nGENIUS | PROBES

NETSCOUT.

Security-hardened distributed monitoring devices that collect key network metrics utilized by the *nGenius* Performance Management System

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 rely on *nGenius* Probes to provide them with unmatched network visibility. In conjunction with the *nGenius* Performance Manager these distributed monitoring devices provide unparalleled application recognition, response time analysis, convergence management, alarming and data granularity.
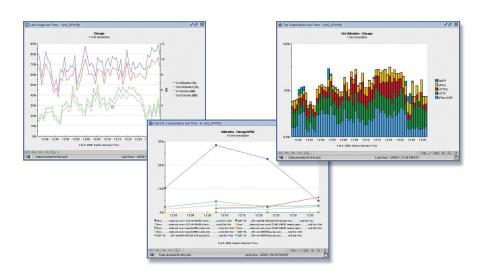
Empowered by CDM

NetScout's Common Data Model (CDM) architecture allows traffic flow data from disparate network technologies, regardless of the location within the infrastructure, to be 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 of *nGenius* Probes

Flexible probe configurations allow the *nGenius* Performance Management System to monitor traffic flows for virtually any network technology or topology and deliver a complete end-through-end view of the performance of applications and services.

The *nGenius* probes are strategically placed on LAN, WAN, ATM and POS network links via passive taps, with the optional monitoring of span switch ports for 10/100/1000 LANs.

With flexible configurations and unsurpassed scalability the nGenius Probes deliver critical network data to the nGenius Performance Manager to provide unprecedented network visibility and insight into network conditions.

How It Works

As dedicated monitoring devices the *nGenius* Probes deliver performance data collected from critical network links or mirrored switch ports throughout the network to the *nGenius* Performance Manager. The ability to monitor a large array of network technologies, both physical and virtual, allows the *nGenius* probes to support the *nGenius* Performance Manager's ability to provide real-time analysis and historical reporting of network metrics.

Highlights

With flexible configurations, scalability and the superior CDM architecture, *nGenius* probes provide end-through-end views of the network, applications and services by:

- Supporting both physical and virtual network technologies to ensure a comprehensive view of the network

- Delivering response time measurements to detect application degradations

- Providing robust real-time analysis and historical reporting with unsurpassed granularity

- Proactively detecting network problems by providing real-time alarms

- Managing converged networks by providing visibility to key performance indicators and critical quality of experience (QoE) metrics

Key Features

Application Recognition and Monitoring

Support for a variety of application types, including

- Well-known and children of well-known applications
- User-defined, custom-developed applications
- Complex applications using port-ranging/port-hopping
- Peer-to-peer applications
- Web-based applications and URLs
- Industry specific applications (e.g. IP FIX for financial, SMS for wireless service provider)

Packet Troubleshooting

- Robust packet capture decode engine (450 protocol family decodes)
- Perform four simultaneous packet captures per interface
- Launch packet capture from the user desktop
- Pre-capture filtering
- Supports capture and upload to *nGenius* Performance Manager
- Configure a data capture to start automatically by matching a pattern of packets

Response Time Analysis/Key Performance Indicators

- Passive application responsiveness measurements
- Supports response time metrics for virtually all application types
- Supports 1-minute granularity: average response time, no. of active sessions, no. of successful transactions, and no. of server error types
- Supports 15 minute granularity: maximum & average response time per client/server pair, total no. of transactions, no. of successful transactions, TCP connect time, no. of active sessions, total packet loss, responses time distribution, no. of timeouts, no. of retries, and application payload
- Supports the measurement of key performance indicators including packet loss, inter-packet delay, client and server errors, and timeouts

Convergence Management

- Supports volume, utilization, host and conversation details for RTP Voice and RTP Video protocols
- Supports application-layer details for call set-up protocols, such as SIP, H.323, Q.931 and MGCP, plus Cisco's SCCP and Avaya's H.323 extensions
- Supports VoIP quality metrics: jitter, call set-up time, packet loss, incomplete and failed calls, and MOS scores
- 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

- 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

Data Granularity

- 15-second, real-time views with 1-second peaks
- 1-minute historically logged data for all application, hosts, and conversation flows

Network Visibility

- LAN – Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet
- WAN – Frame Relay (T1/E1, T3(DS3)/E3/),HSSI, 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

Probe Implementation

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

Exporting data

- Export monitored traffic to nGenius AFMon in storage server mode for storage and network forensic investigation
- Supports 10/100/1000 Ethernet Interface Speeds

Supported Industry Standards

- LAN Probes: 10/100/1000/10000 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, IEEE 802.3ae for 10 Gigabit Ethernet, RFC2021, RFC1757, RFC1213, VLAN standards: 802.1q and Cisco ISL, SNMP Standards: SNMPv1,v2,v3
- WAN Probes: T1/E1/T3 (DS3)/ E3/HSSI: 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: LANE1.0/2.0, 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

Connectivity Specifications

Probe Type	Number of Monitoring Ports	Monitoring Interface Types	Taps and Cables (Order Separately)
Ethernet /Fast Ethernet	2, 4, 8	10/100Base-T: RJ45	T: Active splitter/passive failover, dual redundant 12v power supplies
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
10 Gigabit Ethernet	1	SR Interface: LC LR Interface: LC	SR: Passive 60/40 optical splitter, Multimode (62.5 or 50 Micron) fiber LR: Passive 60/40 optical splitter, Multimode (9 Micron) fiber
WAN T1/E1	2, 4, 8	T1/E1 Interface T1D/E1D Interface	T1/E1: Tap DB26, Probe to Tap DB26, Tap to Net (One of) V.35, X.21 Single or Dual clock, EIA-530, RS449 or RS232 T1D/E1D: Tap DB25 to 4 RJ45, Probe to Tap DB26 to DB25, Tap to Net (T1/D) RJ48 and RJ48 to Bantam, Tap to Net (E1/D) RJ48 to Bantam and RJ48 to Dual BNC and G.703 BNC to BNC
WAN HSSI/T3(DS3)/E3	1, 2	HSSI Interface T3(DS3)/E3 Interface	HSSI: Tap DB26/MD50, Probe to Tap DB60 to 26, Tap to Net MD50 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

Product Specifications

	Specification	Note
Rack Unit	1 Server Rack Unit (1U)	
Dimensions	Chassis:25"D x 17"W x 1.72"H (63.5cm x 43.2cm x 4.4cm)	Certain models are configured in chassis with the dimensions 20.5"D x 17"W x 1.72"H (52.1cm x 43.2cm x 4.4cm)
Weight	24lbs. (10.7kg)	Certain models are configured in chassis weighing 18lbs. (8.2kg.)
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	Certain models are config-ured in chassis with power requirements of 100/240VAC, 4/2A. 60/50Hz, 200W
Regulatory and Agency Approvals	Safety: UL, CSA, TUV, CE, VCI, AUSTEL EMI/EMC: FC15 Class A, CISPIR 22 Class A Harmonic and Flicker Laser Safety: May utilize Class 1 or Class 1M laser device	Laser Safety applies to Gigabit Ethernet models only

NETSCOUT®

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, trouble-shooting, capacity planning, and reporting
- Advanced Intelligence for early detection and in-depth analysis of complex or specialized application 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

DS0801-02revA