

# An Essential Tool for a Healthy Network

Network Instruments' Observer is a rock-solid, feature-rich protocol analyzer that's flexible, easy to use and reasonably priced.

BARRY NANCE

Ask any network administrator: "If you could have just one tool to keep your network up and running smoothly, what would it be?" The answer invariably is a protocol analyzer. A network administrator, troubleshooter or manager knows that a protocol analyzer is the right tool for the job when network problems happen or when he or she just needs to know how healthy - or how busy - the network is.

The best protocol analyzer lets you zoom in to view the contents of individual packets and zoom out to view the sum total of network activity, and it offers fine gradations in between. The best protocol analyzer discovers and identifies network nodes, monitors those nodes for availability and performance, decodes protocols, produces useful statistical summaries of network activity, helps troubleshoot problems and reports on the current status of the network's devices and connections. To zoom in and out on various aspects of the network, it lets you filter traffic based on network address, protocol type and other selection criteria.

***"Network Instruments' Observer earned the top spot in the competition..."***

The best protocol analyzer doesn't stop there. It dramatically speeds up the diagnosis of a network problem by revealing the problem's nature, location and impact. By relating current activity with a previously-captured baseline of

## The Results...

(Graded from A through F, with F = Failing and A = Perfect)

	WildPackets, Inc. EtherPeek NX 1.0	Network Instruments, LLC Observer 8.2	Sniffer Technologies Sniffer Pro 4.5
Features	C	B	C
Protocols	B	A	B
Reports	C	A	C
Ease of Use	B	A	D
Documentation	B	B	B
Installation	B	B	B
Average Score	C+	A-	C

normal activity, it even becomes part of your capacity planning toolbox by informing you of trends and changes.

To find the best protocol analyzer tool, we spent several intensive weeks exercising, stressing, poking and prodding three popular protocol analyzers at our Connecticut-based Network Testing Labs site. We looked at Sniffer Portable 4.5, offered by

Sniffer Technologies (a Network Associates, Inc. business unit), EtherPeek NX 1.0 for Windows, manufactured by WildPackets, Inc., and Observer 8.2, from Network Instruments, LLC.

While all three tools displayed network message contents and network summary data, Network Instruments' Observer earned the top spot in the competition for the breadth of protocols it decodes, its helpful expert mode commentator, its low cost, the ease with which we could navigate its screens to determine the cause of a problem and - most importantly - the wealth, usefulness and clarity of its reports.

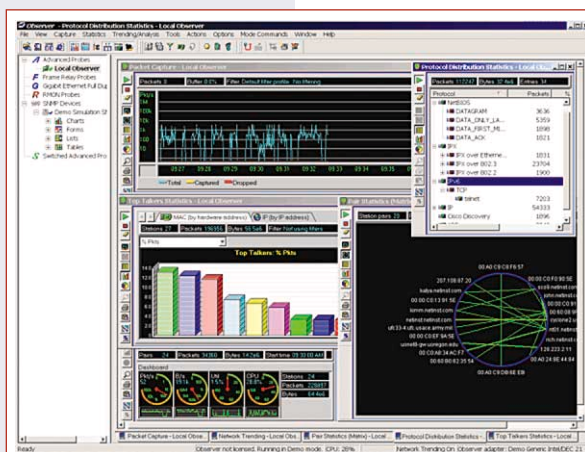
### An EKG for your Network

We found that Observer decodes over 500 protocols. WildPackets claims that EtherPeek NX can decode "hundreds" of protocols, but some of the protocols on the

vendor's decode lists aren't really separate protocols but rather just subprotocols. EtherPeek's total is more realistically about 450, while Sniffer can do just over 450.

