Universidade de Aveiro
Ano 2010

Departamento de Electrónica,
Telecomunicações e Informática

Diogo Nuno Pereira Gomes

Optimização de recursos para difusão em Redes de Próxima Geração

Universidade de Aveiro
Ano 2010

Departamento de Electrónica, Telecomunicações e Informática

Diogo Nuno Pereira Gomes

Optimização de recursos para difusão em Redes de Próxima Geração

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Electrotecnia, realizada sob a orientação científica do Prof. Doutor Rui L. Aguiar, Professor Associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

Apoio financeiro da FCT e do FSE no âmbito do III Quadro Comunitário de Apoio.

o júri

presidente

Doutor Carlos de Pascoal Neto
Professor Catedrático da Universidade de Aveiro

Doutor Aníbal Manuel de Oliveira Duarte
Professor Catedrático da Universidade de Aveiro

Doutor Paulo da Costa Luís da Fonseca Pinto
Professor Associado com Agregação da Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa

Doutor Rui Manuel Rodrigues Rocha
Professor Associado do Instituto Superior Técnico da Universidade Técnica de Lisboa

Doutor Rui Luís Andrade Aguiar
Professor Associado da Universidade de Aveiro

agradecimentos

Este trabalho só foi possível ser realizado graças ao grupo de investigação sobre Redes Heterogéneas (HNG) onde me inseri no Instituto de Telecomunicações – Pólo de Aveiro. Neste grupo encontrei as oportunidades certas para colaborar com grupos de investigação internacionais com os quais pude debater as minhas ideias e aprender mais sobre tecnologias e conceitos avançados de telecomunicações.

Agradeço de forma especial ao meu orientador o Prof. Rui L. Aguiar, sem o qual este trabalho jamais se teria realizado. Pelas conversas que tivemos, nas quais debatemos vigorosamente a tese aqui apresentada, e pelas oportunidades que me criou para o desenvolvimento da minha carreira cientifica e académica.

Agradeço à Fundação para a Ciência e Tecnologia pela bolsa de doutoramento que me foi atribuída.

Agradeço aos meus colegas do HNG pela infindáveis discussões cientificas e sugestões ao meu trabalho que me ajudaram a aprofundar e a melhorar o mesmo.

Agradeço a todos aqueles que trabalharam comigo nos projectos nos quais participei, pois sem eles o meu trabalho perderia todo o seu contexto e relevância.

Agradeço também à Cathy Joaquim pela revisão que fez ao texto desta tese.

Agradeço por fim à minha família que incondicionalmente me apoiou e incentivou para a realização deste trabalho.

palavras-chave

Comunicação em Grupo, Redes de Próxima Geração, Redes 3G, MBMS, IP Multicast, Qualidade de Serviço, Gestão de Recursos

resumo

Esta tese aborda o problema de optimização de recursos de rede, na entrega de Serviços de Comunicação em Grupo, em Redes de Próxima Geração que suportem tecnologias de difusão. De acordo com esta problemática, são feitas propostas que levam em atenção a evolução espectável das redes 3G em Redes Heterogéneas de Próxima Geração que incluam tecnologias de difusão tais como o DVB. A optimização de recursos em Comunicações em Grupo é apresentada como um desafio vertical que deve cruzar diversas camadas. As optimizações aqui propostas cobrem tanto a interface entre Aplicação e a Plataforma de Serviços para a disponibilização de serviços de comunicação em grupo, como as abstracções e mapeamentos feitos na interface entre a Rede Central e a Rede de Acesso Rádio.

As optimizações propostas nesta tese, assumem que o caminho evolutivo na direcção de uma Rede de Próxima Geração é feito através do IP. Em primeiro lugar são endereçadas as optimizações entre a Aplicação e a Plataforma de Serviços que já podem ser integradas nas redes 3G existentes. Estas optimizações podem potenciar o desenvolvimento de novas e inovadoras aplicações, que através do uso de mecanismos de distribuição em difusão podem fazer um uso mais eficiente dos recursos de rede. De seguida são apresentadas optimizações ao nível da interface entre a Rede Central e a Rede de Acesso Rádio que abordam a heterogeneidade das redes futuras assim como a necessidade de suportar tecnologias de difusão. É ainda considerada a possibilidade de aumentar a qualidade de serviço de serviços de difusão através do mapeamento do IP *multicast* em portadoras unidireccionais. Por forma a validar todas estas optimizações, vários protótipos foram desenvolvidos com base num *router* avançado para redes de acesso de próxima geração. As funcionalidades e arquitectura de *software* desse *router* são também aqui apresentadas.

keywords

Group Communication, Next Generation Networks, 3G Networks, MBMS, IP Multicast, Quality of Service, Resource Management

abstract

This thesis addresses the problem of optimizing network resource usage, for the delivery of Group Services, in Next Generation Networks featuring broadcast technologies. In this scope, proposals are made according to the expected evolution of 3G networks into Next Generation Heterogeneous Networks that include broadcast technologies such as DVB. Group Communication resource optimization is considered a vertical challenge that must cross several layers. The optimizations here proposed cover both Application to Service Platform interfaces for group communication services, and Core Network to Radio Access Network interface abstractions and mappings.

The proposed optimizations are also presented taking into consideration network evolution path towards an All-IP based Next Generation Network. First it is addressed the Application to Service Platform optimization, which can already be deployed over 3G networks. This optimization could potentiate the development of new and innovative applications that through the use of broadcast/multicast service delivery mechanisms could be more efficient network wise. Next proposals are made on the Core Network to Radio Access Network interfaces that address the heterogeneity of future networks and consider the need to support broadcast networks. It is also considered the possibility to increase the Quality of Service of broadcast/multicast services based on the dynamic mapping of IP multicast into unicast radio bearers. In order to validate these optimizations, several prototypes were built based on an advanced access router for next generation networks. Such access router functionalities and software architecture are also presented here.

Table of Contents

1. Introduction 1
   1.1 Motivation 1
   1.2 Contribution 2
   1.3 Thesis Structure 3
   1.4 Computational Tools and infrastructure 4
2. The path to converged networks 7
   2.1 Toward next Generation Networks 7
      2.1.1 IP Based Networks 7
      2.1.2 3G Networks 10
      2.1.3 TISPAN 19
      2.1.4 4G Networks 20
   2.2 Group Communication 22
   2.3 The Problem 26
3. Concepts and Abstractions 27
   3.1 Quality of Service in IP based Networks 27
   3.2 Network Level and Application Level QoS Signaling 29
   3.3 Provisioning Mechanisms 33
      3.3.1 IntServ 33
      3.3.2 DiffServ 34
   3.4 Network Technologies role in the Network QoS 36
      3.4.1 Wired Networks 37
      3.4.2 Wireless Networks 40
      3.4.3 Broadcast Networks 43
   3.5 Group Based Communication 45
      3.5.1 IP Multicast 45
      3.5.2 QoS Enabled Multicast 49
      3.5.3 3GPP MBMS 50
4. Optimization of Group Communication through Service and Network Optimizations 55
   4.1 Introduction 55
   4.2 Optimizing Group Communication Services 57
      4.2.1 Limitations and Restrictions 58
      4.2.2 Leveraging the BM-SC towards IMS 60
      4.2.3 Service Enablers for IP-based Content Distribution 64
      4.2.4 Service Oriented Network Management and Control 68
   4.3 Optimizing Group Communications through Service and Network Optimizations 70
      4.3.1 Coping with heterogeneous networks in group communication 71
      4.3.2 IP based Group communication over Heterogeneous networks 73
5. Multicast to Unicast Switching 87
   5.1 IP Unicast/Multicast to L2 mapping 87
      5.1.1 Technological Considerations 87

5.1.2 Dynamic mapping proposal ... 89
5.2 Analysis of the impact of a dynamic L3/L2 Switching Control Mechanism in Mobile TV services ... 96
5.2.1 Service Usage Simulator ... 97
5.2.2 The Scenarios ... 99
5.2.3 Analysis of the Results ... 102
5.2.4 Conclusion ... 108
6. Network Middleware – the Access Router ... 111
6.1 Introduction ... 111
6.2 Advanced Router Mechanism ... 112
6.2.1 The Access Router in Next Generation Networks ... 112
6.2.2 Conceptual Requirements ... 114
6.2.3 Functional Requirements ... 116
6.3 Software Architectures ... 118
6.4 ARM Software Architecture ... 120
6.4.1 The Control Plane ... 122
6.4.2 Information Flow ... 128
6.4.3 Software Framework ... 131
7. Conclusion ... 137
7.1 Review and Discussion of Achievements ... 137
7.2 Future Work ... 139
7.3 Final Remarks ... 140
8. References ... 143
Annex A. Protocols ... 161
A.1 Common Open Policy Service (COPS) ... 161
A.2 Resource Reservation Protocol (RSVP) ... 165
A.3 Next Steps In Signaling Framework (NSIS) ... 169

Table of Tables

Table 1 - UMTS QoS classes (in 3GPP TS 23.107) 12
Table 2 - SWOT analysis of Network and Application layer signaling 31
Table 3 - Delay, Jitter and Loss for IP flows running over a DVB link 84
Table 4 - Simulator Variables 98
Table 5 - Scenario characterization matrix 100

Table of Figures

Figure 1 – The OSI Model and TCP/IP Model respectively 8
Figure 2 – UMTS Logical Architecture 11
Figure 3 - 3GPP - Release 5 - End-to-End QoS Architecture 14
Figure 4 - UMTS Network Architecture (relevant QoS Entities) 15
Figure 5 - Release 8 LTE Overall Architecture (according to 3GPP TS 36.300, TS 36.401) 18
Figure 6 – SAE - Evolved Packet System Architecture 18
Figure 7 - ETSI - TISPAN basic architecture 19
Figure 8 - All-IP 4G Network Architecture (relevant QoS elements) 21
Figure 9 – QoS Procedures enforced by Routers 30
Figure 10 - DiffServ Router Model 34
Figure 11 - DOCSIS Cable Modem protocol stack 39
Figure 12 - MBMS Architecture 50
Figure 13 - MBMS Service Setup Phases 52
Figure 14 – Layered approach to Group Communication Optimization 56
Figure 15 - Network Entity Design 61
Figure 16 - OMA Enabler Interface Categories 65
Figure 17 - Reference Architecture 68
Figure 18 – 3G MBMS vs. 4G Network Multicast/Broadcast QoS Architecture 74
Figure 19 - Heterogeneous Return Channel 77
Figure 20 - 4G Network Multicast/Broadcast Service Setup Message Sequence Chart 79
Figure 21 - 4G Network Multicast/Broadcast Service Mobility 81
Figure 22 - Daidalos Broadcast Technologies Support 82
Figure 23 – Dynamic mapping concept. 89
Figure 24 - Proposed MLDv2 QoS Extension 91
Figure 25 – Prototype evaluation test bed. 92
Figure 26 - Packet Loss for a multicast stream over a WiFi unicast channel and multicast channel (A) and over two unicast links (B) 93
Figure 27 – Packet Rate of a multicast stream over a WiFi unicast channel and multicast channel (A) and over two unicast links (B) 94

Figure 28 – Packet Inter arrival of a multicast stream over a WiFi unicast channel and multicast channel (A) and two unicast channels (B) 95
Figure 29 - Simulator Workflow 99
Figure 30 - Service Distribution amongst Subscribers 100
Figure 31 - Example distribution of 300 terminals 101
Figure 32 - Number of Services available per cell 102
Figure 33 - Number of cells with a given amount of terminals associated depending on the global population of terminals. 103
Figure 34 - Number of switching opportunities in the 3G Scenarios 104
Figure 35 - Number of unicast subscribers per Service in the 3G Scenario 105
Figure 36 - Number of Services per cell 106
Figure 37 - Number of cells given an amount of terminals associated 106
Figure 38 - Number of switching opportunities in the WiFi Scenarios 107
Figure 39 - Number of unicast subscribers per Service in the 3G scenarios 107
Figure 40 – Distribution of terminals amongst services 108
Figure 41 - Switching Opportunities per Cell Density 109
Figure 42 - Positioning of the Next Generation Access Router 113
Figure 43 - Basic Router Architecture 118
Figure 44 - ARM Router Architecture 121
Figure 45 - Functional view of the Control and Management Planes of ARM 122
Figure 46 – Advanced Router Mechanism (ARM) – a next generation router prototype as instantiated in project IST-Daidalos 127
Figure 47 - ARM Boot-Up Sequence 128
Figure 48 - ARM - Flow description classes 129
Figure 49 - ARM - Session Setup 130
Figure 50 – Main Interfaces between ARM and the Linux Kernel 131
Figure 51 - ARM – Framework classes 132
Figure 52 - ARM - module class 133
Figure 53 - COPS Common Header 162
Figure 54 - COPS Object Template 162
Figure 55 - RSVP in a router 165
Figure 56 - RSVP Session Message Sequence Chart 167
Figure 57 - Next Steps In Signaling Framework 169
Figure 58 - NSIS signalling decoupling 170
Figure 59 - GIST usage example 172
Figure 60 - QoS NSLP interfaces in a router 173
Figure 61 - Reservation scenarios using QoS NSLP 174

Acronyms

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ABC	Always Best Connected
ABR	Available bit rate
AF	Assured Forwarding
AN	Access Network
AP	Access Point
API	Application Programming Interface
AR	Access Router
ASM	Any Source Multicast
ATM	Asynchronous Transfer Mode
BE	Best Effort
BGP	Border Gateway Protocol
BM-SC	Broadcast Multicast Service Center
CBR	Constant bit rate
CDMA	Code Division Multiple Access
CDMA/CD	Code Division Multiple Access / Collision Detection
CL	Controlled Load
CN	Core Network
COPS	Common Open Policy Service
CoS	Class of Service
CPU	Central Processing Unit
CS	Circuit Switch

CSCF	Call Session Control Functions
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DCF	Distributed Coordination Function
DCH	Dedicated Channel
DM	Dense Mode
DSCP	DiffServ Code Point
DVB-C	Digital Video Broadcast - Cable
DVB-H	Digital Video Broadcast - Handheld
DVB-S	Digital Video Broadcast - Satellite
DVB-T	Digital Video Broadcast – Terrestrial
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data for GSM Evolution
EF	Expedited Forwarding
ETSI	European Telecommunications Standards Institute
FACH	Forward Access Channel
FLUTE	File Delivery over Unidirectional Transport
FMIP	Fast Mobile IP
FTP	File Transfer Protocol
FTP	File Transfer Protocol
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GS	Guaranteed Service
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transport Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol

IMS	IP Multimedia Subsystem
IP	Internet Protocol
ITU	International Telecommunication Union
JCP	Java Community Process
JSR	Java Specification Requests
LAN	Local Area Network
LoS	Line of Sight
MAC	Medium Access Control
MBMS	Multimedia Broadcast/Multicast Service
MDFP	Media Delivery Function Processors
MGW	Media Gateway
MIP	Mobile IP
MLD	Multicast Listener Discovery
MMS	Multimedia Messaging Service
MMServer	Multimedia Server
MMSP	Multimedia Service Proxy
MPE	Multi-Protocol Encapsulation
MSC	Mobile services Switching Center
MSS	MSC Server
MT	Mobile Terminal
MVNO	Mobile Virtual Network Operator
NGN	Next Generation Network
NSIS	Next Steps In Signaling
OMA	Open Mobile Alliance
OSE	OMA Service Environment
OSPF	Open Shortest Path First
P2P	Peer to Peer
PBNMS	Policy Based Network Management System
PC	Personal Computer

PCF	Point Coordination Function
PCR	Peak Cell Rate
PDA	Personal Digital Assistant
PDB	Per Domain Behavior
PDP	Policy Decision Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PHB	Per Hop Behavior
PHY	Physical
PIM	Protocol Independent Multicast
PIM	Protocol Independent Multicast
PMIP	Proxy Mobile IP
PS	Packet Switch
PSTN	Public Switched Telephone Network
PTM	Point to Multipoint
PTP	Point to Point
QoS	Quality of Service
RFC	Request for Comments
RNC	Radio Network Controller
RP	Rendezvous Point
RPT	Rendezvous Point Trees
RSPEC	Requested Specification
RSVP	ReSerVation Protocol
RTP	Real Time Transport Protocol
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SM	Sparse Mode
SPD	Service Provider Domain

SPP	Service Provisioning Platform
SPT	Shortest Patch Trees
SSM	Source Specific Multicast
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TE	Terminal Equipment
TCO	Total Cost of Ownership
TD	Terminal Domain
ToS	Type of Service
TSPEC	Traffic Specification
UAM	Universal access method
UBR	Unspecified bit rate
UE	User Equipment
UGC	User Generated Content
UMTS	Universal Mobile Telecommunication System
UTRAN	UMTS Terrestrial Radio Access Network
VBR	Variable bit rate
VC	Virtual Channel
VLR	Visitor Location Register
VP	Virtual Path
WAN	Wide Area Network
WWW	World Wide Web
XML	Extensible Markup Language

1. Introduction

1.1 Motivation

Communication is the cornerstone of the information society upon which we live today. In the last century this mostly meant analog telephony, radio and TV. Such media reached our father's homes both through circuit switch and broadcast networks. Reliable propagation of information was ensured through tight control of the circuit switch environment and tight control of the radio spectrum.

Nonetheless in the early 70's the introduction of packet switch networks led to important developments in how communication is performed in the 21st century. Packet switching allows a better usage of resources as more than two communication parties can efficiently use the same communication lines, leading to multiplexing gains. Furthermore, the increased network intelligence and added functionalities enables optimized routing of communication, with inherent self-healing of network paths that might suffer any damage. With the advent of a global packet switched network based on the Internet Protocol (IP), a migration process started in the last two decades towards a global packet switched network, to whom we call the Internet, able to deploy any service, anywhere. Increased added features, such as error detection and correction, fault diagnosis, verification of message delivery, reverse billing/charging and many others, contributed to the growing dominance of packet switched networks over legacy circuit switched networks.

Unfortunately, there are also disadvantages in this migration process. Most packet switch networks do not provide any strict guarantee on the transport pattern packets belonging to a specific communication will be subjected to. In circuit switch networks, a given communication was bound to a reserved circuit with well-defined characteristics, which in turn displayed a coherent pattern for the duration of a communication (referred to as a session). Most packet switch networks do not natively provide mechanisms that ensure a consistent pattern for a communication session, and must rely in added mechanisms and protocols to overcome such limitations.

In the early days of packet switch networks, such concerns where not of much importance due to the nature of the data services used then. But today's networks deploy multimedia services such as VoIP and Video Streaming, which require from the network not only accurate delivery of packets but also the fulfillment of time constrains such as delay and jitter. According to ITU-T [ITU E.800], Quality of Service is defined as "*the collective effect of service performances, which determine the degree of satisfaction of a user of the service*". In this definition *service* refers to support, operability, serviceability and security. Another definition in the field of packet-switched networks and computer networking defines Quality of Service in traffic engineering as "*the probability of the telecommunication network meeting a given traffic contract*" [Oodan 1997]. The concept of Quality of Service is unfortunately commonly misused to refer to enhanced and tight traffic patterns. This is incorrect since the QoS concept also addresses the uncontrolled traffic pattern that characterizes most of the packet switched networks called «Best Effort».

As packet switching networks continue to grow they are further encompassing different types of services, such as Television and Radio. These services are quite different from the services traditionally deployed by telecommunication operators (e.g. Voice). These services can be referred to as Group Based or Group Oriented Communications, since they are targeted at delivery of information not to a single user but to large groups of users. Historically this meant that the networks used to deploy such services were developed with very different requirements. Today the convergence of networks means that any service should be able to be deployed over any technology. As such, group services should be able to be deployed over packet switched telecommunication networks. As a counterpart to this concept, also broadcast networks should be used to deploy other services besides the traditional Television and Radio Service.

It is therefore important to study the means through which Group Services can be deployed in Next Generation Networks and how to most efficiently make use of the underlying technologies when deploying such services supporting the expected level of Quality of Service.

1.2 Contribution

This thesis addresses the challenge of deploying Group Services over Next Generation Networks (NGN) with an efficient use of network resources. Proposals are made on how telecommunication networks can evolve towards NGN from the point of view of services and network support. This thesis includes innovative approaches on how group communication can be improved through optimizations in various points of telecommunications network, as well as through a better use of Network Resources. It also details how the availability of high-level group mechanisms can improve overall user experience and potentiate the creation of new services. Much of this work was integrated by the author into various European projects (IST-DAIDALOS and IST-C-Mobile). The involvement of the author in such projects enabled him to extend this work with complementary aspects such as Mobility [Miloucheva 2006] and Security [Gomes 2006] that enabled a broader view of the problem, beyond the strict QoS [Gomes 2004][Prior 2005][Sargento 2005] and group communication aspects [Gomes 2005a][Gomes 2005b]. These projects further provided for the creation and development of prototypes that enabled the validation of the concepts described in this thesis. Some of such prototypes and developed code were released to the general public under Open Source License for public scrutiny and usage.

Original contributions of this work that are further explored in the scope of this thesis include: the use of a pure IP mechanism for the integration of broadcast technologies in a Next Generation Network environment, which was published in [Gomes 2008a]. The proposal of an IP-based content delivery platform based in the OMA concept of services enablers for a next generation network, published in [Gomes 2008b] and [Santos 2008]. The dynamic mapping of IP multicast into lower layers, published in [Gomes 2007].

1.3 Thesis Structure

In Chapter 2, the reader is introduced to convergence path towards Next Generation Networks (NGN) and to the importance of group communication in these future networks. The reader is presented to the scientific domain covered in this work through an historical review of the basic concepts behind IP based networks, of the evolutions made by 3G Networks from their initial release (Release 99) to the most recent (3GPP LTE), and of what is expected 4G networks to become. The author intends to guide the reader through a personal review of the most relevant evolutionary aspects with impact on the QoS, group communication and resource optimization. A section on the role of QoS summarizes the challenges that need to be tackled in NGN. And a section on group communication presents the opportunities and challenges that need to be overcome for the complete and successful integration of Broadcast Technologies in the provisioning of group services both at the IP Multicast level and at service application level.

In Chapter 3 the basic concepts that support this work are described, such as QoS in IP based networks and the differences between network level and application level QoS signaling. The most important QoS provisioning mechanisms are described and an analysis is made on the impact of several technologies and their broadcast capabilities on the QoS of group communications. Last, the concepts of IP Multicast and 3GPP MBMS are described as representative of the state of the art in deploying group communication services.

In Chapter 4 several proposals are made towards optimizing group communication services in NGN. It starts by an analysis of the limitations and restrictions of existing solutions (such as the 3GPP solution for group communication based on the MBMS), and a proposal is made on an evolutionary path towards a fully distributed and IP based solution drawn around the creation of Service Enablers and their interactions with the network through an IMS interface. It is followed by a section where it is addressed the trend towards a fully IP based heterogeneous network, where the heterogeneity of the technologies involved might constitute a new challenge to group communication services. The co-existence of next generation services and legacy services deployed over multiple technologies with some of them being unidirectional is also considered. A proposal is made under this scope that addresses the integration of such technologies as well as the opportunities that might arise from this heterogeneity. A flexible and dynamic mapping between broadcast/multicast and unicast is here identified as a requirement for this environment.

In Chapter 5 the author details the change of the static mapping between IP Multicast and L2 Broadcast mechanism, substantiating its claim through a prototype and simulation results.

Chapter 6 describes the Middleware and Computational Support developed by the author in order to demonstrate the claims made in the previous chapters. It describes, from a Software Engineering point of view, a possible model for a next generation router operating in the edge of the network, which is able to address the functionalities previously identified as requirements for next generation access routers.

Finally Chapter 7 presents some conclusions on the overall work done with some future work directions.

In the Annex, a short description of the COPS, RSVP and NSIS protocols is included, as support to the work done in Chapter 6, were these protocols were extensively used.

1.4 Computational Tools and infrastructure

Much of the work done in the scope of this thesis was accomplished through the use of several computational tools that assisted in the development of prototypes and their respective validation. Additionally the prototypes were integrated into a network infrastructure that far surpassed the scope of the prototypes, but provided the mean to understand the broader impact of the concepts instantiated by the prototype.

In order to validate the optimizations proposed several prototypes were developed in the C/C++ and Java (J2EE) languages. Prototypes addressing Service Layer optimizations were developed in J2EE and deployed in SUN Microsystems application server Glassfish [Glassfish], making a broad use of the Sailfin project [Sailfin] that implements [JSR 289]. Validation of such prototypes was done in the scope of project IST-C-Mobile based infrastructure. The testbed and components used are described in [CMOBILE D6.2].

Core Network/Radio Access Network optimizations required the development of lower levels prototypes in C/C++ for the Linux Environment which provided the most fertile environment to perform low level modifications such as the one proposed in chapter 5, and the router architecture proposed in chapter 6.

Validation of the optimizations proposed for the Core Network/Radio Access Network was achieved in the scope of project IST-Daidalos, which consisted of an almost full-fledged next generation heterogeneous operator infrastructure. Integrating prototypes in the scope of a larger integration effort is a very challenging task. A description of such infrastructure and the difficulties associated to this integration process is available in [Gomes 2009].

A software quality concern, led to the modeling of the prototypes using the UML language using tools such as Telelogic TAU (Now IBM Rational TAU) [TAU] and boUML [BOUML].

2. The path to converged networks

Today's Network Operators main concern is to deliver innovative multimedia services to its customers regardless of where they are, or of which technologies they have access to. Voice as a service has been gradually losing its importance with data and TV services those with largest forecasted growth [OECD 2007].

The evolution witnessed in telecommunication networks has enabled a paradigm shift from monolithic technologies and services into a heterogeneous environment of technologies, services and providers in highly competitive markets. In such an environment it is important to understand the technologies and services involved in order to better take advantage of possible synergies that ultimately will lead to new services and increased revenues for Network Operators.

2.1 Toward next Generation Networks

2.1.1 IP Based Networks

In the turn of the century we have witnessed the consolidation of IP based networks as the standard model for telecommunications, be it data, voice or video. Packet Switching mechanisms and Network Services have enabled IP based networks to overcome the limitations of underlying technologies, such as lack of QoS mechanisms, security, authentication, authorization, accounting, etc. Public Switched Telephone Networks, that once only provided subscribers with one voice channel, can today provide a myriad of services including digital voice, data and digital TV, thanks to the deployment of an IP layer on top of access technologies such as xDSL.

In an abstract description, an IP based network is a graph composed of nodes and links. Nodes are devices with a defined degree of intelligence that can either be a producer/consumer of information or a router. A router is no more than a node in the path, which forwards the information between the producer and the consumer. Links connect nodes together, often by cables or radio connections, but can also be virtual in the sense that they are purely logic connections between at least two nodes.

The main difference between IP Based Networks and previous network technologies lies in the way that information is exchanged between nodes through the links. In most circuit switched networks the links are strictly reserved by the nodes, regardless if there is any information to be exchanged or not. In Packet Switching networks, of which IP is the foremost technology, information is divided into small amounts of information (packets) that can be serialized and transmitted over shared links, thus improving the overall efficiency of the network through multiplexing gains. Packetization of information is only possible through the digitalization of all information into a set of bits (ones and zeros) and the use of a specific protocol by both endpoints. On the other hand, circuit switched networks are mostly associated with the representation of information in the form of continuous variable waves. These can't be broken down and reassembled according to the links used. Instead Circuit Switching relies on the establishment of a continuous end-to-end channel from the producer to the consumer of information.

Packet switching not only improves network efficiency, but also increases its resilience. In a circuit switched network, if a link faces a malfunction, the end-to-end communication is interrupted. Packet switching networks do not face this problem, as routers can effectively re-route packets (that would otherwise be transmitted through a malfunctioning link) through alternative links. This is possible since all packets independently contain, in addition to the information being transported, routing information such as source and destination of the packet, thus enabling the network to re-route the packets as necessary.

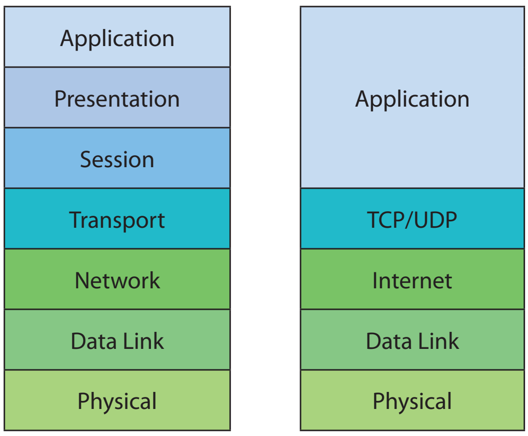


Figure 1 – The OSI Model and TCP/IP Model respectively

A deeper analysis of IP based networks will enable a better understanding on the benefits of Packet Switched technologies.

What are commonly referred to as IP based networks are in fact more than just packet switching networks. When we refer to IP based networks we are not referring to a single technology but to a communication stack made of several layers, each of them made of several technologies some of which can even be circuit switched based. This stack model can be loosely compared to the standard OSI model (Figure 1). The figure shows that the IP protocol plays just a part in the overall stack model and corresponds to the Network Layer of OSI. IP is nonetheless exclusively connectionless, while OSI Network provides both connectionless and connection-oriented services. In addition OSI clearly distinguishes 3 extra layers (Application, Presentation and Session) plus the Transport layer, while TCP/IP mixes some of the functionalities of the Session layer into the Transport Layer (TCP) [ISO 7498] [RFC 1122]. The underlying Link layer and Physical layer can be mapped directly between the two models.

In this layered approach the lowest layer is concerned purely with sending and receiving data utilizing the physical media. At the top, there are protocols designed for specific tasks, such as sending and receiving video, sound and control information (e.g. QoS, Security, A4C). The protocols in between handle functions such as splitting the message data into packets and forwarding them reliably between nodes.

The Internet Protocol [RFC 791] suite provides an excellent cornerstone in the creation of an architecture for converged networks. At the heart of the Internet Protocol suite is the Internet Protocol, which represents the building block that uniformly connects different physical networks with a variety of applications.

The Internet Protocol is the most popular network protocol in the world. IP enables data to be transmitted across and between local area networks, hence the name: Inter-net Protocol. Data travels over an IP-based network in the form of IP packets. Each IP packet includes both a header and the message data itself. The header specifies the source, the destination, and other information about the data, such as size of the packet and upper layer protocols.

IP is a connectionless protocol where each packet is treated as a separate entity, like a postal service. Mechanisms for ensuring that the data sent arrives in a correct and un-tempered manner are provided by higher-layer protocols in the stack.

Each network device has at least one IP address, which uniquely identifies it from all other devices on the network. In this manner, intermediate nodes can correctly guide packets from sources to destinations. Above the connectionless IP protocol, lays another important protocol in this stack: the Transport Control Protocol (TCP) [RFC 793]. TCP provides connection logic and reliability to the IP based network. Therefore, such networks are often referred to as TCP/IP networks. Other transport protocols can be used, such as User Datagram Protocol (UDP) [RFC

768] or the Stream Control Transmission Protocol (SCTP) [RFC 2960].

The layered approach enables IP based networks to build upon existing and novel transport technologies in much the same way as OSI. This is undoubtedly one of the main advantages of IP based networks. An IP based network can interconnect several networks. Each network may be deployed using a different link layer technology, and IP will be providing common services to all networks, all unaware of the underlying link layer networks. The Internet is the best example of such an IP based network. Spreading through almost any existing technology, it provides a never ending number of services to subscribers all around the world, through the most diverse number of technologies, from existing phone land lines to satellite communications.

IP therefore allows for the convergence of multiple link layer and physical technologies. From a situation where a network infrastructure accommodated only one type of link layer technology and service, we now have several link layers technologies and services placed beneath and on top of an IP based network. An IP based network can be connected to other legacy networks, providing almost global availability of all the previously existing services.

There are thus three major factors that create the conditions for network convergence around the IP protocol: packetized transport; support for IP over most link layer technologies; and standardization of communication protocols [Ojanperä 2006]. Digital technology enabled the packetization of information and the dominance of packet switched networks. Physical technologies evolved to a degree where digital information can efficiently and reliably flow between nodes. Standardized communications protocols, built on top of such technologies, provided the abstraction needed for services to be built once and be deployed everywhere.

Through this layered approach, services can become unaware of the network and therefore be deployed anywhere. This property has extensively been explored by Internet Applications. Internet Applications are able to provide their services through any network that is IP enabled. Unfortunately the ability to provide the service is not always matched by the ability to provide it with adequate quality. Many applications (especially multimedia applications) are not capable to provide adequate service over wireless technologies due (for instance) to bandwidth limitations.

2.1.2 3G Networks

After the great success of Mobile Telecommunications in the late 20th century through digital technologies such as GSM [GSMA] and cdmaOne (IS-95) [Karn 1993] which are referred to as the 2nd Generation (2G) of mobile communications, a new standard had to be developed in order to bring new services to 21st century subscribers. This standard was developed in the scope of the 3rd Generation Partnership Project (3GPP) [3GPP], a collaboration between several parties ranging from national standardization bodies ("Organizational Partners") to manufacturers, vendors and mobile operators ("Market Representation Partners"). Work done in 3GPP was put under the scope of ITU-T's IMT-2000 project [IMT-2000] and was initially based on legacy GSM network standards. 3GPP has defined several standards on radio aspects, core network and service architecture. The most important outcome of 3GPP was the definition of the UMTS architecture [3GPP 23.002]. The UMTS architecture was designed to provide support for multimedia communication services and higher data rates while maintaining compatibility with legacy technologies, such as GPRS (General Packet Radio Service) [ETSI GSM 02.60]. GPRS is a standard developed by ETSI for the use of packet data in GSM networks in what constituted an intermediate step towards the 3rd generation of mobile communications (therefore the fact of being referred to as 2.5G) [Scholefield 1997].

3GPP has provided in the last years several releases, which constitute a roadmap towards a next generation of telecommunication networks. Each of these releases is characterized by several milestones in the different standardization activities (which cover both radio and end-user service aspects) occurring inside 3GPP. The several releases do not constitute an end, but are instead a waypoint in a path towards a next generation network whose goals are constantly being updated.

2.1.2.1 UMTS Release 99 (R99)

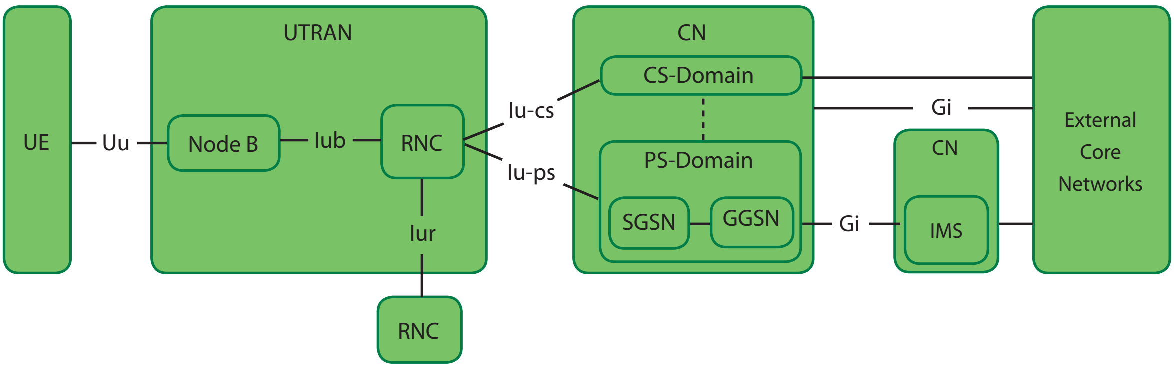


Figure 2 – UMTS Logical Architecture

The UMTS R99 standard release strongly emphasizes the ability of smooth evolution from GSM to UMTS networks [3GPP R99]. The UMTS network had to be backward compatible with GSM networks, and it also had to be able to inter-operate with GSM. Several important enhancements were introduced, compared to GSM. A new radio interface, based on WCDMA FDD (wideband code division multiple access – frequency division duplexing), was introduced accompanied by the introduction of the UTRAN (UMTS Terrestrial Radio Access Network) architecture and the Interfaces Iu/Iub/Iur (see Figure 2).

The User Equipment (UE) connects to the UTRAN via the NodeB using the Uu interface. The NodeB is responsible for transmitting both control and user traffic destined to the UE over the radio interface. Each Node B is connected to a Radio Network Controller (RNC) which is the main control entity in the UTRAN. From the RNC an Iu interface exists that connects the UTRAN to the Core Network (Figure 2). In the case of the Packet Switched – Domain, that entity is the Serving GPRS Support Node (SGSN).

At the service level, the UMTS AMR (Adaptive Multi-Rate codec for UMTS) was introduced as well as Enhanced Call Control. The GLR (Gateway Location Register) is also introduced in R99, providing a proxy for HLR (Home Location Register) to optimize signaling of subscriber information across network boundaries.

Table 1 - UMTS QoS classes (in 3GPP TS 23.107)

Traffic class	*Conversational class conversational RT*	*Streaming class streaming RT*	*Interactive class Interactive best effort*	*Background Background best effort*
Fundamental characteristics	- Preserve time relation (variation) between information entities of the stream Conversational pattern (stringent and low delay)	- Preserve time relation (variation) between information entities of the stream	- Request response pattern - Preserve payload content	- Destination is not expecting the data within a certain time - Preserve payload content
Example of the application	- voice	- streaming video	- Web browsing	- background download of emails

Release 99 is extremely relevant for Advanced QoS in UMTS, as it defined 4 QoS classes: "Conversation", "Streaming", "Interactive" and "Background" (see Table 1).

In this release, QoS is still not addressed end-to-end, and exists only between the UE and the GGSN. QoS setup is based on the PDP Context Establishment Procedure done after the UE attaches to the SGSN [3GPP TS 23.060].

2.1.2.2 UMTS Release 4 (R4)

As a follow-up to the R99 enhancements, Release 4 emphasizes the separation of transport and its control from the Circuit Switched (CS) Core Network (CN) domain, as well as the use of IP transport in the CN protocol [3GPP R4]. A new radio interface is introduced, WCDMA-TDD (wideband code division multiple access – time division duplexing), and UTRAN interfaces and protocols are updated with a TDD counterpart.

In this release new elements are introduced in the core network such as the LCS (Location Server), Media Gateways (MGW) and the MSS (Mobile Switching Center Server – a separate element that evolved from MSC and the VLR). The Media Gateway is responsible for connection maintenance and bearer switching, and the MSS is responsible for the connection control.

Due to these new elements and functionalities, the CS domain is able to scale freely: if more switching capacity is required, MGWs are added; when more control capacity is needed, an MSC server can be added (one MSC server can control several MGWs). The MGW is also able to change from circuit switched call to the packet switched call.

One of Release 4 main accomplishments was the introduction of an All-IP core network that would prepare the way for the inclusion of more IP based features and mechanisms in future releases.

In Release 4 the Radio Access Bearer setup is enhanced with a QoS negotiation and re-negotiation mechanism. Additionally, reliable QoS for the PS domain is introduced, but end-to-end QoS is left to be later included in Release 5 [3GPP R4_R5].

2.1.2.3 UMTS Release 5 (R5)

Release 5 features the introduction of High Speed Downlink Packet Access (HSDPA) which allows data rates of up to 10 Mb/s. As network evolution continues, all traffic coming from the

User Equipment is expected to eventually become IP based and in this release IP Transport is introduced in the UTRAN as an alternative to ATM [3GPP R5]. This evolution was made in Release 5 as a continuation of the IP introduction started in Release 4 in the Core Network. The introduction of IP as a transport protocol in the radio network does not necessarily imply an end-to-end IP network since the UTRAN IP network uses private addresses. Release 5 selected the protocols to transport the Radio and Signaling bearers over IP. UDP is used for the User plane interfaces and SCTP (with additional protocols) is used for Signaling bearers.

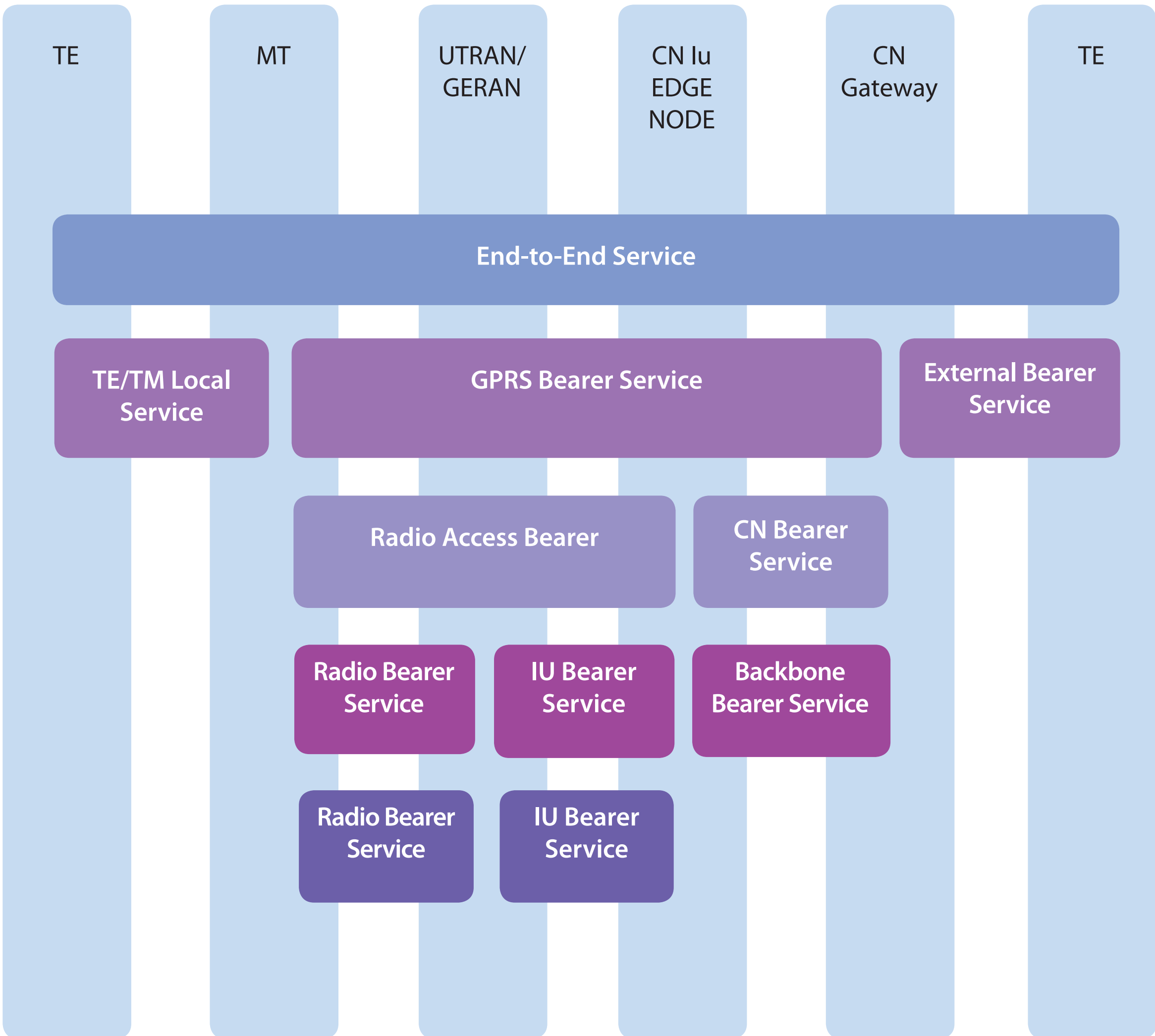


Figure 3 - 3GPP - Release 5 - End-to-End QoS Architecture

Release 5 is the first release to implement an End-to-End QoS concept and an architecture based in IP [3GPP 23.207] (see Figure 3). In this release, the interactions between the TE/MT

Local Bearer Service, the GPRS Bearer Service, and the External Bearer Service are described, and how they provide Quality of Service for an End-to-End Service (see Figure 3). On the IP level, the mechanisms necessary to provide End-to-End Service are described, involving the mechanisms necessary for interaction between the IP level and the GPRS level. Although the initial specification allowed for the inclusion of both IntServ and DiffServ, the later is the most used to provide different service levels, and for the traffic flow classification.

In release 5 the introduction of the IP Multimedia Subsystem (IMS) provided the UMTS architecture with a uniform multimedia network for high-quality voice and other real-time traffic transmissions with mechanisms that fully support Quality of Service and advanced security based on IP [3GPP 22.228].

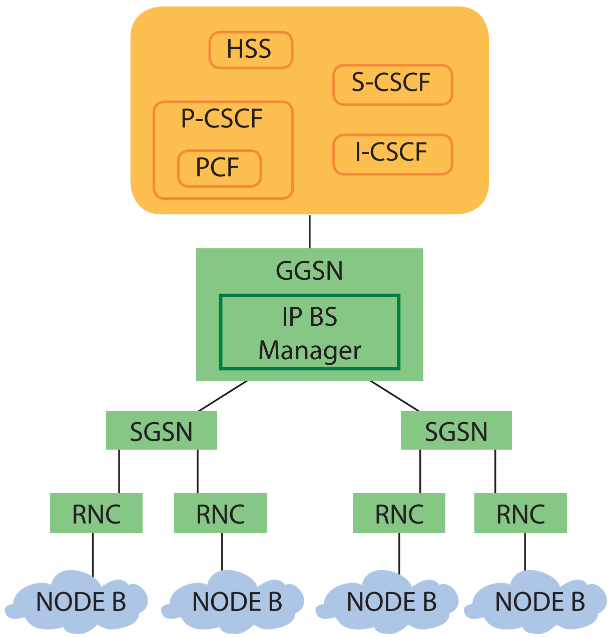


Figure 4 - UMTS Network Architecture (relevant QoS Entities)

The basic network architecture proposed in Release 5 is depicted in Figure 4. This model, although simplified, contains most of the entities involved in resource reservation and QoS provisioning in the UMTS network.

The IMS incorporates the Home Subscriber Server (HSS) and three Call Session Control Functions (CSCF): the Proxy-CSCF (P-CSCF), Serving-CSCF (S-CSCF) and Interrogating-CSCF (I-CSCF). The Gateway GPRS Support Node (GGSN) is then responsible for connecting the Radio network to the IP network and mapping QoS at the IP layer to QoS at the radio layer. A simplified description of the relationships between these entities follows.

Since the IMS belongs to the IP Backbone, QoS is supported by DiffServ mechanisms [RFC

2475]. The GGSN is the entity responsible for providing DiffServ edge functionality. Between the GGSN and the users, four different QoS classes are provided with different QoS guarantees: conversational (the most demanding class), streaming, interactive and background (no QoS guarantees). These classes are mapped into the DiffServ Code Point (DSCP) field of the IP header depending on the bandwidth and resource provisioning.

In this architecture, the P-CSCF enables the coordination between events in the application layer and resource management in the IP bearer layer, acting as a Policy Decision Point (PDP) [Strassner 2003] for the GGSN. The Policy Control Function (PCF) is the logical policy decision element present in the P-CSCF, which uses standard IP mechanisms to implement policies in the IP bearer layer. The PCF makes decisions regarding network based IP policy using policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP Policy Enforcement Point (PEP). This mechanism is called Service-based Local Policy (SBLC).

The I-CSCF is mainly the contact point, within an operator's network, for all IMS connections destined to a subscriber of that network operator or to a roaming subscriber currently located in that operator's service area. The S-CSCF handles the session states in the network, managing ongoing sessions and providing accounting mechanisms. The HSS aids the call control servers in completing the routing/roaming procedures by solving authentication, authorization, name/address resolution, and location dependency issues. [3GPP TS 23.228][3GPP TS 23.002]

Signaling in the IMS is based on the Session Initiation Protocol (SIP) [RFC 2543] and communication between the P-CSCF in the IMS and the GGSN is performed over the *Go* interface using the Common Open Policy Service (COPS) protocol [RFC 2748].

2.1.2.4 UMTS Release 6

In its Release 6, 3GPP adds a very important functionality to the subject of this thesis: the Multimedia Broadcast/Multicast Subsystem (MBMS) [3GPP TS TS 22.146]. MBMS provides functionalities that enable the sharing of radio and core network resources in the Packet Switched domain. It does this by introducing a multicast mode (in addition to a broadcast mode), which enables data to be delivered to only a set of users within a service area, and to charge them accordingly. Further details to MBMS are presented in Section 3.5.2 .

Another important feature added in Release 6 is the Wireless Local Area Networks (WLAN) interworking [3GPP TS 23.234] capability. This new feature seamlessly extends 3GPP services and functionality (such as common billing and the provision of IMS services) between the WLAN and the 3GPP system. This interworking leads to WLAN becoming a complementary radio access technology of the 3GPP system.

In Release 6 new services such as Presence and Speech Recognition were also introduced together with improvements to the IMS subsystem [3GPP R6].

QoS has mostly been untouched.

2.1.2.5 UMTS Release 7

Release 7 continued 3GPP efforts towards a truly all-IP network by further specifying requirements for MBMS and WLAN-Interworking [3GPP R7]. Data rates continue to increase in R7 through HSPA+ (High Speed Packet Access (HSPA) evolution) [3GPP TS 25.999] MIMO functionality is also integrated in UTRA (FDD and TDD) in order to improve system capacity and spectral efficiency [3GPP TS 25.876].

In this release an effort was made to align interfaces and protocols with organizations such as IETF and OMA. One of such examples is the replacement of the RADIUS protocol [RFC 2865] by DIAMETER. Internal harmonizations occur in this release such as Policy and Charging Control, which unites and generalizes the applicability of SBLC and Flow-based Charging under a single interface, providing both resource request and charging [3GPP TS 23.203]. This ultimately led to a new *Gx* reference point, that is realized by combining *Go* and R6 *Gx* within a single protocol (DIAMETER).

2.1.2.6 UMTS Releases 8

This very recent release constitutes the most recent step towards a 4th generation of Radio Technologies [3GPP R8]. Release 8 can be broken into two: the System Architecture Evolution – Evolved Packet Systems (SAE) part [3GPP TS 33.401] and the Long Term Evolution (LTE) – Evolved Packet System RAN part [3GPP TS 36.300].

LTE distances itself from previous releases and provides a new simplified architecture that intends to overcome past limitations in peak data rate, latency, capacity, spectrum efficiency, mobility, etc.

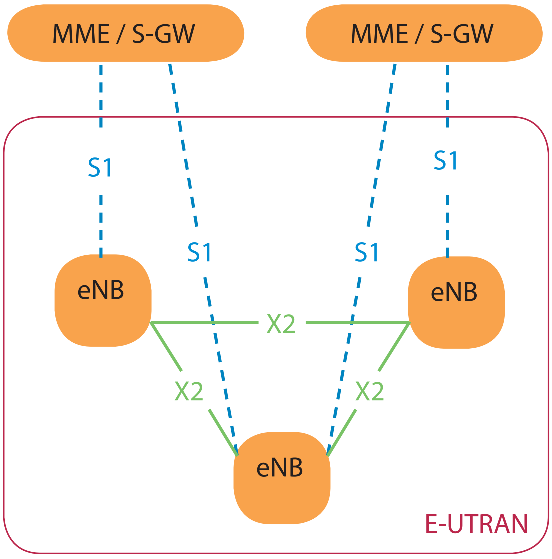


Figure 5 - Release 8 LTE Overall Architecture (according to 3GPP TS 36.300, TS 36.401)

The novel air interface for LTE combines Orthogonal Frequency-Division Multiple Access (OFDMA) based modulation and MIMO for the downlink, together with SC-FDMA (Single Carrier FDMA) for the uplink. This new air interface promises rates as high as 300mbps. Additionally LTE's Enhanced UTRAN (E-UTRAN) features an important Logical separation of signaling and data transport networks [3GPP TS 36.300][3GPP TS 36.401]. Another relevant change from previous radio access interfaces is the smaller number of entities involved (eNB and MME/S-GW) as opposed to previous releases (NodeB, RNC, SGSN) (see Figure 5).

