



SNIFFER® | PORTABLE

The best-in-class, plug-and-play network and application analyzer

Sniffer® Portable Professional network analyzer is a best-in-class, plug-and-play, single-user analyzer for network and application troubleshooting. Sniffer Portable Professional gives network managers on-demand monitoring, packet capture and problem analysis for wired and wireless network segments. Ideal for rapid response to network and application issues on location in the field, the software-based solution offers powerful troubleshooting tools at a cost-effective price point.

Key Benefits

- Faster time-to-knowledge for network and application problems
- Dashboard views with deep drill-down to rich packet-level analysis
- Wired and wireless support in a single, scalable tool
- Best-in-class network and application analysis functionality

Build on the industry's most advanced and widely deployed Sniffer network analyzer software, Sniffer Portable Professional contains best-of-breed network and application performance troubleshooting functionality. Rich expert modes assist users in quickly identifying errors during packet-level analysis for a wide range of protocol decodes covering all of the most common applications and protocols, including protocols used by VoIP and mobility applications. Sniffer Portable Professional delivers intuitive, easy-to-use dashboards and network views that include deep packet drill-down capabilities and support for wired 10/100/1000 Ethernet and wireless 802.11 a/b/g/n networks all in one tool -- yielding consistent operation and functionality, reducing desktop tool clutter and greatly accelerating problem resolution.

Recommended for:

- Rapid identification of application and network performance issues over wired and wireless networks
- Analysis of wired and wireless network links and wireless control infrastructure
- Analysis of applications and services –in production and prior to roll-out
- Second-level security risk assessments

ON-DEMAND MONITORING

Sniffer Portable Professional provides a high-level view of network traffic and application performance using its dashboard view, and drill-downs into deep packet inspection. The dashboard displays important data about the network. It creates statistical measurements about network traffic, providing an accurate picture of network activity in real time. Network managers can easily drill down from the dashboard to view individual hosts and protocols..

Within the Sniffer Portable Professional dashboard network engineers can monitor both network and application statistics.

Network statistics

- Number of packets and bytes
- Percentage of utilization
- Broadcast and multicast counts
- Packet size distribution statistics
- Network error statistics
- Protocol usage statistics

For More information

For more information please visit www.netscout.com or contact NetScout sales at 800-309-4804 or +1 978-614-4000.

Application statistics

- Individual hosts and conversation-pair traffic statistics
- Top talkers, top applications
- Response time statistics
- Applications in use per user
- Show fastest/slowest server-client pair

