Sniffer Global

The industry's first truly enterprise-class portable network and application analyzer

Highlights

- Faster time-to-knowledge for wireless and wired network and application problems
- Dashboard views with deep drill-down to rich packet-level analysis
- Centralized control of tool usage to prevent uncontrolled access to network traffic
- Enterprise scale for deployment flexibility
- Integration with Cisco 3300 Series Mobility Services Engine (MSE) for location-based troubleshooting in wireless networks
- Wired and wireless support in a single, scalable tool
- Best-in-class network and application analysis functionality

Sniffer® Global is the industry's first enterprise-class, plug-and-play network analyzer for wireless and wired networks. Sniffer Global gives network managers on-demand network segment monitoring, best-of-breed protocol decodes and integrated packet-level expert analysis, and unified wired and wireless management with location-based context - all within a secure environment with true enterprise class control. The unlimited user license version of this software-based, portable tool provides total worldwide flexibility in deployment across a distributed organization, allowing anytime/anywhere access with no additional licensing costs.

With more than two decades of industry innovation and technology advances, "Sniffer" is one of the most recognized brand names in the industry. Sniffer Global builds on the best-in-class analyzer functionality of the Sniffer Portable Professional analyzer, adding enterprise-class security and control making it a foundational tool for troubleshooting and maintaining enterprise networks. Unique management capabilities of the Sniffer Global server include:

- Centralized usage controls on a per-user/per-role basis to ensure compliance by limiting who can access sensitive data using the software-based client application
- Policy-based user authentication to avoid compromising network or application security
- Online and offline user activity tracking and reporting to enable better auditing
- Integration with the Cisco MSE to display physical location of wireless devices in context with relevant wireless performances metrics
- Centralized license, upgrade and patch management to ensure consistency and transparency across multiple IT audiences and geographies
- Converged wired and wireless support for plug-and-play analysis of wired and wireless network links and wireless control infrastructure, supporting 802.11a/b/g/n with Wi- Fi Security Support, device and channel utilization and Wi-Fi traffic stats
- Best-in-class protocol decodes and integrated packet-level expert analysis, based on proven, widely deployed Sniffer technology

Recommended Applications

Sniffer Global provides network managers, field technicians and engineers with software to perform on-demand monitoring, packet capture and troubleshooting for wired and wireless network segments - all within a secure environment with true enterprise-class control. Common uses of Sniffer Global include:

- 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
- Location of mobile wireless devices on floor map, using integrated Cisco Mobility Services Engine data
- Second-level security risk assessments

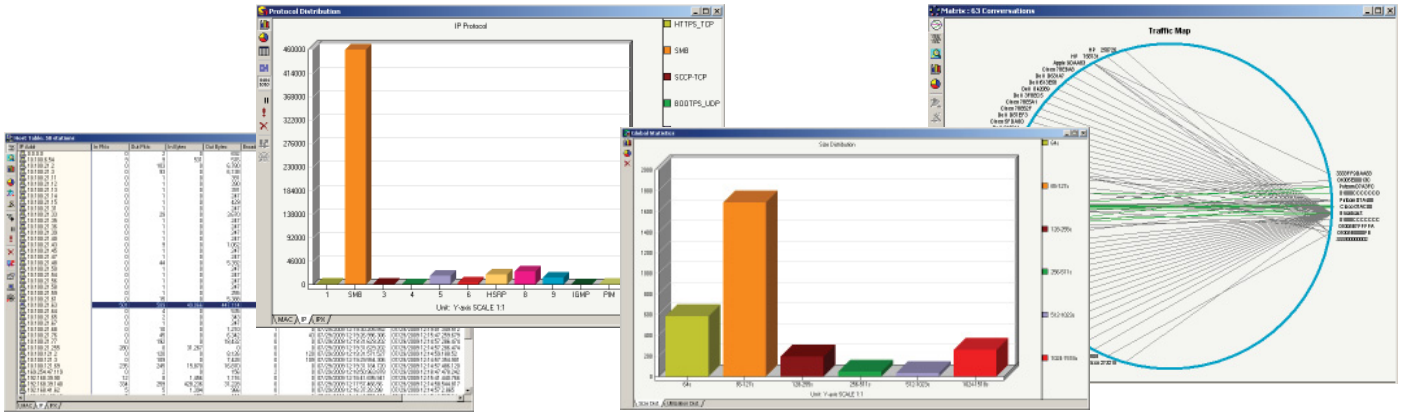

Figure 1: Sniffer Global builds on the best-in-class analyzer functionality of the Sniffer Portable Professional analyzer with on-demand packet capture, Expert analysis and robust decodes, but adds enterprise.

Enterprise-Class Security and Control

Unlike traditional portable protocol analyzers, which gives users full, uncontrolled access to network traffic traversing the wire - a potentially huge security problem - Sniffer Global contains a unique, centralized, policy-based access controls that govern how and what a user can manage on the network using the software-based client application. Before a Sniffer Global user can access network data, the client application logs in to the administrative server to authenticate. The server controls user access to network data and analyzer functions, monitors activity within the tool, and provides auditing and reporting. This helps prevent misuse of sensitive data contained in packet payloads.

Sniffer Global Administrative Server

The Sniffer Global Administrative Server acts as the central administrative point for individual Sniffer Global Application installations. Once the Sniffer Global Administrative Server is installed at a central point in the network, authorized users can download and install individual copies of the Sniffer Global Application using a standard web browser.

