



## OBSERVER VS. SNIFFER

**Network Instruments LLC's Observer Suite 10.1 and Gigabit Rack Mount Probe together are clearly the networking tools of choice for solving – or avoiding – virtually every kind of problem your network might suffer.**

The best protocol analyzer does a great deal more than just decode common protocol streams and provide moving-skyline depictions of network activity levels. Network troubleshooters, engineers, administrators and capacity planners need a protocol analyzer they can use on any network segment, no matter how distant, for any kind of network problem, no matter how intractable.

Whether the underlying connectivity is Gigabit Ethernet, Fast Ethernet, wireless 802.11a/b/g or some other topology, the protocol analyzer must be able to understand virtually every protocol at every level of the OSI Reference Model, quickly help identify and solve any network problem, implement sophisticated filters, triggers and alarms, offer both high-level and detailed expert analysis of network activity, produce useful, timely reports, integrate via SNMP, RMON I and RMON II with other network monitoring tools, use the network frugally, scale well, be intuitively easy to use, enforce good security and be affordable.

Choosing the best protocol analysis tool means you'll have one less thing to worry about in your day-to-day, week-to-week and month-to-month efforts to keep your network up and running, healthy and reliable. It'll also increase the productivity of your network troubleshooters, engineers, administrators and capacity planners.

A protocol analyzer is very likely the most important tool a network staff person will ever use, and Network Testing Labs has tough criteria for protocol analysis tools as well as network probes.

A network probe becomes a network administrator's eyes and ears on the backbone and at each remote site. A really excellent network probe makes troubleshooting and monitoring remote segments as easy as troubleshooting and monitoring local segments. It gives a network administrator every protocol analysis capability for the remote site that the administrator has for the local network.

For every kind of infrastructure, from Gigabit Ethernet to wireless 802.11(x), a network probe must make remote segments appear as if they're local so a troubleshooter can see, understand and fix a problem. The probe must be easy to install and configure, it must be reliable, it must be scalable, it must be secure and it must be cost-effective. Furthermore, the probe must use network bandwidth frugally.

To find out which protocol analyzer and probe you should be using, we recently evaluated Network Instruments, LLC's Observer Suite 10.1 and Network General Corporation's Sniffer Portable 4.8 in a head-to-head comparison. Both vendors claim their respective products meet our criteria for best protocol analyzer. We tested these claims by putting the products through a grueling and comprehensive series of protocol analysis tasks in our lab. We also compared Network Instruments' Observer Suite 10.1 software and Gigabit Rack Mount Probe device with Network General's Sniffer Distributed Expert software and Sniffer s6040 Gigabit probe device.

Our tests revealed Network Instruments' Observer Suite 10.1 is clearly the most capable, sophisticated, easy to use and feature-rich protocol analysis product. Observer Suite showed itself to be the most scalable, most protocol-savvy and most useful. Moreover, the combination of Observer Suite and Gigabit Rack Mount Probe emerged from our battery of stress tests with flying colors. The Network Instruments hardware probe and protocol analysis software easily surpassed Sniffer Distributed Expert and the s6040 hardware appliance in every category.

Network Instruments' Observer Suite and Gigabit Rack Mount Probe wins the Network Testing Labs World Class Award for best protocol analysis tool and network probe.

***“Our tests revealed Network Instruments' Observer Suite 10.1 is clearly the most capable, sophisticated, easy to use and feature-rich protocol analysis product.”***

***-Barry Nance, Network Testing Labs***

## Decoding and Monitoring

Whether Observer Suite or Sniffer Portable decodes more protocols than the other depends on what you consider a distinct protocol and what you consider a sub-protocol, and you could easily conclude either one decodes more protocols. However, the important consideration is whether a particular tool decodes the protocols on your network. In our tests, Observer Suite gained a clear advantage by decoding over 500 distinct protocols at a far lower price than Sniffer Portable.

Here is a list of just a few of the protocols, both common and not-so-common, that Observer Suite supports:

- 3COM - MIP - Extensions to Mobile IP
- 802.11 - WEP - Wireless Encryption Protocol
- Cisco - ISL - Inter-Switch Link Protocol
- Cisco - VTP - Virtual Trunking Protocol
- Oracle - database transactions
- SNA - DIAP - Document Interchange Architecture Protocol
- SQL Server and Adaptive Server Tabular Data Stream (TDS)
- Sun - NIS - Network Information Services
- TCP/IP - IPv6AUTH - Internet Protocol Version 6 Authentication Header - RFC 2402
- TCP/IP - LDAP - Lightweight Directory Access Protocol
- WAN - Frame Relay - Frame Relay
- WAN - HDLC - High level Data Link Control
- WAN - VoFR - Voice over Frame Relay (all Annexes)

Observer Suite's WAN Delay Analysis feature gives network troubleshooters exactly the right detail to help them see WAN link latencies and packet losses. With its coarser granularity and its focus on just mobile and voice applications, Sniffer Portable's equivalent feature is not quite as capable as Observer Suite's. Moreover, Network General charges extra for the Sniffer Portable mobile and voice options.

