diversifEye™ Field Application Notes

Testing DOCSIS® 3.0

Shenick Network Systems

Content

Glossary of Terms

CMTS	**Cable Modem Termination System**
CM	**Cable Modem**
HFC	**Hybrid Fibre Coaxial**
CPE	**Customer Premises Equipment**
DOCSIS	**Data over Cable Service Interface Specifications**
DHCP	**Dynamic Host Configuration Protocol**
MAC	**Media Access Control**
MDD	**MAC Domain Descriptor**
VLAN	**Virtual Local Area Network**
TOS	**Type of Service**
QoS	**Quality of Service**
DSCP	**DiffServ Code Point**
ECN	**Explicit Congestion Notification**
P2P	**Peer-to-Peer**
DDOS	**Distributed Denial of Service**
NS(DAD)	**Neighbour Solicitation (Duplicate Address Detection)**

Introduction

Cable Modems located at the customer premises are responsible for bridging packets from the CPE devices to the Cable Operators HFC (Hybrid Fiber/Coax System) plant. At the Cable Operators head-end the CMTS (Cable Modem Termination System) connects the back office and core network with the HFC network. The main function of the CMTS is to forward packets between these two domains, and between upstream and downstream channels on the HFC network.

Typical CPE devices are set-top boxes, personal computers and home routers. These devices may use IPv4, IPv6 addressing and can employ a wide variety of Ethernet based Layer 4-7 protocols (examples: UDP, TCP, HTTP, FTP, SIP, MPEG…..)

In order to conduct effective testing of the CMTS/Cable Modem environment, the test setup must replicate, as closely as possible, the real world deployment environment. In everyday life multiple individual CPE devices will run a multitude of application types behind each Cable Modem.

This document offers a methodology designed to test the CMTS environment as it moves towards DOCSIS3.0

Summary Testing Requirements and Methodology

1. Verify upstream and downstream bonding capabilities per DOCSIS 3.0 for TCP and UDP traffic

    - For one cable modem (performance of CPE)
    - For a cable modem rack (performance of CPE)

2. Establish a baseline reference for traffic generation and analysis by conducting loopback reference test – establishes best case scenario for traffic load in upstream and downstream direction for each protocol at the IP layer (IPv4 and IPv6) and the service layers above (HTTP, FTP, SMTP/POP3, IGMP etc.)

3. Test and measure, on a per client / per flow basis, with several unique individual voice, and multiple data clients running service applications operating behind each Cable Modem.

    - Run true, stateful TCP based application flows along with video and voice flows. Access real e-mail documents, URLs and attachments in order to emulate realistic, per client web traffic flows.

4. Run tests using appropriate DHCP CPE session establishment with all necessary options enabled, on a per household basis to external DHCP servers. Measure overall and individual client 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.

5. Measure key performance metrics (Quality of Experience) on a per client basis – time to download web pages, ftp file upload/download times, IGMP and/or MLD join/leave latencies, RTP jitter and loss, R-Factor and MOS etc.

    - For one cable modem (performance of CPE)
    - For a cable modem rack (performance of CPE)

6. Measure the effects of dynamic CPE behavior on the cable modems and on CMTS.

    - Observe the effect of one CPE/service application on another CPE/service application behind the same cable modem.
    - 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 tests CMTS ability to deliver individual services to each CPE and application.

7. Run individual voice, multicast and application data on emulated CPEs against external voice, multicast & application data 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 Host-Application architecture makes this possible - assigning VLAN priority (on single and tunneled QinQ) on virtual hosts and DiffServ/TOS classification on each individual application/service.

8. Create statistical profiles to match real world use of voice, multicast and data services and apply on a per client and per application basis.

9. Add 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. Create mix of IPv4 and IPv6 service application flows to verify full DOCSIS 3.0 capabilities.

