Universidade de Aveiro
2008
Departamento de Electrónica, Telecomunicações e Informática

Nuno Gabriel Sarabando

Validação de serviços *Triple-Play* em Nós de Acesso

Validation of Triple-Play services in the Access Node

Universidade de Aveiro
2008
Departamento de Electrónica, Telecomunicações e Informática

Nuno Gabriel Sarabando

Validação de serviços *Triple-Play* em Nós de Acesso

Validation of Triple-Play services in the Access Node

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica da Professora Doutora Susana Sargento, Professora auxiliar convidada do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro, e co-orientação do Doutor Victor Marques, responsável pelo grupo de Desempenho de Rede e Plataformas de Acesso em Rádio e em Cobre, do departamento de Desenvolvimento de Sistemas de Rede, da PT Inovação, S.A.

o júri

presidente

Doutor José Luís Guimarães Oliveira
Professor Associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

arguente

Doutor Rui Pedro de Magalhães Claro Prior
Professor Auxiliar do Departamento de Ciência de Computadores da Faculdade de Ciências da Universidade do Porto

orientadora

Doutora Susana Isabel Barreto de Miranda Sargento
Professora Auxiliar convidada do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

co-orientador

Doutor Victor Manuel Letra Macedo Marques
Gestor de Divisão de Desempenho de Rede e Plataformas de Acesso em Rádio e Cobre do Departamento de Desenvolvimento de Sistemas de Rede da Portugal Telecom Inovação, S.A.

agradecimentos

A toda a minha família, em especial à minha esposa Paula pelo carinho, amor e em especial a todo o apoio prestado principalmente nas horas de “aperto”.

A todos os amigos que sempre estiveram presentes para dar moral, humor e apoio.

A toda a equipa de trabalho DSR4 (antigo SIR6) da PT Inovação, S.A., em especial à Doutora Augusta Manuela e ao Doutor Victor Marques.
Ainda a todo o grupo Netband, que desenvolve e produz tecnologia “Made in Portugal”.

À Professora Susana Sargento, em que a sua ajuda e disponibilidade foi bastante importante na concretização desta dissertação.

Ao Doutor Victor Marques da PT Inovação S.A. pela sua disponibilidade, preocupação, e ajuda durante o trabalho realizado no âmbito desta dissertação e, também, durante a presente colaboração com a PT Inovação S.A.

palavras-chave

TR-101, Triple-Play, mDSLAM-48, AN, LACP, VLAN, QoS, DHCP Relay Agent, PPPoE Intermediate Agent, Multicasting, IGMP, IGMP Snoop, Proxy Reporting.

resumo

Com o grande crescimento das comunicações fixas, as tecnologias de fornecimento de acesso à Internet, como o cabo (*CATV*) e o par de cobre (*xDSL*), têm possibilitado o fornecimento de serviços adicionais para além do típico acesso à Internet de Banda Larga (em que, desde há vários anos o serviço de televisão já existe na tecnologia de cabo). Assim sendo, e ainda devido a uma forte concorrência entre operadores de cabo e de "cobre", o *DSL Forum* apresenta uma solução de arquitectura da rede de acesso e agregação que permite a migração da tradicional tecnologia *ATM* para *Ethernet*, em tecnologias baseadas em *xDSL*.

A migração da arquitectura para uma rede baseada em *Ethernet* permite o fornecimento de serviços adicionais que exijam altos débitos, qualidade de serviço, transmissão de *multicast*, *VOIP*, entre outros.

A presente tese apresenta os requisitos propostos pelo *DSL Forum* para o equipamento da rede de acesso e agregação: o nó de acesso (*DSLAM*), e um conjunto de testes conducentes à validação dos mesmos em laboratório, simulando uma possível rede de fornecedor de serviços.

keywords

TR-101, Triple-Play, mDSLAM-48, AN, LACP, VLAN, QoS, DHCP Relay Agent, PPPoE Intermediate Agent, Multicasting, IGMP, IGMP Snoop, Proxy Reporting.

abstract

With the large growth of fixed communications, the technology that provides Internet access, such as cable (CATV) and copper (xDSL), need to enable the provision of additional services beyond the typical broadband Internet access (where, television service already exists for several years over cable technology). Thus, because of strong competition between cable and copper operators , DSL Forum presents an architecture and aggregation solution for the xDSL based access networks that allows the migration of traditional ATM technology to Ethernet.

The migration of the architecture to Ethernet based network is due to the high speeds offer, and the possibility of additional services supporting quality of service, multicast transmission, VOIP, amongst others.

This thesis presents the requirements proposed by the DSL Forum for the equipment of the access network and aggregation: access node (DSLAM), and their validation in a laboratory environment, simulating service provision scenarios.

Table of Contents

Index of Figures

Index of Tables

Acronyms

AAA	Authentication, Autorization and Accouting
AAL	ATM Adaptation Layer
ADSL	Asymmetric Digital Subscriber Line
AN	Access Node
API	Application Programming Interface
AR	Access Router
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
ATU-C	ADSL Termination Unit – CO
ATU-R	ADSL Termination Unit – Remote
BE	Best Effort
BN-T	Broadband Network Termination
BNG	Broadband Network Gateway
BP	Bridge Port
BRAS	Broadband Remote Access Server
B-RAS	Broadband Remote Access Server
CBR	Constant Bit Rate
CLI	Command Line Interface
CO	Central Office
CPE	Customer Premises Equipment
CPU	Central Processing Unit
C-VLAN	Customer VLAN
DHCP	Dynamic Host Configuration Protocol
DRA	DHCP Relay Agent
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line with Access Multiplexed
DSP	Digital Signal Processing
DST	Daylight Saving Time
ETH	Ethernet
FD	Factory Default
FDB	Forwarding Data Base
FWA	Fixed Wireless Access
GAG	Generic Agent
GARP	Generic Attribute Registration Protocol
GBE	Gigabit Ethernet
GMI	Group Membership Interval
GMQ	General Membership Query
GPON	Gigabit Passive Optical Network
GUID	Global Unic Identifier
GVRP	GARP VLAN Registration Protocol
HDTV	High-Definition Television
HGW	Home Gateway
HSI	High Speed Internet
IA	Intermediate Agent
IC	Integrated Circuit
ICMP	Internet Control Message Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPoA	IP over ATM
IPoE	IP over Ethernet
IPTV	Internet Protocol Television (TV streaming over IP protocol)
ISP	Internet Service Provider

IVL	Independent VLAN Learning
IWF	Interworking Function
LAC	L2TP Access Concentrator
LAG	Link Aggregation Group
LAN	Local Area Network
LCP	Link Control Protocol
LLC	Logical Link Control
LMQC	Last Member Query Count
LMQI	Last Member Query Interval
L2TP	Layer 2 Tunneling Protocol
MAC	Media Access Control
mDSLAM	media DSLAM® (PT Inovação, S.A Trademark [30])
MPLS	Multi Protocol Label Switching
MPLS PE R.	Multi Protocol Label Switching Provider Edge Router
NAT	Network Address Translation
NID	Network Interface Device
NSP	Network Service Provider
OAM	Operation And Maintenance
OSS	Operation Support System
PADI	PPPoE Active Discovery Initiation
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-Confirmation
PADT	PPPoE Active Discovery Terminate
PAT	Port Address Translation
PC	Personal Computer
PDU	Packet Data Unit
PIM	Protocol Independent Multicast
POTS	Plain Old Telephone Service
PP	Probabilistic Priority
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPPoE IA	PPPoE Intermediate Agent
PSVID	Port Service VLAN Id
PVC	Permanent Virtual Circuit
PVID	Port VLAN Id
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RBN	Regional Broadband Network
RED	Random Early Detection
RFC	Request For Comments
RG	Residential/Routing Gateway
SFP	Small Form-Factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSM	Source Specific Multicast
STB	Set-Top Box
STP	Spanning Tree Protocol
SVL	Shared VLAN Learning
S-VLAN	Service VLAN
TFTP	Trivial File Transfer Protocol
TR	Technical Report
TV	Television
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
VC	Virtual Circuit
VCI	Virtual Channel Identifier
VID	VLAN ID
VLAN	Virtual LAN
VoD	Video on Demand
VoIP	Voice over IP
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WFQ	Weighted Fair Queueing
WRR	Weighted Round Robin
xDSL	Family of technologies that provide DSL

Chapter 1: Introduction

1.1. Motivation

Regulatory authority for electronic communications and postal services in Portugal (ANACOM [1]) reported that total subscribers of Broadband[1] Internet Access (also known as High-Speed Internet access) has grown in the third trimester of 2007 (3T07) about 2,3% related to the last trimester (2T07), and about 9,2% related to the homologous trimester of the year 2006. With this increase, there are about 1.680.000 of Internet access subscribers, in which 1.570.000 are Broadband subscribers [2].

There is a clear decrease of dial-up subscribers, which are migrating to broadband access. In that trimester, the number of dial-up subscribers decreased to about 109.000, less than 12.000 than in the previous trimester. At the end of September of 2007, this type of subscriber did decrease 41% related to 12 months before.

In Portugal the biggest part of Fixed Internet Access are broadband customers. They represent near 94% of the total subscribers. This kind of subscribers have grown 3,3% related to last trimester and about 16% related to the same trimester of the last year.

	2007		Variation	
	2nd Trimº	3rd Trimº	3T07 / 2T07	3T07 / 3T06
Total subscribers	1.637.501	1.675.758	2,3%	9,2%
Broadband subscribers	1.516.773	1.566.924	3,3%	16,0%
Dial-up susbcribers	120.728	108.884	9,8%	40,7%

Table 1 - Number of broadband subscriber's evolution

Source: ANACOM [1].

[1] Broadband Internet Access, often shortened to just broadband, is high-speed Internet Access – typically contrasted with dial-up access over a modem. Dial-up modems are generally only capable of a maximum bitrates of 56 kbps, and required full use of telephone line. Broadband technologies supply at least double speed and without disrupting telephone use.

The main technology that is used to offer broadband access is ADSL (Asymmetric Digital Subscriber Line) [3]. This technology represents 62% of the total of broadband accesses (near to 971.000 subscribers). Cable modem is the technology elected by about 37% of broadband subscribers (about 585.000).

	2007		Variation	
	2nd Trimº	3rd Trimº	3T07 / 2T07	3T07 / 3T06
Total Broadband subscribers, where:	1.516.773	1.566.924	3,3%	16,0%
ADSL subscribers	932.177	971.153	4,2%	16,3%
% of total number of Broadband accesses	61,5%	62,0%		
Cable modem sbscribers	576.263	585.066	1,5%	14,3%
% of total number of Broadband accesses	38,0%	37,3%		
Others	8.333	10.705	28,5%	174,9%
% of total number of Broadband accesses	0,5%	0,7%		

Table 2 - Number of broadband subscriber's evolution, using different access technologies
Source: ANACOM [1]

"Others" are represented by Leased Lines and Fixed Wireless Access (FWA) [4]. Those kind of technologies represent only about 0,7% of the total number of subscribers, with large increases, due to Mobile Broadband accesses (see Figure 1). This evolution is due to different network packet based solutions offered to the subscribers.

Referring to fixed broadband access market positions, PT Group had 69,1% at the end of 3T07. It has been decrease 0,6% of the previous trimester, and 2,7% of the corresponding trimester of 2006. Analysed trimester have about 49% of new broadband subscribers that are customers of alternative providers.

In addition to Internet Access, subscribers can enjoy new residential services such as IP telephony, video-conference, IPTV, video on demand (VOD), music on demand, tele-vigilance, amongst others. Such services allow the concept of triple-play and multi-play architectures.

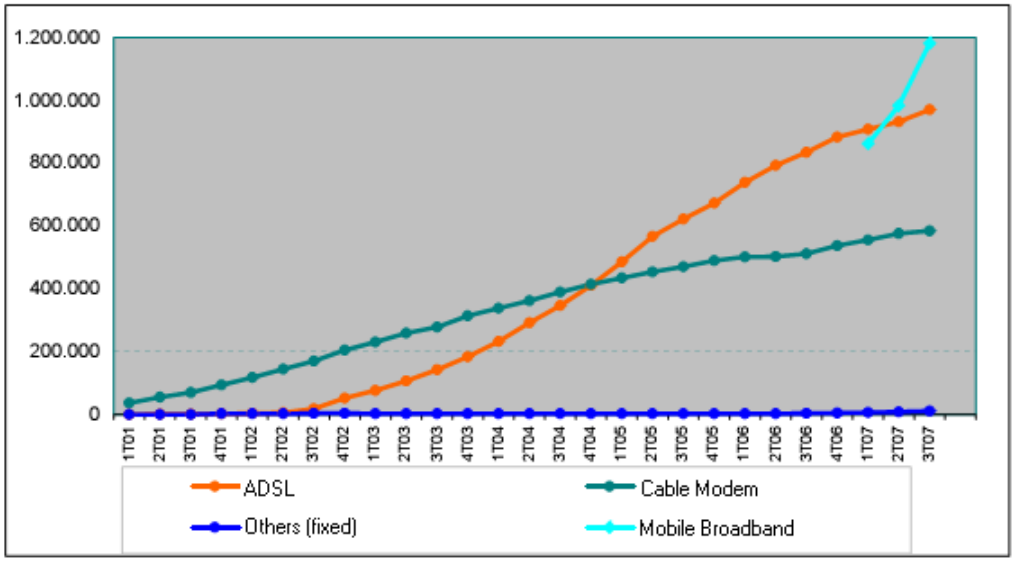

Figure 1 - Broadband subscribers evolution

Source: ANACOM [1]

For this purposes there are some residential, access and core network requirements that need to be implemented and adapted to give support for those kinds of services.

Residential networks may support distribution of different kind of services (maybe from different providers). These different services cannot cause interference between them, and may guarantee a feasible and correct service delivery. Internet access allows web browsing, e-mailing, home banking, amongst others. Using the IP communication protocol, subscribers can access to peer-to-peer services, create residential network, where personal digital devices are connected, like MP3 players, personal computers, media-centers, cameras, printers, DVD and Blue Ray players, game consoles. These devices can be connected through wireless communications, like Bluetooth and Wifi, or through wire connections (Ethernet).

Access Network is an elementary functional block that needs to be upgraded accordingly with new capacities, technologies and services provisioning to be provided to customers.

PT Inovação did develop an Access Node for ADSL access/aggregation network that has support to offer triple-play solutions, the Media DSLAM-48 [30].

The main subject of this Thesis is the validation of the necessary features that Media DSLAM-48 needs to support to enable the delivery of triple-play services on ADSL aggregation network.

1.2. Objectives

The main goal of this Thesis is to present the test and evaluation of PT Inovação Ethernet based IP DSLAM, the mDSLAM-48 (or Media DSLAM-48) [30], accordingly with the requirements of TR-101. This special focus on TR-101 is due to the "how to" an ATM aggregation network can be migrated to an Ethernet based aggregation network. TR-101 provides an architectural/topological model of such an Ethernet based aggregation network that supports the new business and services requirements like protocol translation and interworking, QoS, multicast, security, for a xDSL aggregation network.

1.3. Document Outline

The present Thesis is organized as follows:

- Chapter 2: presents a brief description of normalization organizations and their contributions for network evolutions;
- Chapter 3: gives an overview of DSL Forum Technical Report 101, which proposes the architecture and scenarios that allow the delivery of triple-play services over xDSL Access Network based;
- Chapter 4: presents a global description of mDSLAM-48 hardware and software architecture. An overview of software feature support such as VLANs, DHCP Relay Agent, IGMP Snooping, LACP, etc is also presented.
- Chapter 5: named as Triple-Play Features Validation presents the approved and tested features accordingly to requirements of TR-101 document, and Service Enabling features used for validation purpose.
- Chapter 6: presents the conclusions chapter.

Chapter 2: Standardization Organizations

Current DSL architectures are growing from a "low" speed best effort delivery services network to infrastructures that can support higher user bit rates and services requiring availability, multicast and QoS, difficult to achieve in a pure legacy ATM based environment. Ethernet is a technology that supports the needs of the next generation DSL network based on transport mechanism that enables higher connection speeds, packet based QoS, simpler provisioning and multicast in an efficient manner.
Bellow is presented the main Standardization Organizations and Forums that are relevant for the work presented in this document.

2.1. Digital Subscriber Line Forum

DSL Forum [3] was created in 1994 in order to spread the DSL development and system architectures and protocols for major Digital Subscriber Line (DSL) based applications. The DSL Forum has expanded its efforts to address marketing issues surrounding awareness, and enabling high-speed applications via DSL. It is a world wide consortium of some companies which have weight on different telecommunication and information technology sectors. It has a global representation of the wire-line service providers, broadband device and equipment vendors, consultants and independent testing labs (ITLs). Its main purpose was the establishment of new standards around DSL communication products such as provisioning. This cooperation has brought different standards: ADSL, SHDSL, VDSL, ADSL2+ and VDSL2.

After 2004 the Forum expanded its work into other last mile technologies including optical fiber, without changing its name.
For more information, please refer to [3].

2.2. International Telecommunication Union

The International Telecommunication Union (ITU) [5] is an international organization that regulates international telecommunications and radio standards. Founded as the International Telegraph Union in Paris on 1865, its main tasks are standardization, allocation of the radio spectrum, and organizing interconnection arrangements between different countries to allow international phone calls. Its headquarters are in Geneva, Switzerland and it is one of the agencies of the United Nations.

2.3. ITU Telecommunication Standardization Sector

The ITU Telecommunication Standardization Sector (ITU-T) [6] coordinates standards for telecommunications representing the International Telecommunication Union (ITU).
The ITU-T ensures the efficient and timely production of standards covering all fields of telecommunications, as well as defining tarifs and accounting principles internationally.
International standards that ITU-T produced are referred as "Recommendations". They have this name because they only become mandatory at the time of the final law.
ITU-T standardization cooperates its work with other standard-developing organizations, i.e. the International Organization for Standardization (ISO) and the Internet Engineering Task Force (IETF) [8].
An example of the main achievements is DSL series of standards for broadband, which recommendation series G (Transmission systems and media, digital systems and networks) belongs to [7].

2.4. Institute of Electrical and Electronics Engineers

Institute of Electrical and Electronics Engineers (IEEE) [9] is a professional organization, and an international non-profit for the advancement of technology related to electricity. It has the highest number of members of any technical professional organization in the world (around 365,000 members in near 150 countries).
IEEE's is a "scientific and educational, directed toward the advancement of the theory and practice of electrical, electronics, communications and computer engineering, as well as computer science, the allied branches of engineering and the related arts and sciences"

([10]). IEEE is the biggest publisher of scientific journals and conference organizer. It is also a developer leader of industrial standards in a large amount of disciplines, like electric power and energy, biomedical and health technology, information technology, telecommunications, electronics, transportation, aerospace, and nanotechnology. IEEE participates in institutes of higher learning to induce educational activities such as accreditation of electrical engineering programs.

LAN/MAN standards are very important examples relevant for this thesis, where the notable IEEE standards related to it are:

- IEEE 802 — LAN/MAN
- IEEE 802.1 — Standards for LAN/MAN bridging and management and remote media access control (MAC) bridging.
- IEEE 802.2 — Standards for Logical Link Control (LLC) standards for connectivity.
- IEEE 802.3 — Ethernet Standards for Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- IEEE 802.4 — Standards for token passing bus access.
- IEEE 802.5 — Standards for token ring access and for communications between LANs and MANs
- IEEE 802.6 — Standards for information exchange between systems.
- IEEE 802.7 — Standards for broadband LAN cabling.
- IEEE 802.8 — Fiber optic connection.
- IEEE 802.9 — Standards for integrated services, like voice and data.
- IEEE 802.10 — Standards for LAN/MAN security implementations.
- IEEE 802.11 — Wireless Networking – "WiFi".
- IEEE 802.12 — Standards for demand priority access method.
- IEEE 802.14 — Standards for cable television broadband communications.
- IEEE 802.15.1 — Bluetooth
- IEEE 802.15.4 — Wireless Sensor/Control Networks – "ZigBee"
- IEEE 802.16 — Wireless Networking – "WiMAX"

In this document, we can find references mainly related with IEEE 802.1 [11], as example, 802.1ad, 802.1q, 802.3ad, …

2.5. Internet Engineering Task Force

The Internet Engineering Task Force (IETF) [8] is an organization that develops and encourages Internet standards, cooperating in particular with standards of the TCP/IP and Internet protocol suite. It is an open standards organization, and all leaders and participants are volunteers, even their work is usually made by their employers or sponsors.

It is organized into working groups and informal discussion groups, each treats a specific topic. Each group must complete work on that topic and afterwards is dissolved.

The working groups are organized into areas like: Applications, Internet, Operations and Management, Real-time Applications and Infrastructure, Routing, Security, and Transport. Each area is supervised by an area director (AD) which is responsible for appointing working group chairs. The ADs with the IETF Chair, form the Internet Engineering Steering Group (IESG), which is responsible for the overall operation of the IETF.

Request for Comments (RFC) are published by the IETF and they describe methods, behaviours, research, or innovations applicable to the working of the Internet and Internet-connected systems.

Through the Internet Society, engineers and computer scientists may publish the RFC, either for peer review or simply to convey new concepts or information. The IETF adopts some of the proposals published as RFCs as Internet standards. The list of IETF RFCs may be found on [12].

Internet Protocols such as DHCP, PPP and IGMP, amongst others, are examples of conformed protocols standardized by IETF RFCs.

For IGMP (Internet Grouping Multicast Protocol), as example, there are several different versions: IGMP v1 is defined in RFC 1112 [13], IGMP v2 in RFC 2236 [14] and IGMP v3 in RFC 3376 [15].

2.6. Summary

It is important to recognize that in today's environment, no single body alone can take care of everything. That is, a big collaboration between all concerned bodies is needed.

The relation between ITU, an intergovernmental organization, and other Internet Standard bodies, such as IETF, is an excellent example of cooperation between ITU and external SDOs (Standardisation Organisations). Increasingly, as Internet infrastructure and the

services it enables become integrated into the NGN (Next Generation Networks), the long-established regional and national SDOs will be assuming significant roles.

DSL Forum publishes Technical Reports (TR) with architecture and services proposals that specify services and capabilities accordingly to the some features that may be of interest and important for Providers. That is, DSL forum underlies DSL architecture and explain how it must evolve.

In this thesis, DSL forum is the key driver of DSL architecture evolution, once it enables how to move services providers from basic broadband Web access to higher-value services – essentially, (very) high-speed multimedia applications that exploit convergence among data, voice, and video for things like triple play, IPTV, HDTV, and network gaming.
However, all of those services must be assured also by protocols defined by

- ITU, that defines the standards for DSL protocols,
- IEEE, for the Standards for Local and Metropolitan Area Networks, like Vlans (and Vlan stacking), LACP, QoS, …
- IETF, for the RFCs of IP based protocols, like SNMP, DHCP, PPP, IGMP, …

In this sense, there is a work in set that combine all the mentioned organizations with the objective to create a solution where each one have their fundamental feature.

Chapter 3: Triple-Play Architecture based on TR-101

The present section is based on "DSL Aggregation 101" Light Reading document [16] that summarizes and illustrates DSL Forum Technical Report TR-101 key features.

So, it starts for presenting a brief description of the purpose of the TR-101, whose goals for the operators are the implementation of a IPTV network supply, using for this, the already existent access network (xDSL).

Next, the origin of the TR-101 is presented (that is, history until its origin) followed by a brief description of Technical Reports on which it is based, TR-025, TR-058, TR-059 and TR-092.

Finally, the last section of this chapter, gives, for each main boarded subjects in the document TR-101 (for all Access Network, since CPE to BNG, not only for Access Node), a brief description of each one, over which the tests were centred and performed, and because, they are the reason of the accomplishment of this thesis.

3.1. DSL Forum Technical Reports

In the year of 2006, DSL Forum published Technical Report 101 (TR-101), named "Migration to Ethernet-Based DSL Aggregation". This TR become a definitive receipt for providers that need to migrate infrastructures from ATM to Ethernet based, to improve their DSL networks to better support faster rate technologies (example: ADSL2plus and VDSL2). In parallel, TR-101 specifies the architecture to coordinate service rate management and multicast capability in an Ethernet network without affecting existing services currently being offered.

Based on TR-101, service providers can develop a multi-service end-to-end architecture to support new secure value-added consumer and business services such as Internet Protocol Television (IPTV).

DSL architecture evolution is centralized in the upgrade by services providers from basic broadband Web access to higher-demanding services: high-speed multimedia applications that explore convergence of data, voice, and video (triple play, IPTV, HDTV, gaming, …). For this, service providers have to study how to provide more bandwidth, add more features, and ensure efficient and better service management on their network.

It is a very important step for the underlying of DSL architecture and how it must evolve, because it has to:

- Support open services delivery model to override a wide range of service providers,
- Provide network enhancements to support QoS, multicast access and migration from the current ATM installed base to Ethernet aggregation
- Allow operations to scale effectively and efficiently, which means enhancements to network/service management

Table 3 summarizes the key Technical Recommendations in their historical sequence, that TR-101 is summary based.

Recommendation	Date	Features
TR-025	1999	- Access to ISP data services over ADSL – use Point-to-point Protocol (PPP) techniques. - For access providers, Layer 2 Tunnelling Protocol (L2TP) being the dominant direction at the time
TR-058, TR-059	2003	- Focus on multiservice. - Introduced "application service provider connection model", which is an addon for access provider. - Service rate control no longer controlled by DSL rate training in the DSL Access Multiplexer (DSLAM). Broadband Remote Access Server (B-RAS) controls it based on packet policing/shaping
TR-092	2004	B-RAS requirements accordingly to TR-059 architecture
TR-101	2006	- Migration from ATM aggregation networks to Ethernet based. - Architectural solutions for multicast/IPTV supplier

Table 3 - DSL Forum Technical Recommendations

Source: Light Reading [16].

3.2. Technical Report TR-025

Initially TR-025 [17] was defined to migrate the access of the existing ISPs, essentially a Layer 2 upgrade using the same infrastructure and devices – such as RADIUS – for dialup services (each of the network architecture is based on the PPP over ATM model, and L2TP).

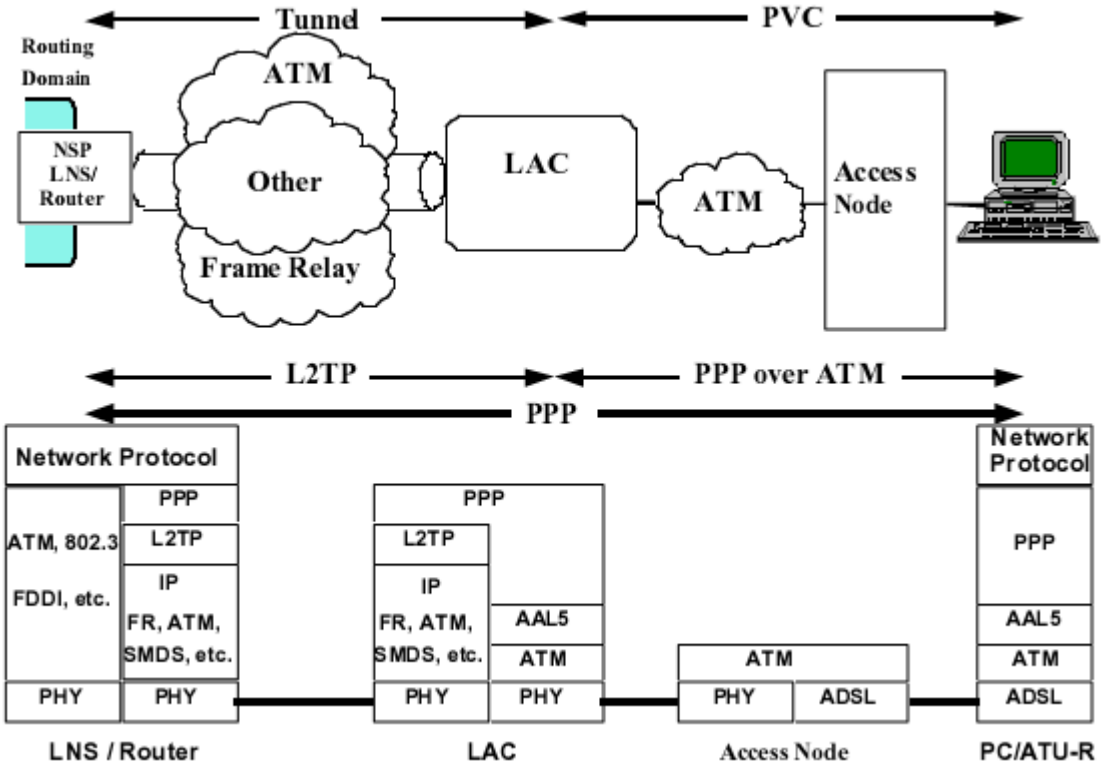

Figure 2 - PPP over ATM and L2TP Access Aggregation

Source:TR-025 [17].

3.3. Technical Report TR-058, TR-059 and TR-092

TR-058 [18] proposes the requirements of a DSL multiservice architecture and evolution from the old deployed DSL architectures (until the moment of its elaboration).

As the architecture was outlined, and the DSL market did proposed new set of requirements for new capabilities, there was the need to drive the migration of existing networks to a multiservice architecture. Based on those drivers, TR-058 defines a list of architectural requirements required in a multiservice architecture. For detailed information on this topic please refer to [18].

As ADSL providers had interests in the expansion of the market they can address, it was necessary to grow their network and increase the add-on value of its expansion. In that case, advancing DSL was the preferred broadband access technology from the point of view of service operators.

To do it they must adopt some critical needs, enhancement:

- The service must be more accessible to subscriber users and to wholesale partners.
- The service must comprise a large market with:
    - Variable speeds,
    - QoS in high priority applications and traffic types,
    - Specific support for IP applications (example: multicasting),
    - Support for new models of business which includes new type of service providers,
    - And support for the new service parameters over different connections to independent service providers from a single subscriber line.
- Essentially, the service must be very competitive with alternative access technology providers (example, cable).

Resuming, the goal of the proposal for new service models was to overview a commonly architecture and a list of service interfaces to submit these needs.

TR-059 [19] proposes a DSL evolution to the deployment and interconnection proposed on TR-058. An outline of QoS applications to be offered to xDSL customers from different service providers was proposed. TR-058 requirements justify this architectural evolution. Resuming, the goal of the architecture presented in TR-059 is the offer of IP-QoS and provide a flexible service combinations to diverse users and service providers. The proposal of the network enhancements to the existent DSL networks are based also on the economic aspects.

TR-092 [20] main propose is the addition of a Broadband Remote Access Server (BRAS). DSL Forum TR-059 presents a outline for an DSL deployment and interconnection architecture, based on the concept for the offer to the customers of QoS based applications

from one or different Service Providers. The BRAS is a fundamental element for that support.

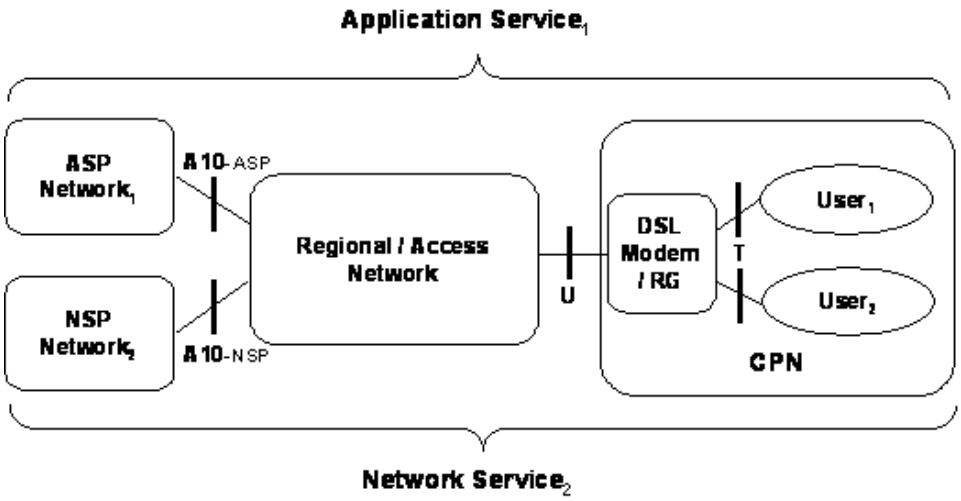

Figure 3 - TR-92 definition of many-to-many access

Source: TR-092 [20].

Figure 3 presents an overview of the concept of distinct many-to-many access as a fundamental rich enhancement of BRAS. These capabilities are possible in an ATM environment, and BRAS device can provide flexibility and scalability in an easy way.

The BRAS can perform some functions (as example, LAC, IP router, or a MPLS PE router) once it aggregates user sessions from the access network. More than basic aggregation capabilities, the BRAS is also the main point for policy management and IP QoS in the Regional/Access Networks. Figure 4 illustrates the logical representation where the BRAS is located in the Regional/Access Network. It is the last IP device between Access and Network Service Providers (ASPs and NSPs) and the subscribers network, and as such is the main device that can manage the IP traffic of the layer 2 Access Network. For this propose, BRAS needs a congestion management that allows the control of IP QoS through downstream elements that are not aware to QoS (enhancing DSL providers to support advanced IP applications).

One of the goals was to enable a new list of business relationships in the network. TR-092 gives the notion that the access provider can manage network using IP layer for application service providers. So it needs an interface to the network service provider, who can handle

the addressing and other connection issues promising that is able to offer higher-value services.

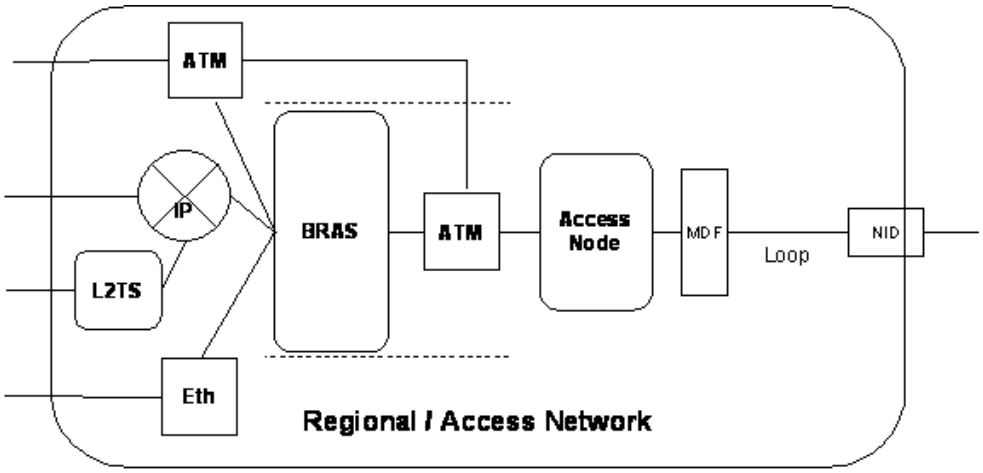

Figure 4 - TR-059 Based Regional/Access Network

Source: TR-092 [20].

Resuming, TR-058, TR-059, and TR-092 looked to multi-services and adding value at Layer 3.

3.4. Technical Report TR-101

This section presents a summary of the motivation for the Ethernet based architecture, and the general overview of TR-101, describing its relation with Technical Reports TR-025, TR-058, TR-059 and TR-092. Presented text is based on Light Reading document [16], which gives a practical overview and resume of TR-101 key features.

After that, there is a section presenting the Architecture related issues. There is no detailed information about the requirements list (some of them are presented in Annex II). However, the fundamental network elements, main technical issues, and the multicast feature, in the access and aggregation network are presented.

3.4.1. Overview

Technical Report TR-092 was oriented to the existing ATM DSL architectures. It inserts useful functionalities in the BRAS. However, bandwidth and ATM limitations on architectures scenarios are requirements that needed to be upgraded to the support of future challenges of service providers.

In TR-025 and TR-059 Access Node works as an ATM aggregator and cross-connect, multiplexing subscriber ATM PVCs from the U to the V interface and de-multiplexing them back on the other direction (see Figure 5 and Figure 6).

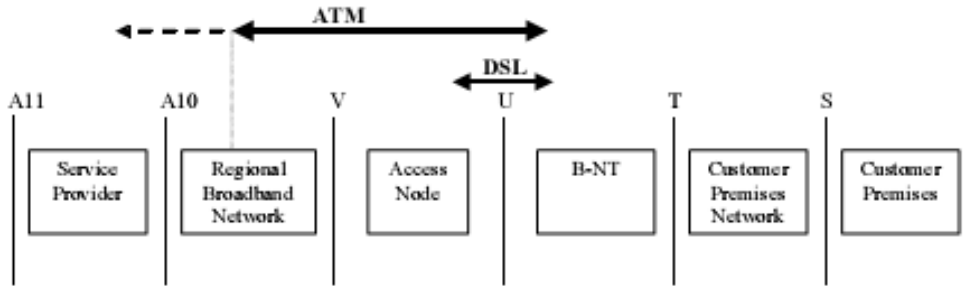

Figure 5 - TR-025 High Level Architectural Reference Model
Source: TR-101 [21].

