

SNIFFER®



MULTISEGMENT ANALYSIS

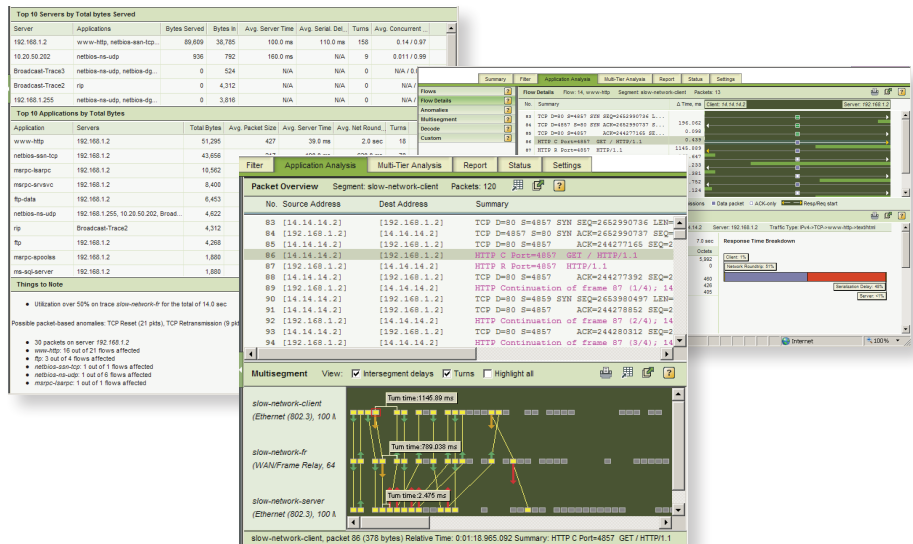
Troubleshooting the toughest networking problems

Benefits

Sniffer MultiSegment Analysis automates complex tasks to slash the time required to solve your most difficult networking problems

Sniffer MultiSegment Analysis:

- Consolidates trace files from across the network into a single session
- Synchronizes timings from one segment to the next
- Coordinates Web and Database transactions
- Pinpoints time delays
- Displays graphic views of application flows across time and space



Sniffer MultiSegment Analysis leverages automation and anomaly algorithms to highlight complex application performance delays.

Most routine networking issues are easily addressed. With proper monitoring, it is a snap to; determine who is downloading a large file, locate the source of a broadcast storm, find a backup running during prime hours, or notice a configuration change has knocked out a quarter of your network. Simple issues are best handled by simple solutions. Then again, not all issues are simple.

Troubleshooting Application Performance Issues

One of the most complex problems IT managers face is diagnosing application performance incidents. To improve availability, these business-critical applications are often distributed across the company, resulting in multiple routing hops traversing the LAN and WAN. In some cases, they are multi-tiered as well, crossing Web, Application and Database servers. In today's Modern IP Networks, complex problems are often obscured by load-balancers, proxies and firewalls, not to

mention all the other applications running simultaneously.

Analyzing the root cause of distributed application incidents requires diligence and understanding. Is the fault in the network, the application, the clients, the servers, or is it something else impacting performance? Such analysis is often time consuming, requiring packet captures from multiple points of the network. In the past, network professionals had to manually correlate network traces and determine the cause through a lengthy deductive process.

Sniffer® MultiSegment Analysis automates this tedious process. This NetScout solution uses sophisticated algorithms to correlate data, and present it in a cohesive collection of traffic flow latency, anomalies, and response times. Such information is useful to both network and application managers. Instead of finger-pointing, it helps people to work together to troubleshoot and solve the toughest networking problems.

