



diversifEye™

Next Generation Network &
Applications Test Solution

Sample Test Scenarios



diversifEye™

Per flow Converged IP Network Test Systems

Sample Test Scenarios

Below is a list of various scenarios, where diversifEye's functionality is used to measure performance.



Triple Play

How can I ascertain on a per-viewer basis what the IPTV performance will be for channel change 'zap' rate testing under a variety of load conditions?

Unlike point-to-point network applications, multimedia applications such as IPTV, data casting (news, stock tickers) and distance learning depend on the ability to send the same information from one server to many users across an IP network. The deployment of this type of multipoint service presents an interesting challenge for network operators that need to understand the performance capability of a multicast infrastructure. The performance of unicast services is measured by sending a number of packets from a server to a user while measuring the delay and loss across the network. These traditional performance metrics are insufficient to quantify a good multicast service.

Multicast delivers IP packets to a group of hosts or users on the network. IGMP is a session-layer protocol used to establish membership in a multicast group - a set of routers and users that send and/or receive multicast data streams from the same source. Routers use three messages to communicate to each other about the multicast traffic. A host uses the report message to join a new group. Query messages are used to discover which hosts are members of a given group. Report messages are sent by hosts in response to queries from a router. Finally, Leave messages are sent when the host wishes to leave a given group. With multicast services like IPTV, capacity planners face additional challenges when testing the limitations of a network design. Multicast protocols can be taxing on the routers resources and therefore additional capacity limitations must be quantified. Meanwhile consumers of IPTV services expect instant channel changing which gives rise to stringent network performance objectives. A sample of performance questions may include -

- What is the IPTV channel-surfing (zap rate) capacity of the network?
- For a number of IPTV multicast groups, what is the time to join each group?
- For a number of multicast groups, what is the time to leave each group?
- What is the packet loss rate, while the users are connected to a group?
- What is the throughput with a single multicast group with one 'virtual customer'?
- What is the throughput with a single multicast group with a million customers?
- What is the throughput with many multicast groups with many users?
- What is the throughput with many groups and users with a high 'zap'-rate?
- How much bandwidth is required for services using different CODECs?



How is the performance of my security infrastructure (Firewall, IDS/IPS, DDoS Mitigation, AntiVirus, AntiSpam system) effected under regular high load traffic conditions and also when both attack traffic and regular traffic are active?

Its not just about modeling and testing individual customer IP application flows but also having the confidence to understand the effect on customer quality of experience under attack conditions. Crippling DDoS (Distributed Denial of Service) attacks and email system integrity during Virus Attacks can cause havoc.

Shenick diversifEye is the first test system to offer attack throughput testing on an 'End to end' basis for DDoS attacks, virus and spam. For example, instead of just generating DDoS attacks in a 'fire and forget mode' Shenick diversifEye can also test how much actually gets through a security device such as Firewall, IPS or DDoS mitigation device. This is because Shenick diversifEye's integrated client and server mode of operation permits both an attacker and victim view. Reflective DDoS attacks are also fully supported in diversifEye with attacker, unwitting participant and victim emulation. Shenick diversifEye can also generate both real viruses as email attachments and also safe mode 'defused' viruses. Every email can have a different attachment to emulate a truly real world scenario mix of regular email attachment traffic, virus/worm and spam emails.

Shenick diversifEye offers the ability to generate very large quantities of peer to peer, web, email (with attached viruses), streaming and multicast traffic in order to determine QoS and QoE (quality of user experience) at both network and application layers. A unique benefit is that Shenick diversifEye emulates and maintains statistics for each and every IP application flow and can therefore provide individual customer and overall collective service response under both regular and attack conditions.



How do I know whether a P2P traffic shaping or mitigation device will actually work under high connection rates, myriad P2P protocols and will my end user customer experience remain consistent under a variety of application load conditions?

Over the past couple of years there have been multiple news reports suggesting that about half of internet traffic transactions now involve peer to peer (P2P) sharing of music, video and other files. While it is commonly held that a large proportion of this file sharing is illegal, the actual P2P protocols themselves are legal. There is plenty of scope for legal file sharing and myriad legitimate P2P applications are emerging. In certain countries, broadband subscribers are even being offered P2P service rates to carry value added applications such as VoIP and extra bandwidth at premium broadband rates. There is an increasing requirement for network service providers and the vendors of P2P mitigation, traffic shaping and policing equipment to test their capabilities in distinguishing illegal vs legitimate traffic.

