



# Observer® Product Family

Powerful, Scalable and Distributed Network Analysis Solutions for Multi-Topology Networks (LAN, 802.11a/g/b, gigabit, WAN)



## Observer

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

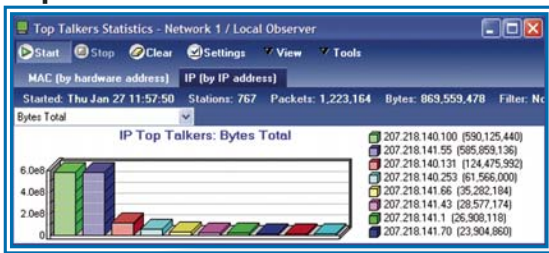
## Expert Observer

Pinpoint difficult problems through Expert Analysis

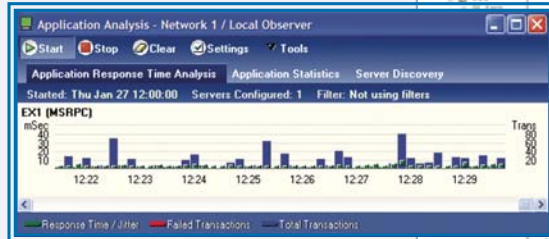
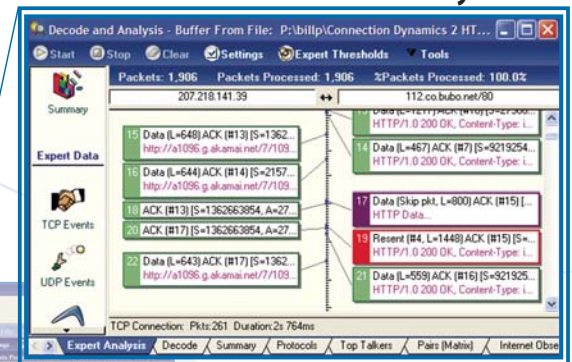
## Observer Suite

The most feature-rich network management and analysis solution

### Top Talkers



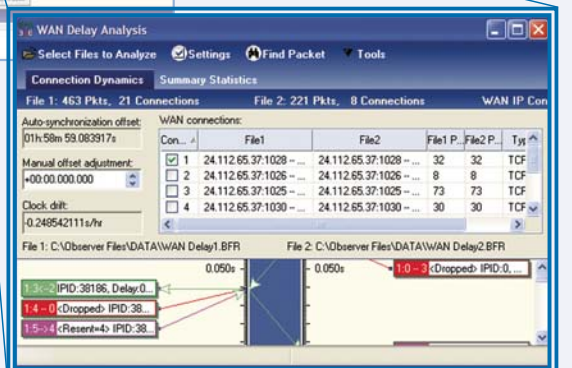
### Connection Dynamics



### Application Analysis



### SNMP Management



### WAN Delay Analysis

The first level of network control is to fully understand network health. With Observer, administrators gain critical insight to make network adjustments for improved efficiency. Observer also offers greater problem solving capabilities for faster troubleshooting.

- Capture, view and decode network traffic in **real-time**
- Analyze network traffic to **diagnose critical problems**
- Collect long-term trending statistics for **proactive decision making**
- Detect abnormalities quickly with custom **triggers and alarms**

### Powerful packet filtering features

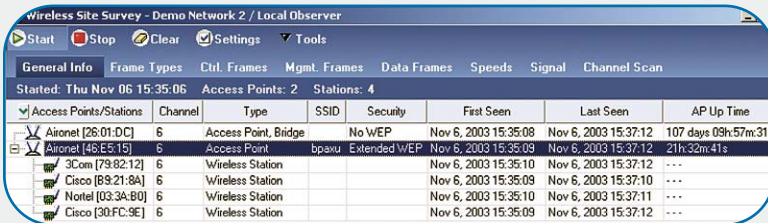
- Include or exclude packets by address, address range, protocol offsets and presets; use **Boolean logic** to create complex filters
- **Design filters visually** with an enhanced graphical interface
- **Instantly create** protocol filters selected from the Protocol Distribution List
- Execute **multiple filters** concurrently
- **Share complete filter libraries** with other Observer users
- **Quickly configure** filters with Fast Post Filtering
- Utilize **data mining** capabilities to search multiple files for any user-defined pattern

