

### PRESS CONTACTS:

#### Connect Public Relations

Spencer Parkinson  
spencerp@connectpr.com  
(801) 373-7888 x119

#### Network Instruments, LLC

Stephen Brown  
sbrown@networkinstruments.com  
(952) 358-3820

### Network Instruments® Delivers Enterprise-Wide Reporting with Observer® Reporting Server

*New Version of Observer Introduces High-Level Reporting, Security Forensics, MPLS Analysis, Expansion of VoIP and Application Analysis, IPv6 Support, and SSL/SSH Decryption*

**Minneapolis, MN – March 12, 2007** – Network Instruments, a leading provider of innovative analysis solutions for in-depth network intelligence and continuous availability, today announced the release of its Observer Reporting Server, which provides high-level reporting on network and application activities across the enterprise. The Observer Reporting Server connects to multiple Observer Suite consoles and aggregates the critical network performance metrics into an overall view of network health.

In addition to providing an easy-to-access view of network performance, reports can be segmented by individual business units, user groups, or infrastructure types. This allows network managers to quickly view bandwidth utilization or application use by department. If managers notice unexpectedly high bandwidth use from a department, they can quickly and seamlessly drill down on the report to the individual link or user detail using the Reporting Server and Observer. Root cause and Expert analysis can then be performed using Observer.

“The Reporting Server with Observer answers the need of enterprise to quickly move from high-level performance monitoring to root-cause analysis,” said Douglas Smith, president of Network Instruments. “With the Reporting Server the network team can view their global network, and within a few clicks they can drill down to isolate any problem on the network.”

#### Security Forensics

Beyond being able to drill from an enterprise-wide view of network activity down to specific links, it is critical for network teams to be able to isolate specific performance problems to a network, application, or security cause. Often IT teams waste hours attempting to replicate the issue or blaming each other for causing the problem.

To facilitate fast problem resolution, Network Instruments has expanded the retrospective network analysis capabilities of GigaStor™ to identify security breaches. GigaStor operates like a security camera recording everything traversing the network for future analysis. With post-capture Security Forensics, GigaStor determines whether a security breach has occurred by comparing the historically captured traffic against a list of thousands of known attacks and anomalies. If a breach has been identified, GigaStor provides drill-down analysis to determine the source and time of the occurrence.

“GigaStor’s comprehensive forensics and Expert analysis has changed the way network, application, and security teams resolve network problems,” said Charles Thompson, manager of sales engineering at Network Instruments. “Rather than arguing about the source of the problem, the teams can focus on the solution. With Security Forensics, GigaStor can now conduct Expert analysis for network, application and security issues, identify the problem, and eliminate the guess work for IT managers.”

#### Observer 12 Features

In addition to Security Forensics and the Reporting Server, Observer offers several new features that expand its position as a leading analysis solution.

#### MPLS Analysis and Troubleshooting

Observer provides detailed analysis of an organization’s MPLS network, including quickly isolating MPLS issues, tracking varying MPLS queues, and segmenting the data by label, precedence, and embedded protocol type.

If an organization is transitioning from ATM or frame relay to MPLS, Observer can provide extensive MPLS reporting to verify that network performance expectations are being met. Service Level Agreements can also be enforced by creating MPLS-specific alarms.

#### VoIP Expansion

According to a recently released Network Instruments survey, 45 percent of network engineers indicated they have VoIP running on their network. The adoption of VoIP will continue to increase during 2007 with 30 percent of respondents planning to implement the technology in the next 12 months. Network Instruments continues to invest and expand the Observer VoIP offering to provide greater support to the countless engineers that use Observer to monitor and optimize VoIP traffic.

Observer now includes support for Avaya CCMS and Nortel UNISlim protocols as well as providing long-term trending for call detail records (CDR).

### **Application Analysis**

Many organizations use Observer for monitoring application performance and isolating application problems. It provides true application response time, allowing network managers to prioritize, configure, and optimize application performance. Observer now offers integrated support for Microsoft Networking (Server Message Block), in addition to Citrix, Oracle, VoIP, Microsoft Exchange, HTTP, DNS, SQL, FTP, POP3, Telnet, SMTP, and SNMP. Managers can also set triggers and alarms on any application metric, ensuring they know about application problems before users are affected.

### **SSL and SSH Decryption**

Observer can be configured with Secure Socket Layer (SSL) and Secure Shell (SSH) certificates to decrypt secure data.

### **IPv6**

In line with a recent government mandate requiring that all government agencies support IPv6 by 2008, Observer now tracks, reports, and monitors IPv6 traffic. All Observer data is listed with the appropriate IPv6 address displayed and, more importantly, IPv6 has been pulled through and integrated with all Observer features, including Forensics, Application Analysis, Expert, and VoIP Analysis.

### **Automatic Packet Correlation**

Observer tracks conversations or transactions as they traverse multiple segments, hops, and routes. Known as MultiHop Analysis, this process has been automated in Observer 12.

### **Product Pricing**

Network Instruments has added many significant enhancements to Observer, and pricing for Observer Standard, Observer Expert, and Observer Suite remains the same. Observer Standard, now with IPv6 support and SSL/SSH decryption, is \$995. Observer Expert, with over 70 VoIP-specific metrics, MultiHop Analysis, MPLS Analysis, Application Analysis, and Stream Reconstruction, is \$2,895. Observer Suite, with an SNMP console and Web Reporting, is \$3,995. Deployment options for the Observer Reporting Server include: software only, hardware appliance, and combination appliance with Observer Suite to connect directly to probes. The Reporting Server price begins at \$10,000. The GigaStor begins at \$20,000 for a two-port configuration. Additional product information is available at [www.networkinstruments.com](http://www.networkinstruments.com).

###

### **About Network Instruments**

Network Instruments provides in-depth network intelligence and continuous network availability through innovative analysis solutions. Enterprise network professionals depend on Network Instruments' Observer product line for unparalleled network visibility to efficiently solve network problems and manage deployments. By combining a powerful management console with high-performance analysis appliances, Observer simplifies problem resolution and optimizes network and application performance. The company continues to lead the industry in ROI with its advanced Distributed Network Analysis (NI-DNA™) architecture, which successfully integrates comprehensive analysis functionality across heterogeneous networks through a single monitoring interface. Network Instruments is headquartered in Minneapolis with sales offices worldwide and distributors in over 50 countries. For more information about the company, products, technology, NI-DNA, becoming a partner, and NI University please visit [www.networkinstruments.com](http://www.networkinstruments.com).