



# Observer® Product Family

## Analysis Solutions for Complex Networks

Supporting: LAN • 10/100 • Gigabit • 10 Gb • Wireless • WAN • DS3/E3 • OC3c/OC12c • SAN • Fibre Channel

## Observer Standard

Protocol analysis, real-time statistics, trending, and network troubleshooting

## Observer Expert

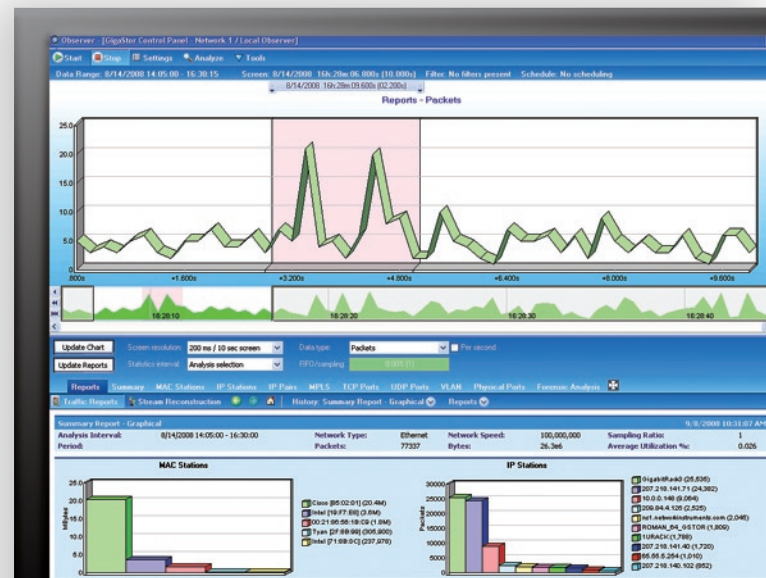
Manage application performance through expert analysis

## Observer Suite

The most feature-rich network management and analysis solution

### The NI-DNA™ Advantage

Network Instruments® designs its solutions in house, so you can be confident they'll work together seamlessly. Our distributed architecture makes it easy to simultaneously monitor all network segments through one interface.



# OBSERVER<sup>®</sup> STANDARD

The first stage of network control is understanding network health. With Observer Standard, administrators gain the insight they need to make network adjustments for improved efficiency.

## Key Features

### Superior Packet Capture and Decode

- Decode over 610 protocols and countless sub-protocols (including wireless)
- Nanosecond resolution provides precise analysis
- Schedule automated packet captures to solve recurring issues

### Network Reporting and Trending

- Collect and store data for long-term reporting and analysis
- View and analyze Internet traffic over time
- Justify capacity upgrades with Comparison Analysis Reports

### Complete Vital Signs Display

- Comprehensive snapshot of error conditions ranked by severity
- Wireless-specific errors (e.g. retries, CRC, short PLCP, transmit errors)

### Powerful Packet Filtering Features

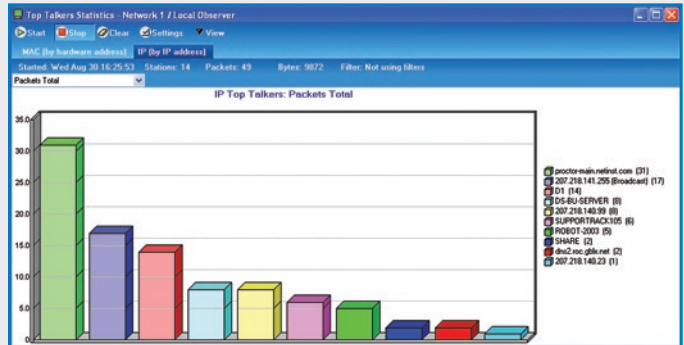
- Include/exclude packets by address, address range, protocol offsets and presets; use Boolean logic to create complex filters
- Design filters visually with enhanced graphical interface
- Instantly create protocol filters selected from Protocol Distribution list
- Execute multiple filters concurrently
- Share complete filter libraries with other Observer users
- Utilize data mining capabilities to search multiple files for any user-defined filter