The eNB (enhanced Node B) does most of the Radio Resource Management while the MME manages mobility, UE identities and security parameters.

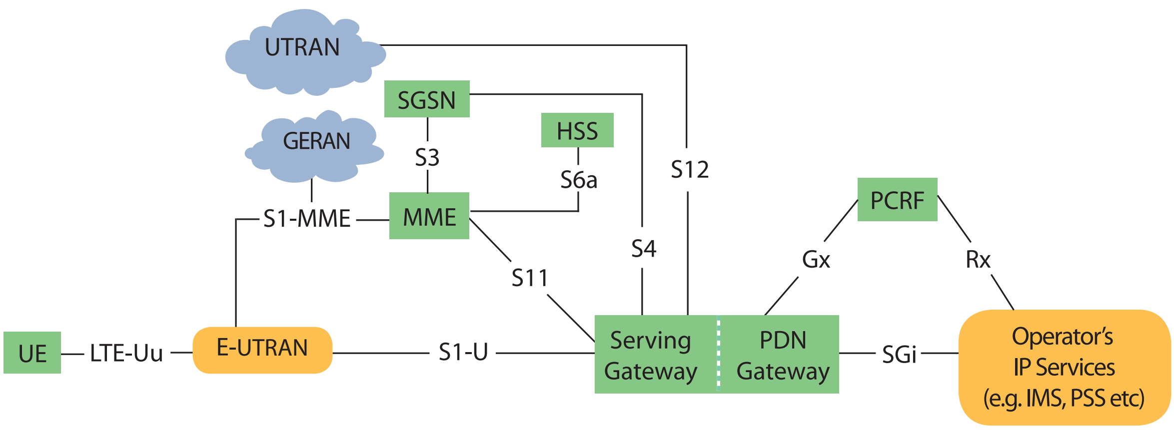


Figure 6 – SAE - Evolved Packet System Architecture

In its most basic form, the EPS architecture (Figure 6) consists of only two nodes in the user plane: a base station and a core network Gateway (GW). The node that performs control-plane functionality (MME) is separated from the node that performs bearer-plane functionality (GW). The GW concept is also extended to other technologies such as WLAN [IEEE 802.11] and WIMAX [IEEE 802.16].

SAE moves forward the objective of achieving a true all-IP network supporting a variety of different access systems (existing and future), mobility and service continuity between these access systems, and access selection based on combinations of operator policies, user preferences and access network conditions [3GPP TS 22.278].

2.1.3 TISPAN

Developed by ETSI to fit the specific requirements of fixed-line providers, TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks) is an extension to the IMS architecture previously described in the scope of 3GPP. TISPAN was developed with the clear objective of a converged wireless and wired network, merged with the Internet. One of the most important features of TISPAN is the fact that it can handle more than just SIP based applications, which comprise most of the applications currently deployed over IP.

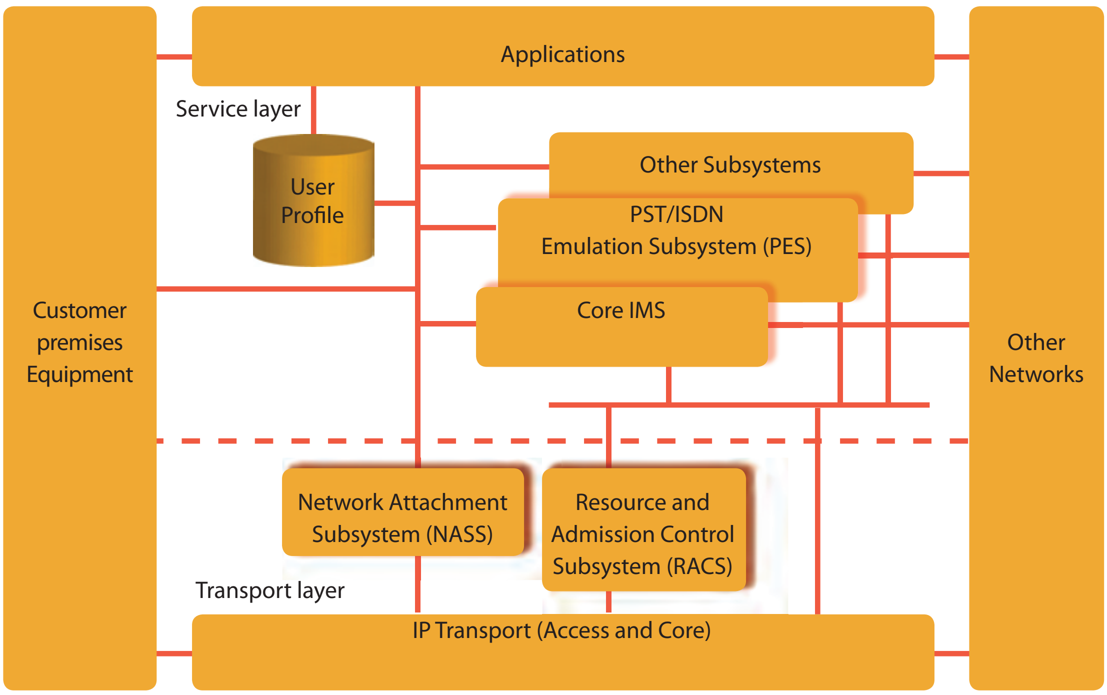


Figure 7 - ETSI - TISPAN basic architecture

The main elements of TISPAN, besides the IMS, are the Resource and Admission Control Sub-System (RACS) and the Network Attachment Sub-System (NASS) (Figure 7). The RACS is responsible for admission control, resource reservations, policy control and NAT traversal [ETSI ES 283 026] while the NASS is responsible for IP address provisioning, network level user authentication, authorization of network access and access network configuration [ETSI ES 283 034].

2.1.4 4G Networks

4G networks were until very recently considered a concept that related to the next evolution on Mobile Telecommunications. 4G networks can provide the same, and even improved, functionalities as 3G UMTS, requiring a smaller number of entities and having lower complexity. 4G networks (also referred to as NGN or sometimes as All-IP networks) define an universal network architecture for heterogeneous environments, where all types of services may be jointly provided, satisfying their diverse requirements.

Today operators are already presenting us with so called 3,5G services. Nevertheless they are referring only to the radio enhancements provided by recent 3GPP releases, and still lack most of the service platforms present in those same releases. 4G networks support to the “legacy” 3G UMTS transport network, as previously presented in Release 8. However, although 3G networks evolved from previous 2G networks (e.g. GSM), 4G networks are mostly transport agnostic and therefore do not constitute a direct migration from 3G UMTS. 4G networks encompass several transport networks such as WiMax, WiFi and even broadcast technologies such as DVB. The emphasis in 4G is therefore on the convergence of the underlying technologies towards IP based Networks in which existing internet services (such as email and WWW) can be delivered together with advanced multimedia services (such as video conferencing and TV) much in the same way as proposed by 3GPP latest releases and TISPAN.

One major issue in 4G network research is the support for all the different access technologies an operator might want to introduce in the future. The existence of different access technologies requires nonetheless a certain degree of intelligence in the core network that needs to adapt and/or police the services being delivered through each interface.

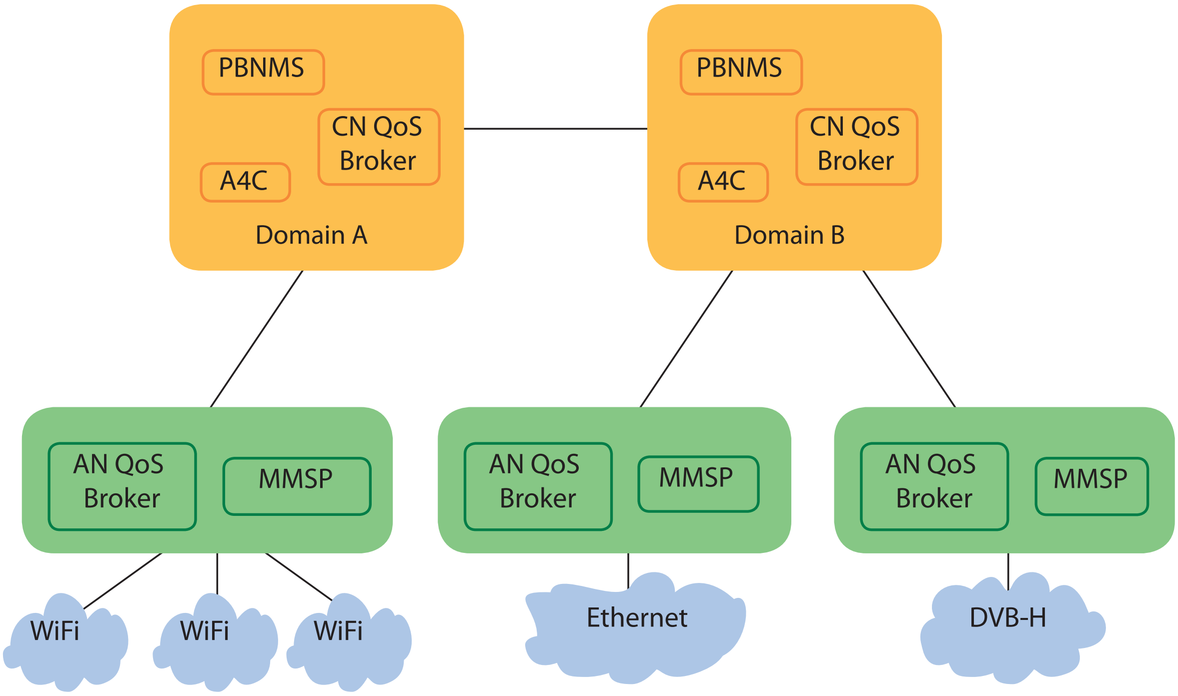


Figure 8 - All-IP 4G Network Architecture (relevant QoS elements)

Figure 8 presents the QoS-related elements of a research oriented All-IP 4G network architecture [Aguiar 2004]. The addition of Core Network Elements such as CN QoS Broker's and CN Router, plus the integration of Multimedia Service Proxies entities leverage to a new degree the concepts already present in the IMS concept of 3GPP and TISPAN. With an added value: these entities are now transport agnostic and will be based in a new version of the IP protocol (IPv6) while TISPAN still relies in IPv4 (due to their need to support legacy applications) and most 3GPP deployments have adopted IPv4 (although IPv4 is considered optional). In this evolution there is a clear separation between Access Network and Core Network. The separation can enable innovative business models in which the Access Network and Core Network can belong to different legal identities. This architecture lightens the infrastructure requirements to operate the network, using fewer entities to provide the same functionalities. DiffServ is used to support QoS in the core network, achieving scalability and performance. In this architecture a key QoS element is the QoS Broker, which performs admission control and manages network resources, controlling routers according to the active sessions and their requirements in much the same way as the RACS in TISPAN. It also performs load balancing of users and sessions among the available networks (possibly with different access technologies) by triggering network-initiated handovers [Melia 2007]. This is an important feature, since it provides the operator with the means to optimize the usage of network resources. Some high level knowledge of running services and available network technologies might, for instance, enable the QoS Broker to move a video stream from a WiFi network to a DVB-T broadcast channel.

This feature is made possible by a close relation between the Multimedia Service Proxy (MMSP), aware of the requirements of user services, and the QoS Broker in the Access Network (AN QoS Broker) [Azevedo 2005]. For the provisioning of multimedia streaming services, Multimedia Servers (MMServer) may also be present, located in the application servers' garden. For scalability reasons, the Core Network (CN) QoS Brokers only deal with aggregates of flows traversing the core network and communication with other administrative domains. The QoS definitions at the domain level are provided by a Policy Based Network Management System (PBNMS), and then proxy by the AN QoS Brokers to the Access Routers (AR) in the different access networks. For authentication and accounting purposes, an A4C server is also present in each domain.

4G networks must nonetheless support all services currently available in 3G networks, ranging from basic telephony to advanced multimedia services such as video conferencing and MMS. While the Multimedia Servers might be deployed inside an application server garden, QoS requirements for these services require the need for a deployment of Multimedia Service Proxies in the Access Networks, where they are closer to the User Equipments and QoS Broker. Multimedia Service Proxies are regarded as representatives of the User Terminals, capable of better relating with the operator infrastructure in order to provide the required QoS to the applications. Nonetheless, they are not enforcement points. The Access Routers are the true enforcements points in this network, connected to the QoS Broker by a PEP/PDP (Policy Enforcement Point/ Policy Decision Point) relationship: the Access Routers receive proper policies issued by the QoS Broker based on higher-level policies provided by the PBNMS and per session requirements provided by the Multimedia Proxy.

The research network described was part of project IST-Daidalos [DAIDALOS], a NGN project supported by the EU FP6 framework, which took place from 2003 to 2008, therefore predating TISPAN and 3GPP LTE/SAE. Many of the features in this network are now present in TISPAN and 3GPP LTE/SAE and show the relevance of the work done in this project. On the other hand, some of the concepts are still to be incorporated into standardization bodies, such as better integration of broadcast technologies, inter-domain QoS and the split of the Core Network (as defined in 3GPP) into Access Networks and Core Network (as defined in the scope of this project).

2.2 Group Communication

Group Communication still accounts for a large share of the telecommunications market through Radio and TV services. These services are still mostly provided to end-users using an over-the-air analog broadcast network. In the last decades these services have been digitalized and provided to users mostly through a broadcast network based in the DVB-C [ETSI EN 300 429] and DAB [ETSI EN 300 401] standards.

Today we are witnessing an explosion in the provisioning of what were usually broadcast services over the Internet, impaired by the inability of Internet Service Providers to provide proper QoS for such services. Instead they have created private distribution networks in order to provide Radio and TV services to their customers in conjunction with voice and data services [TISPAN TS 183 028].

However group communication is not just about broadcast services such as Radio and TV. It is also about services such as audio/video conferencing and, increasingly it is about games where users are engaged in the exchange of information. These services (especially games) are expected to gain more attention from users and therefore require the network to support them accordingly.

Operators must assure that services are delivered with a degree of Quality with which the end-user agrees with. In the case of Radio and TV, the expected quality in a NGN network must match the quality associated with today's Broadcast Networks. In such networks, with a single transmitter making use of the medium, QoS is quite predictable and through a good planning of the network in terms of coverage, all end-users can receive the service with a high level of quality. In NGN this will not be the case as there are more services competing for the medium, and the medium is not accessed by a single transmitter, but by all end-users. The need therefore arises to develop QoS mechanisms to assure QoS for Group based communication scenarios such as the cases of Multimedia Broadcast Services (TV, Radio), Conferencing (Audio/Video) and Gaming. This challenge also involves the study of how the technologies usually involved in group communication, such as the DVB family of technologies, can be integrated into NGN, and how to make the best of their use.

The most efficient way of delivering group services in an IP environment is IP multicast. For heterogeneous environments, IP Multicast provides a common abstraction essential for the service provider: regardless of the technology, group management is handled uniformly. Nonetheless the deployment of IP Multicast has been limited due to inefficient access control and insufficient QoS mechanisms. Furthermore, the uniformity of IP multicast over all access networks hampers an optimum exploitation of the specificities of each technology (e.g. for resource management). This is especially relevant in wireless networks. Wireless technologies can deeply influence IP multicast service capabilities in many ways, such as the unidirectional characteristics of DVB channels or the bandwidth limited broadcast channel of UMTS.

Delivering content to a group has for long been a challenge in IP networks. In its original work, Dearing [RFC 1112] proposed a technique for the transmission of an IP datagram to a “host group” composed of one or many hosts identified by an IP address. This initial work mainly focused in the need to efficiently use network resources to deliver the same content to a group of hosts, and did not take into consideration issues such as security and QoS. IP Multicast scalability relied in not requiring prior knowledge of whom or how receivers behaved. It uses network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. The routers in the network take care of replicating the packet when necessary to reach multiple receivers. [RFC 1112] was also one of the first works to implicitly separate IP address from the host identifier, since in IP multicast the IP address identifies a dynamic group and not an end host. From this pioneering work, several solutions for scalable and efficient mechanisms of content delivery to a large audience have been proposed (e.g. [Dapeng 2001], [Imai 2003]).

Commercially IP Multicast has not faced the expected success mostly due to security concerns and lack of QoS support. An operator willing to deploy e.g. IPTV services over IP multicast requires that only authorized users should be able to subscribe and access the multicast group. Since authorization is performed on a per user basis, through tight control of the multicast subscription mechanism in the access router, operators can limit unauthorized access to a group to certain degree [Satou, 2005]. However unless multicast content is also protected through cryptographic mechanisms, a nearby user can listen to the multicast content that is being locally broadcast to an authorized user [Judge 2003]. Another important issue is QoS assurances. In the common IPTV scenario, a source (Content Provider) sends a single multimedia stream of IP packets to a group, without identifying who belongs to the group. Thus, IP multicast listeners cannot reply back to the source with flow control information, although some work is being carried on scalable flow control mechanisms for IP multicast [Chawathe 2003] no standardized solution exists to date. Note that a scalable flow control mechanism is not the only possible solution, e.g. the IETF Reliable Multicast Transport group [IETF RMT] proposes NACK based protocols and Forward Error Correction (FEC) algorithms, by which listeners can recover from packet loss in the media [Roca, 2002].

After years of dismissal, recent developments in technologies and business models for telecom operators have re-enacted IP multicast as an effective technique of delivering content to a broad set of end-users. Group communications are now seen as promising services by all operators - and not only broadcast ones - a situation that arouse by the increasing integration of communications across platforms. IPTV is one of the main services deployed by telecom operators with the so-called “triple play” offerings. It constitutes the basic group communication service where registered and authorized end-users receive a real-time IP based multimedia stream at the contracted QoS level.

Albeit all the technical hurdles discussed above, industry still pushes a strong use-case for

IPTV services, with some 3G operators in Europe already providing Mobile TV services based on content distribution networks, in the process of migrating to 3GPP-MBMS (Multimedia Broadcast/Multicast Services).

MBMS [Boni 2004] is a 3G subsystem that provides point to multipoint downlink bearer service for IP packets in the packet switched domain. MBMS uses existing common channels, such as FACH, and relies in IETF multicast in the core network, minimizing impact on standards and infrastructure. MBMS supports two modes, broadcast (no billing/user activation) and multicast (billing, multicast join). Although 3GPP-MBMS provides a complete platform that addresses all issues related to Multimedia Multicasting, it is limited by the radio FACH channel to a 384kbps radio bearer in 3GPP R6. Furthermore, MBMS applications must follow very strict API's.

Through MBMS, 3GPP has two ways of delivering a service either through PTP and PTM mechanisms at the Radio Level. This aspect has led to a thorough study by the research community on when to use each of the services [Alexiou 2007], [De Vriendt 2003], [OverDRiVE], [B-BONE]. In such works there is an emphasis on the study of power control mechanisms. Power control plays a very important role in these decisions, since it affects directly the inter-cell interference. In order to efficiently use the available power and radio resources the MBMS can make use either of the FACH channel (which is broadcast) or of several DCH channels, one for each UE. The studies previously mentioned have carried simulations that address a very important question: "When to use a PTP or PTM channel". The threshold for switching between DCH and FACH is nonetheless consistent in all the studies and points towards 5 UE per cell, a point in which communication should be carried no longer using different PTP channels but through a single PTM channel. These studies however address a problem and solution at a very low layer (L1), and are very technology specific.

Besides 3GPP-MBMS, the DVB consortium has also standardized Multimedia streaming over IP Multicast [ETSI TS/EN 3001 192]. In the DVB use-case, a very interesting limitation exists: the channel is unidirectional, requiring an additional channel for signaling (which might not always be available). In the DVB consortium, group security can be achieved using offline mechanisms such as smart cards, and QoS relies heavily on FEC algorithms. These solutions intend to overcome the lack of a reliable return channel, and do so to the expense of a limited set of services and lack of user interactivity (considered a requirement in NGN). Nonetheless DVB is an industry standard with commercially deployed solutions over the world, thanks to its broadband capabilities that easily overcome the overhead created by the FEC headers necessary to deliver multimedia with good QoS.

With many of IP Multicast problems due to the shared transport channel, the idea of using P2P networks and their multiple one-to-one transport channels has sprung in the community, with multicast overlay networks over P2P [Chawathe 2000][Jannottti 2000]. Most of these solutions prove to be scalable and do not face the same QoS and Security problems as native IP multicast. As problems, we lack real time support (media is re-broadcasted over several nodes), inefficient usage of network resources (content must travel through several bottlenecks in the access network several times), and lack of privacy (content is usually cached in each node).

2.3 The Problem

In the previous sections, a historical view state-of-the-art was provided in the area of Next Generations Networks and group communications. These two areas are essential to understand the problem this thesis intends to address.

The work done in 3GPP towards the evolution of Mobile Telecommunications Networks into All-IP based networks, as well as the work done in ETSI TISPAN, shows a clear path towards a 4G network characterized by the convergence of networks under the IP protocol. Unfortunately in this evolutionary path, group communication technologies and services have been considered as additions to the global architecture (as seen in 3GPP MBMS). On the other hand, the great success of IPTV services by Telecom Operators has proved that group communications are an important service, even in Next Generation Networks. Additionally broadcast operators have an important asset in terms of broadcast licenses and technologies that could be used in Next Generation Networks in order to reach users with group based services more efficiently than resorting to unicast technologies.

A next generation operator has therefore a large interest in integrating such broadcast technologies into its set of technologies, since they can free their unicast technology resources from the group based services such as IPTV. The problem set to be addresses in this thesis, is on how to evolve towards a Next Generation Network, integrating group communication technologies and services deeper into the network, in a resource efficient manner.

This thesis intends to describe a NGN architecture in which group communication technologies and services are fully integrated and in which they play an important role in providing services, making an efficient use of the available technologies resources.

3. Concepts and Abstractions

3.1 Quality of Service in IP based Networks

Next Generation Networks design challenges are currently focused on the convergence and inter-working of all existing and emerging, fixed and mobile, wired and wireless network access technologies, including broadcast. The support for such heterogeneous environments provides more flexibility to the network operators. Such flexibility is displayed by the capability of operators to maximize their service coverage through different technologies and the possibility to price according to the access technologies available, dictated by economical viability and business interests.

An important goal for NGN networks is the support for the increasingly wider range of applications that the users expect the network to provide, supporting a good perceived service quality and the flexibility to tailor the services to their own preferences and requirements [Kuan-Ta Chen 2009].

The importance of service applications (e.g. messaging, voice, content delivery) is easily demonstrated by the impact of multimedia services in our daily life, such as newspapers, telephony and television. These mass media services require an increased amount of network resources from communication networks. When considering NGN environments, we must not only consider the requirements of today's mass media services, but also of tomorrows multimedia services such as video conferencing and Digital Interactive TV in an increasingly mobile environment where users want to have their services delivered to them regardless of time, location and technology used to access it.

In such heterogeneous networks the IP protocol, in either of its incarnations (IPv4 and IPv6), provides a technological abstraction to applications and services from the underlying network technologies. IP based mechanisms capable of supporting basic transport services such as Security, QoS, Mobility and A4C can be used over all the technologies, thus providing costs savings in terms of infrastructure. Furthermore, IP is an open protocol seamlessly deployed over the world, providing global connectivity and an almost infinite number of services and applications, essential to the success of any network.

The IP protocol, as a convergence layer, simplifies the support for seamless mobility across heterogeneous networks through mechanisms such MIP [Perkins 2002][RFC 3775], FMIP [RFC 4068], SIP [Wedlund 1999] and PMIP [RFC 5213]. The provision of multimedia (and value-added) services in multi-technology environments requires the definition of a global signaling strategy for addressing the issues of session negotiation, network resource reservation and session and QoS re-negotiation.

It is also agreed that NGN's will need to fulfill the requirements of operators with quite different business interests. The expected basic services to be provided in those networks are still a controversial point among telecommunications operators. In this respect, there are two major and diverging views [Crowcoft 2007]: one, dominated by the "transport vision", in which the telecom operator primarily sells QoS-enabled transport services and the user provides most of the intelligence in terms of multimedia services. Another, dominated by the "service vision", in which the telecom operators are mainly interested in selling more advanced communication services.

These two visions correspond to two different business models, and have a deep impact in the design of the architecture that will be the basis for next generation heterogeneous networks, since the expected traffic and user behavior can be quite different depending on these business views [Dhamdhere 2008]. When proposing solutions for NGN it is important to keep in mind these two diverging trends, as the tools available to do optimizations are different in each of the scenarios.

Nevertheless, in both visions, the scalable support for end-to-end QoS in mobile and heterogeneous scenarios is a major challenge.

The heterogeneity of technologies and their support for different number of services (such as Digital TV in DVB or voice in UMTS), as well as their different capabilities in terms of pure bandwidth capacity (as seen in the 802.11 standards), requires from upper layers proper mechanisms capable of exploiting the best characteristics in each of them. In such an environment, it is hopefully no longer important which technology is being used, but how efficient in terms of QoS parameters is the service being deployed to the user and how much assurance does the operator have that the end user does not perceive any modification on the consumed services, regardless of the technology being used for service delivery.

Ultimately this could mean the capability of the user to signal the operator its QoS perception. This idea, although apparently obvious, is nonetheless undesirable by both the user and the operator. The first would be bothered by the need to constantly interact with its communication device and would surely find it an unappealing experience. For the operator, the QoS as perceived by the user, although valuable, would be considered unreliable, as it would not be submitted to an analytical measurement method. By leaving out this option, it is necessary to rely in the User Application and the Network itself to report and provide the desired QoS.

In the next section two different approaches to QoS signaling will be addressed through an extended comparison analyzing their importance, and summarized using a SWOT approach.

3.2 Network Level and Application Level QoS Signaling

Providing QoS in a communication network means properly matching supply to the demand of resources. In circuit switched networks that would mean provisioning the network with enough circuits capable of coping with peak usage. In packet switched networks, QoS can be associated with over provisioning, by which operators install many more resources than those estimated. This method is called Over Provisioning and is the most common QoS mechanism in today's networks. Nonetheless it is not an efficient mechanism from the point of view of resource management, as most of the network resources are usually not used (by definition).

Another solution to this problem is to use a reservation mechanism through which services can share limited resources, providing graceful degradation to users that do not require stringent QoS levels. In such an environment it is essential that accepted requests do not surpass supplier's available resources. Due to the intrinsic best-effort nature of IP, such situation would create a global starvation of resources, as the few available resources would have to distribute as equally as possible between services. Reservations wouldn't have any effect unless a tight control of the reservations was to be enforced by the network. Most importantly applications would be required to communicate directly with the underlying network. Requiring from the network to have interfaces to any given application.

An additional solution would be to differentiate between services giving different priorities and resources to each one of them. Differentiation would in this solution play the role of implicit reservations. But, as in the previous solution, it all depends of the network and applications. The network must be able to distinguish and enforce differentiated treatment of services and applications must be able to signal to the network their differences.

Before distinguishing Network Layer signaling and Application Layer Signaling it is important to mention what they have in common, and the mechanisms involved in providing QoS in IP based networks.

When the need to manage a resource arises (whichever the resource might be: well, bridge, warehouse, etc) the first task is to control the access to the resource. Without proper access control, management of the resource is virtually impossible as it becomes very difficult to control the usage of resources by demanders.

The primary requirement for QoS provisioning is therefore Connection Admission Control (CAC). Limiting the access to the network by authorized services is essential to guarantee a controllable system and the predictability of its behavior.

Figure 9 – QoS Procedures enforced by Routers

A given service should only be provided with the contracted/signaled QoS. If a service misbehaves and is not promptly policed, resource starvation at system level could take place. It is therefore required the correct policing of services. The policing mechanism must control packet flow and drop if necessary packets belonging to misbehaved services.

In order to enforce QoS at a packet level, a router must enforce three main procedures: Classification/Admission Control, Queuing and Scheduling. [Tanembaum 1996]. The first procedure a packet undergoes is Classification. This initial procedure identifies a service by its packets and policies them according to the requested/configured traffic definitions. After these policing mechanisms, all services behave according to what was contracted/signaled and services can now undergo prioritization/differentiation (misbehaving packets are dropped in the classification policer). This procedure ends by classifying packets according to the available processing queues. The Queuing procedure logically separates service packets making it possible to treat services differently and therefore providing several levels of QoS according to the Scheduling procedure. The Scheduler is here responsible for picking packets corresponding to the different services from the Queues and actually sending them to the network.

The described QoS provisioning concept can still be deployed in several distinct ways. If we consider the 7 layers of the OSI model, this concept can be implemented in each and every layer. In this thesis, focus shall be placed on the 3rd and 7th layer (respectively Network and Application

Layer) due to their broader dissemination in real systems.

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more segments of the Link Layer (OSI's 2th layer), while maintaining the quality of service requested by the Transport layer (OSI's 4^{th} layer). The Network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers (the main fabric of IP networks) operate at this layer.

As for the Application Layer it interfaces the end-to-end points without any interface to the network, and performs common application services. It also issues requests to the lower layers (mainly the presentation and transport layer). Being the top most layer, the Application layer has only end-to-end knowledge of the communication and retains no information of the path followed.

Table 2 - SWOT analysis of Network and Application layer signaling

	Network layer Signaling	Application layer Signaling
Strengths	- Application Independence - Protocol simplicity - Direct interface with the Control Plane	- Best knowledge of the QoS requirements of the application - Tight control over the reservation procedure
Weaknesses	- Application cannot stringently express their QoS needs due to abstraction mechanisms in the Network Layer - Extra interface for applications	- Each application is required to implement in its logic the QoS protocol. - Unaware of the network technologies - Mostly inefficient in resource scarcity scenarios
Opportunities	- True interoperability regardless of application platforms - Capability to provide QoS throughout the network path. - QoS aware routing	- Large service delivery platforms such as IMS can unify applications signaling mechanisms at the application level. - The development of entities capable of translating Application layer signaling into network layer signaling.
Threats	- Unwillingness by application developers to integrate QoS signaling mechanism into their applications. - Cost associated to deploying QoS enabled networks	- Disregard by network operators who do not wish to support heterogeneous QoS mechanisms. - Security mechanisms

Choosing between Network and Application Layer signaling approaches incurs in a trade-off of many aspects, which are detailed in Table 2 using a SWOT analysis.

As seen in the *Threats* row of Table 2 one of the major stakes when choosing between approaches lies in the interest of the players involved. Network Layer signaling solutions are usually driven by network operators while Application Layer signaling solutions are more related to application developers. This fact is mostly due to the functionalities provided by each approach.

Network Layer signaling mechanisms are abstract to the application. They handle at most transport layer information (such as UDP/TCP ports in the case of IP), with complete abstraction of what kind of data is actually being signaled. Its focus is on providing information that can easily be mapped into QoS enforcement mechanisms deployed in the network routers. At the network layer, services are described through the identifiers of the communication (IP addresses), the transport layer parameters (protocol and ports), and traffic specification (might include bandwidth, token bucket parameters, etc).

On the other hand Application Layer signaling mechanisms are usually coupled with applications. Application layer signaling is agnostic of the network path chosen by the network and relies solely on the correct behavior of the applications in the end terminals. The information signaled usually includes application specific information (such as CODECS and message sizes) and leaves to the correspondent application to infer on the appropriate behavior it must display in order to communicate with QoS.

Application developers that mostly have no relationship to network providers, take usually the Application Layer signaling mechanisms as their primary means of QoS. Since they can fully rely on their application to behave correctly, they do not make a requirement the QoS support by the network.

QoS mechanisms only exist in the end points of the communication. Traffic is still handled by the network with no QoS, as routers do not acknowledge any of the information exchanged at the application layer. This would require massive resources (unavailable at routers) to process transport and application states required to decode the Application layer signaling.

Network Layer signaling is therefore the adequate mean to signal a network. Signaling at this level is mostly directed at routers, and the QoS information transport is all of it understandable by routers that can directly map this information into their QoS Mechanisms.

Nonetheless these two approaches are not mutually exclusive. Hybrid versions can be devised through signaling proxies that support both mechanisms, which enable Application Layer signaling translation into Network Layer signaling. Through the use of signaling proxies the two approaches can be bridged at the cost of some added level of complexity associated with any translation mechanism. Network operators must also develop specific proxies for each and every application they intend to support. This constitutes the major inhibitor of such approaches.

3.3 Provisioning Mechanisms

3.3.1 IntServ

Provisioning QoS over a network is a problem that requires the development of an end-to-end solution. The most stringent solution is to explicitly reserve resources in each of the nodes in a network path. IntServ was developed in IETF with this philosophy in mind. IntServ is defined in [RFC 1633], and is based in two basic principles. The first is that network resources should be explicitly signaled by applications taking into consideration their specific needs. The second, is that independent data flows may not interfere with each other. What this means is that the users/applications sitting in the end-points of the network have a great degree of control over what happens in the network, and that the network can/must provide very strict control mechanisms in order to serve such requirements. Ultimately this model would mean QoS levels similar to those found in Circuit Switched Networks that could be configured by the network according to user/application requirements.

In order to describe its requirements, the user/application describes its flow using "Flow Specs" and then convenes this information to the network through a Resource ReSerVation Protocol, named "RSVP" [RFC 2205].

Flow Specs characterize a unidirectional stream of packets flowing from a defined source to a defined destination. A Flow Spec is composed by a TSPEC and an RSPEC. The TSPEC describes the flow that is going to be sent while the RSPEC describes the requirements of this same flow.

TSPEC consists of token-bucket algorithm parameters such as token rate, token size, bucket size, etc (Annex A.2 details the operation of RSVP) while the RSPEC defines how the network must treat the flow.

There are three Classes of Services (CoS) defined:

1. Best-Effort (BE)
2. Controlled Load Service (CL)
3. Guaranteed service (GS)

Best-Effort assumes that the flow requires no special treatment by the network. Controlled Load expects a slightly higher level of quality, with a constant rate of delay and packet loss just as if the network was lightly loaded (Load). Guaranteed Service requires that the network provides absolute guarantees of QoS for the specified TSPEC, with no packet loss and a delay lower than the one defined.

By definition, the GS and CL Class of Services are applied in each node in the path of the communication, which means that every router in the flow's path must support IntServ. The router is therefore able to process RSVP signaling, interpret the Flow Spec and maintain a state machine for each flow that might traverse it. This aspect poses the largest impediment to the deployment of RSVP in the Internet.

The scalability of IntServ in a large network is then very low, due to the requirements it puts into all network elements especially those located in the core, traversed by thousands of flows. Nonetheless the IntServ architecture represents a step forward towards achieving QoS in packet switched networks and can be efficiently used in LAN's in order to provide QoS for sensitive services such as VoIP.

3.3.2 DiffServ

The DiffServ architecture [RFC 2475], also developed by IETF, constitutes an alternative to the IntServ architecture, aiming to solve scalability issues.

DiffServ aggregation of flows under a limited number of types of service, and a simplification of the classification method in each of the core nodes makes it a scalable architecture, capable of delivering QoS to a large user base.

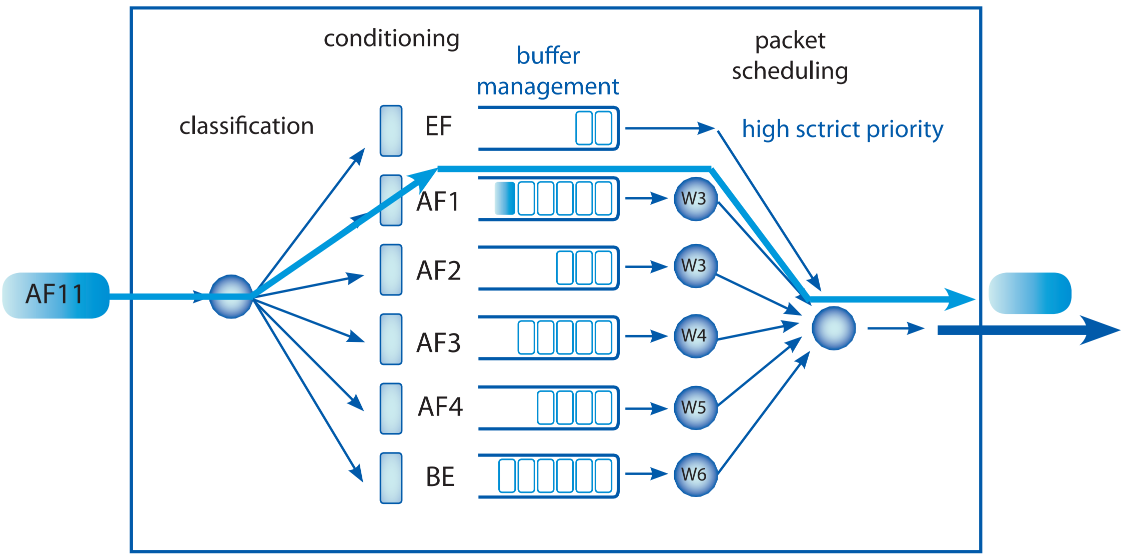


Figure 10 - DiffServ Router Model

The DiffServ model consists on the classification and conditioning of all traffic that enters the network and their differentiated treatment by the core nodes according to different behavior aggregates (Figure 10). A behavior aggregate is the group of all packets that share the same DiffServ Code Point (DSCP) and that flow through the same link in a particular direction. The concept gives DiffServ a characteristic similar to IntServ, in the sense that QoS is a unidirectional property.

The limited number of Services that can be identified through a DSCP is theoretically 64 (DSCP is represented by 6bits), although only 32 are used and the remaining 32 are reserved for tests and local usage. Services are identified through the DSCP present in all packets flowing through the network. The DSCP is made out of 6 bits in the ToS field of the IPv4 header or of the CoS field of the IPv6 header.

In DiffServ, packets sharing the same DSCP are aggregated and treated equally in each router, using the same QoS policy and flows are therefore indistinct. The processing of packets is done per aggregate, based on the definitions of each aggregate; this is called per-hop-behavior (PHB). PHB's are specified by the variables that characterize their buffers and bandwidths, by the relative priorities amongst PHB and by observable variables such as delay and packet loss.

Besides Best Effort, DiffServ defines two PHB's: Expedited Forwarding [RFC 3246] and Assured Forwarding [RFC 2597].

In the DiffServ architecture, PHB's are not globally defined. Each operator can have it's own PHB's and mapping functions of DSCP's into those PHB's. Therefore PHB's must be configured/programmed by each operator to be the same across domain's. A group of nodes that are DiffServ enabled and implement the same PHB's is called a DiffServ domain. A group of DiffServ Domains that cooperate with each other is called a DiffServ region. Since DiffServ domains belonging to the same DiffServ region might implement different PHB's, it is necessary to condition packets between DiffServ domains. To the behavior experienced by a particular set of packets as they cross a DiffServ Domain it is called Per-Domain-Behavior (PDB).

Packet classification in DiffServ can be done based on various fields of a packet. This classification usually takes place in the edges of a DiffServ domain and involves packet marking with an appropriate DSCP. By marking packets in the edges, packet classification in the core can be done solely based in the DSCP, reducing the resources necessary to process the packet. This is the case of all interior nodes of the DiffServ domain, providing the scalability characteristics of DiffServ.

As a major difference between DiffServ and IntServ architectures, DiffServ does not have an explicit signaling protocol. All signaling is done inline through the use of the DSCP field in the packets and by a top-level management system that distributes the policies and rules necessary for the proper classification of packets inside the DiffServ Domain.

This top-level management system should follow [RFC 2638], and uses the concept of a Bandwidth Broker. The Bandwidth Broker is a top-level entity, aware of the network topology and resources. In Figure 8, the QoS Broker's are an evolution of this Bandwidth Broker concept. It can allocate resources and enforce PDB over its domain by pushing appropriate policies/rules into the nodes under its control. One of its main mechanisms is the admission control of new flows. By controlling which flows get admitted into the DiffServ Domain, the Bandwidth Broker can avoid interference and QoS degradation of the flows already in the domain. The admission control takes place in the edge routers of the domain, which through a policy signaling protocol such as COPS or DIAMETER require authorization of the flow to the Bandwidth Broker.

The Bandwidth Broker also plays an important role in Inter-domain traffic exchange. As previously mentioned, a PDB is limited to its domain. Since flows often cross several domains, there is the need for communication amongst domains, much similar to the IntServ architecture communication requirements amongst nodes. The Bandwidth Broker can play the role of domain policy aggregator and negotiate with other Bandwidth Brokers Service Level Agreements (SLA's) [Terzis 1999].

In this context, an SLA represents therefore the agreement between two DiffServ domains on what the PDB of a determined class should be, where the class is identified by the DSCP present in its packets.

3.4 Network Technologies role in the Network QoS

Technology and environment play a very important role on QoS assurances. The technology limitations in terms of assigned capacity, regulations and business plans can constrain the Services being provided. Environment noise and interference, media access control and reliability of links also influence to a great degree QoS.

Environment therefore plays a key role in the provisioning of QoS and must be taken into consideration whenever QoS mechanisms are being discussed, as these need to adapt to the environment. Wired, Wireless and Broadcast networks are hereafter described taking into consideration their resilience to environment interference and capabilities to deploy services with high quality, namely through lower layer's mechanisms.

3.4.1 Wired Networks

A wired network is characterized by the use of a solid medium through which data is transmitted. This medium is in many cases copper, such as in the case of DSL and Ethernet, but can also be plastics or glass, as in SDH. The solid medium is stable (in terms of propagation characteristics) and collision detection is relatively easy to achieve and recover from. These last aspects are of major importance to provide reliable QoS since QoS architectures (as seen in the previous section) rely on the predictability of the network.

Another important aspect of wired network is their incapacity to support mobility. Terminals are attached to a specific point in the network and cannot displace themselves without interrupting communications. This is usually seen as a major drawback of wired networks, but from the QoS point of view, it can be seen as an advantage, as it again makes the network predictable.

Control over the properties of the medium leads to optimizations that ultimately result in larger capacities and/or higher reliability.

All those aspects usually mean wired networks are cheap, and thus resources become mostly over provisioned, with network planning teams able to predict saturation points well in advance.

However, not all wired network technologies are alike. Ethernet (probably the most popular wired network technology) has a shared medium that greatly influences its capacity. A brief description of the basic properties of some wired technologies is given next.

3.4.1.1 Ethernet

In Ethernet early history, the technology relied in a shared coaxial cable that acted as a broadcast transmission medium, in which all equipments attached to the network relied in the CDMA/CD algorithm to share such medium. Today's Ethernet implementation has evolved into point-to-point links connected together by hubs and/or switches in order to increase reliability, and enable point-to-point management and troubleshooting.

Above the physical layer, Ethernet stations communicate by sending each other data packets formatted using the IEEE 802.3 standard [IEEE 802.3]. As with other IEEE 802 LANs, each Ethernet station is given a single 48-bit MAC address that acts as a station identifier, which is used both to specify the destination and the source of each data packet. The identifier enables cards to filter out only the packets addressed to the station. This principle was never designed to address privacy issues but to spare the CPU from processing unaddressed packets. Most of today's Ethernet implementations have a promiscuous mode that enables the delivery of all packets to the CPU.

With popular capacities of 100Mbps and in some cases 1Gbps Ethernet is mostly used in LAN environments where QoS is achieved by over provisioning.

The introduction of the 802.1p [IEEE 802.1p] standard specifies a layer 2 mechanism to give prioritized data a preferential treatment over non-critical data. This is achieved by tagging packets using an IEEE 802.1Q [IEEE 802.1q] extra field (TCI). The tags are used to discriminate packets between the multiple queues within the network elements.

3.4.1.2 ATM

ATM is a connection-oriented, fixed-size cell switching technology that has a large installed base in operation around the world, due to its traffic flexibility and ability to provide quality of service (QoS) [DePrycker 1993].

ATM encodes data into small fixed-size cells (53 bytes; 48 bytes of data and 5 bytes of header information). The use of cells enables the reduction of jitter (delay variance, in this case) in the multiplexing of data streams. Such reduction (as well as low end-to-end round-trip delays) is particularly important when carrying time sensitive information, such as multimedia traffic.

ATM is a channel-based transport layer, using Virtual circuits (VCs). This is included in the concept of the Virtual Paths (VP) and Virtual Channels. VP's and VCs are realized by using a Virtual Path Identifier / Virtual Channel Identifier pair (VPI/VPC) in the header of each cell. This mechanism enables the circuit switch similar behavior of ATM.

Another key ATM concept is that of the traffic contract. When an ATM circuit is set up each switch is informed of the traffic class of the connection: the profile contract.

ATM traffic contracts are part of the mechanism by which "Quality of Service" (QoS) is ensured. There are four basic types (and several variants) each with a set of parameters describing the connection.

- CBR - Constant bit rate: characterized by a Peak Cell Rate (PCR), constant during all time.
- VBR - Variable bit rate: characterized by an average cell rate, which can peak at a certain level for a maximum interval before being considered non-conformant. VBR has real-time and non-real-time variants, and is used for traffic with burst characteristics.
- ABR - Available bit rate: a minimum guaranteed rate is provided.
- UBR - Unspecified bit rate: traffic is assigned all remaining transmission capacity.

Most traffic classes also introduce the concept of Cell Delay Variation Tolerance (CDVT), which defines the clumping of cells in time.

Traffic contracts are usually maintained by the use of shaping, a combination of queuing and marking of cells, and enforced by policing.

3.4.1.3 CATV / DOCSIS

The Data-Over-Cable Service Interface Specification (DOCSIS) [ITU-T J.112B] is a technology standard created by CableLabs to deliver high-speed data over the hybrid fiber-coax (HFC) cable network that constitutes most Cable Operators network deployments. Since the initial intention of such networks was to provide a one-way transmission medium for a TV service the spectrum allocation is very asymmetric (upstream/downstream ratio is set depending on the operator around 1:4 to 1:8). In its 2.0 release DOCSIS [ITU-T J.122] improves the initial TDMA mechanism with a second operation mode using SCDMA (Synchronous Code Division Multiple Access) mechanism.

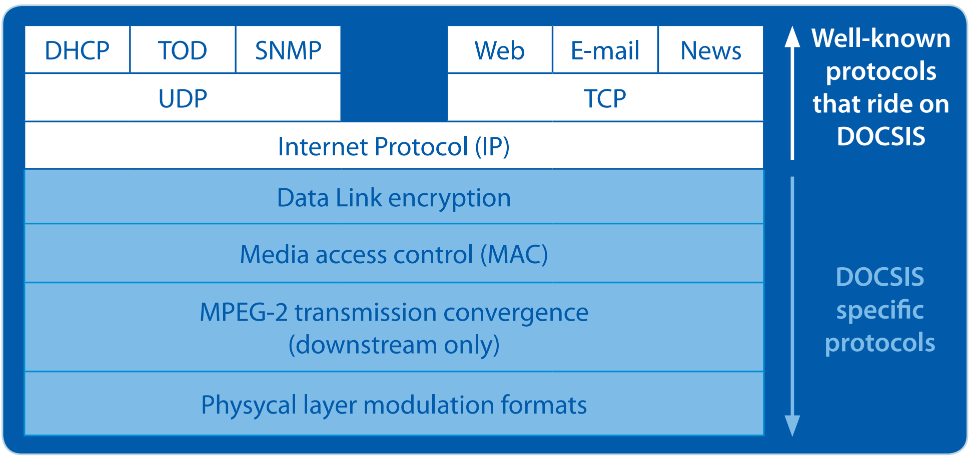


Figure 11 - DOCSIS Cable Modem protocol stack

As seen in Figure 11, DOCSIS has below the IP protocol 3 different layers besides the Physical layer. CATV is oriented to the transmission of Multimedia Services and therefore has adopted MPEG-2 to deliver information in the downstream. MPEG-2 is used as a transmission convergence protocol to allow multiple types of services to share the same RF carries. Although the TV service is deployed immediately on top of MPEG-2, a MAC is necessary to provide the means for the Cable Modem Termination System (CMTS) to control the access by the Cable Modems (CM) to medium. On top the MAC layer the Data Link Encryption layer provides the

CM user with data privacy across the RF network. QoS is provided only between the CMTS and the CM achieved through packet classification and the dynamically creation of service flows that will have distinct priorities.

3.4.2 Wireless Networks

Wireless networks differ fundamentally from wired networks due to the medium properties. The medium used (Radio) is of difficult characterization, as it can depend of several factors such as natural environment properties (chemical composition, temperature, pressure), electromagnetic interference from equipments, reflections and attenuations caused by obstacles and spectrum usage (limitations imposed by regulatory bodies).

Wireless Networks thus pose several added challenges when compared to wired technologies. As a signal propagates through a wireless channel, it experiences random fluctuations in time if the transmitter, receiver, or surrounding objects are moving because of changing reflections and attenuation. Hence the characteristics of the channel appear to change randomly with time, which makes it difficult to design reliable and predictable systems.

Since the airwaves are susceptible to snooping by anyone with an RF antenna, security is a major concern. Modern cellular systems implement some level of encryption. However, with enough knowledge, time, and determination, most of these encryption methods can be broken.

Since terminals are not physically attached to the network they can move around. The network must be able to locate a given user among billions of distributed mobile terminals, and route packets as the terminal moves at speeds of up (in some technologies) to 240km/h.

The shared nature of the medium used requires the supervision of regulators that further limit the access to the medium through regulatory licenses that in some cases are sold at very high-prices (as seen in Europe during the auctions of 3G licenses). This artificial limitation further restricts the amount of resources that can be used by a network operator, constitutes a challenge to operators that must use their spectrum licenses in the most efficient way. The optimization of resources for multicast services is here an important factor.

With so many dynamic factors involved, network management must still be able to allocate in a fair and efficient manner resources to all its users. With so many restrictions and limitations, Wireless Networks cannot spare enough resources to provide QoS through over provisioning of its networks.

Different wireless technologies try to solve this issue from different perspectives.

3.4.2.1 WiFi (802.11)

WiFi is the trademark associated with the implementation of the IEEE 802.11 standard [IEEE 802.11] and its various versions (of which a/b/g/n are the most well known). WiFi networks operate in the unlicensed 2.4GHz (802.11b/g) and 5 GHz (802.11a/h) radio bands, with an 11 Mbit/s (802.11b) or 54 Mbit/s (802.11a or g) maximum data rates.

Since WiFi transmits over the air, it has the same properties as a non-switched wired Ethernet network, and therefore collisions can occur. Unlike a wired Ethernet, and like most packet radios, WiFi cannot do proper collision avoidance and collision detection. The basic 802.11 MAC layer uses the Distributed Coordination Function (DCF) to share the medium between multiple stations. DCF relies on CSMA/CA and optional 802.11 RTS/CTS to share the medium between stations.

The original 802.11 MAC defines another coordination function called the Point Coordination Function (PCF). PCF is available only in “infrastructure” mode, where stations are connected to the network through an Access Point (AP). APs send “beacon” frames at regular intervals (usually every 0.1 second). Between these beacon frames, PCF defines two periods: the Contention Free Period (CFP) and the Contention Period (CP). In CP, the DCF is simply used. In CFP, the AP sends Contention Free-Poll (CF-Poll) packets to each station, one at a time, to give them the right to send a packet. The AP is the coordinator. This allows for a better management of the QoS. Unfortunately, the PCF has limited support and a number of limitations (for example, it does not define classes of traffic).