### Error Tracking displays - see network problems before they become user problems

- Get a snapshot of error conditions with **Network Vital Signs**
- Display wireless errors with **802.11 Vital Signs**, as well as aggregate signal strength, quality, network speeds and more
- Track all errors by topology, then drill down to focus on the problem device with **Network Errors by Station**

### Over 30 Real-Time Statistics for deeper understanding of your network

- Get a comprehensive snapshot of network health with **Network Summary**
- Set **Triggers and Alarms** to flag activities or errors and be notified by e-mail, pager, SNMP trap, etc.
- Obtain insight into the total network load with **Bandwidth Utilization**
- Use **Internet Observer** to track usage by user
- View all access point utilization rates with **Wireless Access Point Load Monitor**
- Analyze conversation response time with **Pair Statistics (Matrix)**
- 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 interface utilization rates
- See bandwidth usage by device with **Top Talkers**
- Determine if VLANs are overloaded and verify VLAN setups with **VLAN Analysis**



Access Points/Stations	Channel	Type	SSID	Security	First Seen	Last Seen	AP Up Time
Aironet [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
Aironet [46:E5:15]	6	Access Point	bpaxu	Extended WEP	Nov 6, 2003 15:35:09	Nov 6, 2003 15:37:12	21h:32m:41s
3Com [79:82:12]	6	Wireless Station			Nov 6, 2003 15:35:10	Nov 6, 2003 15:37:12	...
Cisco [B9:21:8A]	6	Wireless Station			Nov 6, 2003 15:35:09	Nov 6, 2003 15:37:10	...
Nortel [03:3A: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



OBSERVER'S MAIN CONSOLE

### KEY FEATURES

#### Superior Packet Capture and Decode

- Decodes over 500 primary protocols and countless sub-protocols (including Wireless)
- Nanosecond resolution provides precise analysis, even for gigabit networks
- Add administrator comments to any packet for later review
- Dynamic port protocol decode provides complete customization
- Schedule automated packet capture to solve recurring network issues or more elusive problems

#### Network Trending and Reporting

- Collect and store data for reporting and analysis in Network Trending
- View and analyze Internet traffic over time with Internet Trending
- Justify capacity upgrades from Comparison Analysis Reports
- Automate report delivery to Observer and non-Observer users with Report Scheduler

#### Complete Vital Signs Display

- Comprehensive snapshot of error conditions ranked by severity
- Ethernet specific errors with ErrorTrak™ drivers (e.g. packets too big/ too small, CRC, collisions, alignment)
- Wireless specific errors (e.g. WEP, retries, beacons, polls, CRC, short PLCP, transmit errors)

Expert Observer includes all the features of Observer and adds the next level of control by identifying network issues and offering immediate solutions. Dramatically reduce the time it takes to troubleshoot network problems with over 500 real-time experts.

- Predict network bandwidth and response time impacts using **“What-If” Analysis**
- Track and solve application problems with **Application Analysis**
- Receive accurate high-speed, high volume packet capture with a **4GB (maximum) memory buffer**
- View application session flows graphically with **Connection Dynamics**
- Pinpoint difficult problems through real-time or post-capture **Expert Analysis**

### Expert Summary Problem Analysis

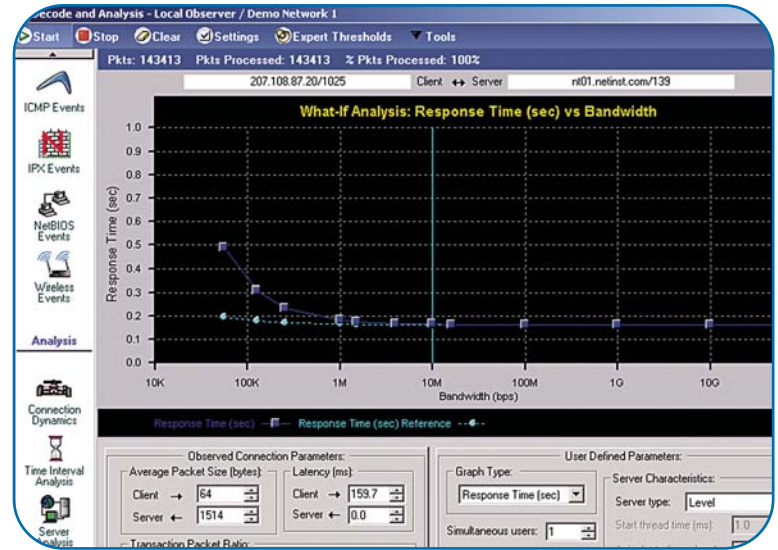
- Error events shown in a single, concise display in real-time
- For connection-oriented problems, double-click for further analysis