All three protocol analyzers can decode the major protocol suites,

including Ethernet, AppleTalk, DECnet, NetBEUI, IPX/SPX, NetWare's file



Observer decodes over 500 protocols and offers a number of special features that make monitoring remote segments a breeze.

sharing NetWare Core Protocol (NCP), System Network Architecture (SNA), IBM's and Microsoft's Server Message Block (SMB), HTTP, VoIP, TCP/IP and the protocols used by TCP/IP utilities such as telnet and ftp. While all three vendors also offer remote capture probes for collecting and analyzing packets from non-local network segments, we noted that Observer's probe offers a number of special features that made monitoring remote segments a breeze. In an 802.11a or 802.11b environment, Observer, Sniffer and WildPacket's separate AiroPeek product all decode wireless messages. Observer, however, comprehensively and clearly shows such detail as wireless CRC errors, low average signal quality, low average signal strength, missed acks, short PLCP errors, high reassociation attempts and other wireless connection attributes.

Network Instruments' Observer includes an integrated SNMP console and management interface, an integrated RMON I/II console and management interface, a built-in Web server along with Web-based access to trend displays and other reports. In our evaluation, we found the EtherPeek NX and Sniffer products lacked the breadth and depth of Observer's reports, especially in the areas of trending and capacity analysis.

***“...Observer's expert mode is more helpful in diagnosing network problems than EtherPeek's or Sniffer's.”***

Observer's many filter options include network address ranges, error conditions, specific protocols and up to twenty concurrent user-definable custom offsets and values. Observer smartly helped us solve the problems we caused in the lab. Furthermore, in a refreshing example of vendor honesty, Network Instruments' Observer even identifies packets it drops when you run it on a slow computer with a bottleneck network adapter. Observer dropped no packets in our tests, but we found the vendor's keen motivation to account for every packet a sharp contrast to other vendors' attitudes. In fact, it's downright admirable.

Observer can use RMON I and RMON II to manage and collect SNMP statistics

from SNMP-aware devices. Moreover, Network Instruments offers local and remote software-based probes customers can configure to use either industry-standard RMON or Network Instruments' enhanced and augmented version of RMON, called Advanced Probe. In RMON mode, Observer's probe behaved exactly as the RMON standard demands. When we configured Observer's software probe to act as an Advanced Probe, our tests revealed that Observer's RMON enhancements make up for virtually all RMON's shortcomings. Network Instruments' RMON enhancements use network resources much more frugally than standard RMON, and they also allow for remote probe redirection, accumulation of network trending data and viewing of Advanced Probe snapshots via a Web browser. As icing on the cake, Observer probes can automatically update themselves when an administrator wants to install Network Instruments updates across a network.

To help EtherPeek monitor remote network segments, WildPackets suggests its customers buy Netopia's Timbuktu Pro. Installing Timbuktu Pro on remote segments lets EtherPeek users remotely perform diagnostics, monitor traffic, trace illicit network activities and debug network hardware and software.

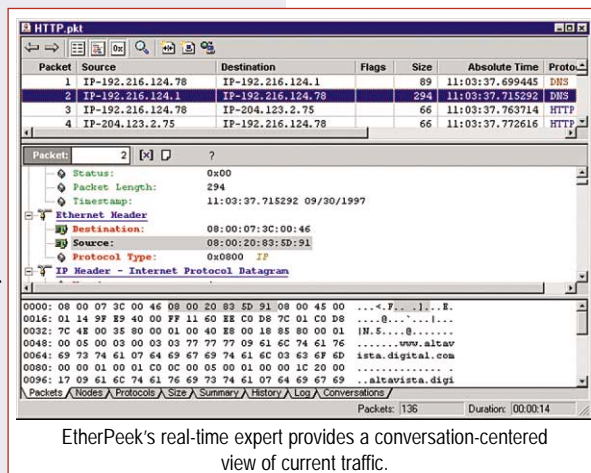
Called Sniffer Distributed, Sniffer's probe and central management components for monitoring remote network segments perform many of the same functions Observer does. Sniffer Distributed gathers statistics on network traffic, protocol distribution and application usage, then forwards the data to a central console. Significantly, Timbuktu Pro and the Sniffer Distributed product lack Observer's Advanced Probe capabilities and thus cannot exceed the design limitations of RMON I/II.