Observer Suite excels at monitoring and providing statistics for VLANs. Users can see real-time VLAN statistics, either independently or in the aggregate. We greatly appreciated this feature in our tests as we verified VLAN configuration data and monitored VLANs for high utilization. Sniffer Portable completely lacks a VLAN analysis feature.

Observer Suite integrates extremely well with SNMP-aware devices. A standard (no extra charge) feature of Observer Suite, the ability to comprehensively monitor and manage SNMP devices was a time-saver in our tests because it meant we didn't have to switch from using Observer Suite to some other SNMP-aware utility when we needed to reset switch or router ports. Just as it lacks a VLAN analysis capability, Sniffer Portable does not have a feature for managing SNMP-aware devices.

## Ease of Use

Observer Suite's clear and easy-to-understand packet decode display stands head and shoulders above Sniffer Portable's decode window. The Observer Suite display sports a wealth of powerful features for zooming in on packet detail, viewing related packets and, with a few mouse clicks, setting up temporary filters or tracking a specific port-pair connection. In our tests, we also found that Observer Suite can zero in on and display conversation response times.

Unlike Sniffer Portable's user interface, Observer Suite's interface is intuitive, powerful and easy to use. For example, Observer Suite anticipates the sort of detail you'll need when you drill down for more information. Sniffer Portable forces the user to navigate into (and through) extra windows that it always shows whether or not those extra windows contain relevant information.

Observer Suite's reports, whether supplied with the product or designed with Observer Suite's report generator, make quick work of such tasks as pinpointing outage trends, revealing bandwidth upgrade needs, identifying network bottlenecks and staying on top of the network's health.

In contrast, Sniffer Reporter is a separate reporting application. It allows users to generate graphical reports based on Sniffer Portable packet captures. Sniffer Reporter's bundled reports include host table lists, protocol distributions and top talker traffic summaries. As with Observer Suite, Sniffer Reporter supports the building of custom reports.

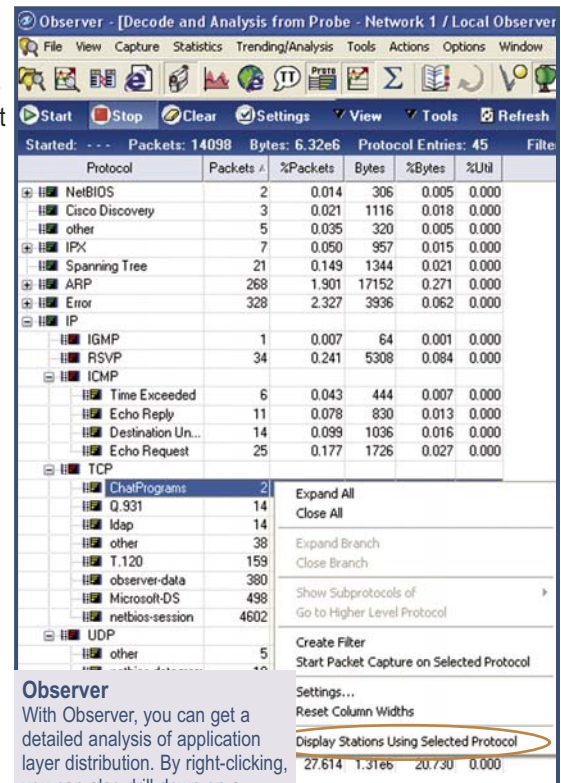
Also included in the Observer Suite product is a smart set of capacity planning tools. For instance, Observer Suite reports long-term trending statistics numerically and graphically. Furthermore, it can export these and other statistics in a variety of formats from its sophisticated database of network activity. Observer Suite's browser-based report generation, along with its third-party tool support, make capacity planning less an art and more a science. In contrast, nearly all Sniffer Portable's reports apply only to the particular packet capture file you're currently investigating.

## Conclusion

Making sure network support staff have the right protocol analyzer is critical. It's the tool troubleshooters, administrators, engineers and planners reach for first when they need to know how the network is doing and what it's carrying. Observer Suite has more features than Sniffer Portable, is easier to use and helps pinpoint network problems more quickly.

