



**diversifEye™**  
**Field Application Notes**

End-to-End IPTV  
Test Strategy

**Shenick Network Systems**



**diversifEye™**

Per flow Converged IP Network Test Systems



## Content

CONTENT.....	2
INTRODUCTION.....	3
SUMMARY TESTING REQUIREMENTS AND METHODOLOGY.....	4
SAMPLE IPTV TEST LAYOUT .....	7
TEST METHODOLOGY .....	9
1. <i>Handle and pass IGMP / MLD control messages and traffic.</i> .....	9
2. <i>Default EPG and Channel zap functionality</i> .....	10
3. <i>Automated Address Allocation</i> .....	11
4. <i>Content Per flow analysis, CPE &amp; Access Scalability performance</i> .....	11
5. <i>AAA Handling and security validation</i> .....	12
6. <i>Measure Key Performance Metrics on a per flow basis</i> .....	12
7. <i>Measure the effects of dynamic CPE behavior on Billing systems</i> .....	13
8. <i>Run Application Tests against Live (External) Equipment</i> .....	14
9. <i>Build Usage with real Behavior, test with real world scenarios</i> .....	15
10. <i>Roadmap testing for future requirements</i> .....	17

## Introduction

This document supports an open test strategy for IPTV networks. The basic IPTV delivery network consists of the 3 main elements – Head End (content ingest), Network (delivery path) and Subscriber Premise (CPE). A complete test strategy must incorporate an end-to-end approach for performance measurements.

In IPTV, the typical device behind a CPE is a set-top box with or without PVR functionality. These devices may use IPv4 and/or IPv6 addressing, and can utilize a wide variety of Ethernet based Layer 3-7 protocols (examples: UDP, TCP, IGMP/MLD, RTSP, HTTP, FTP, SIP, etc).

To conduct effective testing of the IPTV environment, the test setup must replicate, as close as possible, the real world deployment environment. In everyday life multiple individual devices sit behind the CPE all vying for bandwidth, running a multitude of application types. Therefore, it's essential to include other traffic types in the test strategy.

This document provides a methodology designed to test IPTV environments with a key focus on the individual end user experience which includes the device registration process, content request flows and finally the quality of the delivered content.

After establishing a benchmark performance or QoE results on a per flow basis for the IPTV network, the next step is to create client activity with various applications to include real world scenarios that include voice and application data services.

As the network is IP based, it's essential to round up testing by considering various security attack mitigation tests. The test structure has provisions for both regular (HTTP, IGMP, POP3, SMTP etc) application flows and disruptive flows (P2P, DDOS, spam, viruses). All the traffic types Good, Bad, Illegal are run from within the same test GUI for synchronization of cause and effect.

## Summary Testing Requirements and Methodology

The table below is a sample outline of the various nodes and a list of tests to be considered as part of the open test strategy -

	Test Requirement	CPE	Access	Aggregation	Edge	Core	Head End
NETWORK	Content Availability	✓	✓	✓	✓	✓	✓
	Channel Change / Trick Play		✓	✓			
	Latency / Jitter	✓					
MANAGEMENT	CPE Access (Address Allocation)		✓				
	EPG Availability		✓				
	Authentication and Billing			✓			
	Security /Policy Management				✓		
PERFORMANCE	Content Quality	✓	✓	✓	✓	✓	✓
	Service QoS Provisioning	✓					
	Channel Change Efficacy	✓					
SCALABILITY	Content Ingest						✓
	Max STBs per CPE	✓					
	Max CPE per ACCESS Node		✓				
LIVE HEADEND PERFORMANCE	External - Content Quality	✓					✓
	Content Performance	✓					
USER SCENARIO	Active traffic injection incl. (VoD, VoIP, web, email, P2P, etc)	✓	✓	✓			
ROADMAP TEST	IPv4 and IPv6 enabled devices		✓		✓		
	SIP enabled content				✓		

1. Test the network node's ability to pass IGMP / MLD traffic. Configure diversifEye to act as both the client and server for the IGMP / MLD flows.
2. Configure an end point behind the CPE, determine if the end point can access and receive an IP address automatically using DHCPv4 and/or DHCPv6.
3. Service initialization from EPG request to default channel zap. As part of the end point application side emulation and setup, the boot process functionality is simulated on a single and then multiple emulated end points. Essential to performance test power on to receipt of first I-frame or viewable images.

