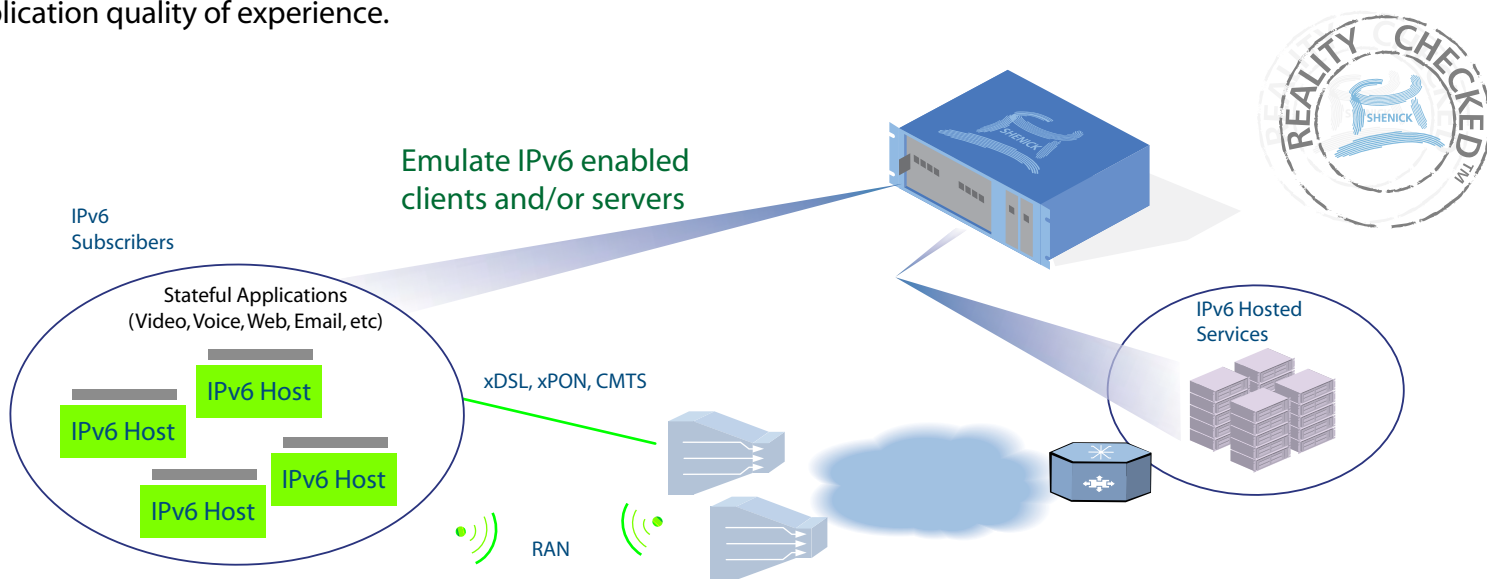




Testing IPv6 with diversifEye™

With the rapid expiration of IPv4 addresses, IPv6 is now a reality. Service Providers and Equipment Vendors are testing infrastructure and solutions to determine the readiness for complete IPv6 roll-outs. IP Networking applications have long since evolved beyond best-effort. Quality and performance are key elements driving the explosion of the internet, along with device and application reliability. IPv6 needs to deliver on the expected high levels of quality of experience.

It's imperative when deploying the new IPv6 address scheme that the deployment is tested to ensure minimum disruption, minimum application quality issues and to assist in overcoming legacy networking problems. An IPv6 end-to-end test strategy will test address assignment, connectivity, accessibility of online services and ultimately application quality of experience.



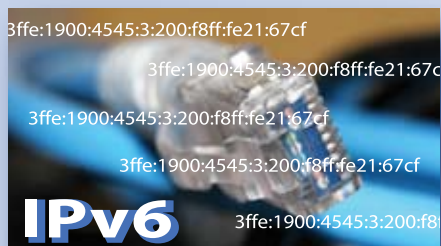
End-to-End IPv6 test strategy

An IPv6 end-to-end test strategy commences with basic IPv6 address assignment. Early stage IPv6 tests include the use of dynamic protocols such as DHCPv6. A follow on test is to assess the accessibility of various IPv6 servers i.e. Can the IPv6 enabled host connect to the secure VPN server. These tests will include performance measurements of IPv6 DNS servers and AAAA entry lookup.

In implementing an end-to-end test strategy, consideration is given to application quality over a number of ports e.g. DNS - 53, HTTP - 80, HTTPS - 443, POP3 - 110, SIP - 5060, etc. Once the fundamental tests are implemented, it's possible to benchmark IPv6 performance against IPv4 enabled application performance. In addition testing should provide insight into mixed environments of IPv6 and IPv4 addresses.

Once a reliable level of performance is defined, further IPv6 infrastructure testing includes varying MTU and fragmentation sizes. Ensuring all the time no impact to application quality. Testing includes a number of fragmentation management options, including measuring fixed size fragmentation over fragmentation based on packet size thresholds.

Application quality is a significant aspect of the overall IPv6 end-to-end test strategy. As a final test, ensure the application quality on delay sensitive applications such as voice and video. In particular, video requires a unique approach for both cable DOCSIS 3.0 and IPTV MLDv1,2.



diversifEye emulates stateful, real-world IPv6 traffic flows which connect to internal or external 3rd party IPv6 enabled servers. diversifEye is an application performance measurement tool, designed specifically to test voice and video application quality. diversifEye is used extensively to benchmark both applications in IPv6 against IPv4 only networks. diversifEye enables emulation of both IPv6 and IPv4 enabled applications in a single test group.

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 IPv6 and/or IPv4 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

- DHCPv6 (support NS-DAD, IA_NA, IA_TA & IA_PD)
- PPPoE
- VLAN & Double Tagging (Q-in-Q) with priority
- Concurrent IPv4 and IPv6 application flows
- MTU - Jumbo frames, Fragmentation Management
- Voice and Video Quality Metrics
- RTSP (Video on Demand)
- SSL, IPSec (IKEv1,v2), TLS, DTLS
- Telepresence (TIP)
- IPTV (MLDv1, 2)
- VoIP (SIP & RTP)
- HTTP (incl. post attachments)
- FTP (passive & active)
- SMTP,POP3 (incl. attachments)
- P2P
- TWAMP
- Attack Traffic - Spam / Viruses / DDOS
- PCAP file replay (>1GB)

Why use diversifEye to test IPv6 deployments?

- **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) over IPv6 enabled flows.
- **Stateful Protocol Flows** Emulate stateful IPv6 flows for unique end points and applications. By using stateful/real TCP flows it's possible to assess individual network node handling performance.
- **Quality of Experience** Ensure in real-time, on a per flow basis that the IPv6 infrastructure QoS settings have no impact on application quality, especially under varying QoS settings.
- **Security Attack Mitigation** It is equally important to measure performance under extreme conditions. The IPv6 network must continue to serve while unwanted traffic such as spam or even DDoS attacks are happening.

diversifEye 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 Telepresence (TIP), Data Applications (HTTP, FTP, POP/SMTP, P2P), IPTV (IGMP/MLD), VoD (RTSP), VoIP (SIP/RTP) all in a single test package.
- TCP Replay Substitution automatically varies payloads so no two PCAP sessions are the same.
- Support for latest security VPNs - SSL, TLS, DTLS, IPSEC(IKEv1 and IKEv2)
- DHCPv4,v6 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, Corrigan Avenue, Dun Laoghaire, Dublin, Ireland

Tel: +353-1-236 7002

Fax: +353-1-236 7020