Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2008

Telmo Filipe Ferreira Pereira

Suporte de Qualidade de Serviço e Mobilidade em Redes WiMAX
Quality of Service and Mobility Support in WiMAX networks

"Our revels now are ended. These our actors,
As I foretold you, were all spirits, and
Are melted into air, into thin air:
And like the baseless fabric of this vision,
The cloud-capp'd tow'rs, the gorgeous palaces,
The solemn temples, the great globe itself,
Yea, all which it inherit, shall dissolve,
And, like this insubstantial pageant faded,
Leave not a rack behind. We are such stuff
As dreams are made on; and our little life
Is rounded with a sleep."

William Shakespeare, The Tempest Act, *scene 1, 148-158*


Universidade de Aveiro Departamento de Electrónica, Telecomunicações e
2008 Informática

Telmo Filipe Ferreira Pereira

Suporte de Qualidade de Serviço e Mobilidade em Redes WiMAX
Quality of Service and Mobility Support in WiMAX networks

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia de Computadores e Telemática, realizada sob a orientação científica da Prof[a]. Dr[a]. Susana Sargento, Professora auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

"Well done is better than well said."
Benjamin Franklin

Esta tese é dedicada à minha família, mas especialmente à minha mãe maravilhosa que me apoia todos os dias, desde o meu primeiro dia de escola e ao meu Pai pelo incansável apoio e determinação que me transmitiu.

o júri / the jury

Presidente / president

Doutor José Carlos da Silva Neves
Professor Catedrático da Universidade de Aveiro

Vogais / examiners committee

Doutor Pedro Nuno Miranda Sousa
Professor Auxiliar do Departamento de Engenharia Informática da Escola de Engenharia da Universidade do Minho

Doutor Susana Isabel Barreto de Miranda Sargento
Professora Auxiliar Convidada da Universidade de Aveiro (Orientadora)

agradecimentos / acknowledgments

À Professora Susana Sargento e ao Mestre Pedro Neves pela sua orientação e apoio ao longo das diversas fases da minha tese.
Ao Professor Rui Aguiar, ao Mestre Daniel Corujo e ao Mestre Miguel Almeida pelas dicas importantes e pelas conversas onde me transmitiram sempre perspectivas relevantes do Mundo das Telecomunicações. Sem a sua ajuda, as conquistas da minha investigação nunca teriam sido alcançáveis.
Aos meus amigos por terem sido leitores prévios deste documento, pelos seus comentários e sugestões que permitiram melhorar a qualidade final da minha tese.
Aos meus colegas e membros do meu grupo de investigação, pela sua amizade e proeminente visão critica.

palavras-chave

Redes Heterogeneas, IEEE 802.16, Gestão de Qualidade de Serviço, IEEE 802.21, Mobilidade, Framework de Gestão de Recursos WiMAX.

resumo

O crescimento exponencial da Internet tem imposto um constante incremento da largura de banda no acesso à Internet e serviços conduzindo em grande medida à adopção massiva da *banda larga*.

O IEEE 802.16 é uma recente tecnologia de banda larga sem-fios com o objectivo de fornecer altas taxas de transferência de dados e ampla cobertura que pode atingir as dezenas de quilómetros, numa variedade de formas, desde ponto-a-ponto até acessos do tipo celular com suporte total de mobilidade.

Embora o IEEE 802.16 se apresente como um dos principais candidatos à próxima geração de redes, é igualmente evidente que, num futuro próximo, a combinação de várias tecnologias será necessária. Com base neste princípio, é vital avaliar e descrever o papel que o IEEE 802.16 pode desempenhar nos ambientes de rede heterogéneos da próxima geração.

Esta tese apresenta um extenso estudo da tecnologia de Banda Larga IEEE 802.16, desenvolvido no âmbito de dois projectos europeus, denominados, WEIRD e DAIDALOS, este último já na sua segunda fase.