### Over 30 Real-Time Statistics for Deeper Understanding

- View comprehensive snapshot of network health with Network Summary
- Use Internet Observer to track conversations of interest
- View access point utilization with Wireless Access Point Load Monitor
- See all protocols and applications with Protocol Distribution
- Predict imminent slowdowns with Network Activity Display
- Scan wireless channels continuously with Wireless Site Survey
- Use Router Observer to display utilization rates
- See bandwidth usage by host with Top Talkers

Access Points/Stations	Channel	Type	SSID	Security	First Seen	Last Seen	AP Up Time
Aloronet (26:01:DC)	6	Access Point, Bridge	No WEP		Nov 6, 2003 15:35:08	Nov 6, 2003 15:37:12	107 days 09h:57m:31s
Aloronet (46:E5:15)	6	Access Point	bpauu	Extended WEP	Nov 6, 2003 15:35:09	Nov 6, 2003 15:37:12	21h:52m:41s
3Com (78:92:12)	6	Wireless Station			Nov 6, 2003 15:35:10	Nov 6, 2003 15:37:10	...
Cisco (83:21:8A)	6	Wireless Station			Nov 6, 2003 15:35:09	Nov 6, 2003 15:37:10	...
Nokia (93:2A:80)	6	Wireless Station			Nov 6, 2003 15:35:10	Nov 6, 2003 15:37:11	...
Cisco (30:FC:9E)	6	Wireless Station			Nov 6, 2003 15:35:09	Nov 6, 2003 15:37:12	...

Wireless Site Survey



Top Talkers



# OBSERVER EXPERT

All the features of Observer Standard, plus problem identification and suggestions for resolution. Dramatically reduce troubleshooting time with over 610 real-time experts.

## Key Features

### Application Transaction Analysis

- Real-time and post-capture analysis, trending
- Receive statistics on errors and monitor response time
- Supports SQL (TDS), Oracle (TNS), VoIP, DNS, FTP, HTTP, POP3, Telnet, SMTP, SNMP, Exchange, Microsoft Networking (SMB), Citrix, FIX, Active Directory (LDAP)

### VoIP and Unified Communications Performance

- Monitor calls in-depth with over 70 VoIP metrics
- Measure call quality based on industry standards
- Acquire relevant, actionable detail and diagnostics
- Save or play voice conversations or streaming video

### Connection Dynamics

- Provide a graphical view of conversations up to the application layer
- Show packet-to-packet delay times, allowing instant identification of long latency and response times
- Flag retransmissions, lost packets, and packets out of order

### Expert Summary Problem Analysis

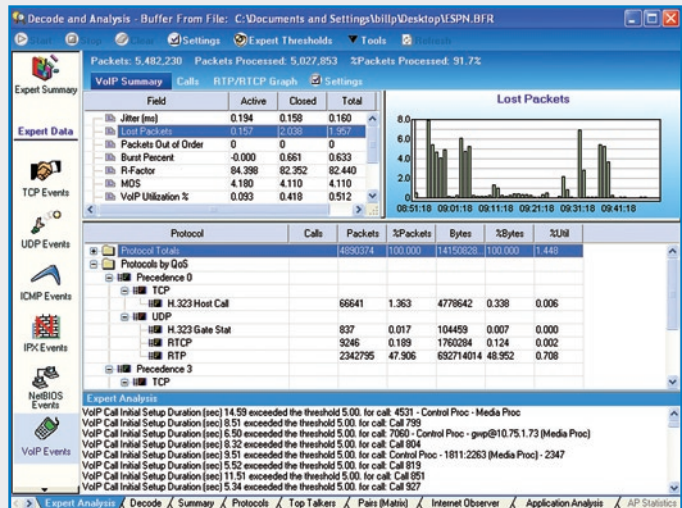
- Error events shown in single, concise display in real-time
- For connection-oriented problems, double-click for further analysis