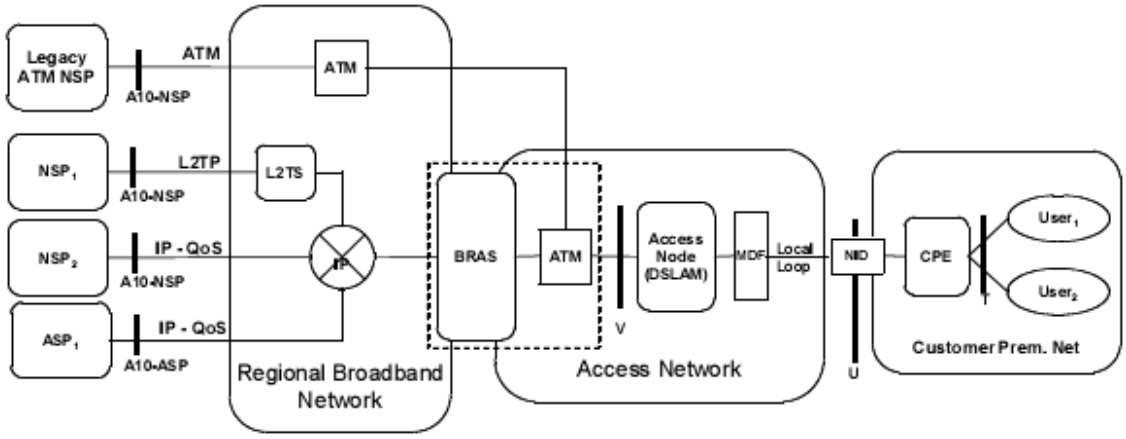

Figure 6 - TR-059 High Level Architectural Reference Model
Source: TR-059 [19].

Traffic that Access Nodes aggregates is forwarded to the BRAS. In TR-025, a BRAS was either located in the regional network or in the service provider network and its functions were point-to-point tunnelling and termination. In TR-059 the BRAS is located on the edge of the regional network and was enhanced with subscriber management, advanced IP processing, and new traffic management capabilities.

TR-101 [21] provides the specifications of the main needed features with the goal of migrating DSL aggregation from ATM to Ethernet. It is not a replacement of ATM-to-Ethernet, once there is also the necessity to offer multicast and video type services in the aggregation network, once an Ethernet infrastructure exists.

TR-101 includes also:

- Multi-service end-to-end architecture that can support IPTV,
- Continues the family requirements of TR-058, TR-059, and TR-092,
- IP QoS in the BRAS/edge routers (renamed as broadband network gateways - BNGs),
- Ethernet QoS in the access node and aggregation network,
- Multicast replication in access node and/or aggregation switch, with IGMP snooping,
- PPP and IP wholesale services,
- Additional IP services (VoIP, ...),
- Possibility of Multicast content delivered by a separate BNG or server.

An architecture based on multi-edge is a new notion of TR-101: having the possibility that different types of service can have their separate and optimized devices, as broadcast IPTV or VOD. So, BNGs that function as BRAS do not need to be the source or personalize the high-bandwidth multicast flows, allowing the distribution of some of the functionalities through other devices in the access network. For this purpose, separate VLANs dedicated to BNGs (one by service) may be used, instead of a single BNG to control all services.
The simplest architecture for multi-edge platform is a dual edge (that probably separate services into video and everything else, once video streams has the highest impact on the network).

3.4.2. Why Migration to Ethernet based

Ethernet is a transport technology that meet the next generation DSL network needs through a transport mechanism that can handle higher connection speeds, packet based QoS, multicast, and redundancy efficiently.
At the application layer, DSL service providers wants to offer enhanced services in conjunction with basic Internet access including entertainment video services (Broadcast TV and VoD), video conferencing, VoIP, gaming, and business class services (example, VPN). Many of these services needs to reach higher DSL synch rates than are typically achieved in typical ADSL deployments (before ADSL 2+, as example). Using new DSL

transmission technologies (as ADSL2+), the most easier and efficient way to obtain the maximum DSL synch rate is to reduce the distance between the AN and CPE locations, (which may require the changing of the location of Access Node). So, the number of Access Nodes deployed within a service provider's network may increase once they are pushed closer to the subscribers edge. Gigabit Ethernet and GPON allow highly efficient transport technologies that may deliver large amounts of bandwidth to a highly distributed Access Node topology.

3.4.3. TR-101 Architecture

Figure 7 shows the basic high-level TR-101 DSL Architecture with Ethernet aggregation based. It assumes an IP-based regional broadband network (RBN) which may be connected to ISPs, network service providers (NSPs), and application service providers (ASPs), although there is provision for direct Ethernet linking to the aggregation network.

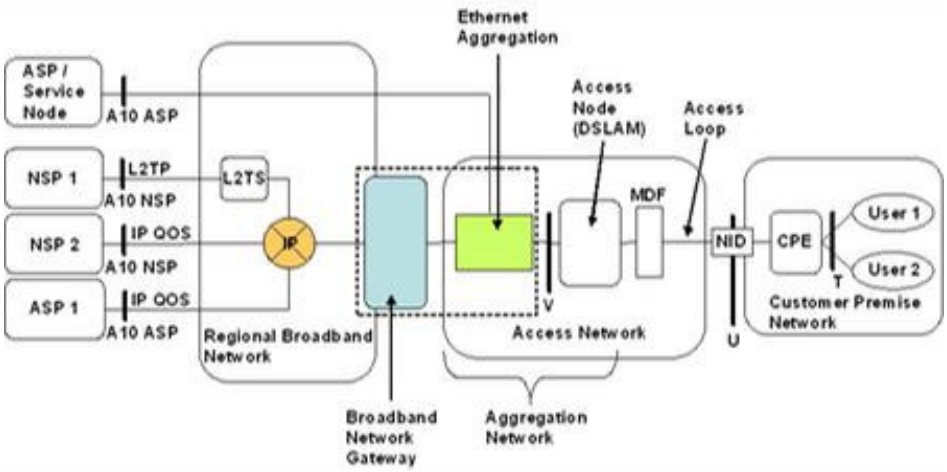

Figure 7 - DSL Forum TR-101 DSL Architecture
Source: Light Reading [16].

Notably, there is no BRAS device. Now, it is the broadband network gateway (BNG). BNG is the access network, which interconnects various DSLAMs, including aggregation network and the V[2] reference point. As the U[3] reference point between the access network and the customer premises network (CPN), the V reference point preserves the

[2] V interface is the Access node uplink interface. TR-101 based architecture defines V interface as Ethernet based.
[3] U interface is defined as subscriber lines of access node (DSLAM).

terminology used in older International Telecommunication Union, Standardization Sector (ITU-T) Recommendations [6].

Higher access speeds require that access node tends to be further out into the aggregation network, and one of the things that an Ethernet architecture allow is the use VLAN approaches to separate traffic services.

The main focus of TR-101, however, is only on part of this architecture (Figure 8). That is, TR-101 concerns mainly in

- the BNG,
- any source video (located in the aggregation network),
- the Ethernet aggregation network module (can be switches, or direct connection from the access node to the BNG),
- the access node –AN (DSLAM),
- the network interface device (NID), and
- customer premises equipment (CPE).

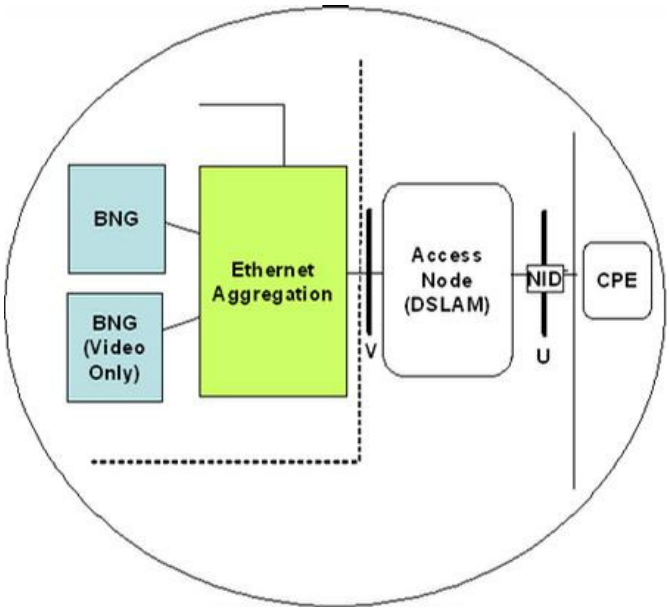

Figure 8 - Focus of TR-101

Source: Light Reading [16].

3.4.4. Network Elements and Features

The following table summarizes the main features of TR-101 as it affects the network elements, accordingly with Figure 8.

Network Element	Features
BNG	-PPPoE and/or IP/DHCP services. -Bandwidth/QOS policy/shapping. -Security. -Multicast control. -Operation and Maintenance (OAM)
BNG (as video source)	-IP/DHCP services for unicast VoD and multicast IPTV. -DiffServ QoS. -Security. -Multicast source. -DHCP relay
Ethernet aggregation	-IP/DHCP services for unicast VoD and multicast IPTV. -DiffServ QoS. -Security. -Multicast source. -DHCP relay
Access Node (DSLAM)	-ATM-Ethernet interworking. -VLAN handling. -Security. -QoS. -Multicast/IGMP. -OAM
CPE	-Routing gateway. -IGMP Proxy

Table 4 - Effect of TR-101 on Key Network Elements

Source: Light Reading [16].

The BNG continues to support PPPoE services, and also IP and DHCP directly. This is due to the avoiding the use of PPPoE and moving directly to IP connectivity.

TR-101 adopt forward bandwidth and QoS policy at the BNG from the TR-059 requirements. However, security implications exists due to the migration from an ATM infrastructure to an Ethernet based, that require that BNG adopt additional requirements. Also, in the multi edge architectures, exists other implications of combining multiple

sources feeding onto a customer loop with the QoS model that the BNG is expected to support.

And, a new set of OAM requirements accordingly with the IEEE and the ITU-T in the connectivity fault management work in 802.1ag [22] and Y.1731 [23] exists due to the migration from ATM to Ethernet infrastructure. More details can be found in [21].

3.4.5. Technical Issues

ATM facilitates traffic management and QoS at Layer 2 in a per-subscriber account. It enables business and residential customers to be multiplexed in the same physical network (accordingly with "standard" DSL architecture - TR-059), and so is well supported by equipment and management systems. Also, it has some inherent security, being a connection-oriented technology which satisfies operators.

Contrasting, Ethernet scales more cost-effectively for 1 or 10-Gbit/s network speeds. QoS is provided via Ethernet priority bits and IP techniques and hierarchical scheduling per-subscriber. However, security was not an original design consideration.

Table 5 summarizes the characteristics translated as specific issues, and the TR-101 solutions.

Issues	Solutions	Technologies
VLAN scaling: 4094 tags are insufficient for any network	Offer multiple tagging strategies	-S-tag per port -S-tag per DSLAM and C-tag per port.
Legacy protocols not mapped on Ethernet	Define interworking models	-PPPoA/PPPoE interworking. -IPoA/IPoE Interworking
Spoofing (Ethernet MAC address), Denial of Service (DOS) attacks, and correct mapping of subscribers to	-Trusted agents in the DSLAM for PPPoE/DHCP. -Ethernet MAC-level	-PPPoE Intermediate Agent. -DHCP Relay Agent. -ARP processing -IP spoofing protection

services	elements to drop malicious customers	
How to communicate the DSL loop status to the BNG (improving service management and QOS purposes)	Extensions to PPPoE/DHCP to send this information to the BNG	PPPoE Intermediate Agent and DHCP Relay Agent adds Access Loop characteristics (encapsulation, syncrate).

Table 5 - Technical Issues and TR-101 Solutions

Source: Light Reading [16].

3.4.5.1. VLANs

Of all the issues presented in Table 5, for mass-market services such as IPTV and VoD, VLANs underpin the multicasting and unicasting services delivered.

TR-101 offers several tagging strategies (that starts and terminates in the Access Node) which allow the service provider to define its own strategy and architecture of VLAN services.

One of the possibilities is: the use of C-VLAN being defined by the inner or customer tag and the S-VLAN being defined by the outer or stack tag in an 802.1ad [24] Q-in-Q VLAN architecture (1:1 Vlan), as:

- S-tag per port, primarily focused on business services;
- S-tag per DSLAM and C-tag per port (analogy to the ATM virtual path (VP) and virtual circuit (VC), as the S-tag playing the role of the VP and the C-tag that of the VC);
- S-tag per DSLAM with MAC-level demultiplexing at the access node (that may identify individual ports).

For multicast data, TR-101 propose a N:1 VLAN per service approach as a resolution to the VLAN scaling issue. In this case,

- Traffic is single-tagged with an S-Tag on the aggregation network;
- Each subscriber interface may belong to different sessions that can be carried in different VLANs;

- The S-Tag can belong to one or more subscriber port (shared by a large number of users). Access Node supports additional features that maintain isolation between users (do not allow Layer 2 user-to-user forwarding) ensuring security.

Resuming, different scenarios can adopt an S-Tag that can be common to:

- All users attached to the same Access Node
- Users sharing the same service
- Traffic to/from a group of Access Nodes.

Section "Multicasting" is useful to better understand the concept of N:1 Vlan, in stacked mode architecture.

3.4.5.2. Quality of Service

TR-101 purposes the use of DiffServ based IP QoS at the Routing Gateway (CPE side) and the BNG.

Biggest important, is the use of three Quality of Service (QoS) models, that are not exclusive mechanisms:

1. Bandwidth partitioning among the Broadband Network Gateways (rate limits on business or application characteristics of the BNG that control each partition).
2. Distributed precedence and scheduling:
   - Ethernet QoS in the Access/Aggregation Network
   - Under congestion drop lower classes traffic
   - Balance between classes but not between users that belong to the same class

   Figure 9 illustrates the distributed precedence and scheduling model with dual nodes.
3. Hierarchical Scheduling on the BNG: scheduling steps sequence to avoid downstream congestion points (BNG port, Access Node uplink, and DSL synch rate) that can be used in combination with the above.

The last point is a specific consideration for multicast. However, it is not a big issue in the Access Node, because it is typically provisioning with bi-directional Gigabit Ethernet (GBE) links that can deliver video traffic with any congestion issue, therefore, leaving the upstream links with low utilization.

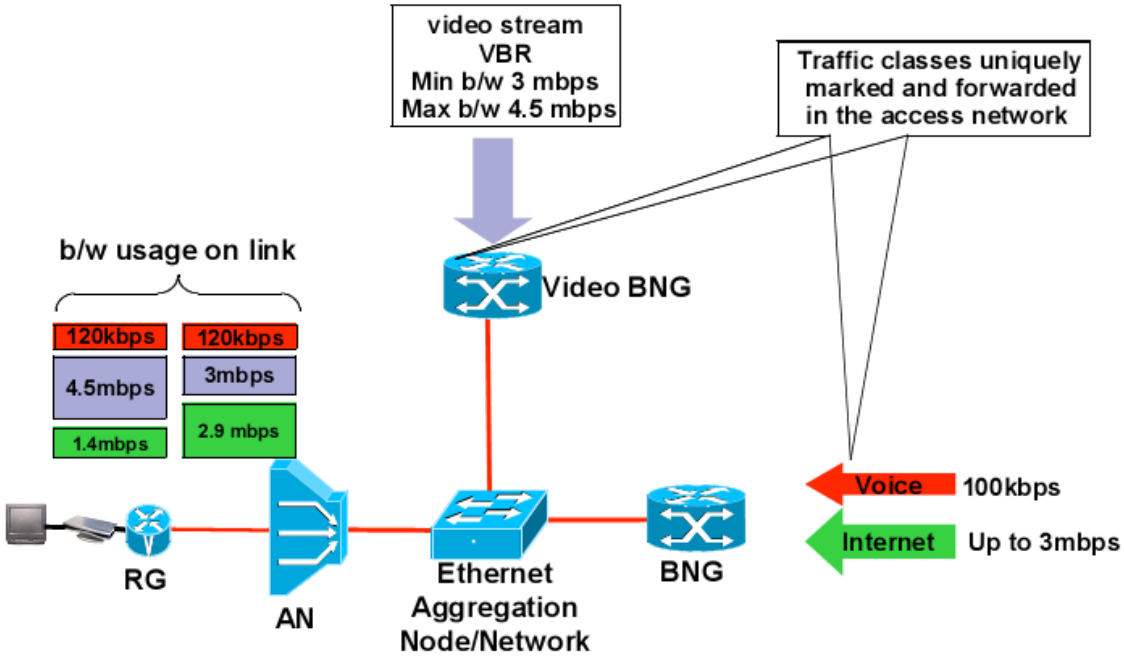

Figure 9 - Example distributed precedence and scheduling model with dual nodes
Source: TR-101 [21].

3.4.5.3. Access Node Protocol Adaptation Functions

IP over ATM

IPoA encapsulation on the U-interface in legacy ATM access networks is predominantly applicable to business users. In such cases, the business user typically has a subnet between the RG and the BNG [25]. IP addresses used in RG network are exchanging using typical routing protocols that run over the ATM PVCs.

Migrating to an Ethernet based network, this model must continue to be supporting, which is done with an IPoA Interworking Function.

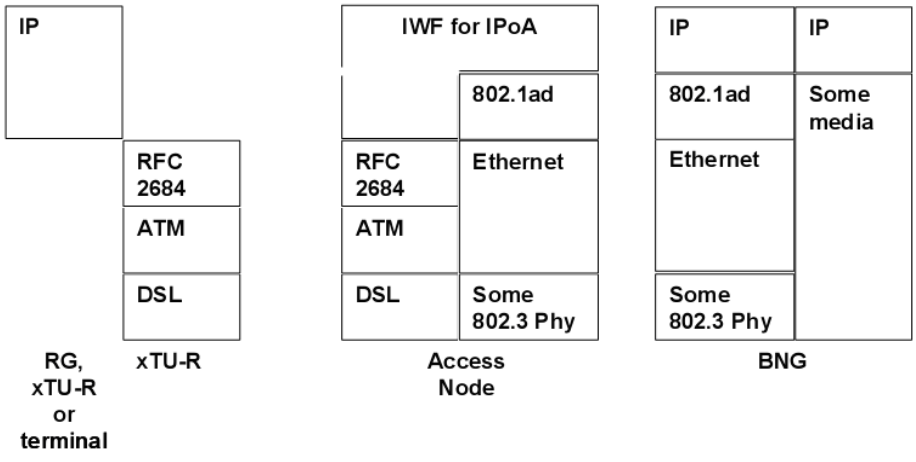

Figure 10 - End-to-end protocol processing for IPoA access
Source: TR-101 [21].

PPP over ATM

The PPPoA access method is not layered on top of Ethernet, the Access Node has to convert the PPP frames to Ethernet protocol and then forward them as PPPoE. The approach taken is to perform conversion between PPPoA and PPPoE at the Access Node.

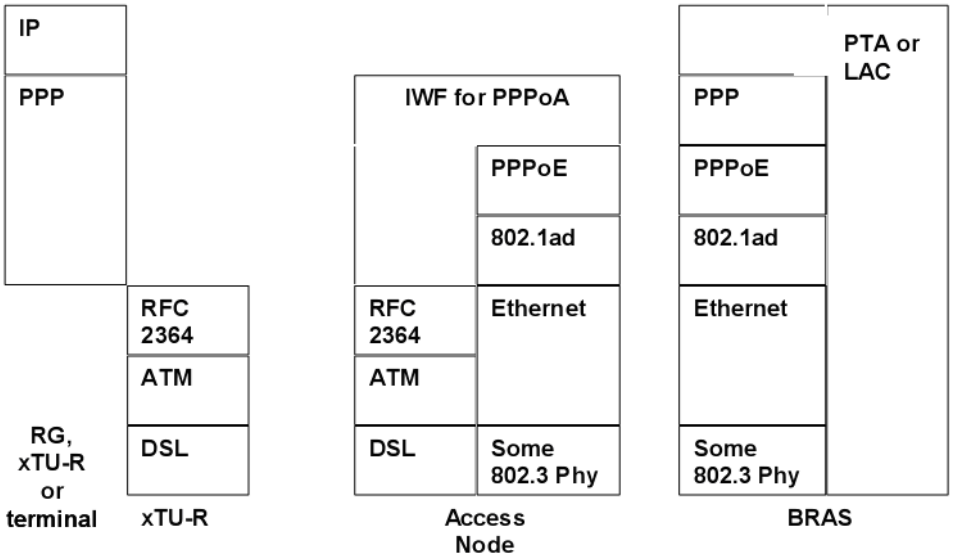

Figure 11 - End-to-end protocol processing for PPPoA access

Source: TR-101 [21].

3.4.5.4. Additional Security Features

Typically, Access/Aggregation Network must prevent problems related to the Ethernet Mac Spoofing and Denial of Service attacks, at the same time that ensures the mapping of services to the customers. Using trusted agents in the Access Node (AN) for PPPoE and/or DHCP and applying Ethernet MAC Level policies to block malicious customers (ie, protecting against MAC spoofing and MAC flooding), can solve some of these typical problems.

Techniques used are the implementation of PPPoE Intermediate Agent (for PPPoE) and DHCP Relay agent (for DHCP) at the Access Node, which adds DSL Forum tag and Option 82 (respectively). This options contains (and must be filled by AN) with Agent Circuit ID and Agent Remote ID with Access Loop ID.

There are also techniques to protect ARP and IP spoofing that are applied at the AN.

3.4.5.5. Access Loop Identification and Characterization

For service management and QoS purposes TR-101 make use of a technique to communicate to BNG the DSL loop status. This technique is basing on an extension to PPPoE/DHCP packets: using PPPoE Intermediate Agent and DHCP Relay Agent (referred in section "Additional Security Features") that adds access loop characteristics (encapsulation, syncrate) and send it (forward) to the BNG. In turn, BNG sends the Access Loop information to the RADIUS server [26].

3.4.5.6. Multicasting

Multicasting characteristics and goals is to try to ensure efficient use of network resources by transmitting only one copy of a multicast packet over a link connection at time, using packet replication if necessary at nodes where links divergence exists. TR-101 has optimized the architecture for multicasting and the affected main devices are four: the CPE as it multicasts into the home network; the access node; the aggregation network; and the BNG. Figure 12 highlights the scope of multicasting in TR-101, which point out the four points referred.

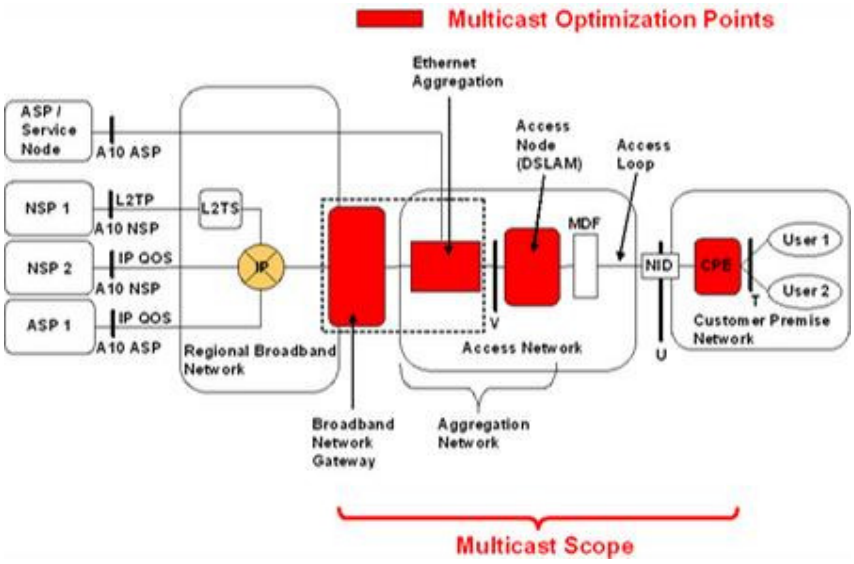

Figure 12 - Multicasting in TR-101 - Architecture with optimization points scope
Source: Light Reading [16].

TR-101's approach for multicasting is based on the following:

- N:1 VLAN used for multicast data delivery (known as "multicast VLAN").

- IGMPv3 [15] processing for resource-efficient IPTV support. IGMPv3 uses proxy-routing on the routing gateway; transparent snooping with or without proxy-reporting on the access and aggregation nodes (with Source Specific Multicast (SSM) support [27] – source IP address matching); and router and PIM/SSM [28] on the BNG (PIM – Protocol Independent Multicast).
- Multicast policy management centralized, with channel-specific access control handled by the IPTV middleware.
- Multicast source may be a distinct BNG, and snooping and proxy at access node summarize customer requests.
- Coordination of access loop state with the BNG(s) when required, handling the gathering of statistics, and dynamically adjusting hierarchical schedulers in the BNG.

N:1 VLANs are an important building block of the TR-101 architecture, defined as: many-to-one mapping between subscriber ports and VLAN. Subscriber ports may be located in the same or different access nodes. Essentially, they are normal VLANs because they group together multiple subscribers into one logical VLAN, typically on a per-service or per-ISP basis.

So, for residential N:1 VLAN users, traffic is single-tagged with an S-Tag throughout the aggregation network. Each subscriber port can handle multiple sessions that can be carried in different VLANs, and the S-Tag can be common to more than one subscriber port or session. S-tag can be used by a large group of subscribers because the access node and access network can maintain isolation between subscriber sharing the same service.

Figure 13 shows how IPTV multicasting could be handled within the TR-101 architecture, using a dual edge (although this is optional) to split off the video services. ASP feeds IPTV multicast streams from the video server to the video BNG using core network. The video BNG is the key point of insertion into the aggregation / access network. STB traffic is sent/received to/from ASP (solid line). However, the per-subscriber control traffic is kept distinct from the multicast traffic, and typically is forwarded through the primary broadband network gateway (broken line).

Note that, TR-101 is not responsible for the definitions of IPTV service layer standardization, as example, Digital Rights Management and Middleware.

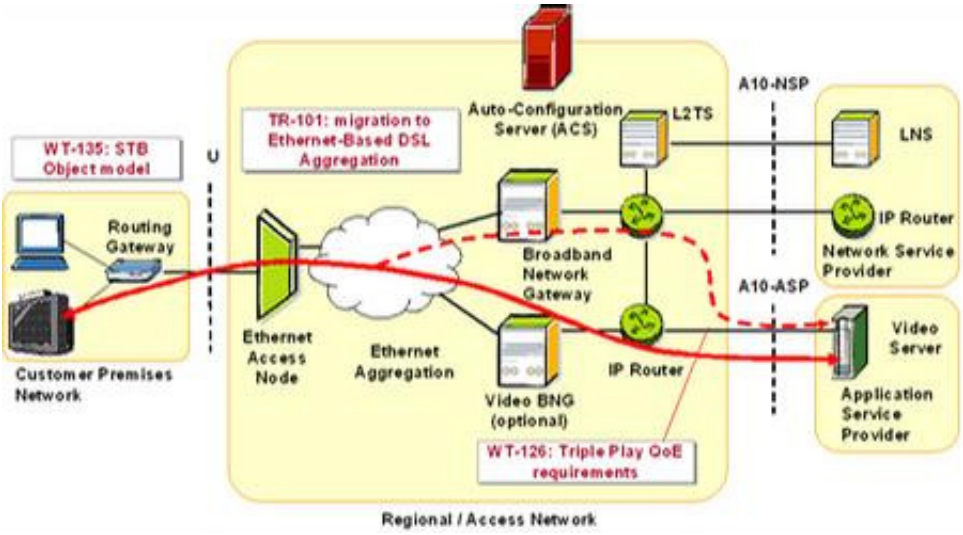

Figure 13 - IPTV Application Based on TR-101 & Associated Multicast Capabilities
Source: Light Reading [16].

Figure 13 also highlights a few other aspects of the DSL Forum architectures – for example, the notion of an auto configuration server, the work on triple-play requirements, and the work on set-top-box object models. Information related to this standardizations (WT-126 "Triple Play Quality of Experience (QoE) Requirements and mechanisms"; and WT-135 "Data Model for a TR-069-enabled STB") can be found in [3], and are not discussed in this document.

3.5. Summary

Following picture represents a summary of the functionalities that TR-101 purposes for each main device of the Access and Aggregation Network in the TR-101 Architecture.

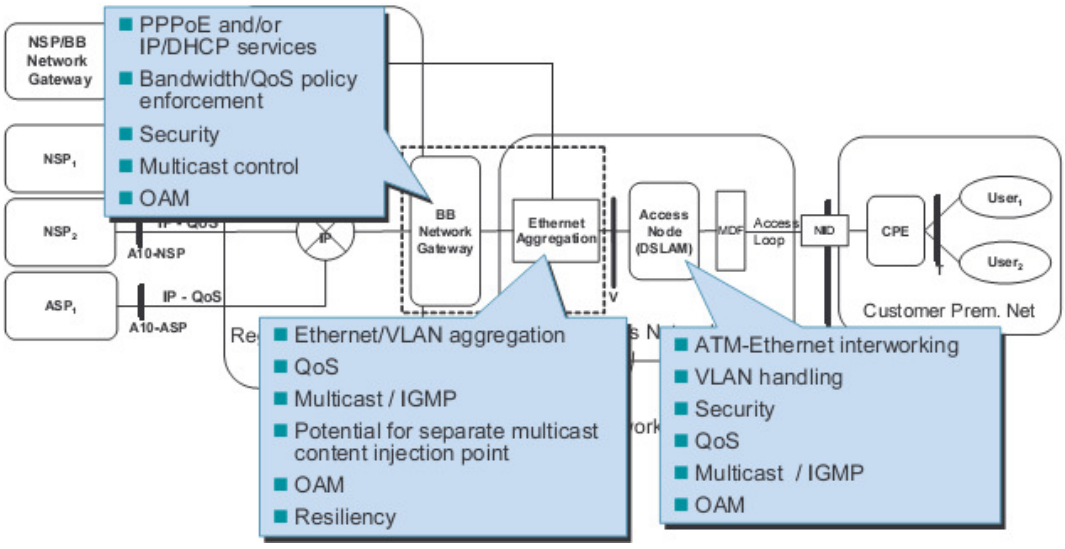

Figure 14 - Summary of TR-101 proposal for Access/Aggregation Network
Source: IPTV Architecture overview [57].

The main functionalities related to the access node are:

- ATM to Ethernet Interworking,
- VLAN,
- Security,
- QoS,
- Multicast / IGMP,
- and OAM.

Chapter 4: mDSLAM-48

4.1. Overview

mDSLAM-48 is an IP DSLAM of PTInovação's "MediaDSLAM" (mDSLAM®) family [30], that answers to the quest for increasing bandwidth in order to support Multimedia applications and Higher Speed Internet access.

This IP/Ethernet based solution brings flexibility and efficiency to the service providers that traditional ATM solutions cannot. IP solution enables the optimal provision of, for example, triple-play services, and high-speed Ethernet interfaces enable video on demand provision.

mDSLAM® family covers a wide range of application scenarios, offering different configurations according to different requirements.

A stand-alone unit, mDSLAM-48, that supports up to 48 subscriber lines with support for ADSL/ADSL2/ADSL2+ (annex A and B) and two electrical and optical Gigabit Ethernet (GBE) uplink interfaces.

Figure 15 - Media DSLAM 48 Box
Source: Media DSLAM / MSAN – Users Manual [33]

A modular unit, mDSLAM-240 composed by one (or two redundant) management and switching boards, 5 line cards slots and 5 splitter slots. Each line has support for 48 xDSL ports, which allow entire system to support up to 240 subscriber lines. Each aggregation board offers 4 GBE Small Form-Factor Pluggable (SFP) optical or electric, and more 5 GBE electric interfaces.

Another modular unit, mDSLAM-480, that is composed by one (or two redundant) management and switching boards, 10 line cards slots and 10 splitter slots. Entire system

offers xDSL service up to 480 subscriber lines. Each aggregation board offers 4 GBE (optical or electrical) uplink interfaces.

The next sections contain a detailed description of stand-alone unit product of mDSLAM® family, over which the work presented on this thesis, was focussed. Triple-play tests are related to the unit Media DSLAM-48 (also known as mDSLAM-48).

Sections 4.2 and 4.3 present the hardware and software architecture overview. Chapter 4.4 overviews main packet capabilities of traffic treatment and triple-play main service enabling features. This information is based on Media DSLAM 48 Application Notes [31].

4.2. Hardware Architecture

mDSLAM-48 main unit (as known as Line Card - Figure 16) is architected as shown in Figure 17.

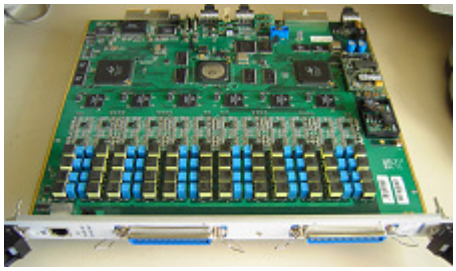

Figure 16 - mDSLAM-48 Line Card
Source: Media DSLAM / MSAN – Users Manual [33].

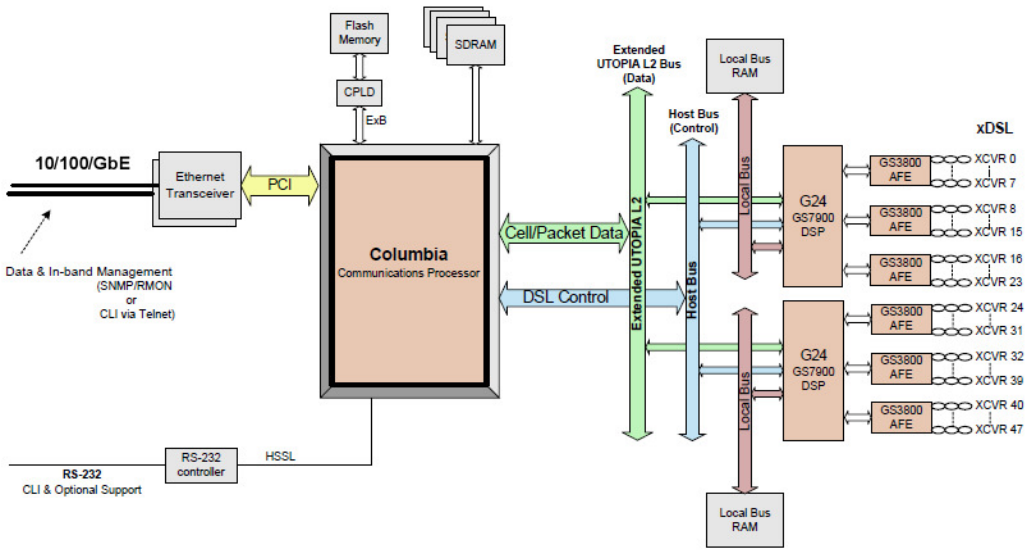

Figure 17 - Functional Block Diagram of mDSLAM-48 main unit
Source: Conexant Application Notes [37].

- Columbia, Conexant's DSL Communication Processor [36], is a RISC-based device specifically optimized for implementing channel aggregation, protocol processing, and Layer 2/3 functions of intelligent DSL systems. (Technical Documents can be found in [36] and [37]).
- Two Optical and Electrical Gigabit Ethernet interfaces, provided via processor's PCI interface and an external Ethernet transceiver chip.
- Forty-eight ports of xDSL are provided by two Conexant G24™ transceiver chips ([36] and [37]).
- One RS-232 port that support CLI interface.

Splitters Unit

Splitters unit is a card that is used to split low (POTS service) from high frequencies (ADSL service) and is connected to POTS lines. It is composed by low-pass and high-pass filters to direct analogue voice to POTS lines and DSL signals to main the processing card.

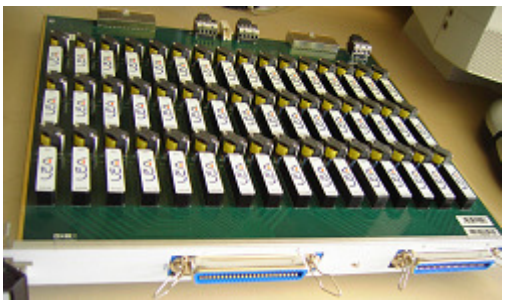

Figure 18 - mDSLAM-48 Splitters Unit

Source: Media DSLAM / MSAN – Users Manual [33].

4.3. Software Architecture

Conexant's Columbia is a multi-processor architecture packet based processing device. One of the processors on the chip is dedicated for control and management functionality and the other processors provide line rate packet processing without involving the control processor.

For both purposes, exists dedicated software for each one:

- Control Plane (CP): protocols component, which defines the direction and purpose of data movement once per session. Typically is Software implemented.

- Data Plane (DP): protocols component, which defines the contents used to decide data movement between systems (in each Packet). Typically is implemented in Hardware.

Figure 19 illustrates a high level view of the multi-processor and the its software mapping.

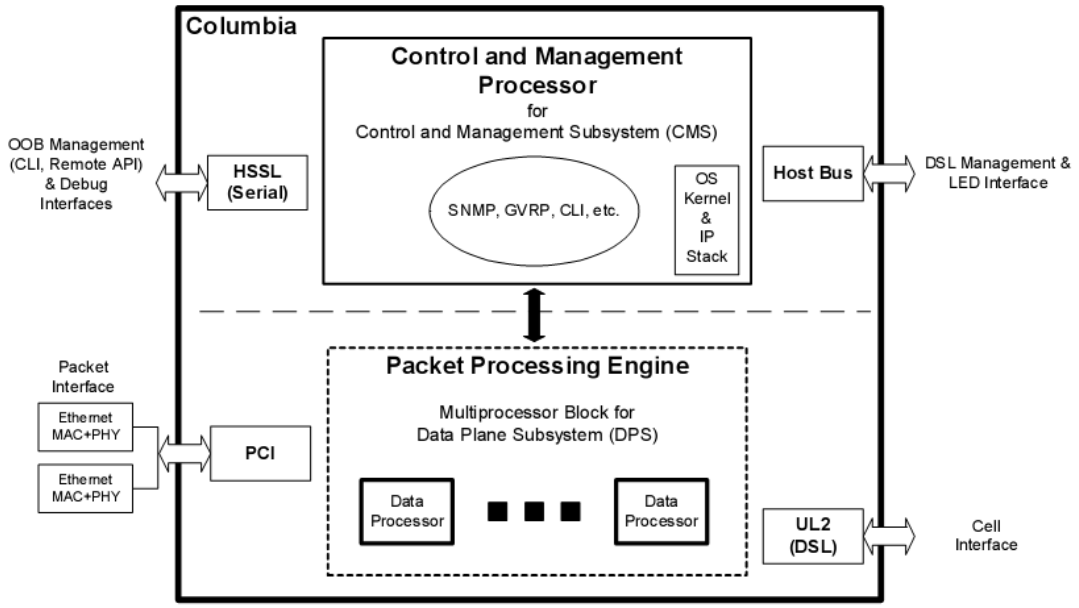

Figure 19 - Columbia Interfaces and Software Partitioning
Source: Conexant Application Notes [37].