CMTS Test Lab Layout

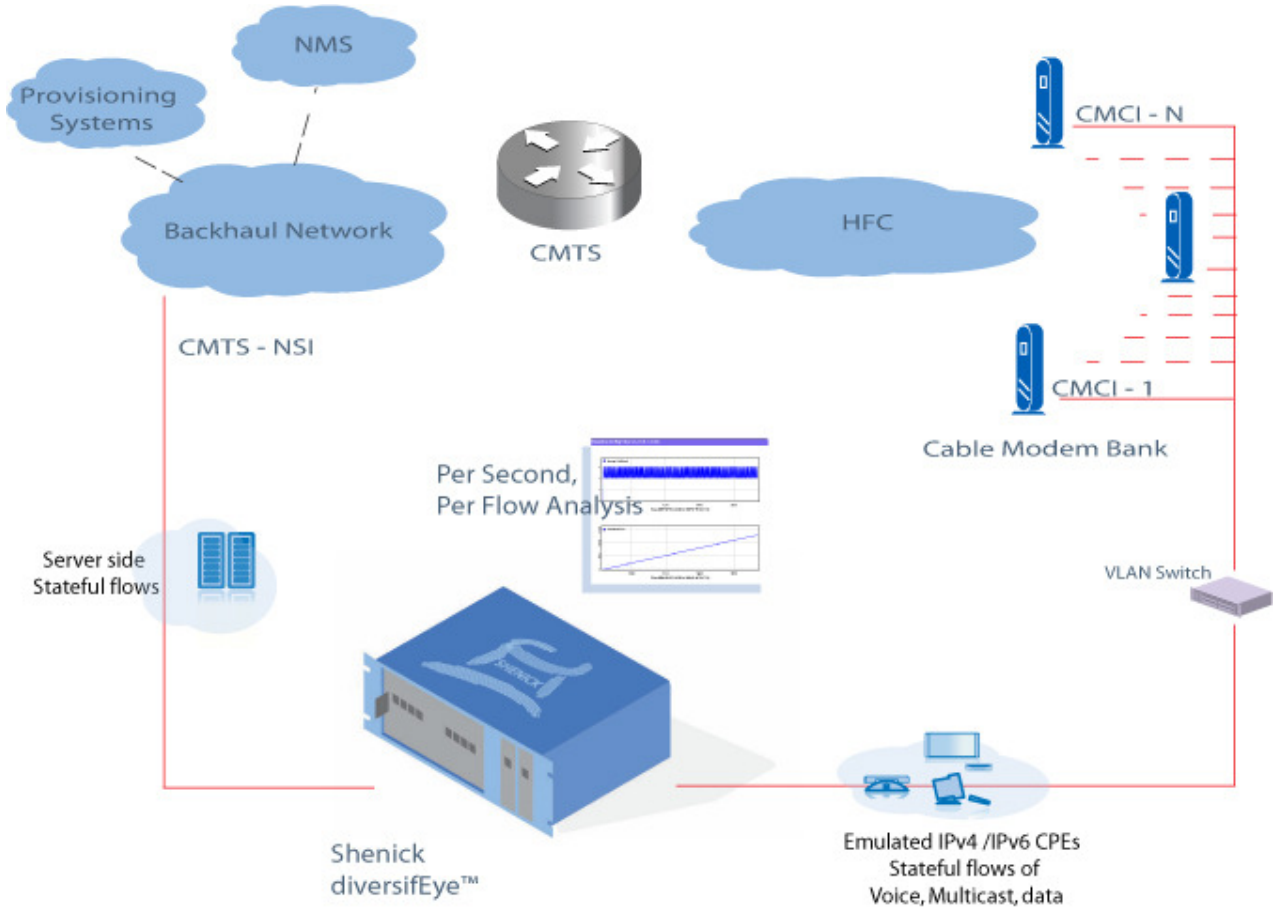

Figure 1 – Typical diversifEye CMTS Lab environment

The diagram above illustrates a typical lab model which replicates, as close as possible, a production deployment CMTS network. This model is necessary to accurately test and analyse the behaviour and performance of the elements in a CMTS environment and verify their ability to deliver real services during their production life cycle.

The CPE connectivity utilizes modem pools or Racks containing banks of cable modems which connect via the HFC network back to the CMTS. The Server side connectivity (CMTS-NSI) is accomplished typically via Gigabit Ethernet connection to an access or backhaul Ethernet switch residing on the network side of the CMTS environment. This usually requires IP connectivity over Ethernet but may also utilize 802.1 VLANs to segregate the traffic services and route/switch to appropriate core elements. On the CPE side the modem banks can be connected via the CMCI port (10/100/1000Mbps) to one or many aggregation switches. These switches allow the tester to connect to a trunk port (again typically Gigabit Ethernet) and provide an individual VLAN for each subscriber. 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 each cable modem.