Os trabalhos desenvolvidos no âmbito do WEIRD estão mais orientados para as redes WiMAX em si, sendo que as suas inerentes capacidades de QoS e o papel assumido pelo 802.16 é, nesta situação, de maior relevo. Uma solução inovadora para controlar dinamicamente os recursos do segmento WiMAX é proposta no presente caso. A solução apresentada está de acordo com as tendências NGN, bem como com as orientações e arquitectura do WiMAX Forum. A interacção com os sistemas WiMAX é efectuada por meio do protocolo SNMP, com base no standard IEEE 802.16f. Além disso, é definida uma camada de abstracção horizontal, escondendo as funcionalidades específicas dos distintos equipamentos WiMAX, proporcionando, assim, robustez e independência de vendedores.

No que diz respeito ao DAIDALOS, foi proposta uma arquitectura distinta de QoS, capaz de fornecer controlo dinâmico de QoS em redes IEEE 802.16, integrá-las com tecnologias heterogéneas e inerentemente integrar a arquitectura com mobilidade. Esta arquitectura usa o IEEE 802.21 com integração de mobilidade e QoS em cenários heterogéneos. O trabalho desenvolvido consistiu essencialmente no desenho, implementação e avaliação de uma aplicação para Controlo de Recursos em Redes WiMAX, e da sua integração com o IEEE 802.21.

Os resultados, obtidos através da experimentação real aplicada a ambas arquitecturas, mostram que é possível fornecer QoS sob cenários dinâmicos, com rapidez de sinalização de mobilidade e QoS integradas.

Keywords

Heteregeneous Networks, IEEE 802.16, QoS Management, IEEE 802.21, Mobility, WiMAX Resource Control Framework

Abstract

The stunning growth of the Internet is imposing higher speed Internet access services and leading in great extent to the broadband adoption.

IEEE 802.16 is a recent wireless broadband technology aiming at providing high data rates over long distances in a variety of ways, from point-to-point to full mobile cellular type access.

Although IEEE 802.16 has emerged as one of the major candidates for next generation networks, it is also clear that in the near future, the combination of several technologies will be required. Based on this, it is vital to evaluate and depict the role that IEEE 802.16 can perform in next generation heterogeneous environments.

This thesis presents an extensive study of Broadband Technology IEEE 802.16, developed under the scope of two European projects, WEIRD and DAIDALOS.

The work developed under WEIRD umbrella is itself more geared to WiMAX networks, exploiting its inherent QoS capabilities, and thus highlighting the IEEE 802.16.

A novel solution to dynamically control the resources of a WiMAX system is proposed in this case. The presented solution is aligned with the NGN trends, as well as with the WiMAX Forum guidelines and architecture. The interaction with the WiMAX systems is performed through SNMP, supporting the standardized IEEE 802.16f MIB and was one of the main focus of this thesis. Furthermore, was defined an horizontal abstraction layer, hiding the WiMAX equipments specific functionalities from the network control plane, thus providing robustness and vendor independency.

In which concerns to DAIDALOS a distinct QoS architecture is proposed, able to provide dynamic QoS in IEEE 802.16 networks, integrate them in heterogeneous technologies and inherently integrate the architecture with mobility. This architecture uses IEEE 802.21 for the tight integration of mobility and QoS in heterogeneous scenarios. Generically it was designed, implemented and evaluated a WiMAX Resource Control Application, that was tightly integrated with IEEE 802.21.

The results, obtained through real experimentation of both implemented architectures, show that it is able to provide QoS under dynamic scenarios, with fast integrated QoS and mobility signalling.