Overall architecture of control and management software is illustrated in Figure 20.

- The Control and Management System (CMS) is composed by Agents, the Open Device Driver Framework subsystem, the DSL PHY Management subsystem and the Operating System Services.
- The Data Plane microcode handles ATM and Ethernet physical interfaces and the AAL5, EOA and Bridge subsystems.

Detailed information can be found in [37].

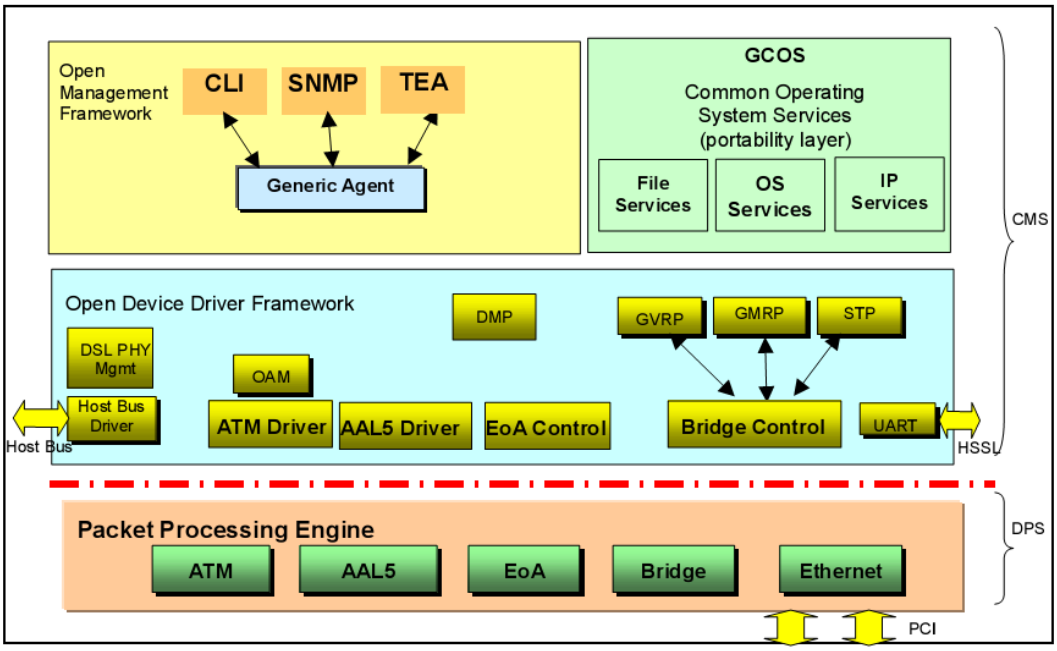

Figure 20 - Management Software Architecture
Source: Conexant Application Notes [37].

4.4. Service Enabling Features

This section presents the main packet features supported and developed in mDSLAM-48. Protocol support is summarized below, followed by sections describing capabilities that focus on packet-based DSL applications. General overview of Link Aggregation, DHCP Relay Agent, PPPoE Intermediate Agent, IGMP Snooping and QoS functionalities, which are elementary to enable the correct triple-play services are also presented in this section

4.4.1. Key Features and Protocols

Main protocol key support and features are:

- RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 [38];
- IEEE 802.1D [39] compliant Ethernet bridging (spanning tree protocol (STP) and 802.1P priority and traffic classes);
- IEEE 802.3ad Link Aggregation [40] (LACP and static link aggregation);
- Rack and stack support across multiple Ethernet uplinks;
- IEEE 802.1Q Virtual Bridged Local Area Networks (VLAN bridging) [41];
- Static VLAN group and membership management;
- Dynamic group and membership management using GVRP (GARP VLAN Registration Protocol) [41];

- Static multicast group and membership management;
- Dynamic multicast group and membership management using GMRP and IGMP;
- MIB support for IETF RFC 2662 ADSL Line MIB [42], IETF Line Extension MIB (Draft), and ADSL Forum TR-024 DMT Line Code Specific MIB [43].

4.4.2. Ethernet Bridge Mode

In packet-based applications where the uplink transport is Ethernet and the service delivery mode is ATM/DSL in – Ethernet out (Cell-in / Packet-out), mDSLAM-48 performs traffic aggregation/de-aggregation and in the current implementation can be configured to operate in "Bridge" mode. mDSLAM-48 primarily performs layer-2 processing by implementing Ethernet Bridging (learning and forwarding), and provides the following capabilities:

- Traffic Classification and Prioritization
- Packet filtering – based upon Layer2, Layer3 and higher layer fields
- Multicast Support (with IGMP snooping and GMRP)
- VLAN support (with GVRP)
- QoS features: Queuing and Scheduling of packets

The two Ethernet PHY devices can be configured as follows:

- Rack and Stack - One of the Ethernet port is used to connect to the Service Provider's. The other connects to a stacked box (daisy-chain);
- Bonding - The two Ethernet uplinks are used as a single (logical) higher speed link (link aggregation).

4.4.3. Bridging Functionality

4.4.3.1. ATM features supported

The following ATM features are presented in mDSLAM-48 system:

- 48 DSL subscriber lines (48 CPE ports);
- supports up to 8 Virtual Circuits (VCs) per DSL port;
- end-to-end and segment F5 OAM cells (OAM support as ITU-T I.610 [6]);
- configuration of the maximum packet size received on the CPE interface;
- CPE-side EoA interfaces support AAL5 layer.

4.4.3.2. Packet Formats Supported

All packets exchanged over ATM are encapsulated as specified in RFC 2684 "Multi-protocol encapsulation over ATM" (update of RFC 1483) [38] before being encapsulated in an AAL5 PDU as defined by the International Telecommunications Union (ITU) standard I.363.5 (see sub-section 4.4.3.3 for additional information of ATM to Ethernet tunnelling of IP and PPP protocols).

Packets exchanged by Gigabit Ethernet interfaces support both the Ethernet2 and the IEEE 802.3 Ethernet standards for transmission and reception of frames.

4.4.3.3. Interworking Function

IP Over ATM

As mentioned in last sub-section, AN function as bridging based solution, however, RFC 2684 Routed [38] (IPOA) must be supported with existing RFC 2684 Bridged [38] Ethernet interfaces. Direct support for routed interfaces is not presented directly on Access Node (AN) software (because it is essentially a bridge). IPOA to IPOE tunnelling, also known as IPOA Interworking Function (IWF), provides support for the termination of IPOA traffic on CPE side and tunnel it towards WAN side Ethernet interface (upstream direction).

Downstream direction can be implemented in two based configurations:

a) limited IP address lookup (route traffic to IPOA interface);
b) MAC address / VLAN lookup without layer 3 IP Address lookup for the IPOE interface on the CPE side.

PPP Over ATM

For this purpose AN encapsulate PPP packets over ATM received from CPE in PPPoE and forwards it to the BBRAS and vice-versa. It is implemented in four steps:

1. PPPoE Session Establishment
2. PPP Session Establishment
3. Data Forwarding
4. Session Tearing Down

1. PPPoE Session Establishment

CPE tries to establish a PPP session sending LCP configuration request. A generic filter rule needs to be applied to forward these LCP packets coming from CPE side to the control plane. Control plane maintains LCP configuration request and, establishes a corresponding PPPoE session (exchanging PPPoE discovery packets with BRAS), using parameters configured on the PPPoE interface.

For session establishment, it is required the following parameters:

- Source MAC address on each PPPoE interface (MAC address profile – similar to the one used on IPOE interface)
- Service name, that corresponds to established section.
- Virtual Vlan Id

2. PPP Session Establishment

After PPPoE session establishment, PPP connection is established between CPE and BRAS. AN sends the latest LCP packet stored to initiate the session, after encapsulating it into the PPPoE packet. In this stage, PPP LCP Packets are forwarded from CPE to BRAS after encapsulating it them into PPPoE packets and vice versa. Remain PPP configuration packets are forward only by data plane

3. Data Forwarding

Forwarding is done by data plane only.

Upstream direction: PPPoA packets are encapsulated in PPPoE packets and sent to Net side. PPPoE packet, contains source MAC address as configured on the PPPoE interface, BRAS destination MAC address (collected after session establishment), Port SVLAN id in of the BP mapped to PPPoE interface and session id allotted by BRAS

Downstream direction: PPP packets encapsulated in the PPPoE packets are received from the NET side. The S-VLANID (and C-vlan Id), PPPoE session Id, Source MAC address and Destination MAC addresses of these packets are used to find the corresponding PPP interface (after removing the PPPoE header packets are forwarded).

4. Session Teardown

When CPE or BRAS side tries to teardown the PPP session, AN tears down the PPPoE session on the WAN side. CPE can tear down the session by sending LCP terminate request. After receiving this LCP tear down request, AN marks the session down and sends the LCP terminate request with a PADT packet to BRAS. BRAS can tear down a session by sending either PADT or LCP terminate request. After receiving any of these packets AN mark the session down and send the LCP terminate request to the CPE.
A session can also teardown if:

- All of the NET side ports go down for *wandntmrintrvl* number of seconds
- The operational status of corresponding ATM VC is remains down for *lowiftoggletimerto* number of seconds
- There is no activity during that session for *inactivitytmrintrvl* number of seconds.

4.4.3.4. Address Learning

MAC Address Learning / Limits

System is capable of performing dynamic MAC address learning by looking at the packets coming in on its various ports, or static address addition, deletion and modification.
Disabling learning on a per port basis along with the static configuration can be used to allow one or more preconfigured devices to access the network using the DSL channel.

System can limit MAC address learned or statically configured entries. Beyond the number of learned MAC addresses limited on EoA (BP) interface, it is possible to configure the maximum number of MAC entries in the complete system, in all CPE ports together, and from downlink port (in rack and stack configuration).

mDSLAM-48 supports *aging out* of dynamically learnt entries in the Address Learning Table. This allows un-used entries in the Address Learning Table to be purged when they have not been used in a period.

Packet Dropping When Either Maximum Is Exceeded

At run-time, when system receives a packet with a new MAC address, it checks to see whether either number (configured maximum number of total MAC addresses OR the

configured maximum number of MAC addresses on this port) has been exceeded. If so, it drops the new packet and increments a counter. If neither limit has been reached, it proceeds to learn the new MAC address.

4.4.3.5. Packet Forwarding

Upstream packets received from the downlink and CPE ports are forward to the NET port by means of a trivial forwarding decision. A forwarding lookup is perform in the MAC Address Learning Table using the VLAN tag and destination MAC address for packets received from the NET port in the downstream direction. Unicast packets are forwarded to one of the CPE ports, the downlink port or the Control module based on the destination address of the packet.

If the forwarding decision fails for a Unicast address, one of two actions can be taken – flood the packet on ports or drop the packet. Dropping of Unknown packets may be desirable if all transactions are initiated by clients at CPE ports. In this case, the client's source address is learning first in the forwarding table. Packet discarding is also appropriate when learning is disabled on all ports and only static addresses are being used.

Flooding may be done if the expected number of unknown packets is small, and the resulting traffic load is acceptable.

In order to control the amount of broadcast traffic, it is possible to determine whether downstream broadcast traffic is to be forward to all ports, or dropped. Broadcast packets received in the upstream are always forwarded to the uplink interface, if not filtered.

A multicast packet can be sent to more than one entity at the same time, accordingly to the IGMP snooping and multicast configuration.

4.4.4. VLANs

4.4.4.1. Characteristics

VLAN support is an integral part of the software. The VLAN tag carries two kinds of information – the VLAN Identifier and the Priority. Both information fields are use by system in order to provide VLAN and Priority support.

This section describes the VLAN features available in the software, while section 4.4.7 below describes the QoS features that use the Priority field in the VLAN tag.

Follows the main VLAN features related supported by mDSLAM-48:

- Number of VLANs supported comply the range of 12-bit VLAN identifier (maximum VLAN ID value as 4095). This allows the service provider to have different VLAN configurations in the system, exploiting VLAN features of security, reduced traffic etc.
- SVL, IVL and SVL/IVL: three types of VLANs accordingly with IEEE 802.1Q [41] – shared VLAN learning, independent VLAN learning and a combination of both.
- Port Based VLAN. It assigns a pre-defined VLAN tag to every packet that from bridge port of CPE before sending the traffic upstream. In the downstream direction, it performs a lookup based upon the (VLAN-Id + destination MAC address). Before sending the packet to the downstream port, it strips the VLAN tag from the packet.
- Multiple VLAN Membership per Port: ability to receive VLAN tagged packets from the Ethernet ports, and a single CPE port to be a member of more than one VLAN. An example is: all voice traffic is delivering by one VLAN, all data traffic is another VLAN, and multicast traffic is one other VLAN and so on.
- Frame Transformation: Untagged frame to Tagged frame or Tagged frame to Untagged frame, which allows the CPE devices to be either VLAN aware or unaware. Similarly the uplink Ethernet device could also be VLAN aware or unaware.
- Maximum number of multicast entries is shared across all VLANs. However, if IVL is used, the same MAC address may belong to different VLANs and may have different group memberships.
- Ingress and Egress Filtering specified by the IEEE 802.1Q standards, by bridge port basis. This enables the bridge to do filtering of input frames, in order to prevent the injection of traffic for a given VLAN on a port on which VLAN is disallowed. By configuring the "acceptable frame types" parameter, bridge can filter frames to prevent the injection of untagged and priority tagged frames on a port on which the reception of untagged and priority tagged frames is disallowed. With Egress filtering along with forwarding logic, the bridge adds and removes tag header from received frames, according to the outgoing port capability.
- Traffic Class Table Configuration: enables the bridge to classify frames into traffic classes in order to expedite transmission of frames generated by critical or time-sensitive services. Traffic Classes and their use are defined in [41].

4.4.4.2. VLAN Stacking Implementation

Access node supports VLAN stacking (Q-in-Q). On a broad level, AN can be configured in one of the following modes:

1. Native Mode: confirms to the normal 802.1Q VLAN support and the system works as is in the model without VLAN stacking.
2. Stacked Mode: VLAN used in VLAN aware networks based on 802.1Q bridging is called C-VLAN (Customer-VLAN), and can be uniquely identified by a C-VLAN tag. VLAN that encapsulates Customer traffic in Provider network is called S-VLAN or Service VLAN (stack VLAN) and is identified by an S-VLAN ID, used as second VLAN tag (bridge port that is connected to provider network is named as *provider port*.

Virtual VLAN

A Virtual VLAN is an abstract configuration with tagged/untagged port member and all other attributes of a VLAN. This may be associated with a S-VLAN and C-VLAN tuple to map these attributes to the pair. If multiple service providers need different behaviour for same C-VLAN, the forwarding space is defined by a S-to-C VLAN combination, which will determine the forwarding behaviour.

In VLAN stack mode, the entire configuration that is supported for a VLAN will be mapped to a virtual VLAN. (The advantage of this abstraction is that all types of customers can be supported simultaneously and the number of Virtual VLANs in the system can be limited only by the available memory.)

Internally, access node performs bridging operations like Ingress VLAN Filtering, Learning, Lookup and Egress VLAN Filtering, on the Virtual VLAN Index. The Virtual VLAN is determined from the C-VLAN and S-VLAN. Lookup, learning, and VLAN filtering, if required, are performed in C-to-S VLAN combination space.

Differentiation of ports

Each port is classified as either a provider port (connected to provider network) or a non-provider port (connected to customer network).

- Over provider port the data frames are transmitted and received with S-VLAN tag.
- Over non-provider port the data frames shall be transmitted and received as either untagged frames or having C-VLAN tags.

Management VLAN

Particularly, Management VLAN and management S-VLAN can be specified at the Ethernet interface level. If not specified, the system considers PVID and PSVID of the bridge port (*gvrp* command in sub-section 5.4.1) on this interface as Management VLAN and S-VLAN respectively. By default, the PVID and PSVID of any port are {1, 1} respectively, implying that the management VLAN and management S-VLANs are by default 1 and 1 respectively.

Both S-VLAN and C-VLAN shall be used for Management in VLAN stack mode. The management S-VLAN and its priority to be used is configurable. Hence it is possible to manage access node from the provider port through one of the following options:

1. If user specifies management VLAN and management S-VLAN (optional in Ethernet creation), these values prevail over PVID and PSVID of the port over it;
2. Double Tagged Frame – Through double tagged frames where both S-VLAN Id and C-VLAN Id are specified;
3. Single Tagged Frame with S-VLAN ID – Through double tagged frames where only S-VLAN ID is specified, C-VLAN Id can be assumed to be the PVID of the port. In this case, if PVID of this port is different from the management VLAN specified in the lower Ethernet interface, then packets will be dropped. So the user is required to either make a match or should not specify management VLAN at Ethernet interface level.
4. Untagged Traffic – Untagged traffic for management is supported only if PVID and PSVID of the bridge port on the Ethernet interface are same with management C-VLAN ID and management S VLAN configured at the Ethernet level; otherwise, it is dropped.

4.4.5. Rack And Stack

Rack and Stack is a feature that allows customers to subtend mDSLAM48's. This feature allows multiple boxes to share a single uplink to the Service provider/Ethernet switch.

Traffic from the devices further down the chain, travel up (the chain) to the first device and are then forwarded to the uplink interface. Data traffic arriving from the stacked device

CPE ports is switching to the uplink Ethernet port and traffic from the uplink port is switching to the stacked device.

4.4.6. Link Aggregation

mDSLAM-48 supports up to two optical and electrical GBE interfaces for data traffic (and in-band management). These Ethernet links can either be used as two independent links (one as uplink and the other as downlink - see 4.4.5 above), or used as a single logical link having twice the capacity.

Access node supports dynamic link aggregation (LACP based) or static link aggregation (static bonding):

- LACP based aggregation is the implementation of the IEEE 802.3ad specification of Link Aggregation which includes the LACP protocol [40]. If LACP is defined, the device at the other end of the aggregated Ethernet links also needs to implement and run the LACP protocol. The protocol provides for dynamic changes to the aggregator configuration such as addition/deletion of Ethernet interfaces, without operator intervention.
- When using static bonding, once LACP is not used, no LACPDU is exchange and hence dynamic reconfiguration is not possible. The interfaces to be aggregate are specifying statically and changes are not possible without manual reconfiguration by the operator.

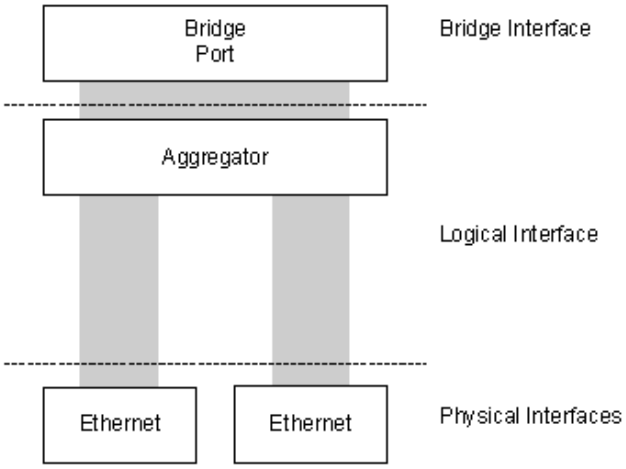

Figure 21 - Link Aggregation

Source: Media DSLAM Application Notes [31]

In both cases, if one interface of the aggregated links fails, the traffic is re-distributed amongst the remaining available link and when the failed link is restored, traffic is again re-distributed. This happens automatically in both cases without operator intervention.

4.4.7. QoS

Quality of Service (QoS) support provided by system in Packet application includes input rate limiting, congestion management, scheduling (Weighted Fair Queuing (WFQ) / Priority), output port rate limiting, traffic classification, regeneration, and prioritization. It is applying in the upstream and downstream flows, where the input is classified into multiple flows and QoS can be controlled by flow.

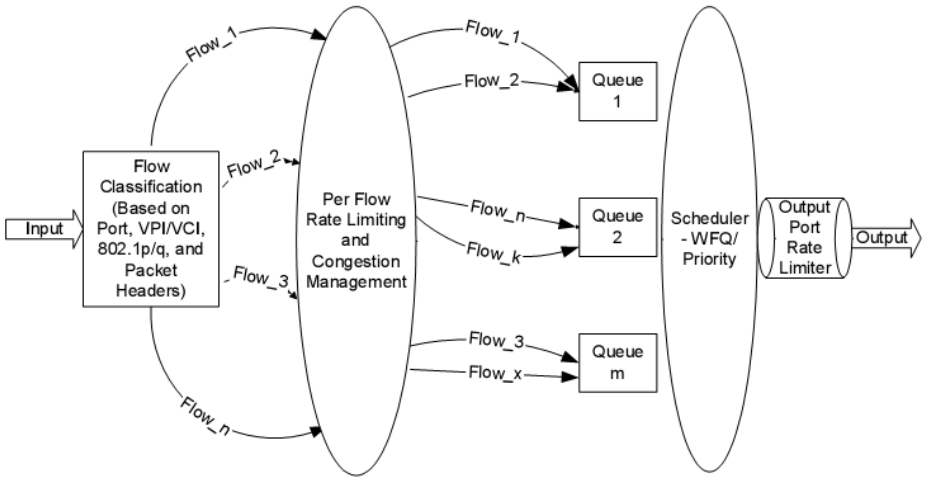

Figure 22 - QoS for Downstream and Upstream Flows
Source: Conexant Application Notes [37].

Figure 22 shows the QoS for upstream and downstream flows in the system.
Some of the functionalities such as rate limiting are not explaining because they are not TR-101 requirements. However, detailed information is in [37].

The cells received from the DSL port (upstream traffic) are classified into various flows. The fields considered for classification include input DSL port, VPI / VCI, VLAN Id and 801.2p priority. The classification criterion is extending to include other fields in the packet such as Diff Servicing Code Point (DSCP). The input rate limiter can control the maximum bandwidth consumed by a flow. If system is experiencing congestion, the congestion manager controls the traffic for this flow and provides support for preventive

measures e.g., Random Early Detection (RED [44]). The traffic from one or more flows is then queued. For the transmit direction, packet transmission on the upstream ports is controlled by the output port rate limiter. If a packet can be transmitted, it is selected from the packet queues using the WFQ algorithm. There can be a maximum of eight queues in the upstream direction towards the Ethernet interface.

The traffic received from the Ethernet port (downstream traffic) is classified into various flows. This classification is based on Destination MAC, VLAN Id and 802.1p priority fields. The classification criteria can be extended to also include other fields in the packet such as DSCP. In case of Multicast and Broadcast, packets may need to be sent to multiple DSL ports. These packets are assigned to multiple flows and QoS is processed independently for each flow. It is likely that priority queuing is configured in the downstream direction on each port and the number of queues is restricted to 3 or 4.

Priority Regeneration

Priority Regeneration is defined as specified in IEEE 802.1p [39]. Each bridge port is associated to a priority-mapping table. Each priority in the incoming tagged packet is mapped in the priority-mapping table with a new priority, which is used in all subsequent processing of the packet inside AN. In that case, packet is modified to reflect the new priority assigned.

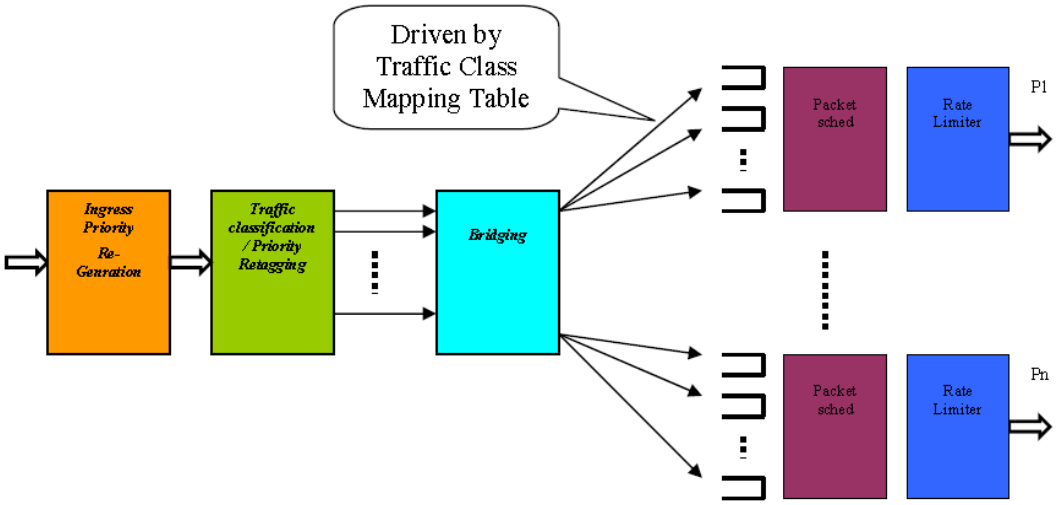

Figure 23 - QoS Handling of downstream traffic

Source: Conexant Application Notes [37]

If no priority-mapping table is configured the priority associated to the packet remains the same.

It is possible to configure a default priority, if AN receives untagged (0 as default).

Traffic Classification and Prioritization

Packet filtering/classification module allows the segregation of incoming traffic into different flows. The processing is driven by user defined rules (users can configure the policies that should be applied in order to classify the traffic).

Typically, filtering / classification is done in the ingress – although the AN allow limited filtering / classification on the egress direction to.

Output Rate Limiting

It is possible to limit the output rate on a DSL port (specified on the ATM port).

Egress Packet Scheduling

In each bridge port – a separate traffic class mapping table is supported – which determines the queue where a packet should be placed - based on the regenerated priority of the packet and traffic classes on the egress port.

Maximum of eight queues per DSL port are supported. The scheduler that serves the queues can be configured to function as:

- Strict Priority,
- Flexibility to define per Queue Minimum Rate Guarantee,
- Flexibility to define per Queue Maximum Rate Limiting,
- Weighted,
- Flexibility to define per Queue Minimum Rate Guarantee,
- Flexibility to define per Queue Maximum Rate Limiting,
- Excess Bandwidth [Port Rate – SUM (Minimum rate guarantee across all the queues)] distributed according to weight assigned,
- Mapping an VC to a Queue.

System provides a separate “traffic class mapping” table for each BP (PVC).

These tables can be configured such that a PVC maps to at most one queue of a DSL port. If the number of PVCs of a DSL port is the same as the number of queues (ie, 8) it can be assured that not more than one PVC is mapped in a queue.

So, system assure ATM like QoS (using ATM scheduler).

Policing

It is achieve using either of the following:

- Per VC IRL,
- Flow based rate limiting.

Per VC QoS

- Configure Dedicated Queue per VC:
  - Using per port traffic class mapping table,
- Configure Per Queue Scheduling Parameters:
  - Minimum Rate Guarantee,
  - Maximum Rate Limit,
  - Excess Bandwidth Sharing Weight,
  - Supporting different ATM traffic classes:
    - CBR – Can be implemented for a Queue with min BW guarantee = max BW guarantee=PCR;
    - UBR – Can be implemented for a Queue with min BW guarantee = 0;
    - UBR+ - Can be implemented for a Queue with min BW guarantee=MCR

    Bandwidth distributions among competing classes for the excess resources are controlling using the weighting based mechanism provided by the Scheduler.

4.4.8. Packet Filtering

Filtering of packets entering mDSLAM-48 from DSL ports or from uplink Ethernet ports ensure security and provide hooks for value add. For the Layer 2 bridge application, packet filtering is provide in a phased manner, ensuring that the basic feature support exists in the initial release of the product followed by support for more complex mechanisms. Also, each filtering rule has a negative impact on the performance of the system as the data packet has to go through multiple processing elements.

Figure 24 illustrates the high level architecture for packet filtering in the system (DPS and CPS refers to Data Plane and Control Plane Subsystem, respectively).

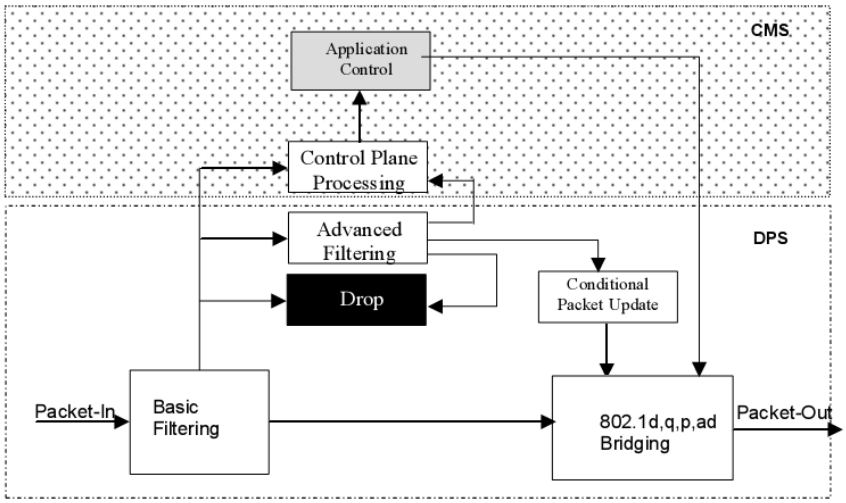

Figure 24 - Packet Filtering Architecture
Source: Conexant Application Notes [37].

The high speed packet filtering blocks implemented in the microcode provide higher throughput but need complex performance optimizations. The control plane processing block is available as a driver in the control/management processor where multiple applications can provide value added filtering.

Typical rules for the basic filtering block are statically configured per port and provide the following functionality:

- All packets on port (VPI / VCI),
- All VLAN tagged packets on port,
- Certain VLAN tagged packets on port,
- All unresolved packets on port (on NET side Ethernet port),
- Broadcast packets on port,
- Multicast packets on port,
- Special MAC addresses (local MAC address).

Filtering capability can be used to filter typical DHCP, IGMP and PPPoE packets that would be processed by the control plane processing layer.

Advanced Filtering and Conditional packet update blocks are implementing in data plane microcode and provide the capability to do multi-field lookup and modifications. The fields of interest are, Ports, MAC address, DSCP, protocol ID, IP addresses and TCP/UDP

port numbers. The rules for advanced packet filtering allow concatenation of multi-field lookup & actions, e.g., one can configure the rule chain as shown in Figure 25. The nesting of rules allows complex filtering to be supported.

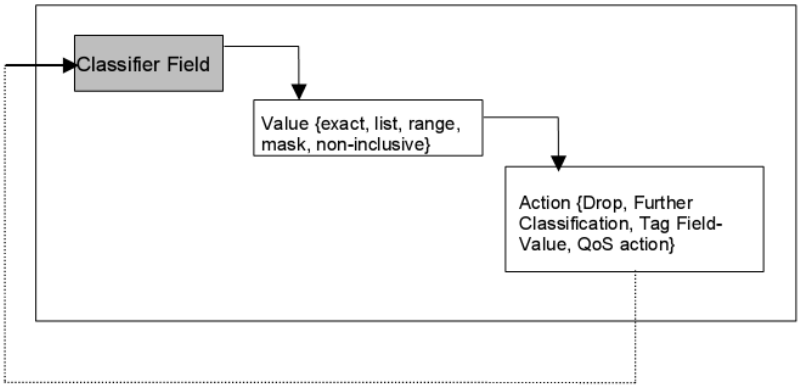

Figure 25 - Packet Filtering rule chain
Source: Conexant Application Notes [37].

4.4.9. IGMP Snooping

IGMP is a communications protocol used to manage the membership of IP multicast groups, which is used by IP hosts and adjacent multicast routers to establish multicast group memberships. Access node software have support for IGMP snooping, which snoops IGMP packets carried in Layer 3, to get desired information, without processing the Layer 3 header. "Snoop" is due to DSLAM is typically a Layer 2 protocol device. Snoop agent learns the ports that want to belong to a multicast group address and populates the multicast forwarding table with that information. With IGMP Version 3, it assures the capability to associate a port to a multicast Group IP and Source IP of the multicast source at protocol level in Control Plane. This enables a multicast receiver host to specify to a router the groups it wants to receive the multicast traffic using IGMP V3.

Access node supports creation of multicast entries in its forwarding table. These entries can be static entries or dynamic entries.
Static multicast entries are entries typically created under management control. These entries remain in the forwarding table until management decides to remove them. These groups membership remains constant until changed through the management interface.
Dynamic multicast entries are entries created under multicast protocol control: IGMP Snooping and Proxy Reporting support. Multicast entries are created when a user wishes to

join a particular multicast group. The membership of these groups is in a state of constant flux and is controlling by the above protocol.

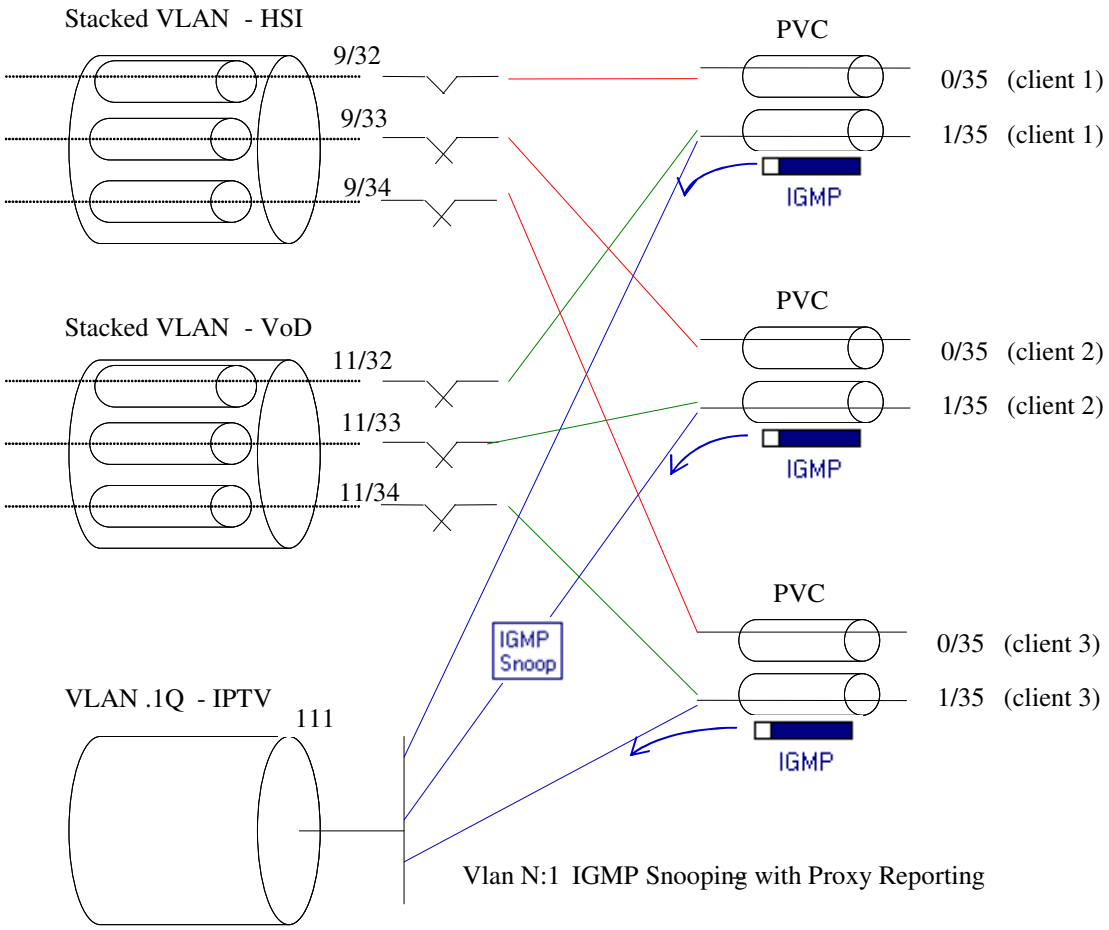

Figure 26 - IGMP Snoop with Multicast VLAN

IGMP Version

Both hosts (DSL side) and multicast routers on upstream ports support IGMP v1, v2 and v3. Supported version is configurable globally in the system.

Multicast Vlan

Access node supports multicast VLAN, which is a concept of sending multicast traffic on one or more designated VLANs identified for multicast, using N:1 Vlans. A multicast VLAN is used for receiving downstream multicast, tagging, sending upstream IGMP reports, and creating layer 2 filtering entries. As illustrated in Figure 26 instead of coming on the same Vlan, IGMP reports come on a 1:1 VLAN mapping, and a software agent

forward (or copy) those packets to a dedicated egress multicast Vlan. Learning is done based on Multicast Vlan and, downstream multicast streams for the same group can be replicated to different subscribers that have distinguished 1:1 VLANs.