The IEEE 802.11e standard [IEEE 802.11e] enhances the DCF and the PCF, through a new coordination function: the Hybrid Coordination Function (HCF). Within the HCF, there are two methods of channel access, similar to those defined in the legacy 802.11 MAC: HCF Controlled Channel Access (HCCA) and Enhanced Distributed Channel Access (EDCA). Both EDCA and HCCA define Traffic Classes (TC). For example, FTP could be assigned to a low priority class, and Voice over IP (VoIP) could be assigned to a high priority class.

3.4.2.2 WiMAX (802.16)

One of the wireless technologies currently receiving more attention by the industry is WiMAX. WiMAX is the trademark created with IEEE 802.16 technology [IEEE 802.16], which intends to provide broadband wireless to large service areas (ranging 50km). Its main features include: Non Line of Sight, QoS designed in for voice/video, differentiated services, very high spectrum utilization (3.8 bit/Hz), up to 280Mbps per base station and true broadband for portable users (based on IEEE 802.16e). These characteristics make WiMAX a very interesting technology to deploy next generation networks on top of.

IEEE 802.16-2004 specifies a Medium Access Control (MAC) layer and several Physical (PHY) layers. Each PHY layer addresses a specific frequency band, providing a very flexible standard. Flexibility means that this technology can operate in LoS (Line of Sight) and NLoS (Non Line of Sight) and under both conditions in which the multipath effect can be negligible or must be carefully analyzed. The MAC layer is connection oriented and provides Quality of Service (QoS) assurances through the usage of service flows and uplink scheduling services. A set of convergence sub layers is defined to map the upper layer packets into the 802.16-2004 systems. The convergence sub layers support packet based protocols, such as IPv4 and IPv6, as well as cell-based protocols, such as ATM. Both point-to-multipoint (PTM) and mesh modes of operation are supported by the standard, although the mesh mode of operation is considered optional.

WiMaX has noticeable features: it is a connection oriented wireless technology and supports both unicast and broadcast connections. Unfortunately commercial implementations have limited the broadcast channels capability to a single 64kbps channel.

3.4.2.3 3G/UMTS

UMTS (Universal Mobile Telecommunications System) is the most prominent incarnation of the 3rd generation of mobile phones being Release 5 probably the most widely deployed (considering the commercial offerings of operators worldwide). Being an almost global network, it must cope with several environment factors, and therefore 3GPP defined several mechanisms that overcome such interferences and limitations.

UMTS supports two basic modes of duplex, frequency division and time division (as discusses in section 2.1.2) and employs coherent detection on uplink and downlink based on the use of pilot symbols.

It further supports inter-cell asynchronous operation and adaptive power control based on SIR (Signal-to-Interference Ratio).

Terminals with HSPA (High-Speed Packet Access) capabilities support data rates of up to 14.0 Mbit/s in the downlink and up to 5.8 Mbit/s in the uplink.

Further details on 3G/UMTS architecture and features can be found in Section 2.1.2.

In order to realize data transport with different QoS attributes, the UMTS architecture defines the concept of bearers [3GPP TS 23.107]. A bearer is an information transmission path with defined QoS attributes such as capacity, delay, bit error rate, etc. A bearer service includes all aspects that enable the transmission of signals at a required QoS between two communication endpoints, such as control signaling, user plane transport and QoS management functionality. Bearer services are provided at different layers and include, but are not limited to the Physical Radio Bearer, Radio Bearer, Radio Access Bearer, RAN Access Bearer, Backbone Bearer, Core Bearer and End-to-end Bearer.

3.4.3 Broadcast Networks

In the scope of this thesis, Broadcast Networks are given an increased relevance. Broadcast Networks are here not defined by the transport medium (Wired vs Wireless), as they can operate over wired and wireless networks alike. The main defining property is that in broadcast networks communication is always group wise, that is, information is not exchanged bidirectionally between two parties but unidirectionally to a group of two or more parties that will have no means of replying back to the sender using the same broadcast mechanism. In addition the information is usually transmitted by a single element of the group, which acts as the source or proxy of information. The main characteristic of a broadcast network is therefore its main limitation: communication is performed unidirectonally in a single direction, from the source to the listeners. In broadcast networks, the listener's equipments hardware is usually limited to reception mode (making them unable to transmit) and only the source can access the medium. This nuance completely avoids collisions and limits interference, providing broadcast networks with increased QoS characteristics. This advantage nevertheless limits the services that can be provided in such networks. Without the ability to reply, listeners are limited to what they receive, and act passively in the communication. Services are therefore limited to the ones where no interaction is required such as TV/Radio and Digital subscription data services using out of band mechanism such as smart cards and narrow-band signaling channels (e.g. GSM, PSTN).

3.4.3.1 DVB

The Digital Video Broadcast (DVB) standard was designed to broadcast digital TV services and has been maintained by the DVB project since 1993 [DVB]. The standard specified by the DVB consortium is used in many countries for the transmission of digital television. IP datacasting [ETSI EN 301 192] is a new technology to broadcast IP based services over the DVB network. The main design goal for IP datacasting is to use the DVB platform to deliver IP based audio, video, data and other broadband information directly to the end user.

There are many digital video broadcasting standards available for this purpose:

- DVB-S [ETSI EN 300 421] for satellite transmissions.
- DVB-C [ETSI EN 300 429] for cable transmission
- DVB-T [ETSI EN 300 744] for terrestrial transmission; it is a worldwide accepted standard designed to deliver HDTV for fixed reception.
- DVB-H [ETSI EN 302 304] for handheld terminals; it is a new standard developed to support the DVB-T for mobile reception.

DVB-S is mostly deployed as unidirectional and the downlink data bandwidth can reach 55Mbps. DVB-C is considered a special case since through the use of the DOCSIS technology on top of DVB-C, bidirectional services can be provided at speeds of up to 300Mbps (using the latest DOCSIS standard). Both DVB-T and DVB-H system are unidirectional and offer a fast and fairly reliable transmission medium, data bandwidth can be up to 24 Mbps for fixed reception and 12 Mbps for mobile reception. There are nonetheless standards such as DVB-RCS and DVB-RCT that provide a very narrow band uplink channels using complementary channels. The return (uplink) channel is usually a point-to-point bidirectional link provided by a different technology such as UMTS or GPRS. Aggregation between downlink and uplink is done at the application level. These technologies are nonetheless very expensive and not widely deployed.

The content, retrieved from any web site, database or other data source, is passed to the service delivery layer. The content adaptation servers in the DVB service delivery layer can be used to aggregate and if necessary to modify and re-purpose content before pushing it to the end-user. From the service delivery layer, data is sent to the IP Encapsulator. The data is encapsulated using Multi-Protocol Encapsulation (MPE), the standard for transporting Internet traffic over broadcast network [ETSI EN 301 192]. The output of MPE is a transport stream, typically in DVB-ASI (Digital Video Broadcasting and Asynchronous Serial Interface) format.

3.4.3.2 3GPP/MBMS

3GPP/MBMS was standardized in Release 6 as a broadcast service that can be offered using the existing UMTS cellular networks [3GPP TS 22.146]. By defining a broadcast service, 3GPP intended to exploit important service scenarios, such as Mobile TV, more efficiently than the initial services deployed using unicast channels.

The radio link between base station and mobile terminal is the most expensive resource in a cellular network and resources are assigned very carefully in that interface. Due to the service-oriented nature of 3GPP, services (which are shared among a large number of user equipments) can make use of common radio resources. Therefore a scenario came up to deploy broadcast alike services over the UMTS networks through the establishment of point-to-multipoint (p-t-m) bearers, using as an example the Forward Access Channel (FACH) [3GPP TS 25.346].

Unfortunately exploiting the shared nature of the radio signal can mean not only the usage of fewer channels, but also a less efficient power control.

In UMTS dedicated channels (DCH) are always bi-directional even if the applications on top and the transport protocol they use generates unidirectional traffic only. The uplink direction is used mainly for fast power control schemes, which results in a nearly constant received signal to interference ratio and block error rate. Ultimately this results in that the transmitter power consumption is optimized to a bare minimum [Alexiou 2007].

If a similar fast power control mechanism were to be used for p-t-m bearers the uplink control load would increase with the number of receivers and could easily exceed the amount of downlink traffic.

As a consequence, the transmit power cannot be controlled as efficiently as on dedicated channels and MBMS is quite inefficient when only a small number of users are using MBMS based services. Furthermore, the bi-directional control channel is still kept, as it is required for normal terminal operation.

The main characteristic of MBMS is therefore this duality between a unidirectional-based technology and the omnipresence of bi-directional channel on the same interface, both under the same service layer.

3.5 Group Based Communication

3.5.1 IP Multicast

With IP becoming a central technology for heterogeneous network integration, it is natural for IP multicast to be seen as the corner stone for reliably providing shared data to several end terminals scattered around different networks. In its essence, IP multicast enables a source to transmit to several destinations using a single communication stream. The network has then the responsibility to duplicate the stream in the necessary network elements (routers) along the path, to reach the multiple end-users. It is also a task of the network to manage end-user changes, in terms of interest and mobility, and optimize the (variable) routes taken by the stream to reach all the end-users.

IP multicast presents obvious bandwidth advantages, since it requires fewer resources to support a large number of users, both from the point of view of the network and of the servers. Network operators can make use of IP multicast to optimize its network resources. Nonetheless, multicast is not as widespread as it would seem obvious in today's multimedia centric networks. Since many installed IP routers need to be upgraded to support IP multicast, given the low costs of upgrading physical networks to new and more resource abundant technologies, and the (until now) few services able to exploit multicast, operators have steadily invested in improving their bandwidth, and not in optimizing their resources. IP multicast was then kept out of the commercial mainstream, although much development and maturing occurred in these years such as the development of more efficient mechanisms (e.g. Source Specific Multicast and its early integration in the standardization of IPv6).

This reality is however changing. It is interesting to notice that BBC & ITV have used IP multicast inside the UK, and that new triple play offerings from companies such as *Portugal Telecom Comunicações* are commercially using IP multicast.

3.5.1.1 IPv4 vs. IPv6

The development of IPv6 has rekindled the interest in IP multicast. IPv6 was developed from the start taking into consideration IP multicast, creating a solid base for the tight deployment of IPv6 and IP multicast. IPv6 multicast is supported by several fields and protocols: a 128 bits group address space, a scope identifier for domain control of the multicast group, a protocol-independent routing protocol, designated by Protocol Independent Multicast (PIM), and group membership mechanisms, designated by MLD (Multicast Listener Discovery) [RFC 3810], which aims to enable hosts to communicate the multicast group they wish to subscribe.

IPv6 multicast is then mature enough to be used as a mechanism to efficiently deliver contents to end-users, while sparing resources in the operator networks and reducing load on the content provider's servers. These added values of IPv6 multicast are the reasons that made interesting its usage inside the 3GPP MBMS sub-system.

Multicast routing uses PIM, and its variants Any Source Multicast (ASM) [RFC 1112], Sparse Mode (SM) [RFC 2362] and Source Specific Multicast (SSM) [RFC 3569] to construct the multicast tree used to forward the multicast packets from the source to the terminals.

IP Multicast has two basic working models: many-to-many and one-to-many. The many-to-many model was first described in [RFC 1112], and refers to applications such as: Teleconferencing where participants are fully connected (every one receives everyone else's data): Database (All copies of replicated file or database are updated at the same time); Distributed Computing (intermediate results are sent to all participants) and ad-hoc service discovery [IETF ZEROCONF]. This model applies mostly to LAN environments where scalability is not a big concern and resources are usually abundant. As for the one-to-many model, its main application is multimedia streaming such as Digital Video (TV alike service) and Software distribution (software is copied on the wire to several end-users). Opposite to the previous model, the one-to-many model can scale over large networks and makes an efficient use of resources.

Another aspect that can influence these models is the amount of candidate listeners. The multicast environment can be either Dense or Sparse, according to the number of candidate listeners. In a Dense environment, it is assumed that everyone would like to receive the multicast flow and any one uninterested must therefore reject the flow. In the Sparse environment, on the other hand, the flow is sent only to the local link and interested parties must search for the flow through a signaling mechanism with upstream nodes. This signaling mechanism has been standardized as PIM or Protocol Independent Multicast and its several versions DM (Dense Mode), SM (Sparse Mode) and SSM (Source Specific Mode). PIM is "Independent" because it does not have a topology discovery mechanism and therefore uses routing information supplied by other routing protocols such as OSPF [RFC 2328] and BGP [RFC 1771]. A brief description of each version and associated concepts is presented next.

3.5.1.2 ASM

ASM or Any-source-multicast [RFC 1112] refers to the operation mode under which any of the group members might participate by sending its own packets to the group. It is the basic concept of multicast where operation is sometimes confused with broadcast but limited to a subset. PIM supports two ASM mechanisms, Dense Mode (DM) and Sparse Mode (SM) being the last the most popular implementation due to its scalability.

3.5.1.2.1 PIM-DM

Dense mode is ideal for groups where many of the users want to receive the multicast stream, meaning that most of the routers must receive and forward these packets (groups of high density).

This scenario mostly holds true in LAN environments where group communication occurs.

PIM Dense Mode [RFC 3973] operates in such environments using a flood algorithm where all nodes are added to the multicast delivery tree. Only afterwards, are nodes not wishing to receive traffic pruned accordingly from the multicast tree. The source initially broadcasts to every router, and thus every node. Then each node that does not wish to receive packets destined for that group will send a prune message to its router. Upon receiving a prune message, the router will modify its state so that it will not forward those packets out that interface. If every interface on a router is pruned, the router will also be pruned.

Additionally, the routers will use reverse-path forwarding to ensure that there are no loops for packet forwarding among routers that wish to receive multicast packets.

In Dense Mode it is very easy to operate the many-to-many model due to the flooding algorithm used for distribution. Dense Mode weakness also comes from the flooding algorithm as each branch is tested periodically for subscription interest.

3.5.1.2.2 PIM-SM

The most commonly implemented form of PIM is Sparse Mode (PIM-SM) [RFC 4601]. As previously mentioned Sparse Mode is quite scalable and therefore well suited for large networks since it reduces the overhead and bandwidth requirements for multicast data streams.

PIM-SM is a protocol that exists exclusively between routers. Hosts (sources or receivers) do not participate in the protocol. PIM-SM shares many of the common characteristics of a routing protocol, such as discovery messages, topology information, and error detection and notification. PIM-SM also differs from traditional protocols since it does not participate in any kind of exchange/propagation of information (tree information is not propagated to all involved nodes and is only local).

PIM-SM routers periodically generate “Hello” messages to discover and maintain state full sessions with neighbors. After neighbors are discovered, PIM-SM routers can signal their intentions to join specific multicast groups. This is accomplished by having a downstream router send an explicit PIM-SM “join” message (not to be confused with IGMP or MLD “join” messages) to the upstream router. The “join” message will specify the group and the source (if applicable) that the router wants to join – this can be represented by (*,G) or (S,G) to subscribe to any source (*) of group G or to source S of group G. The upstream routers can then forward multicast information to the downstream devices. This behavior is diametrically opposite of that of PIM-DM, which will forward data to all routers until told to stop.

PIM-SM, like most other multicast routing protocols, implements forwarding trees for each multicast group. These trees are called Rendezvous Point Trees (RPT) since they rely on a central router called a rendezvous point (RP). Leaf routers that detect multicast listeners via IGMP or MLD generate PIM join messages and send them to the upstream router according to the unicast routing entry that route towards the RP. Multicast sources forward their packets to the RP, which then places them on the shared tree for distribution. After a short period of time, optimized shortest path trees can replace these rendezvous point trees.

3.5.1.3 PIM-SSM

Source Specific Multicast is an evolution of Multicast that tries to fit the requirements of the industry and solve the problems of ASM. Most of the services commercially deployed using multicast are based on a content distribution scenario where a single source provides content to many subscribers (one-to-many). In this scenario, the multicast source is well identified by all subscribers and there is no need for an intermediate node or distribution tree. PIM-SSM [RFC 3569] relates directly to the one-to-many model thus simplifying much of its operation. In PIM-SSM sources are well identified and distribution trees are therefore more efficient and reliable.

PIM-SSM is simpler than PIM-SM because only the one-to-many model is supported. This model fits well content distribution scenarios where large numbers of consumers rely on a single source for content provisioning. This combination of source unicast and group multicast addresses (S, G) identifies a channel in the SSM model. The SSM model thus easily supports broadcast media applications.

PIM-SSM is therefore a subset of PIM-SM. PIM-SSM builds shortest path trees (SPT) rooted at the source immediately because in SSM, the router closest to the interested receiver host is informed of the unicast IP address of the source for the multicast traffic. That is, PIM-SSM bypasses the RP connection stage through shared distribution trees, as in PIM-SM, and goes directly to a source-based distribution tree.

3.5.2 QoS Enabled Multicast

Much work has been done in order to provide IP multicast services with QoS [Striegel 2002]. The work in this area is mostly centered on the creation and management of QoS aware multicast trees [Shuqian 2002]. The integration of the IP Multicast into existing QoS Architectures, such as IntServ and DiffServ, has also been the subject of much research [Cui 2006]. Proposals usually address extensions to existing multicast routing protocols [Bin Wang 2000] that try to create the same QoS constrains found in IP unicast in IP multicast such as admission control and link reservation.

The research in QoS Enabled Multicast has nonetheless been done following a horizontal view, in which most the approaches made to the problem have been made only at the IP level. Approaches that address the global problem of delivering group communication services, instead of focusing solely at the IP level, have the opportunity to address cross layer aspects that might have an impact in the QoS of group communication services deployed over IP Multicast.

3.5.3 3GPP MBMS

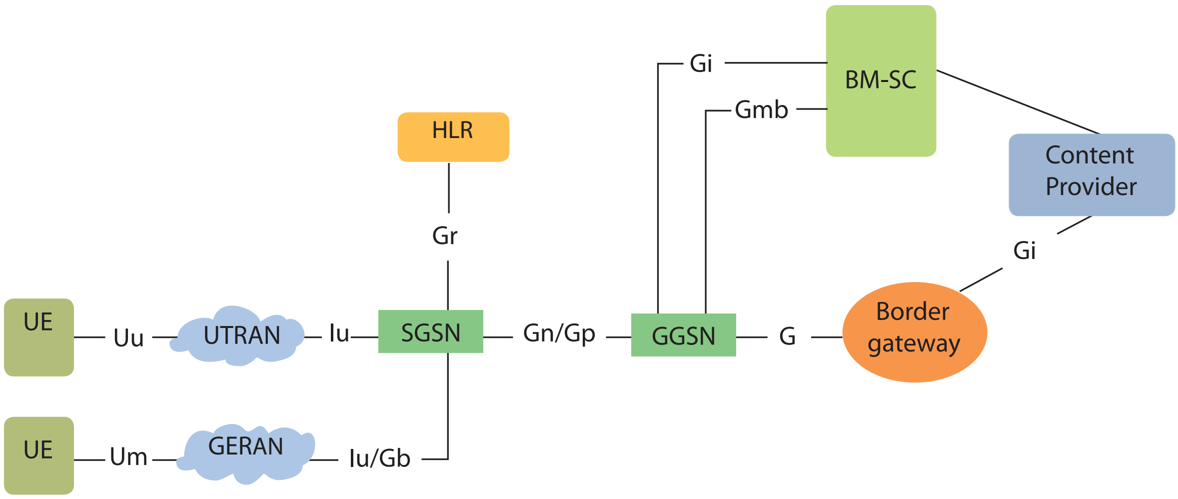


Figure 12 - MBMS Architecture

As stated in the previous section, the Multimedia Broadcast/Multicast Service (MBMS) was initially specified in 3GPP Release 6 (see section 2.1.2). It is a point-to-multipoint service in which data is transmitted from a single entity to multiple recipients sharing the same radio resources, thus providing a more efficient use of resources. To support MBMS (see Figure 12), existing packet switched domain functional entities, such as the GPRS Gateway Support Node (GGSN), Serving GPRS Support Node (SGSN), UMTS Terrestrial Radio Access Network (UTRAN), GSM EDGE

Radio Access Network (GERAN), and the User Equipment (UE) were enhanced. Moreover, new functional entities were added such as the Broadcast-Multicast Service Centre (BM-SC).

3.5.3.1 MBMS Architecture

MBMS provides delivery of IP multicast datagram's from the Gi reference point (see Figure 12) to UEs with a specified QoS. On the control plane, it manages the MBMS bearer service activation status of the UEs, handles authorization of broadcast/multicast services, provides control of session initiation/termination by the MBMS user service, and manages bearer resources for the distribution of MBMS data.

IP plays a key point role in MBMS, being used to identify the particular instance of the bearer service (which is composed by an IP multicast address and an access point name - network identifier) and to manage all MBMS multicast services.

The BM-SC is the element in MBMS that bridges the IP layer and the UTRAN domains, interfacing in one side with the IP Content Provider and in the other with the GGSN. As such, it includes functionalities for user service provisioning and delivery, authorization and initiation of MBMS bearer services, charging and service announcements, and can further be used to schedule and deliver MBMS transmissions. As an advanced feature, the BM-SC can re-broadcast previous transmissions. On the service side, the BM-SC provides the UE with information on the MBMS user service, such as the codec's used, the multicast service identification, addressing and timing. In all these processes, the BM-SC uses IP-oriented protocols for multicast, session description and service announcement, and makes all these services transparent to the RAN and MBMS user service.

The GGSN serves as the entry point of IP multicast traffic as MBMS data. Upon notification from the BM-SC, the GGSN is responsible for setting up the required radio resources for the MBMS transmission.

The UTRAN/GERAN is the responsible for efficient delivery of MBMS data to the designated MBMS service area. This includes the function of choosing the appropriate radio bearer based on the number of users within a cell, prior to, and during a MBMS transmission. Mobility aspects are intrinsically supported in UTRAN/GERAN, but additional mobility aspects need to be supported by the SGSN, such as the capability to store a user-specific MBMS context for each activate multicast MBMS bearer service.

The UE also needs to be enhanced to be able to activate and deactivate MBMS bearer services. Furthermore, the UE may include features such as Digital Rights Management (DRM), security features, service announcement processing, service paging, and capabilities to cope with losses in the reception process (such as buffers and caches).

MBMS can operate in two modes: broadcast mode, where all terminals receive the information; and multicast mode, where only the terminals that subscribe to a specific service receive the information. Although they both use the same resources, they differ on the subscription and management process. The next sections further details these two modes.

3.5.3.2 MBMS Broadcast Mode

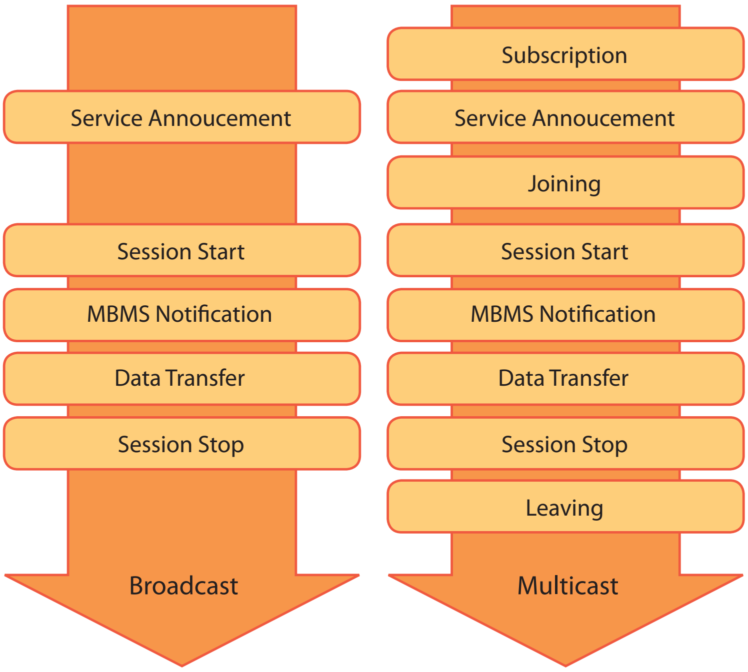


Figure 13 - MBMS Service Setup Phases

Broadcast mode is simpler than multicast, since it does not involve subscriptions management. It is composed by 5 phases (Figure 13): service announcement, session start, MBMS notification, data transfer and session stop.

The service announcement provides the UE with information on available MBMS services, either operator specific or from the outside. The announced information includes parameters required for the service activation such as IP multicast addresses and service start time, and content information.

The BM-SC is then ready to send data. The trigger for bearer resource establishment characterizes the session start phase for MBMS transfer. At this stage, the MBMS notification phase starts, and UEs are informed of forthcoming and ongoing MBMS broadcast data transfers. Finally, UEs are ready to receive data (data transfer). Lastly, after a period of which no data has been sent, the session stop phase releases the bearer resources.

3.5.3.3 MBMS Multicast Mode

Multicast mode is similar to broadcast mode. However, some higher-level mechanisms for subscription management need to be considered. For this purpose, the multicast mode contains 3 more phases: Subscription, Joining and Leaving.

In the subscription phase, the UE must explicitly establish a relationship with the service provider in order to receive the MBMS multicast service: the BM-SC is the responsible for keeping such information. Then, the UE receives service announcements as in the broadcast mode. Based on the received announcements, the UE may initiate the joining phase (typically through MLD messages). Following, the BM-SC starts the session by reserving resources, and informs the UE of forthcoming and ongoing sessions. Finally, the UE receives the desired data. For the session termination, after the session stop phase, a leaving phase is required for the unsubscription of the services.

3.5.3.4 QoS Support

In the MBMS architecture, the network has the ability to control QoS parameters for sessions of multicast and broadcast MBMS bearer services. Furthermore, all QoS attributes related to the UMTS bearer service are applicable to MBMS bearer services, although some differences exist due to the parallel transfer of data to many UEs.

MBMS only supports two traffic classes, the background and the streaming. MBMS bearer services of background class are suited for the transport of messaging or downloading services. Buffering, shaping and packet dropping schemes may be applied to the traffic flow to adapt to the available resources and changing network conditions. MBMS bearer services of streaming class are best suited for the transport of multimedia streaming services, since the network here minimizes the packet transfer delay. When the traffic flow needs to adapt to the available resources, packet dropping is the preferred traffic conditioning action.

A key difference between background and streaming classes in MBMS is the support of a guaranteed bit-rate in the streaming case. Furthermore, the allocation and retention priority of the MBMS bearer service allows for prioritization between MBMS and non-MBMS bearer services.

When considering the whole distribution tree, the same QoS has to be made available for all its branches: it is not possible to have a new branch impacting the QoS of the already established branches (there is no QoS value negotiation between UMTS network elements). This implies that some UEs may not be serviced if their QoS requirements cannot be accepted.

3.5.3.5 MBMS User Services

Besides the delivery mechanism previously described that constitute the MBMS Bearer Service, MBMS also specifies the MBMS User Service [3GPP TS 22.146]. MBMS User Service provides an application independent transport service. Such service can be used by applications to deploy services over the MBMS Bearer Service.

MBMS User Services can be classified into: Streaming services, File download services and Carousel services. A streaming service is constituted by a continuous flow of media. File download enables the reliable delivery of binary data (using FLUTE [IETF RFC 3926]). In addition, Carousel combines aspects of both streaming and file download services to deliver static media.

MBMS User Services feature charging, authentication, privacy, quality of service and subscription mechanisms, which further enrich the application using it.

4. Optimization of Group Communication through Service and Network Optimizations

4.1 Introduction

Group Communication support by today's networks is still regarded as a second tier service in terms of revenue. Since architectures are usually built around the most common scenario (one-to-one communication), less attention is usually given to possible optimizations for group communication in the overall network design. This fact is clear for instance in the 3G's architecture, where the Multimedia Broadcast/Multicast Subsystem was introduced only in a late Release (Release 6) and through decoupled mechanisms (BM-SC is a new entity for the sole purpose of MBMS, replicating unicast functionalities for the special use case of Broadcast/Multicast).

On the other hand, the development of IPv6 was accompanied from the beginning by the introduction of multicast mechanisms into the core of the protocol, in a clear display of the IETF interest for such kind of communication mechanism in future networks.

It is therefore necessary to study and provide a clear evolutionary path for the increased integration of group communication services into current and future networks, which are able to incrementally improve network and service performance and/or resource consumption.

This chapter intends to provide a possible path through which 3G networks can evolve towards Next Generation Heterogeneous Networks supporting optimized group communications. Optimizations will need to be performed at different architectural levels, in accordance with the mechanisms and resources in question at each level.

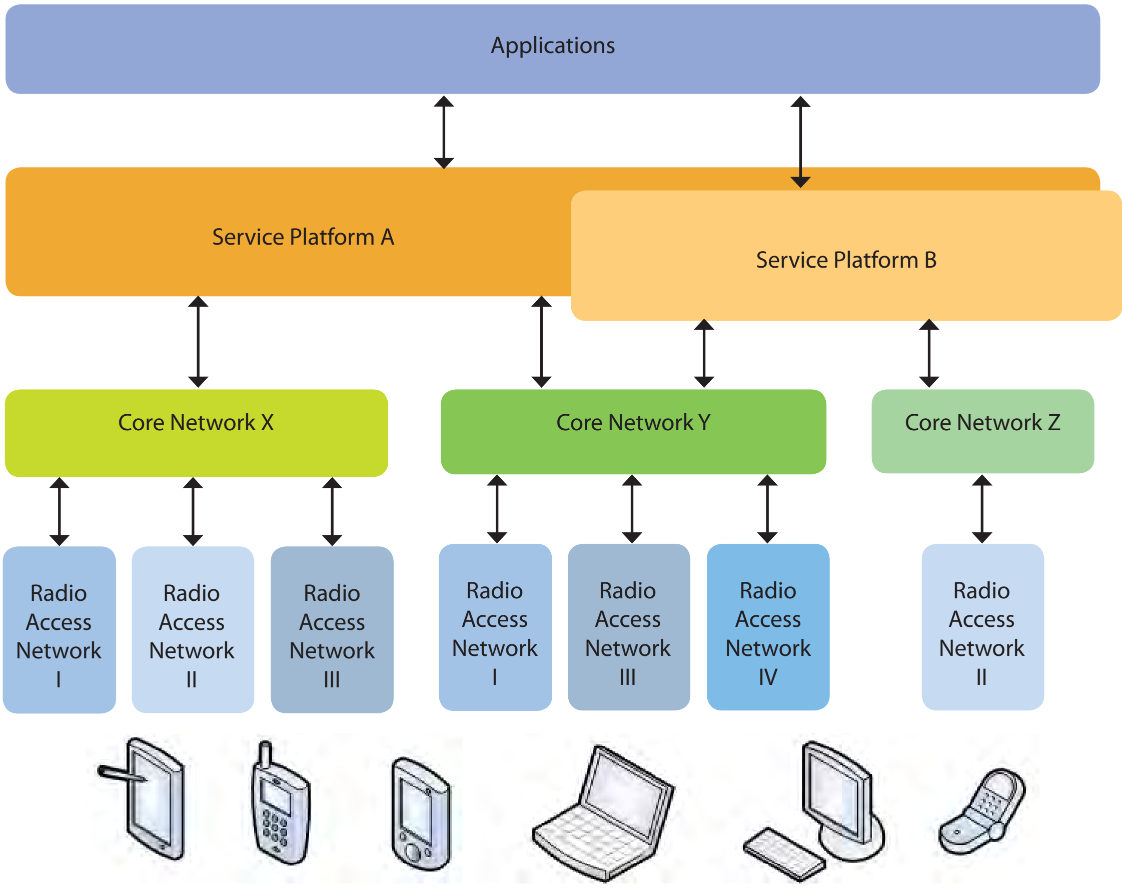


Figure 14 – Layered approach to Group Communication Optimization

Figure 14 provides a generic layered view, depicting the levels and interfaces in which optimizations can be proposed. The reference framework proposed is loosely related to the 3GPP and TISPAN architectures, with the existence of a Service Layer (providing a high-level interface to Applications), followed by a Core Network (based in IP) and the likely existence of more than one Radio Access Network. There is no dependence on specific technologies, since the proposed concepts should be able to be applied to any existing or future technology that can be mapped into one of such layers. In this reference framework, it is acknowledged the possibility of the existence of parallel Service Platforms. The framework caters as well to the existence of Core Networks with a single Radio Access Network that might in some extreme cases be fully coupled with the Core Network (lacking a clear interface between the two).

Another important aspect in this framework are the interfaces. These should be built around open specifications and protocols. Open specifications and protocols are essential to allow component reuse and third-party interaction. These two aspects are important corner stones when building cost-effective innovative services. In addition, the availability of free or open implementations of these specifications is a catalyst for innovation.

Having this reference framework, optimizations for group communication should be proposed at each layer and at each interface. This idea is contrary to existing solutions for group communications, such as MBMS. MBMS was built as a vertically integrated subsystem that provides support for multimedia group communications. This virtual integration of services and Radio Access Network limits the reuse of optimization mechanism deployed by the MBMS at different levels by non-multimedia applications. As an example: as of Release 6, MBMS is limited to a single RAN (UTRAN), limiting the use of the operator to deploy its group communication applications through other technologies such as WiFi. It is therefore necessary to discuss how the current MBMS can evolve towards a NGN system capable of supporting any Application, through any Service Platform and Radio Access Network.

In this chapter, optimizations at the Service and Network Layer shall be proposed in accordance to the expected developments towards Next Generation Networks. 3GPP MBMS will be used as the starting point, and will provide a use case of how proposed optimizations can improve resource usage and group communications. The optimizations considered can be summarized as: improved and optimized support in the service layer for group communication through the creation of new application interfaces; clearer separation of Core Network and Radio Access Network functionalities through the use of Open Standards based interfaces and through a better mapping between IP protocol mode (Unicast/Multicast) and Radio Access Capabilities. The following sections will detail the first two optimizations, while the third optimization will be presented in a separate chapter together with some validation results.

4.2 Optimizing Group Communication Services

The first optimization that shall be considered is focused on the interface between the Application and the Service Platform. The efficient use of resources in the network by group communications is mostly dependent on a correct mapping of application requirements into network services that can be deployed over broadcast/multicast channels in the Core Network and Radio Access Network. In this section 3GPP MBMS will provide a use case example of how this interface is important and can be improved through OMA alike Service Enablers that provide a better abstraction of the network to Applications.

As previously mentioned, 3GPP defined MBMS in order to provide group communications services. MBMS is sub-divided into the Bearer Services and the User Services. The first are in charge of the radio and transport aspects of deploying a Broadcast/Multicast Service while the second are responsible for the aspects regarding service support for the applications deployed on top.

One of the most important features of MBMS is the support for shared channels at bearer level that result in an important saving of radio resources by the operator, from the view point of the User Services. MBMS use of IP Multicast follows the adoptions of open standards from IETF as the path towards convergence with other technologies through the use of IP based protocols.

4.2.1 Limitations and Restrictions

MBMS was devised as a subsystem for Mobile Operators to deploy services such as Mobile TV and Content Casting over their existing networks. Being a late addition to the standard (introduced only in Release 6), its introduction could have disrupted the ongoing work. Therefore MBMS promoted a new separate identity, named BM-SC, which centralizes all MBMS aspects for both Bearer and User Services. This option was a conservative approach, since it minimized changes to the functionality of existing entities that had already been specified in previous releases of the standard. Still, this option had the immediate benefit of operators being able to gradually upgrade their network functionalities with the addition of a single entity. This advantage can unfortunately be also seen as a disadvantage, if one considers the fact that being an independent subsystem, MBMS is competing with other independent platforms such as DVB-H [ETSI EN 302 304] and MediaFLO [MEDIAFLO] for its place in the mobile operator network infrastructure. Competition from these other standards is possibly mostly due to the lack of full integration of MBMS with the remaining 3G infrastructure. Non withstanding the lack of full integration, MBMS is limited to be implemented only by Telecom Operators operating 3GPP based networks, as it requires the core radio infrastructures and operation licenses.

From the viewpoint of an operator, 3GPP-MBMS has several other restrictions such as limited bandwidth, limited coverage and the need for user services to be adapted (at the source) to the conditions of the network, thus restricting the use of the same service over several different networks and bearers. This is a clear barrier to the introduction of new services by content providers that lack knowledge on the operational characteristics of the network.

Success of novel services in next generation networks is extremely dependent on the quick and easy introduction of new contents and services. Players in the telecom market will try to optimize profits by providing the same content and services through as many networks as possible. In turn this will lead network operators to increase the heterogeneity of their networks through the inclusion of new Radio Access Network technologies. The heterogeneity will ultimately lead to an increasing concern by network operators to move their external interfaces from bearers' services towards user services. This trend can be already recognized in the increasing importance of service platforms such as 3GPP IP Multimedia Subsystem (IMS) [3GPP TS 23.228]. The IMS comprises a layered architecture, consisting of Access and Transport Plane, Control Plane and Service planes. IMS provides integration between Service and Network Providers and serves as an aggregation point of heterogeneous networks that encompass more than a single core network. IMS adds a set of functions linked by new standardized interfaces, for the integration of different services, hence offering a large variety and enriched services to end customers. Operating at the Service Platform plane, IMS enables operators to make better usage of their networks especially considering those that pursue the fixed/mobile convergence path, since they can make use of the same mechanisms for both fixed and mobile access technologies.

From the viewpoint of the Content Provider, the use of a platform that abstracts the complexity of the Network Providers network is a key aspect for a broader deployment of services over new channels. Content providers can then focus on the applications and services, and let the running aspects of a network (such as security, A4C, QoS and session management) to be handled by the operator's platform.

Both IMS and MBMS (as described in Release 6) provide Applications with an interface that not only overlaps, but even in some cases duplicates functionalities. The integration between IMS and MBMS is therefore being considered in a study item within 3GPP for inclusion in future releases [3GPP TR 23.847]. The concept supporting this study is the possibility to save radio and core resources by having IMS based application using multicast bearers. In this initial study two main proposals exist: to interface IMS with the BM-SC; or to have the IMS in direct control of the MBMS Bearer Services, with a clear separation between service and transport entities. The first proposal constitutes a remedy to the current situation, since it assumes that the subsystems continue to exist as they are. The second, on the other hand, is more inline with the layered approached described in the beginning of this chapter and that shall be explored in the next section.

4.2.2 Leveraging the BM-SC towards IMS

In a Next Generation context, multiple networks could be used to distribute multimedia content in a seamless way. It is expected that next generation content delivery IP based architectures will resort to IMS as an overlay control layer providing a common platform for various access technologies with most of the logic residing in Application Servers (AS).

This follows the OMA vision that predicts the existence of new enablers that allow interactive content delivery of Broadcast Services over heterogeneous networks to end-users [OMA Arch]. The architecture guidelines for open service deployment developed inside OMA were named OMA Service Environment (OSE) and its components are known as Service Enablers. The targets of this open specification are the rapid development and deployment of application; component reusability; enabling interaction from third parties through a controlled environment; broadening the developer pool; and automating business relationships management. All these are vital to the development of rich applications and services environments.

It is thus natural that the proposed optimization of the interface between applications and service platforms follows these guidelines. It is here proposed that the interface between applications and service platforms is done through an OMA based middleware layer consisting of several Service Enablers for group communications. On the service platform, broadcast/multicast bearer services should be placed under the control of the general control mechanisms, providing the means for services enablers to dynamically switch between unicast bearer services and broadcast/multicast services without any change in terms of interface with the service platform.

The Service Enablers should support features such as interactivity, personalization and community building, making the services even more attractive to customers at the same time that they spare resources through the usage of group communication mechanisms.

This approach reduces the investment of deploying new network components in the Service Platform and optimizes the usage of network resources by making it easy for applications to deliver multimedia content over a broadcast/multicast transmission mode. To this intend the MBMS and IMS integration is carried out by distributing the BM-SC functionalities among several IMS entities such as the PCRF, P/I/S-CSCF's and HSS. Moreover, through the creation of an OMA based Service Enabler Layer it is possible to coordinate the use of unicast or broadcast/multicast bearer services in an abstract layer that applications can relate to (avoiding the need for applications to be aware of the network mechanisms used).

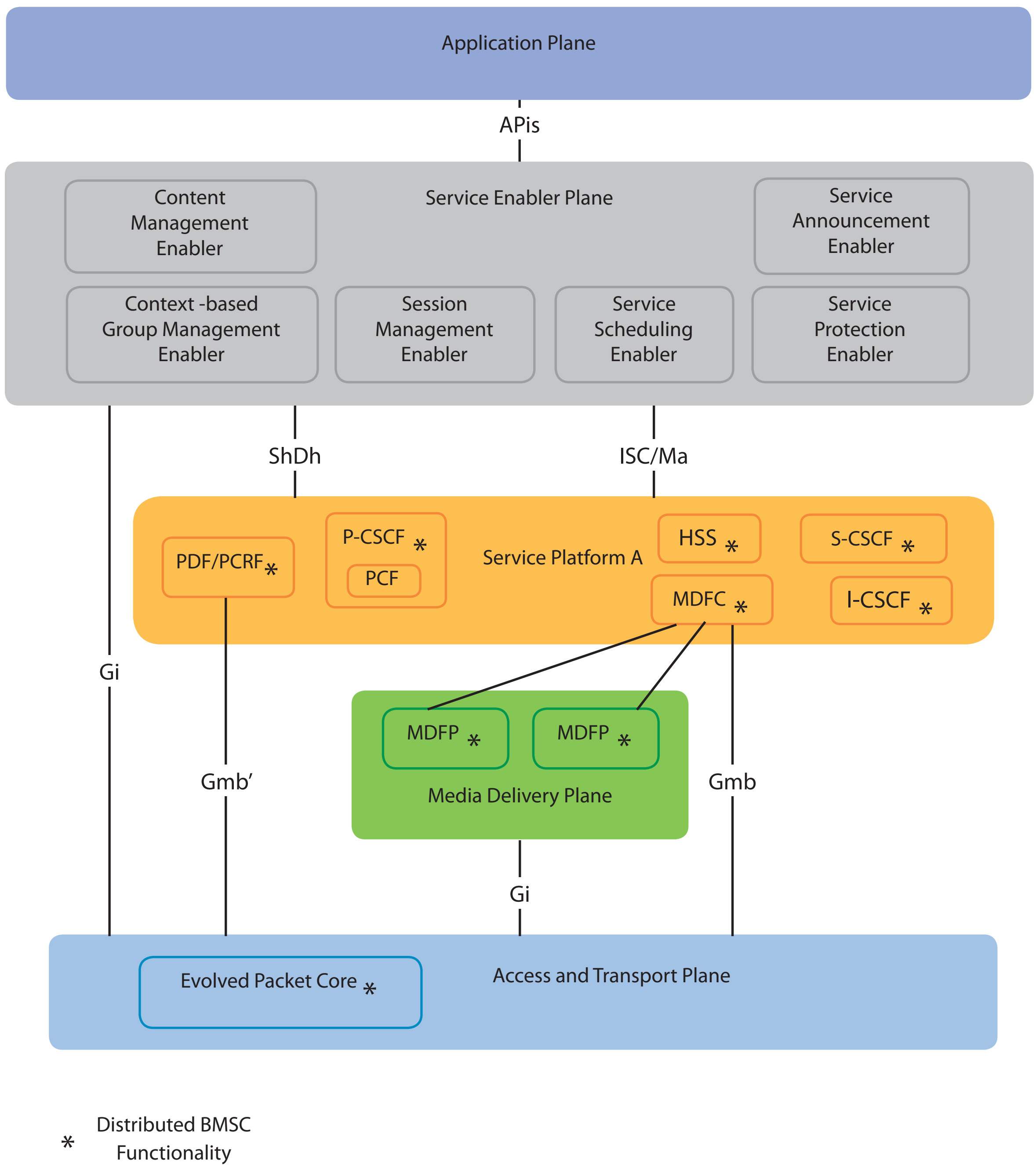


Figure 15 - Network Entity Design

In this optimization proposal, above the Service layer lays an intermediate layer composed of Services Enablers that interface between Applications and the Service Layer. A detailed network entity design of such concept is presented in Figure 15. Such intermediate layer is functionally part of the Service Layer previously defined but is presented separately in order to clearly depict what belongs to IMS from the Services Enablers required to support Group Communication.

The Network Entity Design consists of a five-layered framework, namely, Access and Transport Plane; Media Delivery Plane, IMS-based Control Plane and Service Enabler Plane that constitute the Service Platform; and the Application Plane. In the figure two end points are also presented, more precisely the User Plane and the Content Provider Plane. Most of these planes are already standardized in telecommunication forums.

4.2.2.1 Access and Transport Plane

The Access and Transport Plane encompasses the heterogeneous access networks, having QoS and mobility support. It uses IP-based interfaces for both data and control information in accordance with the conclusions of [3GPP TR 23.882].

4.2.2.2 Media Delivery Plane

The Media Delivery Plane is responsible for media stream processing, as well as media and content relaying from the Content Provider to the end-user, over unicast, multicast or broadcast bearers in the most efficient way. It consists of a set of Media Delivery Function Processors (MDFP) that copes with both streaming and download services. Each MDFP has the ability of receiving data from a content provider and relay the content to a set of subscribed users using the most appropriated channel. The MDFP is responsible for any transcoding operation required. This transcoding may be done in real time for streaming services, or may be performed asynchronously for download sessions. Therefore, the MDFP receives the content from a content provider over an IP-based interface through a unicast channel using File Transfer Protocol (FTP) [RFC 959] for file download, or Real-time Transport Protocol (RTP) [RFC 3550] for streaming. The data is then processed according to the type of media needs and distributed using a unicast, multicast or broadcast channel over an IP connection using FTP, File Delivery over Unidirectional Transport (FLUTE) [RFC 3926] or RTP protocols.

4.2.2.3 IMS based Control Plane

The Control Plane consists of the traditional IMS control entities, which are in charge of session management, and thus coordinate the delivery of information. Although this architecture makes possible the use of unicast, multicast and broadcast channels, the CSCFs functions do not require any modification, and still rely on the profiles stored on the Home Subscriber Server (HSS). Modifications are only needed on the level of information that must now include also multicast information.

Policy and Charging Rules Functions (PCRF) are used to control communication channels based on a set of rules that must now encompass broadcast/multicast. Besides dealing with policy control, PCRFs performs flow based charging that becomes slightly more complex as it must deal with broadcast/multicast services. The Media Delivery Function Controller (MDFC) is responsible for the mapping and control of the media delivery plane.

4.2.2.4 Service Enabler Plane

Following OMA directions, several enablers should now be defined, offering support to a diverse group of application developers and service providers. These Enablers will act as a bridge between end-users and content providers. In order to support unicast, multicast and broadcast communications, and after some discussions with network and content operators inside the C-Mobile project, the following enablers were used:

- The Service Announcement Enabler (SAE) which gives service information to user terminal;
- The Service Scheduling Enabler (SSE) for scheduling in an optimized way the network resources;
- The Content Management Enabler (CME) which allows content publishing and provisioning;
- The Session Management Enabler (SME) for dealing with session issues including QoS, and
- The Context-based Group Management Enabler (CGME) to allow community building.

These enablers were designed to support a set of generic capabilities making possible the use of various communication technologies. The different enablers communicate between each other using specific APIs; furthermore SIP signaling or HTTP may be used when interacting with end-users or content providers. These enablers will be discussed in the next section.

4.2.2.5 Application Plane

The Application Plane allows applications to make use of the capabilities provided by the enablers by means of well defined API's offering to end-users personalized and interactive services over diverse transport bearers, using different transmission modes.

4.2.2.6 User and Content Provider Plane

The User Plane refers to the end-user who gets the content using the mobile network by means of unicast, multicast or broadcast connections. The user gets the content using RTP protocol for streaming and FTP or FLUTE for content delivery.

On the "other end", there is the Content Provider Plane, which consists of the entity that owns the content that is to be delivered to end-users by means of the media processing entities. It uses unicast links to transfer the content to the MDFP entities. The protocols used are RTP for streaming and FTP for content download. The content provider may be a corporate entity or simply an Internet user who wishes to upload its own content (User Generated Content – UGC).

4.2.3 Service Enablers for IP-based Content Distribution

In most cases, Group based services are offered by a single Provider, which deploys a complete architecture infrastructure from content provider servers to RAN. This solution requires a great amount of resources. Innovative services (deployed mostly by third parties) will require that they can be reused over various platforms in order to be cost effective.

Fundamental for the success of the defined Service Enablers are the mechanisms available for interaction with the application and service development community.

The Java Community Process (JCP), one of the many organizations collaborating with OMA, takes a central role in Java-related open specification development and revision. There are five JCP specifications - Java Specification Requests (JSR) - that are especially relevant in a multimedia content distribution context:

- [JSR 116] specifies SIP servlets v1.0 that is the SIP counterpart to the well-known HTTP servlet specification for Java.
- [JSR 141] specifies an API that enables users to manipulate SDP messages.
- [JSR 220] specifies the Enterprise Java Beans 3.0 architecture, empowering development and component reusability.
- [JSR 244] defines the Java Enterprise Edition 5 Specification, commonly known as the Java application server specification.
- [JSR 289] defines the 1.1 versions for SIP Servlets.

For all these JSRs it is possible to find open source implementations, either complete or under development [JSR 289].

Based on these concepts, Application Server and Application Framework specifications [Maximilien 2004] are useful to instantiate OMA concepts and the proposed Service Enablers. Application Servers and Application Frameworks typically define sets of mechanisms in order to improve developer productivity and component reusability and integration. Using these specifications, rapid development is possible because in most cases the developer only has to worry with the service logic. Application Server specifications usually have more advanced security mechanisms and address scalability issues more thoroughly than frameworks. These security mechanisms may be especially useful when integrating with third parties. And provide the necessary guaranties to operators that the services and applications will provide the high level standards in terms of security and reliability that network operation requires.

The proposed optimization of the interface between Applications and the Service Platform required the definition of several OMA-alike enablers, offering support to a diverse group of application developers and service providers, acting as a bridge between end-users and content providers. These enablers were defined assuming that the used application server implements or provides an implementation of [JSR 116] and [JSR 141]. The interface descriptions are based in OSE interface categories [Handa], so the interfaces will be referenced as I0, I1 and I2.