Table of Contents

Index of Figures

Index of Tables

Acronyms

Acronym	*Definition*
AAA	Authentication, Authorization, and Accounting
AC	Admission Control
AF	Application Function
API	Application Program Interface
AR	Access Router
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
ASN	Access Service Network
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BE	Best Effort Service
BFW	Broadband Fixed Wireless
BPSK	Binary Phase Shift Keying
BS	Base Station
BW	Bandwidth
CID	Connection Identifier
CIR	Committed Information Rate
CP	Cyclic Prefix
CPS	Common Part Sublayer
CS	Convergence Sublayer
CSC	Connectivity Service Controller
CSN	Connectivity Service Network
DAD	Duplicate Address Detection
DAIDALOS II	Designing Advanced Network Interfaces for the Delivery and Administration of Location Independent, Optimised Personal Services II
DCD	Downlink Channel Descriptor
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DL-MAP	Downlink Map
DNS	Domain Name Service
DSA-ACK	Dynamic Service Addition Acknowledgment
DSA-REQ	Dynamic Service Addition Request
DSA-RSP	Dynamic Service Addition Response
DSC-ACK	Dynamic Service Change Acknowledgment
DSC-REQ	Dynamic Service Change Request
DSC-RSP	Dynamic Service Change Response
DSD-ACK	Dynamic Service Deletion Acknowledgment
DSD-REQ	Dynamic Service Deletion Request
DSD-RSP	Dynamic Service Deletion Response
DSL	Digital Subscriber Line
E2E	End-to-End
ertPS	Enhanced Real-Time Polling System
ETSI	European Telecommunications Standards Institute

FA Foreign Agent
FDD Frequency Division Duplexing
FEC Forward Error Correction
FHO Fast Handover
FTP File Transfer Protocol
GA Generic Adapter
GHz Gigahertz
GIST General Internet Signalling Protocol
GPC Grant Per Connection
HA Home Agent
HCS Header Check Sequence
HO Handoff
HTTP HyperText Transfer Protocol
Hz Hertz
IE Information Element
IEEE Institute of Electrical and Electronics Engineers
IMS IP Multimedia Subsystem
IP Internet Protocol
ITU International Telecommunication Union
LAN Local Area Network
LEC Local Exchange Carriers
LLC Link Layer Control
LOS Line Of Sight
MAC Media Access Control
MBMS Multimedia Broadcast/Multicast Service
MBS Multicast Broadcast Service
MHz MegaHertz
MIP Mobile Internet Protocol
MN Mobile Node
MS Mobile Station
NAP Network Access Provider
NAT Network Address Translation
NLOS Non Line Of Sight
NMS Network Management System
NRM Network Reference Model
nrt-PS Non Real-Time Polling Service
NSLP NSIS Signalling Layer Protocol
NTP Network Time Protocol
OFDM Orthogonal Frequency Division Multiplexing
OLOS Optical Line Of Sight
PBR Piggyback request
PDU Protocol Data Unit
PDU Protocol Data Unit
PHY Physical Layer
PKM Privacy key Management Protocol
PM Poll-Me bit
PMP Point-to-Multipoint
PS Physical slot

PS	Privacy Sublayer
PSTN	Public Switched Telephone Network
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QoSB	QoS Broker
QoSM	QoS Manager
QPSK	Quadrature Phase Shift Keying
RA	Redline Adapter
RC	Resource Controller
REG-REQ	Registration Request
REG-RSP	Registration Response
RNG-REQ	Ranging Request
RNG-RSP	Ranging Response
RP	Reference Point
RSVP	Resource Reservation Protocol
rt-PS	Real-Time Polling Service
SA	Security Association
SAP	Service Access Point
SDU	Service Data Unit
SFID	Service Flow Identifier
SHO	Soft Hand Off
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SS	Subscriber Station
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time division duplex
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TLV	Type/ length/ value
UCD	Uplink Channel Descriptor
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
UL-MAP	Uplink Map
VLAN	Virtual LAN
VMAC	Virtual Medium Access Control
VoIP	Voice over IP
WEIRD	WiMAX Extensions to Isolated Research Data networks
WiBro	Wireless Broadband
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless local area network based on IEEE 802.11
WWAN	Wireless Wide Area Network

1 Chapter 1: Introduction

Worldwide Interoperability for Microwave Access (WiMAX) is a wireless digital communications system, also known as IEEE 802.16 [802.16-2004], that is intended for wireless metropolitan area networks (MAN). The attractiveness of 802.16 focuses on the capability of running advanced multimedia applications with high-data rates and guaranteed Quality of Service (QoS), but also on the low-cost infrastructure which is involved on its deployment. 802.16 will certainly enrol an important function in next generation networks, bringing the broadband experience to a wireless context gifting the users certain unique benefits and convenience.