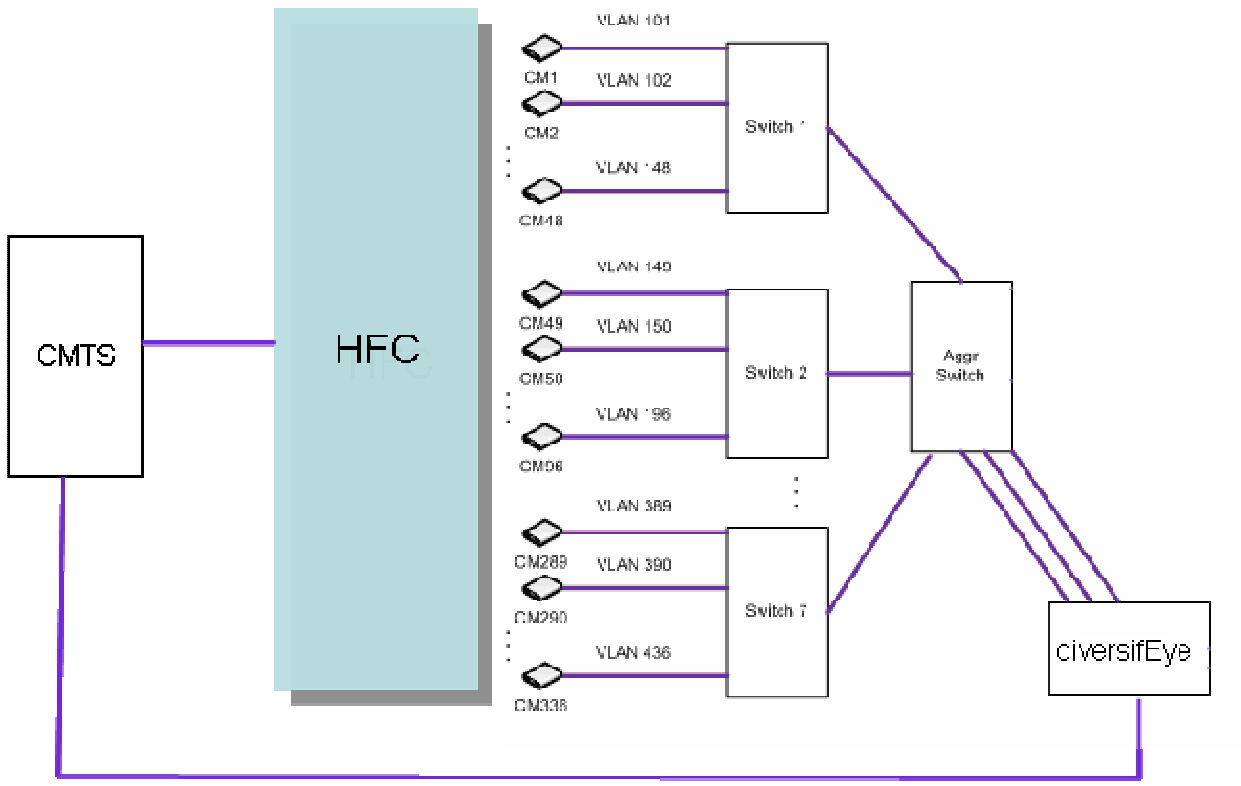

Figure 2 – diversifEye VLAN Aggregation Modem Rack Setup

Using an aggregation model, diversifEye can create one virtual host per cable modem CPE port representing an Ethernet switch residential gateway connection, the host VLAN ID matching the switch trunk port VLAN for each cable 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 each 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

Table 1 – Suggested DiffServ assignments for service traffic

Test Methodology

1. Upstream/Downstream Channel Bonding Test

Prior to running any application tests across the CMTS environment it is good practice to ensure that the cable modems and CMTS are capable of delivering the required bandwidths made available via channel bonding. The channel bonding can be described as the combination of several RF channels into one single virtual channel thus allowing greater speeds to be delivered via the modem.

