



# Test Deep Packet Inspection devices with diversifEye™

Deep Packet Inspection (DPI) is responsible for enforcing traffic shaping and policing and increasingly includes security attack mitigation functions. Fair usage of bandwidth policy management, P2P traffic shaping and filtering, QoS and SLA management, traffic profiling and statistical information gathering are gaining increasing importance. Fundamentally, DPI devices must identify and if necessary act upon each and every network traffic flow.

Testing DPI devices therefore requires a 'Per Flow' approach involving emulation and analysis of multiple application types in real time. Diversity of application types and flows are key to successful DPI testing.



## Example Configurable Application Functionality

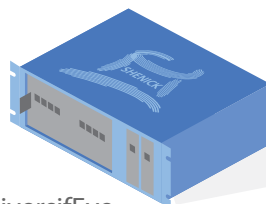
- HTTP : GET, POST, HEAD
- SMTP : FROM, TO
- POP3 : SERVER, USERS, DELETE
- FTP : GET, PUT, CD, LS, PWD
- DHCP : DISCOVER, REQUEST

## Complete TCP/IP Stack Control

- HTTP | SMTP | POP3 | FTP | DHCP | P2P | SIP | RTP | RTSP | SSL/TLS
- TCP | UDP | Replay
- IPv4 | IPv6 | Dual-Stack Lite | IGMP / MLD
- VLAN Tagging | QoS/Diffserv
- PPPoE | Ethernet
- Copper | Optic

## Sample Customizable Content

- HTTP : Header fields, Content real or dummy pages
- SMTP / POP3 : Mail Headers, Content, Attachments
- IGMP/MLD : Run MPEG-2 and MPEG-4 files
- VoIP : Utilize real Voice encoded files
- P2P : bitTorrent™, Kazaa™, edonkey™, Skype™ etc
- Security Attack Type Traffic : DDoS, Spam, Viruses



diversifEye

## Per Flow Emulation, Test and Performance Measurements

## Mix Traffic Types & Usage Profiles

- Concurrent IPv4 and IPv6 Flows
- Good or 'legal' Traffic Flows
- Bad or 'illegal' Traffic Flows

## Sample DPI Test Scenarios

### Per Flow, Emulation and Performance Measurements –

Emulate thousands of real clients running multiple applications. Ensure each client and application are identified correctly. Measure performance impacts such as latency on the individual flows.

### False Positive/False Negative Identification –

Ensure that all emulated flows are classified correctly, with minimum errors in terms of handling. Test that no flow is misclassified e.g. SMTP, POP flow identified as illegal and filtered, and that no illegal flow is passing unchecked.

### P2P identification and control –

Emulate a large number of clients running legal P2P flows and include illegal P2P flows. Ensure the correct identification and control mechanism is occurring on the legal and illegal P2P flows.

### Per flow QoE testing in normal and security attack conditions –

DPI devices are expected to identify and filter illegal traffic such as SPAM, Virus and DDoS attacks. Emulate extreme traffic conditions with good and bad client traffic applications running, ensure all flows are identified and handled correctly.

diversifEye's per flow architecture emulates and measures real/stateful TCP and UDP based application flows. diversifEye offers a mix of standard and non standard video, voice and data application protocols, coupled with the ability to generate concurrent security attack traffic such as distributed denial of service (DDoS).

In addition, diversifEye offers the most realistic and accurate capture replay function in the test industry today to emulate the latest peer to peer (P2P) and other proprietary protocols.



To validate throughput, profiling capabilities and traffic shaping of DPI devices requires real network flows and conditions. diversifEye is a single chassis solution providing the flexibility and functionality to control and deliver these large scale unique conditions.

diversifEye™ is the only integrated network, application and security attack emulation and performance analysis IP test system providing granularity on a per flow basis. Mix real flows and replay functionality to deliver the widest mix of application traffic types.

The Shenick diversifEye platform & GUI supports per flow test and measurement of :

## Analysis Software Overview

- DHCPv4 & DHCPv6
- PPPoE
- VLAN & Double Tagging (Q-in-Q) with priority
- Concurrent IPV4, IPV6 and Dual-Stack Lite flows
- IGMPv1, v2, v3 / MLDv1, v2
- Voice and Video Quality Metrics
- Telepresence
- RTSP (Video on Demand)
- SSL
- VoIP (SIP & RTP)
- HTTP
- FTP
- SMTP
- POP3
- P2P
- TWAMP
- Attack Traffic - Spam / Viruses / DDOS
- PCAP file replay (>1Gb)

## Deep Packet Inspection Testing Efficacy vs Effectiveness

### Efficacy

- Traffic Identification Per-flow granularity is key when measuring DPI performance. It's essential that all flows and applications are unique and different. Determine if all flows identified.
- Fair Usage Policy Emulate multiple flows for unique users and applications, create heavy bandwidth usage flow profiles. Ensure all flows and signatures are profiled and handled correctly.

### Effectiveness

- Quality of Experience Ensure in real-time, on a per flow basis that the system has no impact on revenue generating or delay sensitive applications, especially under varying usage settings.
- Security Attack Mitigation It is equally important to measure performance under extreme conditions. DPI devices must maintain operation throughout extreme conditions such as DDoS type attacks. Emulate a mix of legal and illegal traffic flows, ensure no performance loss on legal flows.

## Key Features And Benefits

- Network QoS and per flow QoE granularity for individual emulated client users across multiple devices and application traffic flow types.
- Latest protocols supported from Data Applications (HTTP, FTP, POP/SMTP, P2P), IPTV (IGMP/MLD), VoD (RTSP), VoIP (SIP/RTP), Telepresence all in a single test package.
- TCP Replay Substitution automatically varies payloads so no two PCAP sessions are the same.
- Support for SSL, TWAMP, IPv4, IPv6 and Dual-Stack Lite.
- DHCP emulation, PPPoE and IPoE Service Interoperability Scenarios. Emulate per device MAC and IP address assignments.
- Security Attack Mitigation support for DDoS style attacks SYN/RST/UDP/ARP floods, reflective DDoS attacks, Ping of death, etc.
- Large memory space (>1Gb) for PCAP replay for Instant Messaging or Web Mail.
- Client and server support on a single blade within one chassis with complete flexibility on port allocation. Full support for multiple daisy chained chassis all controlled from a single GUI.
- Low cost of ownership and ease of use by avoiding multiple test systems and non integrated software applications.

diversifEye™ is a trademark of Shenick Network Systems. All other trademarks are the trademarks of their respective owners.

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, Dublin, Ireland

Tel: +353-1-236 7002

Fax: +353-1-236 7020

web: [www.shenick.com](http://www.shenick.com) email: [info@shenick.com](mailto:info@shenick.com)

© 2010, Shenick Network Systems Limited

(Shenick Version No. - v3.1)