### TCP/UDP/ICMP Events

- Displays protocol-based and application-based problems
- Local traffic is judged using different criteria than WAN/Internet traffic to ensure no false readings are provided
- All common services are tracked and response performance is sorted and flagged by severity
- A generic TCP condition expert tracks all port-based protocols for slow response or other connection issues
- Measures Network Delay to differentiate between network and application problems

### IPX Events

- Displays all communication errors being transferred via IPX/SPX



**“WHAT-IF” MODELING ANALYSIS**

## KEY FEATURES

### Application Analysis

Take troubleshooting to the application layer with your network analyzer

- Real-time and post capture
- Track application session flows and failed transactions
- Receive statistics on errors and monitor response time
- Automate Server/Application Discovery
- Drill down with Connection Dynamics to view conversation flow detail
- Supports SQL (TDS), Oracle (TNS), VoIP, DNS, FTP, HTTP, POP3, Telnet, SMTP, SNMP, and Exchange
- Eliminates need to purchase a separate application monitoring system

### 4GB Memory Buffer

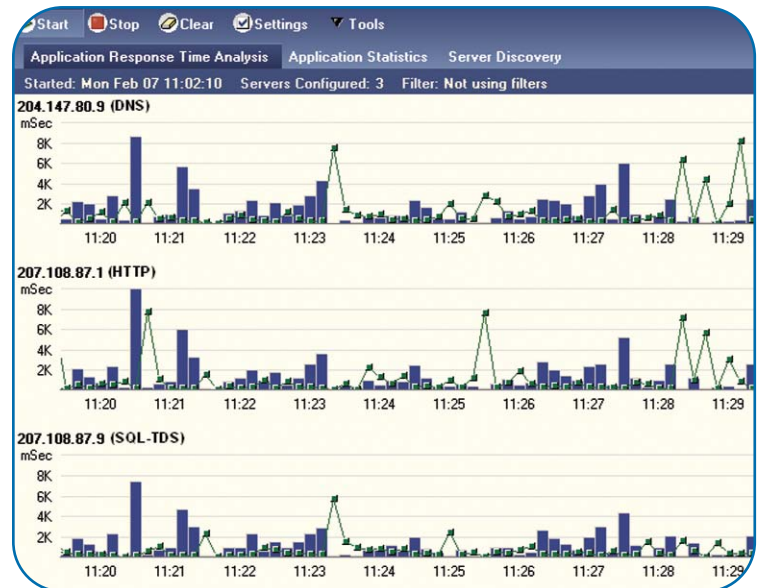
Keep up with enterprise level traffic

- Industry's largest 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
- Guarantees no dropped packets by using reserved memory not associated with Windows

