



Highlights

With flexible configurations, scalability and the superior CDM architecture, the nGenius probe is an intelligent data source, enabling end-to-end views of the network, applications and services by:

- Supporting both physical and virtual network technologies to ensure comprehensive visibility of WAN and network edge deployments
- Forwarding critical response time measurements to detect application degradations
- Managing converged networks by providing visibility to key performance indicators and critical quality of experience metrics
- Enabling the unified approach of the larger nGenius Service Assurance Solution

nGENIUS | PROBES

Dedicated hardware-based intelligent data sources that generate key network metrics utilized by the nGenius Service Assurance Solution

Network environments are ever changing and the task of managing their performance is becoming increasingly complex. Whether the network is contained within a single building or supports a global organization, IT professionals need solutions designed to detect issues, diagnose the root cause, verify changes and manage performance problems for all applications and services.

To meet this need, IT organizations require reliable and consistent information they can trust. The nGenius® Probe is an intelligent data source that meets this requirement by monitoring packet-flow data directly from the network. Strategically placed nGenius Probe devices can be combined with other distributed data sources to provide end-to-end visibility across the network.

Part of the nGenius Service Assurance Solution

The nGenius Service Assurance Solution is a unified service delivery management platform that provides comprehensive, real-time network, application, and service performance intelligence. The unified approach to managing service delivery empowers the IT organization delivering complete visibility across the network. The nGenius Probe is a hardware-based data source that supports this solution. Other data sources include the nGenius InfiniStream appliance, nGenius Virtual Agent, nGenius Integrated Agent, and the nGenius Collector. All data sources forward information to the nGenius Performance Manager. Other components are available as well.

Empowered by the Common Data Model

The NetScout® proprietary Common Data Model (CDM) architecture provides unified metrics that scale across multiple topologies and interfaces. This traffic flow data is integrated into a common repository for consistent analysis, views and reports. CDM provides detailed information for emerging technologies and policy-based configurations, including VoIP, MPLS, QoS, VPNs and NetFlow.

Strategic Network Deployments

Flexible probe configurations allow the nGenius Service Assurance Solution to monitor traffic flows for multiple topologies.

The nGenius probes are strategically placed at edge locations for LAN, WAN, ATM and



Figure 1: With flexible configurations and unsurpassed scalability the nGenius Probes deliver critical network data to the nGenius Service Assurance Solution enabling unprecedented network visibility and insight into network conditions

For More information

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

POS network links via passive taps, with the optional monitoring of span switch ports for 10/100/1000 LANs.

The underlying technology of the nGenius Probe has been expanded to other nGenius data sources to provide more visibility in more network places. The nGenius InfiniStream® appliance includes many functionalities of a probe, but adds robust continuous storage and processing capabilities for comprehensive back-in-time, forensic analysis. The probe technology has also been virtualized into a software-only format with the nGenius Virtual Agent and placed into routing infrastructure devices with the nGenius Integrated Agent. This provides more options for the customer to deploy data sources wherever visibility is required at a price point that meets their needs.

How It Works

As a dedicated packet-flow monitoring device, the nGenius Probe monitors critical network edge links to generate key performance metrics such as traffic, application and service utilization, conversations, error conditions, resource utilization, response time and many others. The hardware-based device extracts its information with multiple interfaces attached directly to the network using either physical taps or mirrored switch ports (for some Ethernet interfaces). All this is done passively, with no impact to the packets traversing the network. Generated metrics are sent to the centralized nGenius Performance Manager as they are polled.

The ability to monitor a large array of network technologies, both physical and virtual, allows the nGenius probes to deliver key network metrics to the nGenius Service Assurance Solution. The nGenius Probe is ideally suited for deployment at the WAN and network edge locations that do not require the continuous capture of network packets. However, when shorter durations of packet traces are required, the nGenius Probe provides on-demand packet capture, copying live packets off the wire for further drill-down and analysis.

Key Features

Packet-Based Application Recognition and Monitoring

Support for a variety of application types, including:

- Well-known, user-defined and complex applications
- Peer-to-peer applications
- Web-based applications and URLs
- Industry-specific applications (e.g. IP FIX for financial, SMS for wireless service provider)

Packet Analysis and Troubleshooting Capabilities

- Provides on-demand packet capture

Response Time Analysis and Key Performance Indicators

- Passive application responsiveness measurements
- Supports response time metrics for virtually all application types
- Supports one-minute granularity: average response time, number of active sessions, number of successful transactions, and number of server error types
- Supports 15-minute granularity: maximum & average response time per client/server pair, total number of transactions, number of successful transactions, TCP connect time, number of active sessions, total packet loss, responses time distribution, number of timeouts, number of retries, and application payload
- Generates metrics used as key performance indicators including packet loss, inter-packet delay, client and server errors, and timeouts
- Supports IP addresses, phone extensions and connect times
- Supports packet-level visibility and decode of voice protocols
- Supports voice configuration data including Codec, dialing plan and QoS assignments

Network Management Metrics

- TCP, HTTP and server-specific performance and error conditions
- Percent utilization and packet/byte counts for link, host, host group, applications, conversations
- Link aggregation combines traffic data from multiple interfaces to support load balanced and redundant links
- Site monitoring tracks traffic from remote offices