Proxy Reporting

Proxy reporting allows the reduction of control traffic on the network and channel zapping delays. Different functions of Proxy Reporting are available:

- Report Suppression: intercepts and summarizes IGMP reports sent by IGMP CPE hosts. Reports are forwarded only if necessary. As example, if the first user joins a multicast channel, IGMP request is sent to upstream, after that, no more "join" reports for that multicast group are sent. For the respective multicast group, AN sends only the response for IGMP queries, or the message related to the last user that wants to remove that channel group (until the "Last Leave").
- Last Leave: intercepts an summarizes IGMP leaves from CPEs. It is sent only, for a multicast group, when the last user quits the referred group.
- Query Suppression: Intercepts and summarizes IGMP queries (from multicast routers). IGMP-specific queries are never sent to subscriber lines, and General Queries are sent to that have at least one Multicast group registered. The response to the Querier is sent by AN.

All original messages from AN (if configured as *ProxyReporting*) have source IP address as "0.0.0.0" and its own MAC address.

Security Related Requirements

A maximum of 1024 entries including both static and dynamically learnt multicast addresses are supported. Multicast MAC address and VLAN identifier identify those entries uniquely. Moreover, following security features are also available

- Maximum multicast limit per port: controls the number of simultaneous channels that can be received by a port.
- Enable/Disable Querier port: control if a port can become a querier or not.
- Version mask configuration: selection of IGMP frames versions supported.
- Rate Limit IGMP frames: limit the number of frames received by subscriber port.

Leave Mode

Leave mode by BP is configurable. Depending on IGMP Snooping configuration as Transparently Snoop or with Proxy Reporting, leave mode behavior differs. So, in Transparent Snooping, exists 2 different leave modes:

- Normal: the leave message is forwarded to a Querier and nothing is done. It is expected that the Querier will send queries after receiving the leave and based on that cleanup will happen;
- Fast Normal: leave is forwarded to the Querier. But for the fast cleanup, group-specific queries are generated by AN without waiting for the queries from the Querier and based on the response, cleanup happens.

In Proxy Reporting, exists 2 different leave modes (independently on the mode, leave is only sent to the Querier if multicast traffic for that group is no more required by any BP in the AN):

- Fast Normal (or Normal): after receiving leave message, AN sends a General Specific Query asking if there are any hosts that want to receive the multicast group, and based on response, cleanup happens.
- Fast: the port from where a Leave message comes is immediately deleted from the group

In case of IGMPv3, there is no designated leave message, but leaving of groups happens through reports indicating state change on Host. Thus, such reports are forwarded if there is a change in state on AN for that Group (detailed information in [15]).

Resuming

- Snoop received IGMP messages to get the corresponding multicast group;
- Support multiple multicast VLANs;
- Update Forwarding table with the Virtual VLAN-ID, Multicast MAC Address and Bridge Port (on which the Report was received);
- Forward Reports to the Querier Port (uplink interface);
- Suppress multiple Version 2 or 3 Reports forwarding for the same multicast group (in the same virtual VLAN) to the uplink port, if report suppression is enabled;
- Proxy reporting by Virtual VLAN, if it is enabled on that Virtual VLAN;

- Age out entries in multicast forwarding table;
- Generate and Forward Queries for ports that are receiving any Multicast groups;
- Statistics.

4.4.10. Access Loop Id and Characteristics

CPEs (subscriber lines) provide last mile connectivity using DSL technology. Access Node terminates xDSL connections and facilitates aggregation and migration to Ethernet technology. Access Network terminates in BNG edge, which in turn, connects to Network Service Provider(s) (NSP) and Application Service Providers (ASPs). Service Provider facilitates infrastructure, backhaul, and application services. Therefore, BNG needs to perform various intelligent functions like AAA, Qos, and Network Management. Port identification of CPE subscriber lines facilitates these functions.

In ATM based aggregation networks, access loop id can be performed in a easy way. Mapping of access loop to ATM PVC between AN and BNG. However, in Ethernet based AN, once ATM PVCs are terminated in AN, BNG can't derive Access Loop ID from "Ethernet" packets. TR-101 solutions, in order to BNG get that information:

- DHCP packets: DHCP Relay Agent (DRA) as specified in RFC 3046 [52];
- PPPoE packets: PPPoE Intermediate Agent (PIA) [21].

On both protocols, AN intercepts upstream packets, append options that identifies access interface (subscriber), remote host, between several information. Typically this is implemented without the changes of destination and source MAC addresses.
The BRAS extracts the Access Loop Identification information from the DHCP request messages for QoS and AAA functions
BNG checks whether PPPoE discovery is allowed for the identified subscriber line (that have influence on PPP authentication phase performed later).

4.4.10.1. DHCP Relay Agent

Typical DHCP negotiation between a DHCP client and DHCP server is illustrated in Figure 27.

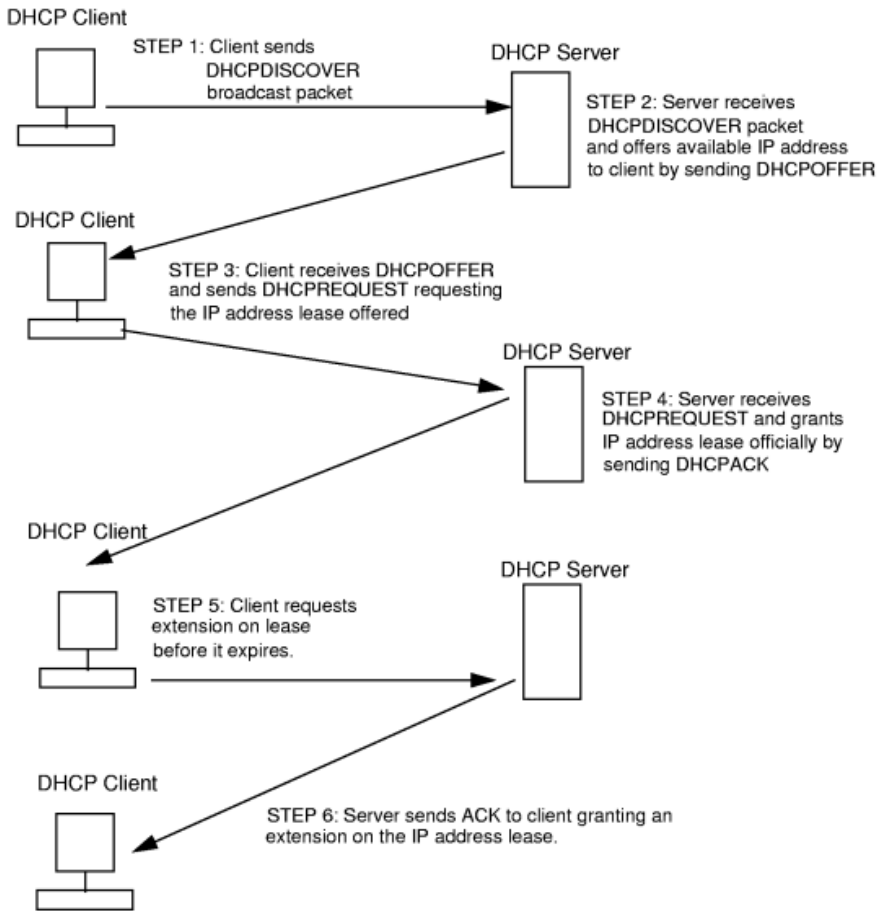

Figure 27 - Typical DHCP negotiation

Source: Hewlett Packard - DHCP negotiation [58]

Relay Agent (Figure 28) inserts in original DHCP requests from client (HGW) option 82 (Remote ID + Circuit ID), and removes option 82 on DHCP responses from server to client. Typically DSLAMs are the entities responsible of DHCP Relay Agent. If DHCP server is option 82 aware, use appended information, and responses to subscribers are sent with the same option 82 received in requests. Option 82 is appended in all packets from subscriber, since first request (step 1) and confirmations (even in step 3 or later in step 5).

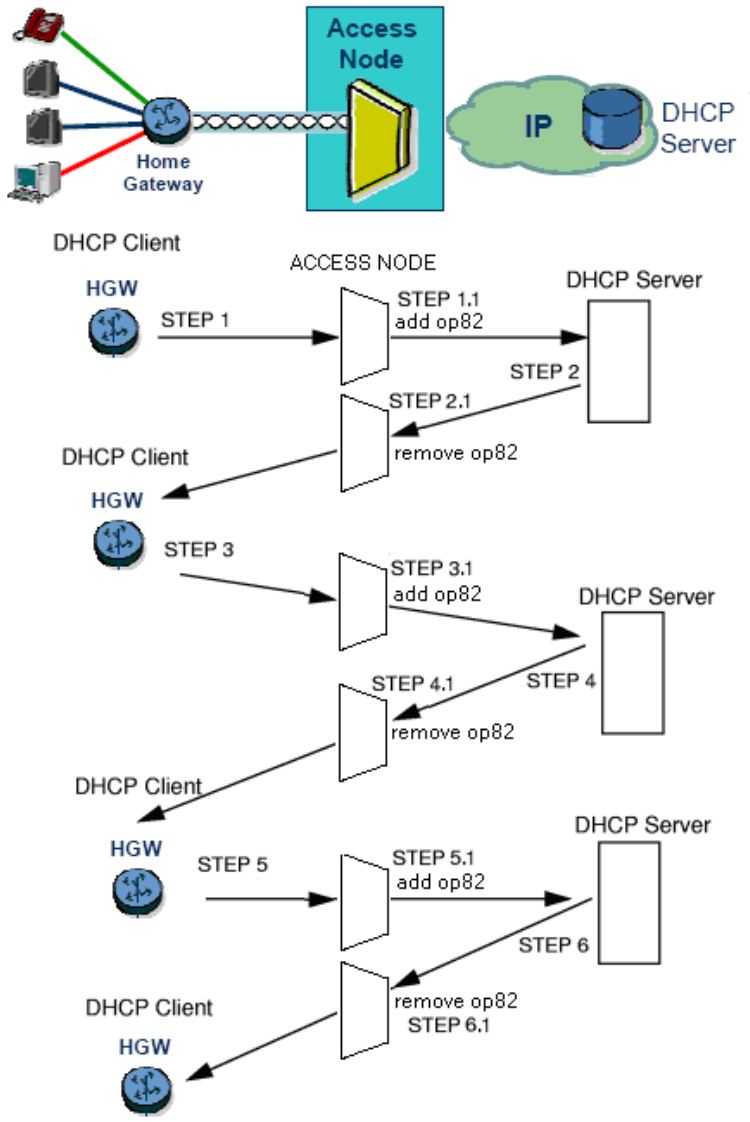

Figure 28 - DHCP negotioation with Relay Agent

4.4.10.2. PPPoE Intermediate Agent

PPPoE is a protocol to support PPP sessions over Ethernet. Sessions are establishing in two different phases: discovery and session. Figure 29 illustrates behaviour explained above. PPPoE Intermediate Agent (PIA) is required in discovery phase (that inserts VSA tag): PADI, PADO, PADR, PADS and PADT packets. Upon reception of a PADI or PADR packet sent by the PPPoE client, the PIA adds a TAG to the packet. TAG contains the identification on which the PADI or PADR packet was received in the AN. After PADS packet, PPPoE Session Stage is ready to be used, and PIA is not required to act in this stage.

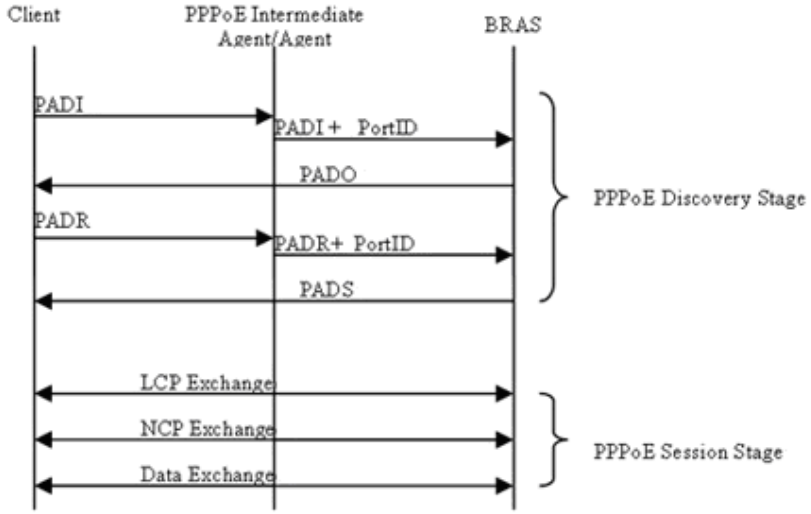

Figure 29 - PPP Session Establishment with PPPoE Intermediate Agent
Source: PPPoE Discovery and Session Stage [59]

4.5. Summary

This chapter presented in general the main features that mDSLAM-48 provides, from the technical characteristics hardware and software modules, Ethernet behaviours, DSL, until the services enabling features described in chapter 5, as example: VLANs, DHCP Relay Agent, or IGMP snooping.

Chapter 5: Triple-Play Features Validation

This section describes the validation tests performed to comply with the requirements described in TR-101 [21], that given the architecture for provision of Triple-Play in access network.

Initially, tests were conducted in PT Inovação, S.A. laboratories using mDSLAM-48 and dedicated test equipments. That is, for validating the configuration given characteristics (features), with the help of some CPEs, switches, computers, sniffing software packages and with traffic generator equipments (Spirent AX/4000 [45], Spirent TestCenter [45], Spirent Smart Bits [45], Agilent N2X [46], Agilent RouterTester 900 [46]).

Later, the same tests were conducted in laboratory that is used for testing and validation of equipments in PT Comunicações, S.A. [47], entering the mDSLAM-48 in the triple-play testing network scenario. Figure 31 illustrates the network diagram used on those tests.

This chapter begins with the presentation of the overall architecture where the Access Node (mDSLAM-48) was inserted. Follows a brief description of access node services requirements and residential network typical architecture. After this overview, test configuration and description is presented for each service, including the referred results. Configuration presented is based on Media DSLAM Application Notes [31], Media DSLAM Cli Manual [32] and Media DSLAM Users Manual [33].
On each subsection, there is a conclusion summarizing if the results obtained are in accordance with TR-101. Main requirements of TR-101 can be located in Annex II for consultation.

The equipment was setup, mostly using CLI commands. There is also the possibility of setting configurations on mDSLAM-48 using the AGORA-NG® [34] management platform. However, since the tests here presented were performed essentially using CLI, there are only a few points that refer AGORA-NG® management platform.

5.1. Target Scenario

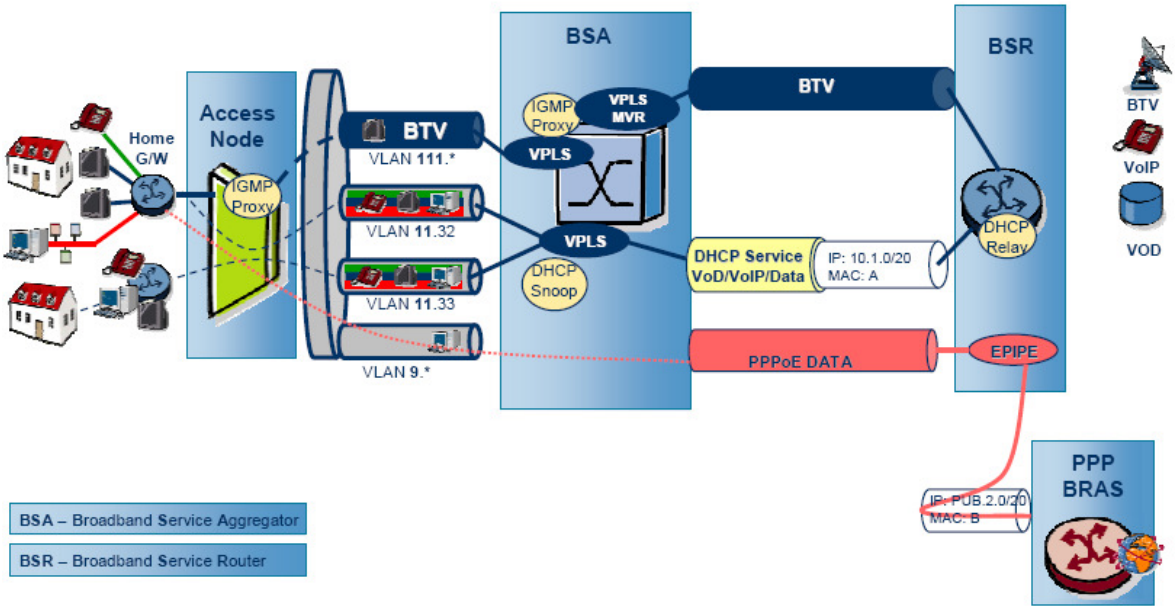

Figure 30 - Triple-Play Transport Network
Source: "IPTV Transport Network" [35]

Network represented in Figure 30 is a possible transport network deployment for triple-play services offer. It gives an overview of all network schematic since the home network devices (home gateway, telephones, TV+STB and PCs), access/aggregation devices (access node and service aggregator), until services platform delivery devices (service router, BRAS, BTV, VoIP and VOD servers).

The goal of this section is the demonstration of tests scenario over Access Node (mDSLAM-48 [30]). Referred scenario is illustrated in Figure 31. Details of AN configuration can be found in next sections. Configurations related to the remaining devices are not presented in the thesis (as RG, Switch-Router, DHCP server, BBRAS, etc).

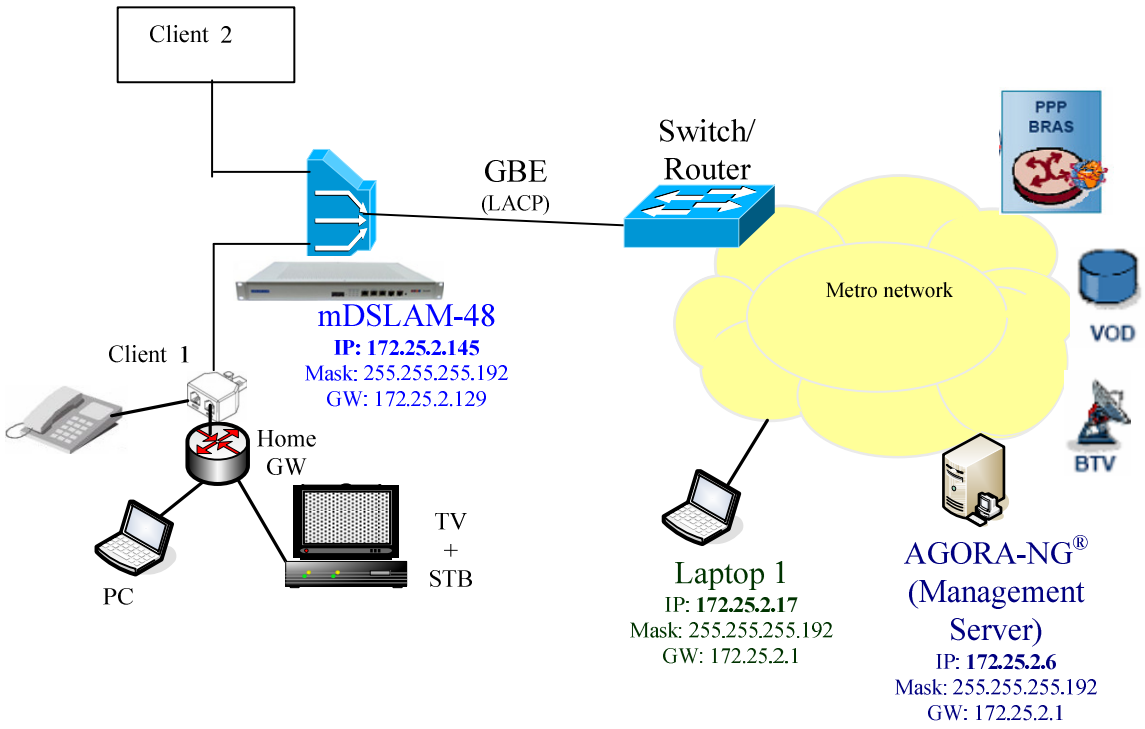

Figure 31 - Network diagram of mDSLAM-48 tests

The main objective of the proposed network (represented on Figure 31) from the point of view of the operator is to provide three different services to its customers:

- High-Speed Internet (HSI),
- Video-on-Demand (VoD) and
- IPTV (Multicast).

Triple-Play service proposed in the tests implemented is composed by analogue telephony service, that is, there is no VoIP service (digital). For this purpose, access node has a Splitter unit (see section 4.2) that joins DSL and POTS services over the same copper pair. Thus, customers still use the analogue phone at home attached to micro filters to prevent interference with and from the ADSL service.

However, AN could be easily configured to function also with a new service configuration to provide VoIP service.

Following sections gives an overview of the required behaviour of access node and home networking. Devices such as DHCP server, IPTV platform provider, PPP termination (BRAS) are mentioned in the respective framework system as necessary. Note that information related to those devices is not detailed.

Access node scenario is presented first and after that, a brief description of home networking behaviour is explained.

5.1.1. Access Node

Provider Network delivers to Access Node (on its uplink GBE interfaces) three main service VLANs, one for each service: HSI, VoD and IPTV.

1. Internet access (High Speed Internet - HSI) is defined with a 1:1 VLAN, which the S-Vlan id is "9", and C-Vlanid corresponds to each of the customers, that is, different C-Vlan id value for each line of subscriber (inside the same S-Vlan id). An example of the packets from/to DSL customer of the first line of access node can have the following tags (on its uplink): S = 9 and C = 32 (as illustrated in Figure 32 and Figure 33).
2. Video on Demand (VoD) service is similar to the HSI service, with the difference that S-Vlan id has a distinct value (accordingly to Figure 32 and Figure 33 value is 11).
3. IPTV service, is provided through a N:1 VLAN (also known as Multicast Vlan), that is, a .1Q VLAN, where only S vlan tag exists. (This VLAN id is the shared by all subscriber lines for the IPTV traffic delivery.)

Initially two different PVC's scenarios were proposed which are represented in Figure 32 and Figure 33.

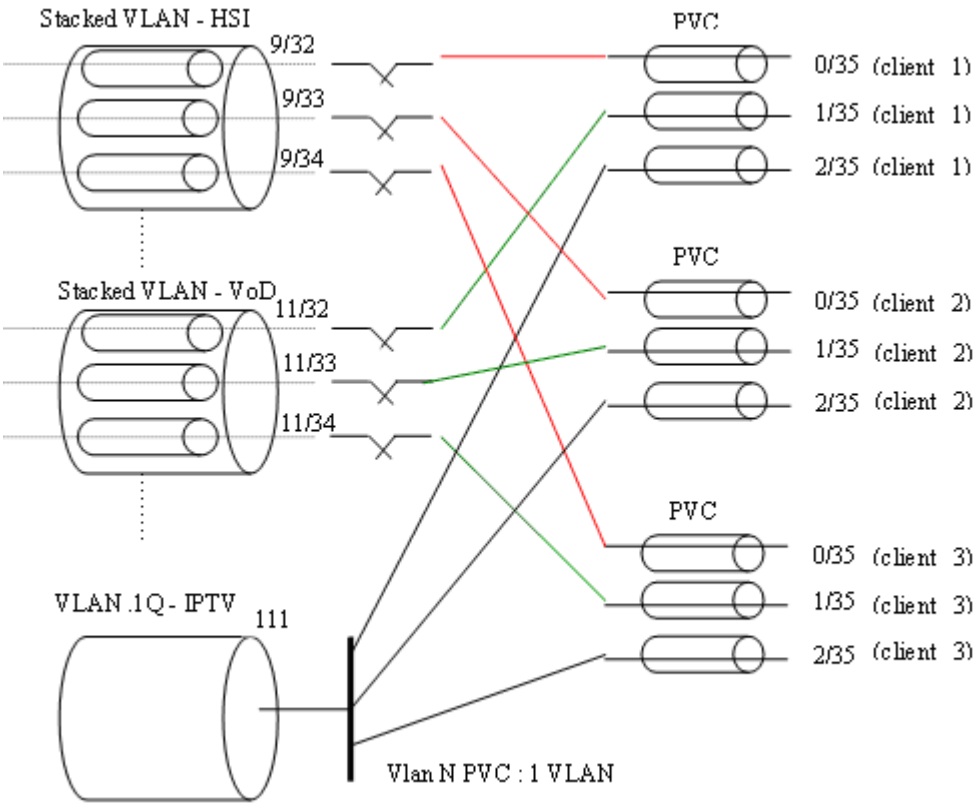

Figure 32 - 3 PVC Scenario

First scenario (Figure 32) sets customer line, with three different PVCs, one by service (0 / 35 - HSI; 1 / 35 - VoD, and 2 / 35 - IPTV). This scenario is only illustrative, because it was the second that was used.

Second scenario (Figure 33) sets only two PVCs, where PVC 0/35 is used for HSI traffic VLAN. The other PVC (1 / 35), is shared by VoD and IPTV traffic VLANs, from CPE side. Through the ability of IGMP Snooping, and Multicast Vlan, AN have an agent that snoops upstream IGMP packages (layer 3), updates a multicast database table, and if necessary, forward them in the uplink to multicast Vlan (and copied also through VOD vlan, if required, - for billing purpose controlled in VOD Vlan, as example). When receiving multicast data (video streams and / or IGMP queries), which are received in N:1 Vlan is forwarded to the RG, by PVC 1 / 35. The remaining traffic received in the AN from the customer in PVC 1 / 35, is traffic that is considered to be forward to S-Vlan id 11 (VoD service), and correspondent inner C-VLAN id tag. Packets received are marked with a C-Vlan tag (assigned to the refered customer, if it first customer, accordingly to Figure 33 receives C=32) and S Vlan-id = 11.

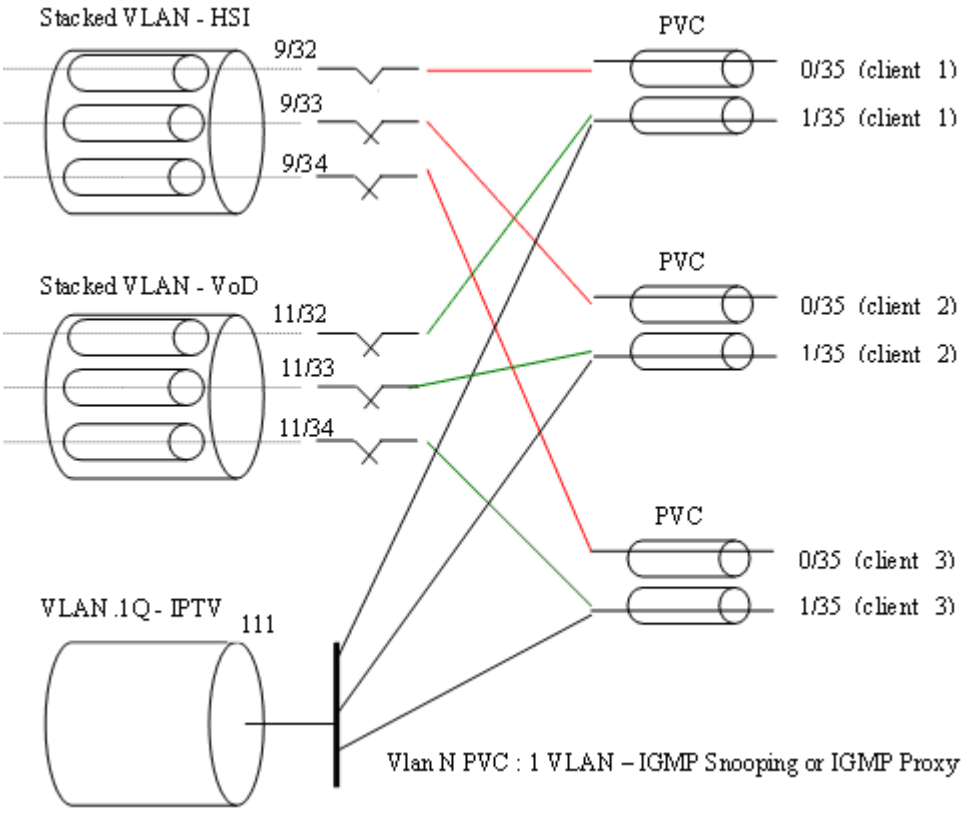

Figure 33 - 2 PVC Scenario

Therefore, tests are focused on architecture of Figure 33, and submitted settings are referred for one or two dsl subscriber lines (in this case, for the first 2 DSL interface represented in the diagram), depending on test validation scenario.
VLANs, DHCP Relay Agent and some of Multicast tests are represented with one DSL subscriber line. Remaining tests where the configuration of two DSL subscribers is fundamental for the feature demonstration, two subscriber lines are referred.

Detailed information related to commands used in the configuration of the Access Node for the features validation can be found in mDSLAM-48 user manuals and application notes [31], [32] and [33].

5.1.2. Residential Network

This chapter approaches basic behaviour of home networking devices, which are present in Figure 34. All devices: RG, TV, STB and PC, were used in the tests (example, detailed information can be found in [48], for home networking scenarios).

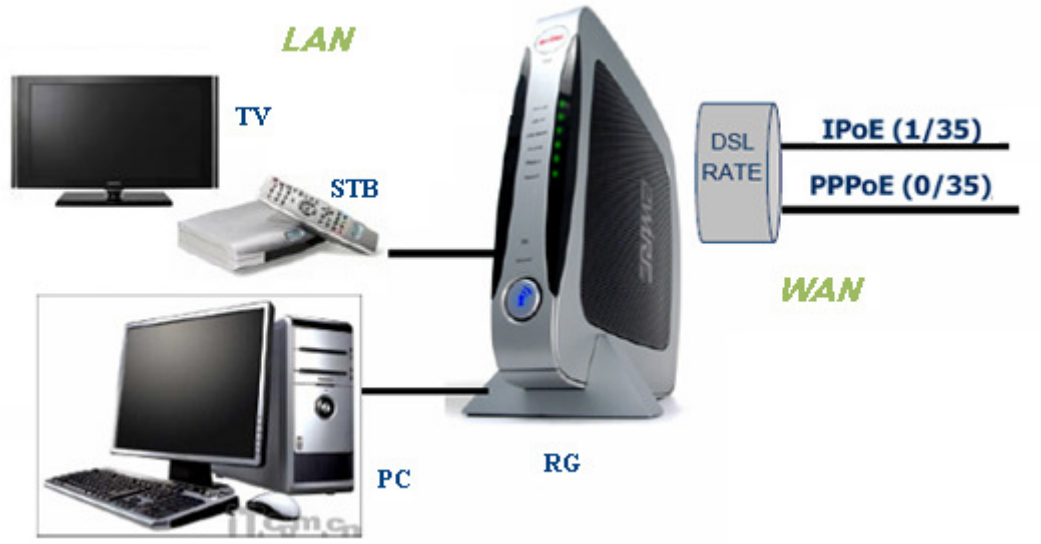

Figure 34 - Residential Network devices
Source: "IPTV Transport Network" [35]

Residential Gateway (RG) devices that was used for the tests were mainly 2 Wire [48]. However, it was used also other CPEs trademarks, configured as "bridging mode" (without

Routing and NAT features) to capture packets in downlink network (Thomson Speedtouch CPEs [49], Billion [50], among others).

RG is configured with two PVCs.

1. The first PVC (0/35) have an PPPoE client, that, after DSL synchronization negotiates PPP session with BRAS that is connected in MPLS network.
2. Second PVC (1/35) is used for VoD and IPTV service purpose. It operate with IP over Ethernet (IPoE). RG have a DHCP client in this PVC that, after DSL synchronization, initializes DHCP negotiation, to get valid IP configuration.

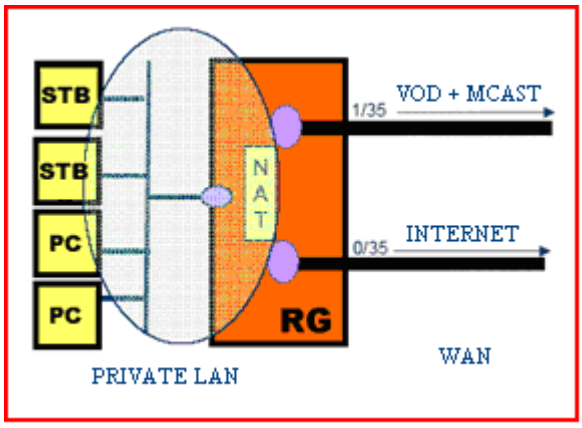

Figure 35 - RG configuration
Source: "IPTV Transport Network" [35]

Residential Gateway act as a fully Router. Devices that are connected to the RG on LAN side (that is a private subnetwork), such as STBs and PCs, request for DHCP dynamic negotiation. RG have a DHCP server on that private subnetwork that offers IP configuration, and information from devices that is to be forwarded to WAN side, is sent using NAT based forwarding. This configuration, amongst other advantages allow the possibility that PCs and STBs can communicate between them seamlessly (allowing the exchange of MP3 files, movies and sharing other information between them, as example), and STBs can access to High Speed Internet.

However, once RG acts as a Router:

- It needs an IGMP agent to act as IGMP snooping, that forwards IGMP messages from STBs throw the correct PVC that is used for multicast traffic (PVC 1/35)[4];
- Remaining general traffic from STBs and PCs (unicast traffic), that is not considered as VoD and IPTV control platform unicast messages, is forwarded through the other PVC (0/35), because it is assumed that it is HSI traffic (it is considered as "default route").
- Traffic that is considered as VoD requests and IPTV platform control messages is forwarded throw the second PVC (1/35 – "VoD + IPTV PVC") due to static routes that are configured in RG. STB have also the IP configuration, by default, for that purposes.

When STB starts up, it requires a configuration image that, with static IP servers configuration and authentication (through STB GUID identifier mapped with RG Wan MAC address), will request data configuration through PVC 1/35 of RG, and on which AN will forward requests and receive corresponding information through 1:1 VoD Vlan.
Detailed information related to STB and IPTV platform can be found in [55] and [56].

This enhanced information related to the Home Networking scenario, reader is able to understand the remaining scenario configuration presented in the following sections.

5.2. Physical Port Configuration

Access node can configure and display for each DSL interface the Physical Line Profile, that is, the flavour and the following parameters:

- Target, Maximum, Minimum, Upshift and Downshift Noise Margin;
- Rate Adaptation Mode;
- Minimum Time Interval for Upshift and Downshift Rate Adaptation;
- Desired Maximum and Minimum Rate Fast/Interleave (upstream and downstream);
- Rate Adaptation Ratio;
- Maximum Interleave Delay;

[4] After analyse IGMP packet, if needed IGMP Querier forward (upstream) IGMP packets to an IGMP Proxy agent, and in turn, (accordingly to IGMP Proxy requirements) it forward IGMP packets an IGMP Client that forward those packets through IPoE PVC. Multicast is also received on this interface – AN sends multicast traffic through this PVC and RG have an IGMP client that controls the requests/forwards of IGMP Queries/Reports from/to AN.

- Alarm (Event) Thresholds (15 minute count threshold) on Loss of Signal, Frame, Power and Link (ATU-C only); or Errored Seconds
- Rate Up and Down Threshold (Fast / Interleave);
- Vendor Id (Read Only);
- Version Number (Read Only);
- Serial Number (Read Only);

Command related to Flavour configuration is:

```
$ (get/modify) adsl line intf ifname dsl-x
IfName                        : dsl-22
Line Type                     : fastOnly        Coding Type       : dmt
(...)
Trans Atuc Actual             : q9925Adsl2PlusPotsNonOverlapped
Trans Atuc Config             : ansit1413 q9921PotsNonOverlapped
q9923Readsl2PotsNonOverlapped q9925Adsl2PlusPotsOverlapped
q9923Adsl2PotsNonOverlapped q9923AnnexMPotsExtUsNonOverlapped
q9925AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsOverlapped
GsDmtTrellis                  : trellisOn
(...)
```

Command related to Profile information is:

```
$ (get/modify) adsl line profile ifname dsl-x
IfName : dsl-22
Profile Description: AGORA-NG_test
ADSL ATUC Configuration :
-------------------------
Rate Adaptation           : adaptAtRuntime
Target Snr Margin(dB/10)  : 60         Max Snr Mgn(dB/10)       : 310
(…)
Min Dnshift Time(sec)     : 0          Fast Min Tx Rate(bps)    : 32000
Intl Min Tx Rate(bps)     : 32000      Fast Max Tx Rate(bps)    : 4096000
Intl Max Tx Rate(bps)     : 4096000    Max Intl Delay(ms)       : 63
(…)
Type                      : fastOnly
(…)
Min Snr Mrg(dB/10)       : 0
(…)
Minimum INP              : InpAuto

ADSL ATUR Configuration :
-------------------------
Target Snr Margin(dB/10)  : 60         Dnshift SnrMargin(dB/10)  : 30
Upshift SnrMargin(dB/10)  : 90         Min Upshift Time(sec)     : 30
Min Dnshift Time(sec)     : 30         Fast Min Tx Rate(bps)     : 32000
Intl Min Tx Rate(bps)     : 32000      Fast Max Tx Rate(bps)     : 256000
Intl Max Tx Rate(bps)     : 256000     Max Intl Delay(ms)        : 16
MSG Min Us                : 16000      Minimum Snr Margin(dB/10) : 0
Maximum Snr Margin(dB/10) : 310
(…)
Min INP                   : Inp0
(…)
```

Using CLI it is not possible to apply a profile description to a set of dsl ports. However, throw management platform, applying an ADSL Profile (Catalogue) on dsl interface sets

the profile intended corresponding to the catalogue. In that case, "Profile Description" parameter gets the name of the applied catalogue on the referred interface.

Detailed information related to the commands that returns current line rates, CPE inventory, SNR margin, attenuation, attainable rate, output power and statistics of line interface, can be found in [33].