### TCP/UDP/ICMP Events

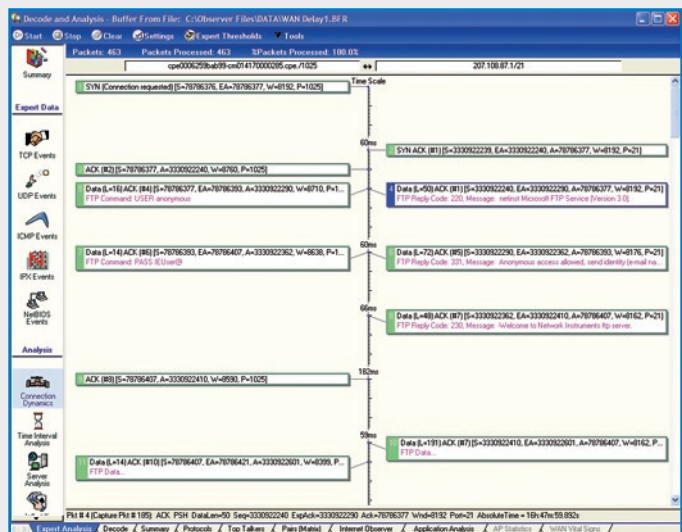
- Common services responses sorted and flagged by severity
- TCP expert tracks port-based protocols for connection issues
- See all conversations
- View volume, response time, network delay, etc.

### Extra-Large Memory Buffer

- Allows for increased packet capture size and extended time frames for Expert Analysis
- User-defined memory model lets each administrator fine tune Observer's individual memory mode usage



VoIP Analysis



Connection Dynamics

### MultiHop Analysis

- Track conversations through multiple segments
- Pinpoint and eliminate transaction delay

### NetFlow and sFlow®

- Collect data from many devices to one console
- Analyze traffic statistics over weeks or months
- Up to 512 NetFlow devices per instance

### Stream Reconstruction

- Recreate communications from captured traffic
- Rebuild web pages, e-mails and VoIP calls
- Document policy violations, investigate network problems, identify unauthorized activities

### Expert Wireless Events (802.11 a, b, g, n)

- Track wireless conversations, logging errors, rogue access points, and other events of interest

### “What-If” Modeling Analysis

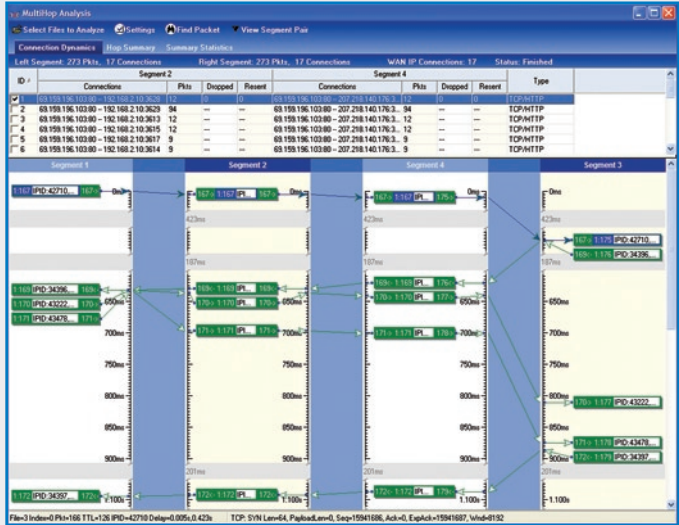
- Track bandwidth capacity changes (e.g. 100 Mbps to 1000 Mbps)
- Review variable changes (e.g. packet size, latency, server load, number of users)
- Measure based on actual client, server, or peer-to-peer conversations
- Plot possible response time, bandwidth utilization, and packet flow

### Server Analysis

- Display server response times charted against the number of simultaneous requests
- Chart response times for recorded request sets, and as request loads increase

### Time Interval Analysis

- Display network errors by time frequency to learn whether a problem is sporadic or consistent
- Show if slow response is due to network load