Step	Request	Protocol
0	MAC Address	Uniquely Assigned
1	IP Address	DHCPv4 or DHCPv6
2	EPG Download	HTTP, FTP
3	Channel Zap	IGMP / MLD

4. Analyze content quality on a per CPE / per end point / per channel basis. Commence with scale testing - emulate a single end point (STB) measure performance, then emulate multiple unique individual end points (e.g. 4 STBs per home) with different activities behind each CPE. Connect to multiple unique content sources to measure content quality.
  - Run true, stateful TCP based IGMP/MLD flows with content. Access real content in order to emulate realistic, per end point activity and IPTV traffic flows.
5. Run tests using appropriate DHCP CPE session establishment with all necessary options enabled, on a per CPE per end point basis to external DHCP servers. Measure overall and individual end point performance within each DHCP session and compare to static method.
  - This provides a unique MAC and IP address per client. The flexible MAC address configuration and unique options assignment is key for validating security in many environments.
6. Measure key performance metrics (Quality of Experience) on a per end point basis – time to download EPG files, IGMP and/or MLD join/leave latencies, RTP jitter and loss, MOS etc.
  - For an individual STB and CPE
  - Observe the effect of an emulated STB activities on another emulated STB behind the same CPE
  - Examine Access/Aggregation performance for multiple STBs and CPEs
7. Measure the effects of dynamic CPE behavior on billing systems.
  - Examine the authentication and billing system to correctly identify STB properties and set policies accordingly in terms of content access.
  - Emulate surges in usage and typical real-world behaviour mechanisms by bringing online individual CPEs or batches of CPEs, either automated or in real time, without stopping the test - Stress test Access, Authentication and Authorization services ability to deliver individual services to each CPE and STB.
8. Examine performance of external multicast servers. This demonstrates real world performance and prepares all individual elements for production deployments. Test and verify appropriate QoS mechanisms to use at L2 and/or L3/4 to classify traffic into each service category.
  - Shenick diversifEye's flexible architecture makes possible the assigning of VLAN priority (on single and tunneled QinQ) on virtual end points and DiffServ/TOS classification on each individual application/service assigned to the end point.

9. Create statistical profiles to match real world use of multicast and data services and apply on a per end point per application basis. Test with secure media TLS/SSL, add other traffic flows (HTTP, SMTP/POP3 and FTP). Include disruptive flows (P2P, DDOS, IGMP floods, spam, and viruses) within the existing test scenarios to verify any security and mitigation functions that may be available. Examine statistics for synchronization of cause and effect on previously gathered performance metrics.
10. Roadmap test future features such as IPv6 or SIP enabled content sessions. Create a mix of emulated end points (STBs) enabled for IPv4 and IPv6 services, determine performance on each of the requested video flows. Test possible IMS functionality, through SIP enabled content sessions.