With its more than 100 expert mode events and easy-to-understand, English language explanations, Observer's expert mode is more helpful in diagnosing

network problems than EtherPeek's or Sniffer's. In addition to decoding many more types of network messages, Network Instruments' Observer includes a Router Observer component for monitoring router activity against thresholds you set, a Web Observer for keeping a watchful eye on Web servers utilization and an Internet Observer for tracking IP message traffic by source and destination. While EtherPeek NX and Sniffer can monitor individual switch ports, Observer's port tracking gives an administrator more useful bandwidth utilization information on both a port-by-port basis and an aggregate switch

throughput basis.

EtherPeek NX helped us pinpoint most of the causes of the deliberate error conditions we set up. However, EtherPeek NX's real-time expert mode feature showed its lack of maturity - it's a



EtherPeek's real-time expert provides a conversation-centered view of current traffic.

fairly recent addition to EtherPeek. The real-time expert provides a conversation-centered view of current traffic, with settable thresholds and filters to let you drill down into network activity. EtherPeek NX's expert view displays its breakdown of latency, throughput, and about 45 other problems (i.e., half of Observer's expert mode events) in a conversation-centered view of traffic. Many EtherPeek NX tests offer user-defined settings and thresholds. To help an administrator focus more narrowly on the problems at hand, these filtering criteria include network address, protocol, port, specified strings of text inside packets, packet length and error codes within packets.

We could also instruct EtherPeek, via what WildPackets calls plug-ins, to verify packet checksums, detect duplicate IP address assignments, log ftp file transfer operation file names, monitor network addresses for continuous connectivity, track telnet sessions and log Web server and news server accesses. A customer who has some programming skills can additionally create tailor-made EtherPeek NX plug-ins.

## Viewing the Reports

Observer's reports show top talkers, protocol statistics, conversation pair statistics, Internet usage, physical layer errors, transport layer errors, router statistics, switch statistics, network utilization and historical trends. The top talkers report contains a list of nodes, by bandwidth usage, and it includes bandwidth percentages, total packets, broadcasts and multicasts. The protocol statistics report categorizes network traffic by protocol, in either tabular or graphical format. The conversation pair statistics report tracks nodes exchanging network messages and graphically illustrates the nodes' conversations by drawing lines between the nodes. The Internet usage report identifies nodes connected to the Internet, by node, service (HTTP, NNTP or FTP) and Internet destination. The physical layer report tells (for Ethernet) the number of wrong-sized packets, CRC errors, collisions and alignment errors.

The server analysis report, which is one of Observer's most useful reports, graphically contrasts server response times vs. the number of concurrent requests. The Router Observer module monitors router devices, displaying total packets, total bytes, packets per second, bytes per second and device utilization. The switch monitor can continuously examine the ports on a switch to show utilization and connectivity.

Observer can also show Web server traffic data, including number of Internet connections and percentage of local network traffic. A vital signs report divulges average and maximum bandwidth utilization, total packets, CRC errors,

alignments errors, wrong-sized packets and collisions, and an Ethernet collision analysis identifies the top ten network colliders.

For browser access to its data, Observer quickly and effortlessly renders reports in dynamic Web page format. Much more

sophisticated than EtherPeek's or Sniffer's simple capture buffers, the database of historical network activity that Observer collects is the ideal foundation for its well-designed trending and capacity planning reports.

EtherPeek NX displays node, protocol, conversation, network, error, size, summary and history information. Node statistics, which are useful for tracking bandwidth usage by node, include real-time packet counts and traffic volumes as well as the total number of network nodes. Protocol statistics show network traffic volume, in packets and in bytes, by protocol and sub-protocol. This data is useful for determining which protocols or sub-protocols are using high amounts of bandwidth. Between pairs of network nodes, conversation statistics show traffic data, in bytes and packets, for each protocol or sub-protocol the pair has used. The packet size distribution statistics reveal

the number of packets, by size, that the network has carried. The summary and history statistics show network performance over time, graphed according to selectable intervals. For a user-specified interval, EtherPeek's graphing and trending feature can collect, analyze and display, via several different graph options,

node, protocol, network or summary statistics. EtherPeek can optionally render the data as Web pages.