MultiHop Analysis

Client IP	Server IP	Type	Start Time	End Time	Description
10.0.0.20	14.233.842.99	HTTP	2008-09-14 14:09:22.213	2008-09-14 14:09:22.428	http://www.google.com
10.0.0.20	72.14.207.109	HTTP	2008-09-14 14:09:25.432	2008-09-14 14:09:25.207	http://www.commentpicker.com
10.0.0.20	206.18.125.55	HTTP	2008-09-14 14:09:27.182	2008-09-14 14:09:26.562	http://www.redfox.com
10.0.0.148	131.107.118.28	HTTP	2008-09-14 15:03:46.803	2008-09-14 15:03:22.888	http://dailymotion.com
10.0.0.148	65.55.25.125	HTTP	2008-09-14 15:04:09.294	2008-09-14 15:04:09.238	http://update.msn.com
10.0.0.148	209.84.4.126	HTTP	2008-09-14 15:04:09.902	2008-09-14 15:04:09.509	http://download.msn.com
10.0.0.148	207.46.209.132	HTTP	2008-09-14 15:05:20.214	2008-09-14 15:05:16.725	http://www.update.com
10.0.0.148	207.46.209.252	HTTP	2008-09-14 15:05:30.119	2008-09-14 15:05:30.191	http://www.update.com
10.0.0.148	68.142.122.46	HTTP	2008-09-14 15:05:19.789	2008-09-14 15:05:26.203	http://www.download.com
10.0.0.148	199.7.48.190	HTTP	2008-09-14 16:04:04.673	2008-09-14 16:04:05.740	http://dailymotion.com
10.0.0.148	68.142.123.64	HTTP	2008-09-14 16:05:25.493	2008-09-14 16:04:11.462	http://www.download.com
10.0.0.148	65.55.5.254	HTTP	2008-09-14 16:05:25.687	2008-09-14 16:05:27.818	http://www.update.com
10.0.0.148	68.142.123.81	HTTP	2008-09-14 16:05:41.825	2008-09-14 16:05:50.419	http://www.download.com
10.0.0.148	68.142.122.102	HTTP	2008-09-14 16:11:36.100	2008-09-14 16:11:22.125	http://www.download.com



Stream Reconstruction

# OBSERVER SUITE

All the functionality of Observer Standard and Observer Expert plus full SNMP and RMON device management and web reporting.

## Key Features

### Web Publishing and Reporting

- Share reports with non-Observer users
- Generate reports dynamically
- Configure reports based on time, station or SNMP data
- Obtain current and historical trends
- Define different access permissions for users

### Complete SNMP Device Management

A single solution for multi-vendor hardware networks, including a remote console for SNMP-compliant devices on your LAN/WAN or the Internet.

- Obtain multiple views of device data
- Review readable and writable SNMP objects through Observer or the web
- Monitor notifications delivered by SNMP traps
- Maintain compatibility with all SNMP versions
- Configure Triggers and Alarms for SNMP data

### Extensive Reporting and Trending

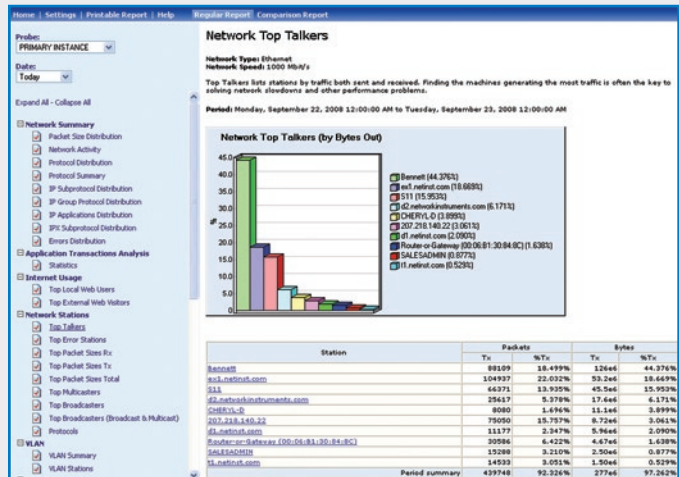
- Report SNMP data in real time
- Collect data for baseline comparisons later
- Share findings with custom charts, tables, lists, and graphical objects (forms)

### RMON Device Management

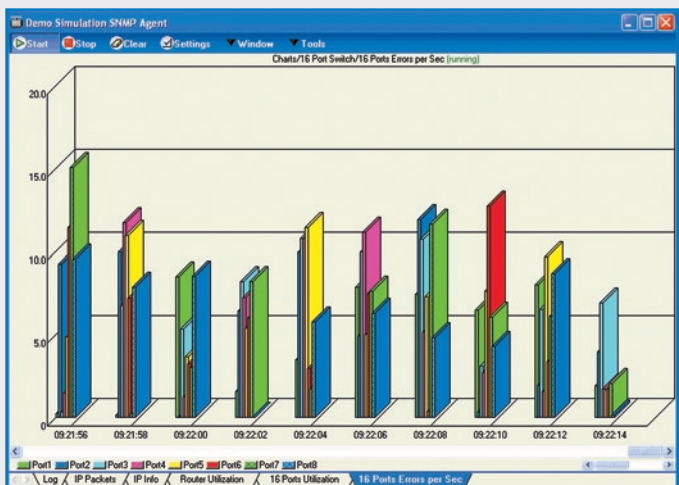
- Fully compliant with RMON and HCRMON standards
- Configurable alarms to warn of impending problems
- Monitor and control any RMON device