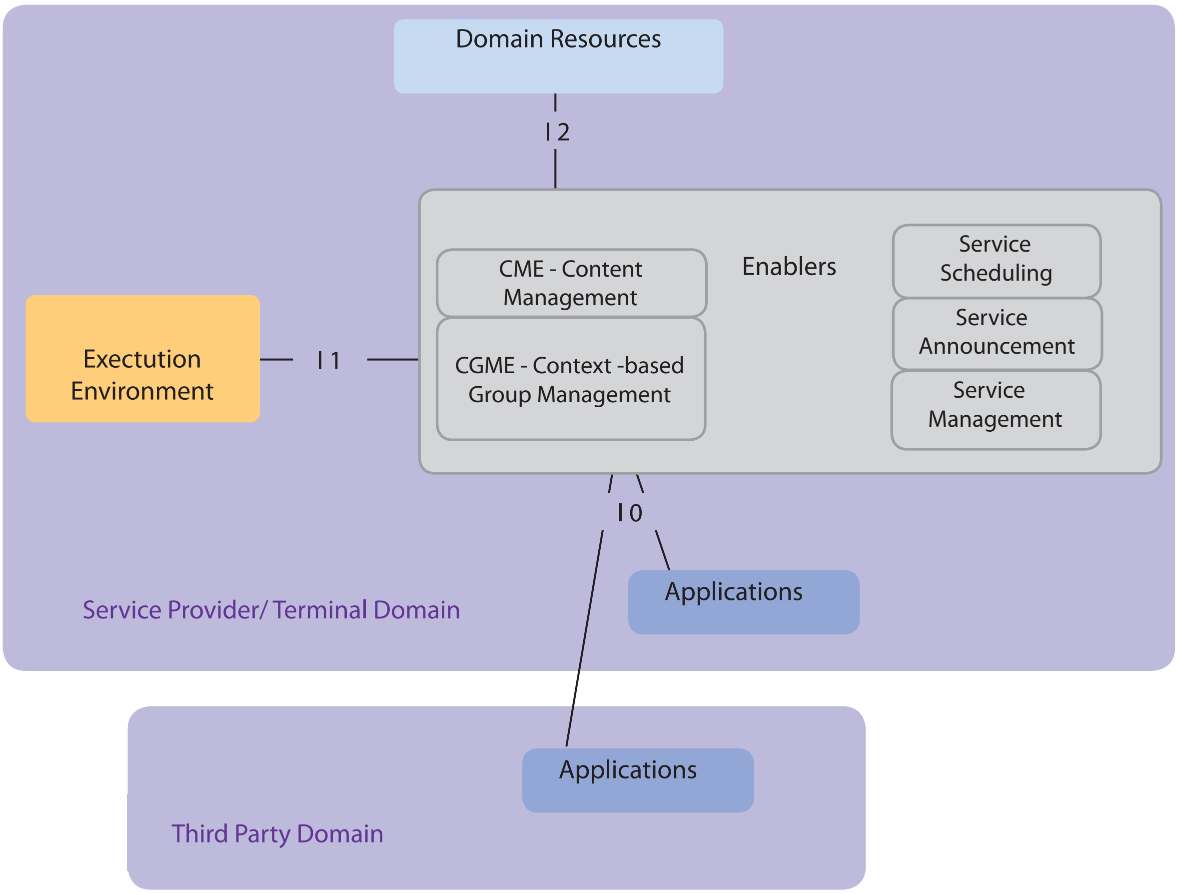


Figure 16 - OMA Enabler Interface Categories

The I0 interface contains the enabler functions available to other applications or enablers. The I1 interface is the management and configuration interface of that enabler. The I2 interface covers the functions that the enabler uses from the domain. In this context, it includes a SIP stack and interface to the other network entities. While some enablers are exclusively present in the service provider domain (SPD), others include components in the terminal domain (TD) [OMA 2007]. The enablers defined are presented in Figure 16.

4.2.3.1 Service Announcement Enabler (SAE)

The Service Announcement Enabler manages high-level service announcements required by applications to be sent to UE. The announcement carries service information to the UE, namely service URI and session times for bounded sessions, as well as a short human readable description related with the service. When the SAE gets an announcement request at the SPD via I0, it uses I2 to send a SIP message to the subscribed users. The announcement information is encapsulated in a XML file, which is delivered to the SAE component at the TD via I2. After receiving the payload, the XML is interpreted internally and relevant information is displayed to the user using I2. The terminal component should also allow other terminal applications to check what announcements were received via I0. In order to optimize the announcements distribution, the XML file can be distributed only to subscribed users that match context related information, in which case the SAE depends on functionality made available by the CGME, as described below.

4.2.3.2 Context-based Group Management Enabler (CGME)

The Context-based Group Management Enabler holds group management functionality based on user context information. It is in charge of managing these groups and providing this information to the interested enablers or parties through I0, so that more dynamic services can be created. Subscriptions of services are also to be handled by this enabler. The CGME is therefore responsible for updating user profiles in the HSS through the l2 interface.

4.2.3.3 Session Management Enabler (SME)

The Session Management Enabler is the main contact point for the end-user because all signaling procedures are managed here. The SME allows applications to request content deliveries through the I0 interface. It is the responsible for receiving or triggering the association of a user/equipment to a specific service. The SME then handles the session data, making it available through I0. The SME shall also setup the necessary media resources. For the setup of the user sessions and media resources, the SME acts as a SIP Back-to-Back User Agent using I2. Finally, the SME is responsible for activating the communication bearers when the session is about to start and to tear them down at the end of the session.

The Session Manager Enabler is the entity in charge of performing bearer selection. Based on (for instance) the user capabilities or network load, the SME may select a unicast, multicast or broadcast communication channel. The appropriate IP address allocation shall also be done by the SME based on the selected bearer.

4.2.3.4 Service Scheduling Enabler (SSE)

The network operator applies admission and policy control within its domain and, therefore, the content provider is not allowed to directly distribute its content to the subscribed users. It is the network operator who manages the scheduling in order to optimize network resources. This control shall be made by means of the Service Scheduling Enabler, which is in charge of assigning the time of the delivery. This function is provided via I0. The optimal schedule is determined taking into account data available from I2, potentially including the users' spatial distribution, the current and estimated Radio Access Network (RAN) capacity, the QoS requirements and the type of service (streaming, carrousel or download).

4.2.3.5 Content Management Enabler (CME)

The CME provides interfaces for the Content Providers to publish and provision content, performing the necessary control of the incoming content. Although content is provisioned in the media layer, all content metadata is made available to other enablers or parties by the CME via the I0 interface at the SPD. The CME also supports the provisioning of user content, enabling greater interactivity. The content provisioning is done using SIP. The terminal-side

CME must provide an automated publishing and provisioning function via I0. Optionally, that functionality may be provided through a user interface, using I2. The SPD CME will receive provisioning requests via I2 and will act as a Back-to-Back User Agent in order to provision the content at the media layer.

4.2.4 Service Oriented Network Management and Control

In the previous section it was discussed the service enabling mechanisms that can optimize the interaction between the network and the application and/or content provider. In this section, such interactions will be described with concrete examples where the Network Operator and Content/Service Operator can both profit from such interaction, highlighting resource optimization benefits.

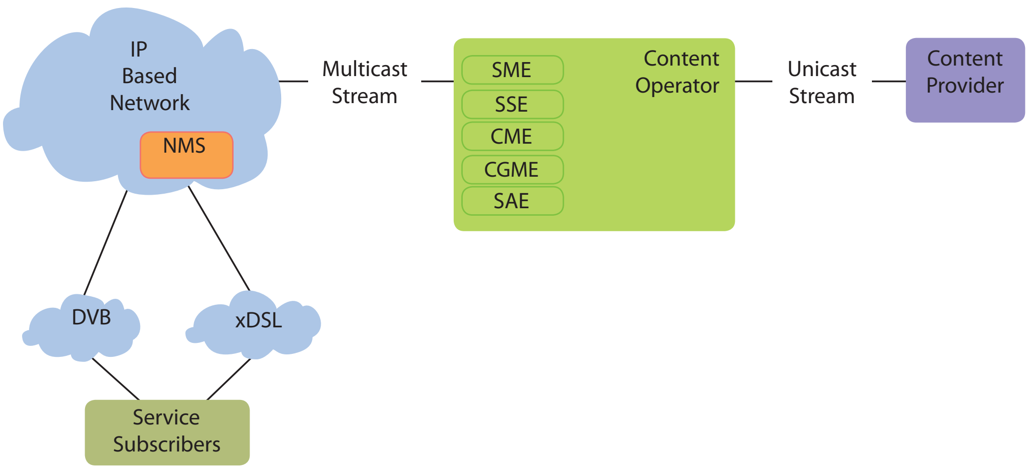


Figure 17 - Reference Architecture

Of the described service enablers, the SME (Session Management Enabler) plays a central role in the interaction between Service and Transport Network. While by definition the Service Enablers are transport agnostic, the SME is the exception that enables a more informed use of the network resources by services. Figure 17 presents the reference scenario for the examples below, which highlight intelligent functions handled through these enablers. In the reference scenario, Content Providers interact with the Service Operator (and its enablers), which in turn manage a heterogeneous network to provide services to the user.

4.2.4.1 Example 1

The first example explores the function of the SME to choose if the requested service should be deployed over a unicast or multicast IP connection.

This choice is important for both Network and Service/Content operators.

In terms of scalability, the use of a multicast connection by the Service/Content Provider frees it from having a provisioning platform capable of supporting thousands of connected users, and of course supporting the cost of such connections.

From the view point of the Network Operator delivering the service over Multicast might mean the use of a different technology with savings in terms of resources, e.g. choosing a broadband unidirectional technology such as DVB instead of a resource sparse xDSL connection.

The SME is able to make these choices because it is aware of the service characteristics (e.g. a streaming service with no interactivity) and can act as a back-to-back user-agent between the end-user and the content provider, thus being able to alter the negotiated parameters between the two endpoints by putting signaling in the right network context. This context is implemented in the MDF that relays the single unicast connection of the content provider to the multicast connection provided to the network users.

The SME is independent of the network infrastructure, and no extra signaling interface is required, besides the interface with the IMS platform (the real responsible for interaction with the network). In this example, the SME can signal the appropriate technology to the IMS platform by choosing a multicast address belonging to a pool of addresses routed through a DVB network for terminals supporting DVB. This solution does not limit the service to DVB capable terminals as secondary addresses can exist for the same service for terminals lacking DVB and maintains the possibility to deliver the service using Unicast to well defined end-users with special requirements such as alternative contents (e.g. subtitles, audio description, codec's, etc).

4.2.4.2 Example 2

Another example that illustrates the resource optimizations possible with the proposed interface enrichment is the ability of the SSE (Service Scheduling Enabler) to schedule non real-time services such as podcasts, according to feedback from the SME that tracks the ongoing sessions per it. The SSE might cooperate with the network management system (NMS) that monitors links usage, delay, jitter, etc. For this an extra interface is required between the Service Enablers plane and the Network Control Plane, but can nonetheless be considered as non-intrusive, since the interface is used only for monitoring and not for control: functionality can stay encapsulated inside a specific Service Enabler.

In such scenario, the SSE would schedule the podcast delivery for a given time, at which it would contact the SME to setup a session. The SME would request the NMS through the appropriate Service Enabler for statistics on the network, possibly detecting over provisioning of some links and under provision of others that might be used for the non real-time provisioning of the podcasts to the end-user terminal. Eventually the SME might decide the inopportunity of the request by the SSE and therefore set the re-schedule of the podcast delivery to later time. This decision would always be taken in consideration of the Service, as not all services can be re-scheduled.

The previous examples illustrate how optimization of functionalities many times described in previous networking research (e.g. [Prior 2005], [Marques 2003], and references within) can be implemented using service logic instead of costly signaling at low level entities, such as access routers.

By moving the intelligence of the overall system from the network to the service plane, the architecture enables Network Operators to focus their efforts in network enhancements while maintaining a strong link to Content Provider through the role of Service Composers, capable of bounding high level services (which are content related, as is the case of metadata) with lower level services (which are mostly network related, such as QoS levels). This is however a new point in the reference layered approach presented in Section 4.1 , that is also possible to optimize.

The next section will therefore focus in the optimizations and network enhancements that NGN might incur.

4.3 Optimizing Group Communications through Service and Network Optimizations

As previously mentioned, one of the most distinguishable characteristics of 4G networks is the multiplicity of radio technologies associated to a single terminal and/or operator. These technologies enable both operator and end-user to make use of new services under "Always Best Connected" (ABC) conditions. Realizing such paradigm is nonetheless of extreme complexity since the technologies share different characteristics among themselves, such as Medium, QoS, Bandwidth.

From the viewpoint of Services deployment, these different characteristics must be abstracted. One of the most important abstractions is the IP protocol on top of which most of today's Services rely. 4G operators will therefore make extensive use of IP based platforms much similar to the 3GPP IMS platform in order to deploy its Services.

In IP based networks, group communication usually refers to the use of IP Multicast for the delivery of content. This is an adequate abstraction for NGN. In section 3.5.1 , it has been detailed the workings of IP Multicast in a generic network without drawing too many considerations on the network in which it is deployed. The fact is that each technology has its own mechanism for group communication that can be used to improve the delivery of IP Multicast. Unfortunately these mechanisms vary from technology to technology and in most cases cannot be reused. It is therefore important to study the mechanisms involved in each technology and to create network control mechanisms that can optimize the deployment of Group Services over IP Multicast in each of the technologies.

4.3.1 Coping with heterogeneous networks in group communication

One of the main assumptions for group communication is that the service being delivered to all group members should have the same characteristics. In the case of 4G networks where the service is deployed on top of multiple technologies this assumptions fails. Each technology is different, especially concerning QoS parameters such as delay, bandwidth and jitter. That said, the service delivered cannot be the same and service adaptations maybe required. In section 2.1.1 , it was nonetheless said that the Service should not be aware of the heterogeneity of the network. This can lead one to conclude that the network provider might carry some sort of service adaptation.

One of the most common service adaptation mechanisms is Content Adaptation. In the presence of a multimedia service the network operator can mediate the service between the content provider and the content consumer and provide an added value service, which consists in the adaptation of the content to sub-groups. In this use-case the service group is divided into subgroups at the network level that receive each the same service using different coding mechanism, bitrates, resolutions, etc. This method evolves from 3G mechanisms described in the previous section (4.2.2.2) and can solve the problem for multimedia services.

Unfortunately, this method is quite intrusive, as it requires the existence of a network mediator that breaks the concept of end-to-end service provisioning in legacy applications, making it only possible for services based on IMS alike service platforms. Furthermore, it solves only the problem of multimedia services (although they are currently considered the most important group communication service), as the content adaptation mechanism are very application specific.

Albeit their differences it is possible to identify the configuration for each technology that enables the existence of a common QoS profile over the global network. The problem therefore becomes how to signal and control each technology bearer in order to adjust the network to the service and not the other way around.

4.3.1.1 QoS Signaling

Most of the required signaling and control mechanism for the process of adjusting the network to the service can be performed through QoS signaling mechanism as already defined in 3GPP and TISPAN. IMS P-CSCF can signal the several network elements using IETF protocols such as COPS and DIAMETER. The signaling information transported in these protocols is nonetheless abstract as it is usually intended for IP based QoS enforcement mechanisms such as the ones described in 3.1 . A mechanism is necessary to assist in the process of mapping IP based QoS parameters into technology bearer parameters. This mechanism constitutes an optimization of the interface between the Core Network and Radio Access Network. This optimization can only be performed by the entity placed in the border of these two layers, the Access Router (AR).

This optimization assumes that AR's can be provisioned by a Policy Based Management System with technology bearer specific configuration mappings that can enable each AR to translate IP based QoS configurations into technology bearer specific configurations.

4.3.1.2 Legacy Services

When discussing the impact of heterogeneous networks, a special attention must be given at legacy services and applications, since the introduction of new technologies must not disrupt the existing ones, under penalty of loss of clients/market. That said, is important to take into consideration that any new proposals towards the introduction of new technologies or services must respect existing standards and transparently support existing group communication mechanisms at both link and transport layer.

IP multimedia multicast services currently deployed in IPTV scenarios must then be taken into consideration in an environment that might encompass technologies that might have very different characteristics. It is not expectable that legacy services can simply be deployed over new 4G networks without any degree of adaptation and control.

Therefore Next Generation Heterogeneous Networks must also provide the proper support for applications that do not rely in a Service Platform. These applications interact directly with the Core Network. In order to perform proper adaptation of such applications, the AR must also be able to support signaling protocols such as RSVP and NSIS that provide the means for applications to signal their resource requirements to the network.

4.3.1.3 Unidirectional Technologies

In the myriad of technologies made available to 4G operators, there is one that excels for group communication through its simplicity and efficiency: DVB. Unidirectional technologies such as DVB, as seen before (3.4.3.1), are characterized by the fact that communication can only be performed in one direction, from a specific source to a group of listeners. Unidirectional radio technologies are not limited to ETSI technologies, namely DVB-S, DVB-T and DVB-H, and are present in 3GPP standards such as the case of MBMS radio bearers (see 3.4.3.2). The use of these technologies in a heterogeneous environment is predictable and desirable as these technologies can support a large number of users with group-oriented services, and making use of a limited amount of radio resources. Unfortunately, not all services can be deployed over such technologies since interaction is not possible; therefore services are required to be aware of the underlining technology. Again, this is a violation of the desired abstraction and uniform approach previously described.

4.3.2 IP based Group communication over Heterogeneous networks

To support heterogeneous access technology environment, operators need to rely in a homogeneous architecture able to integrate all of them. A cross-system approach is thus required, providing an integrated behavior for the whole service delivery, regardless of the Radio Access Network technology being exploited at that instant.

Taking these aspects and requirements into account, this section addresses the delivery of multimedia services in a 4G (next generation) operator architecture capable of deploying multimedia services in a heterogeneous environment, where unicast and broadcast technologies share a common provisioning platform (Service Platform and Core Network). The cross-system solution is able to address this heterogeneous integration problem both in terms of technologies and services provisioning. This solution intends to detail the optimization mechanisms necessary to seamless deploy services negotiated at the Service Platform through the most appropriate Radio Access Network available to the Core Network.

Figure 18 depicts a simplified view of the proposed 4G operator-oriented network architecture. This concept was developed as an architectural subsystem in the more ambitious architecture of the IST-Daidalos project [DAIDALOS] Figure 18 includes only the entities involved in the direct support of multicast and broadcast communication, and part of the legacy 3G network required to deploy the same services. The legacy MBMS sub-system is clearly depicted in this figure in order to present an integrated view of the heterogeneous architecture, and to highlight the main changes applied to cope with RAN heterogeneity.

The heterogeneity of the access technologies implies the existence of an environment where several distinct RAN's (WiFi, DVB-S, 3G, etc) are aggregated by a Core Network that provides key services: A4C (Authentication, Authorization, Accounting, Auditing and Charging); end-to-end QoS; and a Service Platform, here represented by the MMSP.

IPv6 is the reference denominator to transport data over all available technologies, fully replacing the UTRAN/GERAN layers, and presenting a smooth evolution path from 3G architectures. Note however that the focus of this work can be also exploited in terms of an evolution of 3G networks.

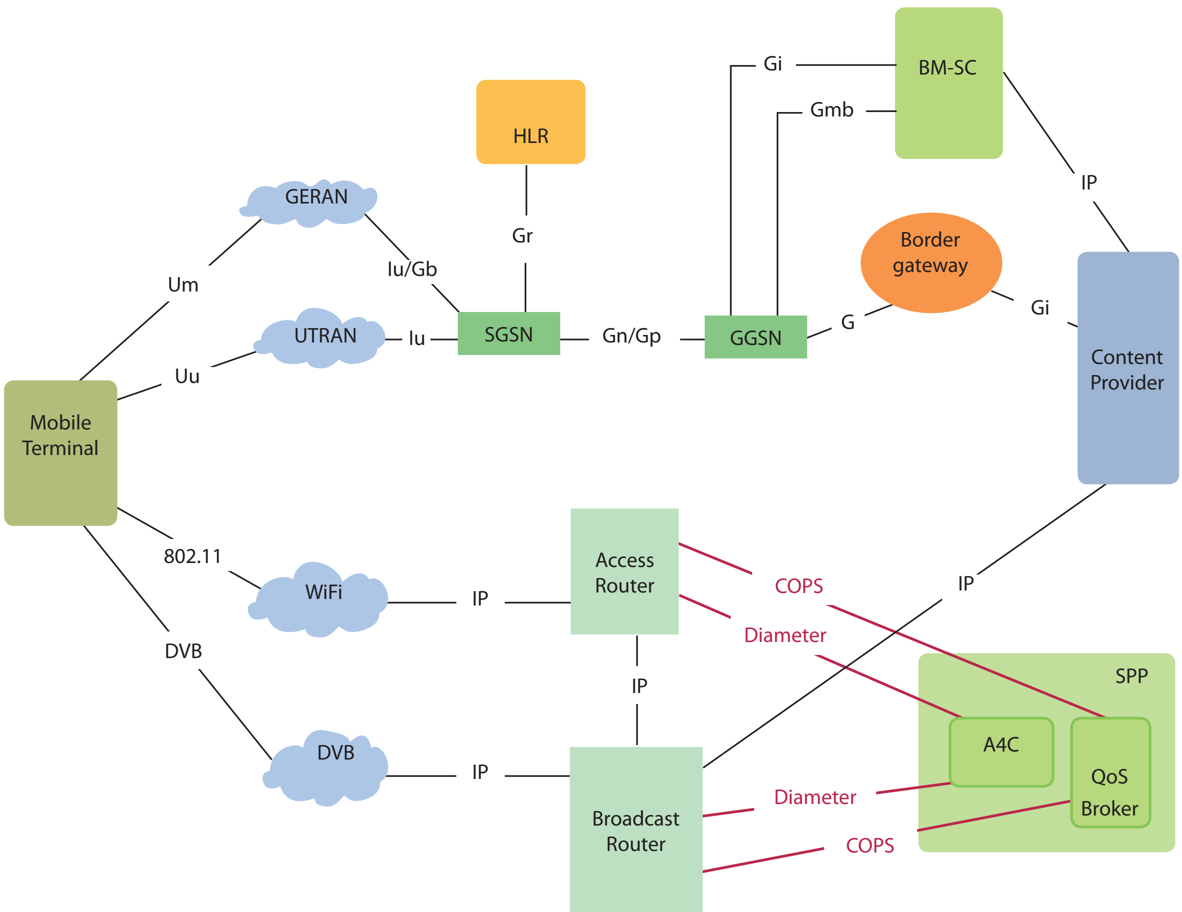


Figure 18 – 3G MBMS vs. 4G Network Multicast/Broadcast QoS Architecture

The core network in Figure 18 contains a Service Provisioning Platform (SPP), composed by several enabling servers, such as the A4C and QoS Broker. The A4C server authenticates and authorizes users and services, and charges users for the accessed services. QoS Brokers manage overall network resources, providing admission control and triggering resource reservation. Mobile Terminals (MT), such as Laptops and Smartphone's, are connected to the network through IP Access Routers (AR), or through a legacy UTRAN network. Each AR, connected to a different access technology, has the functionality to accept, authorize, and enforce per-flow QoS on the access links to the users. Although not clearly represented in the picture, cellular technologies are also controlled directly by an AR, in a similar way to a WiFi Access Point and in accordance with the work being done in 3GPP LTE [3GPP TS 36.300]. Mobility requirements are fulfilled by the usage of Mobile IPv6 [RFC 3775], and the inclusion of fast transfer mechanisms such as PMIP [RFC 5213]. Furthermore, for multicast session state information, context transfer support is required in the ARs for seamless multicast subscription transfer.

On the access link between the MT and the AR, tight resource management is enforced by the QoS Broker, controlling the admission and policing of flows in a per-session basis, taking into account the profile of the users and network resources (this is assisted by a set of active measurements on the network). This profile is sent from the A4C to the QoS Broker on terminal registration, and has information on the set of network level services (classes of service) that may be provided to the user, essentially reflecting the user's contract.

In this architecture, control functionalities (QoS, authentication and authorization) are distributed along the network. This allows the architecture to be free from a centralized entity such as the BM-SC, which vertically controlled all broadcast/multicast aspects. These functionalities can now be distributed by the Core Network and supported by IETF protocols, such as COPS or DIAMETER. This distribution is very advantageous, since it avoids the requirements of an extra control plane entity (essentially removing 3GPP specificities), as the QoS Broker and A4C are already present in 4G architectures to support unicast services.

Nevertheless, to support IP multicast services, the functionalities of the routers and QoS Brokers need to be extended compared to the ones required for the support of unicast services.

Routers will be in charge of all routing mechanisms involved in the establishment, maintenance and management of the multicast network, while the QoS Brokers will be in charge of managing the resources associated with the use of multicast in the network. Agents in the routers provide the necessary mechanisms for the remote control of the routing daemon by the QoS Brokers, using management protocols such as COPS, DIAMETER or Simple Network Management Protocol (SNMP). Multicast IP routing is performed using PIM, and mobile terminals subscribe to multicast services by means of MLDv2 reports. These pure IP mechanisms are parallel to the MBMS Service Setup Phases described in 3.5.3.3 , but void of any Service Logic. As seen before the Service

Logic is part of the Service Platform and is only made available to applications that use the Service Platform. In any case, this simplification should be seen as an added value, as it provides the support for legacy applications unaware of the existence of a Service Platform.

4.3.2.1 Resource Optimization and QoS Support

QoS support in the previously described 4G network follows IETF-based approaches. In the wired access and core networks, DiffServ architecture is used to support QoS, achieving scalability and performance. In the wireless link, IntServ-alike resource management is used to provide better QoS resource control in the wireless part. In both cases, a QoS Broker is the element responsible for the resource reservation and management.

In multicast communications with QoS support, QoS is achieved in a per group basis. Each IPv6 multicast group corresponds to a specific QoS level that has been previously negotiated with the QoS Broker, either through a resource negotiation mechanism, or by a written Service Level Agreement between content provider and network operator.

QoS Brokers need to be aware of multicast routing in order to predict the paths used by the flows. The availability of the information on the user terminals capabilities and authorized services provided by the A4C enables the QoS Brokers to take decisions on the best interests of both users and operator, maximizing network resources. Extensions to the unicast mechanisms of the QoS Brokers [Azevedo 2005] are nevertheless required, including the maintenance of the available multicast groups and respective QoS, and the necessary procedures to unroll a multicast tree in a series of unicast point-to-point links representing each of the tree branches. This remote control of the transport path enables the effective separation of the control plane from the transport plane. This is the opposite of the MBMS solution, where these two planes are coupled in the BM-SC. The BM-SC is both a transport entity (serving as the entrance point into the network for IP multicast streams) and a control entity (responsible for the MBMS Bearer Service). Although this separation in the presented architecture might introduce some decrease in the efficiency (due to the need to involve several different entities), this solution is much more scalable, flexible, and appropriate for a heterogeneous environment, where the same entities in the control plane can effectively control several access technologies regardless of their nature (unicast/broadcast/multicast).

The QoS Broker is therefore responsible for the installation of the filters in the routers, and the configuration of the packet remarking on the network edge, connecting to the content provider. With this mechanism, the content provider packets are delivered with the contracted QoS.

A further resource optimization aspect relies on the QoS Brokers. When a multimedia session starts, the QoS Broker is the responsible for deciding what kind of logical bearer will be reserved in the radio link. If this session corresponds, e.g., to a content, which is popular, a broadcast radio bearer can be used. Otherwise, a unicast bearer may be the best choice in terms of radio resources. Note that the architecture allows a dynamic switching across bearer types (see next Chapter).

4.3.2.2 Interactivity Channel to support broadcast-oriented technologies

The integration of broadcast networks in this architecture, relying in IP multicast, requires the simultaneous existence of an interaction network to provide bidirectional connectivity. This assumption follows the MBMS ideas, which also assumes that there is always a unicast channel besides the broadcast one (the 3G network). The integration of broadcast-oriented technologies, such as DVB, must be achieved by encapsulating the particularities of these technologies under an adequate abstraction layer, and then considering this as yet another IP-supported technology: mobility, security and QoS can now be solved at the IP layer, as discussed above.

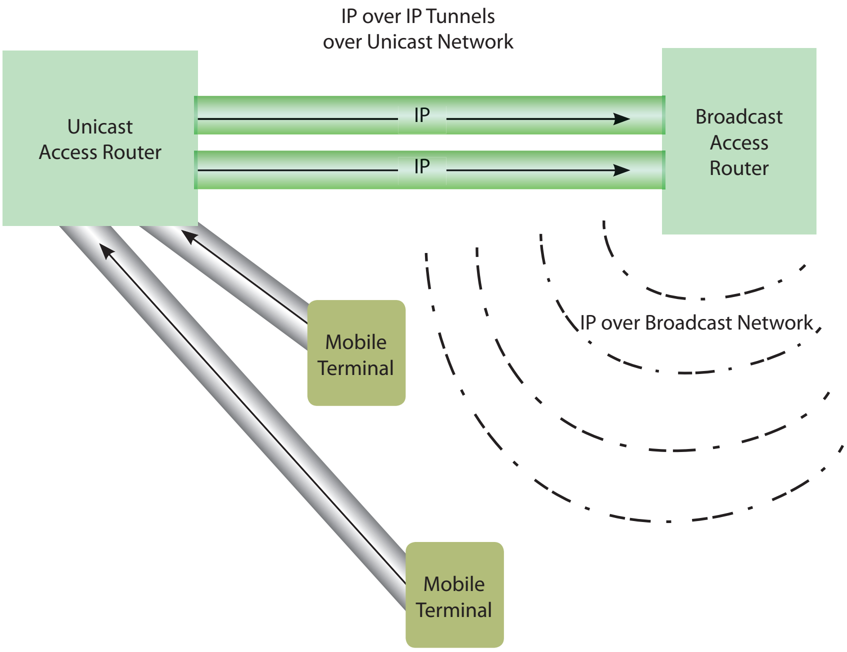


Figure 19 - Heterogeneous Return Channel

The proposed approach follows a model similar to the one described by UDLR [RFC 3077], creating a return channel. However, in this approach, this channel has to be created at the network layer. The return channel provides an upstream connection between the mobile terminal and the AR in the broadcast network where the IPE (IP Encapsulator) resides. The setup of an IP over IP tunnel creates an interaction medium to the unidirectional broadcast channel (Figure 19).

An important reason for the layer 3 tunnels is the requirement for mobility support across heterogeneous technologies. Since the IP tunnel constitutes a generic IP service supported by mobile IP, the terminal can move between networks in the interactive interface, while maintaining its connection in the virtual bidirectional broadcast interface with no synchronization effort.

By creating a tunnel at the IP layer instead of layer 2 (as in UDLR), the architecture supports business scenarios where Wireless and Broadcast operators can be separate entities that the user can contract independently.

The next section will discuss this assuming a DVB network, but the results can be extended to other unidirectional technologies.

4.3.2.2.1 Multicast Session Setup over DVB Network

In order to better understand the mechanism previously described this section presents the setup of a multicast session over a DVB asymmetric bearer. The Mobile Terminal (MT) is necessarily multimode, with at least two interfaces: one connected to the interaction network (MT IN) and another connected to the broadcast network (MT BN). In this scenario the Mobile Terminal requests the content provider a service that needs to be deployed over the broadcast network, either because of the nature of the service (e.g. Live TV Service) or because of service provider preferences (e.g. Stock Market Quotes). The signaling required for this scenario is schematically described in Figure 20.

The Mobile Terminal starts by issuing a generic App_Sig Initiation message (this message can be, as an example, a HTTP GET message) to the content provider in order to subscribe the service. This message contains a request for multicast service, and information on the interactive channel type and content to be received. The content provider replies back with an App_Sig Reply message (which can be a HTTP DATA), informing the MT on the availability of the service on a broadcast network. This message may also contain information on the broadcast network covering the MT and its configuration. These two messages constitute a very thin Service Layer, which could be extended to cover A4C mechanisms, Security aspects and possible QoS negotiation.

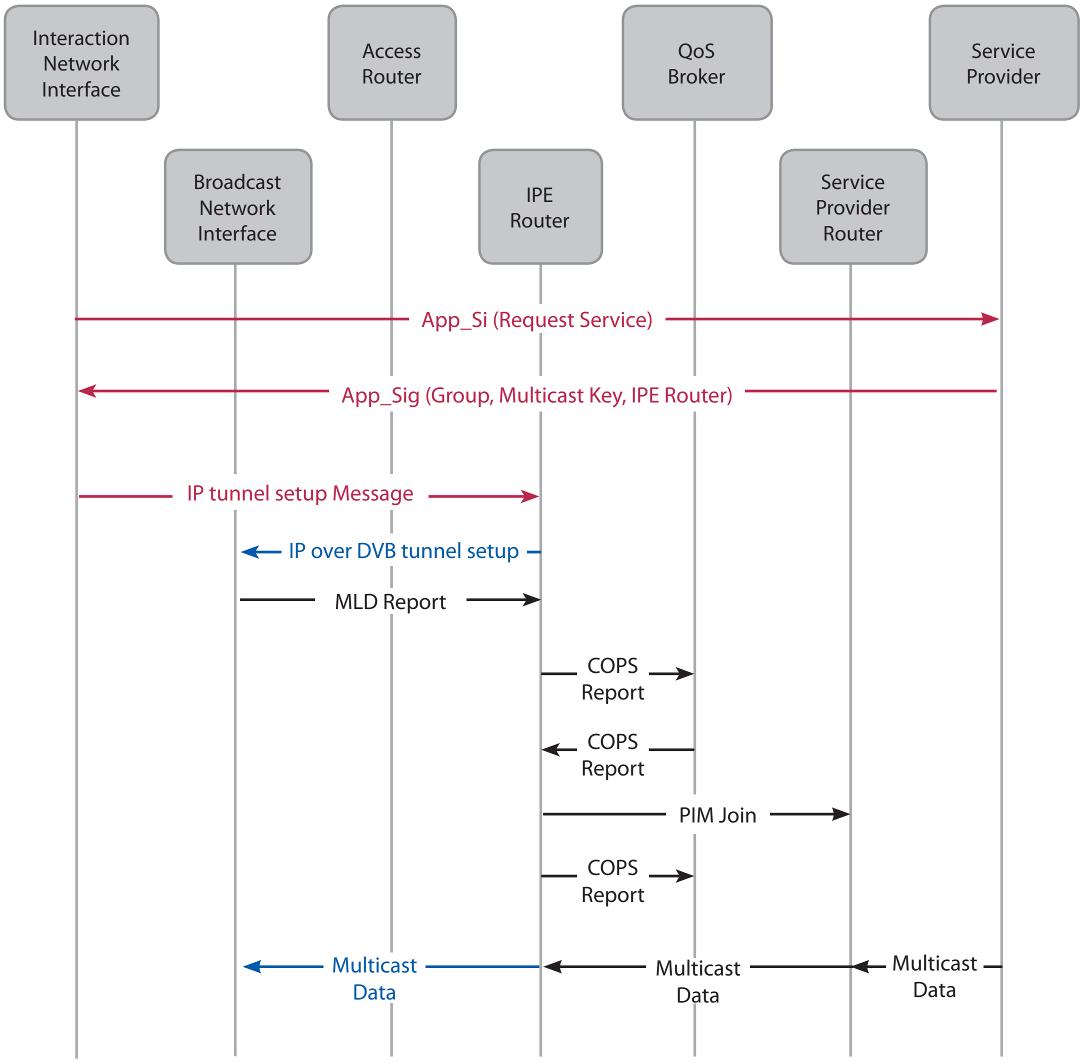


Figure 20 - 4G Network Multicast/Broadcast Service Setup Message Sequence Chart

The Mobile Terminal can then contact the IPE router (Access Router with an attached IPE) through the interaction channel and establish an IP over IP tunnel enabling the interactive channel between both. For this purpose, the Mobile Terminal issues an IP tunnel Setup message to the IPE router, and upon the tunnel establishment, the IPE router answers with an IP over DVB tunnel Setup message, sent through the broadcast network. This tunnel represents a virtual interface in each of the elements forwarding the packets: the packets from the Mobile Terminal to the Access Router are sent using the IP over IP tunnel; the ones from the Access Router to the Mobile Terminal are sent using the broadcast interface. The broadcast/multicast services will only consider this virtual interface, and will not be aware of the complexity of the unidirectional broadcast platform. With this procedure, the broadcast infrastructure becomes completely transparent.

In such a bidirectional environment (after the tunnel establishment), the Mobile Terminal sends an MLD report to join a multicast tree. This request is sent through the tunnel and reaches the designated router within the broadcast network (IPE). In the broadcast network, the router sends a COPS Request message to the QoS Broker to authorize the multicast session. The QoS Broker checks the user profile (sent by the A4C) to decide if the user can have access to the requested service with its characteristics. It also checks if the available resources are sufficient to setup the required multicast tree and to receive the service with the requested QoS. The QoS Broker sends back a COPS Decision message with information on the service authorization. If the answer is positive, the IPE router sends a PIM Join message to the Service Provider router, requesting the respective content. At this stage, the Mobile Terminal is able to properly receive the multicast stream through the unidirectional broadcast access link, with the ability to reply and interact through the IP tunnel established.

This mechanism can also be extended to support IP layer service discovery mechanism, sending to the terminal the information on the broadcast network technology available and respective channels (or in alternative, it is possible to exploit DVB Specific Information (SI) tables during a migration stage). With this information, the Mobile Terminal can then configure itself to attach to the new network as fast as possible, sparing time searching for the proper configurations of the broadcast interface.

4.3.2.2.2 Multicast Session mobility

Mobility must take into consideration the fact that it might be handling different types of mobility, such as: i) mobility between return channel points of attachment (POA) without change in the downlink POA; or ii) mobility of both return channel and downlink channel PoA's. Each of these scenarios has to be handled differently as they involve different entities and services.

Considering the first scenario, and according to the previous section where the interactive channel was described as an IP over IP service, multicast mobility is undistinguishable from the common unicast mobility. As the return channel is a point-to-point service over IP with the Multicast router, the return channel session is seamlessly transferred from the old POA to the new POA without any need to update any multicast context in the Multicast Router.

In the second scenario, the end point of the return channel service will change, requiring the transferal of multicast subscription information to the new POA. This scenario therefore requires the definition of a mobility strategy with support for multicast services. 3GPP-MBMS provides a solution to similar problems, which can be expanded under this heterogeneous context. In MBMS the existence of the "MBMS UE Context" and "MBMS Bearer Context" enables the network to track terminals and bearers involved in multicast/broadcast service. A mobility event triggers the transfer of such context amongst the involved network entities (be it the SGSN's, GGSN's or BM-SC) enabling the proper allocation of resources and provisioning of services. In 3GPP-MBMS these context transfers are done using 3GPP specific interfaces and protocols, and are therefore not appropriate for heterogeneous networks, but the concept is still valid and can be adapted to IP based network and protocols.

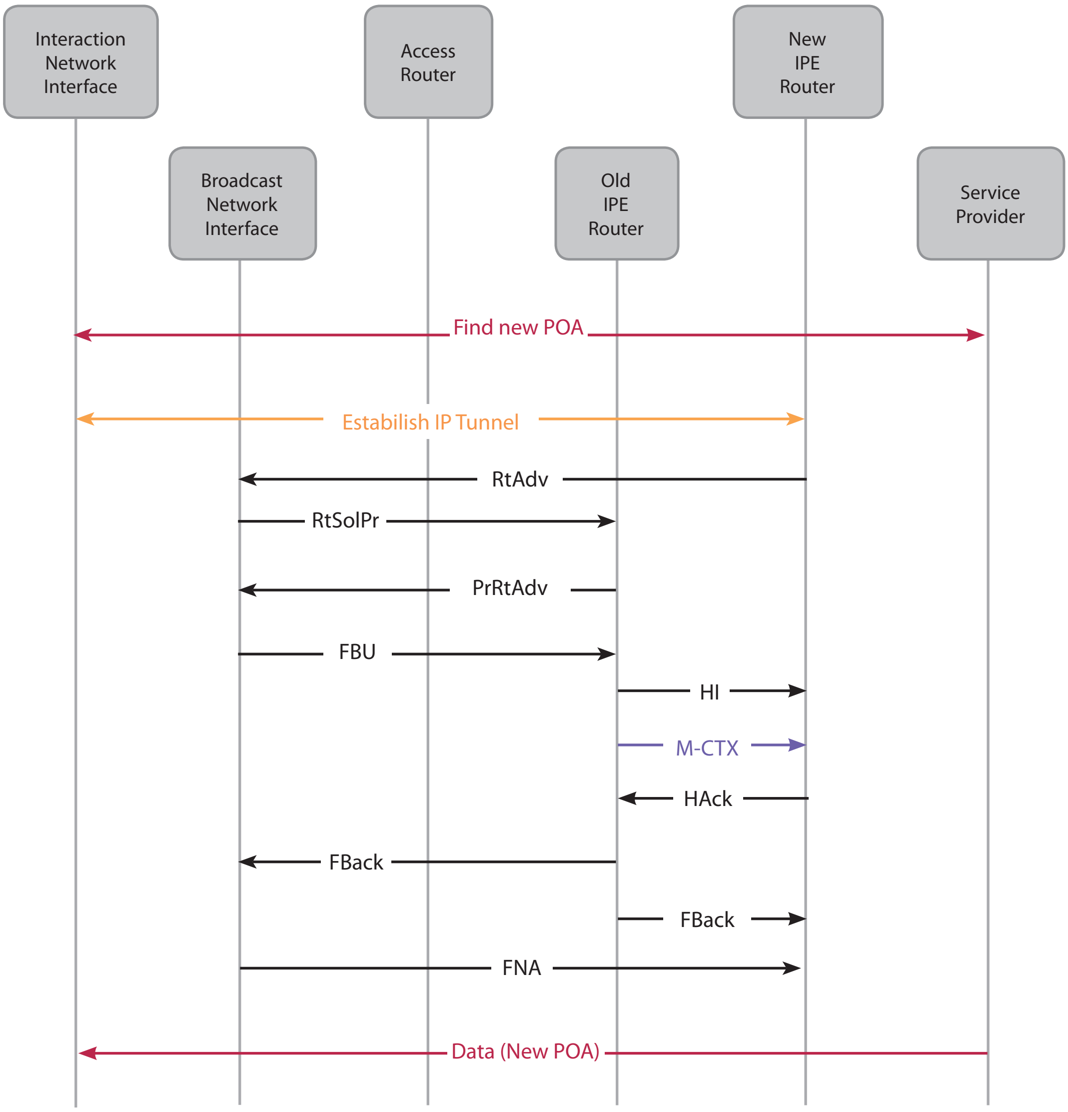


Figure 21 - 4G Network Multicast/Broadcast Service Mobility

In this cross-system approach, relying in IP based interfaces and protocols, the Context Transfer Protocol can be explored to support seamless handover of information between two nodes, therefore able to transfer the required multicast subscription information between the old POA and the new POA. This multicast context transfer re-establishes the listening and routing states for the active multicast groups and sources of the mobile node, when the node selects a new access router. Note that in this architecture, IP multicast group management is based on the Multicast Listener Discovery Protocol version 2 - MLDv2 protocol, which creates a context in the multicast router located in the POA. Such information can then be transferred in advance from the old POA to the new POA if properly triggered by the instantiated Mobility Protocol (e.g. Fast Mobile IPv6 - FMIPv6), used for improving handover performance. Figure 21 summarizes a signaling scenario using FMIPv6.

The first message assumes that the Service Provider is responsible for informing the UE of which operators are serving the desired service, and through directory mechanisms the UE is able to find the new POA. (In the case of DVB technologies, this can be done resorting to the SI Tables, which already transport this kind of information.) After discovering the new POA, the UE establishes the new interaction channel while maintaining the old connection in a procedure classified as a soft-handover. Upon receiving the Fast Binding Update (FBU) and sending the Handover Initiate (HI) messages the old POA sends a Multicast Context Transfer (M-CTX) to the new POA in order for this to re-setup the multicast session. The Handover Acknowledgement (Hack) signals back the old POA that the transfer occurred successfully and the UE can therefore start receiving the multicast stream over the new POA.

4.3.2.2.3 Proof of Concept

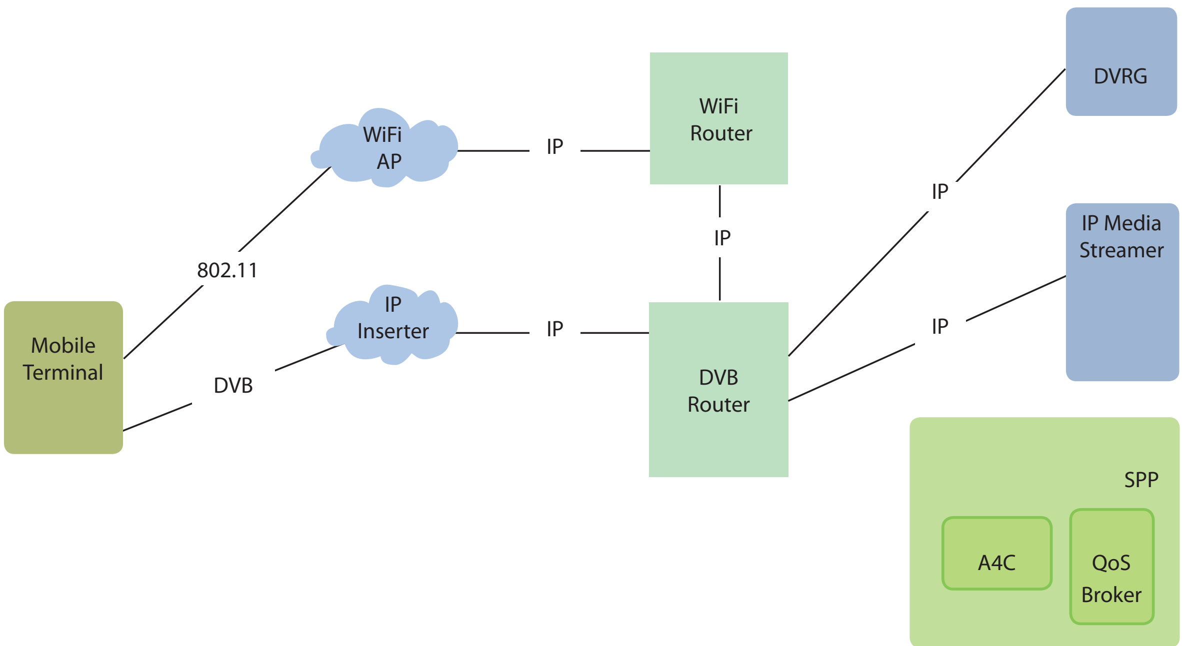


Figure 22 - Daidalos Broadcast Technologies Support

This architecture was developed and trialed in a testbed coupled with the demonstration of the research project IST-Daidalos [DAIDALOS]. A simplified representation of the testbed is presented in Figure 22.

4.3.2.2.3.1 Testbed

The DVB router can in fact be considered as an AR coupled with an IP Encapsulator/Inserter. The functional purpose of this device is to introduce the IP frames into the technology specific frames. DVB encapsulates IP into MPEG-2 TS (Transport Streams). The equipment, which supports this feature, is usually enabled with some processing capabilities that can be extended to include routing capabilities. In the framework of the implementation of this architecture, an inserter was further developed to perform Multi-Protocol Encapsulation (MPE) of IP packets, received from a DVB-AR, into MPEG2 transmission streams. This is performed using a specific Packet ID (PID) filtered by the DVB network interface at the receiver. Signaling, such as router advertisements, is also encapsulated to enable the configuration of the mobile terminals. The IP Inserter (Rohde & Schwarz DTV Data Inserter DIP 010) acts as a multiplexer for the IP contents provided by an IP enabled device with an Ethernet connection. The DVB Recorder and Generator (DVRG) acts like an MPEG-2 carrousel. The multiplexed frames are then forwarded to the Amplifier (Rohde and Schwarz amplifier R&S SV8000 with enhanced firmware), which broadcasts the signal to a DVB enabled Laptop that receives it and de-encapsulates the IP frames, or simply delivers the MPEG-2 contents to the end user. The DVB signal is modulated using the Pro Television Technologies DVB-T Modulator (PT 5780) and the software that converts IP into MPEG streams runs on Linux machines (P4 2.4 MHz CPU).

The software for the terminals and routers was also developed on Linux (kernel version 2.6.10), as it provides good compatibility for the software used in the tests. On the mobile terminal a Technotrend TT-DVB-T USB Budget receiver was used, as well as U.S. Robotics 11 Mbps PCMCIA Cards based on Prism2 chipset.

4.3.2.2.3.2 DVB integration performance

The results were obtained by generating a 4Mbps traffic flow with the MGEN tool. The AR (using WiFi set to 11 Mbps) has a throughput of 5.4Mbps. The reasoning for this particular choice of bitrates is to assure the minimum delay on the Inserter, as well a minimum number for the packet loss in both links (DVB and WiFi).

Table 3 shows the delay for the DVB link according to the bit rate in use. This delay was obtained after synchronizing both machines: the MPE, which is providing the service and the MN with the DVB receiver. Also, for the conditions indicated above, the maximum throughput was of 4216 Kbps (standard 5 MHz DVB-T/H RF channel).

Table 3 – Delay, Jitter and Loss for IP flows running over a DVB link

Bit Rate (Kbps)	Delay (ms)	Jitter (ms)	Loss (%)
4216	23	1	0.1
3938	26	1	0
1939	27	2	0
100	40	4	0

Delay and jitter increase with the decrease of the bit rate. Their variance also increases, as the system operates in a bursty mode. For a 64B/s flow, the first packets would suffer a delay up to 2 seconds, but the latest packets would have less delay to complete the burst, as they would stay less time in the buffers of the Inserter.

The session setup time of a multicast session is around 65ms and is mostly related to the Delay of the DVB link. Results obtained [Sargento 2006] under the same architecture for unicast services show setup times of 25ms. The added setup time is not a problem for normal operation, since it constitutes a once in a session event that does not propagate if a connection with the DVB-AR is maintained over time.

As previously mentioned, multicast mobility is undistinguishable from the common unicast mobility use case. Results presented in [Santos 2006] are in accordance to the results obtained for a handover of the return channel. Due to the lack of additional DVB equipment results on the handover between IPE routers were not possible to be obtained. Nonetheless one can predict that results should only be impacted by the delay of the DVB receiver in changing between channels (technology specific limitation).

Overall, the system performs functionally, with mobility and context transfer times on the order of some dozen milliseconds, but several details on software integration, namely driver, link abstraction and mobile IP stack issues had to be sorted out to achieve these results. In fact, the tunnel encapsulation abstraction proved to be critical to the whole process, and its integration with the mobility stack was complex in terms of software development.

The presented optimization for next generation heterogeneous networks capable of supporting, in the same infrastructure, unicast and broadcast technologies, including unidirectional broadcast networks, enables the convergence of Internet and broadcast systems. Under this proposed optimization, both unicast and multicast scenarios over heterogeneous technologies are integrated. This optimization is possible through an increased complexity of the Access Router which must now map IP QoS configurations into technology bearer configurations, support numerous QoS signaling protocols (both from a Service Platform and Legacy applications) and through the virtualization of complex interfaces that hide from the Core Network the complexity of unidirectional technologies such as the case of DVB.

Wireless and Broadcast operators are complementary and not necessarily competitors in the next generation networks market. Common service platforms for IP based network as the one described in the beginning of the chapter could potentiate synergies across services and operators, cutting cost in terms of Service Platforms and Core Network infrastructure.

Interoperation between layers built on top of different technologies becomes simple through the usage of a common technology such as IP and through the usage of similar service provision concepts such as the ones proposed by OMA.

The optimization here proposed can be discussed as an evolution of the trends present in MBMS and in LTE [3GPP TS 36.300].

5. Multicast to Unicast Switching

In the previous chapter architectural optimizations at the Service Platform Layer and at the Mapping between Core Network and Radio Access Networks were analyzed. In this chapter an optimization at the top of the Radio Access Network is described.

5.1 IP Unicast/Multicast to L2 mapping

The after birth split of IP Multicast from IP Unicast can be considered the root for much of the problems previously presented in section 2.2 . In IP Unicast, messages are delivered to a well-defined receiver (represented by an IP address) while IP Multicast is delivered to a well-defined group (also represented by an IP address) dynamically defined over time. Broadcast can be considered a special case of multicast where all nodes belong to a special group of all nodes.

In the most common communication scenario, Unicast appears as a function in which a sender pushes a message to a single receiver. This then leads to a mapping at L2 level of these addresses (as defined for instance for IPv6 in [RFC 2464]). But for Multicast/Broadcast the communication is no longer a simple function, as to one original message may correspond several receivers - more than one node can receive the same message sent by a single sender. Therefore IP routing is separated into two complete operations: Unicast communications, which is a one-to-one function of the source and destination, and Multicast/Broadcast, which is a one-to-many relationship.