Direction	Downstream	Downstream	Upstream
Channels	DOCSIS	EuroDOCSIS	Both
3.0 4 Channel	171.52 Mbps 152 Mbps	222.48 Mbps 200 Mbps	122.88 Mbps 108 Mbps
3.0 8 Channel	343.04 Mbps 304 Mbps	444.96 Mbps 400 Mbps	122.88 Mbps 108 Mbps

Table 2 – DOCSIS 3.0 Bandwidth table (top value represents theoretical value; bottom figure the maximum achievable bandwidth)

The diversifEye utilizes an application that allows the generation of unicast packets* in either/both directions across the CMTS and Cable modem. This allows for

**Payload size is configurable, typically a large packet size is used e.g. from MPEGTS size to full MTU: 1316-1460 is used to verify best possible speeds achieved. Variable packet/payload sizes are produced during application tests, as default behaviour and reflects real world data transfer patterns*

- Downstream channel bonding
- Upstream channel bonding
- Bi-directional channel bonding

Test	Downstream UDP	Upstream UDP	Bi-directional UDP	Downstream TCP	Upstream TCP	Bi-directional TCP
Single cable modem	Mbps	Mbps	Mbps	Mbps	Mbps	Mbps
Modem Pool	Mbps	Mbps	Mbps	Mbps	Mbps	Mbps

Figure 4 – Channel bonding results table

It is important to test the behaviour of Channel bonding using both stateless UDP and stateful TCP traffic. This will give an indication of how the CM / CMTS will behave when real two-way application traffic is passed.

Most data application traffic will be TCP based (HTTP, FTP, and SMTP/POP3 etc.) and will utilize variable packet rates flowing in both directions at the same time, with dynamic windowing and flow control. This may cause unexpected traffic patterns using the default configuration on the CM / CMTS but reflects genuine traffic that real CPE would generate/receive.

2. Application Reference test

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 the modem/CMTS environment.

With this golden reference it's now possible to test for degradation across the devices under test and the aggregation switch environment is also quantifiable.

By applying an appropriate load with single or multiple applications the required bandwidth in the upstream (FTP PUT, SMTP, HTTP POST VoIP call) and downstream (FTP GET, HTTP GET, Multicast/unicast stream receipt, VoIP call etc.) can be produced. The example below illustrates upstream and downstream load using a multiple application loopback reference test.

