

NETSCOUT® Sniffer Analysis

Why Consider Sniffer Analysis?

Sniffer® Analysis provides a direct-connect interface to nGenius® InfiniStream® appliances to perform unrestricted packet mining, forensic analysis and decodes across the nGenius InfiniStream packet store, solving complex, intermittent issues and performing network-related security forensics. With the option to filter on multiple criteria, users can perform packet analysis with decodes and experts, or drill down into root cause with Sniffer Intelligence using customized charts to visually isolate anomalies. The solution accelerates problem resolution and reduces the impact of service delivery outages and degradations. As management needs increase, the Sniffer Analysis solution can be leveraged into the nGenius Service Assurance Solution.

What Problems does Sniffer Analysis help solve?

Modern IP networks are increasingly complex. This drives a need for granular data and in-depth analysis for troubleshooting elusive problems. Level 2 and level 3 network escalation teams require rapid response tools to isolate and resolve existing problems across expansive, global networks. In some cases, such as network-related security events, the issue only happens once. There is no second chance to capture the flow. Timing is also critical in these situations. Sniffer Analysis can help speed this process, and thereby save the organization critical time and money.

Sniffer Analysis can be used to:

- Provide advanced packet-flow performance metrics for the evaluation of the efficiency of networked applications and services
- Troubleshoot service delivery degradations and slowdowns between network and applications
- Analyze network-related security issues to determine how a virus spreads and where vulnerabilities are being exploited

- Evaluate root cause of voice over IP (VoIP) quality problems in conjunction with sophisticated Sniffer Intelligence and play-back analysis
- Validate that applications and services are being delivered within correct policy and prioritization requirements such as Quality of Services (QoS) classes

What are the benefits of using the nGenius InfiniStream appliance in Standalone mode?

The nGenius InfiniStream appliance automatically records and analyzes packets traversing the network to avoid lost time waiting for problems to reoccur. Sniffer Analysis provides direct access to that robust data store. This directly improves an organization's ability to assure high availability and quality performance of today's complex IP-based business services.

Sniffer Analysis:

- Helps speed problem isolation and resolution for application and network performance issues
- Minimizes duration of service-impacting problems
- Provides a direct-connect, standalone interface, but can simultaneously work in conjunction with the nGenius Service Assurance Solution

The InfiniStream Console

The InfiniStream Console provides a direct-connect interface to one or more nGenius InfiniStream appliances. A traditional traffic-over-time display provides a thumbnail overview of traffic flows crossing the network to quickly spot trends. From there, flexible filtering and mining provide quick access to focus on any particular subset of the data. The user is free to isolate and retrieve captured data from anywhere across the InfiniStream data store. The InfiniStream Console serves as a launch point for back-in-time analysis.

Sniffer Intelligence

Sniffer Intelligence speeds performance analysis and problem resolution. Once a selection of data is isolated within the InfiniStream Console, Sniffer Intelligence modules provide detailed forensics analysis of that data. It automatically recognizes hundreds of well-known applications such as SAP® R/3®, Oracle®, Microsoft® Exchange, and VoIP traffic. Each type of application incorporates a rich set of packet-flow statistic, charts, and graphs to simplify the analysis process. As even more details are required, Sniffer experts and decodes are only a mouse click away to translate complex technical jargon into plain English to better understand, troubleshoot, and tune critical applications and networks. Optional Sniffer Intelligence modules are available for financial trading and mobile carrier applications.

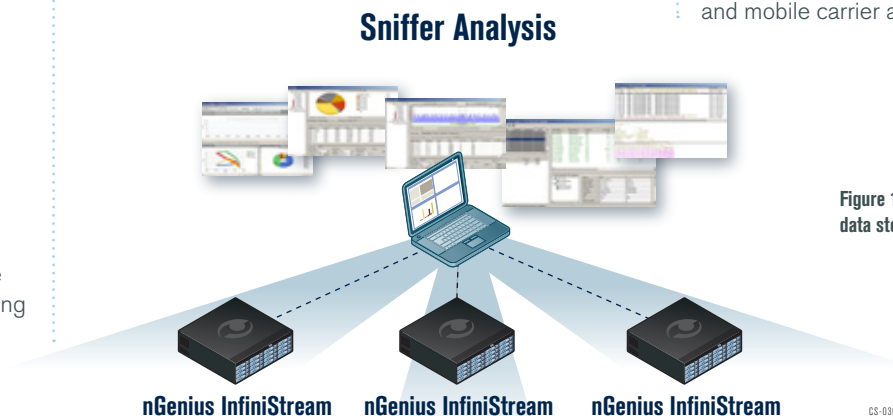


Figure 1: Sniffer Analysis provides a direct link to the rich data store of nGenius InfiniStream appliances.