PACKET CAPTURE, DECODES, EXPERT ANALYSIS

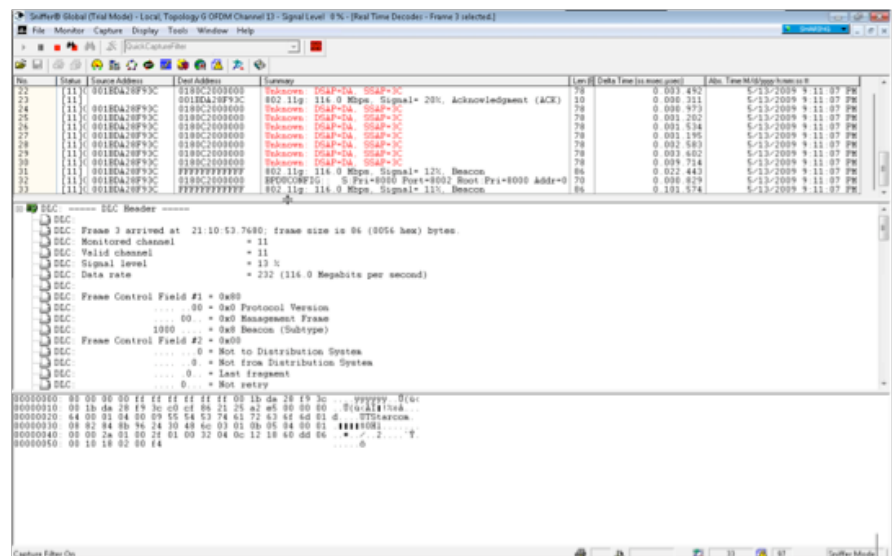
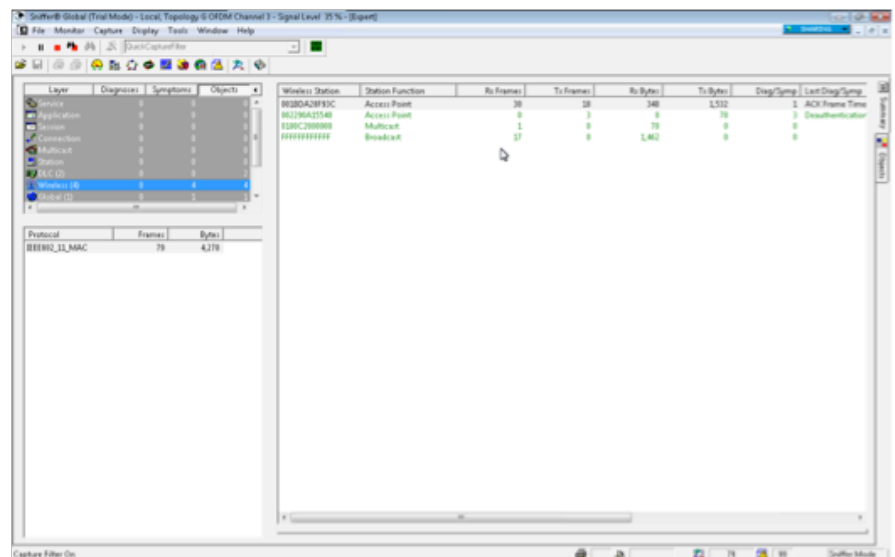
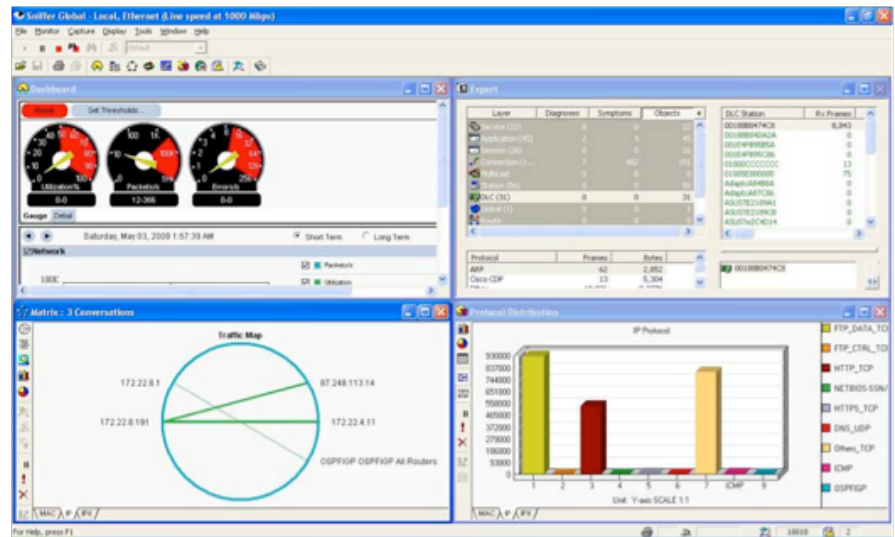
The capture function collects and stores the actual packets from the network. During capture, Expert analysis is performed on packets and results are displayed in an easy-to-read, real time view.

On-Demand and Post-Capture Decode.

Sniffer Portable Professional displays protocol decodes in real-time as packets arrive and decodes application and technology protocols and includes advanced filtering options for drilling down on particular conversations based on IP address or port number. The decode view provides classic, line-by-line protocol interpretation of network data. When real-time contents or content from a capture file is displayed, Sniffer Portable Professional interprets and decodes the protocol. The decode view shows the results of this protocol analysis, displaying packets in three color-coded viewing panes: summary, detail, and hex codes. Capture files are stored short-term, providing a snapshot in time for troubleshooting.