Nowadays, 802.16 networks start to proliferate around the world; however, despite their inherent aptitudes and the variety of possible scenarios where they can be applied, it is clear that there is no single technology that has the potential and the economical viability to accommodate all the demands from users and services. In fact, each technology has its own strengths and drawbacks, and 802.16 is 'just' another technology to go alongside with 2G, 3G, DVB, Ethernet and 802.11.

The new mobile paradigm is enabling a new way of working, playing, and communicating, and is also imposing new challenges to the network operators. With this purpose, the integration of multiple wired and wireless technologies is being studied by IEEE under the 802.21 [802.21] umbrella, which is gaining tremendous momentum.

This document presents an extensive study of the emergent broadband wireless access technology IEEE 802.16, focusing aspects such as Quality of Service management and mobility support.

The presented work was developed under the scope of two European projects, WEIRD [WEIRD-IST] standing for WiMAX Extension to Isolated Research Data networks, and DAIDALOS [DAIDALOS-IST] standing for Designing of Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services, at present time in its second phase.

A generic view of these projects is provided, mentioning relevant aspects, as, conceptual approach and network architecture description, to contextualize this thesis.

The main topic throughout this document is the integration of the network technology IEEE 802.16 in the distinct network environments of aforementioned projects, which imposed obviously, distinct interfaces, and personalised modules design, specification, implementation and evaluation.

On one hand, the work developed under WEIRD [WEIRDD2.3] is in its genesis more turned to WiMAX networks, exploiting its QoS capabilities. A novel solution to dynamically control the resources of a WiMAX system is proposed in this case. The presented solution is aligned with the NGN trends, as well as with the WiMAX Forum guidelines and architecture.

On the other hand, DAIDALOS [D2GlobalArch] goes a little bit beyond WEIRD, and the developed WiMAX Resource Controller was integrated in an heterogeneous network environment, with end-to-end quality of service and mobility support. A distinct QoS architecture is proposed, able to provide dynamic QoS in IEEE 802.16 networks, integrate them in heterogeneous technologies and inherently integrate the architecture with mobility. This architecture uses IEEE 802.21 for the tight integration of mobility and QoS in heterogeneous scenarios.

The interaction with the WiMAX systems is performed through SNMP, supporting the standardized IEEE 802.16f MIB, this is one of the common features shared among both WiMAX Resource Control architectures developed.

Furthermore, as a common denominator, in both cases the results, obtained through real experimentation of the implemented architectures show that it is able to provide QoS under dynamic scenarios.

Additionally in DAIDALOS II, the results demonstrate that the implemented architecture is capable of providing dynamic QoS management with fast integrated QoS and mobility signalling.

The developed work enhances the WiMAX as a broadband Wireless access network supplying full QoS Support and mobility bear, key features in the demanding next generation networks.

1.1 Motivation

Worldwide Interoperability for Microwave Access (WiMAX) is a standards-based wireless broadband solution that has emerged as one of the major candidates for next generation wireless networks.

While analyst predictions on the growth of the WiMAX market vary, this technology is expected to capture a sizable share of the existing wireless broadband market. For example, service providers are evaluating potential WiMAX services and capabilities, and the lure of WiMAX is driving many leading equipment manufacturers and component suppliers to formulate strategic partnerships.

Enabling advanced multimedia applications with its high-data rates, and attracting attention with its low-cost infrastructure, WiMAX continues to gain tremendous impetus in the marketplace.