5.1.1 Technological Considerations

It is therefore understandable the different implementation strategies for IP based Unicast and Multicast/Broadcast communications.

For instance, in switched environments, unicast packets are forwarded to a single node (the receiver), broadcast packets are forwarded to all nodes and multicast packets should be forwarded only to the interested nodes. Unfortunately this is not usually how things often work: e.g. most of today's Ethernet switches do not support the necessary functionalities to avoid sending multicast traffic to all ports. Switches would need to support IGMP/MLD snooping in order to correctly forward multicast packets, but this extra logic increases costs, and as such it is usually a dropped functionality by vendors.

But the largest hurdles with multicast are not in switched environments. In shared mediums such as the popular 802.11, where every node listens to the medium and filters its own frames, the difference between multicast and broadcast at the layer 2 blurs to a point where they are impossible to separate. The 802.11 MAC handles packet losses, but only for unicast transmissions; in broadcast/multicast neither acknowledgments nor retransmissions occur [IEEE 802.11] since no receiver or flow control exist.

Furthermore, Broadcast/Multicast transmissions in wireless environments require that the frames transmitted must reach all nodes in the maximum radius of the sender. The consequence is the need to transmit at maximum power, with implications on the transmission rate. This means that, for example, in the case of 802.11b, broadcast/multicast frames are sent at the base rate (for 802.11b this means only 1Mbps of the theoretical 11Mbps available) without any reliability mechanisms provided either by the IP or MAC layer. Considering that Next Generation Networks (NGN) aim to provide always best connected services (the same service will be made available in a heterogeneous network composed of technologies with different mechanisms for the transmission of Multicast packets) offering a High Definition Multimedia (HDMM) stream with reasonably high rates suddenly becomes very challenging.

As an example, consider a NGN operating an IPv6-based network (such as the one presented in 4.3) supporting DVB, 3GPP-MBMS and WiFi. Figure 18 (previously presented) represents in a very simplified manner a heterogeneous network, including the border routers, the QoS Broker (manager of QoS aspects) and the A4C server (authentication, authorization, accounting, auditing and charging) [Aguiar 2006]. Consider the case of a HDMM stream that is to be distributed through Multicast (it would be very expensive to distribute the stream over unicast in a network with a unidirectional DVB link), an example developed in the IST project DAIDALOS.

In this use case, lets consider terminals with only a single technology interface (terminals with more than one technology could be optimized through the mechanisms previously described), any user equipment (UE) in the DVB network shouldn't have any QoS problems receiving the flow, as the DVB channel has the means to provide more than enough resources for the HDMM stream. Unfortunately the same does not hold true for the 3GPP-MBMS networks, where the channel used to send Multicast traffic has a 384kbps bandwidth. For the WiFi network the same problem appears as Multicast is sent using broadcast frames, which are sent at the base rate (in the 802.11b case this means 1Mbps). The operator could request from the content provider three different multimedia streams for each of its Radio Access Networks, but that would mean increased exploitation costs. Another option would be for the operator to adapt the content to each of its networks using the Service Platform Media Delivery Functions, but those can only be used by a limited number of services.

5.1.2 Dynamic mapping proposal

But should a unicast stream have been used, it could have been able to deliver up to 14.4Mbps in the 3G network (considering HSDPA) and 11Mbps (considering 802.11b). Therefore it is apparent that motivation exists for the case of the transmission of IP multicast packets over unicast L2 links in such a way that the optimum channel is used. In the above mentioned scenario the operator would have been able to deliver the HDMM stream to its users with the best available QoS as long as the last hop could have relied in a Unicast Channel with adequate power control and retransmissions mechanisms provided by the underlying unicast layers. Nevertheless, in usage cases where several UE are listening to the same HDMM stream in the same Radio Access Network, the use of several unicast channels could lead to an early starvation of resources, thus breaking the all Multicast/Broadcast concept of resources optimization through sharing mechanisms.

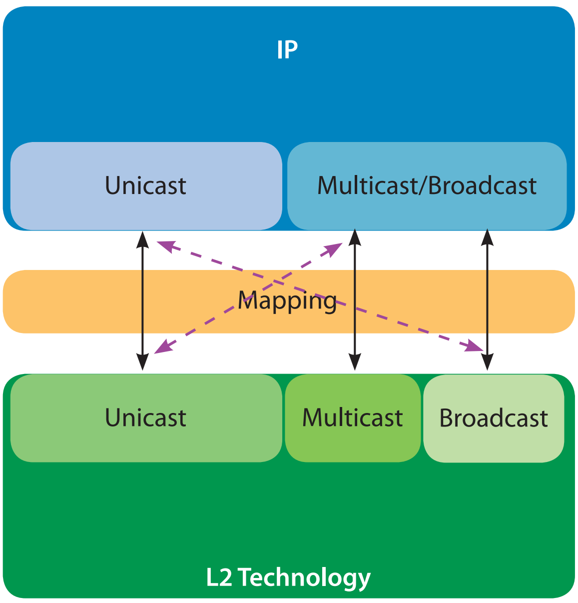


Figure 23 – Dynamic mapping concept.

The solution to these conflicting requirements is fortunately minimally intrusive, as the only modification required to the network is that the mapping between IP and Layer 2 is not statically defined but instead relies in a dynamic algorithm capable of choosing when is it worth forwarding packets in Unicast or Multicast/Broadcast mode, and selecting the best (technology-dependent) layer 2 channel. This concept is schematically presented in Figure 23.

The figure depicts that the interface between the IP Layer (composed of IP Unicast and IP Multicast/Broadcast) and the Link Layer (Unicast, Multicast and Broadcast carriers) can be made through a dynamic mapping that can cross the established on-to-one correspondence between IP modes and L2 Technology bearers.

By breaking this statically defined mapping QoS can be improved in particular situations for services deployed via IP broadcast/multicast. This cannot properly be called an optimization of resources since it actually uses more resources. But can be considered an optimization of the service as it provides better quality for services, under these specific conditions.

5.1.2.1 L3/L2 Switching Control

This optimization requires that multicast routers support a dynamic mapping between IP Multicast groups and L2 Unicast/Multicast/Broadcast. The mapping must be controlled by an algorithm that should not only take into consideration the number of listeners, put also the transmission power requirements, the bandwidth required, subscribers profile and subscribers feedback. For NGN, this algorithm could be as complex as required, incorporating operator policies, and being a function of the technology features related with unicast vs. broadcast channel usage. For scalability and efficiency, dense listener environments would usually map IP multicast into the standard Multicast/Broadcast channels. Nonetheless this sparse/dense threshold must be further evaluated, being not only technology dependent, but also dependent on current traffic flows and user-profiles. Section 5.2 will make such an analysis.

This dynamic mapping aims to optimize overall service usage. As such, the algorithm should consider QoS requirements of this multicast stream, and the network measurements associated should impact the algorithm. Although several works in the area of QoS measurements in IP Multicast environments exist [Bin Wang 2000], none addresses the specificity of this approach, as they center themselves in an end-to-end problem while here it is intended to work only in the last hop - where bottlenecks usually reside and where the dynamic mapping can actually be performed.

For heterogeneous environments, we require a media independent protocol capable of feeding network level reports to the default router. For multimedia applications, RTCP [RFC 1889], seems quite appropriate (albeit coupled to RTP), but would become a superfluous protocol for any other application. On the other hand, group management protocols such as MLDv2 (IPv6) cannot be avoided. The MLDv2 protocol is used to periodically signal listeners and routers subscription information. Extensions to the MLDv2 protocol are hereby defined, integrating extra information on the reception quality of each user. An MLDv2 extension is an appropriate choice since this is a scalable protocol independent of the transport layers, and can provide agnostic QoS information.

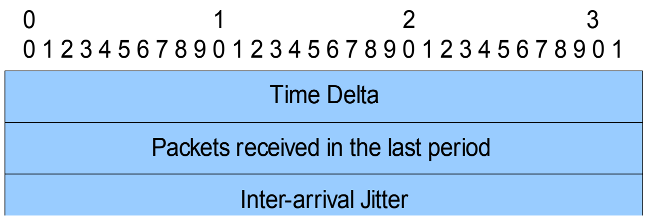


Figure 24 - Proposed MLDv2 QoS Extension

The «The Auxiliary Data field» of the «Multicast Address Record» (Section 5.2.10 of [IETF RFC 1889]) is defined to incorporate information such as time since last MLD message (Time Delta), packets received in the last period (since previous MLD report) and inter-arrival jitter (see Figure 24).

Since MLDv2 messages are periodic, the multicast router can evaluate its listener's data through the QoS Extension. This enables the router to make approximate calculations on the QoS of each and every authorized receiver. The results can then be included in the decision algorithm.

Based on this information, the operator can therefore implement algorithms that are able to trade service quality and power efficiency to a given user (using a unicast L2 bearer) by resource efficiency to multiple users (using a broadcast bearer), without changing its IP multicast service provision infrastructure nor incurring intrusive signaling at the core control plane.

Besides the increased QoS provided by the use of a Unicast Channel, the use of a L2 Unicast channel can also assist the operator in terms of security. At the L2 level, this avoids group security problems, replacing it by a simpler point-to-point security problem, easier to handle by security experts.

5.1.2.2 Prototype evaluation

In order to evaluate the feasibility of this method a prototype was developed. The test network was made of several Linux boxes, implementing a streaming server, a multicast router (running our software) and several terminals accessing the network via WiFi (Figure 25). WiFi [802.11b] has a specific multicast channel, and thus the software was developed for exploiting this channel. Note that the situation with (e.g.) WCDMA environments would be similar, but with other technology specific broadcast bearers.

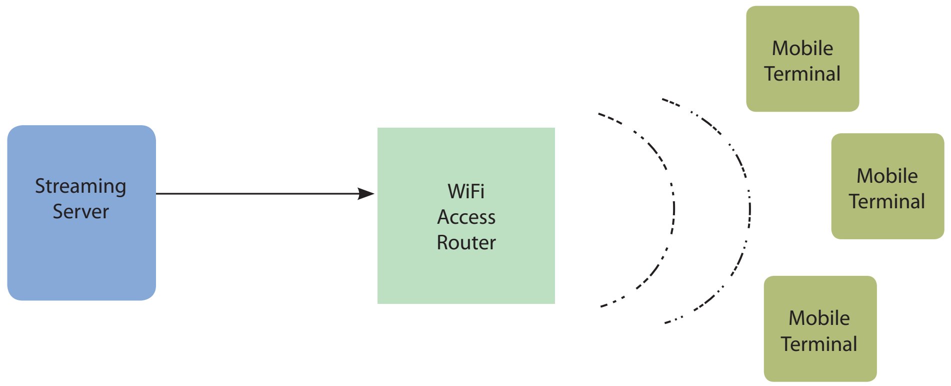


Figure 25 – Prototype evaluation test bed.

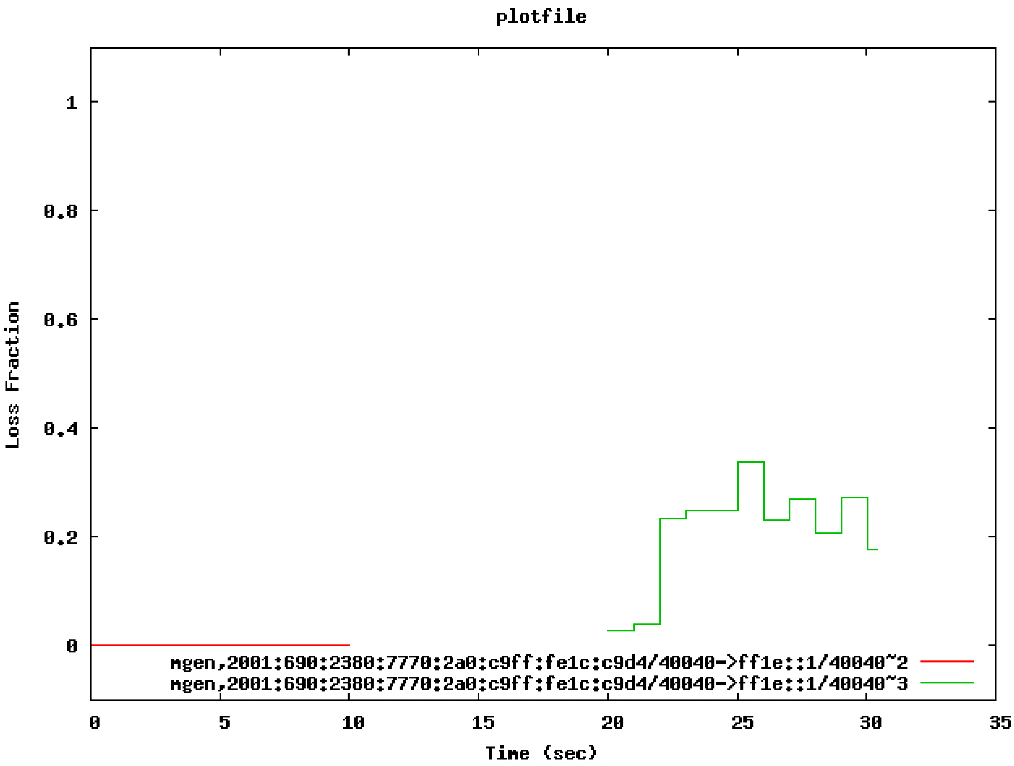
The software developed consisted of a modified version of the multicast router MRD6 [MRD6], to which we further added a listener's database, a conditional forwarder and a basic algorithm that controlled the conditional forwarder. In more realistic environments, this algorithm would be configured by a policy mechanism, but in our case was hard coded. The prototype code is available under the GPL license. Note that the client application software remains unmodified and the terminals do not perceive the operation of our dynamic switching mechanism.

The tests conducted in this platform consisted of sending 1Mbps IPv6 Multicast flows from the streaming server to a variable number of terminals using both VLC [VLC] and mgen-4.2b6 [MGEN].

VLC was used to analyze the behavior of the dynamic mapping and (with the exception of problems associated with packet loss, described below), VLC does not perceive any change on communication when dynamic switching is performed (changing between the L2 multicast channel and the unicast channel of WiFi).

The mgen stream test lasts 10 seconds and is rebroadcasted every 20 seconds. In the 10 seconds window between the end of a stream and the beginning of the next, a new terminal joins the multicast group. The IP multicast listener Join message triggers the dynamic mapping control algorithm (a very simple algorithm was used for illustration purposes):

```
bool mc2un_base::is_it_broadcast(const inet6_addr &grp) {
      if (flows active on broadcast  == 0 ) AND (current flow bandwidth < TECH_LIMIT)
        if(listeners.count(grp)>=THRESHOLD) {
                return true;
        }
        return false;
}
```



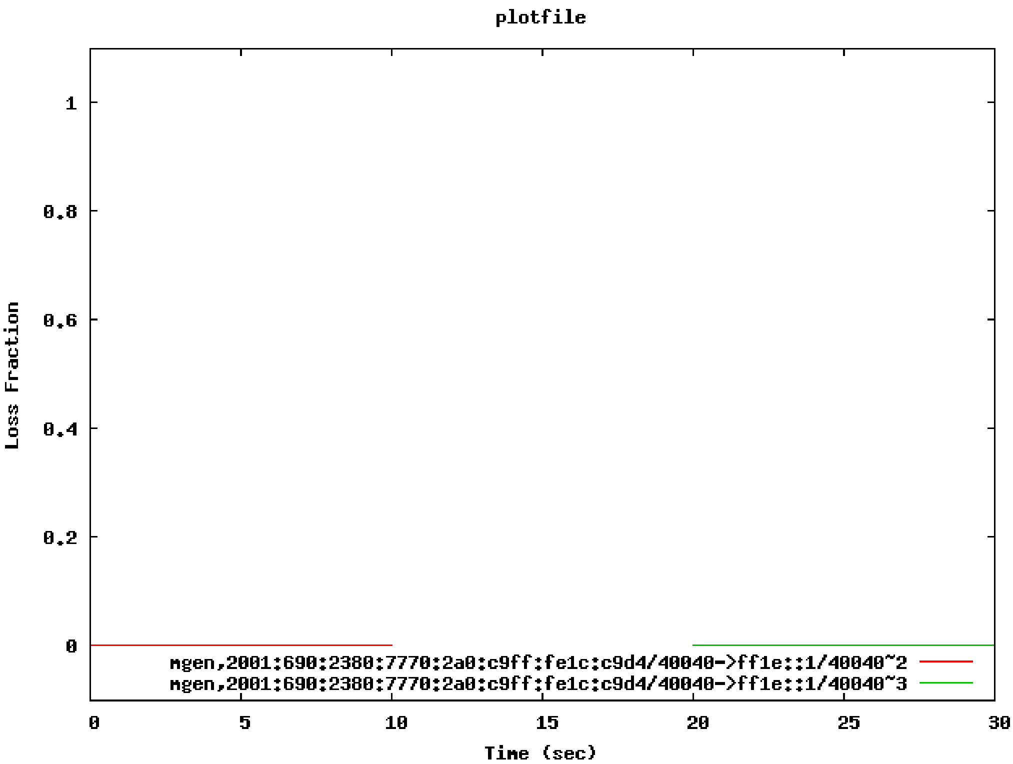
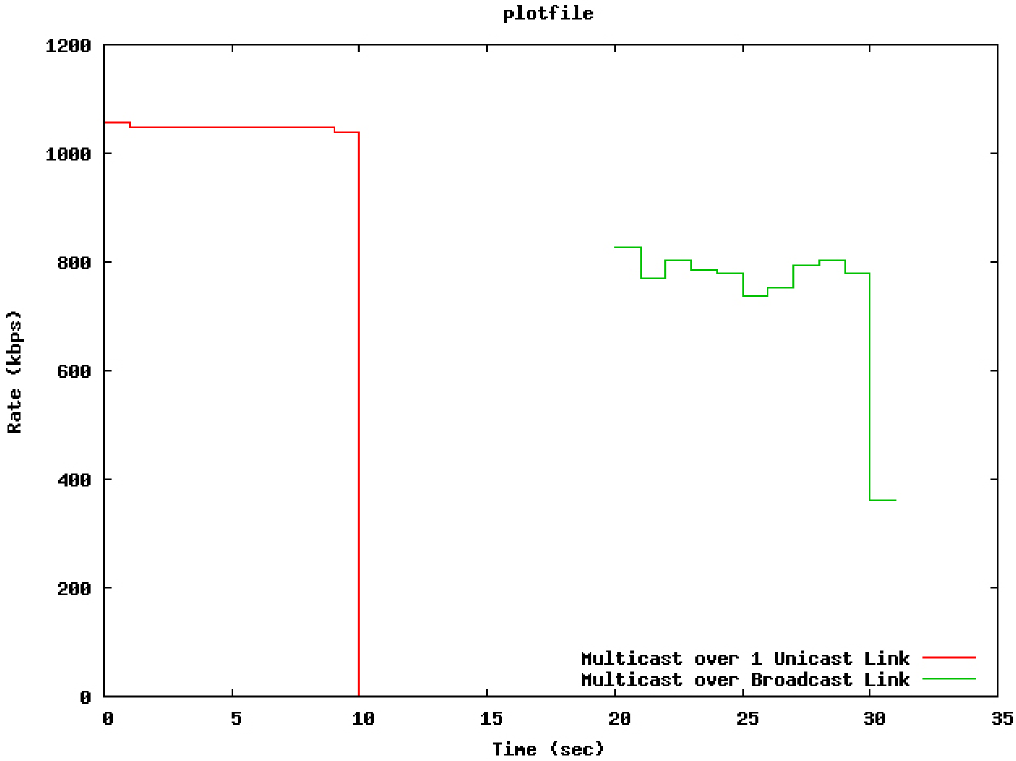


Figure 26 - Packet Loss for a multicast stream over a WiFi unicast channel and multicast channel (A) and over two unicast links (B)



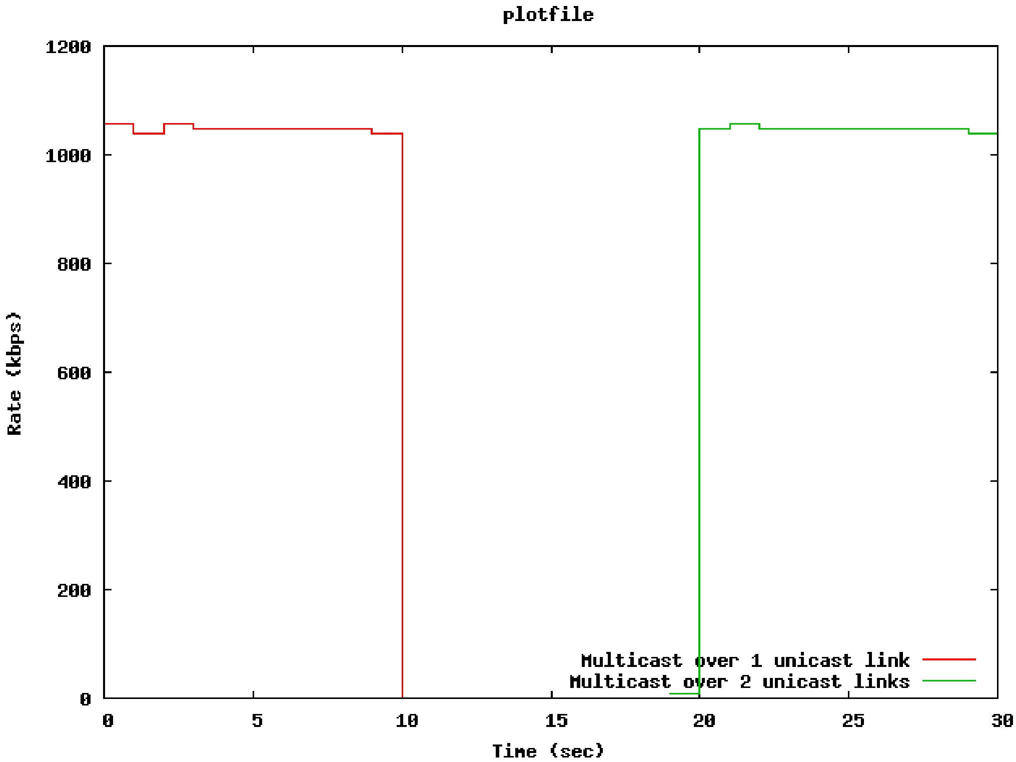
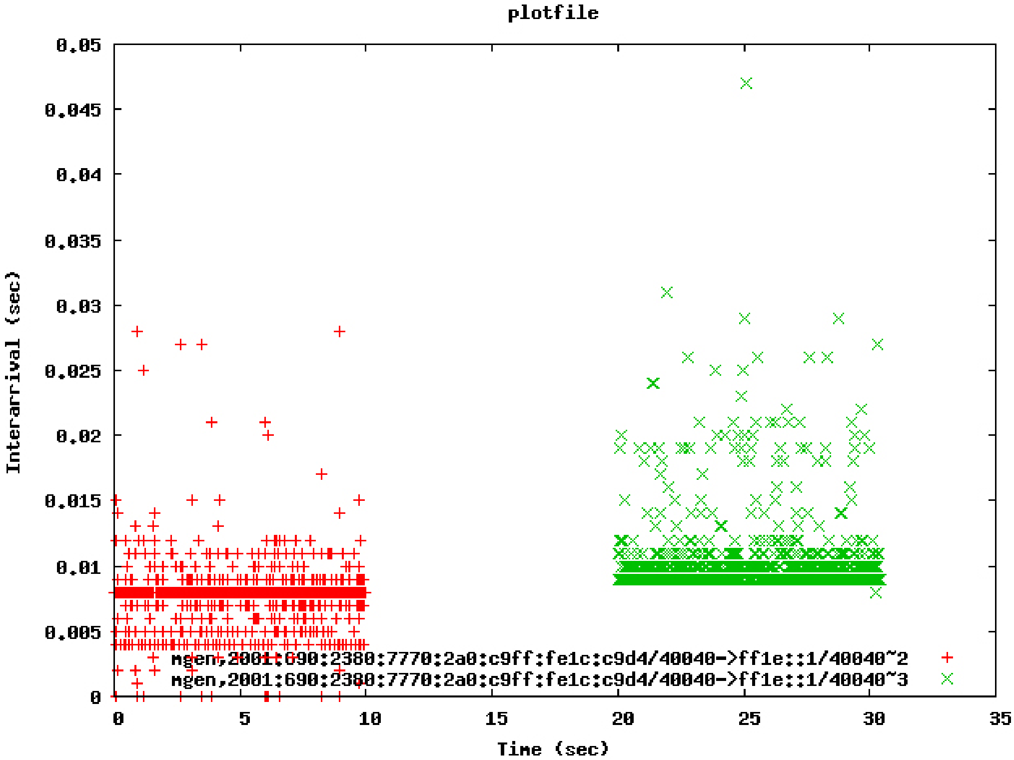


Figure 27 – Packet Rate of a multicast stream over a WiFi unicast channel and multicast channel (A) and over two unicast links (B)



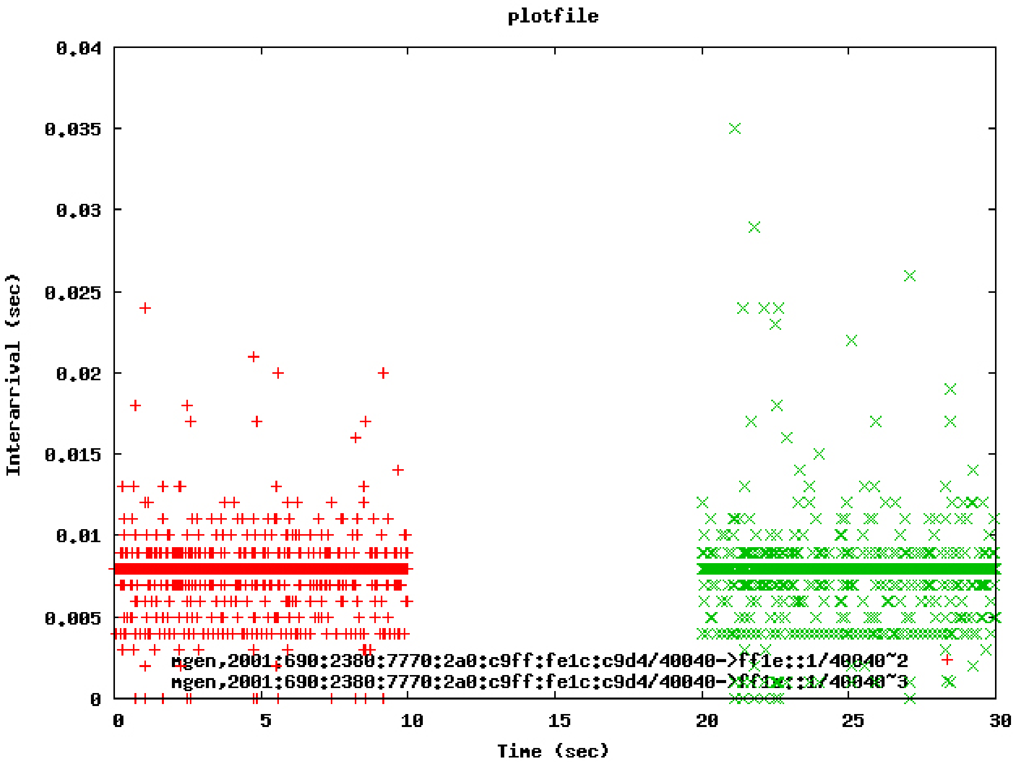


Figure 28 – Packet Inter arrival of a multicast stream over a WiFi unicast channel and multicast channel (A) and two unicast channels (B)

The results of the tests are presented in Figure 26, Figure 27 and Figure 28. Although only one test run is shown, the results were not statistically different between the multiple test runs that were done.

The figures start to show the 1Mbps IP multicast stream as received by the first of the listeners. Being the first listener, the router algorithm decides that it should receive the IP multicast flow over a L2 Unicast link. As such the available channel bandwidth and L2 mechanisms (such as retransmissions) provide a reliable link for the delivery of the IP multicast stream. As soon as a new listener joins the group (at 20 s), the algorithm opts for optimizing access resources and switches the mapping to the standard Multicast/Broadcast channel, which transmits at the base rate of 1Mpbs, using therefore the maximum capabilities of the technology. In our physical scenario packet drops occur at a 20% rate, which without any recover mechanism (such as FEC or retransmissions) can be considered a normal value considering that 10% are accounted by overhead of the LLC, 802.11 and PLCP headers (this overhead exceeds the available bandwidth on the multicast bearer).

Figure 28 shows the difference of behavior of the Multicast/Broadcast channel (versus the unicast channel). Although similar, the multicast channel has a dispersion of inter arrival times consistently shifted upwards several milliseconds. This behavior is different of the unicast transmission, where retransmission mechanisms in L2 play an important role in recovering from packet loss, shown by inter arrival times of less than the base 10ms (Figure 28), meaning that retransmitted packets where sent meanwhile.

5.2 Analysis of the impact of a dynamic L3/L2 Switching Control Mechanism in Mobile TV services

The previous section describes a use case scenario where multicast sessions can be mapped into lower level Unicast or Broadcast bearers depending on the service provision logic of the Network. In order to further study this use case, a service simulation tool was created where the relationship between service subscription, service consumption, network service provisioning and network planning could be studied. The emphasis of such study is to determine the amount of opportunities that occur in a Mobile TV provisioning scenario, to switch the service from a multicast channel into a unicast channel and vice versa. In this analysis it is considered that the mobile TV service is initially served through a unicast channel and that at a given threshold (based on the RAN technology used) the service is switched to a multicast channel in order to optimize resources. The simulator provides a snapshot of an instance in time where service and subscribers have converged in to a stable system. This assumption therefore disregards subscribers joining and leaving the system, but it assists in defining switching thresholds for central algorithms.

5.2.1 Service Usage Simulator

A new simulator tool had to be built for the purpose of this study. The reasons that led to the use of a custom simulator were:

- The simulation would not have any packet transfers. The purpose of the simulation is to empirically study the probabilities of the use case for Unicast to Multicast Switching to happen regardless of the traffic patterns in the network.
- Distribution of Nodes and Points of Attachment are considered important. The possibility of incorporating into the simulation actual data coming from the real world could be important in order to validate the concept.
- There are no "packet concepts" involved. The simulation takes no consideration on the service being provisioned, neither on the protocols being used nor on the load of the nodes.
- The simulated nodes would be static. Again the purpose is to evaluate at a given moment in time, therefore there is no need to have a simulator that moves nodes around.

Given these premises, it was developed a service usage simulator that creates situations where subscribers, cells and services can be deployed, associated and evaluated. The simulator features the possibility of loading cell and terminal positions from external sources such as KML files (supported by Google Earth) enabling the user to easily refer back to real life situations. Besides the ability to load from KML files, the simulator can also store distributions of cells and terminals created in the simulator into this file format enabling an easy visualization tool for debug and reference purposes. The simulator also encompasses a configuration file for the description of services based on shares.

In its current version the simulator supports Uniform and Normal distribution of cells and/or terminals. Services are distributed randomly across terminals based solely on their share of the market. Although not used in this simulation, the simulator supports terminals with several interfaces/technologies, which can ultimately lead to simulations on interface selection based on service consumption. The simulation takes place in a subset of the earth's geographical space with disregard for elevation parameters and makes use of the Haversine Formula [Haversine], which is a commonly used method for calculating the distance between two points on a sphere. While the Earth is not perfectly round, the calculation results are close enough for the purpose of these simulations, and provide a more accurate coverage algorithm which is solely based in the distance from a node to base station than to have simply considered a geometric plain environment. The subset area where the simulation takes place is defined in the configuration file as a square area defined by its southwest and northeast coordinates but can be extended to several such areas. Cells and Terminals are to be placed inside such subset although the generator can make use of different subsets (e.g. for a given simulation terminals can be normally distributed inside this area using two different subsets, thus creating two different “hot zones”). The Normal Distribution used is based on libboost [BOOST] random distribution libraries [BOOST DIST] normal distribution with the mean parameter equal to the center of the subset area and a configurable standard deviation. There is also a Pseudo Uniform Distribution that distributes nodes according to a configurable distance, with the first point being the most southwest point of the subset. The simulator records associations between terminals and cells, terminals and services (terminals play the role of subscribers), service characteristics (such as bandwidth needs and transport characteristics (multicast/unicast)). The simulator was develop in C++ and follows the Object Orientation Paradigm, thus enabling for the easy reuse of the simulator code in the development of new components for new scenarios. The Simulator code is highly portable as it depends solely on the libboost library (for mathematical functions) and libkml [LIBKML] (for KML file support).

The simulator tracks several variables (see Table 4), which can be used to produce reports.

Table 4 - Simulator Variables

Access Point	• The Terminals associated • The Subscribers per Service • The Bandwidth available (unicast and broadcast) • Terminals being served over unicast and multicast • Terminals denied access to unicast/multicast Service (e.g. CAC mechanisms denied access due to insufficient network resources) • Multicast Services available
Terminal	• Access Point to which it is associated (if it is associated) • Interfaces available (each containing the network resources being used)
Service	• Network resources necessary • It’s type (unicast/multicast) • The list of Subscribers/Terminals

The operation of the simulator consists of generating cells and terminals positions in accordance to the configured distributions followed by the placing cells and terminal in the configured map. After that step the terminals are associated to the closest cell and are randomly associated to a service based on the services share. Finally a report is produced in CSV file format containing the desired information. (see Figure 29)

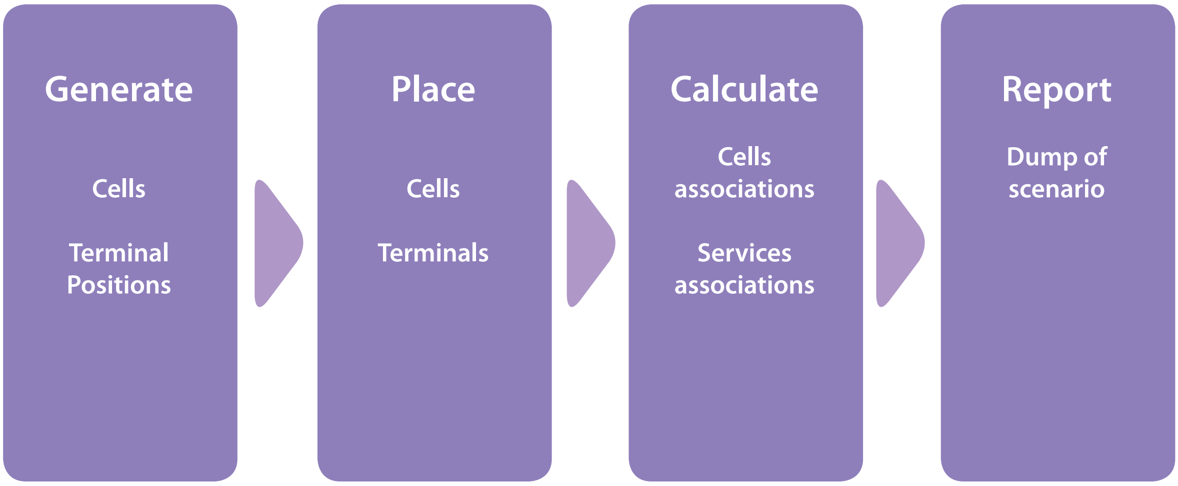


Figure 29 - Simulator Workflow

Statistical analysis is later produced in a spreadsheet software package.

5.2.2 The Scenarios

Several scenarios were considered for the simulation. These scenarios can be subdivided according to the network technology used: WiFi and 3G. All the scenarios take place over a 4km^2 area on the city of Aveiro, Portugal. Scenarios are further characterized by the amount of terminals involved (100, 150, 200, 250 and 300). The number of terminals involved corresponds roughly to a range of 1% to 5% of the population of Aveiro. This range is considered an optimistic value considering 2007 penetration values of Mobile TV in Europe [EC IP/07/1118]. In all the scenarios it was considered the availability of 4 services corresponding to the 4 different Free-to-air TV channels available in Portugal. Main scenario characteristics can therefore be summarized in the following table:

Table 5 - Scenario characterization matrix

	3G Network	WiFi Network
100 terminals	4 services	
150 terminals		
200 terminals		
250 terminals		
300 terminals		

The 3G network scenarios are characterized by cells with a 1km radius and an inter-cell distance of 1,5km (in order to guarantee maximum coverage). While the WiFi network scenarios cells have a 60m radius and inter-cell distance of 100m. Cells are distributed uniformly in a grid around the area in order to perfectly cover all terminals.

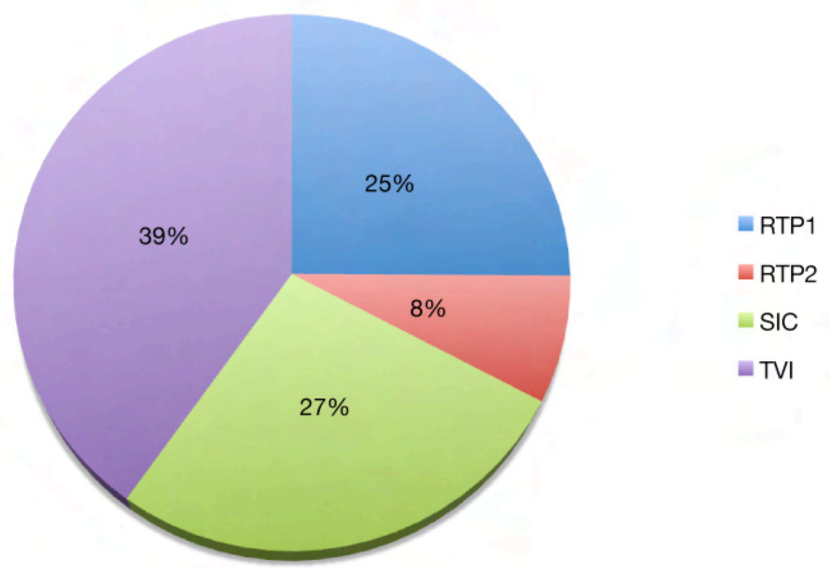


Figure 30 - Service Distribution amongst Subscribers

The 4 different Mobile TV services were considered according to the share ratings provided by marktest [MARKTEST] for the first week of June 2009. These 4 Mobile TV services and shares intend to depict a real service-provisioning scenario where a very small number of channels account for more than 2/3 of the services being consumed (Figure 30). It is assumed that all 4 MobileTV services have the same QoS requirements and service characteristics, although they pose no dependency in this study.

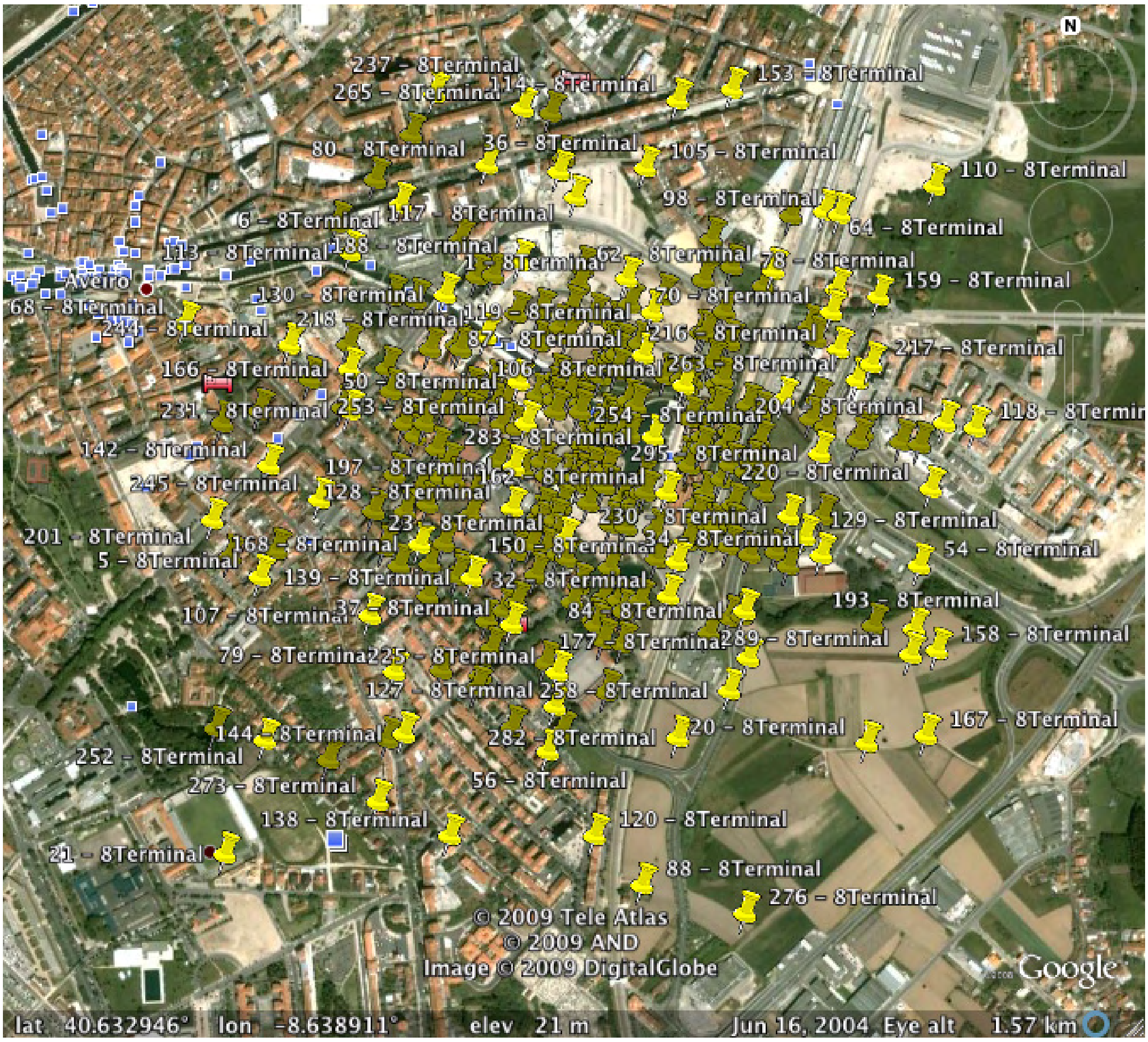


Figure 31 - Example distribution of 300 terminals

In each run of the simulator, terminals are distributed normally around the center of the area with a standard deviation of 250 meters (see Figure 31), each terminal is randomly associated to a MobileTV service subscription and is associated to the nearest Access Point.

For this simulation the output consisted of the list of Access Points involved in service provisioning with information on: the number of Terminals associated to the given Access Point, the number of Stations served with a multicast service (in the scenarios considered this is equal to the amount of terminals as all terminals are consuming a service), the number of Multicast Services provisioned and the number of Terminals receiving each of the available Services.

Each scenario was simulated 5 times and results presented are average values. Random distributions of terminals and services (cells are not randomly distributed) have an error margin of at most 10%.

5.2.3 Analysis of the Results

The analysis of the simulation results will start with the scenarios based on a 3G Network, as they constitute the state of the art in deploying Mobile TV services. Scenarios based on WiFi networks will be analyzed last, taken into consideration that next generation Radio Access Networks tend to smaller cell radius.

5.2.3.1 3G Network

The first result to be considered is the availability of services throughout the network.

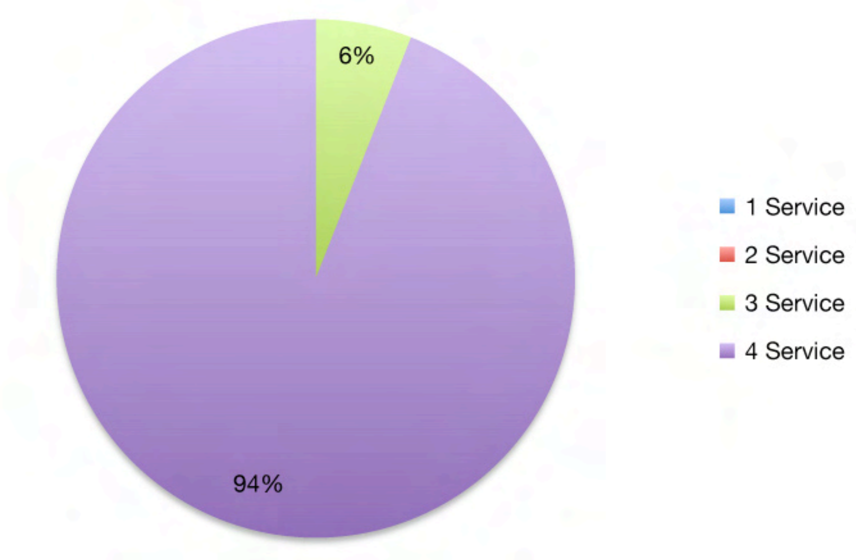


Figure 32 - Number of Services available per cell

In Figure 32 it can be seen that around 94% of the Access Points are provisioned with all the available services (4), that is, 94% of the Access Points, for each service, have at least 1 associated terminal. This result is due to the fact that each Access Point serves a very large number of terminals, therefore usually conveying for a very broad spectrum of possible service subscriptions. The density of the cells in terms of terminals per cell is next depicted.

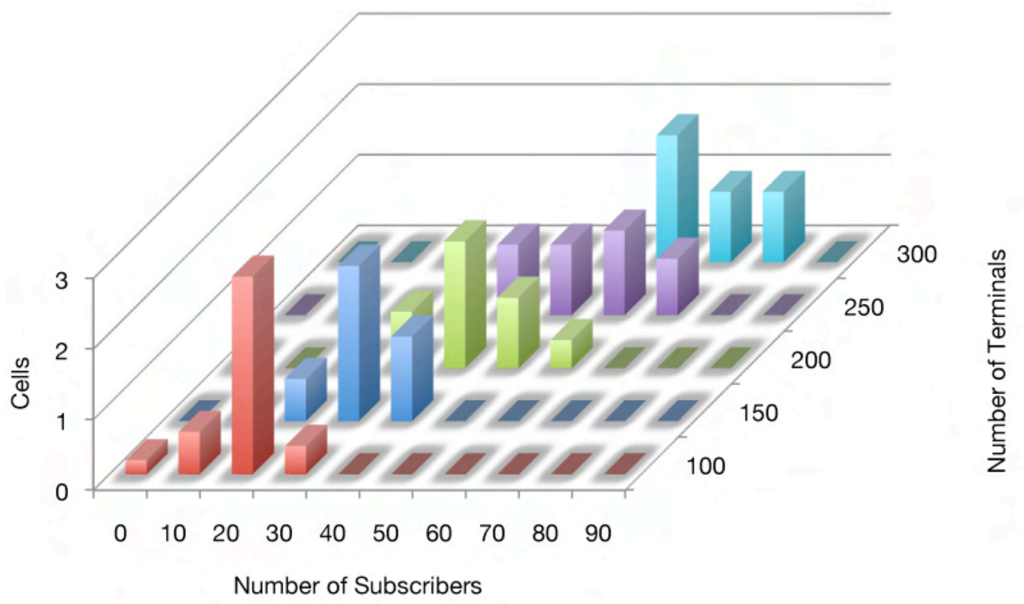


Figure 33 - Number of cells with a given amount of terminals associated depending on the global population of terminals.

In Figure 33 it is presented the average number of cells (in Y coordinate) within a given interval of Terminals associated (in X coordinate) as the population of terminals increases (Z coordinate). From the graph we notice that as the number of terminals increases so do the number of cells with higher density. A higher number of densely populated cells, in which terminals subscription is distributed according to Figure 30, ultimately leads to a situation in which all services are consumed in a cell by more than the number of terminals necessary to consider switching. In such situation the system is stable, with most of the terminals/subscribers receiving the Mobile TV service through a broadcast channel (assumed that it could exist, in a properly designed network).

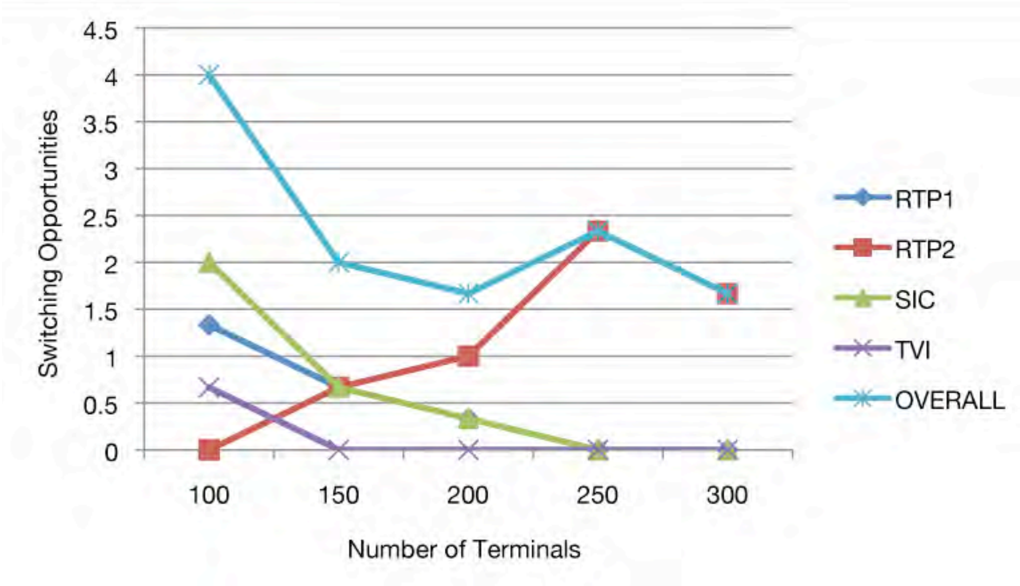


Figure 34 - Number of switching opportunities in the 3G Scenarios

The purpose of the simulation was to study the situations in which a switch from broadcast/ multicast channel to unicast channel might occur (and vice-versa). Given that the optimization proposal and prototype validation was studied and built on WiFi networks, the 3G network simulation had to be based on the studies on power control previously mentioned (section 2.2), in order to analyze what is expected to be the trigger point in 3G networks. It is hereby defined that the switching threshold used for layer 1 purposes (as described in the referenced studies) can also be used as the switching threshold for the purpose of this simulation. The layer 1 mechanisms described in such studies are in accordance to the previous L3/L2 mapping proposal, as it ultimately would lead to the same end result (use of several DCH channels vs. use of a single FACH channel).

The graph in Figure 34 shows that switching opportunities decrease as the number of terminals increases. This is easy to explain: the larger amount of terminals and limited number of services means that a greater number of terminals/subscribers in a dense system, will already share the same multicast channel in order to save network resources. This trend is particularly visible for Service's 1,3 and 4, but is nonetheless contrary to the behavior of Service 2. Service 2 distinguishes itself from the remaining services for being the less popular of the services, with an average subscription rate of less than 10% while the remaining services have averages above the double of this service (Service 1 and 3 around 20% and service 4 with 40%). This differentiating factor can also be seen in the next graph.