On-Demand Expert Analysis

Sniffer Portable Professional analyzes network packets during or post capture and creates alerts for potential problems on the network. These problems are categorized as either symptoms and/or diagnose. During Expert analysis, a database of network objects is constructed from the traffic seen. Sniffer Portable Professional learns all about the network stations, routing nodes, sub networks, and connections related to the packets in the capture buffer. Using this information, potential problems are



detected and the user is alerted to issues that may exist on the network. These problems are categorized as being either symptom or diagnoses.

Focused Filters and Triggers

Filters provide a way to precisely focus on the data needed to troubleshoot network problems and minimize the size of files collected for historical records. Sniffer Portable Professional gives network managers the ability to create filters for the particular traffic needed for network analysis in order to isolate and quickly identify network problems. Triggers can be set to start captures at specific times, or in response to specific events, such as on off-hours or weekends.

Alarms and Notifications

Alarm features provide a comprehensive method of detecting and logging network alarm events. Expert analysis can generate alarms during data capture and log an event in the alarm log when it detects a symptom or diagnosis. Upon startup, Sniffer Portable Professional logs events in the alarm log when a user-specified threshold parameter is exceeded. Abnormal network events can be assigned to one of five different levels of severity: critical, major, minor, warning, and Informational. In addition, severity levels can be associated with up to four alarm notification actions. For example, Sniffer Portable Professional can be configured to send email when a critical or major alarm occurs. Alarm notification actions can be activated during certain time periods within a day, or on certain days of the week.

WIRELESS CAPABILITIES

For performing wireless network analysis, Sniffer Portable Pro installed on a laptop has two connectivity options:

1. Connected to a wired switch span port via Ethernet, Sniffer Portable Professional uses the laptop wireless card in promiscuous mode to monitor wireless traffic from devices within range

2. Connected to a wireless access point via one laptop wireless card, Sniffer Portable Professional uses a second laptop wireless card in promiscuous mode to monitor wireless traffic from devices within range

Wi-Fi Device List

Sniffer Portable Professional provides an inventory of all 802.11a, 11b, 11g and 11n devices operating in the wireless environment. It provides detailed information on the configuration settings that are available or are in use on the devices, including critical parameters such as signal strength, noise, SSID, security settings in use, associated devices, cell power, device activity status, and many more.

Wireless Security Support

In addition to its existing support for WEP decryption, Sniffer Portable Professional can now decrypt WPA/WPA2 PSK (Personal)-encrypted data on 802.11 wireless networks. Users can specify shared passphrases for up to eight separate WPA/WPA2 PSK-encrypted SSIDs.

Rogue Access Point and Rogue Client Detection

Sniffer Portable Professional portable network analyzer automatically identifies and locates unauthorized devices operating in the Wi-Fi environment that may pose a risk to the overall security

of the network. Users can establish an even higher level of organized security by designating a list of approved wireless devices monitoring for exposed wireless stations, ad-hoc devices, and other vulnerabilities.

Post capture, packets can be analyzed to determine if devices were being for denial of service attacks, flooding and other security policy violations.

Detailed Wireless Packet and Frame Analysis

Sniffer Portable Professional displays real-time packet flows for any Wi-Fi asset. Users can track data and management packets live, watch CRC errors, utilization, packet speed, media type and view a real-time decode page for detailed network analysis.