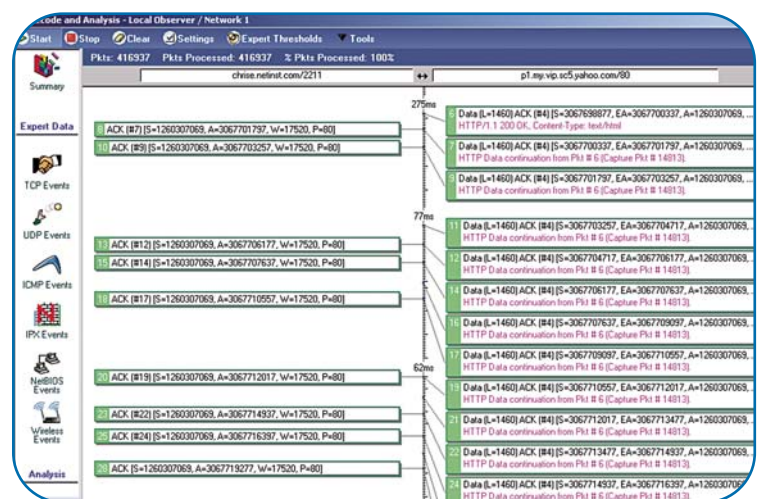
### “What-If” Modeling Analysis

Predict how network changes will affect response times

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



**APPLICATION ANALYSIS**



**CONNECTION DYNAMICS**

## NetBIOS Events

- Displays NetBIOS conditions and events seen over the network

## Expert Wireless Events

- Tracks wireless conversations, logging errors and other events of interest for administrators

## Time Interval Analysis

- Displays network errors organized by time frequency to identify whether a problem is sporadic or consistent
- Shows if slow response is due to network load

## Connection Dynamics

- Provides a graphical view of conversations up to application layer
- Shows packet-to-packet delay times, allowing instant identification of long latency and response times
- Flags retransmissions, lost packets and errors in red for quick identification

## VoIP Expert

- Displays H.323/SIP conversational data
- Monitors VoIP connections to improve VoIP performance across the organization
- Saves or plays voice conversations or streaming video
- Includes jitter and lost packets (percentage) for each direction, total utilization and more

## WAN Delay Analysis

- Analyzes/captures both ends of a conversation across a WAN link to measure response times
- Quantifies transaction time between PC and server using an exclusive method of synchronizing captures
- Determines how long it takes for data to transfer across the WAN

## Server Analysis

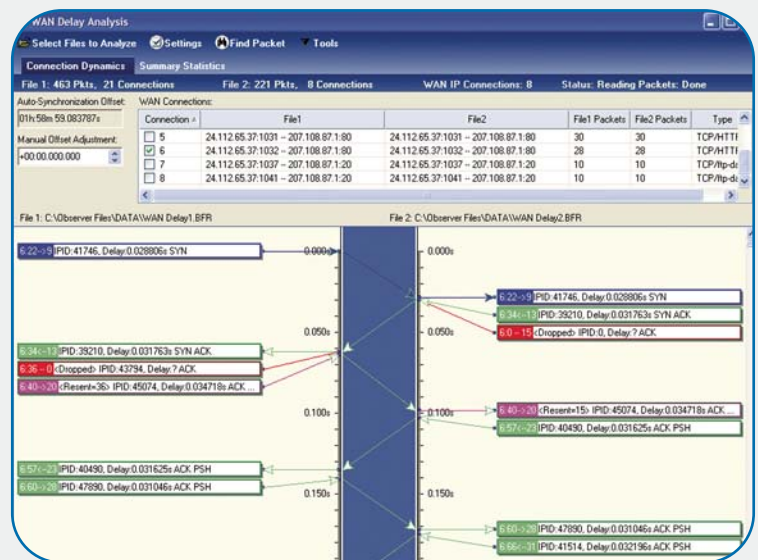
- Displays server response times charted against the number of simultaneous requests
- Charts response times for recorded request sets, and as request loads increase

## Controlled Decode Views

- Limits access to confidential data through a decode screen
- Password protects and limit captures to a set number of bytes



VoIP EXPERT



WAN DELAY ANALYSIS

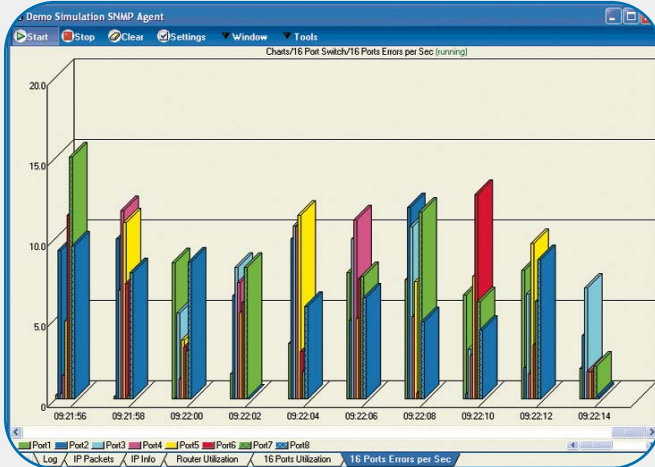
## Intuitive Design for Fast Troubleshooting and Event Isolation

Observer's award-winning user interface lets you navigate easily between heads-up summary displays and highly-detailed databases concerning conditions and activity on your network – all in real time. Data displays are cross-referenced where appropriate, allowing you to drill down to greater detail when examining a particular station or protocol.