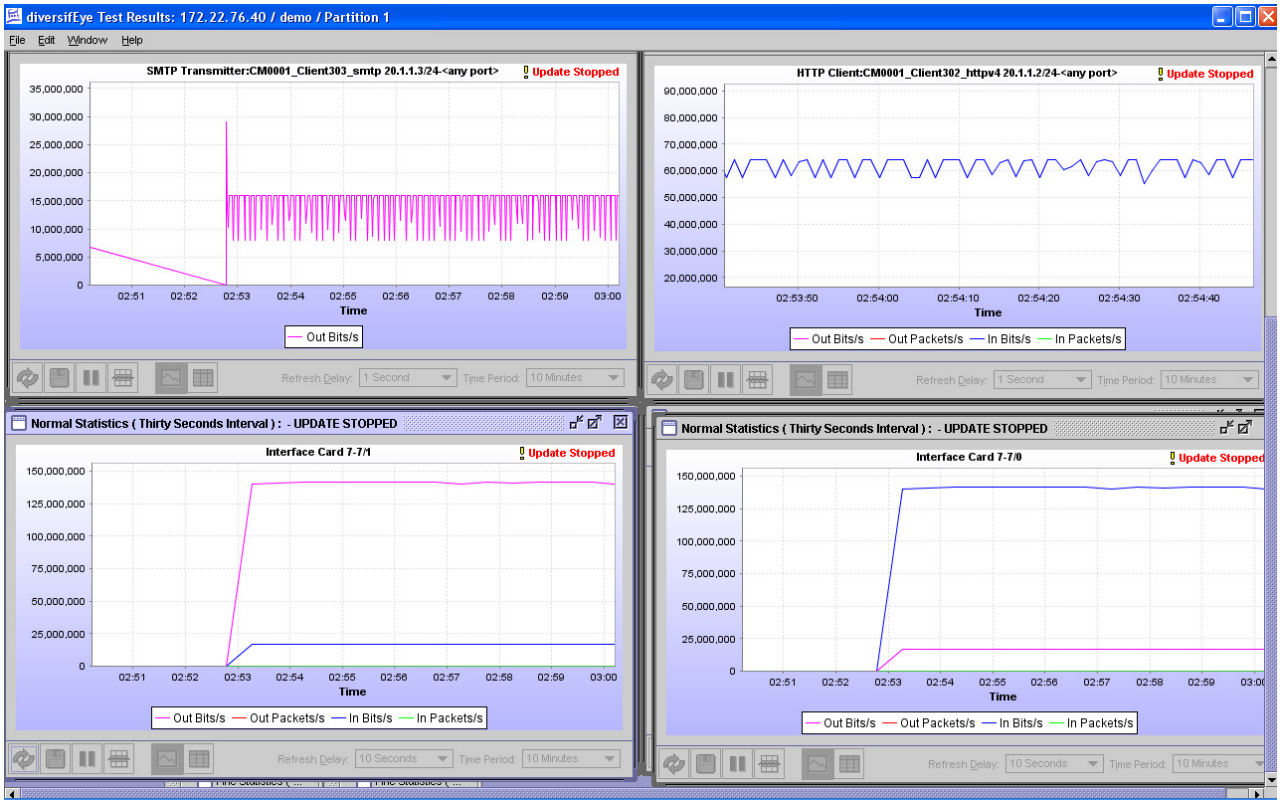

Figure 4 – Application loopback reference test results

The results above show baseline traffic loads for HTTP and SMTP as well as overall loads upstream and downstream on the physical ports.

150 Mbps Downstream and ~20Mbps upstream is representative of a load that can be easily attained by each DOCSIS 3.0 cable modem.

3. Application Testing across the CMTS Environment

A similar test run for loopback reference is now applied to the CMTS environment.

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 server via relay from the CMTS.

When traffic is flowing consistently, measure the bandwidth achieved in the upstream and downstream directions.

Test	Downstream Application1	Downstream Application2	Upstream Application1	Upstream Application2	Total Upstream	Total Downstream
Single cable modem	Mbps	Mbps	Mbps	Mbps	Mbps	Mbps
Modem Pool	Mbps	Mbps	Mbps	Mbps	Mbps	Mbps

Figure 5 – Application Bandwidth Table (Add Columns per application)

(The use of static addressing may not be possible depending on the CMTS and Cable Modem configuration and how it is set up to assign IP addresses for CPE devices.)

4. Application Test across CMTS 2 – DHCP Service Based

This test replicates the multi-application test group used above but brings in another important factor. The use of External DHCP Server to assign the IP address (and router, DNS info etc) used to deliver the service.

It is worth testing and comparing the results to the static tests in step 3 above. This may provide valuable information pre-deployment on whether the CMTS, CM or indeed the DHCP server itself proves to be a bottleneck for service delivery.

(It may be found that a full CM rack using static addressing is passing traffic in a matter of seconds but when assigning addresses externally via relay on the CMTS adds additional processing at the outset, enough for some service requests to fail and have to try to re-negotiate.)

The bottleneck may occur on the CMTS, processing on the DHCP 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.

5. Measure Key Performance Metrics of Applications

The previous tests covered throughput and latency where applicable. 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 applications running on the emulated CPEs as part of the service delivery.

These may include: -

- HTTP Time to Download Web Page
- TCP Connections per second (HTTP, FTP, SMTP, POP3 etc.)
- FTP File/Bytes Downloaded/Uploaded
- SMTP Mail Messages 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)
- Video MOS (Streaming video - multicast and unicast)
- Audio MOS (Streaming audio - multicast and unicast)
- SIP/RTP time to ringing (VoIP)
- SIP/RTP MOS, R-Factor (VoIP)
- P2P Complaint report

These metrics and many more are used in conjunction with the throughput figures to benchmark the CMTS environment, not only for the base delivery of traffic from A to B but for delivery of particular services from end-to-end.

6. Measure Key Performance Metrics with Dynamic Subscriber Behaviour

It's important to test individual application performance on a single CM and compare the resultant metrics to delivery on a wider basis (multiple CMs to full racks worth of CPE traffic flows). This will ascertain the capabilities of the CM to deliver services to a subscriber and the capability of the CMTS to deliver services to all customers. Furthermore this tests reliability and how well services are delivered i.e. without interruption from other subscribers on the same environment.