Sniffer Global Administrative Server provides:

- Policy-based user authentication
- Role-based usage control
- User activity tracking and reporting of both online and offline operations
- Centralized version control and updates
- Modular decode and expert update packs
- Location-based user correlation
- Flexible licensing
  - Enterprise license for unlimited use throughout an organization
  - 10-user license version in which the Sniffer Global Application can be installed on up to 10 laptops

On-Demand Monitoring

Sniffer Global provides a high-level view of network traffic and application performance using its dashboard view and drilldowns 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 Global dashboard network, engineers can monitor both network and application statistics, including:

Network statistics

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

Application statistics

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

Packet Capture, Decodes and Expert Analysis

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

On-Demand and Post-Capture Decode

Sniffer Global displays protocol decodes in real-time as packets arrive. It also 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 Global 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.

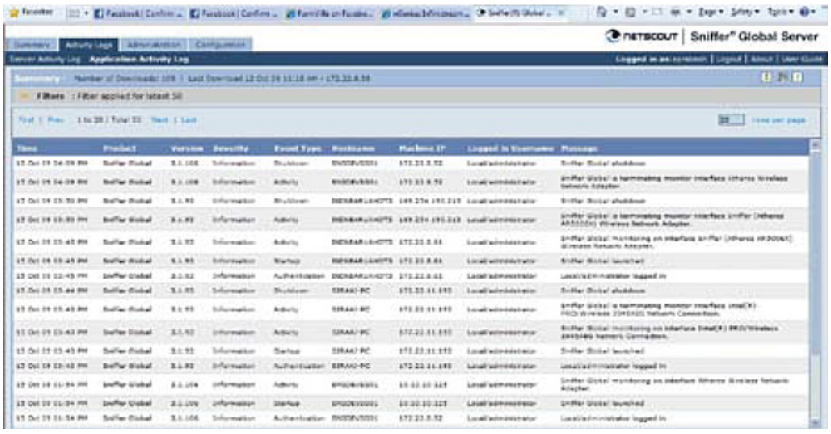

Figure 2: Activity logs track online and offline user activity for reporting and auditing purposes.

On-Demand and Post-Capture Expert Analysis

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

Focused Filters and Triggers

Sniffer Global 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. Filters provide a way to narrow in on the precisely data needed to troubleshoot a network problem. Filters also help reduce the size of files collected for historical records. 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 Global 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 Global Client Application can trigger an alarm and an action can be activated to initiate a packet capture.

Wireless Capabilities

In addition to monitoring wired networks, Sniffer Global provides full visibility into the performance and security of wireless environments.

Wired/Wireless Connectivity

For performing wireless network analysis, the Sniffer Global Application has two connectivity options:

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

Wi-Fi Device List

Sniffer Global 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 Global 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 Global 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.

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

Detailed Wireless Packet and Frame Analysis

Sniffer Global 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.

Figure 3: Integration with the Cisco® 3300 Series Mobility Services Engine (MSE) provides location information in context with wireless statistics for wireless devices in motion.

Integration with Cisco 3300 Series Mobility Services Engine

Sniffer Global solution is the only portable network analyzer to integrate with Cisco® 3300 Series Mobility Services Engine (MSE). The Sniffer Global client application discovers wireless hosts on the network, authenticates with the Sniffer Global Server to receive role-based privileges and request Location Services information to correlate host IP address.

Specifications and System Requirements

Sniffer Global Server

Minimum Hardware Requirements:

- Intel or AMD processor running at 1.6 GHz single or higher or dual or more core running at 1.0 GHz or higher (IA-64 processor not supported)
- 1 GB RAM or higher (2 GB recommended when integrating with Cisco MSE)
- 1GB SATA HDD or higher
- CD/DVD ROM drive
- VGA monitor with 1024x800 resolution
- Network Adaptor Card with 10/100/1000 interfaces

Operating Systems Support:

- Microsoft® Windows® 2008 Server R1 and R2 (32-bit & 64-bit)
- Microsoft Windows 2003 Server SP1 or later (32-bit & 64-bit)
- Virtualized environments configured to emulate these Server environments. Tested with VMware ESX/ESXi Server and Microsoft Hyper-V®

Sniffer Global Application

Minimum Hardware Requirements:

- Intel or AMD processor running at 1.6 GHz single or higher or dual or more core running at 1.0 GHz or higher (IA-64 processor not supported)
- 512MB RAM or higher; 1GB recommend
- 200MB free disk space or more
- CD/DVD ROM drive
- VGA monitor with 1024x800 resolution and support for 256 color or updated VGA driver

Operating Systems Support:

- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Server 2008 (32-bit or 64-bit)
- Microsoft Windows Vista® (32-bit or 64-bit)
- Microsoft Windows 2003 SP1 or later (32-bit or 64-bit)
- Microsoft Windows XP with SP2 or later (32-bit or 64-bit)
- Virtualized environments configured to emulate these operating systems, including VMware workstation/player, VMware® ESX/ESXi Server, and Microsoft Virtual-PC, and Hyper-V

Browser

- Microsoft Internet Explorer® 6.0 SP2, 7 or 8 browser

Network Interface Cards

- Ethernet 10/100/1000 cards with native driver provided by vendor
- Wireless 802.11a/b/g/n cards based on Atheros chipset with Sniffer-enhanced driver (packaged with the software)

NOTE: NetScout recommends having two wireless cards on the system—one for sniffing and another for connectivity. If using the Location Tracking feature, connectivity through a second card (wired or wireless) is necessary.

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

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

Copyright © 2013 NetScout Systems, Inc. All rights reserved. NetScout, nGenius, Sniffer, and InfiniStream are registered trademarks of NetScout Systems, Inc. and/or its affiliates in the United States and/or other countries. All other brands and product names, and registered and unregistered trademarks are the sole property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, and service and support programs.