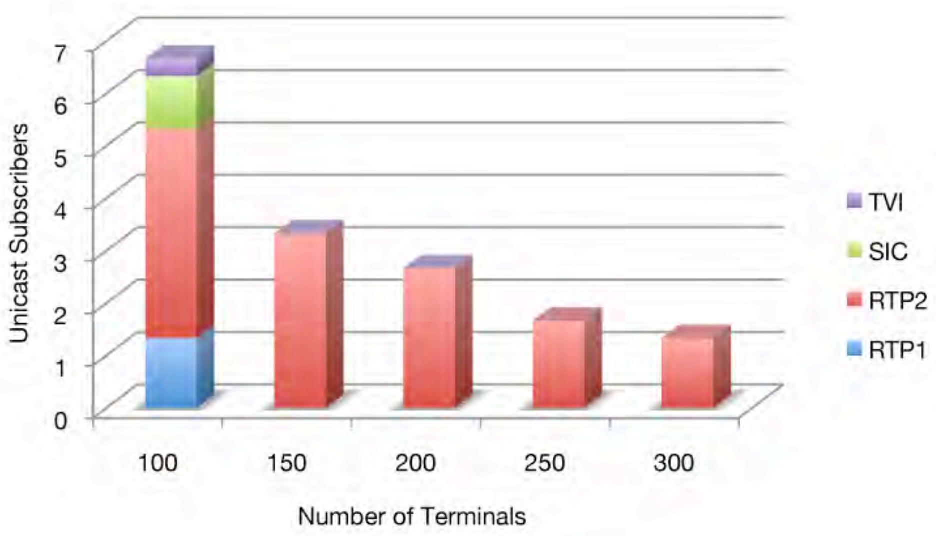


Figure 35 - Number of unicast subscribers per Service in the 3G Scenario

In Figure 35 a decrease in the number of subscribers served by unicast can be seen, which ultimately leads to only Service 2 having subscribers in a position where a switch might occur. With no unicast subscribers left and the number of terminals increasing such as shown in the higher number of cells with higher number of terminals of Figure 33, it is understandable that a turning point takes place for Service 2 somewhere between 62,5 terminals/km^2 and 75 terminals/km^2 (250-300 terminals in the scenario). This is the point where terminals receiving Service 2 through a unicast channel (because they were very few) have all moved to a broadcast/multicast channel (were more terminals can be served by a single broadcast/multicast channel).

5.2.3.2 WiFi

The main difference in terms of the simulation performed between the 3G and the WiFi networks is the amount of cells involved, due to the far smaller size of the WiFi cells. This sole factor is responsible for different results when compared with a 3G network.

As previously done, an analysis of the distribution of services through the network is first presented (Figure 36).

Although more than half of the cells have all the four services, they are far less than what was the case in 3G networks (94% of the cells had all the services). Even of more interest is that 16% have two or less services available (meaning that some services are yet to be subscribed by a terminal in that cell).

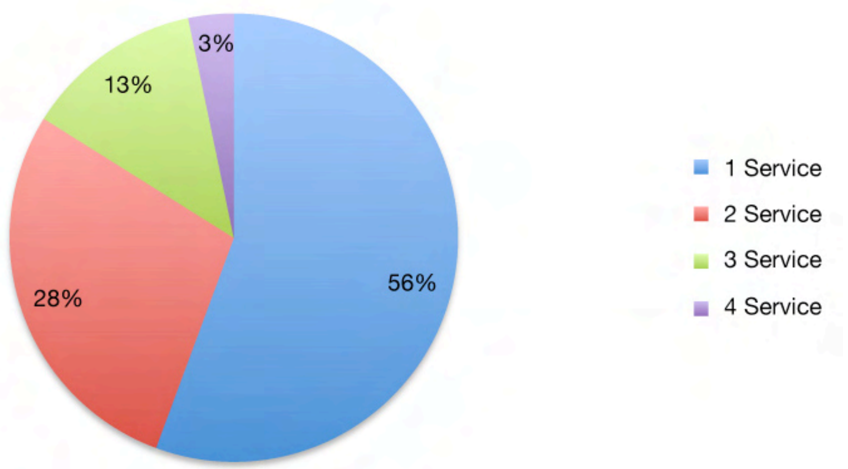


Figure 36 - Number of Services per cell

Since the distribution of terminals is probabilistically the same, as is the service distribution amongst terminals, this difference must be accounted to the different properties of the cells technologies (in the case of this simulation, this means the cell radius). The next graph will help to further understand this situation (Figure 37) .

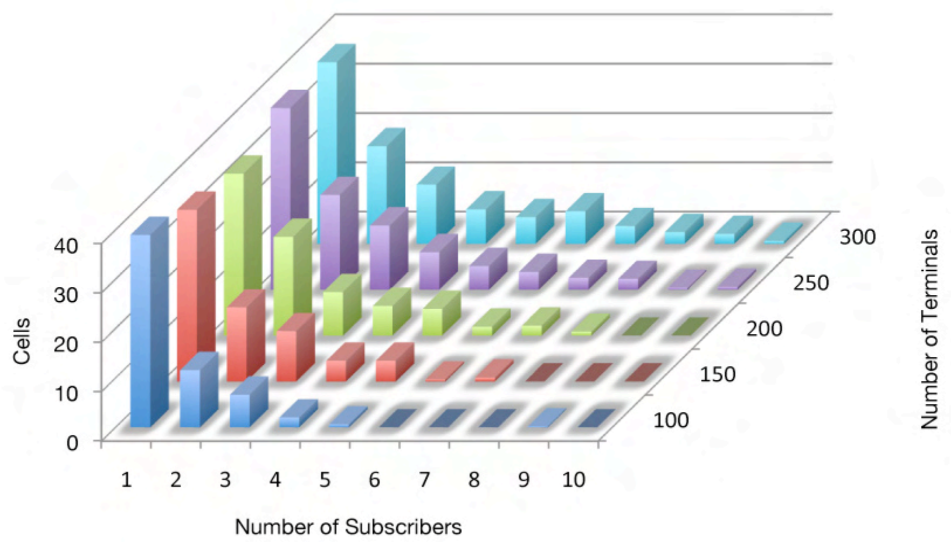


Figure 37 - Number of cells given an amount of terminals associated

Again this graphic shows a behavior much different from that of the 3G-network simulation with cell density growing but not shifting right towards a global amount of very dense cells. What actually happens is that the number of cells with a single terminal is maintained throughout the simulation in spite of increased number of terminals involved. Even though a reasonable percentage of cells has increased its density, this effect is more than compensated by the increased number of cells involved due to the addition of new terminals. Also noteworthy is the fact that the density in the WiFi scenario represents a tenth of the density presented in the 3G-network scenario. This scarcity of terminals per cell ultimately leads to the next graph.

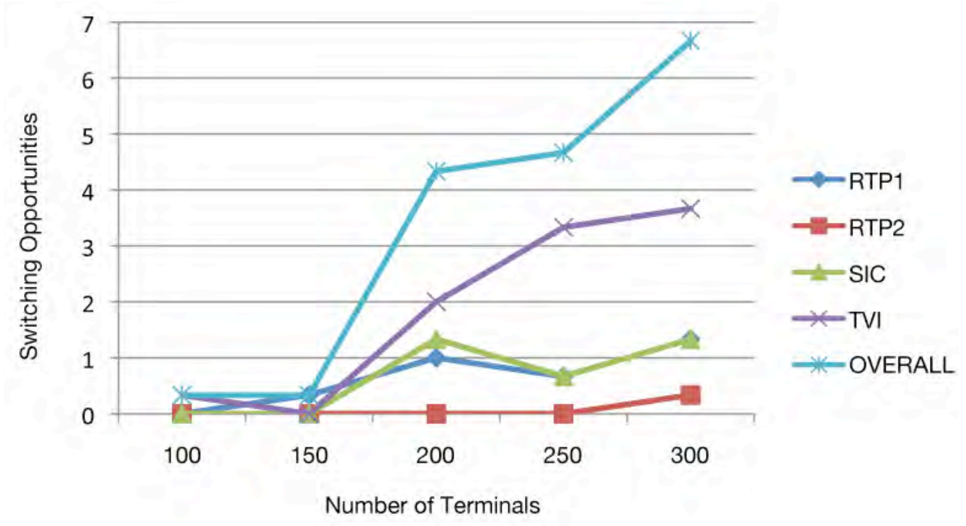


Figure 38 - Number of switching opportunities in the WiFi Scenarios

The trend in Figure 38 is the opposite of Figure 34, with an increasing number of opportunities appearing mostly for the most popular service (Service 4). Again we must refer to the number of unicast subscribers per service to understand these results.

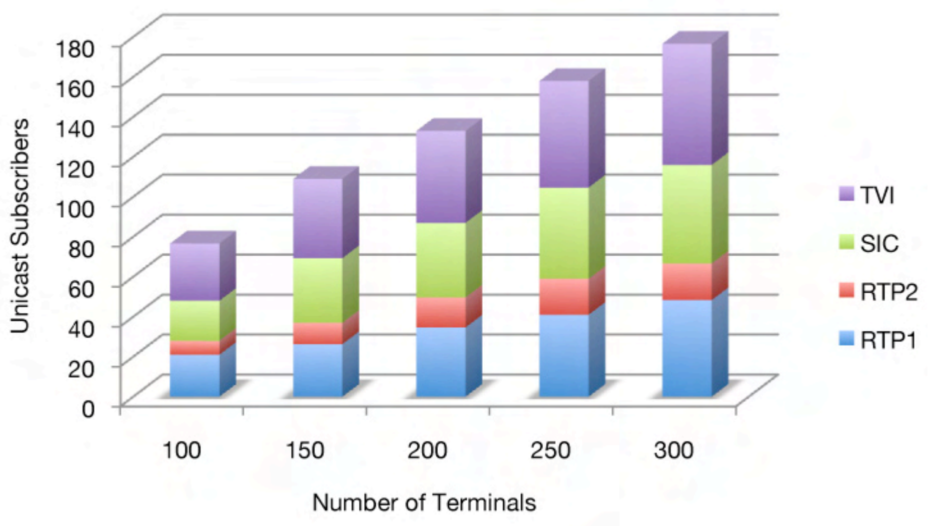


Figure 39 - Number of unicast subscribers per Service in the 3G scenarios

What is seen in Figure 39 is that, as the number of terminals increasess, so does the number of unicast subscribers at a rate proportional to the service share. This is a behavior quite different from the one presented in Figure 35. In the case of the 3G scenarios all cells deployed were handling more than one terminal. This does not apply to the WiFi scenario.

Given the low coverage number of subscribers per cell, this translates into higher opportunities for switching from unicast to multicast (and vice versa). This means that ultimately there will be more Service 4 subscribers with a unicast service than those of Service 2.

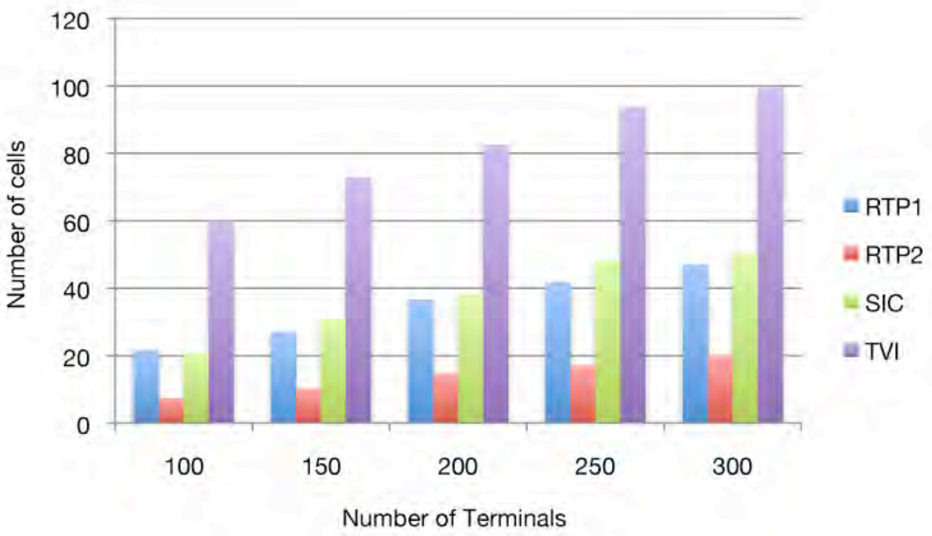


Figure 40 – Distribution of terminals amongst services

As the number of terminals increases so did the area covered by terminals (as the number of terminals increases, so does their dispersion) and consequently the number of cells involved. Ultimately this means that inner cells are serving subscribers through multicast and outer cells are serving subscribers using unicast. Also as the number of terminals increases, switching mostly happens at the cells positioned not in the outskirts or center of the area studied, but at an intermediate zone.

5.2.4 Conclusion

The main conclusion from this simulation work is that assuming a rational allocation of resources and by an adequate algorithm the number of switching opportunities is relatively low (in average well less than 5% of the global population). The second most important conclusion is that the cell technology, through its cell radius, has a dominant impact in the amount of switching opportunities. From the results one can insight a heuristic between the number of switching opportunities and the density of terminals per cell, expressed by the number of service subscribers per area covered by the cell. Figure 41 reformulates such a heuristic.

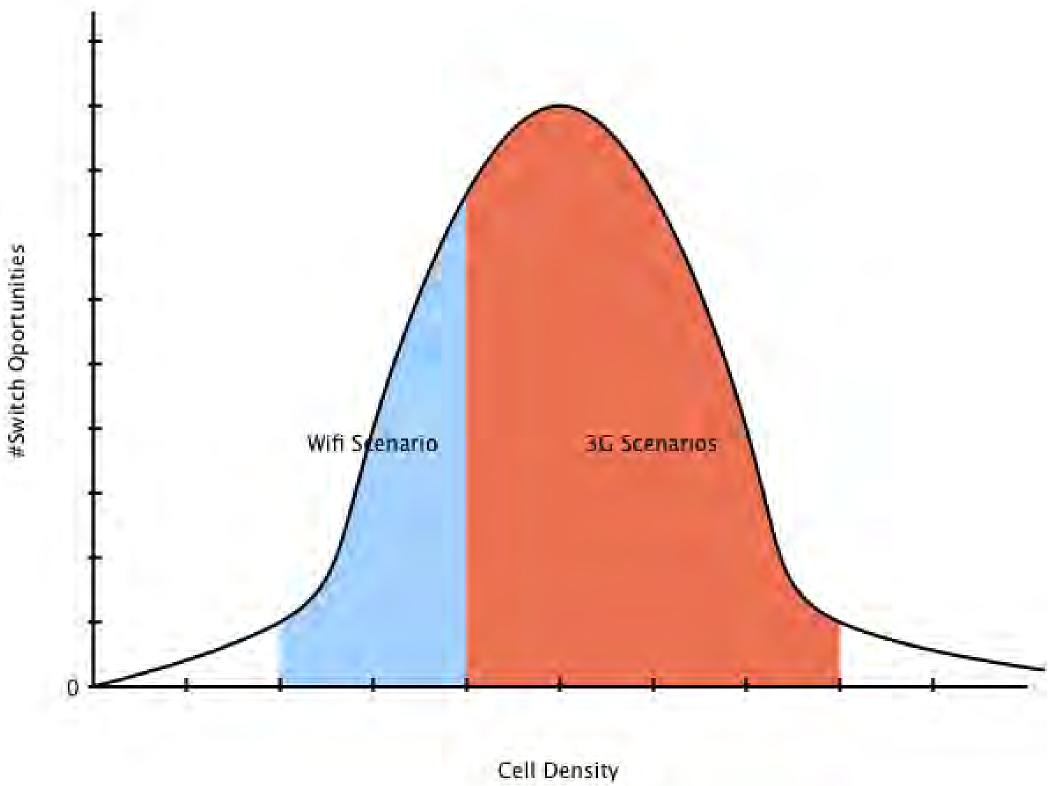


Figure 41 - Switching Opportunities per Cell Density

In the figure, the areas corresponding to each of the considered scenarios are shadowed. In blue (corresponding to the WiFi Scenarios) we have an increase in the number of switching opportunities as terminals increase the density of cells and are switched from unicast to multicast. The WiFi Scenarios are characterized by a relatively large number of cells with very low terminal density. As population grows in these cells, it ultimately leads to the need to switch users into broadcast/multicast channels at a very moderate rate. The general trend in the WiFi scenarios is to have more cells involved. On the other hand, the increasingly higher cell density characterizes the 3G Scenarios, where ultimately all terminals are serviced through Multicast. The tipping point of this graph cannot be found as an exact number as it depends on several factors besides the cell density, which include the number of services involved and their subscription distribution.

6. Network Middleware – the Access Router

6.1 Introduction

In the previous chapters several architectural optimizations for group communications were proposed: definition of optimized service enablers for broadcast/multicast; IP architectural strength in deploying broadcast/multicast services over heterogeneous networks; and dynamic mapping of IP multicast into the appropriate radio bearer. Such proposals required validation, which was achieved through prototyping. Since multiple architectural aspects were addressed, the complexity of these prototypes is necessarily large. This fact made it virtually impossible for a single person to develop all the necessary prototypes. Validation of the proposed concepts through prototyping was therefore only possible through collaborative works, in which the author was involved in projects IST-DAIDALOS and IST-C-Mobile.

In these prototypes the Access Router plays a fundamental role. Being the first contact point between the UE and the Operator Network, the Access Router is the key element of mediation between the two entities for QoS, AAA, Security and mediation between layer 2 and layer 3. Thus Access Routers are key to the validation of the proposed optimizations, and were carefully developed by the author. Furthermore, since the prototypes developed were part of larger concepts being validated, the AR prototype had to feature far more features than those strictly necessary to validate the optimization of resources of group communication. This chapter presents the software router ARM (Advanced Router Mechanisms), as well as the rational for its creation and its functionalities.

6.2 Advanced Router Mechanism

The developed software intended to be more than a conglomerate of loose functionalities fitting the requirements of different projects. From the beginning, it was decided that the AR prototype would be able to stand by itself as complete proposal of what a next generation access router software architecture should be, exceeding the strictly group communication concerns of this thesis.

6.2.1 The Access Router in Next Generation Networks

Next generation networks propose to overcome past concepts, bringing new multimedia applications working under a mobile environment featuring QoS and Security. As mentioned in previous sections, these new networks will require more flexible mechanisms from the Network Operators than those provided by current Networks. Heterogeneity is one of such requirements, as users will demand support for a broader set of technologies raging from WiFi to WiMax, and including Broadcast technologies such as DVB-H. In this scenario, QoS and Security constitute requirements and not desired features, therefore needing to be supported in all edges of the network regardless of the Radio Access Network technology involved. This multiplicity of possible RAN's, likely to be shared by a single element (multi-technology routers/access point), requires the existence of a software convergence layer for multiple technologies API's.

Under these conditions, it is also expected a change in the role of the Access Router, from a mere packet forwarder into a more intelligent network element, capable of removing load associated to the multiple technologies from the more central Service Provisioning Platforms. This support brings added redundancy and resiliency to the network infrastructure, which at the same time further enhances QoS and Security support by means of closer interaction between the RAN and the Core Network.

This view is not entirely novel. Work done in areas such as Active Networks [Tennenhouse 2007] and Software-Programmable Router Operating Systems [Yan 2001] is of great relevance when defining next generation routers. Nonetheless it is here proposed that the evolution to "active" networks will not occur from the core of the network towards its edges, but will instead focus in providing technology specific support in the edge and abstract control mechanisms in the core. The Access Router (the first router in the path of a communication) is in this view the center of such revolution. The centralized functions of the network in terms of Caching, QoS, Resource Optimization and Security must be partially moved to the edges in order to improve the scalability of Next Generation Networks. At the same time, the Access Router can provide better integration of heterogeneous technologies, by making full use of their capacities in the Radio Access Network while still providing a consistent interface to the management service functions deployed in the Core Network. Resource optimization for broadcast/multicast services is then easy to support.

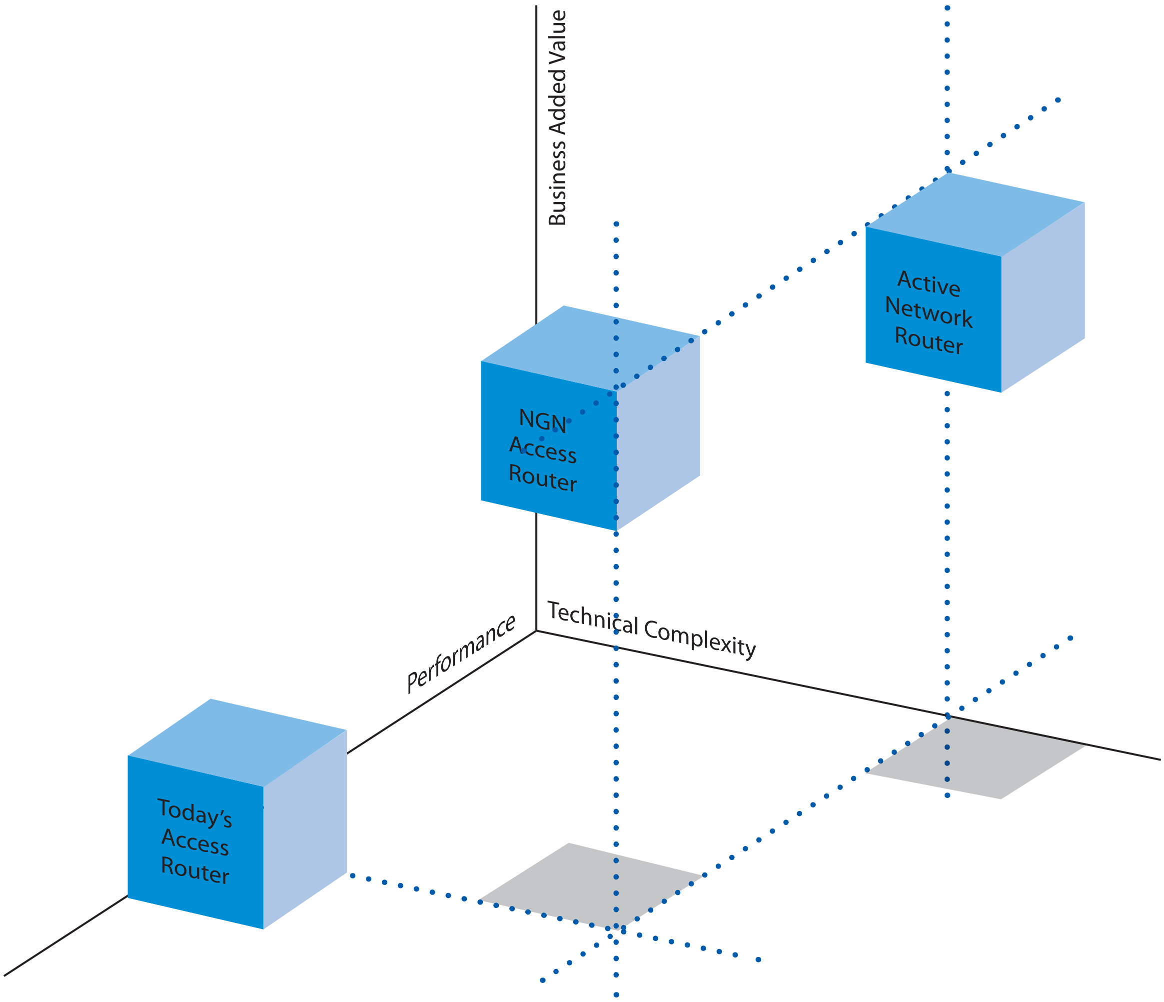


Figure 42 - Positioning of the Next Generation Access Router

As depicted in Figure 42, today's Access Router main advantage relies in its performance capabilities and in the technical simplicity of its functional components. An Active Network Router on the other hand excels these routers, with great technical complexity of its functional components that can dynamically be expanded providing increased levels of added value. Nonetheless this requires a lot of resources and due to hardware platform limitations they fall short of their promises. Next Generation Networks routers need therefore a compromise between these paradigms, in which high performance and technical complexity expectations might be lower, but business added value should match the levels proposed in the area of active networks.

6.2.2 Conceptual Requirements

Taking all previously mentioned aspects into consideration, the Next Generation Access Router should comply with the following basic requirements to achieve NGN goals:

6.2.2.1 Shared Ownership/Virtual Operators

As bandwidth offerings increase, cell radius has taken the opposite path mostly due to technology constrains. In such a scenario, Operators are required to do large investments in order to cover broad areas and reach all possible clients. The increased costs and appearance of new Telecom Operators can nonetheless be overcome by resource sharing (both in terms of licenses and installed resources) amongst operators and by the creation of Virtual Operators (able to operate on top of existing Operators Infrastructures) such as seen in GSM networks. In this case new smaller operators could play a double role of further extending the global connectivity coverage and reaching new costumers. Still under this scenario, Operators will most likely have Access Routers scattered over large geographical regions, probably collocated with competitor operators or even sharing the same resources. Such a scenario might not be that far from us as new MVNO (mobile virtual network operators) already exist around the world and FON [FON] (a WiFi Operator) uses this concept of shared resources ownership with Telecom Operators such as British Telecom or ZON. Next generation Access Routers need therefore to have the capability of running different modules and hardware owned and managed by different business partners, similarly to what happens in today's PC world, where several software vendors share a myriad of hardware components.

6.2.2.2 Flexibility

The previous requirement easily leads to the need for flexible software capable to adapt itself to any environment. Flexible hardware can also be considered as another requirement for next generation heterogeneous networks. An Access Router hardware platform capable of modularly supporting several technologies would enable Telecom Operators to prepare an evolution road-map for their networks, while cutting costs in managing a hardware stock composed by multiple technologies and hardware vendors. The specificity of each L2 technology should be supported by hardware abstractions layers on the Operating Software that can map IP based parameters into specific technology parameters, be it QoS, Security or layer 3 to layer 2 mapping (such as the case described in the previous chapter).

6.2.2.3 Modularity

In the considered heterogeneous environment, with different L2 technologies, the access router hardware platform should be flexible enough to cope with upgrades made by the operators in terms of RAN technologies. But heterogeneity is not just tied to the hardware. In terms of Software functions routers should be able to actively deploy several functions according to networks operators needs. All this flexibility requires Modular Operating Software, capable of adapting to the hardware platform of the Access Router and to the Policies provided by the Network Operator Management Platform. The Operating Software of the Access Router needs to be modular and allow dynamic shift of resources between functions of QoS, Security, Mobility, Policy Based Management and other possible future requirements.

6.2.2.4 Application awareness

The Next Generation AR should have a degree of Application Awareness, enabler of better QoS through the differentiation of application IP flows. This awareness should also constitute a safeguard to Users and Operators, as the router might be required to filter out malicious communications such as Trojans and Worms based on policy provisioned descriptions of the malicious software's communications. This should lead the way into more active and pervasive network elements capable of actively protecting the network from attacks and failures using deep packet inspection mechanisms.

6.2.2.5 Reliability/Robustness

Being the basic providers of connectivity to end-users, Access Routers must provide carrier grade levels of service. Furthermore, Access Routers should be able to run with minimal technical support. Software and hardware based monitoring mechanisms of the router itself should enable the remote maintenance of all systems. This might include possible remote software version upgrades, security patches, fixes and future firmware increments, without the need for any human intervention.

6.2.2.6 Regulatory Conformance

As IP networks become global commodities, legislation and regulation has been approved around the world in order to provide a legal framework. Most of these requirements refer to law enforcement tools and mechanisms, such as logging and traceability of communications, considered by lawmaker's essential tools in justice enforcement.

(Many of these guidelines are present in architectures being discussed for NGN [Xavier 2006]).

6.2.3 Functional Requirements

The conceptual requirements and guidelines previously mention will ultimately mean that several Technical design dimensions need to be covered such as:

6.2.3.1 QoS and Resource Optimization

The next generation Access Router should include IP QoS support by means of standard resource reservations protocols such as RSVP or NSIS, or implicitly using DiffServ Mechanisms or destination based differentiation. Management of the IP based QoS mechanisms should be done by external entities through open interfaces. Resource Optimization should be achieved by smart mechanisms deployed in the access router capable of translating QoS definitions in terms of IP into technology specific parameters. Furthermore it should provide mechanisms that can efficiently map IP services into the most appropriate radio services, a control problem in this thesis.

6.2.3.2 Security

In terms of security, firewall functionalities capable of providing Security for the Network and User Terminal by means of a strict enforcement of rules are necessary. Such rules should be able to be dynamically deployed by the Operator based on current network conditions (e.g. blocking the propagation of an Internet Worm, or stopping a Distributed Denial-of-Service (DDoS)). Security and Access Control mechanism should also be made available at link layer level, through mechanisms such as 802.1x.

6.2.3.3 Mobility

Support for mobility is a key point for next generation networks and the Access Router should modularly support Fast Mobility and Context Transfer, enabling users to roam between Access Routers at high speeds with no degradation in terms of QoS and Security. Technologies such as IEEE 802.21 are extremely relevant in this scope.

6.2.3.4 Policy Based Management

The heterogeneity of the software and hardware of the Access Router, requires an abstract management interface capable of translating existing and future Management (COPS [RFC 2748], SNMP [RFC 1157], DIAMETER [RFC 3588], NETCONF [RFC 4741] and CLI) interfaces into an internal Open Policy Set, which can be openly interpreted by all parties and extended as required by newer functional entities.

6.2.3.5 Software Dynamicity

The Flexibility and Modularity requirement directly translates into the need for dynamic software modules, capable of self confinement (functional independence of modules features) and able to be loaded and unloaded in runtime with no downtime or feature penalty for the remaining modules.

6.2.3.6 Future Proof

The modularity of the Access Router software must encompass the development of new modules as needed by the business plan of the Operator. Specific modules might include support for user driven ad-hoc and mesh networks, L2 optimizations of resources (as needed by technologies such as WiMax) and L3 to L2 mapping of technologies such as Multicast IP to Broadcast technologies.

All these functions will obviously impact the performance of the Access Router, if we consider today's router hardware platforms. Nonetheless under today's PC's technology it is already feasible to have such a low-cost device, capable of supporting QoS, Security and Mobility for a few hundred terminals under a single hardware frame.

6.3 Software Architectures

Routers requirements in general have been described in [RFC 1716] and [RFC 1812]. These documents propose the basic definition of what a router is and of how it should behave in an IP network. Although outdated, they still prove mostly valid for today's routers.

Most of today's Routers are based in closed source projects, but the basic model from which they derive is quite simple and has been previously analyzed [Gottlieb 2002].

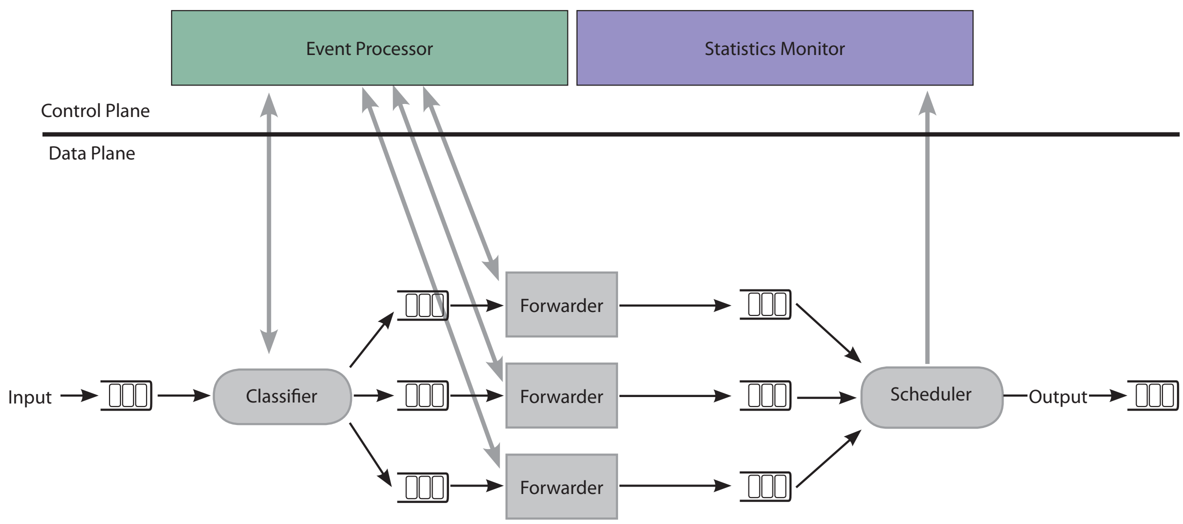


Figure 43 - Basic Router Architecture

This basic model (see Figure 43) defines an Input Port, through which packets arrive to the router operating system, in the form of a memory buffer on the Network Card. From this buffer a Classifier picks up packets and sorts them between forwarding queues based on header information of the packet such as source, destination and protocol. The Forwarder deals with processing the packet (includes routing and packet filtering), and putting it in Output Queues, where a Scheduler picks up the packet and sends it back to a network card through the Output Port.

These functions were defined as very simple in order to achieve high levels of performance. In such a basic model, complexity in a router comes from possible parameterization of the Classifier and Scheduler through well-defined configurations, and has been the subject of much research [Nandy 1998][Qie 2001]. This model restricts itself to a Data Plane and Control Plane with minimum functionality in order to boost performance. However today's routers have evolved past the basic control and management needs and now integrate new functionalities at higher levels. Amongst these it's worthwhile to mention the Event Processors that can trigger alarms to the network operator, and the Statistics Monitor that provide information on the status of the router. These two functions constitute a thin Control Plane layer, as they can act upon the underlying functions in extreme situations (e.g.: traffic congestion). Further functionalities such as Remote Management mechanisms (e.g. SNMP, SSH, telnet) provide an even thinner Management Layer, as it should provide only the most basic management functions of configuration necessary for the Access Router to connect to the Core Network Management functions. It is important to state that these aspects pose no limitation on today's access router, rather the opposite; the wired router is highly efficient in providing IP connectivity at low Total Costs of Ownership (TCO) rates.

Several Open Source research projects, such as «Click», «Scout» and «Router Plugins», have addressed the task of developing novel router architectures. These projects share a common goal: to provide a modular architecture for building routers, and further evolve their functionalities. These architectures focus on extensibility, dynamicity of modules and new functionalities, as well as on the development of new Schedulers and Forwarders.

The Click Modular Router Project [Morris 1999] provides simple building blocks called «elements» that can be composed together in order to implement more complex composite elements, in a recursive process until the desired functionality is achieved. The elements may have multiple ports to connect to other elements. Both input and output ports may be either push-type (through which a packet must be sent) or pull-type, allowing the creation of custom Classifiers, Forwarders and Schedulers. Click has been extensively used in multiple applications [Agarwal 2005][Braem 2005].

The Router Plugins architecture (also referred to as the Crossbow project) [Decasper 2000] on the other hand, tries not to create a new execution flow, but instead focuses in enabling limited extensions to the IP routers. These extensions can be placed at well known points of the routers execution flow, and can enable per flow behaviors such as new routing protocols, packet scheduling and security processing of IP flows.

Scout [Mosberger 1996] is a modular communication oriented operating system. Although initially developed as a stand-alone operating system, it became also available as a Linux Router. Scout and Crossbow implementations are similar in the sense that both focus on the flow of packets, called «path» by Scout. Paths are in Scout composed of «stages», which are instances of «modules». Each module implements a well-understood protocol, such as IP or TCP. Paths are created on demand at run time, and each path corresponds to a unique IP flow.

In common, they all share flexible mechanisms, able to implement almost any kind of routing mechanisms, at the cost of performance. Further these routing projects goals are to create new data planes (with the exception of Router Plugins), and draw less attention to the definition of Control and Management Mechanisms. A new architecture for the Access Router is then proposed.

6.4 ARM Software Architecture

One of the main constrains of today's commercial Access Routers is the legacy software architecture that companies tend to perpetuate in new releases. It is also known that manufacturers have built their platforms upon legacy requirements, most of them not suited for the requirements presented in the previous section. The opportunity to evolve in the area exists by integrating new concepts and software paradigms in the design and conception of a new clean architecture for access routers.

The router model previously (Figure 43) presented is adequate for the common router, composed of few well-defined hardware and software interfaces. However the Access Router, as previously discussed, may become a modular hardware platform possibly comprised of several hardware Interfaces.

This leverages current router modules, where the forwarding functions in the Data Plane are controlled by rules provided by the Control and Management Plane. These rules are dynamic and the forwarder can feedback the classifier providing a simple mechanism to process complex forwarding rules. Rules instantiated by the Control Plane are provided by policies processed in the Management Plane coming from a central policy decision point (PDP) in the network, thus enabling the network operator to consistently manage a large set of routers. This concept changes the simpler data path inside the router from a linear path from input to output, to a slightly more complex (but more flexible) path where dynamic rules dictate the Data Path. Next

Generations Networks will most probably provide their services over a wireless environment; this fact impacts the functionalities of the router. The wireless environment is, by definition, a less secure environment with usually less bandwidth and QoS (due to the wireless medium properties). Therefore the access interface of the Access Router needs extra control and monitoring than the core interface where the medium is more reliable and bandwidth tends to abound or be over provisioned. The proposed software architecture approaches this need by creating virtual interfaces that abstract each of the wireless technologies specific functions. To the high-level control mechanism all access technologies are regarded equally, and it is the task of the virtual interface to translate parameters from L3 into L2. Additionally advanced features that might pose performance issues are only made available to the access interfaces.

Most of the added complexity of this router proposal lies in the control and management plane, which constitute the core of the prototype developed.

In Figure 44 the ARM architecture is presented as an evolution of the basic router architecture presented in Figure 43. The main difference between the two lies in the Control Plan. In the ARM Router Architecture the control plane is composed of several subsystems: the Input Subsystem, Session Handler, Data Plane Management and Policy Subsystem. Each of these subsystem address specific tasks and are globally coordinated by central management entities located in the Core Network (e.g. Bandwidth Brokers, A4C servers), through the Policy Subsystem. The Control Plane functionalities here proposed were non-existing in the Linux Operating System and had to be implemented.

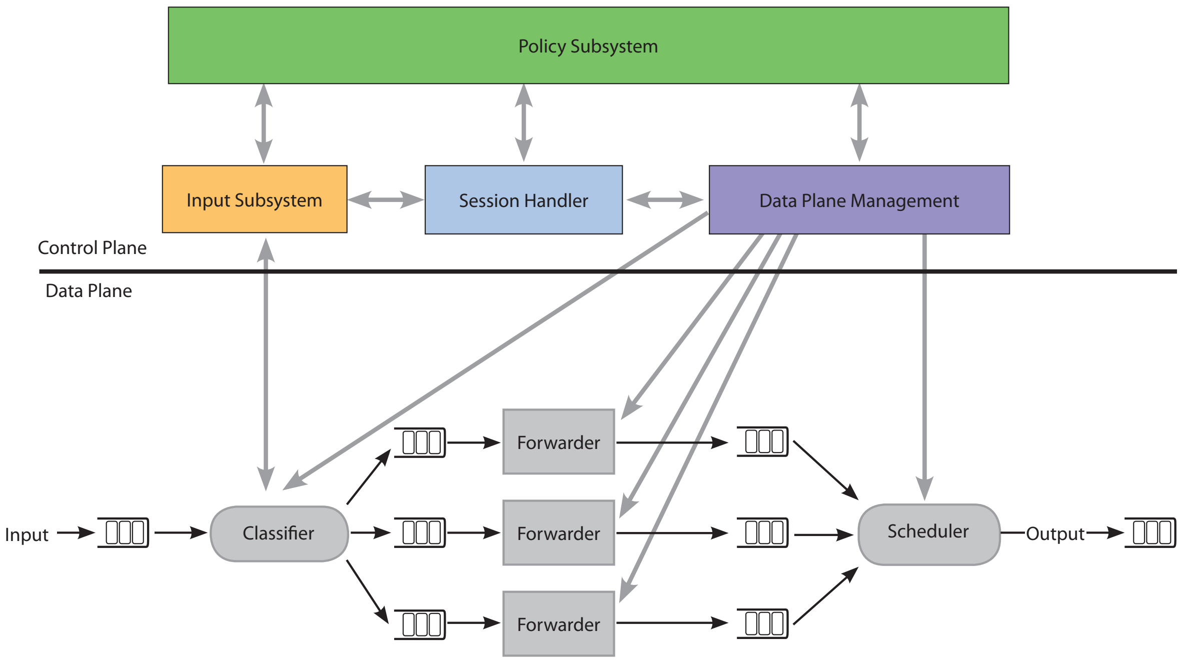


Figure 44 - ARM Router Architecture

Basic Data Plane functionalities such as Routing, QoS enforcement mechanism and Firewall enforcement mechanism rely on already well developed functionalities inherent to the Linux Operating System.

6.4.1 The Control Plane

When faced with the requirements, described in the previous sections, for modularity of the functions and software, the Object Oriented Paradigm appears as the right paradigm for the task of modeling and development of this new architecture. The functional modularity mentioned in the requirements can be described in terms of software objects. Each router functionality such as Interfaces, Control Subsystem, Input Subsystem and further Advanced functionalities can be realized by objects.

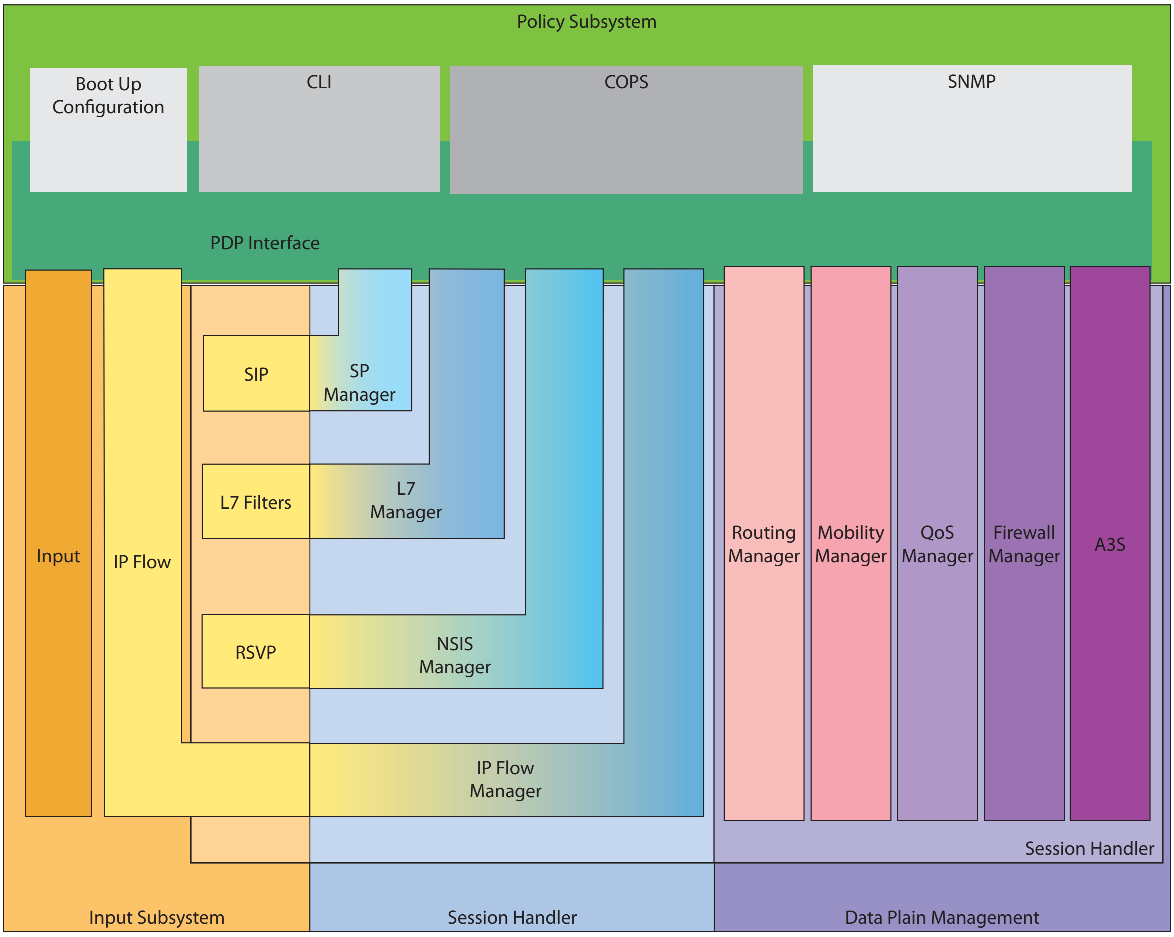


Figure 45 - Functional view of the Control and Management Planes of ARM

The identified modules can be grouped together according to the kind of functionality provided. In Figure 45 the identified modules are grouped together and placed according to the interfaces they provide.

The modules can be grouped primarily as belonging to one of three subsystems: Policy Subsystem, Input Subsystem and Control and Management Subsystem. The separation of these subsystems is based on the level of abstraction the software modules must have. The Policy Subsystem is purely based in abstract policies, while the Input Subsystem and Control and Management Subsystem is based in interfaces with the Data Plane and must therefore be technology aware. The Input Subsystem differentiates itself from the Control and Management Subsystem by interfacing directly with IP flows, while the second interfaces solely with enforcement mechanism available at the Data Plane. Furthermore the Control and Management Subsystem can be divided into two: the Session Handler modules and the Data Plane Management modules. The first group is in charge of managing the ongoing IP sessions and the second in controlling the Data Path enforcement mechanisms. Each of these groups is next detailed.

6.4.1.1 Policy Subsystem

Direct access to the router is usually limited and commercial routers usually implement only remote CLI (Command Line Interfaces). Due to popularization of web technologies these interfaces have evolved into web based interfaces. Nonetheless these interfaces lack the scalability requirements of a network operator that deploys hundreds or even thousands of Access Routers. A modular interface to the network operator is therefore necessary. It further should be capable of coping with changes in terms of management protocols in the operator's management platforms.

The Policy Subsystem main purpose is interfacing with Policy Decision Points (PDP), entities capable of coordinating a global policy for the usage of the network. As coordination point the PDP centralizes some of the control that had been distributed by the Access Routers. It has a centralized point of view over the network resources and events taking place, which enables it to take better decisions on admission control, QoS profiling of new flows and resource optimization. This architecture therefore tries to achieve the best of two worlds: a scalable distributed system of Access Routers controlled centrally by means of policies dynamically provisioned to the routers.

Key to the functioning of this architecture is the Policies ontology that should be extensive and flexible without falling into redundancy.

The Policy Subsystem [Shepard 2000][Changkun 2000] relies on a PDP Interface whose task is to abstract the complexity of its interfaces with well-defined Policies ontologies (such as the ones used in COPS, DIAMETER and SNMP) and the remaining modules that require policies from this subsystem.

The proposed architecture depicts currently three interfaces, each with a different mechanism for policy provisioning. The CLI constitutes the most basic interface, which relates to current practices, providing a direct Human Interface to the provisioning of policies. This interface lacks nonetheless the support for real-time policy outsourcing.

On the other hand the COPS Interface provides the required mechanism, using an object-oriented protocol. Similarly the SNMP Interface provides a mechanism for remote management of the Access Router using industry proven methodologies. These interfaces are not limited and can be further extended (e.g. Diameter).

6.4.1.2 Input Subsystem

The Input Subsystem constitutes the main event generator of the router. The Input Subsystem, through its interface with the Data Plane, is responsible for instantiating rules in the Classifier for the processing of all tracked sessions at maximum speed at the Data Plane Level. The Data Plane Classifier handles packets based on such rules. Whenever a packet does not match any of the installed rules, the Input Subsystem is triggered and receives such packet. A Packet might reach the Input Subsystem for two reasons: either it belongs to a new flow (which needs to be processed by the router previous to its forwarding) or the packet requires advanced processing of its contents (such as packet inspection or in band signaling processing).

The most common case is the existence of a new flow, and the Input Subsystem creates a Control Plane data structure that holds the characterization of the flow (its IP's, protocol, and ports) and the Data Plane Identification (ID) of the packet. The Input Subsystem modules are responsible for handling the Flows by mapping multiple packets through their ID's to the Flow structure and vice-versa. Each module in this group shares a common group of functionalities referred hereby as Session Manager. Each Session Manager tracks its own Flows and packets per mechanism (SIP, L7, NSIS, etc), while the **IP Flow** module acts as an independent repository of packets per flow, during the time the different modules of the router process the Flow in order to determine if the flow is to be processed by itself. After a flow has been terminated, the module in charge is required to free the data structure in the Session Manager that does the mapping and of removing any Data Plane rules. The Input Subsystem is also responsible for triggering the remaining router modules.

6.4.1.3 Session Handler

Session Handler Modules focus on processing special protocols or functions, making it possible to provide a customized flow management that acknowledges protocol specificities. These modules can register with the Input Subsystem, and to be triggered to process new incoming flows. Their task is to extract information from the Flow and request from the PDP appropriate rules for flow processing in the router. This will usually mean QoS and Firewall issues, but might also involve special routing of packets.

The **SIP Manager** acts as a transparent lightweight proxy that is capable of providing call control for SIP based services. The control might include redirection services, codec filtering, call admission or simple flow information extraction for the creation of QoS and Firewall rules. The SIP Manager, upon picking up a flow from the Session Handler interacts with the remaining Management Modules and Policy Module(s), in order to fully process the packets, retrieve policies and install the aforementioned rules. This functionality can relieve IMS entities of some tasks, improving therefore their scalability.

The **L7 Manager** is very similar to the previous module but focuses on a more generic class of flows. Such flows include HTTP, P2P protocols in general and other non SIP protocols which will further be referred to as Legacy Flows. While SIP signaling provides a description of the flow, most Legacy Flows do not; as such the L7 Manager relies mostly on policies to characterize the Flows it handles. The policy's are defined centrally by the network operator and stored in the PDP for retrieval by the routers. They can define QoS policies for protocols (e.g. P2P traffic should be considered low priority) or can even block access to determined locations (e.g. web sites containing law infringing contents).

The **NSIS Manager** on the other hand, due to NSIS protocol nature, enables quick retrieval of information on the flow. It explicitly includes information on the required QoS and Firewall rules. The NSIS Manager can also act as a transignaling agent [Gomes 2004]. The NSIS Manager on the source Access Router exports the Flow information to its PDP, which after validating the flow, forwards it to the destination Access Router (or Domain border router). On the destination Access Router the NSIS Manager generates a new NSIS state. This scenario enables a mixed environment, where IntServ and DiffServ architectures can coexist.

The **IP Flow Manager** constitutes the main interface with the input subsystem as it is considered the default case. It is through the IP Flow Manager that flows reach other flow management modules. This module is responsible for a first analysis of the packet provided by the input module and for routing it to the proper Session Handler module. This module generically handles any other flow not handled by the afore mentioned modules. This usually means proprietary protocols not recognized by the L7 Manager or encrypted data flows that can only be processed based on their source and destination IP's and DSCP. Flows handled by the IP Flow manager have their QoS enabled by the DSCP of its packet, and possible combinations of IP header information. The IP Flow Manager actually models the standard behavior of today's routers, in the sense that it only handles IP level tags.

6.4.1.4 Data Plane Management

The second subset of the Control and Management Subsystem acts as an interface tool for the creation of rules on the data plane.

Besides implementing routing daemons (RIP, OSPF, etc…) the **Routing Manager** can be used to create tunnels between networks, or interact with other control protocols such as MPLS or ATM. The Routing Manager is also responsible for interacting with Multicast and Broadcast routing mechanisms, by providing policies for proper use of these transport capabilities, such as multicast group creation policies and switching (refer to chapter 5).

The **Mobility Manager** provides an interface to mobility events. These events involve mobility of terminals in and out of the network served by the router. This module serves the need to install Data Plane rules quickly based on context transferal from other routers, required in order not to disrupt communications on a moving terminal.

The **QoS Manager** provides translation of QoS policies into system dependent QoS rules that enforce QoS per flow or aggregate on the Data Plane. It also serves the purpose of interfacing with technology specific parameters of the installed interfaces. Technologies such as 802.16 and 802.11e that natively support QoS can be configured by means of a QoS abstraction layer provided by the Virtual Interface mentioned before, that is accessed by the QoS Manager module.