The goal is to emulate, as closely as possible real-world usage. This means all CPEs may not be online at the same time, or users may not be using the same applications at the same time either. 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 are should be documented and tested.

Sample scenarios include surges of new CPEs and CMs on a CMTS or support of a new application/service being brought online or added as a new feature (e.g. PacketCable VoIP service)

How will the new service or new subscriber load impact existing users/applications? Is quality of experience adversely affected?

These varying usage scenarios document visibility on where QoS implementations are required for classifying different traffic types so the application delivery is assured against lower priority traffic, in heavy usage periods. Thus ensuring another key feature of the CMTS environment is tested adequately and also proves confidence in the CMTS ability to deliver services can be quantified and guaranteed.

7. 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 not only emulating the CPE traffic, but has also emulated the server side traffic, providing Web, eMail, FTP, VoIP and video services using CMTS network side test ports.

The same subscriber side testbed can now be switched to connect to real (testbed) headend and internet 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 client 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 traffic is delivered over lower priority traffic particularly under congestion. This can be achieved at the emulated CPE 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. An example of some traffic classifications is shown in Figure 3 above.

8. Build Usage Profiles Based Upon User Behaviour

After testing dynamic behaviour by bringing CPE traffic in and out of service, in the steps above, the behaviour is deployed a cross a test group enabling individual properties for each host and/or application.

Each individual CM is made to exhibit unique behaviour, or is grouped into similar users, with similar behaviour. For example on a typical CMTS servicing a rack of modems - 20% of those modems could utilise P2P applications along with web browsing, sending/receiving mail, joining group communications sessions such as gaming or streaming, exhibiting heavy or power user behavior.

Whereas 50-60% may only just surf the web and download email for a part of the duration of the test run. All of this type of behaviour can be predefined in the host and application level properties of diversifEye.

9. Add Disruptive Traffic Patterns to Test Security and Mitigation Features

P2P has already been mentioned and its place as a disruptive traffic vs. broadband service enabler is widely debated. Other more specific attack mitigation scenarios are available to be added to test scenarios; these may include DDOS Attacks (sending SYN floods, RESET floods etc) in and out of the CM-CMTS environment or by the propagation of VIRUS mails.

Other important emerging attack scenarios include the exploitation of IGMP such as Membership report blasts for multicasting/group communications to exhaust resources. This testing will be specific to the environment under test and particular supported scenarios.

** This is not including the DHCP server, which is an external server but is a key element to the test environment providing service activation for the Cable Modems and CPE*

10. Create a Mix of IPv4 and IPv6 Traffic

This step is a crucial test for the testing of DOCSIS3.0 compliance and support within the CMTS environment. The CM is required to operate in an IPv4 only, IPv6 only, *Alternate Provisioning Mode (APM) and **Dual-Stack Provisioning Mode (DPM)

If the CM does not receive an MDD (MAC Domain Descriptor) message from the CMTS the CM will use IPv4 only, if an MDD is sent from the CMTS the CM uses the provisioning mode dictated in the MDD TLV fields. The provisioning modes use DHCPv4 and DHCPv6 to allocate the appropriate address to the CM and to CPE

***APM** - Attempts to assign an IPv6 address over DHCPv6 which allows for fallback to DHCPv4 and IPv4 mode if the v6 process fails.

****DPM** - Assigns an IPv6 address and an IPv4 address to the CM allowing full support for both v4 and v6 traffic across the CM and CMTS. This will, in turn allow the scenario where IPv4 CPE and IPv6 CPE can connect and utilise services via the CM across the CMTS environment.

The v6 address assignment is worth more detailed examination as a CPE has to apply the same principles to obtaining an address across the CMTS as does the Cable Modem. The following flow diagram outlines this requirement and shows the sequence of control packets required (taken from the CableLabs DOCSIS Specification): -