Beyond feature comparison and productivity, the two products have very different price tags. Sniffer Portable's high price is unwarranted, and we believe you'll find the difference in Return on Investment (ROI) between Observer Suite and Sniffer Portable to be striking. Observer Suite is clearly the best bang for the buck.

Based on our testing, we recommend you take a close look at Network Instruments' Observer Suite.



Category and Weight (%)	Network Instruments, LLC Observer Suite 10.0	Network General Corporation Sniffer Portable 4.8
Monitoring and Analysis (30%)	A	C
Protocols (30%)	A	A
Ease of use (20%)	A	C
Reports (10%)	A	C
Documentation and Installation (10%)	A	B
Overall Score	A	C+

**Report Card**  
Grade scale is A through F, with F=Failing and A=Perfect

## Remote Monitoring and Troubleshooting

Unfortunately, Sniffer Distributed cannot decode packets in real-time. You must first capture packets in a capture buffer and then stop the capture operation before you can begin to examine and analyze those packets.

Observer Suite, on the other hand, does offer real-time packet decoding in addition to capture buffer-based decoding. Observer Suite's huge 4 GB packet capture buffer can keep up with and store eight times more data than Sniffer Distributed can. When you're troubleshooting traffic flows and packet contents for a busy Gigabit backbone link or central switch, the extra packet buffer space can spell the difference between getting in one fell swoop just the data you need and taking several stabs at trying to have the capture buffer open at the exact moment a problem situation crosses the wire. For capacity planning purposes, Observer Suite offers a truly excellent "what if" analysis feature that's especially useful when you're allocating bandwidth to WAN links. Observer Suite acquires actual client/server transactions data from a probe and then plots response time, utilization and traffic flow statistics within different scenarios. You can, for instance, quickly see the effect of changing a WAN link from 768 kbs Frame Relay to a full T1 or the effect of increasing the number of users.

Observer Suite is head-and-shoulders above Sniffer Distributed as a capacity planning tool. The Sniffer Distributed capacity planning feature, an option that Network General calls nPO Visualizer, uses Application Response Time (ART), Frame Relay details, and its own expert analysis statistics to display trends and utilizations. However, Sniffer Distributed lacks the sophisticated "what if" analysis that's built into Observer Suite.

Observer also does a superior job of monitoring and controlling WAN-dispersed RMON-aware devices. Fully compliant with RMON-I and RMON-II, Observer Suite offers sophisticated thresholds you can set to warn of imminent device problems. Sniffer Distributed assumes you use a separate, third-party network management tool for understanding and responding to RMON messages.

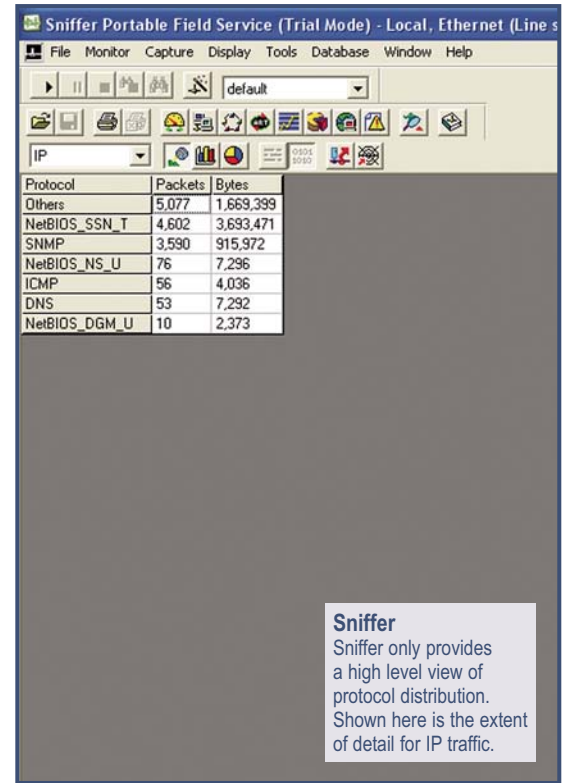
## Ease of Use

While Sniffer Portable and Sniffer Distributed are separate software products, each with its own code base and user interface, Observer Suite has the same consistent, well-designed interface when used on probe-equipped segments as it does for a local network segment. Having to turn to different tools with different user interfaces, even ones from the same manufacturer, complicates a network troubleshooter's life tremendously – especially when you're faced with multiple concurrent problems to solve. Observer Suite's well-designed, consistent and cohesive basic architecture is far superior to Sniffer's different-products-from-different-programming-teams approach.