Alarming and Event Identification for the nGenius Service Assurance Solution

- Define alarms for link utilization, CRC errors, application utilization, application response time, application availability as well as broadcast packets, multicast packet and multicast packets on the LAN
- Burst alarms at millisecond resolution
- "Power alarms" highlight root cause by gathering top users and applications automatically at violation time for segments exceeding utilization, responsiveness and availability thresholds
- Supports rising, falling and time-over-threshold templates
- Supports auto-actions to trigger scripts, packets decode and SNMP traps

Network Visibility

- LAN: Ethernet, Gigabit Ethernet
- WAN: Frame Relay (T3(DS3)/ E3/), ATM: (T3(DS3)/E3, OC-3c, OC-12c), POS: (OC-3c, OC-12c, OC-48c)
- Virtual Channels: VLANs, DLCIs, PVCs, QoS Groups (via DSCP)
- Encrypted Channels: MPLS, IP-enabled VPN

Implementation Options

- In-line connection via passive tapping device
- Span via switch mirror port for 10/100/1000 Ethernet

Supported Industry Standards

- LAN Probes: 10/100/1000 Ethernet: IEEE 802.3 standard for 10/100Base-T, IEEE 802.3ab standard for 1000Base-T, IEEE 802.3z standard for 1000Base-LX/1000Base-SX/1000Base-TX, RFC2021, RFC1757, RFC1213, VLAN standards: 802.1q and Cisco® ISL, SNMP Standards: SNMPv1,v2,v3
- WAN Probes: T3 (DS3)/ E3: IEEE 802.3 standard for 10/100Base-T, RFC1490 and Cisco ISL, SNMP Standards: SNMPv1,v2,v3
- ATM Probes: T3 (DS3)/E3/OC-3c/OC-12c: ATM Forum Standards: LANE 1.0/2.0, MPOA 1.0, RFC1577, SNMP Standards: SNMPv1,v2,v3
- POS Probes:OC-3c/OC-12c/OC-48c: SONET/SDH Standards ITU-T G707, Bellcore/Telcordia® GR-253, PPP over SONET/SDH RFC 2615, PPP in HDLC-like framing RFC1662, SNMP Standards (Communication): SNMPv1,v2, v3

Convergence Management

- Supports volume, utilization, host and conversation details for RTP voice and RTP video protocols
- Supports application-layer details for call setup protocols, such as SIP, H.323, Q.931 and MGCP, plus Cisco SCCP and Avaya H.323 extensions
- Supports VoIP quality metrics including jitter, call setup time, packet loss, incomplete and failed calls

Data Granularity

- Fifteen-second, real-time views with one-second peaks
- One-minute historically logged data for all application, host, and conversation flows

Product Specifications

	Specification	Note
Rack Unit	1 Server Rack Unit (1RU)	
Dimensions	Chassis:25"D x 17"W x 1.72"H (63.5cm x 43.2cm x 4.4cm)	
Weight	24lbs. (10.7kg)	
Management Port	RJ45	
nGenius Flow Director Port	RJ45	
Console Port	DB9F	
Environmental Specifications	Operating Temperature: 50° to 104°F (10° to 40°C) Operating Humidity: 5% - 95% (non-condensing)	
Power Requirements	100/240VAC, 6A, 40/40Hz, 350W	
Regulatory and Agency Approvals	Safety: UL, CSA, TUV EMI/EMC: FCC Part 15 Class A, CISPR 22 Class A CE, VCCI, NOM Laser Safety: May utilize Class 1 laser device	Laser Safety applies to Gigabit Ethernet models only

Connectivity Specifications

Probe Type	Number of Monitoring Ports	Monitoring Interface Types	Taps and Cables (Order Separately)
Gigabit Ethernet	SFP Pluggable: 2, 4, 8 SX/LX/TX configurable combinations 10/100/1000Base-T: 2,4, 8	SFP (SX) Interface: LC SFP (LX) Interface: LC SFP (TX) Interface: RJ45 10/100/1000Base-T: RJ45	SX: Passive 60/40 optical splitter Multimode (62.5 or 50 Micron) fiber SC LX: Passive 60/40 optical splitter, Multimode (9 Micron) fiber SC T: Active splitter/passive failover, dual redundant 12v power supplies
WAN T3(DS3)/E3	1, 2	T3(DS3)/E3 Interface	T3 (DS3)/E3: Tap DB15, Probe to Tap DB15, Tap to Net BNC
ATM T3(DS3)/E3	1, 2	T3(DS3)/E3 Interface	T3 (DS3)/E3: Tap DB15, Probe to Tap DB15, Tap to Net BNC
ATM OC-3c/OC-12c	1, 2	OC-3c/OC-12c MM: LC OC-3c/OC-12c SM: LC	MM: Passive 60/40 optical splitter, Multimode (62.5 or 50 Micron) fiber SC SM: Passive 60/40 optical splitter, Multimode (9 Micron) fiber SC
POS OC-3c/OC-12c/ OC-48c	1, 2 (OC-3c/OC-12c) 1 (OC-48c)	OC-3c/OC-12c MM: LC OC-3c/OC-12c SM: LC OC-48c: LC	MM: Passive 60/40 optical splitter, Multimode (62.5 or 50 Micron) fiber SC SM: Passive 60/40 optical splitter, Multimode (9 Micron) fiber SC OC-48c: Passive 70/30 optical splitter, Multimode (9 Micron) fiber LC



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

For More information

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, 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.

DSES_31_2010 Rev B