

Threshold & Event Notification



Real Traffic flows



Per flow Measurements



Secure VPNs



Latest Applications



diversifEye™

Per flow Covered
Network Test Systems

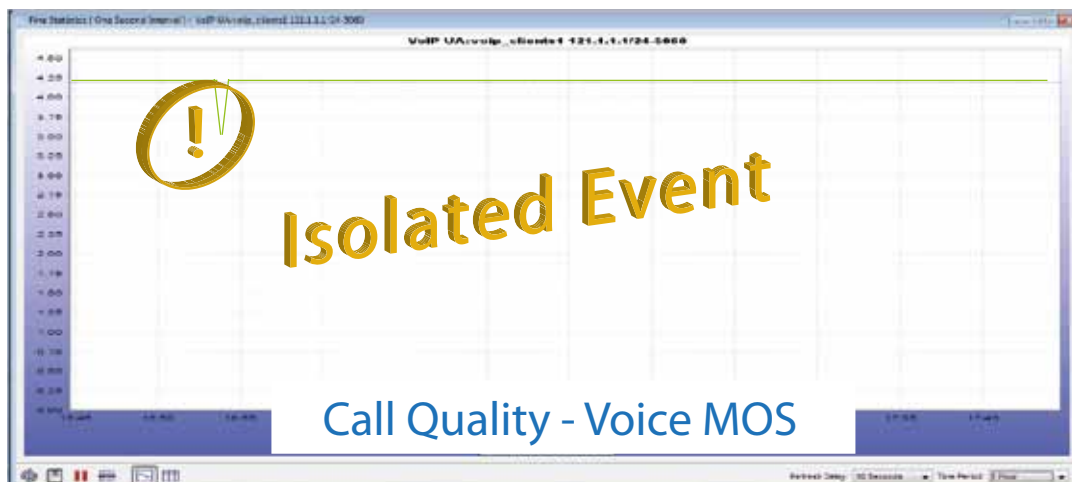
Improving performance in Reliability Tests

Defining Network or device reliability is often seen as achieving an acceptable level of performance which is sustainable for 99.999% of the time. Qualifying reliability is a straight forward task. However, when asked "How do you improve performance during reliability testing?", a simple task now becomes mission impossible.

There is any number of ways to test a device or network for reliability. The most influential is to show reliability in terms of end-user Quality of Experience. Another important aspect of reliability testing is the ability to accurately repeat tests.

The ability to identify when an issue occurs and then correlate the issue with any influences in the surrounding environment is the fulcrum on which performance of reliability tests can be improved.

However, the pin-pointing of the cause to the issue in reliability testing can be likened to finding a needle in a haystack. Post analysis will show an issue occurred but offers no real value in determining cause and effect. The only precise method of identifying cause is to identify and capture when the issue occurs live, during testing.



An aggregated or mean value representation of performance can result in isolated events going un-noticed.

To improve performance in reliability testing, these isolated per flow event instances need to be accounted for.

Per flow Emulation & Performance Measurements



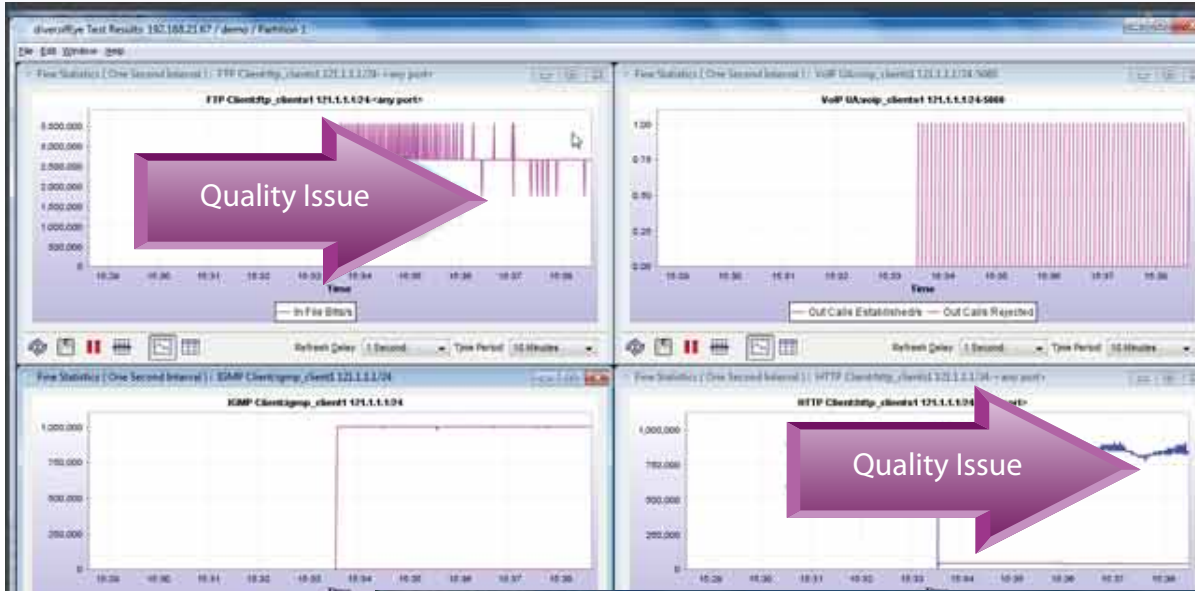
diversifEye is the only solution available today providing per flow emulation of stateful traffic flows representative of real-end users and activities. Emulation provides the ability to accurately repeat tests. Another benefit of diversifEye is the ability to measure performance on each and every emulated flow, providing unrivalled granularity in determining Quality of Experience. Using diversifEye, users can test and measure performance on any of the following network types or protocols -

