on the correct operation of the network, the more critical network reliability issues become. Increased network complexity and demands for increased reliability have focused attention on the ability of network management tools to perform the job for which they are intended.

Increasingly, these tools must be able to keep up with the demands of emerging and convergent technologies, as well as be affordable, easy-to-use, and offer continuous ROI.

With so many technological advances and so many hardware permutations possible, it is easy to go wrong when establishing a viable network

environment. If the network is designed and managed properly, optimum performance and reliability are achievable.

Deploying consistently-performing networks capable of delivering data on demand is even more crucial in hospital environments. A medical college remotely but integrally connected to several critical care facilities is a prime example of an institution that must have uninterrupted network access. Implementing a trouble-free network environment is a key factor in successfully fulfilling the charter to deliver immediate and often vital care.

“

OmniPeek gives us the ability to troubleshoot and monitor quickly and effectively. It's also a gorgeous tool for securing our network and detecting network attacks.

—Dr. Steven M. Erde

*Chief Security Officer and
Senior Director of the Office of
Academic Computing
Cornell University Weill Medical College*

”

Using OmniPeek, network engineers can:

- Analyze traffic from any local network segment, including 10GbE, Gigabit and WAN segments, as well as any network segment configured with OmniEngine
- Analyze and troubleshoot both data and media traffic using one single product
- Not only view the high-level network traffic via “Dashboard,” but also drill down to see which nodes are communicating, which protocols and sub-protocols are being transmitted, and which traffic characteristics are affecting network performance
- Change filters on the fly without having to stop and restart packet captures
- View packet-stream based analytics by conversation pair, instantly locating network events
- View local captures, remote captures, or a combination of local and remote captures
- View network traffic in its intended form like PDF, HTML pages, Email, IM, etc.

The Medical College

The Weill Medical College of Cornell University, located in New York City, is among the top-ranked clinical and medical research centers in the country. The Weill Graduate School of Medical Sciences is part of a large biomedical complex that includes three major medical centers in the region. Cornell’s faculty includes a handful of Nobel laureates and the University, in addition to offering degrees in medicine, offers Ph.D. programs in biomedical research, education, and patient care. The Weill Medical College is divided into 20 academic departments: seven focus on the sciences underlying clinical medicine and thirteen encompass the study, treatment, and prevention of human diseases and maternity care. In addition to its affiliation with New York Presbyterian Hospital, Weill Medical College and Graduate School maintains major affiliations with Memorial Sloan-Kettering Cancer Center, Hospital for Special Surgery, and with the metropolitan-area institutions that constitute New York Presbyterian Healthcare Network.

Delivering Critical Data for Critical Care

Beyond coping with the increasing complexity of the distributed networking environment, network managers in medical facilities have the additional pressure of insuring network availability in a crisis-laden environment. Tools that are easily deployed and provide immediate visibility to all elements of the network are essential.

“We needed to figure out what is happening on our huge, diverse network at any moment. OmniPeek gives us the ability to troubleshoot and monitor quickly and effectively. It’s also a gorgeous tool for securing our network and detecting network attacks,” says Dr. Steven M. Erde, Chief Security Officer and Senior Director of the Office of Academic Computing, Cornell University Weill Medical College.

The IT staff of Cornell Weill Medical College is responsible for delivering network access at all hours and at all times - a critical requirement. Their constituency must have an unfailing, efficient, and secure network to exchange and maintain the confidentiality of patient information. In order to deliver critical data on demand, Cornell’s IT staff needs the right tools to insure uninterrupted productivity.

Network analyzers, essential tools for essential networks, have had to keep pace with the demands of modern networks for increased productivity and data delivery requirements. It no longer suffices for an analyzer to capture packets and know how to decode every protocol under the sun. Not only does the network analyzer have to evolve to keep up with new protocols and applications, it must be able to diagnose problems associated with the various media running on today’s networks automatically.

Cornell Weill’s Broad, Distributed Network Environment

Cornell Weill Medical College is linked to New York Presbyterian Hospital, Memorial Sloan-Kettering Cancer Center, the Hospital for Special Surgery, and Rockefeller University with an extensive, tightly integrated switched Gigabit Ethernet network. At the present time, the collapsed backbone Gigabit network spans a Metropolitan Area Network (MAN) and includes additional WAN lines.

Three overlapping ISPs link Cornell Weill Medical College to the outside world. At peak hours, network traffic consists of roughly 10,000 internal logical addresses, and runs 30 40 MBits/sec. With over 250 Mbits of internet connectivity, the network must be able to handle massive amounts of traffic on a daily basis.

Dr. Steven M. Erde, Chief Security Officer and Senior Director of the Office of Academic Computing at the University, relates that monitoring and troubleshooting this huge, diverse network is their main issue, while security is another important concern. “We want to figure out what is happening with our network at any moment. We also need to be able to detect web attacks, viruses, worms, and security breaches.”

About WildPackets

WildPackets, Inc., founded in 1990, develops network and application analysis solutions that enable organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. WildPackets has amassed more than 6,000 customers and its products are sold in over 60 countries in all industrial sectors. Customers include Safeway, Boeing, Siemens, AT&T, Motorola and over 80% of the Fortune 1000. For further information, please visit www.wildpackets.com.

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

WildPackets, Inc.

1340 Treat Blvd., Suite 500
Walnut Creek, CA 94597
www.wildpackets.com

Trouble-Free Networking with OmniPeek

To gain the visibility to adequately analyze their network traffic, Dr. Erde turned to OmniPeek. As the Cornell campus network converged media and new technologies into an increasingly diverse and complex infrastructure, Dr. Erde looked to OmniPeek's Expert System to sort through, analyze, diagnose, and isolate his large volumes of network data. Expert Systems need to be precise in pinpointing problems, relevant for current networks and topologies, able to accurately detect real symptoms, and diagnose real problems. OmniPeek has been designed to excel at all of these requirements, incorporating industry leading expert technology to provide precise, contemporary analysis of today's complex networks.

"OmniPeek gives us the ability to create complex filters, including random ASCII strings. The advanced filter settings allow us to detect new web attacks. It's so easy to code a filter and search for actual attack strings in the clear. It's our main tool for securing the network."

Dr. Erde has realized additional benefits through employing the many relevant features of OmniPeek. His "favorites" list of features/benefits includes:

- Readily customizable filters that ease the process of monitoring and troubleshooting
- Advanced, accessible interface for easily identifying complex network issues
- Real-time multiple trace file analysis
- Ability to easily detect breaches and secure the network
- Ability to automatically code a filter to identify web attacks

Optimizing Network Reliability

Sophisticated network management tools that help ensure the availability of mission critical networks are in high demand. To do the job, network management tools with expert systems need to be more precise in pinpointing problems than ever. They need to be relevant for current networks and topologies. They need to detect real symptoms and diagnose real problems. And, they need to provide information based on real experience, yet allow customization to accurately reflect a specific network environment.

OmniPeek has been carefully designed to help IT Professionals analyze and diagnose increasingly diverse volumes of network data, providing precise, contemporary analysis of the problems facing today's networks. It has given Cornell Weill Medical College and its sister organizations the ability to monitor, troubleshoot, create reports, and enjoy an increasingly secure network that delivers critical information consistently and on demand.