5.3. Logical Port Configuration

Typically, the configuration used is based on TR-101 architecture for protocol adaptation function of IPoE over ATM, which is illustrated by Figure 36. The IPoE IWF used is based on Bridge ports (BP). Such BPs are created over EoA interface and over Ethernet uplink interfaces. So, BPs allows that access node function as "pure" Ethernet Switch, because there are BPs in the uplink and also in the downlink interfaces.
Note that typically, once there are two GBE (uplink) interfaces they are configured with Link Aggregation (Static or LACP). So, BP is created over this logical interface (for "switching" behaviour there is only one logical uplink interface, and the control protocol that is underneath controls both of the GBE uplink interfaces).

As presented in the following interfaces configuration sections, adopted nomenclature and mapping for the BPs identifiers in the access node are:

- BP id's from 1 to 48, are mapped to dsl ports 1 to 48 respectively (those are associated with the first PVC for each subscriber interface),
- BP id 50 is mapped to uplink logical aggregated interface, and
- BP id's from 51 to 98 are mapped to dsl ports 1 to 48 respectively (those are associated with the second PVC for each subscriber interface).

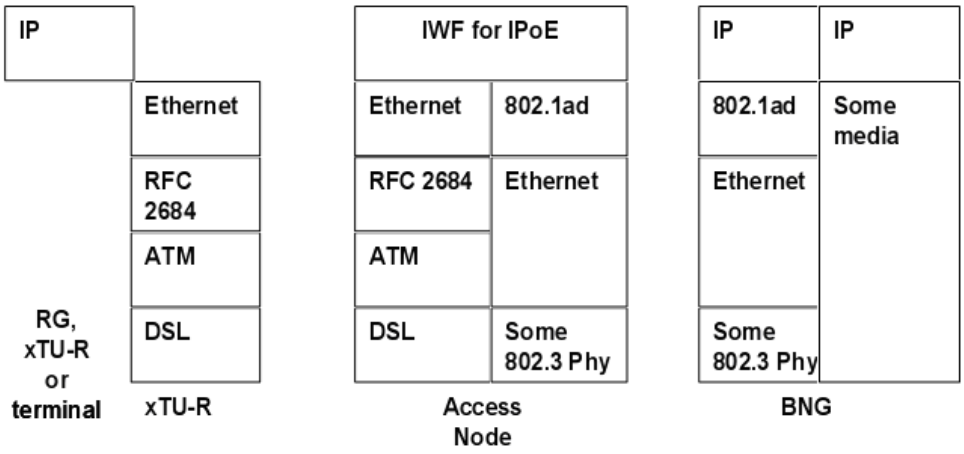

Figure 36 - TR-101 definition of End-to-End protocol processing for IPoE access
Source: TR-101 [21].

5.3.1. Downlink Interfaces (DSL)

Follows a typical configuration for a Downlink Interface (DSL port), illustrating the architecture of 2 PVCs scenario (Figure 33). Configuration refers to the first subscriber line of access node.
(Commands related with physical DSL system enabling parameters are already configured when system starts up with FD (see section "Factory Default" in Annex I).

Physical Profile:

```
$create dsl system
$create atm port ifname atm-1 lowif dsl-1
```

Creation of HSI PVC:

```
$create atm vc intf ifname aal5-1 lowif atm-1 vpi 0 vci 35  => PVC (AAL5)
$create eoa intf ifname eoa-1 lowif aal5-1                 => EOA layer
$create bridge port intf ifname eoa-1 portid 1 status enable   => BP (1)
```

The creation of VoD / IPTV PVC is identical (BP 51), whereas, used PVC is *vpi* as 1 and *vci* as 35, and the number of *aal5* and *eoa* interfaces is 51.

After this, DSL interface #1 is configured with physical and logical layers to operate successfully. After this, BPs are ready to be configured with services VLANs.
From this point on forward, for VLAN configurations, DHCP, PPPoE, IGMP, etc, "BP" nomenclature is used instead of "PVC".

Connecting CPE device (ADSL Router) in the subscriber line, it synchronizes successfully. Checking its web terminal after synchronization, PVCs 0/35 and 1/35 are all in *up* state.

5.3.2. Uplink Interfaces (GBE)

Present configuration referes to LACP based configuration because the other end device (Switch/Router) requires dynamic link aggregation (LACP). After this configuration, aggregated interface is able to configure VLANs (management and traffic services).

Configuration

```
              Create Ethernet Interface (Physical interfaces)
$ create ethernet intf ifname eth-1 / eth-2
Aggregated Logical Interface (with an IP address for management purpose):
$create aggr intf ifname aggr-1 enable ip 172.25.2.145 mask
255.255.255.192
$create lacp aggr  aggrifname aggr-1 aggrtype lacp     => enable LACP
                                                       interface
$modify lacp aggrport info ifname eth-1 /eth-2 aggrstatus enable =>
                         activate aggregation mode for eth-1/2
$ create bridge port intf portid 50 ifname uplink status enable    =>
                              Create BP and associate it to LACP
                              interface (uplink interface)
      Creation of Default Route:
$create ip route ip 0.0.0.0 mask 0.0.0.0 gwyip 172.25.2.129
```

Following commands return the output of the configuration and interface status:

```
$get ethernet intf ifname eth-1
Interface            : eth-1
(...)
Speed                : 1000BT
Oper Status          : Up                Admin Status : Up

$get aggr intf IfName aggr-1
IP Address           : 172.25.2.145      Mask : 255.255.255.192
(...)
Oper Status          : Up                Admin Status         : Up

$get lacp aggr aggrifname aggr-1
Aggr IfName         : aggr-1
Mac Address         : 00:06:91:00:28:37  Aggregate : True
Actor Sys Priority  : 10                 Partner Sys Priority : 32768
Actor Sys ID        : 00:06:91:00:28:37
Partner Sys ID      : 00:03:FA:61:13:C0
Actor Oper Key      : 40                 Partner Oper Key     : 40
Actor Admin Key     : -                  Collector Max Delay  : 0
Aggregation Type    : Lacp

$get lacp aggrport info
Interface               : eth-1             Port is Aggregate          : True
Actor Oper Key          : 40                Partner Oper Key           : 40
Actor Admin Key         : -                 Partner Admin Key          : 1000
Actor Port Priority     : 10                Partner Admin Port Priority : 9
Actor System Priority   : 10                Partner Oper Port Priority  : 128
Actor System ID         : 00:06:91:00:28:37 Partner Admin Sys Priority  : 9
Actor Port              : 1                 Partner Oper Sys Priority   : 32768
Partner Admin Sys Id    : 01:02:03:04:05:06 Partner Admin Port          : 1
Partner Oper Sys Id     : 00:03:FA:61:13:C0 Partner Oper Port           : 2318
Port Actor Admin State  : activity timeout aggr defaulted
Port Partner Admin State : timeout aggr defaulted
Port Actor Oper State   : activity timeout aggr sync collect distrib
Port Partner Oper State : activity timeout aggr sync collect distrib
```

```
Attached Agg ID          : aggr-1            Selected Agg ID            : aggr-1
Aggregation Status       : Enable            LACP Packet's Prio         : 0
(...)
```

```
$get lacp aggrport list aggrifname aggr-1
Aggr IfName : aggr-1
Port List   : eth-1 eth-2
```

Tests

Suppose that, if there is a problem on interface eth-1, this interface stops to belong to the aggregated interface. Following command can be used for debug:

```
$get lacp aggrport list aggrifname aggr-1
Aggr IfName : aggr-1
Port List   : eth-2
```

The issue could be due to physical link fails (check link status of interface *eth-1*). If not, that is, link is physically up, one reason could be due to LACPDUs failure, and so logical interface will intend to use only *eth-2* as aggregated.

After all services configured on the system (VLANs: HSI, VoD, and IPTV, DHCP Relay Agent and IGMP Snooping), a list of tests was done to validate LACP module:

- Unplug physical link: the service did not stop to be delivered to the connected customers;
- With optical GBE links, disabling TX or RX Laser: once the other end does not receive LACPDUs on that interface, after 3 timeouts (details of standard operation can be found in [24]), it assumes only the other interface as up, and all of the traffic is redirected to it. After that, service continues successfully delivered to subscriber line.
- IP connectivity: using “telnet” and “ping” command to access node is not loss, when interface eth-1, or eth-2 is unplugged. After interface plug in, situation establishes (traffic is redistributed using original algorithm of source Mac address hashing).
- Using Spirent SmartBits [45] traffic generator, emulating packets with distinct source MAC addresses, it is possible to check the load balancing, by MAC address. It is only possible to view when there is a considerably amount of traffic over the interface. As example, if a simple “ping” command from different sources is used, all the traffic goes through the first Ethernet interface, ie, there is no perception of load balancing.

Conclusion

This configuration and behaviour of access node is accordingly with requirements R-34, R-35 (Annex II). Considering requirement R-37 it is not available in access node, because there is only two uplink GBE interfaces available, which are configured as one LAG. For

that purpose, at least two uplink link aggregation modules are required for the implementation of two LAG to function in a ring topology.

5.4. VLANs

Stacking mode enables features that meet custom VLAN stacking requirements (see R-33), as illustrated in Figure 33.

Accordingly, with requirement R-08, the Ether type field for the 802.1ad tagging, i.e. S-Tags, should be configurable (per Access Node). Value used is "0x8100" (as IEEE 802.1Q). This value is used for backward compatibility with other provider equipments.

5.4.1. Management VLAN

Commands bellow illustrates a possibility of Management Vlan configuration:

```
                Management Vlan (mapped to Virtual Vlan above)
$create vlan static vlanid 2 vlanname GESTAO egressports 50 untaggedports
50
$create vlan svlanid 2 svlantype residential          => Create S-Vlan
$create vlan virmap svlanid 2 cvlanid 2 vvlanid 2     => Mapping S to C
                                                 vlans (Virtual Vlan)
$modify gvrp port info portid 50 psvlanid 2 portvlanid 2  => AN origin
           traffic will go out with S-vlan = 2, and C-vlan (untagged)=2
```

- Egress ports: 50 (BP that belongs to VLAN (only Uplink logical aggregated interface)).
- Untagged ports: 50. (Once this is a vlan with S-tag, and C-tag is untagged)

As AN is configured in stacked mode, it is necessary to configure BP 50 as provider port:

```
$modify gvrp port info portid 50 ppstatus enable
```

Tests

After configuration, a *ping* and *telnet* connection from Laptop 1 to mDSLAM-48 was tested with success. Disconnecting both GBE interfaces, IP communication fails.

At this point, it is possible to configure all the system remotely, through Laptop1 (telnet). Those tests approves R-08 and partially R-33 (partially because it is totally approved in multicast and HSI / VOD vlan services section).

5.4.2. VLAN 1:1 (HSI and VoD VLAN)

Requirements R-04, R-05, R-06, R-07 and R-09 are demonstrated in the following sub-sections.

5.4.2.1. S-Tag and C-Tag to untagged frames

Configuration of AN, accordingly to R-05, for BP 1, of subscriber line #1, is as follows. BP 1 belongs to HSI VLAN (S-Vlanid 9). The configuration of second BP (51) of that subscriber line is identical, however VOD VLAN is used, that is, S-VLAN id 11.

S-Vlan Creation:

```
$create vlan svlan svlanid 9 svlantype residential
```

Virtual VLAN Configuration:

- Egress Ports - list of BPs that belong to VLAN;
- Untagged Ports - list of ports that remove tags in the egress direction.

If BP 50, is defined as an *untagged*, it have a different behaviour from subscriber BPs. That is, defining it as untagged, upstream traffic is forward with S-Vlan tag only. Defining BP subscriber as untagged, downstream traffic is forward with no Vlan Tag. If subscriber port is not untagged, downstream packets are forwarded with C-VLAN tag.

```
$create vlan static vlanname HSI932 vlanid 932 egressports 1 50
untaggedports 1
```

S- to-C VLAN mapping (VVlanid is the same as Virtual VLAN)

```
$create vlan virmap svlanid 9 cvlanid 32 vvlanid 932
```

Marking Upstream Packets (ingress packets of subscriber BP) with:

- C-Vlanid (*portvlanid*)
- S-Vlanid (*psvlanid*)
- *IngressFiltering*: when true, as BP receives tagged frames from subscriber, if frame tag is different from C-Vlanid configured, frame is dropped. If it has the same id, it is forward. If configured as false and, received frames have a different C-Vlan id, if that C-Vlan id is configured in another BP of the system, packet is forwarded with original C-Vlan id.

```
$modify gvrp port info portid 1 psvlanid 9 portvlanid 32 ingressfiltering true
```

If upstream packets are C-tagged packets, AN have another option behaviour configurable. If ingressfiltering of an BP of S-Vlan is configured as false, AN can "preserve" C-Vlan of upstream packets received or "non-preserve" applying C-Vlan id configured on related BP. The same options also for QoS priority bits of C-Vlan (C-Vlan QoS Preserve mode, as preserve or non preserve).

```
$modify vlan svlan svlanid 9 cvlanpreservemode nonpreserve cvlanqospreservemode nonpreserve
```

At this point, a CPE configured with PPPOE client (mapped to BP 1) was connected to the AN, in DSL line #1. After DSL synchronization, PPPoE session was established successfully, which means that AN applies S-tag and C-tag in the upstream direction, and removes them in downstream direction. (CPE sends and receives untagged PPPoE related messages).

5.4.2.2. S-Tag to C-Tag tagged frames

Difference from the current configuration (R-06) to the above sub-section (R-05) is that, upstream packets received from CPE line have tag information. AN has different features that can be configured for this purpose.

```
$create vlan svlan svlanid 9 svlantype residential
$create vlan static vlanname HSI9xx vlanid 100 egressports 1 50
untaggedports none
$create vlan virmap svlanid 9 cvlanid 4097 vvlanid 100
$modify gvrp port info portid 1 psvlanid 9 portvlanid 32 ingressfiltering
false
```
(portvlanid can be any value)

Three different tests are presented to explain different possible behaviour configuration:

1. AN preserves C-tag id and Priority value (QoS preserve mode) that is received

```
$modify vlan svlan svlanid 9 cvlanpreservemode preserve
```
(preserve any C-vlan tag value)

```
$get bridge port priomap portid 1
PortId        : 1          UserPriority : 0    RegenUserPrio : 0
(...)
PortId        : 1          UserPriority : 6    RegenUserPrio : 6
PortId        : 1          UserPriority : 7    RegenUserPrio : 7
```

2. AN changes mapping of priority received on BP 1 (receive priority as "1", and regenerates to "4")

```
$modify bridge port priomap portid 1 usrPrio 1 regenPrio 4
```

3. Preserve QoS mode received in *.1Q* frame:

```
$modify vlan svlan svlanid 9 cvlanpreservemode preserve
cvlanqospreservemode preserve
```

Results

Upstream traffic flows was simulated with SmartBits device connected to a CPE with PVC 0/35 configured as pure bridge to the LAN side.

1. Sending upstream packets with C-Tag id as "34", and Priority value as "1", AN add S-tag "9", keep C-tag and Priority of C-tag. Once priority mapping for BP is default (0 → 0, 1 → 1, …, 7 → 7), S-tag receives the same priority value as original C-tag.
2. Sending upstream packets with C-Tag id as "34", and Priority value as "1", AN add S-tag "9", keeps C-tag id ("34"), and changes priority of C-tag from "1" to "4" (also adds this priority – "4" – to S-tag).
3. Sending upstream packets with C-Tag id as "34", and Priority value as "1", AN add S-tag "9", keeps C-tag id ("34") and priority of C-tag as "1". However, S-tag is added with priority accordingly to map (receives C-tag with prio as "1" which is mapped to "4"). So, S-tag receives priority "4")

All tests (upstream direction) were performed successfully. Note that, tests were made over HSI BP, but they could be also implemented over VOD BP.

5.4.2.3. Remove VLAN Tag

This test is related to downstream packet flows (R-07).

Related to S-tag removal, as AN receives downstream packets, automatically removes S-Vlan tag (S-vlan, only exists on Provider BP). Removing of C-Vlan id is configurable on a VLAN and BP mapping based (for each S-to-C Vlan– ie, on Virtual Vlan id).

The test to remove both S-tag and C-tag was already performed on section 5.4.2.1 on PPPoE session establishment. (note that, in this case, for VVlanid 932, BP 1 is configured as untagged).

To remove only S-Vlan tag, complementing tests made in sub-section 5.4.2.2, BP 1 can not be an untagged port (see VVlan ID 100). In this case, sending downstream packets with S-Vlan id = "9" and C-Vlan id = "34", CPE receives packets with C-Vlan id "34", successfully (AN does not change priority bits of C-VLAN tag).

5.4.2.4. Acceptable Frame Types

Accordingly with R-09, AN allow the configuration of acceptable frame types per BP as "ALL" or "TAGGED"

```
$get gvrp port info
Port Id                        : 1
(...)                              Accept Frame Types : all
(...)
```

Configuring BP 1 with "accept frame types" as:

- "all": AN accepts (and forwards in the upstream) tagged and/or untagged packets;
- "tagged": PPPoE session with 2Wire CPE is not established because it sends untagged packets, and they are dropped at BP 1. If Bridging CPE configuration is used, and using SmartBits to send tagged traffic (with C-Vlanid 32) mDSLAM add S-Vlan tag ("9") and forward traffic flows.

Packets that not match the configured "accept frame type" are discarded.

5.4.2.5. Priority Marking

This sub-section refers R-20.

- Related to untagged traffic, priority marking is configured by default priority of BP:

```
$get bridge port prioinfo portid 1
DefaultPriority    : 0          (...)
```

Default value is "0", to change default priority:

```
$modify bridge port prioinfo portid 1 defPrio 5

$get bridge port prioinfo portid 1
(...)
DefaultPriority    : 5          (...)
```

Sending upstream untagged packets on BP 1, AN adds S-Vlan id "9" and C-Vlanid "32", both with priority value as "5".

- Related to tagged traffic, this test was already performed on section 5.4.2.2.

5.4.2.6. Default Tagging

This sub-section refers R-23. As mentioned before, default tagging of BP 1 applies on untagged packets received (applied on S-tag and C-tag).

```
$get bridge port prioinfo portid 1
(...)
DefaultPriority    : 4          (...)
```

It is possible to (re)mark priority values of C-tag and / or S-tag with filter rules. To validate this feature, it was performed two distinct tests:

Test 1: Remark only C-tag, accordingly to a Ethertype (PPPoE discovery – ethertype 0x8863), mapped on BP 1 (*eoa 1*)

```
$create filter rule entry ruleid 1 action retagprio priority 6
$create filter subrule ether ruleid 1 subruleid 1 ethertypefrom 0x8863
ethertypecmp eq
$modify filter rule entry ruleid 1 status enable statsstatus enable
$create filter rule map ruleid 1 ifname eoa-1 stageid 1
```

Capturing upstream packets in uplink port, PPPoE discovery packets are marked with C-priority as "6" (due to filter rule) and S-tag as "4" (default BP tag); other packets have both C-tag and S-tag priority as "4" (default BP tag).

Test 2: Re-mark C-tag and S-tag with different values

```
$create filter rule entry ruleid 1 action retagserviceprio priority 2
$create filter rule actionmap ruleid 2 orderindex 1 action retagprio
priority 7
$create filter subrule ether ruleid 1 subruleid 1 ethertypefrom 0x8863
ethertypecmp eq
$modify filter rule entry ruleid 1 status enable statsstatus enable
$create filter rule map ruleid 1 ifname eoa-1 stageid 2
```

Capturing packets, PPPoE discovery packets are marked with C-tag priority as "6" and S-tag as "7"; other packets have both C-tag and S-tag priority as "4".

5.4.3. VLAN N:1 (Multicast VLAN)

Tests related to N:1 VLAN are available in section 5.8 below.

5.5. Security Considerations

5.5.1. User isolation

This feature is accordingly with R-40, to prevent user-to-user communication. This prevention feature is available in both N:1 and 1:1 Vlans.

In N:1 Vlans, configuring AN global system forwarding as "Residential mode", assures that traffic from subscribers is always forwarded to the uplink interface, meaning that, user-to-user traffic is not possible. If "Unrestricted" bridging mode is configured, user-to-user communication is allowed.

Using 1:1 VLANs, that have only one CPE BP and uplink BP, AN prevents always traffic forwarding between different S-to-C vlan mapping, even if S-Vlan id remains the same. This feature is independently of global forwarding configuration mode.

5.5.2. Broadband Network Gateway MAC Address Spoofing

Different solutions are available to prevent Broadband Network Gateway (BNG) Mac Address spoofing, as requirement R-91.

Dynamic MAC learning is used, system has a parameter named *forwarding data base* (FDB) *modify* which is configured as *enable* or *disable*. This parameter is configured by BP. Using it as *enable* in both BPs (net side and subscriber side), when a MAC address is learned on BP 50, if the same MAC address arrives on BP 1, MAC address learned entry will flap from BP 50 to BP 1 FDB entries. To prevent spoofing from customer side, DSL BPs must have FDB modify disable, and Provider Port (BP 50) must have this parameter configured as enable.

```
$ modify bridge port intf portid 1 fdbmodify disable
$ modify bridge port intf portid 50 fdbmodify enable
```

A CPE as bridging mode is connected, and a PC is configured with a PPPoE session (spoofing in the PC the same MAC address as BNG). The first packet of PPPoE negotiation is forwarded to the BNG (if BNG Mac address has not been yet learned in BP 50 for the referred VLAN). After the first packet reply from BNG to CPE, AN learns BNG

Mac address on BP 50, and deletes the entry from BP 1. Remain packets with source of PC Mac address are drop on BP 1.

If it is used other MAC address on CPE side, PPPoE session is established with success.

5.5.3. Number of learned MAC Addresses

MAC address learning can be limited by BP, to comply with R-92 and R-93, preventing MAC address flooding in AN.

```
$modify bridge port intf portid 1 maxucast 2

$get bridge port intf portid 1
(...)       Max Unicast Addresses  : 2      (...)
```

Initial test was to limit number of learned MAC addresses on BP 1 to value 2, after learning of 2 subscriber MAC addresses, change the configuration to only 1.

Connection two PCs on a DSL modem (in Bridge mode), their MAC addresses are learnt

```
$get bridge forwarding
MAC Addr           PortId     VlanId     Status
(...)
00:10:4B:36:F5:62  1          932        Learned
00:17:42:00:DB:23  1          932        Learned
(...)
```

Changing value of MaxUcast from 2 to 1 on BP1, only a MAC related to one of the PCs is learned (the first which send upstream packets):

```
$get bridge forwarding
MAC Addr           PortId     VlanId     Status
(...)
00:10:4B:36:F5:62  1          932        Learned
(...)
```

5.5.4. MAC Address Learning

It is possible to enable or disable MAC address learning by BP to comply with R-44.:

```
$modify bridge port intf portid 1 learning disable
```

Connecting a DSL Router that tries to establish a PPPoE connection, it is performed successfully, and MAC address is not learned on AN. There is no entry for that VLAN 932, with BP 1.

Changing this parameter to enable, and restaring the synchronization of DSL Router, PPPoE session is established and MAC address is learned.

```
$get bridge forwarding
MAC Addr           PortId     VlanId     Status
(...)
00:10:4B:36:F5:62  1          932        Learned
(...)
```

5.6. Filtering

5.6.1. Layer 2 Filter

AN have filtering rules to be compliant with R-94. Following sub-sections presents those filtering rules. More than one solution for each type of filter is available to apply. In the meanwhile, follows only one example for each one.

5.6.1.1. Source Mac address

i. Allow Mac Address

This solution is implementing with Global Access Control List (ACL). However, this test must only accept referred MAC address.

```
$create acl global macentry macaddr 00:10:4B:36:F5:62 deny disable
track enable
$modify bridge port intf portid 1 aclGlbDenyApply enable

$get bridge port intf portid 1
(...)
Acl Global Deny Apply  : Enable
Acl Global Track Apply : Enable
```

Following command returns the number of times that port is changed:

```
$get acl global macentry
Mac Address                  : 00:10:4B:36:F5:62
(...)      Number of times Port changed : 2
```

Configuring PC device with MAC address 00:10:4B:36:F5:62 it establishes a PPPoE session, through BP 1 of AN. However, if different MAC is used, PPPoE interface does not establish session (BP 1 drop packets – and MAC address is not learnt on FDB).

ii. Deny Mac Address

Test is the same as performed in section above. However, *deny* parameter is configured as *enable*.

```
$create acl global macentry macaddr 00:10:4B:36:F5:62 deny enable track
enable
(...)
```

Connecting a CPE as bridging mode and a PC with MAC address 00:10:4B:36:F5:62 that tries a PPPoE session, packets are dropped at AN. Using different MAC address, PPPoE session is established successfully, which validates the requirement.

5.6.1.2. Destination Mac address

i. Allow Mac Address

```
$create filter rule entry ruleid 7 action allow
$create filter subrule ether ruleid 7 subruleid 1 dstmacaddrfrom
00:00:00:00:00:10 dstmacaddrcmp eq
$modify filter rule entry ruleid 7 statsstatus enable status enable
$create filter rule map ruleid 7 ifname eoa-1 stageid 1
```

This test was performing using SmartBits packets generator, with destination MAC address as 00:00:00:00:00:10. Sending upstream packets with that Mac address, AN forward them. However, if different MAC address is used, it is also forward. This can be solve using a filter that "denies" all packets with destination MAC address "different" from "00:00:00:00:00:10". However, if there is a list of different MACs to be "allow" per BP, it is necessary to implement one filter rule by BP. This solution is not the better approach. (This is a point for future development, if any service operator intends to use it).

ii. Deny Mac Address

To deny a MAC address, following configuration of the rule *action* is used, maintaining remaining configuration of the above filter.

```
$create filter rule entry ruleid 7 action drop
(...)
```

Configuring SmartBits to send packets with destination MAC address 00:00:00:00:00:10 (DSL side) BP 1 drop packets (and MAC address is not learning on FDB). However, if different MAC is used, packets are forward successfully.

5.6.1.3. Reserved MAC Addresses

Accordingly with R-95, AN must filter reserved group MAC destination addresses. System has a reserved profile for this purpose:

```
$get resvdmac profile param
Profile ID : 1          Multicast address : 01:80:C2:00:00:02
Action     : Participate
(...)
Profile ID : 1          Multicast address : 01:80:C2:00:00:21
Action     : TransformedBcast
```

Where:

- **Participate** – packets are delivered to the module that interprets packets (*01:80:C2:00:00:02 – LACP*)
- **TransformedBcast** – changes packets to Broadcast ,that is, packets are forward to all BPs that belongs to referred VLAN (*01:80:C2:00:00:21 – GVRP*).

Profile mapped to Vlan:

```
$get vlan static vlanid 932                    (...)
Egress ports                    : 1     50     (...)
Reserved Mac Profile Id         : 1            (...)
```

It is also possible to add new reserved MAC addresses to the profile or create new profiles:

```
$create resvdmac profile param Profileid 1 mcastaddr 01:80:c2:00:00:01
action participate


$create resvdmac profile info profileid 3
$create resvdmac profile param Profileid 3 mcastaddr 01:80:c2:00:00:24
action participate
$create resvdmac profile param Profileid 3 mcastaddr 01:80:c2:00:00:25
action transformedbcast
```

Example of applying a new profile in Vlan map 9/32:

```
$modify vlan static vlanid 932 resvmacprofileid 3
```

Using above profile (#3), sending packets using destination MAC addresses referred, captured packets (in the uplink interface), are related only to MAC address that is mapped to *Transform to Broadcast*. The other stream of packets are configured as participate, so they are not forward. If different MAC addresses of those referred on profiles are used *(in the 01:80:C2 range)*, they are not forward to the uplink.

5.6.1.4. Ethertype Filter

R-26 requires an Ethertype filter that can be achieve using filter rules to drop packets with intended Ethertype. Example, to drop PPPoE packets on BP 1, following filter is used:

```
$create filter rule entry ruleid 10 action drop
$create filter subrule ether ruleid 10 subruleid 1 ethertypefrom 0x8863
ethertypecmp eq
```

```
$modify filter rule entry ruleid 10 statsstatus enable status enable
$create filter rule map ruleid 10 ifname eoa-1 stageid 1
```

Connecting a CPE (*2Wire* – that has a PPP client) it is not possible to establish PPPoE session. Using other CPE in bridging mode, and Smartbits device is used to send any other type of frames different from PPPoE, AN forward them through uplink interface.

5.6.2. Layer 3 Filter

R-26 requires also filtering features on Layer 3 protocol. This issue can be implemented with rules similar to Layer 2 filters, however, they snoop on L3 protocols. All described rules were tested and their behaviour was as expected. Complete filter rule set is presented in the first filter below. Remaining commands for the last three subsections are identical to IP Source (allow) sub-section.

IP Source (Allow):

```
$create filter rule entry ruleid 11 action allow
$create filter subrule ip ruleid 11 subruleid 1 srcipaddrfrom 10.0.0.1
srcaddrcmp eq
$modify filter rule entry ruleid 11 status enable statsstatus enable
$create filter rule map ruleid 11 ifname eoa-1 stageid 1
```

IP Source (Deny):

```
$create filter rule entry ruleid 12 action drop
(...)
```

IP Destination (Allow):

```
$create filter rule entry ruleid 13 action allow
$create filter subrule ip ruleid 13 subruleid 1 dstipaddrfrom 10.0.0.3
dstaddrcmp eq
(...)
```

Filter rule presented allow the referred destination MAC address packets. However, if packets have different MAC addresses, AN does not drop them. Following solution may be used for this purpose ("*deny packets with MAC address different than…*"):

```
$create filter rule entry ruleid 13 action drop
$create filter subrule ip ruleid 13 subruleid 1 dstipaddrfrom 10.0.0.3
dstaddrcmp neq
(...)
```

IP Destination (Deny):

```
$create filter rule entry ruleid 15 action drop
$create filter subrule ip ruleid 15 subruleid 1 dstipaddrfrom 10.0.0.3
dstaddrcmp eq     (...)
```

5.7. Access Loop Identification and Characterization

Following sub-sections demonstrate that AN complies with R-127, R-129, R-130 and R-132, that require that AN add and remove Access loop identification and Characterization over CPE requests and server replies, respectively.

First, is presented DHCP Relay Agent configuration and validation features, followed by PPPoE Intermediate Agent.

5.7.1. DHCP Relay Agent

DHCP Relay Agent (DRA) intercepts upstream packets (DHCP request), append DHCP option 82 (op82), and send it to the upstream. AN configuration for the accomplishment of R-96 is presented below. This configuration enables DRA based on RFC 3046 [52]. Information containing in op82 is presenting in command set bellow. DRA is set on BP 51 (PVC 1/35 of subscriber line #1), ie, BP that is used for VoD and IPTV traffic. S-Vlan 11, C-Vlan 32 and S to C VirtualVlan (1132) creation is identical to HSI vlan referred on chapter "VLAN 1:1 (HSI and VoD VLAN)" (inside section 5.4.2.1).

BP 51 is used due to a DHCP client on PVC 1/35 of CPE, and needs to be identified on IPTV controller platform, to be authenticated and authorized successfully (BP 1 have PPPoE client, which establishes PPPoE session for HSI access).

Configuration

(Upstream packets Filter)

```
$create filter rule entry ruleid 1 action sendtocontrol description
DRA_CNTRL snooplevel bridge
$create filter subrule udp ruleid 1 subruleid 1 srcportfrom 68 srcportcmp eq
$modify filter rule entry ruleid 1 status enable statsstatus enable
$create filter rule map ruleid 1 ifname eoa-51 stageid 1
```

(Downstream packets Filter)

```
$create filter rule entry ruleid 2 action sendtocontrol description
DRA_CNTRL snooplevel bridge
$create filter subrule udp ruleid 2 subruleid 1 srcportfrom 67 srcportcmp eq
$create filter rule map ruleid 2 ifname alleth stageid 1
$modify filter rule entry ruleid 2 status enable statsstatus enable
```

(Intermediate Agent profile)

```
$create ia profile entry profileid 1
$modify ia profile entry profileid 1 acifieldlist AniVal L2Type Chassis
Rack Slot Port Vpi Vci
```

```
$modify ia profile entry profileid 1 chassisval 1 rackval 1 slotval 1
```

DRA Instance

Uplink Interface (BP 50)

```
$create dra instance entry portid 50 vlan 4097 profileid 1 status server
$modify dra instance entry portid 51 vlan 4097 configsuboption portid
portno 1
```

Downlink Interface (BP 51)

```
$create dra instance entry portid 51 vlan 4097 profileid 1 raival
"100512345P5390" status client
```

Modify VLAN 1132 (Virtual Vlan ID) to support DRA:

```
$modify vlan static vlanid 1132 drastatus enable
```

Enable Global DRA:

```
$modify dra global config status enable
```

Results of IA Profile and DRA instance:

```
$get ia profile entry profileid 1
(...)
ACI Field List : AniVal Slot L2Type Port Vpi Vci
Sub Option     : Aci Rai EncapType AccessLoopChar
(...)

$get dra instance entry portid 51
Port Id                      : 51                  VLAN            : 4097
Profile Id                   : 1                 DRA status      :
client
Option82                     : AddAlways
Config Sub-Option            : None
Agent Circuit Id             : -
Remote Agent Id              : 100512345P5390
SyncRateInfoField            : ActualDataRateupstrm ActualDataRatednstrm
MinDataRateupstrm MinDataRatednstrm
DRA Act For Op82 From Client : drop
DRA learning                 : enable            Port No         : -
VCI                          : 35                VPI             : 0
L2 type                      : atm               Encap Type      :
Llcmux
DRA Add Op82 To Unicast      : enable
```

Option DRA Learning enables / disables IP to MAC mapping (learning) by VLAN:

```
$get vlan static vlanid 1132
VLAN Index                    : 1132
Egress ports                  : 50    51
(...)
DRA Status                    : Enable
(...)

$get dra global config
```

```
DRA global Status
-----------------
Enable
```

After CPE synchronization, captured upstream packet from CPE is illustrated in Figure 37.

To disable DRA instance on Bridge Port, accordingly with R-97, following command is used: `$modify dra instance entry portid 51 vlan 4097 status disable`
After the disable of *dra instance* on BP 51, upstream DHCP packets captured on AN uplink does not contain option 82.

Suboptions presented in op82 are:

- 0x01 (01): Agent Circuit ID
- 0x02 (02): Agent Remote ID
- 0x90 (144): Access Loop Encapsulation
- 0x81 (129): Actual Upstream
- 0x82 (130): Actual Downstream
- 0x83 (131): Minimum Upstream
- 0x84 (132): Minimum Downstream

5.7.1.1. Option 82

Using IA profile, AN have the possibility to select which sub options are added on option 82, that accomplish R-98. Follows an example, of insertion of Circuit ID:

```
$modify ia profile entry profileid 1 suboption aci

$get ia profile entry
Profile Id     : 1                  (...)
Aci Prefix Str : -
ACI Field List : AniVal Chassis Rack Slot L2Type Port Vpi Vci
Sub Option     : Aci
(...)
```

It is possible to select the behaviour of AN related to Option 82, by BP, as “disable”, “add always” or “add if not exists”.

```
$modify dra instance entry portid 51 op82
op82 {opts} :                Option to add Option 82 Tag
  disable|AddAlways|AddIfNotExists
```

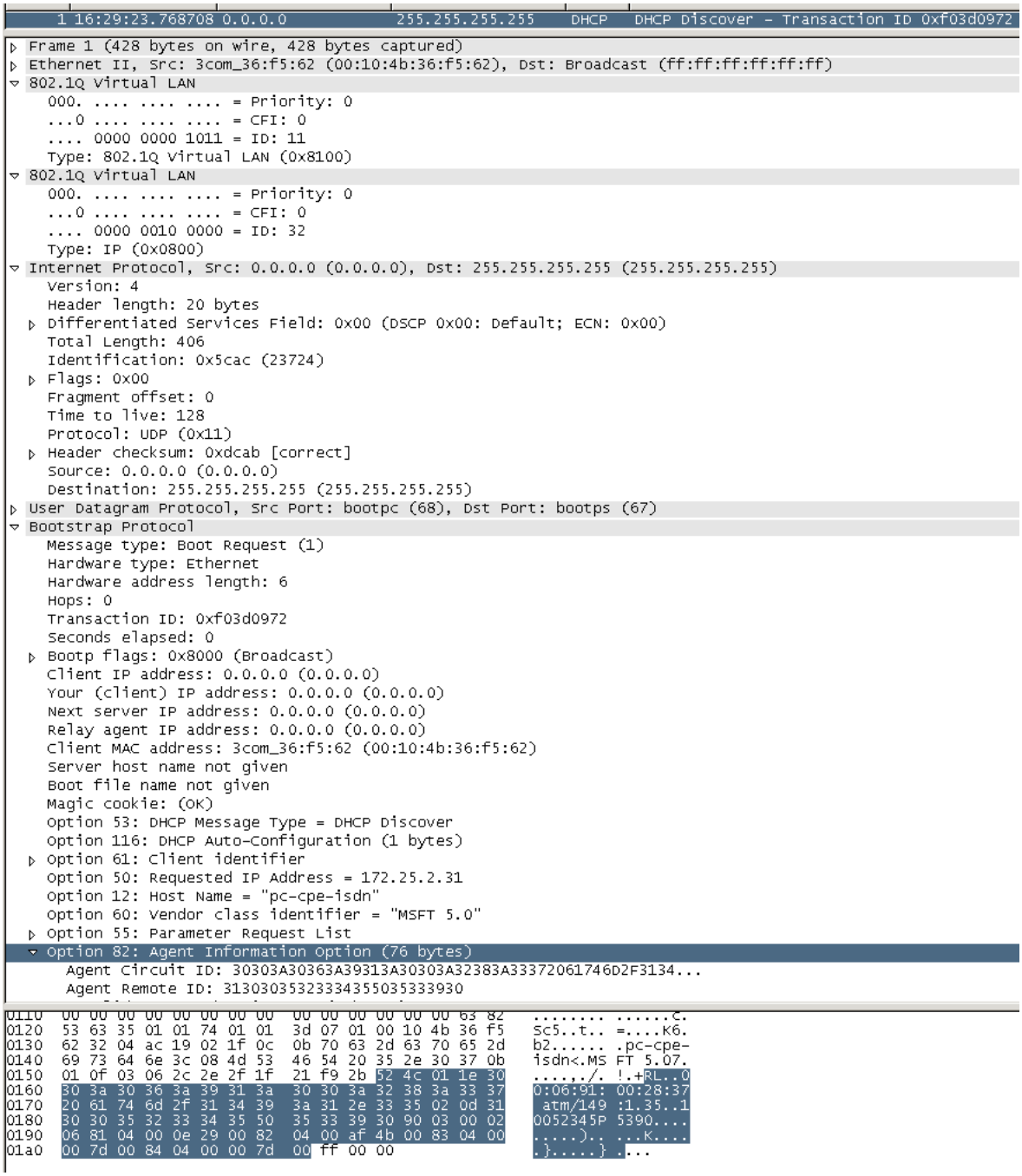

Figure 37 - DHCP Request with op82

Testing option on op82 = disable, option 82 is not added on upstream packets. If op82 = Addalways, upstream packets captured have option 82.