How it works

Sniffer MultiSegment Analysis leverages the packets recorded by nGenius InfiniStream and extends troubleshooting, effectively slashing the time required to solve distributed application performance issues. This is accomplished by automating complex tasks that would otherwise need to be performed manually:

- Multiple trace files are brought together in a single database to create an analysis session
- Sniffer MultiSegment Analysis automatically discovers which packets and applications were seen at multiple points within the network
- It utilizes complex algorithms to synchronize the packet and flow timings both within and among the separate files (this allows for detailed intersegment timing analysis; in addition to total application turn times)
- Anomalies are noted for each flow, including the percentage of time spent on the client, server, and network



Proven Analysis Methods

Successful troubleshooting requires a logical, systematic approach. Sniffer MultiSegment Analysis builds this into the product. Users begin with a high-level application summary view across the enterprise. To isolate problems, troubleshooters often filter by applications, critical servers, and/or time ranges. Additional steps include reviewing anomalies or application flows that make up the data stream, which can be broken down into the associated packets and viewed from different network vantage points. This allows the user to determine both if and where a particular application was degrading. For example, screens clearly show if more time was spent on one network segment than others.

Nagging problems are sometimes ignored in hopes they will “just go away”. In fact, they rarely do. Sniffer MultiSegment Analysis, used with the “back-in-time” analysis capabilities of nGenius InfiniStream, provides the ability to address these intermittent or difficult to reproduce problems.

Multi-Hop Analysis

Distributed applications sometimes include a combination of web-based, front-end transactions that eventually hit a back-end database. These “n-tiered” applications are especially difficult to troubleshoot, because separate packets streams are seen on each side. Questions often arise such as:

- Why is one transaction slower than others?
- How much time is spent on the database server vs the Web server?
- What are the actual SQL commands generated?
- Which front-end transaction caused the database to grind to a halt?
- How can the different pieces be tied together?

For these complex applications, Sniffer MultiSegment Analysis can coordinate transactions across multiple hops to

provide front and back-end transaction details. This capability is especially helpful with troubleshooting multi-tiered web applications that commonly generate http/s and SQL traffic. Supported SQL types include Oracle, IBM DB2, MySQL and Microsoft SQL Server.

Visibility into Networked Applications

Sniffer MultiSegment Analysis demonstrates that NetScout knows more about packet-flow technology than anyone else in the industry. The product is unique in its ability to accept captures from as many as eight network segments, allowing even the most complex applications to be thoroughly analyzed. The product was designed to mimic the deductive logic and thought process typically employed by senior network engineers to solve multifaceted network performance issues. As a result, it automates many labor intensive processes used by top network technicians. Algorithms are used to match packets across the network, even when Network Address Translation (NAT) is in effect.

Comprehensive Reporting Capabilities

Results from Sniffer MultiSegment Analysis screens are available in printable form. Individual charts and graphs are easily transferred into other documents for archival. These reports often serve as forensic proof points for network and application managers to collaboratively address problems and prevent them from happening again.

Sniffer MultiSegment Analysis provides comparative reports to present side by side analysis of similar traffic captured at different times. This provides insights into how network configuration changes directly affect traffic. For example, these “before and after” reports can prove if a server or application’s average response time was directly improved (or degraded) after a configuration or networking change. So, not only can you solve the toughest networking problems, you can also prove the solutions worked!

About NetScout Systems

NetScout Systems provides advanced network and application service assurance solutions that deliver complete visibility into real-time, packet/flow-based operational intelligence. IT operators at the world’s largest enterprises, government agencies, and service providers use the Sniffer and nGenius solutions to troubleshoot service degradations faster and more efficiently in order to reduce MTTR.

Our world-renowned Sniffer and nGenius solutions include:

- Intelligent Data Sources for high capacity, deep-packet recording and monitoring
- Analysis Software for real-time and historical network and application performance management, troubleshooting, capacity planning, and reporting
- Advanced Intelligence for early detection and in-depth analysis of complex or specialized application services
- Comprehensive, global support, consulting and training services

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

©2008 NetScout Systems, Inc. All rights reserved. NetScout, the NetScout logo, Network General, the Network General logo, nGenius, Sniffer, InfiniStream, Business Container, Business Forensics, NetVigil and Quantiva are trademarks or 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.