- Observer offers multiple methods of obtaining the '30,000 foot view' of your network, letting you focus on the big picture. For example, review total bandwidth utilization, total error counts, etc. Observer's **Network Vital Signs** display (customized for each topology) tracks all of these metrics in an easy-to-read, real-time summary display.
- View numerous detailed line-item reports, updated in real-time with Observer's **Network Trending and Reporting**. Sort line items by any criteria (station, protocol, error rate, etc.). Observer also offers customizable graphing options.
- **Cross Mode Drill Down** quickly provides more detail on any issue. For example, right-click on any station in the Top Talkers list to jump immediately to the list of protocols being used by that station, or the list of devices communicating with it.
- The **Triggers and Alarms** Log Window allows custom notifications of network thresholds to be setup quickly and easily. Activate, deactivate and manage all of your alarm settings from the main window.

For the most complete level of network control, acquire all the functionality of Observer and Expert Observer plus full SNMP and RMON device management with Web Reporting from Observer Suite.

- Optimize network devices (including switches and routers) with a full **SNMP management console**
- Monitor LANs/WANs from a central location using **RMON1, RMON2** and **HCRMON** collection consoles
- View statistics from any browser using the built-in **Web reporting** service



**SWITCHED PORT ERRORS PER SECOND**

### Custom Decode Kit

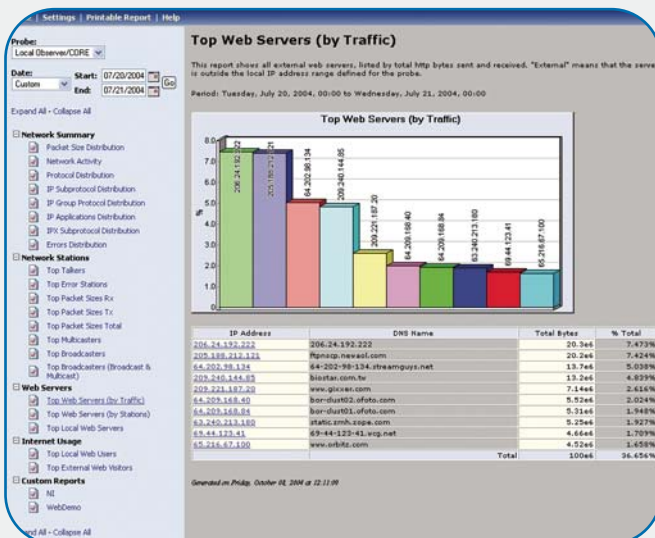
- Add custom, proprietary or additional protocols to Observer decodes
- Full wireless support

### Switch Station Locator

- Displays names or addresses of devices by switch port using SNMP

### Full XML/SOAP Support

- Obtain access to error, capacity and historical network data to any application that supports XML or SOAP (Simple Object Access Protocol)



**WEB REPORTING**

## KEY FEATURES

### Complete SNMP Device Management

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

### Full Support

- Obtains multiple views of device data
- Reviews both readable and writable SNMP objects through Observer or a Web browser
- Monitors and set notifications triggered by SNMP traps
- Maintains compatibility with all SNMP versions through an included MIB compiler
- Configures Triggers and Alarms for SNMP data

### Extensive Reporting and Trending

- Reports SNMP data in real-time
- Collects data for baseline comparisons later
- Shares findings with tailor-made charts, tables, lists and graphical objects (forms)

### Use Web Publishing Service to report from any browser

Whether they're internal employees or outside consultants, a Web browser is all they need to view data and generate reports of their own. You control the level of access.