R-99 requires that downstream replies to CPE must be intercepted by AN to remove option 82, and then forward them to CPE. It is an automatic feature of AN.

Using DSL router configured in bridging mode, and connecting a PC device on it, enabling DHCP negotiation (over BP 51), and capturing packets on its interface, the result is accordingly with the requirement. Capturing packets in the uplink of AN, it is possible to check that DHCP upstream packets are delivered to BNG with option 82. Downstream (reply) packets from BNG to CPE have the same option 82. Capturing these (downstream) packets on DSL side, they do not have option 82. It is proved that AN removes option 82 in downstream packets.

5.7.1.2. Forwarding to user ports

Access node DHCP Forwarding based decision (of downstream flow) is:

1. Based on op82 (circuit id, to get destination port)
2. If op82 is not present or if op82 info is invalid, mDSLAM-48 forward packets based on destination MAC address (if DRA learning is enabled);
3. If option 2 fails, checks if Chaddr exists, and for that VLAN find on forwarding DB (based on upstream packets)
4. If all described options failed, packet forward is done based on Vlan configuration

```
$get vlan static vlanid 1132
(...)
Find One Port Fail Act          : TransparentlyForward
```

Available options are:

```
$modify vlan static vlanid 1132 findoneportfailact
findoneportfailact {opts} :                DRA forward Type
  drop|floodtrusted|TransparentlyForward
```

- Drop: drop packets;
- Floodtrusted: packet is flooded to BP that belongs to referred vlan and are configured as trusted;
- TransparentlyForward: forward to all egress BP of referred vlan

Note that, for (1:1) VLAN that have only one CPE egress port and uplink egress port, second and third options have the same behaviour once exists only one subscriber BP for that Vlan.

To approve R-100, 4 different configurations were tested. Those tests were implemented with CPE that have a DHCP client. Follows the configurations and result behaviours:

1. BP Mac learning enable; DRA learning enable; Vlan "FindOnePortFailAct" as drop → Client receives DHCP offer packets (downstream packets);
2. BP Mac learning disable; DRA learning enable; Vlan "FindOnePortFailAct" as drop → Client receives DHCP offer packets (downstream packets);
3. BP Mac learning disable; DRA learning disable; Vlan "FindOnePortFailAct" as drop → Client does not receives DHCP offer packets (downstream packets);
4. BP Mac learning disable; DRA learning disable; Vlan "FindOnePortFailAct" as TransparentlyForward → Downstream DHCP Offer packets are forward to Client.

5.7.1.3. Broadcast to Unicast Packets

Default configuration of DRA on mDSLAM-48 is to forward upstream DHCP packets with source and destination MAC addresses as they are received, that is the expected behaviour of R-101.

```
$get vlan static vlanid 1132
(...)
DRA Bcast To Ucast                : Disable
BNG MAC address                   : FF:FF:FF:FF:FF:FF       (...)
```

Tests already implemented approved this behaviour (see Figure 37).

However, destination MAC address of upstream DHCP packets can be changed from broadcast to unicast, enabling *drabcasttoucast* parameter and detailing *BNGMAC* as a valid MAC address, example 00:03:FA:00:00:02.

5.7.1.4. Giaddr

By default, this parameter is not enabling. Captured packets do not have this option (see Figure 37). This means that R-102 is approved.

5.7.1.5. Discard DHCP Requests – Untrusted Ports

DRA instance allow the behaviour to apply on upstream DHCP packets (on CPE BPs) if they already have option 82: "drop", or "forward", which are options described in R-104.

```
$modify dra instance entry portid 51 vlan 4097 op82fromclientact
op82fromclientact {opts} :Action on receiving option 82  drop|forward
```

This test was implemented with 2 AN, 2 CPEs configured in bridging mode, and 2 PCs (one as DHCP client – PC1- and the other as sniffer – PC2). First access node (AN 1) adds option 82 on upstream DHCP packets from PC1. AN2, have a bridged CPE to which AN1 is connected (and function as client of AN2). Configuration was done over AN2. If op82 is configured as drop, AN2 drop DHCP requests. If configured as forward, it forward packet as is received from CPE (same op82 inserted by AN1). If op82 has value "addIfnot exists", in this case, AN2 does not add op82. If configured as "addalways", AN2 replace received op82 (of AN1) by op82 configured in AN2 for the respective BP.

5.7.1.6. Forwarding to upstream port(s)

R-105 requires that all DHCP requests from subscriber lines are forward only through uplink interface. Once VLANs are configured as ***residential bridging mode***, CPE DHCP requests are always forward through uplink BP.

5.7.1.7. Agent Circuit ID

Agent circuit id is sub-option 1 of option 82 (R-112). It encodes uniquely *dsl* line and AN parameters in the form of string, as "*Access-Node-Identifier atm slot/port:vpi.vci*". This can be automatically or manually generated (R-123 and R-124). One of the automatic parameters used to identify is lower MAC address value (from both GBE interfaces), as mentioned in R-125. Configurations below shows that parameters of agent circuit id are configure manually (as R-126).

Figure 38 belongs to upstream DHCP requests captured in the uplink of AN. It represents agent circuit id with automatic values.

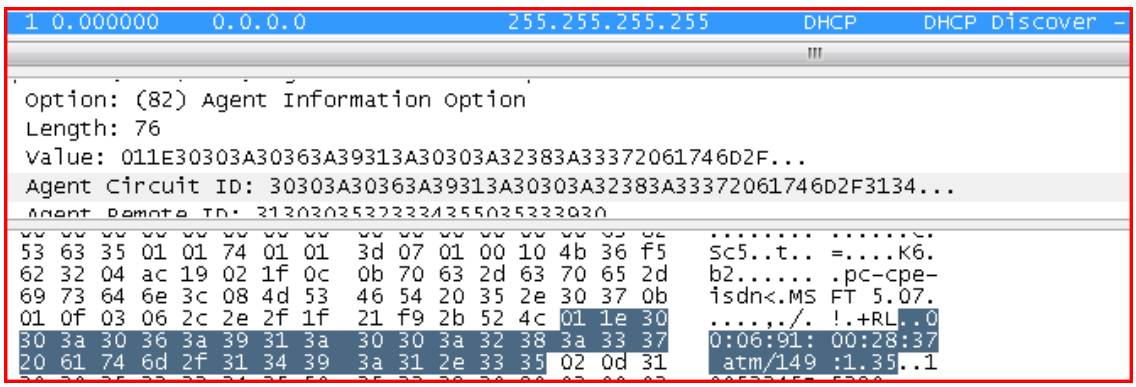

Figure 38 - Agent Circuit ID

Agent Circuit ID (ACI) is configured globally using IA profile:

```
$get ia profile entry profileid 1
(...)
Aci Prefix Str : -
ACI Field List : AniVal Slot L2Type Port Vpi Vci
Sub Option     : Aci Rai EncapType AccessLoopChar
Chassis        : -                 Rack     : -
Frame          : -                 Slot     : -
Sub Slot       : -
```

Possibilities for ACI are:

```
acifieldlist {opts}+ :                Bitmask for agent circuit Id
{AniVal|Chassis|Rack|Frame|Slot|SubSlot|L2Type|Port|Vpi|Vci|VlanTag+|None
```

All of these parameters are automatically obtain, if not specified by user. However, ACI may be configured manually by bridge port DRA instance:

```
$get dra instance entry
Port Id   : 51              VLAN: 4097              (...)
Agent Circuit Id             : -                  (...)
```

BP manual configuration, if mentioned, has precedence over global IA configuration.

This feature was approving with following configuration:

```
$get dra instance entry portid 51 vlan 4097
Port Id          : 51            VLAN            : 4097
Profile Id       : 1             DRA status      : client
Option82         : AddAlways
Config Sub-Option: None
Agent Circuit Id : -
Remote Agent Id  : 10052345P5390
SyncRateInfoField: ActualDataRateupstrm ActualDataRatednstrm MinData
Rateupstrm MinDataRatednstrm
DRA Act For Op82 From Client : drop
DRA learning                 : enable          Port No         : -
VCI                          : 35              VPI             : 1
L2 type                      : atm             Encap Type      : Llcmux
DRA Add Op82 To Unicast      : enable

$get ia profile entry profileid 1
Profile Id     : 1                 ANI Type : auto
ANI value      : -
Aci Prefix Str : -
ACI Field List : AniVal Chassis Rack Frame Slot L2Type Port Vpi Vci
Sub Option     : Aci
Chassis        : 1                 Rack     : 2
Frame          : -                 Slot     : 3
Sub Slot       : -
```

Upstream DHCP packet, receives following ACI result on op82: “00:06:91:00:28:37 atm 123 /149:1.35” (Figure 38). Which corresponds to

- AN MAC address (Auto AN identification (if not specified, lower MAC address is used – this can be changed, configuring ANIVAL parameter)

- Atm (L2 type)
- Chassis, Rack and Slot (123);
- Port id: (149)
- VP/VC (1/35)

Maximum number of characters is only 63 (as defined in R-122), if user tries to configure more than 63, it returns error:

```
$modify dra instance entry portid 51 vlan 4097 configsuboption aci acival
"012345678901234567890123456789012345678901234567890123456789012345678901234567890123"
Error: Invalid parameter length
acival "<name>"
```

5.7.1.8. Agent Remote ID

Selection of Agent Remote id (ARI) sub-option is configure on IA profile, and is a manual defined value (as R-113 defines):

```
$modify ia profile entry profileid 1 suboption
suboption {opts}+ :                  Bitmask for Option tag
  {Aci|Rai|EncapType|AccessLoopChar}+|None
```

Value of ARI is configured by DRA instance on each BP:

```
$get dra instance entry portid 51 vlan 4097
(...)
Remote Agent Id                : 10052345P5390
(...)
```

If ARI have more than 63 characters, AN returns error message (as defined in R-113, ARI must not exceed 63 characters, identically to R-122 related to ACI).

After the configuration of ARI and, after CPE synchronization, DHCP captured packets on AN uplink have Remote ID as “10052345P5390” (Figure 39).

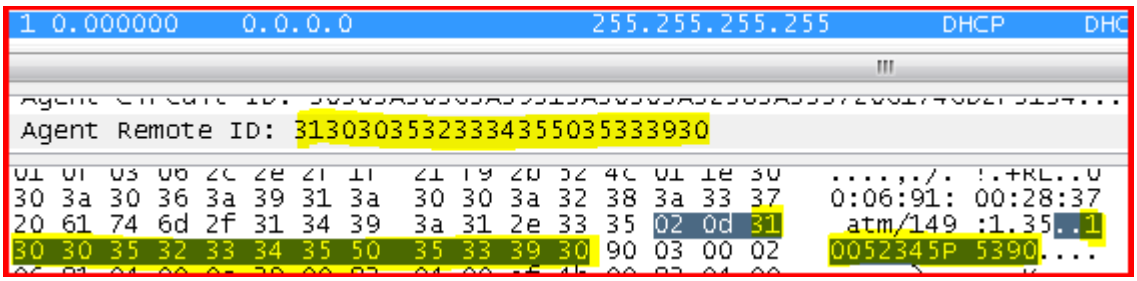

Figure 39 - Agent Remote ID

5.7.1.9. Vendor-specific Options

IA profile has option to select if vendor-specific info is inserting in option 82 or not. This option is accordingly with R-114, and is referred as “AccessLoopChar”.

```
$get ia profile entry profileid 1
(...)
Sub Option      : Aci Rai AccessLoopChar
(...)
```

DRA instance selects which parameters are select. Example:

```
syncratefields {opts}+ :                Bitmask for Sync rate info sub option
  {ActualDataRateupstrm|ActualDataRatednstrm|MinDataRateupstrm|
  MinDataRatednstrm|AttainableDataRateupstrm|AttainableDataRatednstrm|
  MaxDataRateupstrm|MaxDataRatednstrm|MinLpDataRateupstrm|MinLpDataRatednstrm|
  MaxDelayupstrm|ActualDelayupstrm|MaxDelaydnstrm|ActualDelaydnstrm}+|None
```

Using following command set information that corresponds to sub-options 0x81 (129), 0x82 (130), 0x83 (131) and 0x84 (132), is illustrated in Figure 40:

```
$get dra instance entry portid 51 vlan 4097
(...)
SyncRateInfoField             : ActualDataRateupstrm ActualDataRatednstrm
MinDataRateupstrm MinDataRatednstrm       (...)
```

Comparing captured packets (Figure 40) with output of commands below, it is possible to check that values inserted in packets are correct (example for actual downstream data rate – sub-option 0x82 (130)):

```
$get adsl atuc channel ifname dsli-1
(...)                Curr Tx Rate(bps)          : 11488000
(...)
```

0x00af4b00 <-> 11488000 (bps)

This result concludes that vendor specific options are inserted as expected.

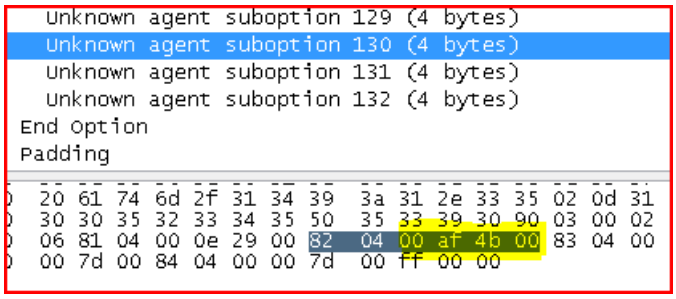

Figure 40 - Sub-option 0x82 – Actual Downstream data rate

5.7.1.10. DHCP Statistics

Access Node provide DHCP Relay Agent statistics, by BP:

```
$get dra global stats portid 51              Port Id          : 51
```

```
                DHCP Received                          DHCP Sent
DHCP Discover   : 1   DHCP Request : 1       DHCP Discover   : 0   DHCP Request : 0
DHCP Release    : 0   DHCP Ack     : 0       DHCP Release    : 0   DHCP Ack     : 1
DHCP Nack       : 0   DHCP Inform  : 0       DHCP Nack       : 0   DHCP Inform  : 0
DHCP Decline    : 0   DHCP Offer   : 0       DHCP Decline    : 0   DHCP Offer   : 1
                DHCP Discarded               DHCP Invalid    : 0
DHCP Discover   : 0   DHCP Request : 0
DHCP Release    : 0   DHCP Ack     : 0       $get dra stats entry portid 52
DHCP Nack       : 0   DHCP Inform  : 0       Port Id : 52            VLAN  : 4097
DHCP Decline    : 0   DHCP Offer   : 0       Dhcp Pkt Received  : 2  DhcpPktSent:2
                                             Dhcp Pkt Discarded : 0
```

Where:

- *Dhcp Pkt Received* is the sum of received packets (includes Discover and Request packet)

- *Dhcp Pkt Sent* is the sum of sent packets by BP (includes Offer and Ack packet).

5.7.2. PPPoE Intermediate Agent

Following configuration is enough to satisfy the list of requirements of TR-101 accordingly to PPPoE Intermediate Agent (PIA): R-115, from R-118 till R-127, R-129 and R-131. Detailed information can be found in AN documentation [30] and TR-101 requirements [21]. This configuration is implemented over BP 1 (S Vlan id 9, and C-Vlan id 32), where CPE that is connected have a PPPoE client that tries to establish a PPP session with BBRAS of Internet Access Service Provider.

```
$ create filter rule entry ruleid 1 action sendtocontrol description
PIA_CTRL snooplevel bridge
$ create filter subrule ether ruleid 1 subruleid 1 ethertypefrom 0x8863
ethertypecmp eq
$ modify filter rule entry ruleid 1 status enable statsstatus enable
$ create filter rule map ruleid 1 ifname eoa-0 stageid 1
$ create ia profile entry profileid 1

$ create pia instance entry portid 1 vlan 4097 profileid 1 status enable
$ create vlan static vlanname HSI vlanid 9 piastatus enable
$ modify pia global config status enable
```

This configuration was tested and the equipment has the behaviour accordingly to requirements (Figure 41). Although, the behaviour of PIA is very similar to DRA, once the goal is the same, where the only difference resides in different packets in negotiation establishment.

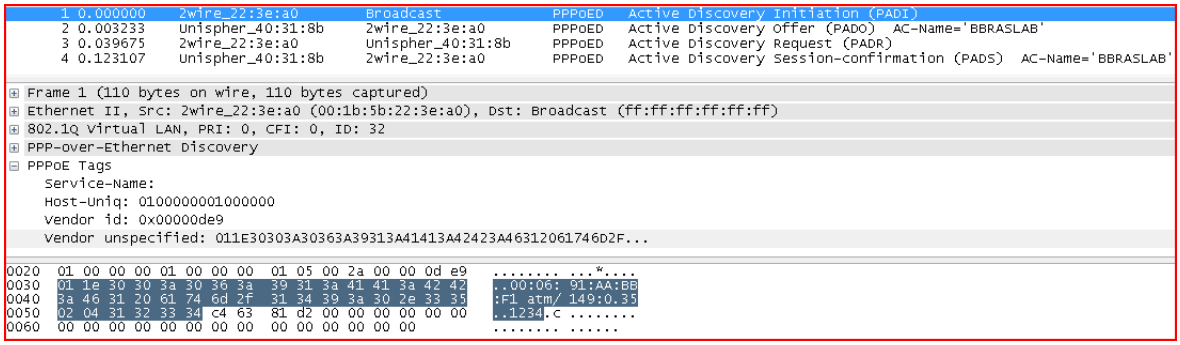

Figure 41 - PPPoE Access Loop Identification TAG

5.8. Multicast / IGMP Snooping

5.8.1. Characteristics

5.8.1.1. Global Parameters

Following command returns IGMP snoop global parameters (by default this is accordingly with RFC 2236 [14], however it is possible to modify each one).

```
$get igmpsnoop cfg info
Query Interval             : 125        Query Response Interval : 10
StartUp Query Interval     : 31         UnSolicRprtInterval     : 10
Anxious Timer              : 125        V1 Host Timer          : 260
Last Member Query Interval : 10         Robustness Variable     : 2
Igmp Snoop Status          : Disable
Version Mask               : v1 v2 v3
Report Suppression Status  : Disable    Proxy Report Status: Disable
StartUp QryCount           : 2          Last Member QryCount    : 2
```

Description:

Igmp Snoop Status enable / disable IGMP snoop in the system;

Report Suppression Status enable / disable Report Status in the system. This is used only for backward compatibility, otherwise, proxy reporting must be used;

Proxy Report Status enable / disable IGMP snoop with Proxy Reporting in the system;

Version Mask: mask IGMP versions supported in the system (IGMP messages from non-supported mask are dropped);

Query Interval: parameter that enables the calculation of Group Membership Interval (GMI). After this amount of time as been achieved, if no reports or queries are received, entry will age out;

Anxious Timer: defines maximum time (seconds) before which the IgmpSnoop module will forward all IGMP membership reports received;

V1 Host Timer: max. time (seconds), for which the IgmpSnooping module can assume that there are Version 1 group members present, for the group for which this timer is running;

Robustness Variable: tune the expected packet loss on the network;

UnSolicRprtInterval: defines interval between unsolicited membership reports of a group sent for robustness no of times (is used only if ProxyReporting is enabled).

LastMembQueryIntvl: defines Last Member Query Interval (LMQI) that is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. A reduced value results in reduced time to detect the loss of the last member of a group.

LastMemberQryCount: (LMQC) defines the number of Group-specific or Group and Source-specific queries sent before assuming there are any listener for this Group.

5.8.1.2. Bridge Port Parameters

```
$get igmpsnoop port info
Port Index                : 51
Port Igmp Snoop Status    : Enable     Leave Mode       : Normal
IGMP Packet's Prio        : 0          MaxGroupAllowed  : 256
Querier Status            : Enable     McastVlan Status : Enable
No McastVlan Match Action : Drop
```

Port Index*:* identifies bridge port for which IGMP snoop is enabled/disabled;

Port Igmp Snoop Status: enable/disable IGMP snoop on the referred BP;

Leave Mode: defines the Leave message processing for that BP;

MaxGroupAllowed: limits number of simultaneous multcast groups allowed on that BP

Querier Status: identifies referred BP as a querier port or not;

McastVlan Status: control the status of Multicast VLAN for that port.

No McastVlan Match Action: defines the action to be taken when multicast VLAN cannot be determined for a port where multicast vlan option is enabled. Drop, Transparently forward as data, and Learn based on ingress VLAN are the values available for that parameter.

5.8.1.3. VLAN Parameters

```
$get vlan static vlanid 111
(...)
Igmp Snoop Action               : TransparentlyForward
Igmpsnoop ProxyReporting Status : Enable
Igmpsnoop ingress Priority      : 5        (...)
```

Igmpsnoop ingress Priority: defines ingress priority to be forced on the incoming frame. It defines the priority configuration per VLAN for IGMP PDUs or proxy report generated by the IGMP proxy function.

Igmp Snoop Action: defines IGMP snooping action as learn, drop or transparently forward (as data) mechanism. This is valid, if IGMP snoop is enabled globally.

Igmpsnoop ProxyReporting Status: defines if for that vlan IGMP snoop act as transparently IGMP snoop or Proxy Reporting snooping.

5.8.1.4. Debug / Statistics

It is possible to check if a determinate multicast group is being delivered at the AN

Example, after customer 1 (STB 1) joins channel group 01:00:5E:20:00:21 and customer 2 (STB2) joins 01:00:5E:20:00:06 multicast group, they are registered on AN:

```
$get bridge mcast forwarding

Vlan Index   : 111        Mac Address : 01:00:5E:20:00:06
Egress ports : 50    52
Group Learnt : 50    52

Vlan Index   : 111        Mac Address : 01:00:5E:20:00:21
Egress ports : 50    51
Group Learnt : 50    51
```

Check if the line card is replicating the multicast group to the bridge ports

Example, if there exists more than one BP registered in the same multicast group:

```
$get bridge mcast forwarding
Vlan Index   : 111        Mac Address : 01:00:5E:20:00:06
Egress ports : 50    51    52
Group Learnt : 50    51    52
```

With the help of the following command (and command above) it is possible to check if a multicast group is being delivered to the customer side:

```
$get interface stats ifname eoa-51
(...)
In Mcast Pkts      : 63            Out Mcast Pkts     : 321173
(...)
```

The press of last command more than once, if the output of "Out Mcast Pkts" is being increased (as fast as enough), at the same time that it is possible to check if BP is registered on a multicast channel using command related to multicast forwarding database, the user concludes that frames are being delivered to the customer.

5.8.2. Tests

5.8.2.1. Configuration

Configuration accordingly with scenario of Figure 33 is presented below. This scenario has a dedicated Multicast Vlan (N:1). Note that, BPs 51, 52, … which are marked as VoD default Vlan (1:1), are used for the transmission of Multicast traffic. So, using IGMP snooping it is possible to snoop IGMP reports from CPE and forward them to Multicast

Vlan (accordingly to the configuration), and downstream multicast traffic is delivered to the subscriber through multicast Vlan over PVCs 1/35.

General configuration of multicast Vlan and IGMP Snooping with Proxy Reporting:

Configuration set of Multicast VLAN and priority (defining port members accordingly with R-218):

```
$ create vlan static vlanid 111 vlanname IPTV egressports 50 51 52
untaggedports 50 51 52
$ create vlan svlan svlanid 111 svlantype residential
$ create vlan virmap svlanid 111 cvlanid 4097 vvlanid 111
$ modify vlan static vlanid 111 drastatus disable
$ modify vlan static vlanid 111 igmpsnoopingressprio 5
```

C-Vlanid as 4097 (Unregistred Vlan) means that C-Vlan "does not matter", and, once BP 50 (uplink) interface is an untagged port, Vlan 111 is defined as N:1 VLAN.

Filter rule that enables snoop and forwarding of IGMP packets to IGMP SNOOP agent module, that will process IGMP frames:

```
create filter rule entry ruleid 3 action sendtocontrol* description
IGMP snooplevel bridge applywhenreq enable
create filter subrule ip ruleid 3 subruleid 1 prototypefrom 2
prototypecmp eq
modify filter rule entry ruleid 3 status enable statsstatus enable
create filter rule map ruleid 3 ifname eoa-51 stageid 1
(...)
create filter rule map ruleid 3 ifname alleth stageid 1
```

* In filtering rule, if action is defined as *copytocontrol*, IGMP reports are forwarded to multicast Vlan, and a copy is also forwarded to 1:1 VoD Vlan. Using *sendtocontrol*, IGMP frames are forwarded only through Multicast Vlan.

It is necessary to enable IGMP Snooping as Learn in VoD VLAN to allow the snoop of IGMP messages from CPEs to multicast VLAN (this configuration is accordingly with R-221, which requires the enabling/disabling of IGMP snoop per Vlan basis):

```
$modify vlan static vlanid 1132 igmpsnoopaction Learn
```

Enable *Igmpsnoop* per bridge port, indicating that, subscriber ports are not *querier* ports.

```
$ modify igmpsnoop port info portid 50 status enable
$ modify igmpsnoop port info portid 51 status enable mcastvlanstatus
enable querierstatus disable
```

Creating Multicast VLAN requires the definition of allowed multicast groups. Defining *grpipaddr* as 0.0.0.0, system accepts requests for any multicast groups on the set of port list, which complements R-218:

```
$ create igmpsnoop mvlan config grpipaddr 0.0.0.0 srcipaddr 0.0.0.0
vlanid 0 mcastvlanstag 111 mcastvlanctag none portlist 51 52
```

Command above configures group ip address and / or source IP address allowed on a multicast Vlan. Using *0.0.0.0* value means that any IP group / source is allowed. Referred command is approved by R-219 of TR-101. Validation feature can be checked in sub-section 5.8.2.4.

Activate ProxyReporting in Vlan 111 and globally in the system:

```
$modify igmpsnoop cfg info proxyreportstatus enable
$modify igmpsnoop cfg info status enable
$modify igmpsnoop cfg info reportsup enable

$modify vlan static vlanid 111 igmpsnoopaction TransparentlyForward
igmpsnoopproxyreporting enable
$modify vlan static vlanid 111 igmpsnoopaction Learn
```

This configuration allows that AN distribute multicast traffic over subscriber lines 1 through multicast Vlan (.1Q) 111, using IGMP Snooping with Proxy Reporting (which approves also R-216). The configuration for the remaining subscriber ports is identical, using correspondent bridge and *eoa* ports (BP 52, 53 … and *eoa-52, eoa-53,* …).

Using architecture represented on Figure 31, STB is now able to get multicast channels, and check if they are being submitted in the AN, using commands presented in section 5.8.1.4.

5.8.2.2. Identification and Processing IGMP messages

TR-101 requirement R-202 defines that IGMP snoop must be selected by BP and/or VLAN.

To disable on a port, and allow that messages are transparently forward:

```
$modify igmpsnoop port info portid 51 status disable
```

To disable on a VLAN:

```
$modify vlan static vlanid 1132 igmpsnoopaction TransparentlyForward
```

Tests return (with one or the other configuration above) that IGMP packets are not forwarded to Multicast Vlan N:1, but they are forwarded through 1:1 VoD Vlan – multicast channels stop to be delivered to STB.)

5.8.2.3. Dropping IGMP messages

R-203 defines that IGMP messages can be discarded by port and/or VLAN.

Drop by:

→ Vlan: `modify vlan static vlanid 1132 igmpsnoopaction drop`

→ Port: `$modify igmpsnoop port info portid 51 status disable`

Testing this configuration returned that IGMP reports from CPE are not dropped; because they are forwarded trough 1:1 Vod Vlan (command only disables IGMP snoop module on BP 51). To discard IGMP packets and do not forward them through any VLAN, it is necessary to apply a filter, as example:

```
$create filter rule entry ruleid 4 action drop
$create filter subrule ip ruleid 4 subruleid 1 prototypefrom 2 prototypecmp eq
$modify filter rule entry ruleid 4 status enable
$create filter rule map ruleid 4 ifname eoa-51 stageid 1
```

After this, tests returned that IGMP messages from CPE are discarded by Access Node on referred BP.

5.8.2.4. Matching and Non-Matching Groups

R-204 defines that AN must have the possibility to configure matching groups for a multicast VLAN. Following command allow the configuration of a matching group mapped to a list of bridge ports. By default, the configuration used accept any multicast group joining, however, for this requirement it is necessary to remove configuration that is described on 5.8.2.1, and refers explicitly the matching multicast group.

```
$create igmpsnoop mvlan config grpipaddr 232.32.0.6 srcipaddr
0.0.0.0 vlanid 0 mcastvlanstag 111 mcastvlanctag none portlist 51
```

On BP 51 (subscriber 1), when user tries to get a multicast channel different than 232.32.0.6, it is not received because it is restricted only to *Multicast matching groups*

configured, and *join requests* are dropped in BP. So, 232.32.0.6 requests are forwarded through vlan 111, and the remaining requests are discarded by AN.

To allow the forwarding of message requests related to "non-matching" groups, filter rule of IGMP_SNOOP module is configured with "*copytocontrol*" option (section 5.8.2.1). Requests for multicast group "232.32.0.6" are forwarded through both VLANs (VOD and multicast), and message requests for "232.32.0.1" are forwarded only through VOD VLAN.

Test used to approve R-205 that refers to IGMPv3 requests of a mix of matching and non-matching groups in the same message, was done with help of Spirent TestCenter [45]. Using configuration presented in last section, and configuring the source to require more than one Multicast group, as example, beyond of 232.32.0.6 also 239.5.5.1 and 239.255.255.250 multicast groups. Only a packet related to the request of 232.32.0.6 is forward to the uplink. IP source used is 0.0.0.0, because it is an original request from AN.

5.8.2.5. Multicast traffic from user port

Injecting multicast traffic from subscriber line to the AN using VLC tool [53] with a video stream, AN forwards traffic through 1:1 VoD Vlan of the corresponding BP. To drop this traffic injection as defined in R-206, AN needs a filtering rule that is applied in subscriber bridge ports to stop multicast traffic injection.
Following filter set is an example. Multicast stream is UDP packet based, and destination MAC address is a multicast MAC based. However, it needs a negation of broadcast packets, to allow that broadcast are forwarded to 1:1 VoD vlan.

```
$create filter rule entry ruleid 5 action drop
$create filter subrule generic ruleid 5 subruleid 1 offsethdr
ethernet offset 0 mask 0x01000000 valuefrom 0x01000000 gencmp eq
$create filter subrule generic ruleid 5 subruleid 2 offsethdr
ethernet offset 0 mask 0xFFFFFFFF valuefrom 0xFFFFFFFF gencmp neq
$create filter subrule generic ruleid 5 subruleid 3 offsethdr
ethernet offset 4 mask 0xFFFF valuefrom 0xFFFF gencmp neq
$modify filter rule entry ruleid 5 status enable statsstatus enable
$create filter rule map ruleid 5 ifname alleoa stageid 1
```

After filter configuration, the injection of a video stream was done, and UDP streams are being dropped by AN. It is possible to check it with filtering statistics:

```
$get filter rule stats ruleid 5
```

```
Rule Id : 5          Num Hits : 2394
```

Ping requests (broadcast packets) are forwarded normally to the uplink, by 1:1 VoD Vlan.

5.8.2.6. Discard IGMP Queries from user ports

By default, disabling *querier* port on BP *igmpsnooping* related configuration, AN automatically drop *Querier* Messages from CPE side, as defined in R-207.

This feature was tested with success, connecting a CPE modem as bridging mode, and connecting a multicast router that sends IGMP Queries. Those queries are not forwarded to uplink in any VLAN (Multicast or VOD). Changing IGMP Snoop action parameter of VoD VLAN as "transparentlyforward" instead of "learn", IGMP queries are transparently forwarded through VOD VLAN.

5.8.2.7. Rate Limit IGMP messages from user ports

Accordingly with R-208, AN must rate limit IGMP messages received in user ports. Configuration for this purpose is as follows (detailed information can be found in Media DSLAM Application Notes [31]). Filtering rule associated to a profile with an algorithm (single rate two color marker) is used:

```
$create filter rule entry ruleid 100 action ratelimiter actionval 0x0010
$create filter subrule igmp ruleid 100 subruleid 1
$create filter rule map ruleid 100 ifname all stageid 1
$modify filter rule entry ruleid 100 status enable statsstatus enable

$create rl profile info profileid 1 rate 100 mbs 80 type sr2cm level
packet
$create rl actionprofile info profileid 1 result conform action allow
$create rl actionprofile info profileid 1 result violate action drop
$create rl instance info instanceid 1 profileid 1 actionprofileid 1
$create bridge rlinstance map portid all instanceid 1 flowtype 16
```

This test was not possible to approve, because there was no conditions to check if the "rate limiting" is overloaded or not.

5.8.2.8. IGMP versions supported

R-209 requires that AN supports IGMP v3 as defined in RFC 3376 [15]. This feature must be configurable per VLAN basis, but AN defines the version to be used globally. Version mask defines the supported versions.

```
$get igmpsnoop cfg info
(...)    Version Mask                : v1 v2 v3    (...)
```

Disabling ProxyReporting feature in multicast VLAN, its behaviour is IGMP Transparent Snooping:

```
$modify vlan static vlanid 111 igmpsnoopaction TransparentlyForward
igmpsnoopproxyreporting disable
```

In this case, with report suppression disabled, all IGMP messages from subscribers are forward to the uplink. Connecting STB1, and requesting multicast group 232.32.0.6, its request is forward to the uplink (with original source IP address of CPE1). Requesting from STB2 in the second subscriber line the same multicast group, the request is also forward to the uplink (with source IP address of CPE2), and both entries (BP 1 and 2) are learned in multicast database for multicast group 232.32.0.6. The same test, using IGMPv1 and IGMPv2 requests are sent successfully to the multicast Vlan.
Removing supported version v1 and v3 from the list of version mask, IGMP messages of v1 and v3 are dropped, and IGMPv2 packets are transparently forward and learned in multicast database.

R-247 and R-248 defines the configuration of IGMPv3 proxy reporting that must be configurable on a per VLAN basis. AN allows the selection on multicast VLAN of *ProxyReporting* enable or disable. To use Proxy Reporting it must be also globally enabled in the system.

```
$modify igmpsnoop cfg info proxyreportstatus enable
```

Above command enabling Proxy Reporting globally and command below is used for VLAN purpose.

```
$modify vlan static vlanid 111 igmpsnoopaction TransparentlyForward
igmpsnoopproxyreporting enable
$modify vlan static vlanid 111 igmpsnoopaction Learn
```

5.8.2.9. Snooping IP Addresses / MAC level filter

R-210 of TR-101 defines that AN must snoop multicast source IP address and destination IP group address from IGMPv3. From this it must set the corresponding MAC group address, entering it in the multicast database forwarding. Tests related to snooping source IP address weren't possible to implement because STBs and RG used didn't have the possibility to insert IP Source in IGMPv3 messages.

In the meanwhile, multicast MAC address is snooped and learned in multicast database forwarding table:

```
$get bridge mcast forwarding

Vlan Index    : 111                    Vlan Index    : 111
Mac Address   : 01:00:5E:05:05:01      Mac Address   : 01:00:5E:20:00:21
Egress ports  : 50    51               Egress ports  : 50    51
Group Learnt  : 50    51               Group Learnt  : 50    51
```

This table is dynamically updated (create and delete) when AN receives IGMPv3 messages from subscriber lines to join or leave a multicast group, which is accordingly with R-211.

5.8.2.10. IGMP Immediate Leave

R-212 defines that AN must support immediate leave on user ports, when using in transparent snooping. AN support fast or normal leave modes. Test was done with BPs (51 and 52) configured as fast and both subscribers joined to multicast group 232.32.0.6. After leave message of first subscriber (and capturing packets in CPE bridging mode), traffic stops to be received (AN removes BP 51 from that multicast entry). BP 52 is not affected and continues to receive multicast traffic.

5.8.2.11. Dropping IGMP Leave for group 0.0.0.0

R-214 defines that leave messages for group “0.0.0.0” must be discarded by AN. Using traffic generator to simulate a request of join and leave messages for “0.0.0.0” group. Packets are dropped in BP (checking statistics of discarded packets, they increase for each packet received), and there are no packets in the uplink side.