- Access (DSLAM, FTTx, CMTS, WiMAX)
- Aggregation Switches/Routers
- LTE (eNodeB, PDN, SGW)
- Telepresence (Video & Audio)
- CMTS DOCSIS® 3.0 / EuroDOCSIS 3.0 / EdgeQAM
- Triple Play - IP TV, VoIP, Data
- DPI (Deep Packet Inspection) / DLP (Data Loss Prevention)
- Intrusion Detection/Prevention/Firewalls
- Application Servers (web, email, ftp)
- OTT - Adaptive Streaming
- Address Assigment (DHCP, PPPoE)
- Secure VPN (IPSec - IKEv1/IKEv2, SSL, TLS, DTLS)
- TWAMP
- IPv6 migration (IPv6, Dual-Stack Lite, 6rd, 6to4)
- WAN Optimization
- DNS
- Security Attack Mitigation Strategies (spam, virus, DoS)

Thresholding and Event Notices

A crucial aspect in improving performance in reliability tests is to identify issues live during tests. diversifEye's Thresholding and Event functionality is the fulcrum on which success is hinged.

diversifEye's thresholding feature uses a set of algorithms to actively monitor the performance on any number of unique performance metrics. Thresholds can be applied to each and every emulated application flow. On traversing the threshold, diversifEye generates event notices. diversifEye's event notices represent a violation of the threshold value or clearance state, the violation no longer exists. To remove any in-accuracy in reporting events diversifEye enables users define rules to prove that a violation or clearance is true.



diversifEye provides performance measurements on each and every flow.

Each application has its own unique set of metrics.

Thresholds can be applied to any metric, logical expressions are used to bind metrics to give more advanced handling.

diversifEye GUI client or Command Line Interface are used to display Event Notices during live tests.

Event Notices are exported as a part of the Detailed Analysis Reports.

Event Notices can be utilized in the CLI to trigger more advanced features e.g. email warning that a threshold rule has been violated.

The screenshot shows the main interface of the diversifEye GUI. At the top, there's a menu bar (File, Edit, View, Window, Admin, Help) and a toolbar. Below that is a 'Test Groups' tree on the left and a main table of applications. The table has columns for Name, Type, Description, Host, Host IP, Port, Represents, Association, and Spontaneousness. Below the table, there are summary statistics: 'Total: 307', 'Enabled & In Service: 307', and 'Active: 254 of 307'. At the bottom, there's an 'Events for Test Group: j77yln_jmy' table with columns for Date/Time, ID, Correlation ID, Event Type, Threshold Name, Threshold Rule, and Source. A purple arrow points to this table with the text 'Detailed Event Notification - time stamping Quality Issue'.