The only way to do this is by establishing a test environment in which individual P2P sessions can be generated using a variety of such protocols while also including a real world mix of other internet application protocols such as HTTP, SMTP, IGMP, Streaming etc. Shenick diversifEye provides the capability of establishing programmable signature based P2P sessions in a fully meshed mode of operation while concurrently generating high volume application flows. One of the most important aspects associated with performance relates to how the insertion of these P2P devices in a network effects user quality of experience. Testing such infrastructure for performance bottlenecks is the primary goal and Shenick diversifEye provides this within a completely integrated test environment.



How well do my WEB SERVERS, EMAIL SERVERS, STREAMING, CACHE SERVERS, LOAD BALANCERS, L4-7 SWITCHES perform under increasing user connection rates and what are the true limitations of my applications infrastructure?

True performance limitation and user quality of experience testing for your L4-7 applications requires an emulation environment that offers the ability to emulate real application conditions experienced in real life.

The only way to do this within the confines of a test environment is to emulate and track the performance of real stateful application traffic flows under normal network conditions and to also consider the effects of security attacks (for example, DDoS) and associated performance overhead.

diversifEye is designed to test the performance of a Web Server by emulating the browsing behavior of thousands of Web clients and capturing metrics that indicate system performance and user satisfaction . Simply stated, how many HTTP clients can the SUT successfully process? For a Web Server this problem is complicated by the fact a client may have an open connection but not actively transferring data. Therefore, capacity limitations for the Web Server are subdivided and various test procedures undertaken such as:

- Maximum Number of HTTP Get Requests Per Second
- Maximum HTTP Connection Establishment Rate
- Maximum Network Utilization
- Maximum Number of Simultaneous Open Connections

Typically performance is measured and compared against stated objectives. As with many mission critical systems, the goal is to determine what conditions cause the system under test to breach its performance thresholds.

For example, the HTTP Get Response time is a critical measurement of performance for a Web Server. If a browser does not get a prompt response, studies reveal that the user is likely to give up and seek out a different page. This metric is associated with a performance threshold. As typical user Get Response Time rises above the threshold, performance is deemed insufficient. Furthermore, a statistical analysis is often used to balance system costs with user experience. A user can tolerate some slow downloads, if they happen infrequently. In other words the performance objective may be extended to state that the system under test had adequate capacity while 95% of Web Requests are measured below the desired threshold. In addition, other metrics give an indication of a quality service. In order to keep response times low, excessive TCP congestion must be avoided and a number of TCP counters may be used to indicate potential performance issues. For example, TCP retransmissions and Out of Sequence packets.

Once the tests are run and performance limitations understood, the information can be used as a form of Admission Control, where an IT Manager is aware of the consequences of granting system access to more users than it is rated for.

Shenick is an award winning provider of IP communications test and measurement systems. Shenick's diversifEye and servicEye are used to assess and monitor network, application and security infrastructure performance limitations.

diversifEye™ and servicEye™ are integrated network, application and security attack emulation and performance assurance test systems which are used by major IP-oriented network service providers, communications equipment manufacturers, large enterprises and governments.

Shenick's diversifEye addresses key next-generation converged network and application performance issues covering IPTV, Voice, Data, IMS, Security Attack Mitigation, Traffic Shaping/Peer to Peer (P2P), Application Server, Metro Ethernet and IPv4/IPv6 hybrid network deployments.

Shenick's servicEye is an active quality assurance solution, born out of award winning and industry proven quality assessment technology with a focus on end-end performance measurements, including subscriber/client premises.

Shenick is the proud recipient of Internet Telephony's 2009 IPTV Excellence and 2008 Product of the Year and IPTV Excellence awards. Adding to these achievements are the Frost and Sullivan 2008 Global Technology Innovation Award for DPI. Other awards from Frost and Sullivan include the 2007 Global Product Innovation Award, 2006 Emerging Company of the Year Award in the Communications Test and Measurement industry sector along with the 2005 European Product Line Strategy Award.

Shenick Network Systems

Ireland : Brook House, Corrig Avenue, Dun Laoghaire, Co Dublin, Ireland

t: +353-1-2367002

info@shenick.com
sales@shenick.com

Regional Support Email Contact Details -

Americas: amer-support@shenick.com

Asia Pacific: apac-support@shenick.com

Europe, Middle East & Africa: emea-support@shenick.com

Global Sales & Support

North America : 533 Airport Boulevard, Burlingame, CA 94010, USA

t: +1-650-288-0511

© 2010 Shenick Network Systems Limited. All rights reserved, subject to change without notice. diversifEye and servicEye are trademarks of Shenick Network Systems, all other names are trademarks of their respective owners and hereby acknowledged.