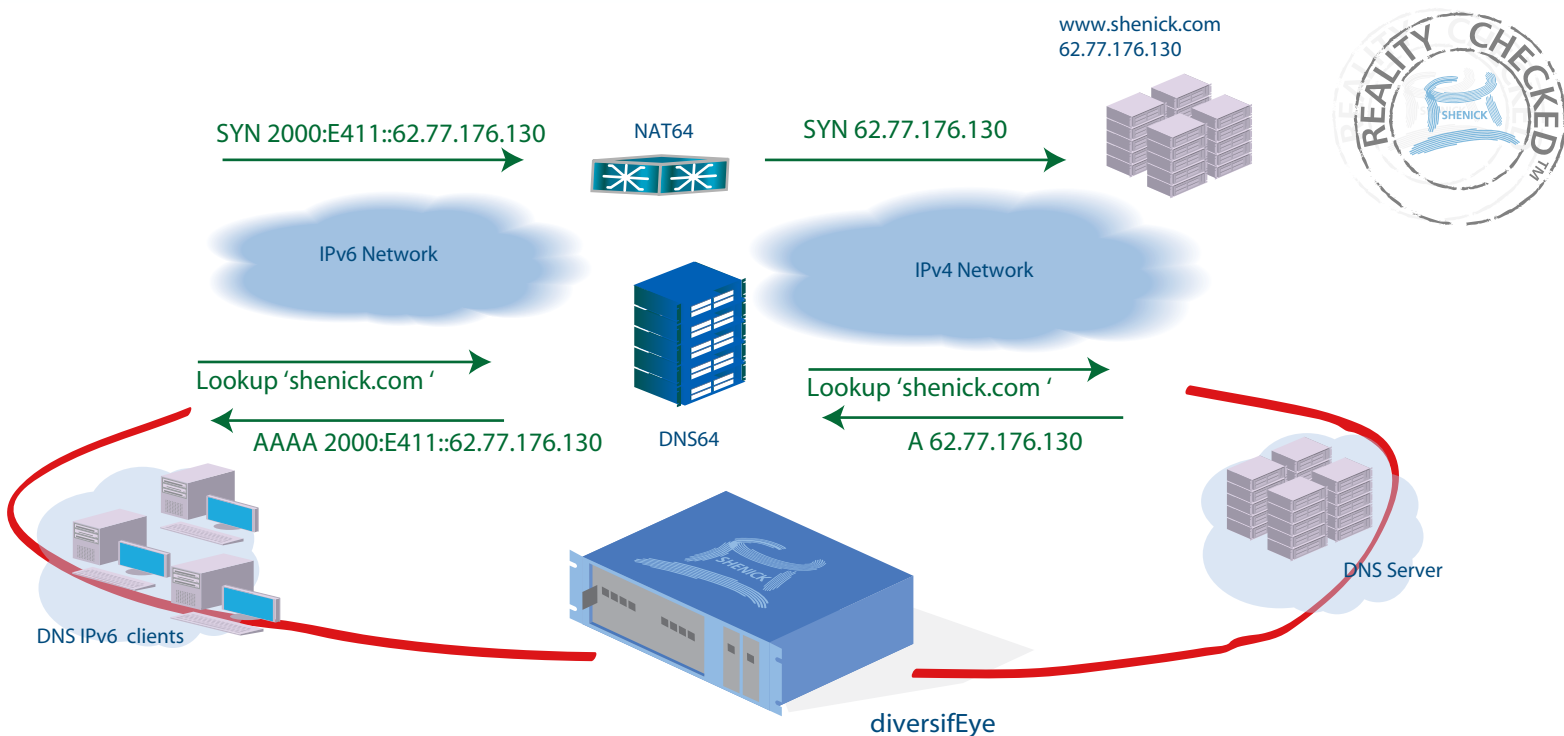




DNS testing with diversifEye

Domain Name Server (DNS) testing is available as part of diversifEye's standard test functionality. diversifEye provides valuable per flow Quality of Experience insight into DNS performance, which includes assessments on capacity.

An integrate part of diversifEye's DNS test functionality is to generate stateful application flows. diversifEye's DNS enabled applications are used to generate real requests e.g. (HTTP 'Get - shenick.com') which first result in a DNS server query. On receipt of a response from the DNS server, the DNS enabled application uses the IP address answer to continue the stateful request for the media.



Testing DNS64 / NAT64

diversifEye's DNS clients are used in testing IPv6 migration strategies. An evolving practice among Service Providers is to use DNS64 to facilitate lookups or queries of resources that are hosted on the IPv4 enabled network. DNS64 combined with NAT64 provides an alternative to tunnelling mechanisms such as Dual-Stack Lite.

In a NAT64/DNS64 environment diversifEye provides capacity and throughput performance measurements on the devices independent of each other or as a combined system.

diversifEye emulates both DNS clients and/or the DNS server with the V4 address table translations. Equally diversifEye's DNS clients may interact with 3rd party DNS servers.



diversifEye is used to generate a mix of legal and illegal traffic flows, this extends to the DNS client. diversifEye's emulated DNS clients can be configured with malformed requests which include Header, body or Labels.

In addition, diversifEye's emulated DNS clients can be used in a denial of service type attack by generating a large volume of requests without waiting for responses.

diversifEye™ is the only per flow test and measurement solution enabling thresholding and event notification, along with offering integrated network, application and security attack emulation and performance analysis for IP flows.

The diversifEye per flow architecture provides unrivaled control on a per flow basis for load testing. diversifEye's traffic profiling may include a mix of encrypted and non encrypted application flows.

The Shenick diversifEye supports per flow test, measurement and thresholding of :

Analysis Software Overview

- DHCPv4 & DHCPv6, PPPoE
- DNS
- VLAN & Double Tagging (Q-in-Q) with priority
- Concurrent IPv4 and IPv6 application flows
- IGMP V1, V2, V3, MLD V1, V2
- Voice and Video Quality Metrics
- Telepresence
- RTSP (Video on Demand)
- VoIP (SIP & RTP)
- HTTP
- HTTP adaptive streaming
- FTP
- SMTP / POP3
- P2P
- TWAMP
- Attack Traffic - Spam / Viruses / DDOS
- PCAP file replay (>1GB)
- IPsec / SSL / TLS / DTLS

Why use diversifEye to test network infrastructure performance

- **Real Voice and Data** diversifEye's media flows use real voice and data when emulating end points. Measure performance of video/voice quality, includes MOS scores.
- **Stateful Protocol Flows** Emulate stateful IP flows for unique end points and applications. By using stateful / real TCP flows it's possible to see how networks adjust or vary window sizes.
- **Quality of Experience** Ensure in real-time, on a per flow basis that network QoS settings have no impact on application quality, especially under varying QoS settings.
- **Security Attack Mitigation** Test and measure performance under extreme conditions. Networks must continue to serve while unwanted traffic such as spam or even DDoS attacks are happening.

diversifEye Summary Features and Benefits

- Per flow testing with thresholding and event notification.
- 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, Adaptive Streaming), 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 TWAMP, IPv4, IPv6 and /or 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.

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 email: info@shenick.com

© 2011, Shenick Network Systems Limited

(Shenick Version No. - v1.0)