- Publishes network "Weather Reports" for your corporate intranet/extranet
- Provides non-Observer users with secure access to network or WAN baseline data
- Accesses current or historical statistics from any browser, anywhere
- Provides real-time statistics with granularity down to one minute
- Defines different access permissions for each user
- Gives in-house administrators control over access to sensitive data
- Displays report data based on time, stations, switches and SNMP info
- Obtains current or historical data and usage trends based on specific stations

### Monitor and Control any RMON-standard Device

RMON is the industry standard for traffic management and packet level data collection for multi-segment LANs.

- Fully compliant with all RMON1 and RMON2 specifications
- Configurable alarms to warn of impending problems
- RMON console supports high capacity RMON (HCRMON)

### Supports all 21 RMON and HCRMON groups including:

- Packets received/sent/dropped
- Statistics by host
- Statistics by conversation between two sets of addresses
- Lists of events
- Distribute reports via Web or e-mail



# Choose Your Level of Control

## Packet Capture and Decode

Decode over 500 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

## Cross Mode Drill Down

Instantly displays detailed data information

## Network Trending and Reporting

Network Trending Dashboard Display  
Efficiency History  
Comparison Analysis Reports and Summary  
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 alerts when security threats are detected  
Choose alert method (e-mail, pager, etc.) and schedule response (e.g. launch program)

## Error Tracking

Network Vital Signs Mode  
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

OBSERVER

## Over 500 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

## Security Features

3DES Encryption

HP OpenView Integration

## Unique Expert Analysis

Time Interval Analysis  
Connection Dynamics  
WAN Delay Analysis  
Server Analysis  
"What-If" Modeling  
VoIP Analysis

## 4GB Memory Buffer

Designed for enterprise-level traffic  
Guarantees no dropped packets

## 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

EXPERT OBSERVER

## SNMP Device Management

Review readable and 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 all 21 RMON and HCRMON groups  
Enhanced RMON Filtering

## Web Publishing Service

Publish network health reports to intranet or extranet

OBSERVER SUITE

## SYSTEM REQUIREMENTS

Operating Systems Supported: Windows® XP, 2000, 2003

For minimum and recommended system requirements, please visit our website at: [www.networkinstruments.com/products](http://www.networkinstruments.com/products)

# Proven Network Management, Analysis and Troubleshooting Solutions

for local

The award-winning Observer family of products from Network Instruments combines a comprehensive, freestanding management and analysis console with high-performance distributed Probes to provide integrated monitoring and management of your entire network (LAN, 802.11a/b/g, gigabit, WAN).

## Console Options

### Observer

- Decodes over 500 protocols and countless subprotocols
- Long-term network trending and analysis
- Over 30 real-time statistics
- Supports Ethernet (10/100/1000), 802.11a/b/g, Token Ring, and FDDI

### Expert Observer *(All the features of Observer plus)*

- Application Analysis
- "What-if" Modeling Analysis
- Monitors over 500 real-time Expert Events
- Connection Dynamics
- Full-duplex gigabit and WAN

### Observer Suite *(All the features of Expert Observer plus)*

- Complete SNMP device management
- Full supports for RMON1, RMON2, and HCRMON
- Automated reporting - Web or e-mail
- Full-duplex gigabit and WAN

and remote

Network Instruments provides a complete set of remote monitoring solutions so administrators can acquire identical management and analysis information from local to remote networks.

- Gain multiple points of visibility
- Manage remote networks as if they were local (24 x 7 x 365)
- Eliminate the time and expense of travel
- Select Probes to fit any topology or infrastructure

## Probe Software Options

### Advanced Single Probes

- Complete Observer data collection for remote sites, local/remot segments or switches
- Web accessible for a quick snapshot
- Full password protection of data
- Support for wired and wireless networks

### Advanced Multi-Probes *(All the features of Advanced Single Probes, plus)*

- Simultaneous monitoring for up to 64 network interfaces
- Numerous Observer consoles can attach to a Probe or communicate with each other
- Multiple users may collaborate by viewing data from a single probe
- User defined levels for different degrees of Probe access
- Manage access rights by feature at the user level
- 3DES encryption option for data transfer

### Advanced Expert Probes *(All the features of Advanced Multi-Probes, plus)*

- View remote Expert Analysis in real-time or post-capture
- Conserve bandwidth by only transferring Expert results, not raw data packets

## Probe Hardware Options

### Customizable Configurations

- Portable analyzer systems
- Rack mountable, ready-to-go
- Direct, passive links for independent views

### Complete Product Line

- 10/100 Appliance
- 10/100/1000 Appliance
- Full-duplex 10/100 Appliance
- Gigabit Probe Appliance
- GigaTrunk™ Probe Appliance
- GigaStor™ Probe Appliance
- WAN Probe Appliance
- Wireless Probe Appliance



# HOW WELL DO YOU KNOW YOUR NETWORK?

## With Observer you can answer these questions and more:

### Are my host sessions “hanging?”

Observer’s capture and decode will show which system sent the last packet and which system failed to respond—client or server.