Observer Suite's data mining feature makes the analysis of existing capture files much easier, particularly voluminous files from long capture sessions or from busy Gigabit links. Observer Suite offers a wide range of sophisticated filters you can set (and remember for subsequent analysis) prior to loading a capture file. You in essence get to reduce the data analysis job to a manageable size. Sniffer's filters are not as sophisticated as Observer Suite's, and Sniffer lacks Observer Suite's data mining feature.

With Observer Suite, multiple people (administrators, troubleshooters, engineers and capacity planners) can access Observer Suite through the same network interface adapter at the same time. To our delight, we found that Observer Suite even provides a collaboration mode for team-oriented problem solving. Using Sniffer Distributed in a multi-user environment is virtually impossible. Sniffer Distributed simply was not designed for multiple users.

Installing and configuring the Gigabit Rack Mount Probe is child's play. The Quick Start Guide needs only 11 pages – even including the requisite electrical safety guidelines – to comprehensively and clearly explain setting up a Rack Mount Probe. You only need to connect the power and network cables, initially use a monitor and keyboard to give the unit an IP address and then simply access the probe from the central Observer console. In contrast, the s6040's installation documentation consists of over 40 pages of material.



The Observer Suite and Gigabit Rack Mount Probe documentation set does a much better job of explaining and describing the effective use of the products than the Sniffer Distributed and s6040 documentation does. The Network Instruments documentation's high-quality table of contents and index will quickly take you to the reference data or list of steps to follow if you're ever unsure how to use some Observer Suite feature. The Sniffer Distributed documentation, on the other hand, isn't always logically laid out and is sometimes difficult to follow.

## Conclusion

When used with one or more Gigabit Rack Mount Probes, Observer Suite is simply the best protocol analysis and monitoring tool for troubleshooters, network administrators and capacity planners who need to keep network backbones and WAN segments healthy and ready for business.

Category and Weight (%)	Network Instruments, LLC Observer Suite 10.0 and Gigabit Rack Mount Probe	Network General Corporation Sniffer Distributed Expert and s6040 Probe
Monitoring and Analysis (30%)	A	C
Protocols (30%)	A	A
Ease of use (20%)	A	C
Reports (10%)	A	B
Documentation and Installation (10%)	A	C
<b>Overall Score</b>	<b>A</b>	<b>C+</b>

Report Card  
Grade scale is  
A through F,  
with F=Failing  
and A=Perfect



### Testbed and Methodology

We ran each protocol analyzer software product on a Windows XP-based Dell Latitude D505 computer equipped with a 1.5 GHz Pentium processor, 512 MB RAM and 30 GB hard drive.

We connected each protocol analyzer to all our Fast Ethernet network's six segments, one segment at a time. Each segment consisted of a NetWare 5.0, Windows NT 4.0 or Windows 2000 file server, an Oracle 8i, Microsoft SQL Server or Sybase Adaptive Server database server, a Netscape or Internet Information Server (IIS) Web server and 100 Windows 98, Windows ME, Windows NT, Windows XP, Windows 2000, Macintosh System 8, and Red Hat Linux 6.2 clients. The six-segment network also contained SNMP-aware switches, Cisco routers, a Covad Communications SDSL Internet link, Frame Relay DSU/CSUs and RMON I/II hardware probes.

We confronted each protocol analyzer with several problems, including unresponsive devices, connectivity breaks, excessive traffic levels (overall, port-specific Denial of Service attacks and specific protocol traffic), duplicate IP addresses, a malfunctioning switch, a malfunctioning router and dropped packets.

### About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analysis, feature articles, in-depth technology workshops, cover stories, buyer's guides and in-depth technology outlooks. Our experts have spoken on a number of topics at Comdex, PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.

### About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products. Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for ComputerWorld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World and many other publications. He's authored thousands of magazine articles as well as popular books such as Introduction to Networking (4th Edition), Network Programming in C and Client/Server LAN Programming.

He's also designed successful e-commerce Web-based applications, created database and network benchmark tools, written a variety of network diagnostic software utilities and developed a number of special-purpose networking protocols.

*You can e-mail him at [barryn@erols.com](mailto:barryn@erols.com).*

#### Vendor Details

**Network Instruments, LLC**  
10701 Red Circle Drive  
Minnetonka, MN 55343  
(952) 932-9899  
[www.networkinstruments.com](http://www.networkinstruments.com)

**Network General Corporation**  
178 E. Tasman Drive  
San Jose, CA 95134  
(408) 571-5000  
[www.networkgeneral.com](http://www.networkgeneral.com)