The **Firewall Manager** assumes an important role in actively policing which users are authorized, which services they are entitled to, and which flows are allowed to flow through the network. Again as in the QoS Manager case, the Firewall Manager provides a translation mechanism between generic firewall rules and system dependent firewall commands.

Closely related to the Firewall Manager the **A3S** (Authentication, Authorization, Accounting) module provides as the name implies Authentication and Authorization of the Terminal/User pair. The A3S should either provide an 802.1x that allows the terminal to authenticate, or could instead provide an interface to a different Authentication Protocol. Further it provides the necessary mechanisms to record and export to a central Accounting Server, data on the usage of services. This information should be as extensive as required by new business models that might account for Volume, Time, Services, or any combination of these.

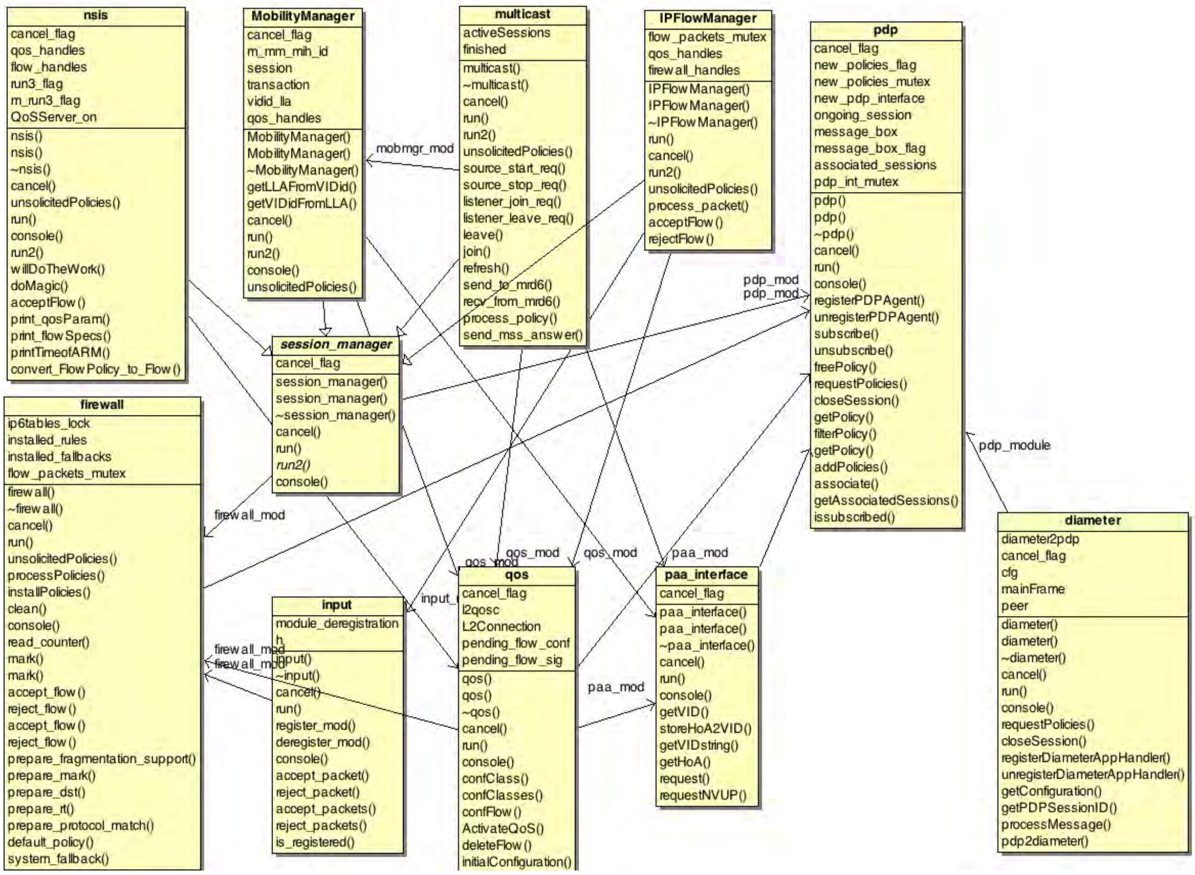


Figure 46 – Advanced Router Mechanism (ARM) – a next generation router prototype as instantiated in project IST-Daidalos

Further models can control the Data Plane and underlying technologies can be introduced into this group such as the **Broadcast/Multicast to Unicast mapping** module described in the previous chapter, or a **Service Discovery** module.

These modules provide an abstraction between the Management and Control Plane implemented in user space and the Data Plane, which might reside in Kernel space for performance issues.

As previously mentioned this router software architecture was prototyped and integrated within a larger prototype of a NGN in IST project Daidalos. The prototype named ARM (Advanced Router Mechanism) implements several of the proposed architecture modules as shown in the UML Class diagram (Figure 46) of the main prototype classes (auxiliary classes were left out of the diagram in order to make it more concise).

In accordance with project changes over time, some modifications were performed such as: the addition of a Diameter Interface and support for 802.21 in the Mobility Manager module. The limited amount of changes required in core modules proved that the prototype was future proof and could encompass new concepts and modules without undergoing changes in the existing code base.

6.4.2 Information Flow

The previous section has detailed the functions provided by each module proposed for the architecture, but did not describe the flow of information inside of the router. In this section the information flow defined by the author and used in the project IST-Daidalos is described.

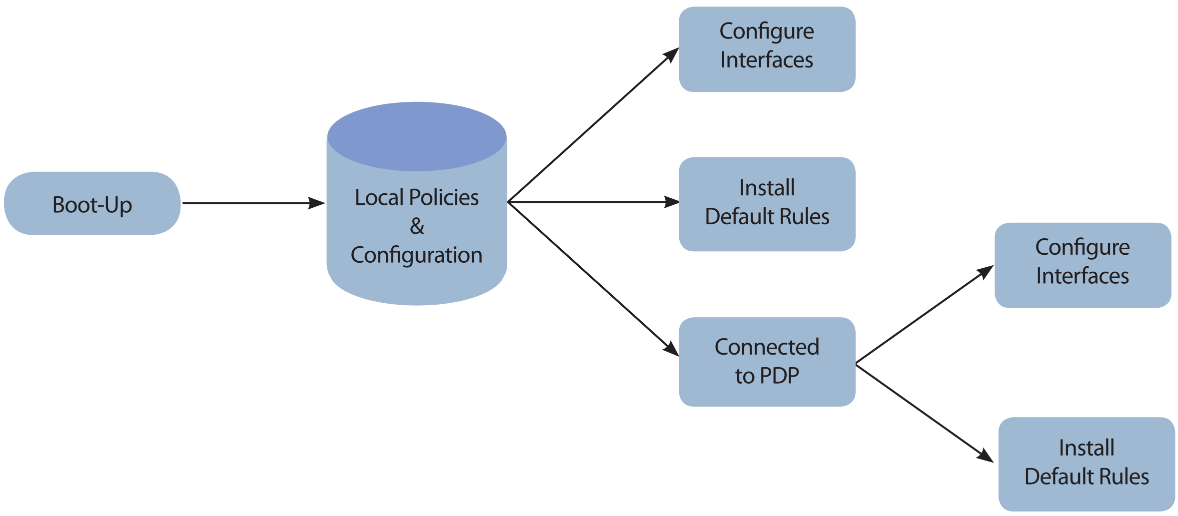


Figure 47 - ARM Boot-Up Sequence

To analyze the information flow that crosses the Access Router, it is first necessary to consider the boot-up sequence. The boot-up sequence (Figure 47) starts by reading local policies and configuration from a local repository that lies on the Access Router system. This information initializes the Data Plane state, configuring interfaces and default rules. During this phase the Access Router establishes connections to the PDP, from where it can receive updates to its initial configuration.

After terminating the boot up sequence the Router is able to forward packets based on default rules. These rules should, by default, limit access to the network, requiring that any terminal first register with the A3S module (using e.g. EAP).

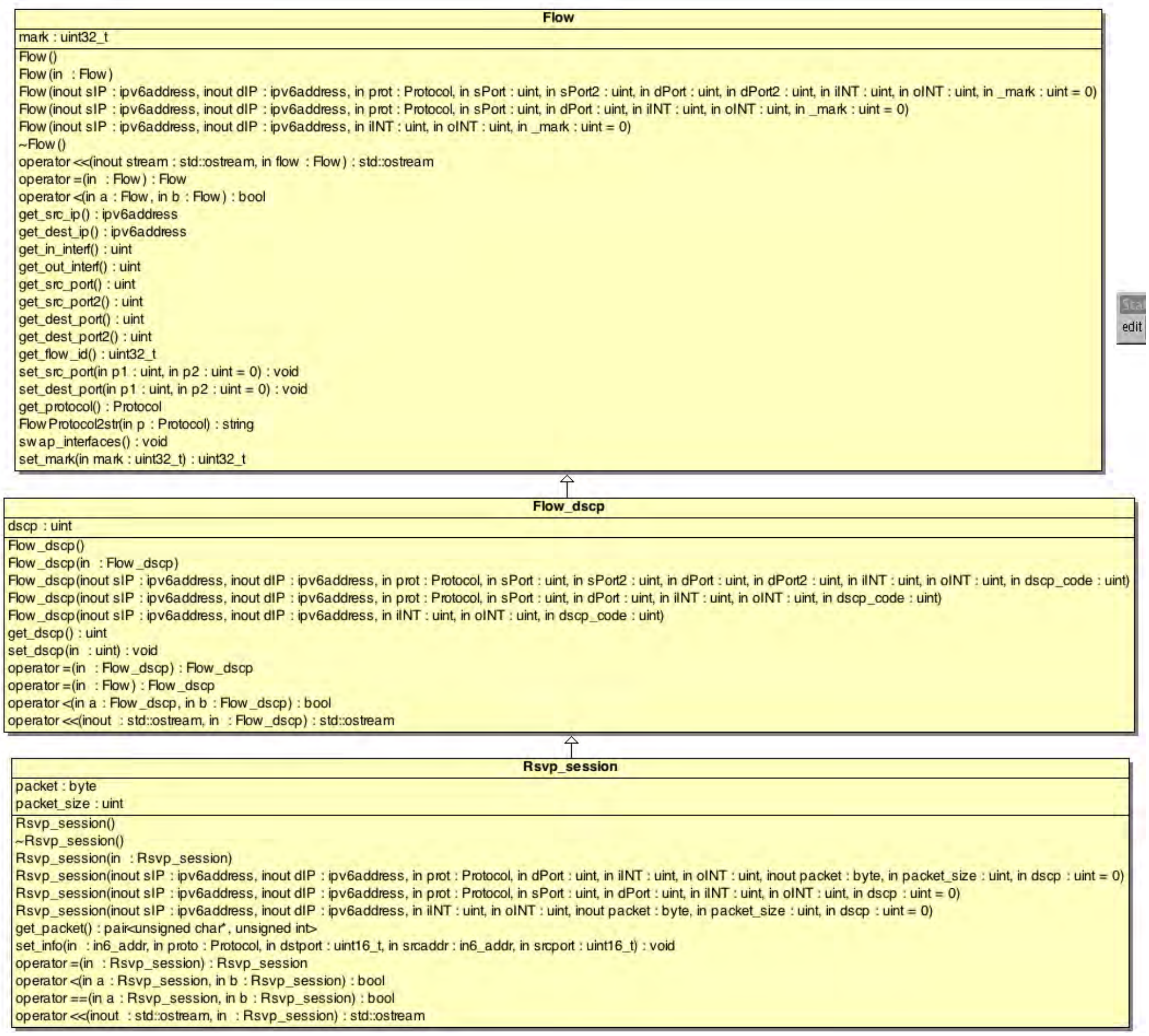


Figure 48 - ARM - Flow description classes

After the Terminal Authentication, services can be authorized per flow taking into account the policies provisioned into the PDP. A packet corresponding to a new flow will reach the Input Subsystem, which based on the available modules could in a worst case scenario be handled by the IP flow module (Figure 49). The choice of which module will process the packet is based on a priority list defined upon boot-up through the policies provisioned by the PDP. The Input Module should pickup the packet from the Data Plane and stores its flow information on the Sessions Handler, from which the IP Flow Manager would have pooled for new flows. Depending on the module that processes the flow, its information can be extended with different parameters. Therefore OOP inherency was used to acknowledge these differences while maintaining the same interface as seen in Figure 48.

The IP Flow Manager would next interface with the PDP through the PDP interface abstraction module, which based on configuration would use one of the available interfaces, again based on priority defined in policies. Upon callback by the PDP Interface the IP Flow would be required to interface with the necessary Manager Modules in order to enforce the policies provided by the PDP Interface. Data Plane Managers such as the QoS Manager and Firewall Manager would then process the generic rules and create new data rules, in order to provide the flow with QoS and firewall transversal.

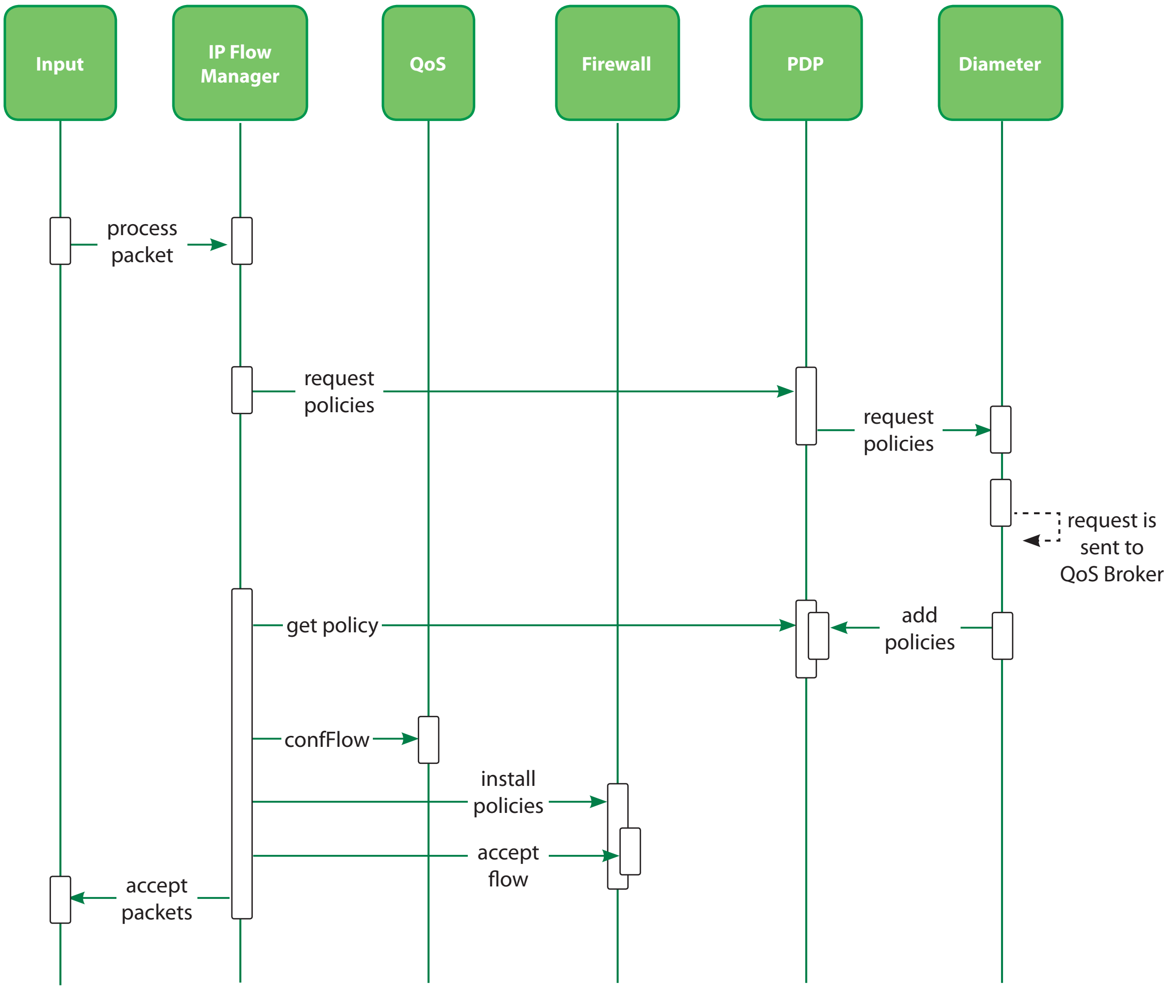


Figure 49 - ARM - Session Setup

After this process had been concluded, the IP Flow Manager would have the responsibility of freeing the packets held so far in the Session Handler. It should further keep track of the flow for the lifetime of the flow in the current Access Router, that is, until the Terminal moves to a new AR or the flow terminates. A message sequence chart of this process as implemented in the prototype is presented in Figure 49.

An important aspect depicted in the figure is the fact that most of the interactions between modules occur asynchronously. The *input*, the *IPFlowManager*, the *pdp* and the *diameter* modules do not block waiting for an answer from the next module. They instead use a message queue algorithm that enables the prototype to process flows at great speeds at the lower levels even if the process at higher levels takes a longer time.

6.4.3 Software Framework

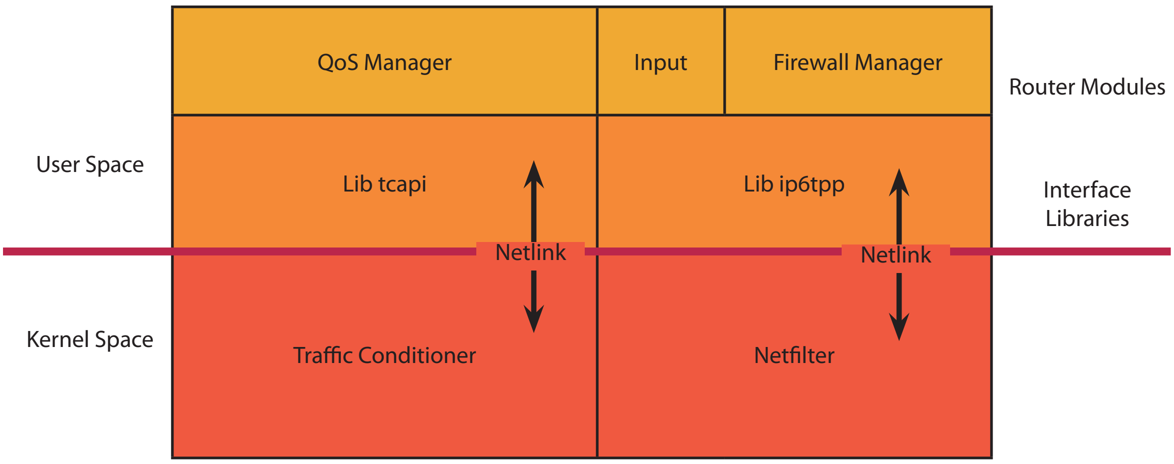


Figure 50 – Main Interfaces between ARM and the Linux Kernel

The platform used was Linux kernel 2.6, which provided a proven data plane and the necessary control mechanism to that same data plane. Linux also provided the tools to create a Control and Management Plane in User Space where the object oriented Control Plane was programmed using C++. One of the requirements of the Access Router was the need to be Fault Tolerant, that is, the router should be able to recover from software and hardware errors without remote assistance, and preferably without human intervention. That ultimately led to a design resembling “micro kernel” architectures [Golub 1992]. It basically consists of a framework class capable of launching several threads, and the sole purpose of the framework class is to keep these same threads running.

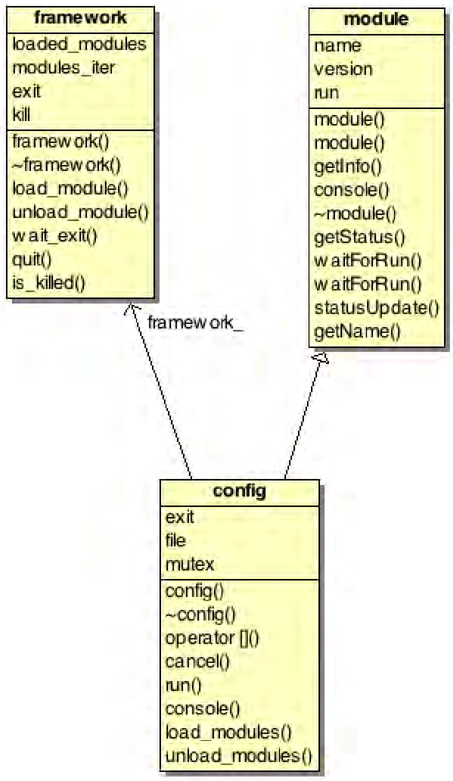


Figure 51 - ARM – Framework classes

The framework resembles a skeleton holding together the several components of the router, which in this case are its modules. It has no routing functionality and its thread is the main thread of the router process. The framework reads from the boot up configuration module (an instantiation of the config class) a list of bootstrap modules required for basic operation. As depicted in Figure 51, the framework class is very simple and reduces itself to loading and unloading modules. In the main() function of the router program the framework is the only class instantiated, after which the configuration module can be loaded. Afterwards it is the task of the configuration module to iteratively load the remaining modules.

The description of the modules in the previous section assumes a certain degree of independence between modules, mainly between Managers (although modules can call functions in other modules, they do not have dependencies). Taking into account this aspect and the performance requirement of the Access Router in processing thousands of packets per second, the modules became independent threads [Vibhatavanij 2000]. Using POSIX Threads the modules are loaded and run by the framework from which they detach leaving a data pointer to the class (kept in the «struct module_info» in the «loaded_modules» map). This data pointer is managed by the framework and enables any module to reach any module for seamless inter-class interfaces on the memory level. This property proved to be both practical to the programmer (enabling it to create simple interfaces between modules) and to the overall performance of the system. Another added value of this solution is the possibility created by threaded modules to be loaded and unloaded in runtime, which was one of the requirements stated in a previous section.

6.4.3.1 Modules

The code presented in Figure 52, summarizes the class module from which all the router modules inherit their properties. The code presents the module class as a child of the parent class Thread. This parent class is defined in the PThreadsmm library, which was also developed for the purpose of this prototype. The Thread class from PThreadsmm library abstracts the complexity of dealing with POSIX Threads and mimics as close as possible the standard JAVA Thread class, in an effort to follow some standardization rules.

```
class module : public Thread
{
     public:
            module() : Thread(true,asynchronous,true) {
                   name="void";
                   version=0;
                   type=ARM::UNKNOWN;
                   statusUpdate(booting);
            };
            module(const module &) {
                   throw module_exception(EXCEPTION_NO_COPY);
            };
            std::string getInfo() {
                   std::stringstream s;
                   s << name << " - " << version;
                   return s.str();
            };
            virtual void console(const std::string &cmd) {
                   std::cerr << "default console" << std::endl;
            };
            virtual ~module() {
                   statusUpdate(stoped);
            };
            const module_status getStatus() const {
                   return status;
            };
            const void waitForRun() {
                   run.wait();
            };
            const void waitForRun(unsigned long miliseconds) {
                   run.wait(miliseconds);
            };
            const void statusUpdate(module_status s) {
                   status = s;
                   if (status==running) run.broadcast();
            };
            const std::string getName() const {
                   return name;
            };
     protected:
            std::string name;
            int version;
            ARM::module_type type;
            module_status status;
            Condition run;
};
```

Figure 52 - ARM - module class

A module, as defined in the prototype, shares three important properties: name, version and type. Name and version enable the framework to refer to the proper module, while type indicates to which subsystem the module belongs. Due to the nature of the modules it is forbidden the creation of any copy constructor, else it might have been possible to end up with misleading threads competing for the same functions in the router.

After being loaded, any module can require the framework to load additional modules based on its dependencies. This capability allows the PDP Interface to load and unload running modules based on policies, as described in the requirements section. An operator could therefore proceed remotely with distributed router upgrades by sending through the network a policy indicating the location of a new module; the router would then download the new module and load it in runtime. For this to happen it is needed to have loadable-shared objects. Therefore, and in addition to the Thread property of each module, it was necessary to separate them individually into shared objects that can be loaded and unloaded in runtime by the framework without any strict dependencies. The load and unload procedures of the framework makes use of the dlopen() and dlclose() functions [Norton 2000] to perform this task.

6.4.3.2 Implementation Issues

Several implementation issues had to be solved during the development. There was a lack of an Open Source implementation of the COPS protocol and old or deprecated interface libraries to the QoS and Firewall kernel space mechanism.

The first issue involved programming Object Oriented COPS, Netfilter and Traffic Conditioner [Almesberger 1998] API's. This was done using C++ in order to seamless integrate with the underlying Linux C interfaces. These API's provided the necessary mechanisms to create several of the main modules in the architecture, namely the COPS PDP Interface, the QoS Manager and Firewall Manager. Communication in these libraries is handled between user space and kernel space through Netlink Sockets, which although not very efficient are a well known standard interface (Figure 50).

The QoS Manager module, as previously described, is responsible for managing the QoS subsystem of the router. Linux already implements several QoS functionalities such as filter classifiers and queues under the Traffic Conditioning API. The broad set of QoS mechanism implemented by Linux such as Class Based Queue (CBQ) and Hierarchical Token Bucket (HTB) provides the necessary flexibility to instantiate the rules and policies an operator may define. These Linux mechanisms are usually controlled through a command line interface called «tc». This interface to the kernel space uses a netlink socket to send configurations from the user space. The tcapi library [TC API] makes use of this same netlink socket, and provides a simple C interface to software developers. Nonetheless this library is unmaintained and lacks support to more recent mechanisms such as HTB. A new library has therefore been developed. The new library [LTCMMM] was developed in C++ and is published under an Open Source License.

In this prototype implementation, two modules share an important interface with the Kernel Space. The Input and Firewall Manager require access to the packets flowing in the kernel space in order to process, control or route packets properly. The Linux kernel Netfilter subsystem provides all these mechanisms. Its common interface is the user space command «iptables».

Similarly to «tc», «iptables» interfaces the user space and kernel space through a netlink socket. Unfortunately there was no library available that made use of netlink socket, so a new library was developed (libip6tpp). This library also object oriented and developed in C++ provides an easy interface to the Linux Netfilter subsystem.

The Linux Netfilter subsystem provides the means to reroute packets from the kernel space to the user space Input module. The input module uses the Netfilter QUEUE hook to read packets in to the user space memory where it can process the packet, after being processed the packet can be resumed to the kernel in the same position of the data plane. The Firewall Manager makes broader usage of the Netfilter subsystem, as all firewall rules can be directly instantiated in this subsystem. The Firewall Manager module therefore needs only to translate the firewall policies into Netfilter rules, which are sent through the libip6tpp.

Besides the User to Kernel Space interfaces, the prototype interfaces with the Policy Decision Point (PDP) through a COPS interface. This interface makes use of yet another external library developed for this prototype. The COPSpp library is a library that models the COPS objects into C++ objects. Such modeling proved to be very important, as it enables system designers to easily extend the COPS protocol through Client Specific Objects.

Another interface developed in the prototype is an RSVP processing module (similar to the proposed NSIS processing module). This module enables the processing of RSVP messages coming from the terminal, from which QoS requirements can be extracted. This module prototype has enabled the demonstration and evaluation of the Transsignalling scenario described in [Gomes 2004] and evaluated in [Sargento 2006].

Proving the flexibility of this proposed architecture, the A3S module was implemented and integrated independently. In this case the A3S module which provided Authentication, Authorization and Accounting, was a daemon already developed that needed only to be integrated within the proposed architecture in order to be provided with a consistent interface with the PDP (from which the A3S module also depends). Due to the nature of the used Operating System, UNIX Sockets were used to create a communication channel between the A3S and the remaining integrated system. The Unix Socket provided a slightly less efficient interface for the communication of policies, but enabled the seamless integration of the existing A3S module.

7. Conclusion

7.1 Review and Discussion of Achievements

As Networks evolve, a convergence of technologies is occurring. This convergence is gathering under a single network a myriad of technologies and services. Services targeted at groups, such as IPTV, have been deployed over diverse technologies from CATV to 3G wireless networks. Mobile Telecommunications network have been provided with Broadcast/Multicast technologies such as MBMS, at the same time that existing technologies, such as DVB, have been integrated into telecommunication networks. This thesis has focused in optimizing resources in this converging environment. Resource optimizations can be achieved for group communication, from aspects like Service Optimization, Support for Heterogeneous Networks (with special regard for unidirectional ones such as DVB) and IP to L2 channel mapping.

The challenge presented to the author in the beginning of its work was how to deploy a generic group based service in a Next Generation Network. From this point, the research work evolved towards optimizing NGN architecture for the purpose of distributing such services.

The work presented starts by addressing possible evolutions to the 3GPP MBMS. The evolutions considered are mainly architectural and address the fact the MBMS was designed as an independent subsystem, which can be integrated into the overall 3GPP architecture. Such integration is possible not only through the integration of MBMS BM-SC Broadcast/Multicast specific functionalities into the existing 3GPP Entities such as the PCRF, P/I/S-CSCF and HSS, but also through the creation of a richer Service Enabling Platform based in OMA concepts that better map application requirements into the proper distribution technology (either unicast or multicast). Through an intelligent Service Layer, applications can better resort to the functionalities provided by the network for the delivery of content. The proposed Service Layer and its Enablers provide a richer interface to applications than that provided by IMS, as they encapsulate several network aspects irrelevant to the application provider. Furthermore these Enablers are provided by the network operator and can therefore include a better knowledge of how the service should be deployed in terms of transport technology, QoS, AAA, Mobility and Security.

Fundamental to this conception is the need for a better integration of Radio Access Networks under a single Core Network to which the Service Layer is connected. The Core Network must provide a seamless abstraction of the underlying technologies, specially considering Broadcast technologies that are mostly unidirectional. The work presented, addresses the integration of such technologies from a service independent point of view. A solution for the integration of unidirectional technologies into a NGN is proposed through the use of an IP based mechanism. Such integration, purely based in IP mechanisms, can be used for both unicast and multicast services although the most efficient use is made by multicast services.

Another important optimization aspect addressed in this work is the creation of a dynamic mechanism for the mapping between IP unicast/multicast services into L2 unicast/broadcast/multicast channels according to the available RAN resources. These optimizations follow a layered approach to group communication Optimization. This layered approach addresses the heterogeneity of Service Platforms, Core Networks and Radio Access Networks that will inevitably constitute NGN.

All these proposals were evaluated in prototypes developed by the author under the scope of different projects (IST-Daidalos and IST-C-Mobile). A key piece for these projects demonstrations was the ARM concept of a Next Generation Access Router. The ARM is presented here as a concept of what the author believes should be a next generation router capable of supporting the optimizations it has proposed for group communications. Next Generation Networks pose several opportunities and requirements for Operators. A new set of services and access technologies will come that will require more from user terminals and network alike. User expectation of a more intelligent network will surely drive operators to develop pervasive services that require more intelligence in the network (mainly on its edges). The ARM architecture was developed with this scenario in mind, and provided a software framework in which the optimization concepts proposed could be trialed and analyzed.

The work done impacted larger network concepts, such as those developed in projects IST-Daidalos and IST-C-Mobile. Furthermore through several published articles in conferences and magazines referenced throughout the text.

7.2 Future Work

Given the wide amount of concepts and ideas pursued in this work, it would be impossible to consider this a closed chapter in terms of research. Several ideas were left to be pursued in future work. I hereby summarize some of the most important ideas that could be further developed.

Recent 3GPP releases have moved towards the vision proposed in Chapter 4, but still lack a vision of Multicast/Broadcast services integration with other technologies, especially the European standard for Mobile TV (DVB-H). Therefore, it still exists the need to further research the synergies that can be created through the new concepts introduced in 3GPP for the integration of technologies such as WiFi, to cover unidirectional broadcast technologies such is the case of DVB-H. Furthermore OMA BCAST is still to prove itself in the market place and the need therefore exist to further study alternatives in the area of Service Enabling platforms for broadcast services. For instance, it could be interesting to develop a service platform based on context information which can be used to create novel broadcast services such as location based advertisement insertion into global broadcast TV services, social multimedia services (end-users belonging to the same social network are provided with contextualized content) and context based network provisioning (services are delivered according to the end-user equipment context).

Another aspect that should be further studied is the use of Fountain Coding Algorithms in non 3GPP technologies. Fountain Coding Algorithms could be used to create different QoS levels through the use of different interfaces to deliver the packets. The research on this topic would cover the use of Fountain Coding Algorithms at the IP layer instead of existing work in 3GPP that is focused in the link layer and application layer. Doing so would maintain the abstraction achieved in the concept presented.

The dynamic mapping of IP into L2 mechanisms could also in the future be pursed in new directions such as what was done in [Gomes 2006], but should be further studied from the view point of QoS. The possibility to switch between Multicast and Unicast can be leveraged not only from the point of view of network optimization, but can also constitute an opportunity for market breakdown between normal users (who would receive services using "broadcast quality") and premium users (who would receive the same service using "unicast quality"). Future work will consider improvements to the algorithm taking into consideration IP and MAC layer measurements, as well as operator policies, and QoS requirements. Nevertheless, for concept demonstration purposes, the proposed algorithm is adequate.

7.3 Final Remarks

In retrospective, the work performed over this period of 5 years witnessed technologies evolving to situation in which the early visions went from “far future” into “near future”, much in the same way that 3GPP Long Term Evolution (LTE) technology is now the next technology to deploy.

When the work started, next generation broadcast technologies such as MBMS and DVB were still being finalized. Although they already indicated a strong potential for use in next generation networks, not many working groups were actively considering them. This ultimately led to a late adoption of MBMS by 3GPP (only available in Release 6) and to an almost un-existing deployment of DVB-H by Mobile Telecommunication Operators. MBMS is currently being more actively pushed into the market, as manufactures have gradually integrated its features into their equipments. As for DVB-H, it has been adopted as the European standard for mobile television, which has put some pressure into national regulators. Unfortunately these technologies are mostly far from the Portuguese market as they were when this research work started. In the author opinion this is mostly due to the limited number of services provided, which is currently reduced to a minor number of mobile TV channels. It is also true that there are no equipments with the proper radio interfaces in the market. Market rules state that there can only be supply of such equipments if a demand exists. It is therefore important to develop new services and to create new means of delivering information through broadcast technologies. In a short term this might mean new service platforms, but ultimately this will also mean new ways of delivering information regardless of the underlying network technology.

When the author was first presented to the challenge of broadcast/multicast service delivery a sophism quickly came up that there could exist a need to transfer IP unicast sessions into IP multicast sessions transparently for the end-users equipments in order to optimize network resources. The author considers this a sophism. After much work into the subject, an example service could not be found that would have the required conditions to be made into a multicast service, without being already a multicast service. An IP multicast session basic principle is that all listeners share the session and therefore the contents of such session, while in an IP unicast session users have their own session. Transport Protocols and Security issues aside, and considering only the service, the author foresees no service were either service provider or end-user would profit from having the service initially delivered using IP unicast and not using IP multicast right from it’s start.

IP multicast was designed with efficiency purposes in mind and in order to fully replace IP unicast in the delivery of a single session to two or more users. It is necessary that service providers acknowledge the benefits of IP multicast, and incorporate IP multicast into their systems, or that they make a more extended use of the Service Platforms provided by Telecom Operators such as OMA BCAST or the one proposed in this work. This should eventually cause a demand for IP Multicast enabled operators and to a more efficient use of broadcast technologies to deliver such services.

8. References

[3GPP R4_R5] 3GPP "Summary of Content of Rel-4 and foreseen content of Rel-5", Online, Available from Internet, http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_14/Docs/PDF/SP-010724.pdf, accessed 1 June 2009

[3GPP R4] 3GPP "Overview of 3GPP Release 4 - Summary of all Release 4 Features", Online, Available from Internet, http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel4%20features_v_2004_07_16.zip, accessed 1 June 2009

[3GPP R5] 3GPP "Overview of 3GPP Release 5 - Summary of all Release 5 Features", Online, Available from Internet, http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel5_features_v_2003_09_09.zip, accessed 1 June 2009

[3GPP R6] 3GPP "Overview of 3GPP Release 6 - Summary of all Release 6 Features", Online, Available from Internet, http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel6_V_2006_09_08.zip, accessed 1 June 2009

[3GPP R7] 3GPP "Overview of 3GPP Release 7", Online, Available from Internet, http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel-07_description_20090608.zip, accessed 1 June 2009

[3GPP R8] 3GPP "Overview of 3GPP Release 8", Online, Available from Internet, http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel-08_description_20090608.zip, accessed 1 June 2009

[3GPP R99] 3GPP "Overview of 3GPP Release 99 - Summary of all Release 99 Features", Online, Available from Internet, http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel99_features_v2004_07_20.zip, accessed 1 June 2009

[3GPP TR 23.847] 3GPP TR 23.847, "Enhancements to IMS service functionalities facilitating multicast bearer services."

[3GPP TR 23.882] 3GPP TR 23.882 "3GPP system architecture evolution (SAE): Report on technical options and conclusions"

[3GPP TS 22.146] 3GPP TS 22.146, "Multimedia Broadcast/Multicast Service (MBMS); Stage 1"

[3GPP TS 22.228] GPP TS 22.228, "Service requirements for the Internet Protocol (IP) multimedia core network subsystem", (Release 10)(SA1)

[3GPP TS 22.278] 3GPP TS 22.278, "Service requirements for the Evolved Packet System (EPS)"

[3GPP TS 23.002] 3GPP TS 23.002, "Network architecture", (Release 8)(SA2)

[3GPP TS 23.060] 3GPP TS 23.060, "General Packet Radio Service (GPRS); Service description; Stage 2"

[3GPP TS 23.207] 3GPP TS 23.207, "End-to-end Quality of Service (QoS) concept and architecture", (Release 8)(SA2)

[3GPP TS 23.228] 3GPP TS 23.228, "IP Multimedia Subsystem (IMS); Stage 2", (Release 8)(SA2)

[3GPP TS 23.234] 3GPP TS 23.234, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description", (Release 8)(SA2)

[3GPP TS 25.346] 3GPP TS 25.346, "Introduction of the Multimedia Broadcast/Multicast

Service (MBMS) in the Radio Access Network (RAN); Stage 2"

[3GPP TS 25.876] 3GPP TR 25.876, "Multiple Input Multiple Output (MIMO) antennae in UTRA"

[3GPP TS 25.999] 3GPP TR 25.999, "High Speed Packet Access (HSPA) evolution; Frequency Division Duplex (FDD)"

[3GPP TS 33.401] 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture"

[3GPP TS 36.300] 3GPP TS 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2"

[3GPP TS 36.401] 3GPP TS 36.401, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Architecture description"

[3GPP] On-line. Available from Internet, http://www.3gpp.org, accessed 1 August 2009.

[Agarwal 2005] Agarwal et al. "Scalable network path emulation". 13th IEEE International Symposium on Modeling (2005) pp. 219- 228

[Aguiar 2004] Rui L. Aguiar, Dennis Bijwaard, Jürgen Jähnert, Paul Christ, Hans J. Einsiedler, "Designing Networks for the Delivery of Advanced Flexible Personal Services: the Daidalos approach", Proc. IST Mobile Communications Summit 2004, Lyon, Jun 2004

[Aguiar 2006] Rui L. Aguiar, Hans J. Einsiedler, Roger P. Karrer, "Daidalos: the operator's vision of the next-generation Internet", Proc. IEEE INFOCOM 2006 Poster, Barcelona, Apr 2006

[Alexiou 2007] Alexiou et al. "Power Control Scheme for Efficient Radio Bearer Selection in MBMS". World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a (2007) pp. 1 - 8

[Almesberger 1998] W. Almesberger, "Linux Traffic Control – Implementation Overview", Technical Report SCC/1998/037, EPFL, November 1998

[Azevedo 2005] Azevedo R., Oliveira A., Fontes F, Guerra D, Esteves P, Mota T, "End-to-End QoS Implementation in a B3G Network", Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop, pp. 122-127, Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT/SAPIR/ELETE'05), 2005.

[B-BONE] IST-2003-507607 (B-BONE), Deliverable of the project (D2.5), "Final Results with combined enhancements of the Air Interface", Available at: http://b-bone.ptinovacao.pt

[Boni 2004] Boni et al. "Multimedia broadcast multicast service-technology overview and service aspects". 3G Mobile Communication Technologies, 2004. 3G 2004. Fifth IEE International Conference on (2004)

[BOOST DIST] "Random Number Library Distributions", On-line. Available from Internet, http://www.boost.org/doc/libs/1_39_0/libs/random/random-distributions.html, accessed 1 June 2009.

[BOOST] "Boost C++ Libraries", On-line. Available from Internet, http://www.boost.org/, accessed 1 June 2009.

[BOUML] "BOUML – a free UML tool box", Online, Available from Internet, http://bouml.free.fr/, accessed 1 June 2009.

[Braem 2005] Bart Braem, "Implementation and Evaluation of an Ad-hoc On-demand distance vector router", https://euterpe.cmi.ua.ac.be/~bbraem/thesis/thesis.pdf

[Changkun 2000] W. Changkun, "Policy-based network management", Proceedings on International Conference on Communication Technology, WCC - ICCT 2000, Volume 1, pages 101-105.

[Chawathe 2000] Chawathe et al. "RMX: Reliable multicast for heterogeneous networks". IEEE INFOCOM 2000 (2000) pp. 795-804

[Chawathe 2003] Chawathe. "Scattercast: an adaptable broadcast distribution framework". Multimedia Systems (2003) vol. 9 (1) pp. 104-118

[Chen 2001] Yan and Chen. "Resource management in software-programmable router operating systems". IEEE Journal on Selected Areas in Communications (2001)

[CMOBILE D62] Diogo Gomes et al. "Deliverable D6.2 - Performance analysis results for MBMS enhancements", Project IST-C-Mobile, May 2008.

[Crowcroft 2007] Crowcroft. "Net neutrality: the technical side of the debate: a white paper". ACM SIGCOMM Computer Communication Review (2007)

[Cui 2006] Jun-Hong Cui, et al, "AQoSM: scalable QoS multicast provisioning in Diff-Serv networks", Computer Networks: The International Journal of Computer and Telecommunications Networking, 16 January (2006), v.50 n.1 p.80-105.

[DAIDALOS] On-line. Available from Internet, 2009http://www.ist-daidalos.org, accessed 1 August

[Dapeng 2001] Wu et al. "Streaming video over the internet: Approaches and directions". IEEE transactions on circuits and systems for video (2001) vol. 11 (3) pp. 282-300

[De Vriendt 2003] De Vriendt et al. "Multimedia broadcast and multicast services in 3G mobile networks". Alcatel Telecommunications Review (2003)

[Decasper 2000] Decasper et al. "Router plugins: a software architecture for next-generation routers". IEEE/ACM Transactions on Networking (TON) (2000) vol. 8 (1) pp. 2 - 15

[DePrycker 1993] M. DePrycker, "Asynchronous Transfer Mode", 2nd ed. London: Ellis Honvood, 1993

[Dhamdhere 2008] Dhamdhere, A. and Dovrolis, C., "Can ISPs be profitable without violating "network neutrality"?". In Proceedings of the 3rd international Workshop on Economics of Networked Systems, Seattle, WA, USA, August 22 - 22, 2008

[DVB] On-line. Available from Internet, http://www.dvb.org/, accessed 1 August 2009

[EC IP/07/1118] ”Commission opens Europe’s Single Market for Mobile TV services“, On-line, Available from Internet, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/1118, accessed 1 June 2009.

[ETSI EN 300 401] ETSI EN 300 401, “Radio broadcasting systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers”

[ETSI EN 300 421] ETSI EN 300 421, “Digital Video Broadcasting (DVB); Framing Structure, Channel Coding and Modulation for 11/12 GHz Satellite Services”

[ETSI EN 300 429] ETSI EN 300 429 , “Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for cable systems”

[ETSI EN 300 744] ETSI EN 300 744, “Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television”

[ETSI EN 302 304] ETSI EN 302 304, “Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)”

[ETSI ES 283 026] ETSI ES 283 026, “Protocol for QoS reservation information exchange between the SPDF and the Access-RACF (A-RACF)”

[ETSI ES 283 034] ETSI ES 283 034, “Network Attachment Sub-System (NASS) - e4 interface based on the DIAMETER protocol”

[ETSI GSM 02.60] ETSI GSM 02.60 Digital Cellular Telecommunications System (Phase 2+): General Packet Radios Service, Service Description Stage 1

[ETSI TS/EN 301 192] “ETSI EN 301 192”, Digital Video Broadcasting (DVB); DVB specification for data broadcasting”

[FON] On-line. Available from Internet, http://www.fon.com, accessed 1 August 2009.

[Glassfish] “GlassFish – Open Source Application Server”, Online, Available from Internet, https://glassfish.dev.java.net/, accessed 1 June 2008

[Golub 1992] Golub et al. "Microkernel operating system architecture and mach", In Proceedings of the USENIX Workshop on Micro-Kernels and Other Kernel Architectures, 1992.

[Gomes 2004] Gomes et al. "A transsignaling strategy for QoS support in heterogeneous networks". Lecture notes in computer science (2004) vol. Volume 3124/2004 pp. 1114-1121

[Gomes 2005a] Diogo Gomes, Emiliano Guainella, Claudio Sansone, Susana Sargento, Rui Aguiar, Francesco Delli Priscoli, "A Next-Generation IPv6 QoS Architecture Integrating Heterogeneous Multicast and Broadcast Networks - Part 1 ", ICT 2005, Cape Town, RSA, May 2005

[Gomes 2005b] Diogo Gomes, Emiliano Guainella, Claudio Sansone, Susana Sargento, Rui Aguiar, Francesco Delli Priscoli, "A Next-Generation IPv6 QoS Architecture Integrating Heterogeneous Multicast and Broadcast Networks - Part 2 ", ICT 2005, Cape Town, RSA, May 2005

[Gomes 2006] Gomes D and Aguiar RL. "Privacy through Virtual Hording". Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE (2006) pp. 1 - 6

[Gomes 2007] Gomes and Aguiar. "IP Multicast Dynamic Mapping in Heterogeneous Environments". Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on (2007) pp. 1 – 5.

[Gomes 2008a] Gomes et al. "A Cross-System Approach for Multimedia Services with IP Multicast in 4G Networks". Wireless Personal Communications (2008).

[Gomes 2008b] Gomes et al. "IP-based content delivery over Next Generation Networks". International Journal of Internet Protocol Technology (2008).

[Gomes 2009] Gomes et al. "Deploying and testing a NGN testbed", Proc. 2009 TridentCom, Washington D.C., April 2009

[Gottlieb 2002] Gottlieb Y, Peterson L. "A comparative study of extensible routers". Proceedings of the 2002 IEEE Open Architectures and Network Programming Conference, New York, NY, June 2002; 51-62.

[GSMA] On-line. Available from Internet, http://www.gsmworld.com, accessed 1 August 2009.

[Handa] Arun Handa." System Engineering for IMS Networks". Newnes (2009)

[Haversine] "Haversine formula", On-line. Available from Internet, http://en.wikipedia.org/wiki/Haversine_formula, accessed 1 June 2009

[IEEE 802.11] IEEE802.11-1999, "IEEE Standard for Information technology – Telecommunication and information exchange between systems – Local and metropolitan area networks – Specific requirements – part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications', 1999.

[IEEE 802.11e] "IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems – Local and Metropolitan area networks – specific parts 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Ammendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005

[IEEE 802.16] IEEE802.16-2004, "IEEE Standard for local and metropolitan area networks; Air Interface for Fixed Broadband Wireless Access Systems", 2004.

[IEEE 802.1p] IEEE 802.1D-1998, "Information Technology - Telecommunications and Information Exchange Between Systems - Local Area Networks - Media Access Control (MAC) Bridges", Institute of Electrical and Electronics Engineers, 01-Jan-1998

[IEEE 802.1q] IEEE 802.1Q-2003, "Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks", Institute of Electrical and Electronics Engineers, 01-May-2003

[IEEE 802.3] IEEE 802.3-1998, "Information Technology - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications" Institute of Electrical and Electronics Engineers, 28-Sep-1998

[IETF RMT] On-line. Available from Internet, http://www.ietf.org/dyn/wg/charter/rmt-charter.html, accessed 1 August 2009

[IETF ZEROCONF] On-line. Available from Internet, http://www.zeroconf.org/, accessed 1 August 2009

[Imai 2003] Yuji et al. "XCAST6: eXplicit Multicast on IPv6". 2003 Symposium on Applications and the Internet Workshops (SAINT 2003 Workshops) (2003) pp. 238

[IMT-2000] On-line. Available from Internet, http://www.itu.int/home/imt.html, accessed 1 August 2009.

[ISO 7498] "Information Processing Systems – Open Systems Interconnection – Basic Reference Model", IS 7498, ISO/IEC, 1984.

[ITU E.800] INTERNATIONAL TELECOMMUNICATION UNION ITU-T, E.800 (1994) Series E: Telephone Network and ISDN, Quality of Service, Network Management and Traffic Engineering, Terms and Definitions Related to Quality of Service and Network Performance Including Dependability.

[ITU-T J.112B] ITU-T Recommendation J.112 Annex B "Data-over-cable service interface specifications: Radio-frequency interface specification"

[ITU-T J.122] ITU-T Recommendation J.122 "Second-generation transmission systems for interactive cable television services - IP cable modems"

[Judge 2003] Judge and Ammar. Security issues and solutions in multicast content distribution: a survey. Network, IEEE (2003) vol. 17 (1) pp. 30 - 36

[Jannottti] J. Jannotti, D. Gifford, K. L. Johnson, M. F. Kaashoek, and J. W. O'Toole Jr. "Overcast: Reliable Multicasting with an Overlay Network". In Proceedings of the Fourth Symposium on Operating System Design and Implementation (OSDI), October 2000

[JSR 116] J. C. Process. SIP servlet API. Java Specification Requests JSR 116, Java Community Process, May 2002.

[JSR 141] J. C. Process. SDP API. Java Specification Requests JSR 141, Java Community Process, March 2003.

[JSR 220] J. C. Process. Enterprise JavaBeansTM 3.0. Java Specification Requests JSR 141, Java Community Process, July 2004.

[JSR 244] J. C. Process. JavaTM Platform, Enterprise Edition 5 (Java EE 5) Specification. Java Specification Requests JSR 141, Java Community Process, May 2006.

[JSR 289] J. C. Process. SIP Servlet v1.1. Java Specification Requests JSR 141, Java Community Process, July 2008.

[Karn 1993] P. Karn. "The Qualcomm CDMA digital cellular system". In Proceedings of the USENIX Mobile and Location-Independent Computing Symposium, pages 35--39. USENIX Association, August 1993.

[Kuan-Ta Chen 2009] Kuan-Ta Chen et al. "OneClick: A Framework for Measuring Network Quality of Experience". INFOCOM 2009. The 28th Conference on Computer Communications. IEEE (2009) pp. 702 – 710

[LIBKML] Mash Bridge, et al. "*a KML library written in C++ with bindings to other language"s,* On-line. Available from Internet, http://code.google.com/p/libkml/, accessed 1 June 2009.

[LTCMMM] Hugo Santos, "LTCM - Linux QoS API Library", On-line. Available from Internet, http://artemis.av.it.pt/~ltcmmm, access 1 December 2008.

[MARKTEST] On-line. Available from Internet, http://www.marktest.pt/, accessed 1 August 2009.