WiMAX has numerous applications that can be tailored to a variety of market segments.

The Figure 1 depicts the breadth of potential WiMAX applications for service providers. It also shows that WiMAX could even be used in the enterprise environment and the transportation and homeland security industries.

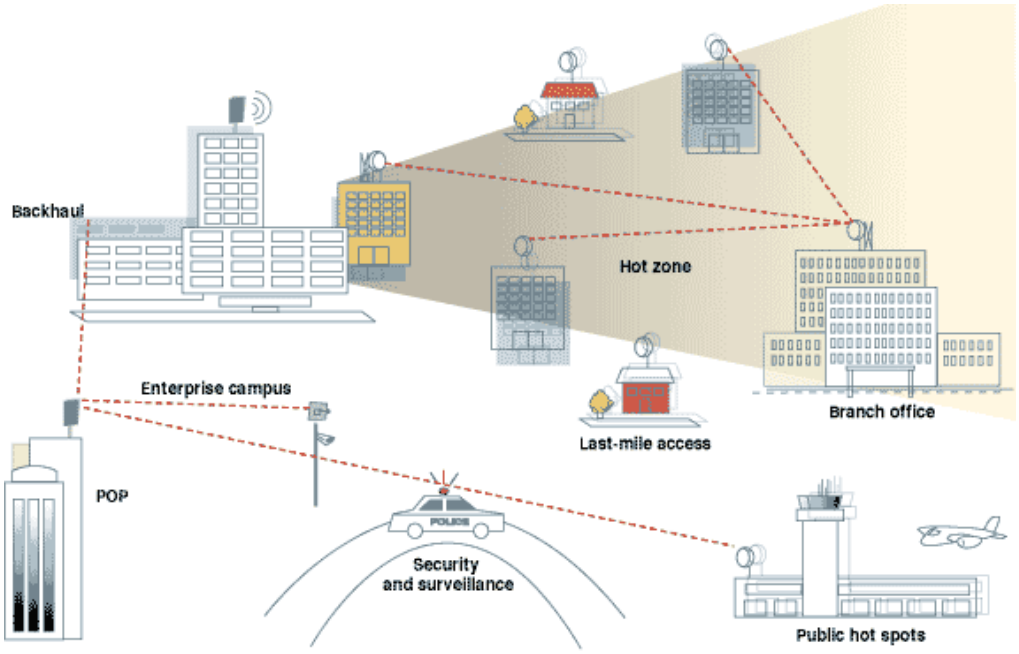

Figure 1: Potential WiMAX applications [WiMAXAppl]

"WiMAX is envisioned as the future leading standardized BWA technology. It effectively addresses several different types of potential customers and situations, especially where alternative DSL solutions [DSLForum] are either not available or not economically viable.

Its ability to support both LOS and NLOS connections make it suitable for ubiquitous service offering in rural and urban areas alike. Its high speed and symmetrical bandwidth can satisfy the needs of individual customers, public administrations, and enterprises of all sizes. Cellular coverage makes its deployment extremely fast and relatively inexpensive.

Some experiments in a variety of countries confirm that expectations in terms of coverage, performance and usage scenarios are indeed justified. Test applications include such different services as fast internet access, high quality audio and video communications, education and entertainment, tele-medicine, tele-metering and telesurveillance.

In the same way WiMAX can be well integrated in fixed or mobile networks, and that it makes an excellent complement to WiFi both as hot-zone feeder and for continuous indoor/outdoor coverage. It can also be effectively paired with DVB-T for implementing T-Government and other highly interactive services.

Aspects like full worldwide interoperability, market diffusion and technological evolution are expected to draw WiMAX equipment costs well below those of any alternative technology available today.

Additionally, as the standard evolves from nomadicity to mobility support [802.16-2005], WiMAX could indeed become the key to fixed/mobile convergence, coming from both ends. If in addition new frequency ranges will be specified, below 2GHz, it could also represent more than a first step beyond current 3G systems.