# Sample IPTV Test Layout

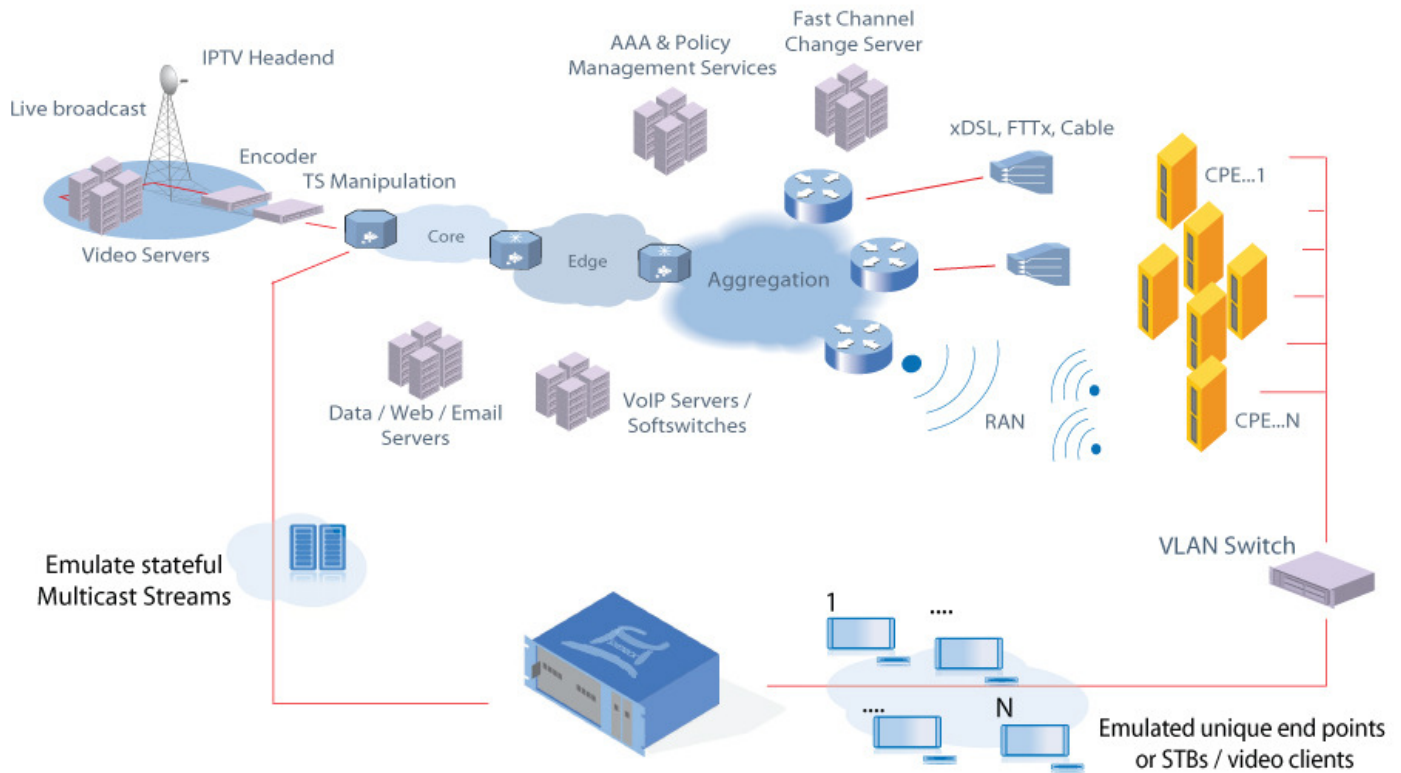


Figure 1 – Typical diversifEye IPTV test environment

The diagram above illustrates a sample network model which replicates, as close as possible, a production deployment. diversifEye is used to emulate both end points and server side multicast streams, this feature is necessary to accurately test and analyse the behaviour and performance of each of the elements in the IPTV network. Once the devices are benchmarked it's possible to test in an integrated environment against live services.

To provide complete end to end performance visibility, a modem pool or rack containing banks of modems is utilized (essential in latency and jitter measurements). The modem banks are connected to the test equipment via a single or multiple aggregation switches. These switches allow the tester to connect using a trunk port (typically Gigabit Ethernet) and provide individual VLANs for each end point's subscriber activity. The VLAN also shares an untagged VLAN port (Typically 10/100 Ethernet) on the switch which in turn connects to each CPE Ethernet port on the modem.