[Marques 2003] Marques et al. "An IP-based QoS architecture for 4G operator scenarios". IEEE Wireless Communications (2003) vol. 10 (3) pp. 54-62

[Maximilien 2004] Maximilien and Singh. "A framework and ontology for dynamic Web services selection" Internet Computing, IEEE (2004) vol. 8 (5) pp. 84 - 93

[MEDIAFLO] On-line. Available from Internet, http://www.mediaflo.com/, accessed 1 August 2009.

[Melia 2007] T. Melia , A. Oliva , I. Soto , P. Serrano , R. Aguiar, "Network controlled handovers: challenges and possibilities", Wireless Personal Communications: An International Journal, v.43 n.3, p.959-974, November 2007

[MGEN] Naval Research Laboratory, “Multi-Generator (MGEN)”, On-line. Available from Internet, http://www.videolan.org/vlc/, accessed 1 June 2009

[Miloucheva 2006] I. Miloucheva, H. J. Einsiedler, D. Gomes, K. Jonas, “QoS based multicast architecture for heterogeneous mobile IPv6 environment”, ICT 2006, Funchal, Portugal, March 2006

[Morris 1999] Morris et al. “The Click modular router2. SOSP ‘99: Proceedings of the seventeenth ACM symposium on Operating systems principles (1999) pp. 217 – 231

[Mosberger 1996] Mosberger and Peterson. “Making paths explicit in the Scout operating system”. USENIX 2nd Symposium on Operating Systems Desing and Implementations (1996)

[MRD6] H. Santos, “MRD6, an IPv6 Multicast Router”, On-line. Available from Internet, http://fivebits.net/proj/mrd6, accessed 1 June 2009

[Nandy 1998] Nandy et al. “A connectionless approach to providing QoS in IP networks”. High Performance Networking (1998)

[Norton 2000] J. Norton. “Dynamic class loading for C++ on linux”, Linux Journal, (73), March 2000. http://www2.linuxjournal.com/lj-issues/issue73/3687.html

[OECD 2007] Organisation for Economic Co-operation and Development. “OECD Communications Outlook 2007”, 2007.

[Ojanperä 2006] T. Ojanperä. “Convergence Transforms Internet”. Wireless Personal Communications (2006) vol. 37 (3-4)

[OMA 2007] Open Mobile Alliance (2007) “OMA Service Environment, OMA-AD-Service-Environment-V1_0_4-20070201-A”.

[OMA Arch] OMA Arch Doc, “Architecture of the Mobile Broadcast Services”

[Oodan 1997] Oodan et al. “Quality of service in telecommunications”. London: The Institution of Electrical Engineers (1997).

[OverDRiVE] IST-2001-35125 (OverDRiVE), Deliverable of the project (D08), "Spectrum Efficient Multicast and Asymmetric Services in UMTS", Available at: http://www.comnets.rwthaachen.de/~o_drive/publications/OverDRiVE_wp1d08_v100.pdf

[Perkins 2002] Perkins. "Mobile IP". IEEE Communications Magazine (1997) pp. 84-99

[Prior 2005] Rui Prior et al. "Heterogeneous Signaling Framework for End-to-End QoS Support in Next Generation Networks". System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on (2004) pp. 305c - 305c

[Qie 2001] Qie et al. "Scheduling computations on a software-based router". ACM SIGMETRICS Performance Evaluation Review (2001) vol. 29 (1) pp. 13 - 24

[RFC 1112] Stephen E. Deering. "Host extensions for IP multicasting". IETF Request for Comments (RFC 1112), August 1989

[RFC 1122] Robert Braden. "Requirements for Internet Hosts -- Communication Layers", October 1989. RFC 1122

[RFC 1157] J. Case, M. Fedor, M. Schoffstall, and J. Davin. "A simple network management protocol (SNMP)". RFC 1157, Network Working Group, 1990

[RFC 1633] Braden, B., Clark, D., and Shenker, S., "Integrated Services in the Internet Architecture: an Overview", RFC 1633, IETF, June 1994.

[RFC 1716] P. Almquist. "Towards requirements for IP routers", Nov. 1994. RFC 1716

[RFC 1771] Yakov Rekhter and Tony Li. "A Border Gateway Protocol 4 (BGP-4)". RFC 1771, March 1995.

[RFC 1812] F. Baker, "Requirements for IP version 4 routers," Request for Comments (RFC) 1812, June 1995.

[RFC 1889] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A transport protocol for real-time applications", IETF RFC 1889, January 1996.

[RFC 2205] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource Reservation Protocol (RSVP) version 1 functional aspects", RFC 2205, IETF, Sept. 1997.

[RFC 2328] J. Moy, "OSPF Version 2", IETF RFC 2328, April 1998.

[RFC 2362] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", Jun 1998, RFC-2362.

[RFC 2464] M. Crawford, "Transmission of IPv6 Packets over Ethernet Networks," RFC 2464, Internet Engineering Task Force, Dec. 1998.

[RFC 2475] D. Black, S. Blake, M. Carlson, E. Davies, Z. Wang, and W. Weiss. "An Architecture for Differentiated Services. Network Working Group", RFC 2475, December 1998.

[RFC 2475] S. Blake, et al., "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC 2543] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg. "SIP: Session Initiation Protocol". RFC 2543, IETF, March 1999.

[RFC 2597] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. "Assured Forwarding PHB Group". RFC 2597, IETF, June 1999.

[RFC 2638] Nichols, K.; Jacobson, V.; Zhang, L. "A Two-bit Differentiated Services Architecture for the Internet". RFC 2638 (Informational) - The Internet Engineering Task Force, Juli 1999

[RFC 2748] J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Raja, and A. Sastry, "The COPS (Common Open Policy Service) Protocol", IETF RFC 2748, January 2000.

[RFC 2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC 2960] R. Stewart et al. "Stream Control Transmission Protocol". RFC 2960, Internet Engineering Task Force, Oct. 2000.

[RFC 3077] E. Duros, W. Dabbous, H. Izumiyama, N. Fujii and Y. Zhang. "A Link-Layer Tunneling Mechanism for Unidirectional Links". RFC 3077, IETF Network Working Group, March 2001.

[RFC 3084] K. Chan, D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith, and R. Yavatkar, "COPS Usage for Policy Provisioning", IETF RFC 3084, March 2001.

[RFC 3246] B. Daview, et al., "An Expedited Forwarding PHB (Per-Hop Behavior)", IETF RFC 3246, March 2002.

[RFC 3344] D. Johnson, C. Perkins, J. Arkko, "Mobility support in IPv6", RFC 3775,June 2004

[RFC 3550] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. "RTP: A transport protocol for real-time applications". RFC 3550, Internet Engineering Task Force, July 2003

[RFC 3569] S. Bhattacharyya. "An Overview of Source-Specific Multicast (SSM)", July 2003. Internet Engineering Task Force, RFC 3569.

[RFC 3588] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko: "DIAMETER Base Protocol", RFC 3588, September 2003

[RFC 3775] D. Johnson, C. Perkins, J. Arkko, "Mobility support in IPv6", RFC 3775,June 2004.

[RFC 3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004

[RFC 3926] T. Paila, M. Luby, R. Lehtonen, V. Roca, R. Walsh, "FLUTE - File Delivery over Unidirectional Transport", IETF RFC 3926, October 2004.

[RFC 3973] A. Adams, J. Nicholas, W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM)", IETF RFC 3973, January 2005

[RFC 4068] R. Koodli, "Fast Handovers for Mobile IPv6", RFC 4068, July 2005

[RFC 4261] J. Walker, A. Kulkarni, “Common Open Policy Service (COPS) Over Transport Layer Security (TLS)”, RFC 4261, December 2005.

[RFC 4601] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, “Protocol Independent Multicast - Sparse Mode (PIM-SM)”, IETF RFC 4601, August 2006.

[RFC 4741] R. Enns, “NETCONF Configuration Protocol”, IETF RFC 4741, December 2006.

[RFC 5213] S. Gundavelli, “Proxy Mobile IPv6”, RFC 5213, August 2008

[RFC 768] Postel, J. B. “User Datagram Protocol”. Internet Engineering Task Force, August 1980. RFC 768

[RFC 791] Postel, J., “Internet Protocol - DARPA Internet Program Protocol Specification”, STD 5, RFC 791 USC/Information Sciences Institute, September 1981

[RFC 793] Postel, J. “Transmission Control Protocol: DARPA Internet Program Protocol Specification”. RFC 793, September 1981

[RFC 959] Postel, J, Reynolds J., “File transfer protocol (FTP),” Request for Comments (RFC) 959, Oct. 1985

[Roca 2002] Roca, V. and Mordelet, B. 2002. “Design of a Multicast File Transfer Tool on Top of ALC”. In Proceedings of the Seventh international Symposium on Computers and Communications (Iscc’02) (July 01 - 04, 2002). ISCC. IEEE Computer Society, Washington, DC, 953

[Sailfin] “SailFin Project”, Online, Available from Internet, https://sailfin.dev.java.net/, accessed 1 June 2008

[Santos 2006] Justino Santos, Nuno Sénica, Susana Sargento, Rui L. Aguiar, “Mobility in Heterogeneous networks: Integration Process”, Proc. Conference on Mobile and Ubiquitous Systems 2006, CSMU, Guimarães, Jun 2006

[Santos 2008] Santos, J., Gomes, D., Sargento, S., Aguiar, R. L., Baker, N., Zafar, M., and Ikram, A. “Multicast/broadcast network convergence in next generation mobile networks”. Computer Network. 52, 1 (Jan. 2008), 228-247

[Sargento 2005] Susana Sargento, Rui Prior, Filipe Sousa, Pedro Gonçalves, Janusz Gozdecki, Diogo Gomes, Emiliano Guainella, Antonio Cuevas, Woztek Dziunikowski, Francisco Fontes, "End-to-end QoS Architecture for 4G Scenarios ", IST Mobile Summit 2005, Dresden, Germany, June 2005.

[Sargento 2006] Susana Sargento, Diogo Gomes, Alfredo Matos, Rui L. Aguiar, "QoS Signalling in 4G Scenarios", Proc. 2006 IST Mobile Summit, Myconos, Greece, Jun 2006

[Satou 2005] Satou et al. "Authentication, Authorization and Accounting Framework for Multicast Content Delivery". Communications, 2005 Asia-Pacific Conference on, October 2005, pag 630-635.

[Scholefield 1997] Scholefield. Evolving GSM data services. Universal Personal Communications Record, 1997. Conference Record., 1997 IEEE 6th International Conference on (1997) vol. 2 pp. 888 - 892 vol.2

[Shepard 2000] S.J. Shepard, "Policy-based networks: hype and hope, IT Professional", Volume 2 Issue 1 , Jan.-Feb. 2000, pp. 12

[Shuqian 2002] Yan, Shuqian, Michalis Faloutsos, and Anindo Banerjea, "QoS-Aware Multicast Routing For The Internet The Designing And Evaluation Of QoSMIC," IEEE/ACM Transactions on Networking, Feb 2002, Vol. 10, Issue 1, pp. 54-66.

[Strassner 2003] J. Strassner, "Policy-Based Network Management: Solutions for the Next Generation", Morgan Kaufmann, 2003

[Striegel 2002] A. Striegel, G. Manimaran, "A survey of QoS multicasting issues", IEEE Communications Magazine 40 (6) (2002) 82-87.

[TAU] "IBM - Rational Tau – Software", Online. Available from Internet, http://www-01.ibm.com/software/awdtools/tau/, accessed 1 June 2009

[TC API] TC API Project, http://www-124.ibm.com/developerworks/ projects/tcapi

[Tenembaum 1996] A.S.Tanembaum, Computer Networks, Prentice-Hall, 1996.

[Tennenhouse 2007] Tennenhouse and Wetherall. "Towards an active network architecture". ACM SIGCOMM Computer Communication Review (2007) vol. 37 (5) pp. 81 - 94

[Terzis 1999] A. Terzis, L. Wang, J. Ogawa and L. Zhang, A two-tier resource management model for the Internet, in: Proceedings of Global Internet, 1999

[TISPAN TS 183 028] ETSI TISPAN NGN Specifications, "Common Basic Communication procedures - Protocol specification"

[Vibhatavanij 2000] K. Vibhatavanij, "Simultaneous Multithreading-Based Routers", Proceedings. 2000 International Conference on Parallel Processing, August 21-24, 2000 pages 362 – 369

[VLC] "open-source multimedia framework and player", On-line. Available from Internet, http://cs.itd.nrl.navy.mil/work/mgen/, accessed 1 June 2009

[Wang 2000] Wang and Hou. Multicast routing and its QoS extension: problems, algorithms, and protocols. IEEE Network (2000) vol. 14 pp. 22-36

[Wedlund 1999] Wedlund, E. and Schulzrinne, H. 1999. Mobility support using SIP. In Proceedings of the 2nd ACM international Workshop on Wireless Mobile Multimedia, Seattle, Washington, United States, August 20 - 20, 1999.

[Xavier 2007] Xavier and Ypsilanti. Universal service in an IP-enabled NGN environment. ITU Workshop on What rules for IP-enabled NGN's (2006)

Annex A. Protocols

A.1 Common Open Policy Service (COPS)

Developed inside IETF by the Resource Allocation Protocol (RAP) charter, and published in January 2000 as RFC 2748, the Common Open Policy Service (COPS) Protocol provides policy based control of QoS signaling protocols and management of resources.

The protocol follows a client/server model in which clients are Policy Enforcement Points (PEP's) and servers are Policy Decision Points. The PEP is a component at a network node and PDP is a remote entity that may reside at a policy server. The PEP represents the component that always runs on the policy aware node. It is the point at which policy decisions are actually enforced. Policy decisions are made primarily at the PDP.

COPS is a reliable and synchronous protocol, due to the use of TCP (port 3288). The basic behavior of COPS involves an event, which triggers a Request to the PDP. According to its policy database, the PDP sends a Decision to the PEP and waits for a Report. The COPS protocol embodies several concepts developed by the Policy Framework charter of IETF, thus providing the means for the PDP to administer, configure and apply policies.

Messages can be authenticated, and further security can be achieved, by running COPS over TLS [RFC 4261] or over IPSec. The protocol was initially defined for an outsourcing environment, in which all policies installed at the PEP are results of events triggered in this element. However it has been extended [RFC 3084] to support the outsourcing model, by which the PDP can asynchronously provide the PEP with Policies based in events foreign to the PEP.

According to the client/server model, it is the PEP that must connect to the PDP, authenticate itself and receive its base configuration on boot up. After this phase, the PEP should stand by, sending periodical Keep-alive, and Accounting information (according to the initial configuration provided by the PDP). The PDP can provide new configurations as it sees fit.

On an event, the PEP must request the PDP for a policy, the decision must be enforced and a Report on the status of the enforcement must be sent back. All communications between PEP/PDP carry a handle that is used to signal policy updates and event refreshes. In the absence of communication with a PDP a Local PDP (LPDP) should exist in order to provide basic policies to the PDP.

The COPS protocol is described through objects. Every object is identified by a header of three fix length fields (Length in octets, C-Num and C-Type). Objects can be grouped together to form messages. Each message is composed of a Common Header (Figure 53) and a number of Objects. All objects, and therefore messages, are 32 bit aligned, meaning that padding can/must be done.

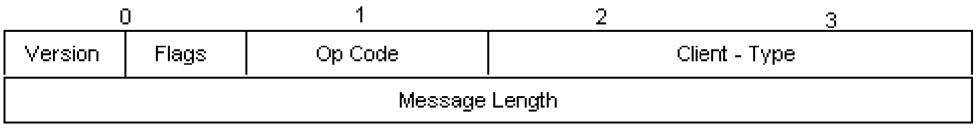


Figure 53 - COPS Common Header

The Op Code field indicates the COPS operation: Request (REQ), Decision (DEC), Report State (RPT), Delete Request State (DRQ), Synchronize State Req (SSQ), Client-Open (OPN), Client-Accept (CAT), Client-Close (CC), Keep-Alive (KA), Synchronize Complete (SSC) and the Client-Type provides the context (PDP or PEP). Next to the Common header a variable number of objects appear according to the operation. All objects share a common template shown in Figure 54.

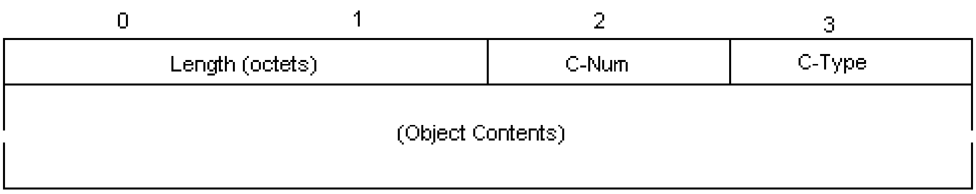


Figure 54 - COPS Object Template

The defined COPS objects are:

- *Handle Object (Handle):* Contains a unique value. This object is used in every single message to reference the state.
- *Context Object (Context):* Specifies the kind of event that triggered a query: Admission Control, Resource-Allocation, Outgoing-Message or Configuration Request

- *In-Interface Object (IN-Int):* Identifies in which interface the event originated, plus the origin address of the packet that triggered the event.
- *Out-Interface Object (OUT-Int):* Identifies to which interface the event is destined, plus the destination address of the packet that triggered the event.
- *Reason Object (Reason):* Reveals the reason of a Delete-Request-Message (DRQ): Unspecified, Management, Preempted, Tear, Timeout, Route Change, Insufficient Resources, PDP's Directive, Unsupported Decision, Synchronize Handle Unknown, Transient Handle, Malformed Decision or Unknown COPS Object from PDP.
- *Decision Object (Decision):* Decision made by the PDP: Null Decision, Install or Remove. Flags further indicate the contents of the Decision: Stateless Data, Replacement Data, Client Specific Decision Data or Named Decision Data.
- *LPDP Decision Object (LPDPDecision):* Decision made by the PEP local policy decision point (LPDP). May appear in requests. Such objects are formatted the same as Decision Objects.
- *Error Object (Error):* Identifies a particular COPS protocol error: Bad handle, Invalid handle reference, Bad message format, Unable to process, Mandatory client-specific info missing, unsupported client-type, Mandatory COPS object missing, Client Failure, Communication Failure, Unspecified, Shutting down, Redirect to Preferred Server, Unknown COPS Object, Authentication Failure, Authentication Required.
- *Client Specific Information Object (ClientSI):* This Object encapsulates client specific objects/attributes of a protocol or internal state.
- *Keep-Alive Timer Object (KATimer):* Specifies the maximum time interval over which a COPS message must be sent or received. It also serves the purpose of resetting this timeout.
- *PEP Identification Object (PEPID):* Used in Client Open messages this object contains an ASCII string that uniquely identifies the PEP within the policy domain and is persistent across PEP reboots.
- *Report-Type Object (Report-Type):* Type of Report: Success, Failure, Accounting.
- *PDP Redirect Address (PDPRedirAddr):* Upon closing a session the PDP might redirect the PEP to a new PDP by supplying the new PDP address and port.
- *Last PDP Address (LastPDPAddr):* Upon a Client-Open Message a PEP must indicate the previous address of the PDP to which he was connected.
- *Accounting Timer Object (AcctTimer):* Specifies the minimum time interval for periodic accounting type reports.
- *Message Integrity Object (Integrity):* This object includes a sequence number and a message digest useful for authenticating and validating the integrity of a COPS message.

These objects are combined in to messages. Although objects can be combined in several ways, the following operations are well defined and constitute the core of the protocol:

Request (REQ): A PEP sends these messages to outsource the decision to the PDP. This message creates a new state in the PDP identified by the Handle which has a PEP scope. The handle provides a context by which the PDP can reconfigure and issue new decisions related to the initial request.

Decision (DEC): This message relates directly to the previous, as each Request must be answered with a Decision. The Decision message usually carries several COPS Specific Objects containing configuration directives only applicable to that specific PEP.

Report State (RPT): After a Decision message and in order for a consistent state to be maintained in the PDP, the PEP must report the result of the installation of the policies sent in the Decision message. Further the Report State message can be used to report accounting values.

Delete Request State (DRQ): When a state is removed from the PEP (probably because the event that triggered the first request has terminated) it must signal to the PDP that the state must be removed.

Synchronize State Request (SSQ): This message provides a way for PDPs to reset their state to a consistent state with the PEP.

Synchronize State Complete (SSC): This message terminates the process initiated by the previous messages.

Client-Open (OPN): This message must always be the first message sent by the PEP to the PDP. It not only registers the PEP with the PDP, but also provides the trigger for initial policy configuration of the PEP.

Client-Accept (CAT): In response to the Client-Open message the Client-Accept provides basic configuration of the Keep-Alive and Accounting mechanisms.

Client-Close (CC): Whenever a PDP or PEP needs to disconnect, this message must be sent in order to remove previous states in either elements.

Keep-Alive (KA): Provides basic connectivity check on the protocol level.

A.2 Resource Reservation Protocol (RSVP)

The Resource Reservation Protocol, defined in RFC 2205, provides the means to instantiate the IntServ architecture. The RSVP protocol provides a peer-to-peer mechanism by which hosts can signal to the network, the QoS requirements for a specific flow or application. According with IntServ, resources are reserved in the whole path of the flow, creating soft-states in each node of the network. Reservations done by RSVP are unidirectional therefore providing functional differentiation from sender and receiver.

RSVP works as background process of the host/router, interfacing between applications in the host and the traffic enforcement mechanisms of the router. The RSVP daemon further interfaces with QoS mechanisms of the host/router such as the Classifier, Admission Control Function and Packet Scheduler (Figure 55). These mechanisms are usually collectively referred to as "traffic control". Additionally the RSVP daemon interfaces with a Policy Controller, in charge to checking for administrative permission to reserve the signaled QoS.

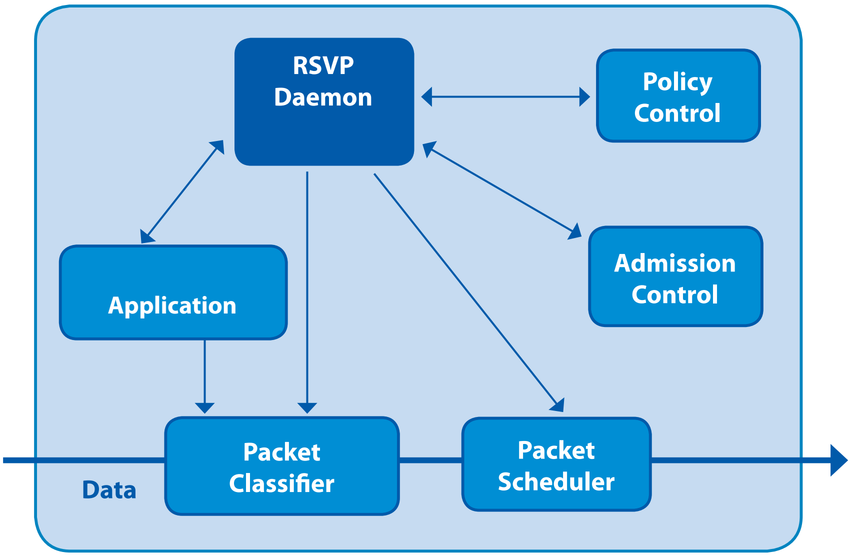


Figure 55 - RSVP in a router

RSVP operation in a node consists of two initial decisions taken by the Policy Controller and the Admission Control Function. These two decision-taking modules check the availability of authorizations and resources on the node. Next, and if both decisions are positive, the RSVP process sets the parameters of the Packet Classifier and Packet Scheduler of the link layer interface to obtain the signaled QoS.

RSVP can be used by unicast and multicast applications in order to reserve network resources, as it is able to adapt dynamically to changing group memberships as well as to changing routes. Multicast support is also assured by the receiver-oriented signaling, as the receiver of a data flow is responsible for initiating and maintaining the resource reservation for that flow. RSVP is also simplex (reservations are made for unidirectional data flows), an important attribute to take in consideration when considering many-to-many communications in which flows tend to be asymmetric and need to be aggregated in order to scale. The soft state of the reservations made in each node requires a periodic refresh, hence the support for dynamic and automatic adaptation to network changes (nodes can leave from a multicast router without leaving resources locked). Finally RSVP provides a degree of independence from future revisions as it provides several reservation styles (or options) and its traffic and policy controls are independent and opaque to the protocol.

A.2.1 Data Flows

In RSVP, a data flow is a sequence of datagram's that have the same source and destination (regardless of whether that destination is one or more physical machines). Data flows have the same QoS. QoS requirements are communicated via a flow specification, which is a data structure used by hosts to request special services from the network. A flow specification describes the level of service required for that data flow. This description takes the form of one of three traffic types. These traffic types are identified by their corresponding RSVP class of service: Best-effort, Rate-sensitive or Delay-sensitive.

Best-effort traffic is the so called traditional IP traffic. Applications range from file transfer, using FTP and P2P protocols, to transactional traffic, such as HTTP. These types of applications require reliable delivery of data regardless of the amount of time needed to achieve that delivery. Best-effort traffic types rely upon the native TCP mechanisms to re-sequence datagram's received out of order, as well as to request retransmissions of any datagram's lost or damaged in transit. Therefore QoS constrains are loosely considered in a best-effort environment.

Rate-sensitive traffic requires a guaranteed transmission rate from its source to its destination. An example of such an application is SIP telephony. Voice is encoded at a constant (or nearly constant) rate, and requires a constant transport rate, such as a circuit-switched connection. By its very nature, IP is packet-switched. Thus, it lacks the mechanisms to support a constant bit rate of service for any given application's data flow. RSVP enables constant bit-rate service in packet-switched networks via its rate-sensitive level of service. This service is referred to as guaranteed bit-rate service (GS).

Delay-sensitive traffic is traffic that requires timeliness of delivery and that varies its rate accordingly. MPEG-II video, for example, averages about 3 to 7 Mbps, depending on the amount of change in the picture. As an example, 3 Mbps might be a picture of a painted wall, although 7 Mbps would be required for a picture of a football match. MPEG-II video sources send key and delta frames. Typically, 1 or 2 key frames per second describe the whole picture, and 13 or 28 frames (known as delta frames) describe the change from the key frame. Delta frames are usually substantially smaller than key frames. As a result, rates vary quite a bit from frame to frame. A single frame, however, requires delivery within a specific time frame or the CODEC is incapable of doing its job. A specific priority must be negotiated for delta-frame traffic. RSVP services supporting delay-sensitive traffic are referred to as controlled-delay service (non-real-time service) and predictive service (real-time service).

A.2.2 Operation

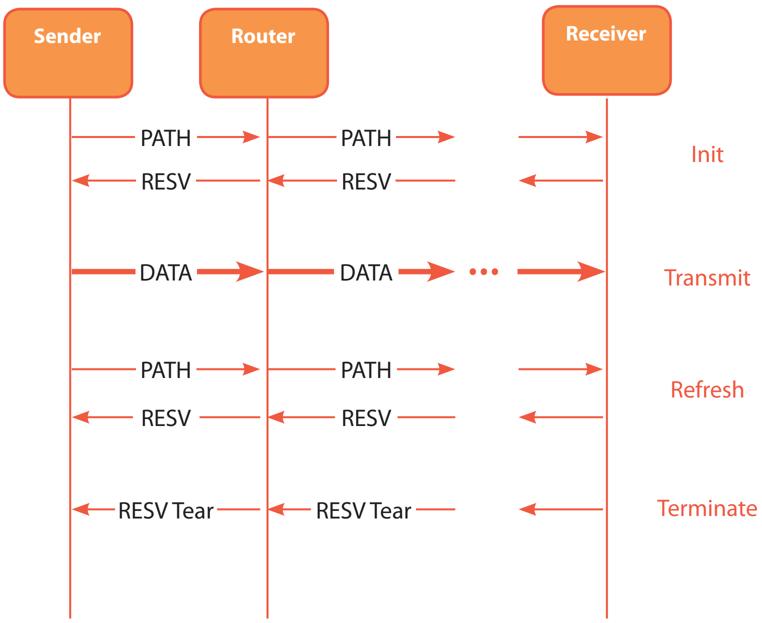


Figure 56 - RSVP Session Message Sequence Chart

It is next described the general operation of the protocol as well as a description of its messages (Figure 56).

There are two primary types of messages: Path messages (PATH) and Reservation messages (RESV).

The PATH messages are sent from the sender host along the data path and store the path state in each node along the path. The path state includes the IP address of the previous node, and some data objects such as the «sender template» (to describe the format of the sender data), the «sender tspec» to describe the traffic characteristics of the data flow and the «adspec» that carries advertising data committed to the PATH message by the nodes traversed.

Reservation messages (RESV) are sent from the receiver to the sender host along the reverse data path. At each node the IP destination address of the RESV message will change to the address of the next node on the reverse path and the IP source address to the address of the previous node address on the reverse path. The RESV message includes the flowspec data object that identifies the resources that the flow is reserving.

The «Flowspec» identifies the particular quality of service required by the flow, as is therefore passed from the application to the hosts and routers along the path.

The «Flowspec» consists of: Service class, Reservation spec (RSPEC) which defines the QoS and Traffic spec (TSPEC) which describes the data flow.

A RSVP host that needs to send a data flow with specific QoS will transmit a RSVP path message that will travel along the unicast or multicast routes pre-established by the working routing protocol (RSVP is agnostic of the underlying routing protocol). If the path message arrives at a router that does not understand RSVP, that router forwards the message without interpreting the contents of the message and will not reserve resources for the flow.

Upon reaching its destination, the PATH message will trigger a reservation based on the requested parameters. For this the admission control and policy control process the requested parameters and can either instruct the packet classifier to correctly handle the selected subset of data packets or negotiate with the upper layer how the packet handling should be performed. Finally it will forward the request upstream (in the direction of the sender). At each node the RESV message «Flowspec» can be modified by a forwarding node (e.g. in the case of a multicast flow reservation the reservations requests can be merged). Each node in the path can either accept or reject the request.

Three error and confirmation message exist: path-error messages, reservation-request error messages, and reservation-request acknowledgment messages.

Path-error messages result from path messages and travel toward senders. Path-error messages are routed hop-by-hop using the path state. At each hop, the IP destination address is the unicast address of the previous hop.

Reservation-request error messages result from reservation-request messages and travel toward the receiver. Reservation-request error messages are routed hop-by-hop using the reservation state. At each hop, the IP destination address is the unicast address of the next-hop node. Information carried in error messages can include the following: Admission failure, Bandwidth unavailable, Service not supported, Bad flow specification, Ambiguous path.

Reservation-request acknowledgment messages are sent as the result of the appearance of a reservation-confirmation object in a reservation-request message. This acknowledgment message contains a copy of the reservation confirmation. An acknowledgment message is sent to the unicast address of a receiver host, and the address is obtained from the reservation-confirmation object. A reservation-request acknowledgment message is forwarded to the receiver hop by hop (to accommodate the hop-by-hop integrity-check mechanism).

RSVP teardown messages remove the path and reservation state without waiting for the cleanup timeout period. Teardown messages can be initiated by an application in an end system (sender or receiver) or a router as the result of state timeout. RSVP supports two types of teardown messages: path-teardown and reservation-request teardown. *Path-teardown messages* delete the path state (which deletes the reservation state), travel toward all receivers downstream from the point of initiation, and are routed like path messages. *Reservation-request teardown messages* delete the reservation state, travel toward all matching senders upstream from the point of teardown initiation, and are routed like corresponding reservation-request messages.

A.3 Next Steps In Signaling Framework (NSIS)

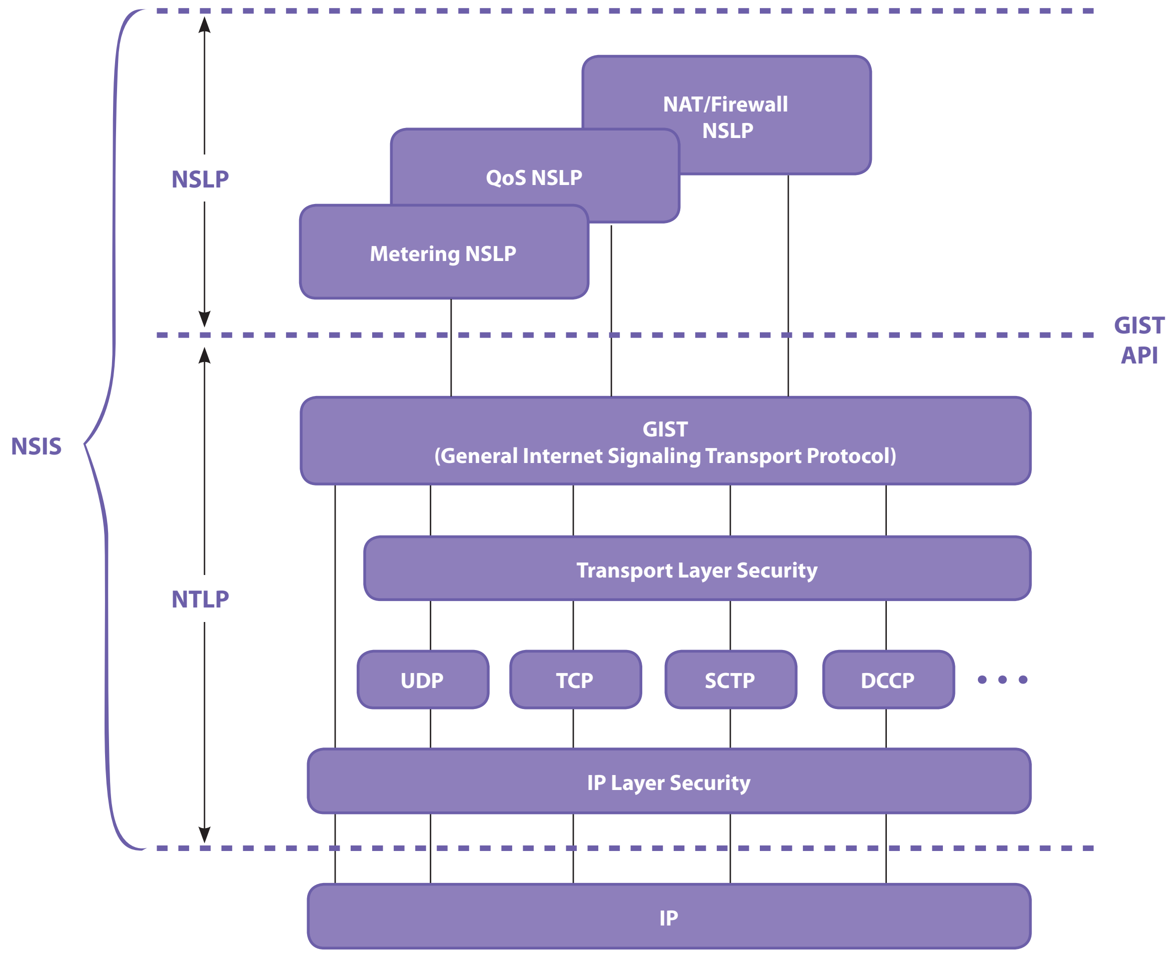


Figure 57 - Next Steps In Signaling Framework

Next Steps in Signaling (NSIS) framework is an evolving communication protocol intended to facilitate signaling at the Transport layer. NSIS is expected to support services and resources such as NAT (Network Address Translation), QoS (Quality of Service) and TURN (Traversal Using Relay NAT). This work is carried out by IETF in NSIS charter. The work carried in this working group has so far led to the actual development of two layers of protocols: the NSIS Transport Layer Protocol (NTLP) and NSIS Signaling Layer Protocols (NSLPs) which are commonly but improperly referred to as the NSIS protocol.

From the beginning, the NSIS working group had as requirements the need to provide components that could be reused in different parts of the Internet for different needs, without requiring a complete end-to-end deployment and most importantly that those mechanisms would fit more than just QoS requirements (namely Resource Reservation). The mechanism used to achieve this flexibility was to divide the signaling protocol stack into two layers: a generic (lower) transport layer, the NTLP, and an upper layer specific to each signaling application, the NSLP.

The lower layer or NTLP is responsible for creating a signaling overlay network on top of which the NSLP can operate. This property confers an additional flexibility to the overall NSIS framework since it provides the means to transverse several network bottlenecks such as NATs, Firewall and Proxies.

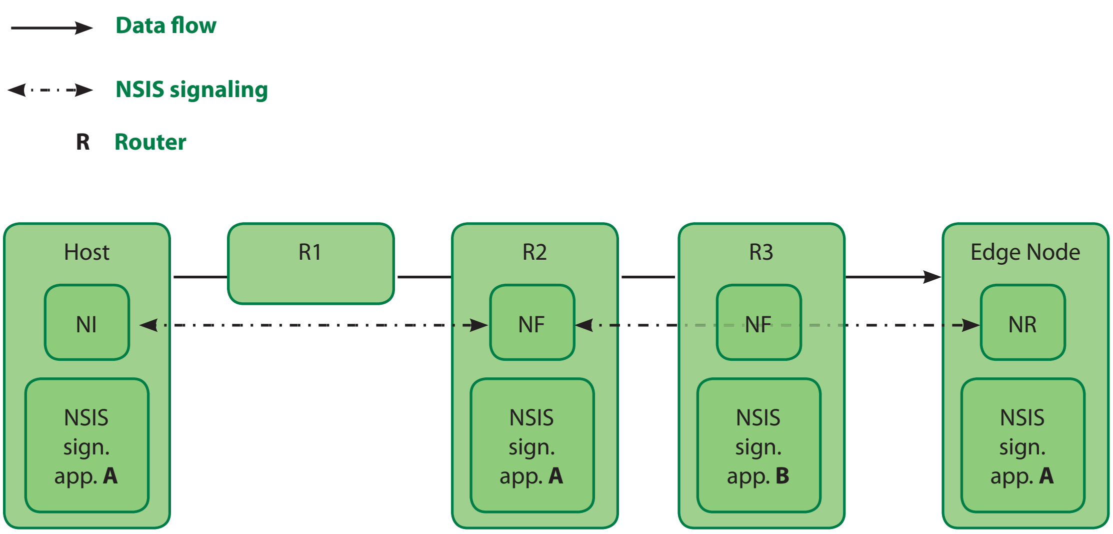


Figure 58 - NSIS signalling decoupling

NSIS was designed to support a diverse set of signaling application that need to install and/ or change network state. These states are related to a given packet flow and are installed and processed in the NE (NSIS Entities - nodes which are NSIS enabled) along the path. This ultimately means that not all NE need to support all functionalities nor must all nodes must support NSIS. The corollary is that two NEs might communicate directly, but need not to be network wise adjacent. In an NSIS signaling path there is dissociation between the NSIS message path and the actual path that the NSIS packets take. This separation is achieved through the separation between the NTLP of which the best-known instantiation is the GIST (General Internet Signaling Transport) Protocol and the NSLP such as the QoS NSLP, NAT/FW NSLP or Metering NSLP.

NTLP is in charge of dealing with issues related to the transport such as path NE discovery, overlay transport paths, etc. In the particular case of GIST it can run on top of TCP, UDP, SCTP and DCCP.

NSLP on the other hand is the *defacto* signaling protocol, that instantiations one of the several functionalities such as QoS, NAT transversal/Firewall and Metering to name a few.

The NSIS layered approach enables it to be extensible and enough generic and flexible to cope with new functionalities that might be required in the future. The separation between NSLP and NTLP constitutes also one of the biggest differences to RSVP, which combined peer discovery and QoS functionality into a single protocol that did not cope well with addendums to the initial specification.

The introduction of a Session Identifier concept potentiated important advancements to the way signaling is done. In NSIS a packet flow consists of a sequence of unidirectional data packets with a very specific source and destination that follow a single data path. A Flow Identifier identifies a packet flow. In addition the Session Identifier can identify an application Session regardless of the amount of Flow Identifiers.

Another important NSIS aspect is the fact that it supports more than just end-to-end signaling. In can also perform edge-to-edge (where only domain nodes talk to each other) and end-to-edge (where a host node can talk to a network node).

A.3.1 GIST

GIST, as a NTLP, provides a mechanism for the delivery of NSLP messages from an Initiator (QNI) to a Receiver (QNR). A flow of GIST packet is unidirectional and any bidirectionality is achieved through a pair of GIST flows. GIST relies heavily on existing transport protocols such as UDP/TCP/SCTP or DCCP and can support advanced security mechanisms such as TLS (Transport Layer Security).

GIST provides both the discovery of NE through the data path and the establishment of a MRS (Message Routing State) for each session. GIST is considered a soft-state protocol that maintains two states related to the transport of signaling messages: a flux state that keeps tracks of messages sent and an association state that tracks GIST peer nodes. GIST is a TLV (Type-Length-Value) based protocol that consists of 6 major types: Query, Response, Confirm, Data, Error and MA-Hello.

- GIST-Query is used before any association is established in a datagram mode.
- GIST-Response is used to transmit information back to the issuer of a connection and must follow the reverse path of a Query
- GIST-Confirm concludes the handshake phase.
- GIST-Data contains MRI (Message Routing Information) and Session Identifiers and a pay loader containing the NSLP packets.
- GIST-Error is used to convey error information at the transport layer.
- GIST-MA-Hello is used only in connection mode to announce the destination NE that the session is to be maintained.

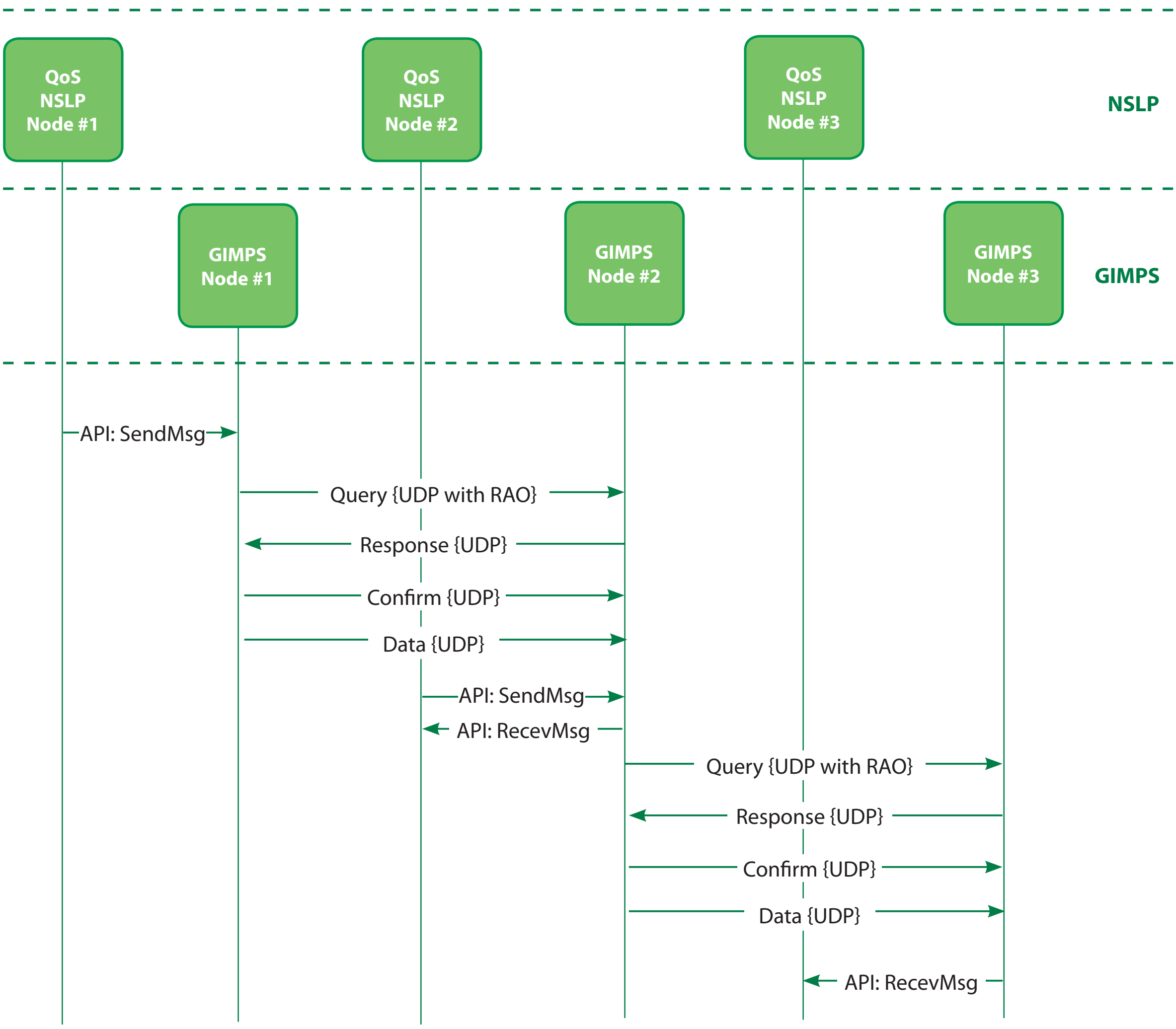


Figure 59 - GIST usage example

In Figure 59 a NSIS system is presented, where one can see the GIST interactions. In this network nodes are presented, with each running a QoS NSLP application. Transport and Application layers are separated in order to better depict each of their functions. One can see that GIST works in a hop-be-hop process that takes places N-1 times (where N is the number of network nodes) and in a sequence.

A.3.2 QoS NSLP

One of the main purposed of the NSIS charter was the development of a replacement for RSVP. Together with GIST, QoS NSLP provides functionality similar to RSVP and further extends it. The QoS NSLP is independent of the underlying QoS specification or architecture and provides support for different reservation models.

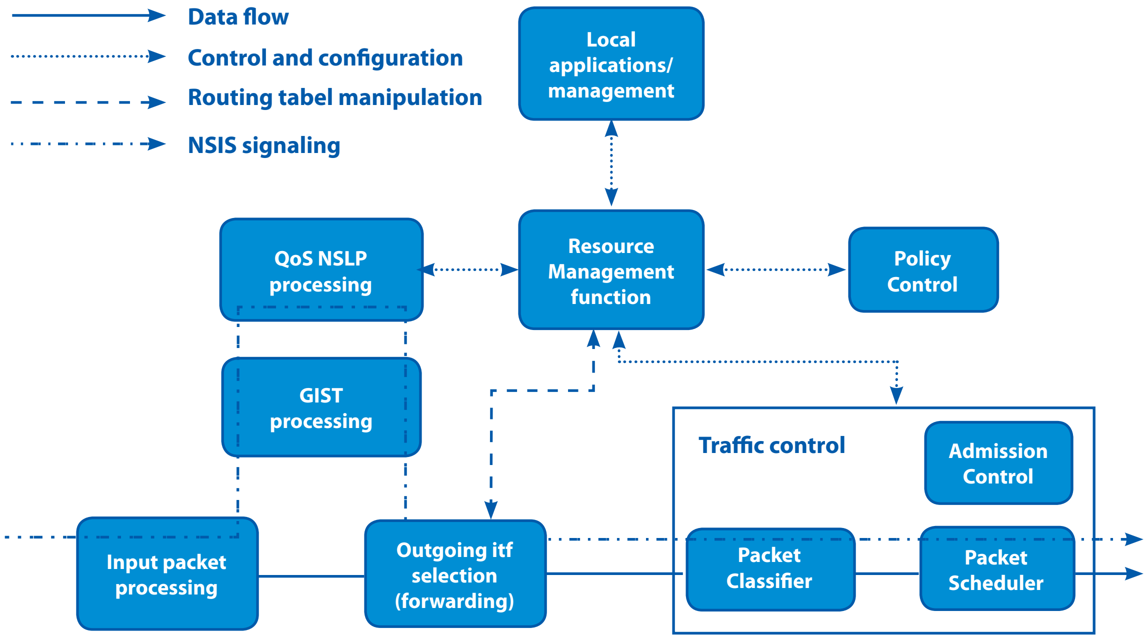


Figure 60 - QoS NSLP interfaces in a router

Figure 60 depicts a basic router model associated to a QoS NSLT implementation. At the core of the model we have the Resource Management Function that can receive control information from one of three possible sources: Policy Control Module, a Local Applications or the QoS NSLP processing module. Considering the QoS NSLP processing module: Whenever a packet is received it must be processed; in case of a NTLP packet such as a GIST packet it is routed to the GIST processing module which provides QoS NSLP message to the QoS NSLP processing module and further lets the packet back to its normal path. Only QoS NSLP messages are forwarded to the QoS NSLP processing module.

QoS NSLP messages can be:

- RESERVE – This directly manipulates the Resource Management Function through a QSPEC object, which can create, update or remove a QoS configuration.
- QUERY – This is used to retrieve information's on a given path to a destination without performing any reservation, constituting a pre-reserve.
- RESPONSE – this message is used to convey the information requested in the QUERY message
- NOTIFY – is used in the same way as the RESPONSE message but needs not to relate to a QUERY and is therefore asynchronous. Used to signal state changes and errors.

The next figure presents two possible QoS Reservation scenarios using QoS NSLP. The Sender-initiated reservation flow is in all-similar to the RSVP use case, while the Receiver-initiated reservation includes an extra QUERY message that is followed by the same signaling flow in the opposite direction.

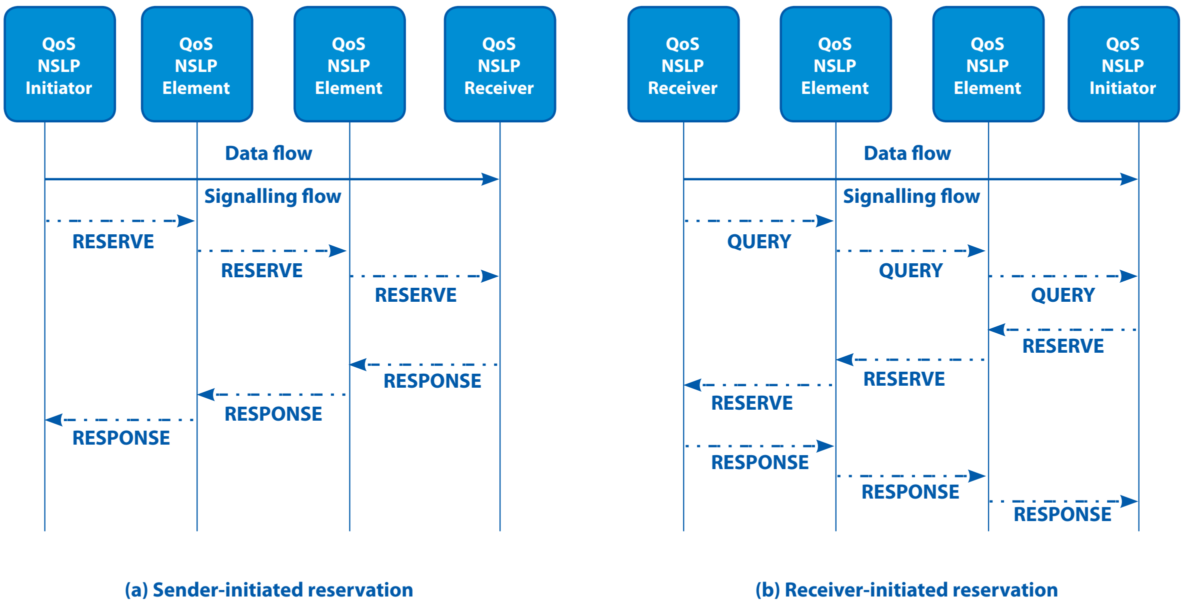


Figure 61 - Reservation scenarios using QoS NSLP

The NSIS charter is nonetheless not concluded, and modifications to the messages and procedures are still expected.