5.8.2.12. Marking Priority in IGMP Traffic

R-215 defines that IGMP upstream packets must be prioritized by AN with configured priority-bits.

```
$modify vlan static vlanid 111 igmpsnoopingressprio 5
```

R-250 defines that, Proxy-Reporting function, must insert priority bits in IGMP traffic initialized by AN. Figure 42 illustrates responses to query messages, with priority as 5.

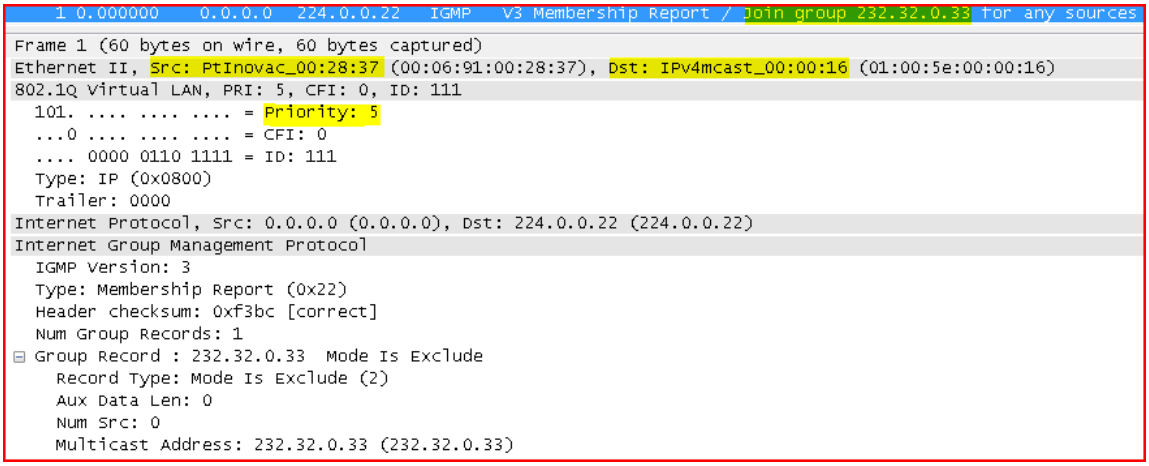

Figure 42 - IGMPv3 Report from Access Node

5.8.2.13. Statistics

R-217 requires a list of detailed statistics by VLAN, DSL port by VLAN, and by multicast. AN does not provide all statistics referred in the list. Meanwhile it supports the following list of statistics:

VLAN, or bridge port and multicast group (or all):

```
$get igmpsnoop port stats

VLAN Index           : 111
Mcast Group Address  : 01:00:5E:20:00:21
Port Index           : 51
Query Received       : 5          Report Received : 8
(...)
```

Forwarding Multicast database:

```
$get bridge mcast forwarding
Vlan Index    : 111        Mac Address : 01:00:5E:05:05:01
Egress ports : 50    51
Group Learnt : 50    51
(...)
```

Most of statistics are listed values, instead of a nominal number of a referred action. That is, AN returns a detailed list of active groups, instead of returning the total “number” of active groups, as example.

To check if a multicast group is being received by AN, a filter rule can be used:

```
$ create filter rule entry ruleid 4 action allow description
IGMP_DEBUG__COUNT_GROUP
$ create filter subrule ether ruleid 4 subruleid 1 dstmacaddrfrom
01:00:5e:20:00:06 dstmacaddrcmp eq
$ create filter rule map ruleid 4 ifname alleth stageid 1
```

```
$ modify filter rule entry ruleid 4 status enable statsstatus enable
```

As multicast group 232.32.0.6 is receiving in the uplink, the statistics are incremented:

```
$get filter rule stats ruleid 4
Rule Id : 4          Num Hits : 9558
$get filter rule stats ruleid 4
Rule Id : 4          Num Hits : 9758
(...)
```

5.8.2.14. Simultaneous Multicast groups per Port

R-220 defines that BP must have a parameter that limits simultaneous multicast group for that BP. Access node command used is:

```
$get igmpsnoop port info portid 51
(...)          MaxGroupAllowed  : 256      (...)
```

Changing parameter to value "1", and using 2 STBs in the same subscriber line (BP 51), each one requiring a different multicast group at the same time, only one STB (the first that request a multicast group) receives multicast group – because it is the first that requested, and AN learns the first request. If second STB requests the same multicast group of STB1, it receives also multicast group. Changing *maxgroupallowed* value from "1" to "2". Both STBs are able to receive different multicast streams at the same time.

5.8.2.15. IGMP Proxy Query Functions

R-249 defines that AN must function as proxy reporting for query functions. Capturing packets in both uplink and downlink sides, where CPE1 is receiving multicast. After a general query from multicast router, AN generates a General Membership Query (GMQ) to subscriber lines that have at least one multicast group registered in AN.

Also, as referred in named point "Leave Mode" of 4.4.9 sub-section, when BP is configured as Normal (or Fast Normal) leave mode, after CPE "leave" message (Figure 43), AN generates a General Specific Query (GSQ) asking if user "really wants to leave the group" (Figure 44).

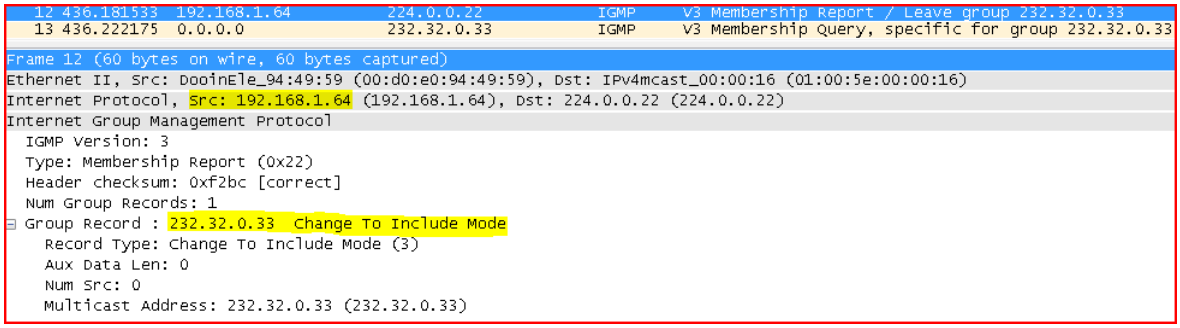

Figure 43 - Subscriber leave message of group 232.32.0.33

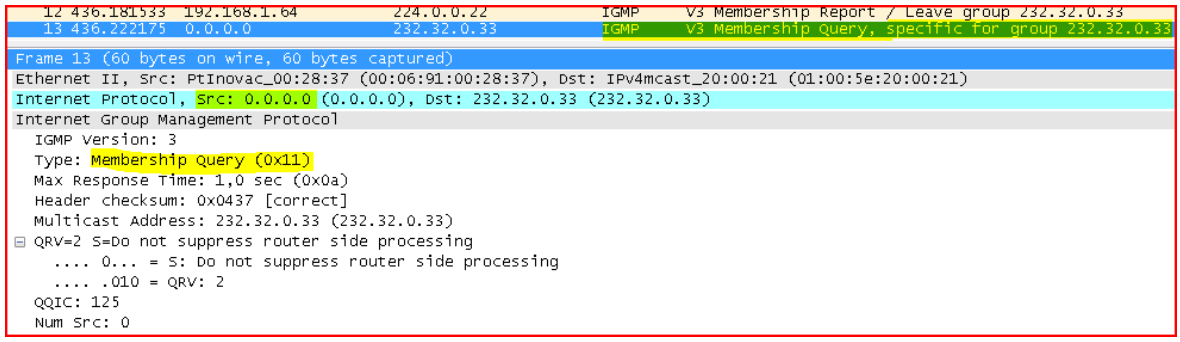

Figure 44 - Specific Query from Access Node to CPE

5.9. QoS

Most of test demonstrations of the next subsections are mainly in subsection “PVC Bundle” (5.9.4) which is able to demonstrate traffic mapping used for QoS.

5.9.1. Traffic Classes and Queues

AN have 8 traffic classes in the system, and 8 queues per DSL (Downlink) and Ethernet (Uplink) Interface. Mapping of priority-bit to queue is configurable (see example below), and is as per R-45, R-46, R-49, R-50, R-53 and R-54.

```
$modify bridge port trfclassmap portid 51 regenPrio 7 trfClass 0
```

This mapping is done based on regenerated priority (obtained from default priority if untagged packet is received, or from priority bit if tagged packet is received, even from CPE or Ethernet side.

```
$get bridge port trfclassmap portid 51
PortId       : 51          regenPrio : 0     TrafficClass : 2
PortId       : 51          regenPrio : 1     TrafficClass : 0
PortId       : 51          regenPrio : 2     TrafficClass : 1
PortId       : 51          regenPrio : 3     TrafficClass : 3
PortId       : 51          regenPrio : 4     TrafficClass : 4
PortId       : 51          regenPrio : 5     TrafficClass : 5
PortId       : 51          regenPrio : 6     TrafficClass : 6
PortId       : 51          regenPrio : 7     TrafficClass : 7
```

(Nomenclature used for TrafficClasse 0 to 7 is mapped on Classid 1 to 8)

Mapping is applied by BP, in which can be defined number of traffic classes used for each BP. That is, depending on mapping table, if 8 p-bits are mapped on all 8 different traffic classes, it is not possible to configure less than 8 classes (For the last example):

```
$get bridge port prioinfo portid 51
(...)  DefaultPriority   : 0          NumTrafficClass : 8    (...)

$modify bridge port intf portid 52 status disable
$modify bridge port prioinfo portid 52 numTrfClass 6
Error: Number of Traffic Classes conflicts with User Priority to
Traffic Class mapping for the given port
```

If untagged traffic is received, it is marked with default priority value, accordingly with above BP configuration.

After marking (or if traffic is tagged and accordingly to received tag p-bit value), it becomes the "user priority" and is processed accordingly with following table map:

```
$get bridge port priomap portid 51
PortId        : 51         UserPriority : 0    RegenUserPrio : 0
PortId        : 51         UserPriority : 1    RegenUserPrio : 1
PortId        : 51         UserPriority : 2    RegenUserPrio : 2
PortId        : 51         UserPriority : 3    RegenUserPrio : 3
PortId        : 51         UserPriority : 4    RegenUserPrio : 4
PortId        : 51         UserPriority : 5    RegenUserPrio : 5
PortId        : 51         UserPriority : 6    RegenUserPrio : 6
PortId        : 51         UserPriority : 7    RegenUserPrio : 7
```

After this process, the association between p-bit and traffic class is used to decide accordingly queue that is used.

Follows an example of how to map priorities on 4 queues,

- priority 0 and 1, mapped on queue 1 (trafficclass 0)
- priority 2 and 3, mapped on queue 2
- priority 4 and 5, mapped on queue 3
- priority 6 and 7, mapped on queue 4

```
modify bridge port trfclassmap portid 51 trfclass 0 regenPrio 0
modify bridge port trfclassmap portid 51 trfclass 0 regenPrio 1
modify bridge port trfclassmap portid 51 trfclass 1 regenPrio 2
modify bridge port trfclassmap portid 51 trfclass 1 regenPrio 3
modify bridge port trfclassmap portid 51 trfclass 2 regenPrio 4
modify bridge port trfclassmap portid 51 trfclass 2 regenPrio 5
modify bridge port trfclassmap portid 51 trfclass 3 regenPrio 6
modify bridge port trfclassmap portid 51 trfclass 3 regenPrio 7
```

5.9.2. Queues Size and Scheduling

Queue sizing is defined in R-57, and is changed with:

```
$modify trfclass profile class profileid 1 classid 1 ?
[ size <dec> ]                    Queue size of the traffic class
(...)
```

Size of queue is defined in number of packets in traffic class.

R-51, R-52, R-55 and R-56 defines that AN must support strict priority scheduling for at least 4 queues, according to an assigned priority and weight.

By default, SPPROFILE exists in the system and it is associated on all ATM and Ethernet interfaces at creation instance. SPPROFILE is a Strict Priority Scheduling.

```
$get atm port ifname atm-1 / eth-1
(...)
ProfileName          : SPPROFILE
(...)
```

Creation of custom profiles can be done as follows:

```
$create sched profile info name teste iftype atm algo custom
```

For Ethernet interface, only "pp" (Probabilistic Priority) algorithm is available; for ATM interfaces, only "custom" algorithm is possible.

```
$create sched profile info name teste1 iftype eth algo custom
Error: Algorithm is not compatible with profile interface type
algo pp|custom
iftype eth|atm
```

PP algorithm: traffic class parameter determines the probability with which its corresponding queue is served when it is polled by the server

Custom: user define (with flexibility) parameters *minimum rate*, *maximum rate*, and *excess bandwidth sharing wheight*. Scheduling is done based on these parameters among classes.

```
$get sched profile info

Profile Name: teste
Scheduling Algorithm : custom     Interface Type : atm

Profile Name         : teste1
Scheduling Algorithm : pp         Interface Type : eth
```

After profile creation, default values of parameters can be changed

```
$get sched profile class name teste
```

```
Profile Name          : teste
Class Id              : 1
Profile Class Param1  : 10          Profile Class Param2  : 0
Profile Class Param3  : 0           Profile Class Param4  : 0
Profile Class Param5  : 0
(...)
Profile Name          : teste
Class Id              : 8
Profile Class Param1  : 80          Profile Class Param2  : 0
Profile Class Param3  : 0           Profile Class Param4  : 0
Profile Class Param5  : 0
```

(Default values of those parameters are calculated as "classid * 10", however their default value is only an indicative value).

To modify profile:

```
$modify sched profile class name teste classid 1 ?
Parameter                           Description
---------                           -----------
[ param1 <dec> ]                     First parameter of the profile
class
       (...)
[ param5 <dec> ]                     Fifth parameter of the profile
class
```

Where,

- **Param1**, specifies the first parameter of class queue in the scheduling profile.
    - For PP algorithm, it is the weight of the class queue (from 1 to 100). If 100 is configured, Strict Priority is used in PP scheduling. This weight will be normalized with the sum of all classid wheights.
    - For Custom algorithm, it specifies excess bandwidth sharing wheight of the class, from 1 to 100.
- **Param2**, specifies the second parameter of class queue in the scheduling profile.
    - For PP scheduling algorithm, it is ignored.
    - For Custom algorithm, it specifies the Minimum bandwidth (Kbps). Zero value means **no minimum** bandwidth guarantee for the class.
- **Param3**, specifies the third parameter of class queue in the scheduling profile.
    - For PP scheduling algorithm, it is ignored.
    - For Custom algorithm, it specifies the Maximum bandwidth (Kbps). Zero value means **no maximum** bandwidth guarantee for the class.
- **Param4** and **Param5**, specifies the fourth and fifth parameters of class queues in the scheduling profile. For PP and Custom algorithms it is ignored.

So,

- Custom algorithm define minimum and maximum bandwidths for each queue;
- PP algorithm define weights for each queue and its behaviour is as WRR (if param1 is 100 –SPPROFILE algorithm is used –param1 is used, and the remaining are ignored)

5.9.3. Traffic Classification

R-58 requires that traffic must be classified with different priority bits depending on classification criteria presented as follows.

User Port: (physical or logical) – it is possible to configure default priority for received untagged packets per BP;

```
$get bridge port prioinfo portid 51
(...)  DefaultPriority   : 4          (...)
```

Ethertype: traffic classification can be applied using filtering rules:
(Example of retagging priority (C-prio, or S-prio) to "5" of packets that accomplish ethertype as 0x0806 – ARP):

```
$create filter rule entry ruleid 1 action retagprio /
retagserviceprio priority 5
$create filter subrule ether ruleid 1 subruleid 1 ethertypefrom
0x0806 ethertypecmp eq
$modify filter rule entry ruleid 1 status enable statsstatus enable
$create filter rule map ruleid 1 ifname alleoa stageid 1
```

Received Ethernet Priority bits: they can be re-mapped in new priority bits accordingly to regeneration table map (see 5.9.1).

IP Protocol ID: using rules, identically to Ethernet rules, however, they are applied on IP layer. Example of mapping new priority bits to IGMP traffic:

```
$create filter rule entry ruleid 8 action retagprio priority 6
$create filter subrule ip ruleid 8 subruleid 1 prototypefrom 2
prototypecmp eq          (IGMP)
$modify filter rule entry ruleid 8 status enable statsstatus enable
$create filter rule map ruleid 8 ifname alleoa stageid 1
```

After this configuration, upstream ARP packets received on AN uplink have C and S-priority 5, IGMP packets have priority 6 and untagged packets from CPE have default priority as 4.

5.9.4. PVC Bundle

PVC bundle is defined in R-59 and R-60, and the priority associated with the packet is used as deciding factor to select the underlying VC. A VC can be mapped to none priority, one or more. All priorities, which are not mapped to any valid VC, are mapped to the default downstream VC.

Two kinds of upstream priority configurations are possible:

- Regeneration priority (*upstrmregenprio*): Only the priority-tagged packet received on the CPE side are tagged (with the *upstrmregenprio*).
- Default Priority (*upstrmdefprio*): Only the priority-untagged packet received on the CPE side are tagged (with the *upstrmdefprio*).

Configuration example:

```
create atm port ifname atm-1 lowif dsl-1
create atm vc intf ifname aal5-1 lowif atm-1 vpi 0 vci 35 enable
create atm vc intf ifname aal5-2 lowif atm-1 vpi 0 vci 36 enable
create atm vc intf ifname aal5-3 lowif atm-1 vpi 0 vci 37 enable

create atm vcaggr map mapid 1 vc aal5-1 dnstrmpriolist 0 1
upstrmdefprio 3 upstrmregenprio 6
create atm vcaggr map mapid 1 vc aal5-2 dnstrmpriolist 2 3
upstrmdefprio 3 upstrmregenprio 6
create atm vcaggr map mapid 1 vc aal5-3 dnstrmpriolist 4 5
upstrmdefprio 2 upstrmregenprio 4

create atm vcaggr intf ifname vcaggr-1 mapid 1 defaultdnstrmvc aal5-
2 enable
create eoa intf ifname eoa-1 lowif vcaggr-1
create bridge port intf portid 1 ifname eoa-1 status enable
```

Tests for this purpose were done with a CPE that supports 4 Ethernet interfaces and WAN interface. So, mapping Ethernet 1, 2 and 3 directly on each PVC (0/35, 0/36 and 0/37, respectively) it is possible to inject and capture traffic to approve the functionalities of PVC bundle in AN.

As described, injecting:

- Downstream traffic with priority:
  - 0 and 1: they are received on Ethernet #1 of CPE
  - 2 and 3: received on Eth 2
  - 4 and 5: received on Eth3
  - Remaining priorities (6 and 7): received on Eth 2
- Upstream traffic through each CPE Ethernet and received in AN uplink interfaces:
  - Eth 1 and Eth 2:

- Untagged traffic: is received with priority bits 3
- Tagged: is received with priority bits 6

- Eth 3:
  - Untagged traffic: is received with priority bits 2
  - Tagged: is received with priority bits 4

Results are accordingly with the specification.

5.10. Interworking Functions

In current scenario, mDSLAM-48 function as a simple bridge, and all Ethernet packets coming from CPE nodes are simply forwarded to WAN side.

However, for legacy systems that are ATM based, CPE are maintained as PPPoA and IPOA as a mechanism for connecting to the service provider. So, AN needs to support PPPoA to PPPoE and IPoA to IPoE inter-working functionality.

5.10.1. IPoA IWF

IPOA IWF is defined by R-63 to R-68 of TR-101.

CPE side:

```
modify adsl line intf ifname dsl-1 enable
create atm port ifname atm-1 lowif dsl-1
create atm vc intf ifname aal5-1 lowif atm-1 vpi 0 vci 35
create ipoa intf ifname ipoa-1 lowif aal5-1
create macprofile global profileid 1 macaddr 00:06:91:00:28:37
create ipoe intf ifname ipoe-1 lowif ipoa-1 macaddrprof 1
create bridge port intf ifname ipoe-1 portid 1 status enable
```

MAC address profile may assign a MAC address to interfaces (can be used in IPoE and PPPoE interfaces). After profile creation and at IPoE instance creation MAC profile is associated on IPoE interface.

NET side:

Uplink Interface configuration remains the same configuration used in all tests (with LACP and BP id 50). In context of IPoA to IPoE tunnelling, an additional parameter is

configured, ProxyARPstatus, that determines if arp requests would be received and handled through Uplink interface (check upstream configuration – IP route command).

Upstream implementation is similar to a "half router", once downstream flows are MAC address based forwarding, and upstream is IP based lookup. Default route is configured to allow that CPE traffic is always forwarded to WAN side. Default Gateway must be BBRAS IP address, and *ProxyARPconfiguration* allows dynamic *arp* configuration. (Vlan configuration is identical to the configuration presented in section 5.4.2.1).

```
create rid static rid 932
create ip route rid 932 ip 0.0.0.0 mask 0.0.0.0 gwyip 192.168.57.1 ifname ANYWAN
create ip route rid 932 ip 192.168.57.10 mask 255.255.255.255 ifname ipoe-0
ProxyArpStatus enable gwyip 192.168.57.10
create bridge static ucast vlanid 932 ucastaddr 00:60:08:76:55:6A portid 50
```

Tests were made with BBRAS IP address 192.168.57.1, and CPE (IPoA) IP address 192.168.57.10.

Downstream

Packet Decision Procedure is as follows:

1. Receiving packet on NET side destined to IPoE interface;
2. Using destination MAC address and Virtual VlanID (S to C mapping), MAC address lookup happens;
3. IP lookup is required and a limited IP lookup will happen for his IPoE packet. Packet is forwarded based on IP and RID lookup;
4. After success IP lookup, packet is encapsulated in the routed RFC2684 LLC/VC format and sent to CPE side interface (Virtual VLAN ID combination is used to check CPE interface and packet is forwarded to the required interface).

Additional configuration require on BP 50 is a filter for downstream IPoE packet that is forward to processor in order to deliver to Proxy ARP module:

```
$create filter rule entry ruleid 1 action copytocontrol description
IPOE_CONTROL applywhenreq enable
$create filter subrule ether ethertypefrom 0x806 ethertypecmp eq
dstmacaddrfrom ff:ff:ff:ff:ff:ff dstmacaddrcmp eq ruleid 1 subruleid 1
$create filter rule map ifname alleth stageid 1 ruleid 1 orderId 1
$modify filter rule entry ruleid 1 status enable
$modify bridge port intf portid 50 ProxyArpStatus enable
```

Tests

Connecting a CPE terminating IPOA with IP address 192.168.57.10 (configured as Routed RFC 2684 [38]) (default Gateway as 192.168.57.1).

After DSL synchronization, pinging from CPE to another network, it is possible to see (capturing upstream packets on AN NET side):

- Requests from CPE have
  - S-Vlanid = 9, and C Vlan id = 32;
  - Source MAC addres = 00:06:91:00:28:37;
  - Destination MAC address = BBRAS MAC address (00:60:08:76:55:6A);

If AN receives an ARP request from BNG (BBRAS as tested) for IP used by CPE (192.168.57.10), AN replies with MAC address configured in MAC profile (00:06:91:00:28:37) as source MAC address – upstream direction.

Resuming, IPOA function works as the requirements of TR-101.

5.10.2. PPPoA IWF

PPPOA IWF is defined by R-69 to R-76 of TR-101.

Uplink interface configuration remains the same used in above section. CPE side configuration is as follows:

```
create atm port ifname atm-0 lowif dsl-0
create atm vc intf ifname aal5-0 lowif atm-0 vpi 0 vci 32
create pppr intf ifname pppr-0 lowif aal5-0 enable
create macprofile global profileid 1 macaddr 00:bb:cc:dd:ee:f1
create pppoe intf ifname pppoe-0 lowif pppr-0 macaddrprof 1 disable
modify adsl line intf ifname dsl-0 enable

create filter rule entry ruleid 2 action sendtocontrol description PPPR_CONTROL
create filter subrule ppp ruleid 2 subruleid 1 prototypefrom 0xC021 prototypecmp eq
modify filter rule entry ruleid 2 status enable statsstatus enable
create filter rule map ruleid 2 ifname allpppoe stageid 1 orderid 1
modify pppoe intf ifname pppoe-0 enable
create bridge port intf ifname pppoe-0 portid 1 status enable
```

DSLF IWF PPPoE Tag:

```
$create pia instance entry portid 1 vlan 4097 profileid 1 status enable
raival "Teste PTIn"
$modify vlan static vlanid 1 piastatus enable
$modify pia global config status enable
```

```
$modify pia instance entry portid 1 vlan 4097 iwftagfromclientact forward
insertiwfsubop enable
```

Connecting a CPE terminating PPPoA (configured accordingly to RFC 2684 [38]), after DSL synchronization, it is possible to see (capturing upstream packets on AN NET side):

- after session establishment (CPE modem with PPP session up), mDSLAM-48 statistics:

```
$get pppoe session stats ifname pppoe-0
(…) Session Id    : 19      Peer Mac Addr          : 00:14:A9:F1:66:A0
Num of PADI Tx           : 23                  Num of PADI Timeouts  : 14
Num of PADR Tx           : 6                   Num of PADR Timeouts  : 0
Num of PADT Tx           : 5                   Num of PADT Rx        : 1
Num of PADT Rejected     : 0                   Num of PADO Rx        : 6
Num of PADO Rejected     : 0                   Num of Multi PADO Rx  : 0
Num of PADS Rx           : 6                   Num of PADS Rejected  : 0
Num of Malformed Pkts Rx : 0                   Num of Generic Err Rx : 0
Version                  : 1                   Type                  : 1
Connect Time             : Thu Jan 01 14:50:12 1970
Duration (s)             : 19                  (…)
```

- captured packets on uplink are PPPoE encapsulated packets
- session ID acquired, can be checked in statistics above;
- Disconnection BBRAS (forcing a new session), and connecting another CPE to get the same session id as the first CPE, mDSLAM-48 updates session ID (already learned for another session ID). The first one that already was learned gets new session ID.
- Last point was implemented with 2 simultaneous PPPoE sessions active in AN;
- Once, both CPEs share same MAC address, PPPoE sessions are distinguished by "Host-Unic" tag
- Disconnecting CPE, AN sends a PPPoE PADT packets informing BBRAS that this session as been terminated.
- Configuring inactivity timer (example, for 120 seconds), if there are no packets exchanged between CPE and BNG, after 2 minutes session is tear-down (AN sends PADI packets with the goal to re-negotiate session establishment).
- With PIA profile, AN add DSLF IWF PPPoE tag with sub-option code field 0xFE and its length field is 0x00.

- Once CPE does not send PPPoE frames, it is not possible to implement R-85, which is to drop CPE packets if they contain DSL IWF PPPoE tag.

Those tests approved PPPoE to PPPoA Interworking Function.

5.10.3. Multi session Support

It is possible to configure multi-session support, ie, in the same physicl DSL link, it is possible to configure different PVCs that have PPPoA and IPoA interfaces over each one. The configuration is the same as mentioned in last 2 chapters.
It was tested with successfully results.

5.10.4. Auto Sensing On / Off

R-62, when applied auto-sensing off, requires the configuration that is the same performed on Logical Port Configuration (section 5.3).

Related to Auto-Sensing enabled, the configuration is performed as follows:

ATM layer:

```
$create atm port ifname atm-5 lowif dsl-5
```

AAL5 interface, with autostatus enable and auto (encapsulation sensing):

```
$create atm vc intf ifname aal5-5 lowif atm-5 vpi 0 vci 35 mgmtmode
dataandmgmt autostatus enable auto
```

EoA interface (configstatus as config, that is, enable interface after packet reception; and a timer that indicates interface as down):

```
$create eoa intf ifname eoa-5 lowif aal5-5 configstatus config
inactivitytmrintrvl 10
```

PPPoA / PPPoE interface:

```
$create macprofile global profileid 1 macaddr 00:11:22:33:44:55
$create pppr intf ifname pppr-5 lowif aal5-5 configstatus config enable
$create pppoe intf ifname pppoe-5 lowif pppr-5 macaddrprof 1
```

(Conversion of LCP packets from subscriber (PPPoA) to PPPoE):

```
$create filter rule entry ruleid 5 description PPPR_CONTROL action
sendtocontrol
$create filter subrule ppp ruleid 5 subruleid 1 prototypefrom 0xc021
prototypecmp eq
$modify filter rule entry ruleid 5 status enable statsstatus enable
$create filter rule map ruleid 5 ifname pppoe-5 stageid 1

$modify pppoe intf ifname pppoe-5 enable
```

IPoA / IPoE interface:

```
$create ipoa intf ifname ipoa-5 lowif aal5-5 configstatus config enable
$create ipoe intf ifname ipoe-5 lowif ipoa-5 macaddrprof 1 enable
```

Mapping BP 5 over possible interfaces for auto-sensing: pppoe, eoa e ipoe, is using virtual interface “vir-5”.

```
$create bridge port map ifname pppoe-5 portid 5
$create bridge port map ifname eoa-5 portid 5
$create bridge port map ifname ipoe-5 portid 5
$create bridge port intf ifname vir-5 portid 5 status enable
```

Results:

1 - after PPPOE session:

```
$get eoa intf ifname eoa-4
IfName                  : eoa-4      LowIfName    : aal5-4
FCS                     : False
Pkt Type                : ALL
InActivity Tmr Interval : 10
M2VMac Database Id      : none
Config Status           : Config-InUse
Oper Status             : Up         Admin Status : Up

$get ipoa intf
Ifname        : ipoa-0     Low IfName   : aal5-4
Config Status : Config-NotInUse
Oper Status   : dormant    Admin Status : Up

$get pppr intf
Ifname               : pppr-0     Low IfName      : aal5-4
Max PDU Size         : 1492       Ter Ack TimeOut : 5
Lowif Toggle TimeOut : 5
Nature               : dynamic    Config Status   : Config-NotInUse
PPPOA Packet's Prio  : 0
Oper Status          : dormant    Admin Status    : Up
```

2 - after PPPOA session:

```
$get eoa intf ifname eoa-4
IfName                  : eoa-4      LowIfName    : aal5-4
FCS                     : False
Pkt Type                : ALL
InActivity Tmr Interval : 10
M2VMac Database Id      : none
Config Status           : Config-NotInUse
Oper Status             : dormant    Admin Status : Up
```

```
$get pppr intf
Ifname               : pppr-0     Low IfName      : aal5-4
Max PDU Size         : 1492       Ter Ack TimeOut : 5
Lowif Toggle TimeOut : 5
Nature               : dynamic    Config Status   : Config-InUse
PPPOA Packet's Prio  : 0
Oper Status          : Up         Admin Status    : Up

$get ipoa intf
Ifname        : ipoa-0     Low IfName    : aal5-4
Config Status : Config-NotInUse
Oper Status   : dormant    Admin Status : Up
```

As demonstrated, auto-sensing is a good feature to be implemented when the operator have subscriber that uses different CPE features.

Configuration illustrated had a very good behaviour, exchanging CPE configuration on the fly, AN resumes the new sensed interface very well, and service remains available in a few moments.

5.11. Summary

As demonstrated in present chapter, access node is approved to deliver triple-play services accordingly with requirements presented in DSL Forum Technical Report TR-101, which main focus is regarding 1:1 and N:1 VLANs, forwarding mechanisms, link aggregation, DHCP Relay Agent, PPPoE Intermediate agent, multicast Ethernet snooping, quality of service, and interworking functions.

Chapter 6: Conclusions

The work presented in this Thesis overviews the delivery of triple-play services from service and telecommunications providers, using xDSL access technology. The main focus is on the access node features accordingly with TR-101 requirements list.

The architecture used for the delivery of triple-play services is Ethernet based: pure Ethernet in the uplink side (GBE) and Ethernet over xDSL (EoA) technology in the downlink side. Ethernet based architecture facilitates mainly the delivery of multicast streams, using high debit capacities and the layer 3 snooping mechanisms from service provider network to subscriber lines.

This document starts with the overview of actual service provider networks, describing the motivation for the evolution for new services delivery due to the offer of high capacities of xDSL technology. It is complemented with an introduction of standardization organizations that are helpful for the definition of presented requirements and standard definitions. The main important organization is the DSL Forum due to the technical report that is the blueprint of requirements list presented in this thesis. However, ITU-T, IEEE and IETF are very important also, because each one is dedicated to some tasks and technology definitions, that collaborates between them and complementing to each other.

Chapter 3 presented the global architecture defined by DSL forum for the delivery of triple-play services using xDSL technology based access networks. This architecture defines the needs of some basic modules in each network elements. Those indispensable network elements are Broadband Network Gateway for Data, Video and Broadcast services, Ethernet aggregation element (typically a Switch/Router), Access Node and CPE. Enhancing access node, its required main points are the ATM to Ethernet interworking functions, handling of VLAN purposes, access loop identification, security, QoS, and multicasting support. Some functions described require layer 3 processing, such as IGMP, and once access node is a layer 2 equipment, it requires snooping/filtering modules for those functionalities.

Equipment named as mDSLAM-48®, which is an IP DSLAM solution of PT Inovação was designed and developed to function as a "TR-101 required Access node". Hardware and software architectures are presented in chapter 4. The most enhanced functionalities are Ethernet bridge learning and forwarding mechanisms, VLAN, multicast, link bonding, rack and stack, QoS and packet filtering support.

Finally, last chapter (5) reports triple-play features validation accordingly with the list of requirements of DSL forum document. All tests were successfully carried and validated in laboratory scenario, emulating service provider network with IPTV and VOD platform, and Internet access. As expected there are some functionalities that are not totally accordingly, but can be implemented using other approach solutions, as described. Some functionalities need to be upgraded and others implemented in the future.

Tests related to the uplink interface using LACP protocol had been successfully carried in order to be approved for real service functioning. However, there are functionalities that are not available, and others that exist, that should be deeply tested in the future. The functionalities that, at the moment, are not available, are related to Load Balancing, making the hashing of the traffic by MAC address destination, source or destination MAC address, IP source and/or destination address (at the moment, hashing is done only by source MAC address). Tests were done with both LACP interfaces of access node configured as "fast timeout". Protocol allow the use of "slow timeouts", however, this configuration was not tested, because it is not used in the commercial platform.

Other issue is related to VLAN statistics that are not supported in the system. It is possible, only resorting to filter rules. However, filter rules can count statistics for incoming packets, and it is not possible to count packets in the egress direction, due to hardware limitation.

Results of the tests related to priority marking and re-marking are are very intuitive. PVC Bundle tests have results related to queues scheduler that illustrates the behaviour according with the algorithms. However, tests related to Queue sizing are not easier tests because they must be very precise and there were no conditions for their realization. This was impossible to approve.

The tests performed with the objective of approving all triple-play services simultaneously were well conducted using at least, two subscriber lines with two personal computers downloading different files and using http access to different web pages: one STB in each subscriber, using one of them receiving a TV multicast channel, and the other receiving a video on demand stream. Later, zapping was done in the first customer, and the second

STB did not have any changes. In both cases, receiving distinct services did not affect each other.

Present document demonstrates that this Access Node is an add-on value for any service provider that needs to migrate their xDSL technology access network to Ethernet based. Due to its dimension and number of subscriber lines capacity, it is advantageous to be used in sites that serves low density population. A building, or even a hotel where telephony subscriber lines exists, without the possibility to change its infrastructure for an Ethernet based architecture, can implement a solution as the presented access node.