SPECIFICATIONS AND SYSTEM REQUIREMENTS

Sniffer Portable Professional Administrative Server

Minimum Hardware Requirements:

- Intel or AMD processor, 2.0 GHz or higher, single or dual core/processor
- 2GB RAM or higher
- 150 GB SATA HDD or higher
- CD/DVD ROM drive
- Ethernet 10/100/1000 NIC

Name	Type	SSID	ESSID	Encryption	Authentication	Network	Mod	Valid	Total	Used	Signal	Signal	In-Band	Out-Band	In-Pkts	Out-Pkts	Broadcast	Multicast	Busy Pkts
WLAN11	AP	1111111111	1111111111	WEP	Open	11111111	802.11a	100	100	0	-70	-70	100	100	100	100	0	0	0
WLAN12	AP	22222222	22222222	WPA2	TKIP/AES	22222222	802.11n	50	50	0	-65	-65	50	50	50	50	0	0	0
WLAN13	STA	33333333	33333333	WPA2	TKIP/AES	33333333	802.11n	10	10	0	-75	-75	10	10	10	10	0	0	0

Operating Systems Support:

- Microsoft Windows 2003 Server SP1 (32-bit & 64-bit)
- Microsoft Windows 2008 Server SP1 (32-bit & 64-bit)

Sniffer Portable Professional Client Application
Minimum hardware requirements:

- Intel or AMD processor, 1.6GHz or higher, dual core or more processor
- 512MB RAM or higher, recommend 1GB
- 200MB free disk space or more
- CD/DVD ROM drive
- 800x600 VGA monitor

Operating System Support

- Microsoft Windows XP SP2
- Microsoft Windows Vista (32-bit or 64-bit)
- Microsoft Internet Explorer 6.0 SP1 or Internet Explorer 7.0 browser

Supported Wireless NICs

- Windows XP: Atheros AR5002X, AR5004X, AR5005X and AR5006X chipset based 802.11 a/b/g combo cards only
- Windows Vista: Atheros AR5002X, AR5004X, AR5005X, AR5006X and AR5008X chipset based 802.11 a/b/g/n combo cards (any combination)

Certified on:

- Netgear Double 108Mbps Wireless PC Card WG511U (Windows XP & Vista)
- D-Link AirPremier™ AG DWL-AG660 (Windows XP & Vista)
- Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Card (CB21) (Windows XP & Vista)
- TRENDnet TEW-621PC Wireless N-Draft PC Card (Windows Vista only)
- D-Link DWA-652 Xtreme N Notebook Adapter (Windows Vista only)
- Gigabyte AirCruiser N300 Dual mini GN-WI06N-RH (Windows Vista only)

Popular Protocols (full list available online)

802.11a/b/g/n, 802.11e/h
 10/100/1000, MobillIP, SMPP, HTTP, POP, FTP, SMTP, TELNET, RTP, SIP, SCCP
 MPEG-2, Citrix ICA, Oracle-TNS, SQLNET
 DICOM, FIX, FMCAST

SUMMARY OF KEY FEATURES:

On-Demand Monitoring	Packet capture, protocol decodes, Expert Analysis	Wireless Analysis
Network statistics <ul style="list-style-type: none"> ▪ number of frames/bytes, ▪ percentage of utilization ▪ broadcast and multicast counts ▪ Packet size distribution statistics ▪ Network error statistics ▪ Protocol usage statistics 	Packet Capture	Auto discovers wireless devices within range
Application statistics <ul style="list-style-type: none"> ▪ Individual station and conversation-pair traffic statistics ▪ Top talkers, top applications ▪ response time statistics for upper layer protocols 	Real-time and Post-capture Decode	Automatically Detect Rogues and Network Vulnerabilities
	Real-time Expert Analysis	Detailed Wireless Packet and Frame Analysis
	Focused Filtering and event triggers	
	Event notification and alarming	



©2009 NetScout Systems, Inc. All rights reserved.

Corporate Headquarters

310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 888-999-5946
www.netscout.com

European Headquarters

NetScout Systems (UK) Ltd.
100 Pall Mall
London SW1Y 5HP
United Kingdom
Phone: +44 (0)20 7321 5660

Asia/Pacific Headquarters

Room 105, 17F/B, No. 167
TunHwa N. Road
Taipei, Taiwan
Phone: +886 2 2717 1999
www.netscout.cn

NetScout, the NetScout logo, nGenius, Sniffer, InfiniStream are registered trademarks of NetScout Systems, Inc. Other brands, product names and trademarks are property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.