Name	Type	Description	Host	Host IP	Port	Represents	Association	Spontaneousness
4712 Performance Test 01	Test Group							
FTP Client	Application	FTP Client	192.168.21.67	192.168.21.67	21	Application		
VoIP	Application	VoIP	192.168.21.67	192.168.21.67	5060	Application		
KMP	Application	KMP	192.168.21.67	192.168.21.67	80	Application		
HTTP Client	Application	HTTP Client	192.168.21.67	192.168.21.67	80	Application		

Date/Time	ID	Correlation ID	Event Type	Threshold Name	Threshold Rule	Source
11/07/2011 11:38:34	33	53	Violation	Test_Threshold_MOS	In Bit = 70000000	Source
11/07/2011 11:38:35	34	54	Violation	Test_Threshold_MOS	In Video = 90000000	Source
11/07/2011 11:38:36	35	55	Clear	Test_Threshold_MOS	In Bit = 70000000	Source
11/07/2011 11:38:37	36	56	Clear	Test_Threshold_MOS	In Video = 90000000	Source
11/07/2011 11:38:38	37	57	Violation	Test_Threshold_MOS	In Bit = 70000000	Source

Live Event Capture

Pin-pointing cause and effect is critical in the mission to improving performance in reliability testing. Imagine capturing data before and after a quality issue arises!

diversifEye not only provides the ability to capture data surrounding the threshold violation but also enables users replay the traffic to accurately pin-point any issues.

Per flow Traffic

Emulation & Analysis

diversifEye System Overview

diversifEye™ consists of a fully integrated, highly scalable hardware and software platform. diversifEye™ is shipped with a complete range of software modules and sample test cases covering all application scenarios.

The diversifEye™ GUI client is noteworthy for its ease of use while offering full automation and batch testing functions through the diversifEye™ Job function or scripting interface. diversifEye™ allows users to easily generate fully automated reports and statistics, offering both real time and offline processing of results both during testing and post analysis.

- Stateful traffic Emulation, 1GbE and 10GbE
- Per flow Thresholds
- Multiuser and Extensive Post analysis Reporting
- Fully Compliant TCP Stack with Stateful Traffic
- Command Line Interface

19" rack mountable chassis



Contact Information

North America | 533 Airport Boulevard, Burlingame, CA 94010, USA
Tel: +1-650-288-0511 Fax: +1-650-745-2641

Europe | Brook House, Corrig Avenue, Dun Laoghaire, Ireland
Tel: +353-1-236-7002 Fax: +353-1-236-7020

Web: www.shenick.com email: info@shenick.com

About Shenick

Shenick Network Systems delivers award-winning per-flow IP communication test and performance measurement solutions, which enable service providers, network equipment manufacturers and enterprise and government organizations to test and deliver revenue-generating infrastructure and services.

Shenick addresses next-generation converged IP network and application performance issues for OTT Video, IPTV, VoD, Multi Play (VoIP video, data), Telepresence, IPsec/SSL secure VPN, Security Attack Mitigation, Deep Packet Inspection (DPI), Traffic Shaping, Peer to Peer (P2P), Application Server Test, Metro Ethernet and IPv4/IPv6 hybrid network deployments.

Established in 2000, Shenick has deployed its diversifEye™, and serviceEye™ Spider integrated network, application and security attack emulation and performance monitoring systems globally.

Software Overview

- Per flow Thresholding
- Secure VPN client emulation (SSL/TLS/DTLS)
- IPsec IKEv1, IKEv2
- TelePresence end point emulation (TIP)
- PPPoE client and PPPoE server
- DHCPv4/v6 client and DHCPv4 server
- VLAN & Double Tagging (Q-in-Q)
- DNS client/server
- TWAMP - RFC 5357
- IPTV - IGMP V1, V2, V3 & MLD V1, V2
- MPEG2-TS over TCP Analysis (China IP-TV 2.0)
- VoD - RTSP (supports fast-forward, rewind and pause functionality)
- SIP and HTTP enabled VoD
- VoIP - SIP & RTP, Dual Hosted IPv4 & IPv6 UACs, B2BUA (RFC3261)
- OTT - HTTP adaptive streaming
- IMS - SIP enabled RTSP sessions
- RTP - Latency performance measurements
- Voice & Video quality metrics - No Reference Analysis
- HTTP - Get/POST functionality. Customizable Headers with automated substitution
- SMTP - Customizable Headers with automated substitution. Include email attachments
- POP3
- P2P
- FTP - Passive and Active
- Spam / Viruses / DDOS
- PCAP file replay - Accepts file sizes > 1Gigabit
- TCP Replay - Multiple (payload) substitutions in each flow in the PCAP
- UDP/IP Playback - Emulate Skype type applications
- Concurrent IPv4 and IPv6 application flows
- Dual-Stack Lite, 6rd, 6to4
- GTP Tunneled Applications
- Automation

Software libraries and GUI interfaces are standard and compatible across all chassis types. Applications are both IPv4 and IPv6 enabled. Software support for up to 6 concurrent users.