Annex I

Factory Default

```
verbose off
modify bridge tbg info floodsupport disable
modify vlan static vlanid 1 floodsupport disable
create user name root passwd root root
create ethernet intf ifname eth-1
create ethernet intf ifname eth-2
create aggr intf ifname aggr-1 ip 172.25.2.145 mask 255.255.255.192
create lacp aggr aggrifname aggr-1 aggrtype lacp
modify lacp aggrport info ifname eth-1 aggrstatus enable
modify lacp aggrport info ifname eth-2 aggrstatus enable
create bridge port intf ifname uplink portid 50 learning enable fdbmodify enable
modify gvrp port info portid 50 ppstatus enable
modify bridge port intf portid 50 status enable
create vlan static vlanid 2 vlanname GESTAO egressports 50 untaggedports 50
create vlan svlan svlanid 2 svlantype residential
create vlan virmap svlanid 2 cvlanid 2 vvlanid 2
modify gvrp port info portid 50 portvlanid 2 psvlanid 2
modify aggr intf ifname aggr-1 mgmtvlanid 2 mgmtsvlanid 2
create ip route ip 0.0.0.0 mask 0.0.0.0 gwyip 172.25.2.129
create snmp comm community public ro
create snmp comm community private rw
create snmp host ip 172.25.2.6 community private
create snmp host ip 172.25.2.6 community public
create snmp traphost ip 172.25.2.6 community public version v1 port 1233
create dsl system
create filter rule entry ruleid 1 action sendtocontrol description IGMP snooplevel bridge
applywhenreq enable
create filter subrule ip ruleid 1 subruleid 1 prototypefrom 2 prototypecmp eq
modify filter rule entry ruleid 1 status enable statsstatus enable
create filter rule map ruleid 1 ifname all stageid 1
modify igmpsnoop cfg info status enable proxyreportstatus enable
create filter rule entry ruleid 2 action sendtocontrol description DRA_CNTRL snooplevel
bridge
create filter subrule udp ruleid 2 subruleid 1 srcportfrom 68 srcportcmp eq
modify filter rule entry ruleid 2 status enable statsstatus enable
create filter rule entry ruleid 3 action sendtocontrol description DRA_CNTRL snooplevel
bridge
create filter subrule udp ruleid 3 subruleid 1 srcportfrom 67 srcportcmp eq
create filter rule map ruleid 3 ifname alleth stageid 1
modify filter rule entry ruleid 3 status enable statsstatus enable
create ia profile entry profileid 1 suboption aci rai
create dra instance entry portid 50 vlan 4097 profileid 1 status server
modify dra global config status enable
create sched profile info name ATM-149 algo custom iftype atm
create sched profile info name ATM-150 algo custom iftype atm
(…)
create sched profile info name ATM-195 algo custom iftype atm
create sched profile info name ATM-196 algo custom iftype atm
create atm port ifname atm-1 lowif dsl-1 profilename ATM-149 disable
create atm port ifname atm-2 lowif dsl-2 profilename ATM-150 disable
(…)
create atm port ifname atm-47 lowif dsl-47 profilename ATM-195 disable
create atm port ifname atm-48 lowif dsl-48 profilename ATM-196 disable
modify adsl alarm profile ifname dsl-1 atucinitfailtrap true atucoptrapenable true
modify adsl alarm profile ifname dsl-2 atucinitfailtrap true atucoptrapenable true
(…)
modify adsl alarm profile ifname dsl-47 atucinitfailtrap true atucoptrapenable true
modify adsl alarm profile ifname dsl-48 atucinitfailtrap true atucoptrapenable true
end
```

2 PVC Scenario Configuration

Example of configuration of 3 subscriber lines on mDSLAM-48 accordingly with the scenario presented on Figure 31and Figure 33.

```
create ethernet intf ifname eth-1
create ethernet intf ifname eth-2
create aggr intf ifname aggr-1 enable ip 172.25.2.145 mask 255.255.255.192
create lacp aggr aggrifname aggr-1 aggrtype lacp
modify lacp aggrport info ifname eth-1 aggrstatus enable
modify lacp aggrport info ifname eth-2 aggrstatus enable
create bridge port intf portid 50 ifname uplink
modify gvrp port info portid 50 ppstatus enable
modify bridge port intf portid 50 status enable
create vlan static vlanid 2 vlanname GESTAO egressports 50 untaggedports 50
create vlan svlan svlanid 2 svlantype residential
create vlan virmap svlanid 2 cvlanid 2 vvlanid 2
modify gvrp port info portid 50 portvlanid 2 psvlanid 2
modify aggr intf Ifname aggr-1 mgmtvlanid 2 mgmtsvlanid 2
create ip route ip 0.0.0.0 mask 0.0.0.0 gwyip 172.25.2.129
create dsl system
modify adsl line profile ifname dsl-1 atucgstxstartbin 0x20 atucgsrxendbin 0x1F
modify adsl line profile ifname dsl-2 atucgstxstartbin 0x20 atucgsrxendbin 0x1F
modify adsl line profile ifname dsl-3 atucgstxstartbin 0x20 atucgsrxendbin 0x1F
create atm port ifname atm-1 lowif dsl-1
create atm vc intf ifname aal5-1 lowif atm-1 vpi 0 vci 35
create eoa intf ifname eoa-1 lowif aal5-1
create bridge port intf ifname eoa-1 portid 1 status enable
create atm port ifname atm-2 lowif dsl-2
create atm vc intf ifname aal5-2 lowif atm-2 vpi 0 vci 35
create eoa intf ifname eoa-2 lowif aal5-2
create bridge port intf ifname eoa-2 portid 2 status enable
create atm port ifname atm-3 lowif dsl-3
create atm vc intf ifname aal5-3 lowif atm-3 vpi 0 vci 35
create eoa intf ifname eoa-3 lowif aal5-3
create bridge port intf ifname eoa-3 portid 3 status enable
create vlan svlan svlanid 9 svlantype residential
create vlan static vlanname HSI932 vlanid 932 egressports 1 50 untaggedports 1
create vlan static vlanname HSI933 vlanid 933 egressports 2 50 untaggedports 2
create vlan static vlanname HSI934 vlanid 934 egressports 3 50 untaggedports 3
create vlan virmap svlanid 9 cvlanid 32 vvlanid 932
create vlan virmap svlanid 9 cvlanid 33 vvlanid 933
create vlan virmap svlanid 9 cvlanid 34 vvlanid 934
modify gvrp port info portid 1 psvlanid 9 portvlanid 32 ingressfiltering true
modify gvrp port info portid 2 psvlanid 9 portvlanid 33 ingressfiltering true
modify gvrp port info portid 2 psvlanid 9 portvlanid 34 ingressfiltering true
modify vlan svlan svlanid 9 cvlanpreservemode nonpreserve
modify vlan static vlanid 932 drastatus disable
modify vlan static vlanid 933 drastatus disable
modify vlan static vlanid 934 drastatus disable
create atm vc intf ifname aal5-51 lowif atm-1 vpi 1 vci 35
create eoa intf ifname eoa-51 lowif aal5-51
create bridge port intf ifname eoa-51 portid 51 status enable
create atm vc intf ifname aal5-52 lowif atm-2 vpi 1 vci 35
create eoa intf ifname eoa-52 lowif aal5-52
create bridge port intf ifname eoa-52 portid 52 status enable
create atm vc intf ifname aal5-53 lowif atm-3 vpi 1 vci 35
create eoa intf ifname eoa-53 lowif aal5-53
create bridge port intf ifname eoa-53 portid 53 status enable
create vlan svlan svlanid 11
create vlan static vlanid 1132 vlanname vod32 egressports 51 50 untaggedports 51
create vlan virmap svlanid 11 cvlanid 32 vvlanid 1132
modify gvrp port info portid 51 psvlanid 11 portvlanid 32 ingressfiltering true
modify bridge port intf portid 51 status disable
modify bridge port prioinfo portid 51 defPrio 4
modify bridge port intf portid 51 status enable
create vlan static vlanid 1133 vlanname vod33 egressports 52 50 untaggedports 52
create vlan virmap svlanid 11 cvlanid 33 vvlanid 1133
modify gvrp port info portid 52 psvlanid 11 portvlanid 33 ingressfiltering true
modify bridge port intf portid 52 status disable
modify bridge port prioinfo portid 52 defPrio 4
modify bridge port intf portid 52 status enable
create vlan static vlanid 1134 vlanname vod34 egressports 53 50 untaggedports 53
```

```
create vlan virmap svlanid 11 cvlanid 34 vvlanid 1134
modify gvrp port info portid 53 psvlanid 11 portvlanid 34 ingressfiltering true
modify bridge port intf portid 53 status disable
modify bridge port prioinfo portid 53 defPrio 4
modify bridge port intf portid 53 status enable
create filter rule entry ruleid 1 action sendtocontrol description DRA_CNTRL snooplevel
bridge
create filter subrule udp ruleid 1 subruleid 1 srcportfrom 68 srcportcmp eq
create filter rule map ruleid 1 ifname eoa-51 stageid 1
create filter rule map ruleid 1 ifname eoa-52 stageid 1
create filter rule map ruleid 1 ifname eoa-53 stageid 1
modify filter rule entry ruleid 1 status enable statsstatus enable
create filter rule entry ruleid 2 action sendtocontrol description DRA_CNTRL snooplevel
bridge
create filter subrule udp ruleid 2 subruleid 1 srcportfrom 67 srcportcmp eq
create filter rule map ruleid 2 ifname alleth stageid 1
modify filter rule entry ruleid 2 status enable statsstatus enable
create ia profile entry profileid 1
modify ia profile entry profileid 1 suboption aci rai
create dra instance entry portid 51 vlan 4097 profileid 1 raival "1005123456P5390" status
client
create dra instance entry portid 52 vlan 4097 profileid 1 raival "1005789012P5390" status
client
create dra instance entry portid 53 vlan 4097 profileid 1 raival "1005789012P5390" status
client
create dra instance entry portid 50 vlan 4097 profileid 1 status server
modify dra global config status enable
create vlan static vlanid 111 vlanname IPTV egressports 50 51 52 53 untaggedports 50 51 52
53
create vlan svlan svlanid 111 svlantype residential
create vlan virmap svlanid 111 cvlanid 4097 vvlanid 111
modify vlan static vlanid 111 drastatus disable
modify vlan static vlanid 111 igmpsnoopingressprio 5
create filter rule entry ruleid 3 action sendtocontrol description IGMP snooplevel bridge
applywhenreq enable
create filter subrule ip ruleid 3 subruleid 1 prototypefrom 2 prototypecmp eq
modify filter rule entry ruleid 3 status enable statsstatus enable
create filter rule map ruleid 3 ifname eoa-51 stageid 1
create filter rule map ruleid 3 ifname eoa-52 stageid 1
create filter rule map ruleid 3 ifname eoa-53 stageid 1
create filter rule map ruleid 3 ifname alleth stageid 1
modify igmpsnoop port info portid 50 status enable
modify igmpsnoop port info portid 51 status enable mcastvlanstatus enable querierstatus
disable
modify igmpsnoop port info portid 52 status enable mcastvlanstatus enable querierstatus
disable
modify igmpsnoop port info portid 53 status enable mcastvlanstatus enable querierstatus
disable
create igmpsnoop mvlan config grpipaddr 0.0.0.0 srcipaddr 0.0.0.0 vlanid 0 mcastvlanstag
111 mcastvlanctag none portlist 51 52 53
modify igmpsnoop cfg info proxyreportstatus enable
modify igmpsnoop cfg info status enable
modify igmpsnoop cfg info reportsup enable
modify vlan static vlanid 111 igmpsnoopaction TransparentlyForward igmpsnoopproxyreporting
enable
modify vlan static vlanid 111 igmpsnoopaction Learn
modify adsl line intf ifname dsl-1 enable
modify adsl line intf ifname dsl-2 enable
modify adsl line intf ifname dsl-3 enable
```

Annex II

Access Node main Requirements of TR-101

VLANs

R-04 The Access Node MUST be able to attach an S-Tag to untagged frames received on user ports in the upstream direction.

R-05: The Access Node MUST be able to attach an S-Tag and C-Tag to untagged frames received on user ports in the upstream direction (see 5.4.2.1).

R-06: The Access Node MUST be able to attach an S-Tag to C-Tagged frames received on user ports in the upstream direction (see 5.4.2.2).

R-07: The Access Node MUST be able to remove VLAN Tag identification from frames received from the aggregation network (i.e. downstream direction) before sending them on user ports. The options for removal are S-Tag only, or both S-Tag and C-Tag (see 5.4.2.3).

R-08 The Ethertype field for the 802.1ad tagging, i.e. S-Tags, MUST support at least the standardized value 0x88a8. However, for backward compatibility reason, this field SHOULD be configurable (per Access Node).

R-09: The Access Node MUST allow per port configuration of the 'acceptable frame types' to be one of the following values: 'VLAN tagged', 'untagged or priority-tagged' and 'admit all' (i.e. accepting VLAN-tagged, untagged and priority-tagged frames). Frames not matching the configured 'acceptable frame types' MUST be discarded (see 5.4.2.4)

R-20: For each port configured as 'untagged or priority-tagged' or 'admit all', the Access Node MUST allow the operator to configure whether it should copy the priority marking of the received upstream priority-tagged frame to the S-tag (and C-tag, if applicable) or whether it should override it using an ingress to egress priority mapping (see 5.4.2.5)

R-23: Any untagged or priority-tagged frame received on port configured as 'untagged or prioritytagged' or 'admit all' MUST be tagged with the default tagging, unless matching an Ethertype filter associated with this port (see 5.4.2.6).

R-26: The Access Node MUST be able to assign an Ethertype filter to a given port.
At least the following types MUST be supported
- PPPoE (Ethertype =0x8863 and 0x8864)
- IPoE (Ethertype=0x0800)
- ARP (Ethertype=0x0806)

R-33 the Access Node MUST support the following VLAN allocation paradigms:

- *Assigning the same S-VID to a group of ports. This paradigm is denoted N:1 VLAN to indicate many-to-one mapping between ports and VLAN. Example criteria for grouping are same originating VP, same service, same 'destination' service provider.*
- *Assigning a unique VLAN identification to a port using either a unique S-VID (802.1q VLAN) or a unique (SVID, C-VID) pair (QinQ VLAN). The uniqueness of the S-VID MUST be maintained in the aggregation network. This paradigm is denoted 1:1 VLAN to indicate a one-to-one mapping between port and VLAN.*

General Forwarding Mechanisms

R-34 The Access Node MUST support Link Aggregation according to 802.3ad for link resiliency reasons

R-35 The Access Node SHOULD support Link Aggregation according to 802.3ad for load balancing reasons

R-37 *an Access Node having multiple uplinks (not members of the same 802.3ad link aggregation group) should be able to perform VLAN aware bridging between its uplinks.*

This requirement enables deploying Access Nodes in a ring topology.

R-40: The Access Node MUST be able to prevent forwarding traffic between user ports (user isolation). This behavior MUST be configurable per S-VID

R-44: The Access Node MUST be able to disable MAC address learning for 1:1 VLANs.

QoS

R-45, R-46: The Access Node MUST support at least 4 traffic classes and SHOULD support at least 6 traffic classes for Ethernet frames, and MUST support configurable mapping to these classes from the 8 possible values of the Ethernet priority field.

R-49, R-50, R-53, R-54: The Access Node MUST support at least 4 queues and SHOULD support at least 6 queues per user/network facing port and, one per traffic class.

R-51, R-55: The Access Node MUST support scheduling of user/network queues according to strict priority among at least 4 queues.

R-52, R-56: The Access Node SHOULD support scheduling of user/network queues according to their assigned priority and weight. The number of priorities MUST be at least 4, however multiple queues may be assigned to the same priority. Queues assigned to the same priority MUST be scheduled according to a weighted algorithm (like WFQ) with weights assigned through provisioning. This mechanism provides support for mapping diffserv PHBs (e.g. EF, AF, BE, LE) to the Ethernet queues.

R-57: The Access Node MUST support setting the maximum size/depth of all queues.

R-58: The Access Node MUST be able to mark or re-mark the Ethernet priority bits based on the following classification criteria:

- *User port (physical or logical)*
- *Ethertype (i.e. Ethernet Protocol ID)*
- *Received Ethernet priority bits*
- *IP protocol ID (specifically support classification of IGMP)*

R-59: For each VC belonging to a PVC bundle, the Access Node MUST support configuration of valid Ethernet priority values.

R-60: The Access Node MUST be able to distribute downstream traffic destined for a PVC bundle based on the Ethernet priority values of each frame.

R-61: The Access Node MUST be able to automatically sense the following protocol encapsulations to match the ADSL CPE modem's configuration.
1. PPPoE over ATM (RFC 2516/2684)
2. IPoE over ATM as per RFC 2684 bridge mode
3. IP over ATM as per RFC 2684 routed mode
4. PPP over ATM (RFC 2364)

R-62: The Access Node MUST be able to turn auto-sensing off on a per port basis

IP over ATM (Interworking Function)

R-63: The Access Node SHOULD support an IPoA IWF.

R-64: The IPoA IWF MUST be based on the 1:1 VLAN paradigm, using a unique <C-VID, S-VID> pair per business user; the C-VID indicates the access loop and the S-VID indicates the Access Node

R-65: For upstream packets, the IPoA IWF MUST use a MAC source address that is under the control of the Access Node (e.g. the MAC address of the Access Node uplink).

R-66: For upstream unicast packets, the IPoA IWF MUST use a MAC unicast destination address of the BNG

R-67: For upstream multicast and broadcast packets, the IPoA IWF MUST derive the MAC destination address using the standard multicast/broadcast IP address to MAC address conversion algorithm.

R-68: Upon receiving ARP requests sent by the BNG, the IPoA IWF SHOULD be able to reply with the appropriate MAC address used as the source address for upstream packets.

PPP over ATM (Interworking Function)

R-69 The Access Node MUST set-up an interworked PPPoE session as per RFC 2516 to carry PPP frames received from an ATM VC configured on the access loop.

R-70 Once this interworked PPPoE session has been established, the Access Node MUST encapsulate all PPP frames it receives on this ATM VC into this interworked PPPoE session.

R-71 The Access Node MUST check Session-IDs received from a BNG to ensure the (Session-ID, BNG MAC address, Access Node MAC address, VLAN) 4-tuple is not already in use on the Access Node, and MUST remove the old session if it exists. This requirement aims to cover the case where a session was torn down at the BNG but is still considered active at the Access Node (i.e. when a PADT was lost but the session has not yet been timed out) and the BNG tries to 're-allocate' the same session-id to a new session.

R-72 The Access Node SHOULD store the latest LCP configure request until PPPoE negotiation completes successfully, at which point the Access Node forwards the most recent LCP configure request to the BNG.

R-73: The Access Node MUST support concurrent establishment of multiple interworked PPPoE sessions.

R-74: If the Access Node initiates more than one PPPoE session using the same source MAC address and VLAN, the Access Node MUST distinguish between different users' sessions during the PPPoE discovery phase, for example by using either the Host-Uniq tag or the Relay-Session-ID tag. An Ethernet Aggregation Node MUST NOT add the Relay-Session-ID tag.

R-75: The Access Node MUST remove state for an interworked PPPoE session and send a PPPoE PADT message to the BNG upon a loss of connectivity to the customer; this can be indicated by loss of DSL synchronization on the associated customer line.

R-76: The Access Node MUST implement a mechanism to remove state when an interworked PPPoE session terminates. This mechanism MUST handle both signaled (graceful) termination and Access Node recovery following non-graceful teardown (e.g. PADT loss, BNG restart etc.).

L2 Security Considerations

R-91: The Access Node SHOULD provide a mechanism to prevent Broadband Network Gateway (BNG) MAC address spoofing

R-92: In order to prevent source MAC address flooding attacks, the Access Node MUST be able to limit the number of source MAC addresses learned from a given bridged port

R-93: This limit MUST be configurable per user facing port.

R-94: The Access Node SHOULD allow configuring the following filters and applying them to ports:
1. Source MAC address filter. This filter may be used in one of the following ways:
i. Allowing access from specific devices (i.e. MAC address).
ii. Denying access from a specific MAC address.
2. Destination MAC address filter. This filter may be used in one of the following ways:
i. Allowing access to specific destinations.
ii. Denying access to specific destinations

R-95: The Access Node SHOULD provide filtering of reserved group MAC destination addresses (in the 01:80:C2 range)

Access Loop Identification and Characterization

R-96: The Access Node MUST be able to function as a Layer 2 DHCP Relay Agent on selected untrusted user-facing ports of a given VLAN (described in Appendix B – Layer 2 DHCP Relay Agent in TR-101)

R-97: The Access Node MUST be able to disable the Layer2 DHCP Relay Agent on selected userfacing ports of a given VLAN. Note that a DHCP relay function in the RG and a Layer 2 DHCP Relay Agent in the Access Node are mutually exclusive functions.

R-98: The Access Node MUST, when performing the function of a Layer 2 DHCP Relay Agent, add option-82 with the 'circuit-id' and/or 'remote-id' sub-options to all DHCP messages sent by the client before forwarding to the Broadband Network Gateway

R-99: The Access Node MUST, when performing the function of a Layer 2 DHCP Relay Agent, remove option-82 information from all DHCP reply messages received from the Broadband Network Gateway before forwarding to the client.

R-100: A server-originated broadcast DHCP packet MUST NOT be bridged to untrusted user-facing ports by an Access Node except through the action of the Layer 2 DCHP relay agent. Through examination of option-82 and/or the chaddr field, the Layer 2 DHCP relay agent MUST transmit these packets, after removal of option-82, only to the untrusted interface for which it is intended

R-101: The Access Node MUST NOT, when performing the function of a Layer 2 DHCP relay agent, convert the DHCP request from the client from a broadcast to a unicast packet

R-102: The Access Node MUST NOT, when performing the function of a Layer 2 DHCP relay agent, set the 'giaddr' on the DHCP request from the client

R-104: The Access Node MUST, when performing the function of a Layer 2 DHCP relay agent, discard any broadcast or unicast DHCP request packet that contains option-82 and enters from an untrusted user-facing port

R-105: The Access Node MUST, when performing the function of a Layer 2 DHCP relay agent, only forward DHCP requests to the upstream designated port(s) to prevent flooding or spoofing.

R-112: The Access Node DHCP Relay Agent MUST be able to encode the access loop identification in the "Agent Circuit ID" sub-option (sub-option 1). The encoding MUST uniquely identify the Access Node and the access loop logical port on the Access Node on which the DHCP message was received. The Agent Circuit ID contains a locally administered ASCII string generated by the Access Node, representing the corresponding access loop logical port (Uinterface).(The actual syntax of the access loop identification in the Agent Circuit ID is mandated by TR-101 in section 3.9.3)

R-113: The Access Node DHCP Relay Agent MUST have the option to use the "Agent Remote ID" sub-option (sub-option 2) to further refine the access loop logical port identification. The Agent Remote ID contains an operator-configured string of 63 characters maximum that (at least) uniquely identifies the user on the associated access loop on the Access Node on which the DHCP discovery message was received.

R-114: The Access Node DHCP Relay Agent MUST support inserting vendor specific information per RFC 4243

R-115 The Access Node MUST implement a PPPoE intermediate agent as described below.
The PPPoE Intermediate Agent intercepts all upstream PPPoE discovery stage packets, i.e. the PADI, PADR and upstream PADT packets, but does not modify the source or destination MAC address of these PPPoE discovery packets. Upon reception of a PADI or PADR packet sent by the PPPoE client, the Intermediate Agent adds a PPPoE TAG to the packet to be sent upstream. The TAG contains the identification of the access loop on which the PADI or PADR packet was received in the Access Node where the Intermediate Agent resides. If a PADI or PADR packet exceeds 1500 octets after adding the TAG containing the access loop identification, the Intermediate Agent must not send the packet to the Broadband Network Gateway. In

response to the received PADI or PADR packet, the PPPoE Intermediate Agent should issue the corresponding PADO or PADS response with a Generic-Error TAG to the sender.

R-118 Both Access Node and Broadband Network Gateway MUST support the PPPoE access loop identification tag as specified above.
R-119 The Access Node MUST encode the access loop identification in the "Agent Circuit ID" suboption (sub-option 1). The encoding MUST uniquely identify the Access Node and the access loop logical port on the Access Node on which the discovery stage PPPoE packet was received. The Agent Circuit ID contains a locally administered ASCII string generated by the Access Node, representing the corresponding access loop logical port (U-interface). The actual syntax of the access loop identification in the Agent Circuit ID is mandated by this document in section 3.9.3.
R-120 The Access Node MUST have the option to encode the user identification in the "Agent Remote ID" sub-option (sub-option 2). The Agent Remote ID contains an operator-configured string of 63 characters maximum that uniquely identifies the user on the associated access loop logical port on the Access Node on which the PPPoE discovery packet was received. The actual syntax of the user identification in the Agent Remote ID is left unspecified in this document.

R-121 The Access Node MUST replace the DSLForum PPPoE vendor-specific tag with its own if the tag has also been provided by a PPPoE client.

R-122: The Agent Circuit ID field inserted by the Access Node DHCP Relay Agent and PPPoE Intermediate Agent MUST NOT exceed 63 characters

R-123: The value of the Agent Circuit ID MUST be explicitly configurable, per individual access loop and logical port. When not explicitly configured, it MUST be automatically generated using the default or flexible syntax described in following requirements

R-124: The Access Node DHCP Relay Agent and PPPoE Intermediate Agent MUST use thefollowing default syntax to automatically generate the Agent Circuit ID field, identifying access loop logical ports as follows:
"Access-Node-Identifier atm slot/port:vpi.vci" (when ATM/DSL is used)
"Access-Node-Identifier eth slot/port[:vlan-id]" (when Ethernet/DSL is used)
In this syntax, Access-Node-Identifier MUST be a unique ASCII string (not using character spaces). The Access-node-identifier, L2 type (ATM, ETH) field and the slot/port fields are separated using a single space character. The slot identifier MUST NOT exceed 6 characters in length and the port identifier MUST NOT exceed 3 characters in length using a '/' as a delimiter. The vpi, vci and vlan-id fields (when applicable) are related to a given access loop (U-interface).

R-125: The value of Access-Node-Identifier MUST be configurable per Access Node, using an element management interface. The Access-Node-Identifier MAY be derived automatically from an already defined object ID (e.g. IP address of management interface)

R-126: It MUST be possible to override the default syntax of circuit ids, and let the operators configure a more flexible syntax for the Agent Circuit ID, with flexibility in the choice of elements used in the automated generation of circuit-IDs. Such syntax is unique per Access Node. The flexible syntax MUST allow the concatenation of 2 types of elements:

- *Strings of ASCII characters configured by the network operator. This will typically include characters used as separators between variable fields (usually # . , ; / or space)*
- *Variable fields whose content is automatically generated by the Access Node. The minimum list of those variable fields is given in table 2 – circuit id syntax of TR-101 [21]. Fields should include information which doesn't vary over time for a given access loop.*

R-127: The Access Node MUST be able to insert the access loop characteristics via its PPPoE intermediate agent and/or via its layer2 DHCP Relay agent. It MUST be possible to enable/disable this function per port, depending on the type of user

R-129: In all cases (PPPoE intermediate agent, DHCP-Relay), the access loop characteristics information MUST be conveyed with a loop characteristics field structured with type-length-value sub-fields (described in Appendix C - PPPoE Vendor-Specific DSLF Tags and Appendix D - DHCP Vendor Specific Options to Support DSL Line Characteristics in TR-101). Sync data rate values MUST be encoded as 32-bit binary values, describing the rate in kbps. Interleaving delays MUST be encoded as 32-bit binary values, describing the delay in milliseconds (the complete set of sub-options is listed in table 3 – page 56 in TR-101)

R-130: In the DHCP Relay case, the access loop characteristics information MUST be conveyed by the DHCP option-82 field, with a vendor-specific sub-option, encoded according to RFC 4243, with the enterprise number being the DSL Forum enterprise code, i.e. 3561 in decimal (0x0DE9 in hexadecimal), corresponding to the IANA "ADSL Forum" entry in the Private Enterprise Numbers registry.

R-132: The PPPoE intermediate agent and DHCP relay agent on the Access Node SHOULD insert the following sub-option (in the same manner described in R-130 and R-131) to signal to the BNG the data-link protocol and the encapsulation overhead on the Access Loop.

Multicast

R-202: The Access Node MUST support the identification and processing of user-initiated IGMP messages. When this function is disabled on a port and/or VLAN, these messages are transparently forwarded.

R-203: The Access Node MUST support dropping of all IGMP messages received on a user port and/or VLAN.

R-204: The Access Node MUST support matching groups conveyed by IGMP messages to the list of groups corresponding to a multicast VLAN associated with this port. When there is no match, the IGMP message

MUST be either forwarded as regular user data or dropped. This behavior MUST be configurable. When there is a match, the IGMP message MUST be forwarded within a multicast VLAN, and enter the IGMP snooping function

R-205: Upon receipt of an IGMP v3 report carrying information on a mix of 'matching' and 'nonmatching' multicast groups, the Access Node SHOULD be able to copy the frame to the IGMP snooping function as well as forward it as user data (or drop it, as configured).

R-206: The Access Node MUST support mechanisms to stop user ports injecting multicast traffic to the aggregation network. This behavior MUST be configurable per port and/or VLAN

R-207: The Access Node MUST be able to discard IGMP queries received from user-facing ports on a multicast VLAN

R-208: The Access Node MUST be able to rate limit IGMP messages received from user-facing ports on a multicast VLAN

R-209: The Access Node MUST support an IGMP v3 (as per RFC 3376) transparent snooping function. This feature MUST be configurable on a per VLAN basis. Note: V3 includes support of earlier versions of IGMP. Specifically, this function is responsible for configuring multicast filters such that packet replication is restricted to those user ports that requested receipt

R-210: The Access Node's IGMP v3 transparent snooping function MUST support the capability to snoop the multicast source IP address and destination IP group address in IGMP packets and to set the corresponding MAC group address filters

R-211: The Access Node's IGMP v3 transparent snooping function MUST be able to dynamically create and delete MAC-level Group Filter entries, enabling in turn, selective multicast forwarding from network-facing VLANs to user-facing ports.

R-212: The Access Node MUST support IGMP immediate leave as part of the IGMP transparent snooping function.

R-214: For security purposes, the Access Node MUST drop any user-initiated IGMP Leave messages for group '0.0.0.0'

R-215: The Access Node MUST support marking, in the upstream direction, user-initiated IGMP traffic with Ethernet priority bits.

R-216: The Access Node MUST support forwarding user initiated IGMP messages to a given multicast VLAN to which that user is attached.

R-217: The Access Node SHOULD provide the following statistics.
Per VLAN, per multicast group counters:

1. Total number of currently active hosts

Per DSL port, per multicast VLAN counters:

1. Total number of successful joins

2. Total number of unsuccessful joins

3. Total number of leave messages

4. Total number of general queries sent to users

5. Total number of specific queries sent to users

6. Total number of invalid IGMP messages received

Per multicast VLAN counters:

1. Current number of active groups

2. Total number of joins sent to network

3. Total number of joins received from users (sum of items 4 and 5 below)

4. Total number of successful joins6 from users

5. Total number of unsuccessful joins from users

6. Total number of leave messages sent to network

7. Total number of leave messages received from users

8. Total number of general queries sent to users

9. Total number of general queries received from network

10. Total number of specific queries sent to users

11. Total number of specific queries received from network

12. Total number of invalid IGMP messages received

R-218: The Access Node MUST support configuring which user ports are members of a multicast VLAN.

R-219: The Access Node MUST allow the configuration of IP multicast groups or ranges of multicast groups per multicast VLAN based on:

- *Source address matching*
- *Group address matching*

R-220: The Access Node MUST be able to configure per DSL port the maximum number of simultaneous multicast groups allowed.

R-221: The Access Node MUST support enabling IGMP snooping on a per VLAN basis

R-247: The Access and Aggregation Nodes MUST support IGMP v3 snooping with proxy reporting.This feature MUST be configurable on a per VLAN basis

R-248: The Access and Aggregation Nodes MUST allow selection between transparent snooping and snooping with proxy reporting on a per-VLAN basis.

R-249: The IGMP snooping with proxy reporting function MUST support IGMP proxy query functions

References

[1] Autoridade Nacional de Comunicações (ANACOM), 2008
URL: http://www.anacom.pt

[2] Serviço de Acesso à Internet - 1º trimestre de 2008, ANACOM, 2008
URL: http://www.anacom.pt/template12.jsp?categoryId=258722#n3

[3] Digital Subscriber Line Forum, DSL Fórum, 2008
URL: http://www.dslforum.org/

[4] Sistemas de Acesso Fixo Via Rádio (FWA), ANACOM, 2008
URL: http://www.anacom.pt/template15.jsp?categoryId=155713

[5] International Telecommunication Union (ITU)
URL: http://www.itu.int/net/about/landmarks.aspx

[6] *International Telecommunication Union – Telecommunications* (ITU-T).
URL: http://www.itu.int/ITU-T/

[7] G Series Recommendations – Transmission systems and media, digital systems and networks. (ITU)
URL: http://www.itu.int/rec/T-REC-g

[8] *Internet Engineering Task Force* (IETF).
URL: http://www.ietf.org/

[9] *Institute of Electrical and Electronics Engineers* (IEEE)
URL: www.ieee.org

[10] IEEE Constitution.
URL: http://www.ieee.org/web/aboutus/whatis/Constitution/index.html

[11] IEEE Std 802, IEEE *Standards for Local and Metropolitan Area Networks*.
URL: http://ieee802.org/

[12] *Request For Comments* (IETF RFCs).
URL: http://www.ietf.org/rfc.html

[13] *Internet Grouping Multicast Protocol* version 1 – RFC 1112.
URL: http://tools.ietf.org/html/rfc1112

[14] *Internet Grouping Multicast Protocol* version 2 – RFC 2236.
URL: http://tools.ietf.org/html/rfc2236

[15] *Internet Grouping Multicast Protocol* version 3 – RFC 3376.
URL: http://tools.ietf.org/html/rfc3376

[16] Light Reading: DSL Aggregation 101.
URL: http://www.lightreading.com/document.asp?doc_id=111395&print=true

[17] Technical Report TR-025 "Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL", DSL Forum, September 1999.
URL: http://www.dslforum.org/techwork/tr/TR-025.pdf

[18] Technical Report TR-058: Multi-Service Architecture & Framework Requirements, DSL Forum, September 2003.
URL: http://www.dslforum.org/techwork/tr/TR-058.pdf

[19] Technical Report TR-059 "DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services", DSL Forum, September 2003.
URL: http://www.dslforum.org/techwork/tr/TR-059.pdf

[20] Technical Report TR-092, "Broadband Remote Access Server (BRAS) Requirements Document", DSL Forum, August 2004.
URL: http://www.dslforum.org/techwork/tr/TR-092.pdf

[21] Technical Report TR-101, "Migration to Ethernet-Based DSL Aggregation", DSL Forum, April 2006.
URL: http://www.dslforum.org/techwork/tr/TR-101.pdf

[22] IEEE 802.1ag - Connectivity Fault Management.
URL: http://ieee802.org/1/pages/802.1ag.html

[23] Y.1731 - OAM functions and mechansims for Ethernet based networks.
URL: http://www.itu.int/itudoc/itu-t/aap/sg13aap/recaap/y1731/

[24] "Provider Bridges", IEEE 802.1ad, Institute of Electrical and Electronics Engineers (IEEE), 21 Sep 2005.
URL: http://www.ieee802.org/1/pages/802.1ad.html

[25] M. Laubach, "Classical IP and ARP over ATM", RFC 2225, Internet Engineering Task Force (IETF), April 1998.
URL: http://www.faqs.org/rfcs/rfc2225.html

[26] C. Rigney, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, Internet Engineering Task Force (IETF), June 2000.

URL: http://tools.ietf.org/html/rfc2865

[27] S. Bhattacharyya, "An Overview of Source-Specific Multicast (SSM)", RFC 3569, Internet Engineering Task Force (IETF), July 2003.
URL: http://www.ietf.org/rfc/rfc3569.txt

[28] *"Protocol Independent Multicast (PIM)",* Internet Engineering Task Force (IETF), April 2008.
URL: http://www.ietf.org/html.charters/pim-charter.html

[29] PT Inovação, S.A.
URL: http://www.ptinovacao.pt

[30] mDSLAM®, NETBAND, PT Inovação, May 2008.
URL: http://www.ptinovacao.pt/produtos/P&S_PTIN.html

[31] Media DSLAM 48 BOX Application Notes, PT Inovação, Novembro 2007.

[32] Media DSLAM CLI Reference Manual, PT Inovação, Outubro 2006.

[33] Media DSLAM / MSAN – Manual de Utilização, Versão 1.0, PT Inovação, Janeiro 2007.

[34] AGORA-NG®, NETBAND, PT Inovação, May 2008.
URL: http://www.ptinovacao.pt/produtos/P&S_PTIN.html

[35] Serviços de Formação, PT Inovação, May 2008.
URL: http://www.ptinovacao.pt/formacao

[36] Conexant Systems, Inc, 2008.
URL: http://www.conexant.com/

[37] Conexant Systems, Inc, Licensee Server, 2008.
URL: https://ls.conexant.com/ls2/

[38] Multiprotocol Encapsulation over ATM Adaptation Layer 5, Internet Engineering Task Force (IETF), September 1999.
URL: http://www.ietf.org/rfc/rfc2684.txt

[39] IEEE 802.1D – "Media Access Control (MAC) bridges", Institute of Electrical and Electronics Engineers (IEEE), June 1994.
URL: http://www.ieee802.org/1/pages/802.1D.html

[40] IEEE 802.3ad Link Aggregation, (IEEE 802.3 Ethernet based LANs), Institute of Electrical and Electronics Engineers (IEEE), March 2000.
URL: http://www.ieee802.org/3/ad/

[41] IEEE 802.1Q - Virtual Bridged Local Area Networks, Institute of Electrical and Electronics Engineers (IEEE), November 2006.
URL: http://www.ieee802.org/1/pages/802.1Q.html

[42] Definitions of Managed Objects for the ADSL Lines, RFC 2662, Internet Engineering Task Force (IETF), G. Bathrick, August 1999.
URL: http://www.ietf.org/rfc/rfc2662.txt

[43] ADSL Forum Technical Report TR-024 "DMT Line Code Specific MIB", DSL Forum, June 1999.
URL: http://www.dslforum.org/techwork/tr/TR-024.pdf

[44] Random Early Detection, Wikipedia, March 2008.
URL: http://en.wikipedia.org/wiki/Random_early_detection

[45] Spirent Communications.
URL: http://www.spirent.com/

[46] Agilent Technologies.
URL: http://www.home.agilent.com

[47] PT Comunicações, S.A.
URL: http://www.ptcom.pt/

[48] 2Wire, Inc.
URL: http://www.2wire.com/

[49] Thomson DSL Modems & Gateways.
URL: http://www.thomson.net/GlobalEnglish/Products/dsl-modems-gateways/Pages/default.aspx

[50] Billion Electric Co. Ltd.
URL: http://www.billion.com/

[51] Juniper Networks, Inc.
URL: http://www.juniper.net/

[52] DHCP Relay Agent Information Option, RFC 3046, IETF, January 2001.
URL: http://www.ietf.org/rfc/rfc3046.txt

[53] VideoLAN - VLC media player.
URL: http://www.videolan.org/

[54] SNTP: D. Mills, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, RFC 2030, IETF, October 1996.
URL: http://www.faqs.org/rfcs/rfc2030.html

[55] Microsoft MediaRoom®.
URL: http://www.microsoftmediaroom.com/

[56] Meo.
URL: www.meo.pt

[57] IPTV Architecture Overview, Sven Ooghe, April 2006 (DSL Forum)
URL: http://www.dslforum.org/mktwork/download/sooghe0406_iptvgeneva.pdf

[58] DHCP, HP documentation
URL: http://docs.hp.com/en/B2355-90685/ch06s02.html

[59] PPPoE Discovery and Session Stage
URL: http://www.cnii.com.cn/20070108/ca408270.htm