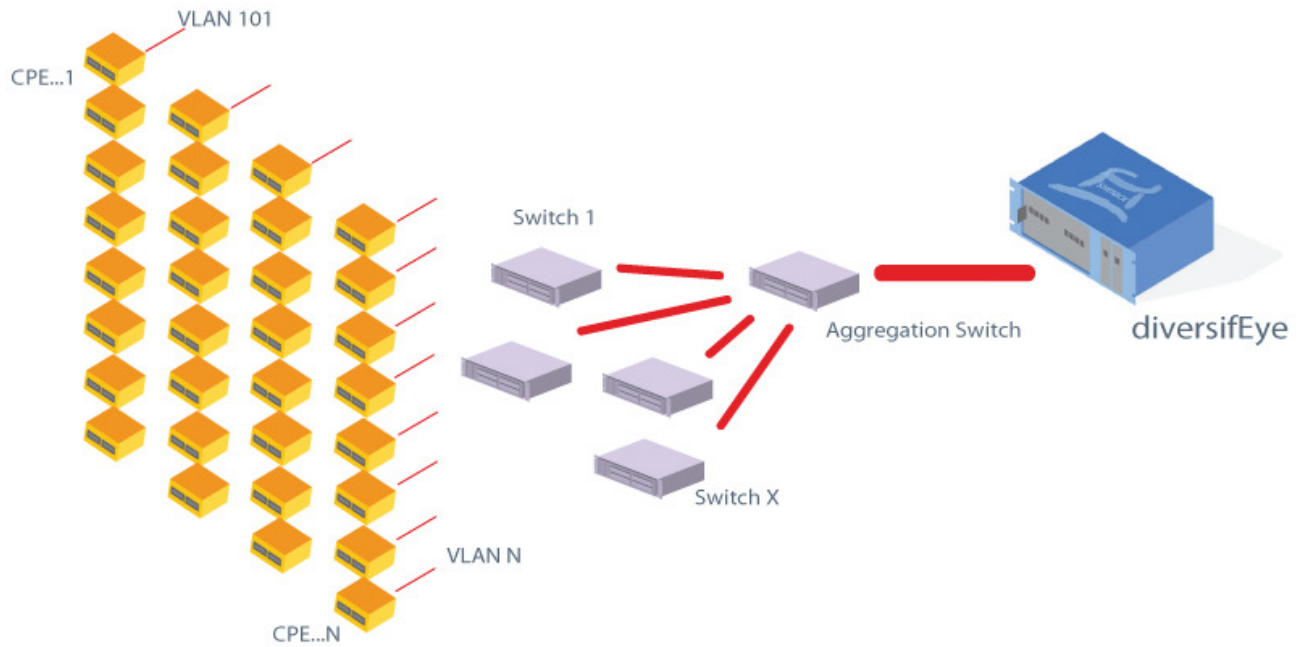


Figure 2 – diversifEye VLAN Aggregation Modem Rack Setup

Using an aggregation model, diversifEye can create one virtual host per modem port representing an Ethernet switch residential gateway connection, the host VLAN ID matching the switch trunk port VLAN for each modem. Multiple services can be configured on each virtual host to deliver and receive real subscriber based traffic.

With this method DiffServ/TOS can be used to classify the service. A typical classification list is shown in the table in figure 3 below, the 8 bit binary scheme and subsequent decimal value used covers DiffServ Code Point (DSCP - 6 bits) and Explicit Congestion Notification (ECN - 2 bits).

Alternatively, diversifEye can generate multiple virtual hosts per CPE port, allowing the use of VLAN priority per service, if required, which has the effect of multiple visible devices behind a CPE, requesting services or different service categories. The use of double tagging, (802.1QinQ) allows the devices to communicate across the aggregation environment for the cable modem pool maintaining priorities for the services inside the tunneled VLAN.

Service	DSCP	Binary (8 bit)	Decimal
Interactive Voice	EF	10111000	184
Voice Signalling	CS5	10100000	160
Business Critical	AF31	01101000	104
OAM&P	CS2	01000000	64
Bulk Data	AF1	00101000	40
Best Effort	DF	00000000	00

# Test Methodology

## 1. Handle and pass IGMP / MLD control messages and traffic.

The focus of this opening test is to validate the basic IGMP / MLD messaging and control features along with any provisioning needed to establish IPTV services. The following tests should be considered:

1. IGMP / MLD port initialization and Query forwarding
2. IGMP / MLD group join / leave actions
3. IGMP / MLD Membership report processing and forwarding
4. IGMP / MLD Leave Group report processing and forwarding
5. IGMP / MLD multicast membership timeouts
6. Simultaneous join / leave operations on a single end point
7. IGMP / MLD unrecognized / unsupported message processing and forwarding
8. IGMP / MLD membership proxy report processing and forwarding
9. non IGMP / MLD multicast traffic on IGMP reserved networks
10. IGMP / MLD packet error processing
11. IGMP / MLD Provisioning

The test cases under this section will verify capabilities of the IGM / MLD membership reports, leaves, and queries based on the above detailed behavior on the configuration. At this stage its worth considering the inclusion of multiple STBs behind the CPE, there should be a minimum of 2 STBs with 4-6 STBs as the preferred test.