The nGenius InfiniStream Appliance

The nGenius InfiniStream appliance enables forensics analysis by capturing network traffic 24x7 and storing it to disk for later analysis. The product leverages a highly available Linux®-based O/S and is designed for high performance. Intelligent deep packet capture and analysis is always-on, high-speed capture, recording and statistical analysis of rich packet details for granular post-event analysis.

All nGenius InfiniStream models support Sniffer Analysis. These are available in two product families:

- nGenius InfiniStream 2900 Series
- nGenius InfiniStream 6900 Series

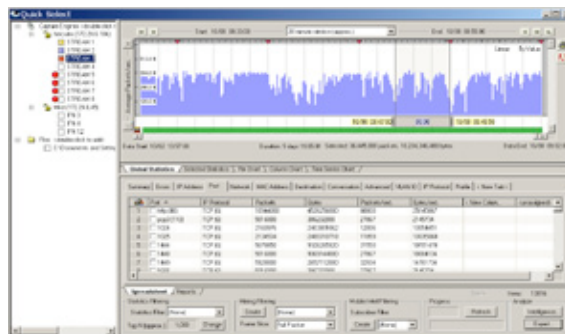


Figure 2: The InfiniStream Console depicting streams from multiple interfaces merged into a single view.

nGenius InfiniStream 2900 Series Appliance

The nGenius InfiniStream 2900 Series appliance, in a space-saving 1RU form factor, provides 'always-on' packet capture and analysis into access layer or branch offices. Specific functionalities of the nGenius InfiniStream 2900 Series appliance include:

- 500 GB of storage capacity for continuous recording
- Small, 1RU footprint profile that can be rack mounted in either 4- or 2-post deployments
- Low power consumption

nGenius InfiniStream 6900 Series Appliance

The InfiniStream 6900 Series is a high performance, resilient appliance for 'always-on' packet capture and analysis in core, distribution, and data center locations where high concentrations of business data conversations converge. Specific functionalities of the nGenius InfiniStream 6900 Series appliance include:

- Robust storage capacity options from 2 to 16 TB
- Multiple high-performance, multi-core processors for speed and performance
- Highest port density, with broadest range of link interfaces/speeds
- Variety of configurations to support high-capacity links, such as 10 Gigabit Ethernet, Gigabit EtherChannel, or multiple Gigabit Ethernet links
- Redundant power and storage drives for highly resilient operation
- RAID multi-drive storage for accelerated simultaneous recording
- Hot-swappable drives and power supplies

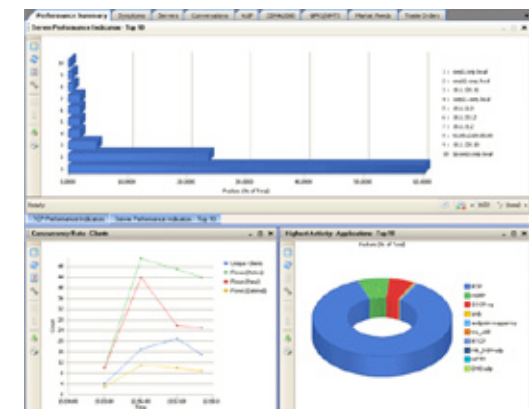


Figure 3: Sniffer Intelligence graphically represents data for quick analysis.



Corporate Headquarters

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

European Headquarters

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

Asia/Pacific Headquarters

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

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

© 2010 NetScout Systems, Inc. All rights reserved. NetScout, nGenius, Sniffer, and InfiniStream are registered trademarks and the NetScout logo is a trademark 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 Systems, Inc. reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, and service and support programs.