Sniffer Portable displays useful statistics in its own right and the vendor offers an optional, separate reporting tool. The

Sniffer Reporter's tabular and graphical reports show top hosts by traffic, top hosts by protocol, a matrix identifying top conversation pairs and protocol

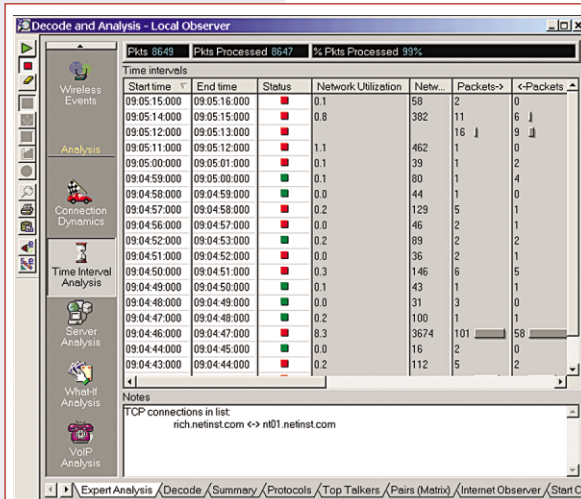
distributions. A global statistics report discloses traffic by segment, errors by segment, segment size distribution and segment utilization. An alarm report reveals alarm details the Sniffer captured.

## Working with these Tools

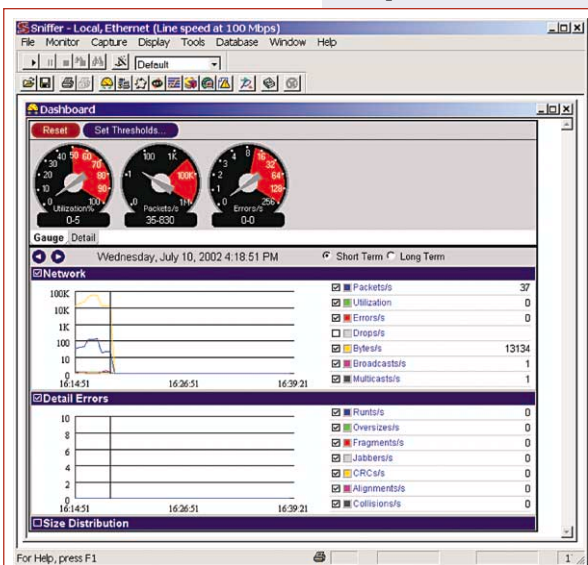
Observer's user interface offers a sleek tree, toolbar and multiple child window view of network activity. Selecting the elements to monitor and the statistics to collect is simple. In the expert summary problem analysis, which shows a list of error events, a double click drills down into the capture buffer detail for further analysis. Double-clicking on any of the protocol-based or application-based problems shown in the TCP/UDP/ICMP experts window drills down to the conversation level to show which pairs of nodes are involved in the problem. The expert window shows network errors organized by time of day to help you judge whether a problem is intermittent or consistent. Observer also displays a window containing a graphical view of network conversations. Alongside each conversation pair are statistics showing packet-to-packet delay times, retransmissions and lost packets. Clicking on a conversation pair drills down to a list of packets exchanged by the nodes, with the contents of each packet displayed in a separate window. Each Observer activity presentation is a child window that updates in real time, and you can have as many concurrent windows open as you wish - a nice feature.

For captured packets, you can choose which columns you want EtherPeek NX's user interface to show. The selectable columns include source and destination logical addresses, protocol types, packet sizes and time stamps.

EtherPeek's name table holds device and



Observer's expert window shows network errors organized by time of day to help judge whether a problem is intermittent or consistent.



Sniffer's user interface uses a simplistic dashboard to show network utilization, packets per second and error counts.

protocol name-address equivalences for your network. On a network that uses DNS, EtherPeek can automatically discover names for the devices at each IP address. Editing EtherPeek's name table by hand is a tedious chore.

Like Observer's graphical network map of network dialog pairs, EtherPeek NX's peer map plots those network nodes that are talking to each other. EtherPeek NX draws an expanding ellipse of node addresses and plots lines between the source and destination IP addresses that it displays. Observer draws a more-easily managed circle of conversation pairs, and Observer did a better job of detecting and displaying node names on its chart. Coping with EtherPeek NX's display of IP addresses was more difficult.