When the IGMP / MLD messaging functionality is verified the focus now is on multicast frame replication and filtering. IGMP / MLD multicast settings will be tested in a mix with regular multicast data against various multicast provisioning options. Testing will validate that other multicast settings do not affect IPTV operations. The following types of tests should be conducted:

1. Multicast Provisioning
2. IPTV traffic in regular multicast environments

Once the IGMP/MLD functionality is proven, it's essential to establish a benchmark for QoS standards for all topologies. Once basic QoS standards are verified they will be applied to more complex topologies and configurations to determine if any of the network elements basic QoS settings degrades content performance or becomes ineffective. The following performance measurements are utilized in the benchmarking:

1. Latency and jitter Analysis
2. Bit error and packet loss

Test	Join Time	Leave Time	Packets in after Leave	Jitter Buffer Overrun	Jitter Buffer Underrun	Latency
Single Modem	ms	ms				
Modem Pool	ms	ms				

## 2. Default EPG and Channel zap functionality

Due to the dynamic nature of real TCP traffic, its best practice to perform a loopback reference test to determine the sum total of the application load achievable in terms of throughput and latency across an individual modem and further across access nodes.

It is advised to run the test across one Modem initially to verify connectivity and traffic flows. Also use Static addressing for the CPE. This means the test is not engaging the service layer for address assignment which may also introduce initial overhead. This may be quantified in the next step with a full system test using the service layer external DHCP/PPPoE server.

Test	TCP Timing SYN DATA	Mean Time to transfer file	Mean Join Time	Time to first I-frame
EPG	ms	ms	_____	_____
Default Channel Zap	_____	_____	ms	ms

### 3. Automated Address Allocation

It is worth testing and comparing the results to the static tests in step 2 above. This may provide valuable information pre-deployment on whether the DHCP/PPPoE server itself proves to be a bottleneck for service delivery.

(It may be found that a full modem rack using static addressing is passing traffic in a matter of seconds but when assigning addresses externally via DHCP/PPPoE servers, the service requests may fail and have to try to re-negotiate.)

The bottleneck may occur at processing on the DHCP/PPPoE server or congestion on the link in between. This is valuable information to development teams as well as systems engineering when dimensioning for production deployment.

### 4. Content Per flow analysis, CPE & Access Scalability performance

Analyze content quality on a per end point per channel basis, using the individual end points behind each CPE connect to multiple unique content sources.

This simple test will verify the bandwidth capabilities of the CPE, in addition the test will show up the performance of the aggregation nodes ability to deal with separate unique multicast address requests.

Examine the incoming content quality, verify MOS scores greater than a given threshold i.e. 4.5 for video in multimedia content.

Test	CPE...1	CPE...	CPE...	CPE...N
Bandwidth	Mbps	Mbps	Mbps	Mbps

Test	Channel ID...1	Channel ID...-	Channel ID...-	Channel ID..N
Time to first I-frame	ms	ms	ms	ms
Number of I-frames				
Video/Audio MoS				

## 5. AAA Handling and security validation

Performance test Access, Authentication and Authorization configurations. Test the timing performance for previously unregistered end points i.e. connecting to the network for the first time. Examine the timing performance for previously registered end points i.e. appearing online after a power-off period.

Using unique MAC addresses establish if the emulated end points can gain access to the network and furthermore access the correct content paths. Dynamically bring hosts in/out of service during live testing, similar to subscriber day time activity or else set all out of service depicting power failures.

Test for false positives / false negatives, the correct identification of the MAC address and configuration but incorrect handling and management, in addition test for false negatives in which an unregistered MAC address attempts access to the network.

## 6. Measure Key Performance Metrics on a per flow basis

The previous tests quantified network functionality and bandwidth requirements. However, diversifEye's key strength is the per application, per flow analysis. This fundamental principal enables investigation of metrics for Quality of Experience measurements i.e. statistics for IPTV flows and applications running on the emulated STBs as part of the service delivery.