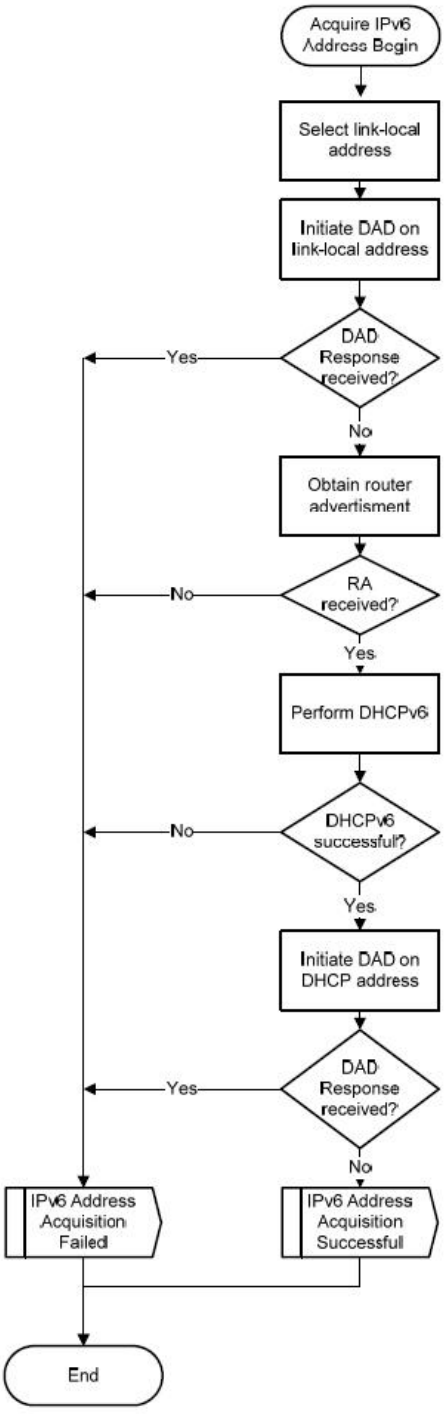

Figure 6 – DHCPv6 Address Flow Diagram

As the diagram shows the flow uses DHCP with the CMTS issuing DHCP Relays to the DHCPv6 server. The key aspect is the use of Duplicate Address Detect NS(DAD) packets for the link local and assigned (global) address. A more detailed flow can be seen below, showing a ladder diagram of the control packet sequence: -

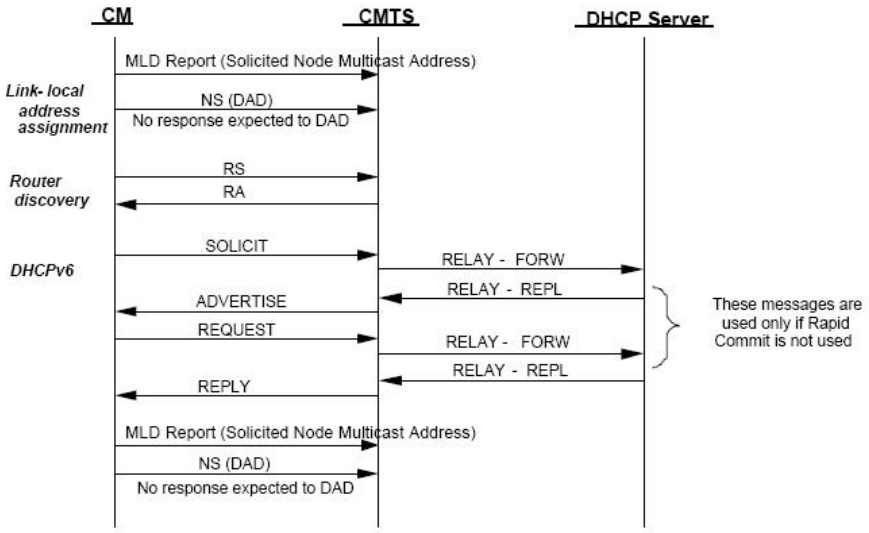

Figure 7 – DHCPv6 Address Assignment Ladder Diagram

Without these NS (DAD) messages the CMTS cannot update its neighbour cache and therefore cannot route packets on behalf of the CPE across the CMTS environment.

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 Cable Modem

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

Multiple Cable Modems

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

Cable Modem Rack

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

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 IPTV monitoring 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 2008 Product of the Year and IPTV Excellence awards. 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
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

Germany : Elsterweg 140, D-72793 Pfullingen, Germany
t : +49-7121-383-6882

Singapore : 3 Raffles Place, #07-01 Bharat Building, Singapore 04817
t: +65-9788-5945