### Other Great Features

- Full XML/SOAP support
- Custom decode kit for additional/proprietary protocols



Web Reporting



Switched Port Errors per Second

## OBSERVER STANDARD

### Packet Capture and Decode

Decode over 610 primary protocols  
Countless subprotocols  
Nanosecond resolution  
Automate packet captures  
Security controls

### Unlimited Filtering Options

Use Boolean logic for creating complex filters  
Design filters visually  
Instantly create protocol filters from list  
Share filter lists between Observer users  
Filter for virus and attack signatures  
Fast Post Filtering for quick execution  
Pre-Filtering for data mining

### Network Trending and Reporting

Network Trending Dashboard Display  
Efficiency History  
Comparison Analysis Reports  
Ready-Made Reports  
Custom Reports  
Report Scheduler

### Triggers and Alarms

Flag activities or errors with a predefined list  
Set custom notifications based on any filter  
Receive immediate security alerts  
Choose alert method and schedule response

### Error Tracking

Network Vital Signs  
Wireless Vital Signs  
Network Errors by Station

### Real-Time Statistics

Network Summary  
Bandwidth Utilization  
Top Talkers  
Internet Observer  
Protocol Distribution  
Network Activity Display  
Wireless Site Survey  
Wireless Access Point Load Monitor  
Switch Statistics  
Router Observer  
Pair Statistics  
VLAN Statistics  
Network Delay

IPv6 Support

## OBSERVER EXPERT

*All the features of Observer Standard plus:*

### Over 610 Real-Time Experts

Directional indicators for full-duplex capture  
Expert Summary Problem Analysis  
TCP/UDP Events  
ICMP Events  
IPX Events  
NetBIOS Events  
Expert Wireless Events  
NetFlow/sFlow® Integration  
HP OpenView Integration

SSL Decryption

### Expert Analysis

Connection Dynamics  
MultiHop Analysis  
Server Analysis  
"What-If" Modeling  
Time Interval Analysis  
MPLS Analysis

### Extra-Large Memory Buffer

Designed for enterprise-level traffic  
Guarantees no dropped packets

### Stream Reconstruction

E-mail, HTTP, and VoIP

### Application Analysis

Real-time and post capture  
Monitor response time  
View total/failed transactions  
Track application session flows  
Provide statistics on errors  
Automate server/application discovery  
Long-term trending  
FIX, 29West, NASDAQ decodes

### VoIP Analysis

Aggregate statistics  
In-depth call metrics  
QoS reporting  
Quality Scoring

### Third-Party Support

Cisco NetFlow  
sFlow®

## OBSERVER SUITE

*All the features of Observer Expert plus:*

### SNMP Device Management

Review readable, writable SNMP objects  
Monitor and set notifications based on traps  
Supports SNMP 1, 2 and 3 with MIB compiler

### Network Trending and Reporting

Report SNMP data in real-time

### Switch Station Locator

Identify users' port location by switch

### RMON Device Management

Full support for RMON/HCRMON  
Enhanced RMON Filtering  
WAN RMON

### Web Publishing Service

Publish health reports to web

SOAP (Support Automated Report Delivery)

**Operating Systems Supported:** Windows® 2003, XP, XP x64

For minimum and recommended system requirements, please visit our web site 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).

### Solution Bundles

Contact a Network Instruments representative or dealer to ask about product bundles that cover all of your network management needs.



### Corporate Headquarters

Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA  
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801

[www.networkinstruments.com](http://www.networkinstruments.com)

### European Headquarters

Network Instruments • 4 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom  
telephone + 44 (0) 1959 569880 • fax + 44 (0) 1959 569881

[www.networkinstruments.co.uk](http://www.networkinstruments.co.uk)