Measure key performance metrics (Quality of Experience) -

- For an individual STB and CPE
- Observe the effect of an one emulated STB activities on another emulated STB behind the same CPE
- Examine Access/Aggregation performance for multiple STBs and CPE flows

Performance measurements should include a mix of activity performance and the received/incoming content quality:-

- Time to access network
- Time to download EPG
- TCP Connections per second
- Multicast Join Latency – Max, Min, Mean (IP Video or group communication environments – gaming)
- Multicast Leave Latency – Max, Min, Mean (IP Video or group communication environments – gaming)
- Multicast Joins initiated/completed, Multicast leaves initiated/completed

- Time to first I-frame
- Bits in after leave initiated
- Video MOS (Streaming video - multicast and unicast)
- Audio MOS (Streaming audio - multicast and unicast)

## **7. Measure the effects of dynamic CPE behavior on Billing systems**

It's important to facilitate testing of access, authentication and authorization systems especially where premium content is available. Including these tests ensures the correct information is gathered as part of the billing system. For integration purposes it's important to benchmark performance of a single CPE and emulated STB and then compare the resultant metrics to a wider basis (multiple CPEs to full racks worth of CPE traffic flows). This will ascertain the capabilities of the AAA management and billing system together to deliver services to a subscriber and the capability of the management system to deliver services to all customers. Furthermore this tests reliability and how well services are delivered i.e. effectiveness and efficacy of the subscriber databases.

The goal is to emulate, as closely as possible real-world usage. This means that all the emulated STBs may not be online at the same time, or users may be viewing different channels, or even channel zapping. In diversifEye, CPEs may be set in and out of service, or delays set to effectively replicate the tea time rush.

NOTE: In the real world people do not mass join and request the same services at the same time. This is not typical real world behavior. It may represent a valid scenario for user behaviour in a power outage and restoration. Different busy hour scenarios and traffic usage profiles should be documented and tested.

Sample scenarios include tea time surges, after tea premium content requests.

- Examine the authentication and billing system to correctly identify STB properties and set policies accordingly in terms of content access.
- Emulate surges in usage and typical real-world behavior mechanisms by bringing online individual CPEs or batches of CPEs, either automated or in real time, without stopping the test - Stress test Access, Authentication and Authorization services ability to deliver individual services to each CPE and STB.

Examine content quality on each of the individual emulated end points in terms of video and audio MoS performance.

Test databases for false positive / false negatives –

- Correctly identifying STB and unique identifiers such as MAC addressing, port address, etc but refusing access to premium content
- Incorrectly identifying STB and unique identifiers such as MAC addressing, port address but allowing access to premium content access.

These varying usage scenarios document access functionality, and more importantly the verification that the correct information is collected as part of a billing system. The tests also provide visibility on QoS implementations and the ability to deliver services can be quantified and guaranteed.

## **8. Run Application Tests against Live (External) Equipment**

Up to this point diversifEye has been used mostly in 'closed loop' or full end-to-end testing. This means diversifEye has been emulating the STB traffic and the server side multicast video services.

The same subscriber side testbed can now be switched to connect to the real head end and EPG sharing services to evaluate and measure how the system performs in a less controlled, real world environment. This can be termed 'open loop' where diversifEye is providing only the end point side load, the server is provided either by a testbed 'model' of the production network or via controlled connection to the production network This provides visibility of how the system will perform for users post deployment.

The use of specific QoS profiles at the Layer 2 or higher can be implemented and tested to verify that correctly classified multicast traffic is delivered over lower priority traffic particularly under congestion. This can be achieved at the emulated STB host level using VLAN tagging and priorities matched to each traffic type, or at the application level where a TOS/DiffServ Code Point can be assigned as a traffic classifier to distinguish traffic to different priorities.

## 9. Build Usage with real Behavior, test with real world scenarios

After testing dynamic behaviour by bringing STB traffic in and out of service, in the steps above, the behaviour is deployed across a test group enabling individual properties for each host and/or STB activity such as channel zapping tables, channel zap rate, period of time spent viewing a channel before automatically channel zapping.

Each individual STB is made to exhibit unique behaviour, or is grouped into similar users, with similar behaviour. For example on a typical Access node servicing a rack of modems - 60% of the modems could be requesting the same channel, whereas 1-2% maybe viewing a channel with specific content.

Whereas 10-15% maybe channel hopping, with a further 5-6% may only be coming online. All of this type of behaviour and activity can be predefined on a per end point host and on a per multicast application level within diversifEye's per flow architecture.

### Add other Traffic Patterns to measure impact on content quality

In the real world, subscribers will utilize multiple applications, generate unique activity requests and TCP flows. The IPTV multicast flows are not the only traffic type traversing the network, therefore tests should be generated in which other traffic types are present. At a minimum these extra traffic flows require bandwidth and it's important to note that these traffic flows may also be paid subscription enabled services.