Sniffer's user interface uses a simplistic dashboard to show network utilization, packets per second and error counts. One Sniffer window displays a scrolling list of captured packets, while another contains an expandable tree view of protocol event alarms you can set. For a particular packet selected in the scrolling packet list window, another window displays decoded detail.

We found we had to spend quite a bit of time examining Sniffer Portable's displays of decoded packets to solve our test problems. Unfortunately, Sniffer's designers have made locating and understanding culprit packets more difficult than they need to be. On the other hand, Sniffer does a good job of interpreting the attributes and proposals associated with an IPsec handshake, which can be invaluable to anyone who needs to troubleshoot IPsec configurations.

All three products are easy to install and come with clear, easy-to-understand documentation.

## Conclusion

Network Instruments' Observer emerged the clear winner in our tests. It's a world-class protocol analyzer that we feel no network administrator should be without.

## Network Testing Labs' Testbed and Methodology

We ran each protocol analyzer software product on a Windows 98-based Dell OptiPlex G1 computer equipped with a 350 Mhz Pentium II processor, 64 Mb RAM and 4 Gb hard drive. The machine's network adapter varied in the tests. For EtherPeek NX, we used a Farallon

Communications, Inc. PN996L-TX Fast Ethernet PCI bus network adapter. For Network Instruments' Observer, we installed an OBSPCI Fast Ethernet PCI bus network adapter. Sniffer Portable listened on the network via an Adaptec ANA-6911A Fast Ethernet PCI bus network adapter.

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 ten Windows 98, Windows ME, Windows NT, Windows 2000 Professional, Macintosh System 8, Red Hat Linux 6.2 and OS/2 Warp 4.0 clients. The six-segment network also contained SNMP-aware switches, Cisco 3500 routers, a Covad Communications SDSL Internet link, Frame Relay DSU/CSUs and RMON I/II hardware probes.

We confronted the protocol analyzers with six problem situations. First, we configured an SMTP mail server to reject relay requests and then sent the server e-mail from bogus, unauthenticated user IDs, an action which produced SMTP Error Code 550 responses. We attempted to log on to Microsoft and Novell file servers with invalid user ID and password credentials. Next, we powered off a file server while clients were accessing it. Using custom-written packet-generating software, we then sent badly-formed SQL\*NET transactions to an Oracle server and badly-formed TDS transactions to a Sybase server. We caused physical layer Ethernet problems by using a cable deliberately wired to produce Near-End Cross Talk (NEXT). We also asked the protocol analyzers to help us diagnose a too-busy switch as well as find a misconfigured Cisco router. To determine a protocol analyzer's accuracy, we flooded our network with a known number of diverse protocol messages and note whether each product captured and decoded all the traffic.

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

## Product Facts

### Observer 8.2

Starts at \$995, \$3,995 as tested  
Network Instruments, LLC  
8800 West Highway Seven, 4th Floor  
Minneapolis, MN 55426  
toll free: (800) 526-7919  
voice: (952) 932-9899  
fax: (952) 932-9545  
[www.networkinstruments.com](http://www.networkinstruments.com)

### Sniffer Portable 4.5

\$11,995 as tested  
Sniffer Technologies (a Network Associates, Inc. business unit)  
3965 Freedom Circle  
Santa Clara, CA 95054  
toll free: (800) 764-3337  
voice: (972) 308-9960  
fax: (810) 963-4069  
[www.sniffer.com](http://www.sniffer.com)

### EtherPeek NX 1.0 for Windows

\$3,495 as tested  
WildPackets, Inc.  
2540 Camino Diablo  
Walnut Creek, CA 94596  
voice: (925) 937-7900  
fax: (925) 937-2479  
[www.wildpackets.com](http://www.wildpackets.com)

*Barry Nance is a networking expert, magazine columnist, book author and application architect. He has 29 years experience with IT technologies, methodologies and products. Over the past dozen years, his network laboratory has evaluated thousands of hardware and software products for ComputerWorld, BYTE Magazine, Government Computer News, PCMagazine, Network Computing, Network World and other publications. He's authored thousands of magazine articles and three popular books, 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.*