### Do I need a faster WAN/Internet connection?

Router Observer shows averages by minute and by hour for router interface usage statistics.

### Can’t log in?

Packet Capture can display login negotiations, retransmissions and response times to locate the problem.

### What is my switch throughput?

Observer’s Switched Bandwidth Utilization shows switch throughput and effective switch efficiency.

### Is there a tool that can monitor my VoIP connections?

Observer’s complete decode of H.323, including VoIP, ensures you will have the tools you need when voice and data problems arise.

## Example problems Expert Observer can help you isolate:

### What’s causing the slowdown?

Expert Analysis will provide a summary of conclusions about any problems and possible causes, in real-time or upon completion of capture.

### Why has the company’s main database server become so slow?

Expert Events and Server Analysis will identify the client/server relationships automatically and display expert analysis statistics, including slow response times, busy network or server problems and retransmissions.

### Will upgrading to gigabit Ethernet improve my network response time?

With “What-If” Analysis, predict the impact of infrastructure changes by creating unlimited scenarios based on captured data.

## How can I isolate intermittent problems?

Use Time Interval Analysis to view errors by time periods and clarify if a problem is sporadic or consistent. Data transmissions are displayed as a “drill down” from any problem identified in the IP/TCP/UDP/IPX, NetBIOS/NetBEUI Experts.

## Can I get more detail about a particular conversation?

Connection Dynamics allows you to analyze and graphically view any conversation’s behavior—displaying inter-packet timing between stations and conversational events, highlighting retransmissions and application detail.

## Use Observer Suite to answer these questions and more:

### Can I view utilization and errors on a multi-interface router?

You can use SNMP Reporting to query any router and view link utilizations and errors in chart or graphical form. Additionally, long-term Network Trending can offer period and comparison reports for management and SLA verification.

### I have outside consultants working on my LAN that need to constantly see traffic data. Can I provide them with this access without giving them packet decode abilities, which would compromise network security?

Yes. With the Web Reporting Service, you can provide access to trending flow and SNMP data, without the security risk of sending decoded packets.

## About Network Instruments

Network Instruments is the industry-leading developer of distributed, user-friendly and affordable network management, analysis and troubleshooting solutions. The award-winning Observer family of products combines a comprehensive management and analysis console with high-performance remote Probes to provide integrated monitoring and management for the entire network (LAN, 802.11 a/b/g, gigabit, WAN). All Network Instruments products are designed utilizing our Distributed Network Analysis (NI-DNA™) architecture. With NI-DNA, the Observer solution set simplifies network troubleshooting and management, optimizes network and application performance, and scales to meet the needs of any organization. Founded in 1994, Network Instruments is headquartered in Minneapolis, Minnesota with offices in London, Paris, Toronto and multiple cities throughout the United States with distributors in over 50 countries. More information about the company, products, innovation, technology, NI-DNA, becoming a

partner, and NI University can be found at: [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.

### Contact Us

Corporate Headquarters  
Network Instruments, LLC  
8800 West Highway Seven  
Fourth Floor  
Minneapolis, MN 55426  
USA  
800-526-7919 toll-free  
(952) 932-9899 telephone  
(952) 932-9545 fax  
[www.networkinstruments.com](http://www.networkinstruments.com)

European Office  
Network Instruments  
7 Old Yard  
Rectory Lane  
Brasted, Westerham  
Kent TN16 1JP  
United Kingdom  
+ 44 (0) 1959 569880 telephone  
+ 44 (0) 1959 569881 fax  
[www.networkinstruments.co.uk](http://www.networkinstruments.co.uk)