- Emulate other subscriber traffic flows and determine the impact on performance of the incoming streaming multicast content.
- Examine the impact of IPTV enabled QoS services on other traffic types.

It's important to consider test functionality for secure media flows, handling TLS / SSL enabled flows versus the plain unsecure IP flows. Test secure and unsecure flows alongside each other. Using the above test scenarios consider the impact on content quality.

Include a number of applications and activity and model the appropriate network traffic. In addition, utilize the per flow testing and measurement functionality to determine how the network's biased IPTV QoS settings impact each of the following individual applications or combinations of these applications on the network:

- RTSP
- VoIP
- Dual Stack VoIP
- RTP
- HTTP
- P2P
- Latency
- TCP Replay
- SMTP
- POP3
- DDOS
- FTP
- TWAMP

## Test Security and Mitigation Features by adding disruptive traffic flows

A number of attack mitigation scenarios are available and may easily be added to test scenarios; these may include DDOS Attacks (sending SYN floods, RESET floods etc) against specific key servers, in addition it's possible to test the impact on service availability and quality of the delivered content when VIRUS mails are circulating the network.

When examining for vulnerabilities, it's essential to include multiple attack options:

1. SYN Flood - floods a specific IP Address with SYN packets.
2. RESET Flood -floods a specific IP Address with RESET packets.
3. UDP Flood - floods a specific IP Address with UDP datagrams.
4. Ping Flood - floods a specific IP Address with ICMP echo request (ping) packets.
5. ARP Flood - floods the subnet with requests for a specific IP Address.
6. Ping of Death - sends ICMP echo requests to the specified IP Address.
7. Teardrop Attack - sends a UDP datagram in 2 IP fragments to the specified IP Address.
8. Reflective SYN Flood - sends a flood of SYN packets (i.e. TCP connection requests).
9. UDP Fragmentation Attack - sends a single IP fragment that contains part of a UDP datagram to the specified IP Address.

Other important emerging attack scenarios include the exploitation of IGMP such as Membership report blasts for multicasting/group communications to exhaust resources.

## 10. Roadmap testing for future requirements

Future proof networks by testing IPv6 migration scenarios. Emulate a mix of STBs enabled for IPv4 and IPv6 addressing, determine performance in terms of

1. Address allocation timing performance.
2. Requested video flows.
3. Security Vulnerabilities.

Testing can be performed in each mode, comparing the throughput and quality of experience metrics for the mixed applications, taking into account the principles used above for comparing results:

### Single Modem

- IPv4 Only – Mixed Application tests
- IPv6 Only – Mixed Application tests
- Dual Stack (Mix of Ipv4 and IPv6) – Mixed Application tests

### Multiple Modems

- IPv4 Only – Mixed Application tests
- IPv6 Only – Mixed Application tests
- Dual Stack (Mix of Ipv4 and IPv6) – Mixed Application tests

### Modem Rack

- IPv4 Only – Mixed Application tests
- IPv6 Only – Mixed Application tests
- Dual Stack (Mix of Ipv4 and IPv6) – Mixed Application tests

### Further roadmap tests

Consider testing access functionality using the SIP protocol. As an example SIP enabled RTSP sessions could be one of the application flows on the network.

The functionality is defined in the ETSI IMS standard ETSI TS 183 063 v2.0.2. This describes the use of SIP to negotiate a series of user operations for on demand content. SIP is used to negotiate the RTSP control and media flows with the IMS core servers and using RTSP to initiate the download of the requested stream from the server.

The IMS servers are responsible for allocating bandwidth and opening TCP/UDP ports to allow sessions to operate successfully.

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 a service assurance solution, born out of award winning and industry proven IPTV quality assessment technology that provides a completely integrated IPTV monitoring solution.

Shenick is the proud recipient of Internet Telephony's 2009 & 2008 IPTV Excellence awards and 2008 Product of the Year. Adding further 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](mailto:info@shenick.com)  
[sales@shenick.com](mailto:sales@shenick.com)

### Regional Support Email Contact Details -

Americas: [amer-support@shenick.com](mailto:amer-support@shenick.com)

Asia Pacific: [apac-support@shenick.com](mailto:apac-support@shenick.com)

Europe, Middle East & Africa: [emea-support@shenick.com](mailto: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.