Depending on the specific market situation and regulation, WiMAX could in the next years represent a unique opportunity to reshuffle the competitive scenario, foster fixed/mobile convergence, overcome possible risks of digital divide, and effectively support economic growth and people welfare in developed and developing countries alike." Figure 2 presents how Wimax is positioned against its possible barriers.

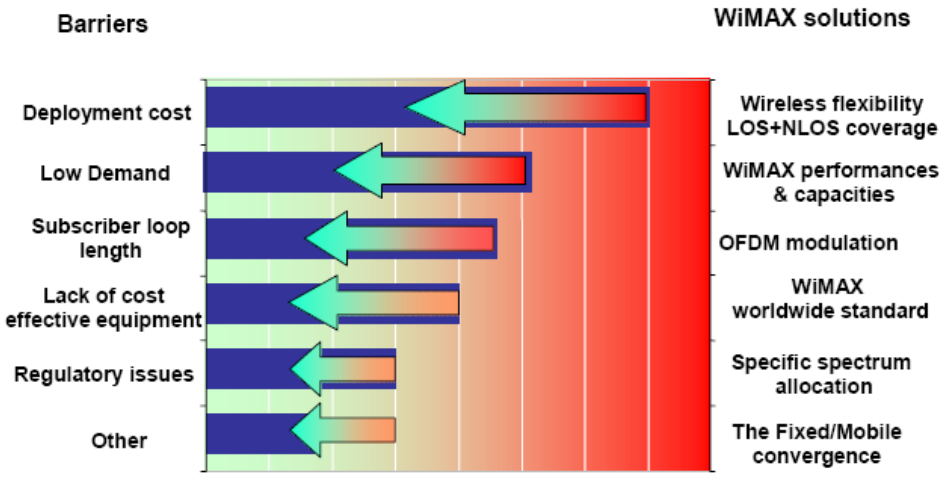

Figure 2: How WiMAX will break the barriers to broadband [DigitalDivide]

The high potential of WiMAX, my personal interests in the networking area, in particular, topics like Quality of Service, mobility and wireless networks, and the presented challenges were sufficiently motivated to choose this Thesis.

1.2 Objectives

This thesis intends to give an including perspective about the IEEE 802.16 technology and about its integration in the next generation networks, having in consideration its inherent challenging and demanding requirements like Quality of Service and Mobility support.

The main objective of this thesis is to enhanced IEEE 802.16 technology integrating it in a heterogeneous network, with support of mobility and Quality of Service. This includes, specify, develop, implement and evaluate part of a network architecture with E2E Quality of Service [WEIRDD2.3][D2_E2E_QoS] and mobility support [QoSMobilityin4G].

More specifically, this thesis can be divided more or less clearly in two phases.

The first one in which is intended to study the supported QoS mechanisms in the 802.16 technology and to design a common approach to WiMAX Radio Access Control by means of the SNMP, supporting the standardized IEEE 802.16f MIB[802.16f].

And a second phase in which is aimed to implement and evaluate a WiMAX Radio Resource Controller to supply QoS Management in the WiMAX segment and provide means to allow mobility support, concerning the distinct WEIRD and DAIDALOS II distinctive requirements.

1.3 Publications

The work carried out under the subject of this thesis was published/submitted in two conferences and one magazine.
The work accomplished in the first phase of WEIRD project was published in the *13th IEEE Symposium on Computers and Communications (**IEEE ISCC08, April 2008**)* [Neves-ISCC2008], comprising the specification and evaluation of the developed and implemented QoS architecture.
The work developed under the scope of DAIDALOS II was submitted to the *16th IEEE International Conference on Network Protocols (IEEE ICNP08 - July 2008).* This paper presents the integration of IEEE 802.16 in an heterogeneous network environment with dynamic QoS Management and mobility support, evaluating the signalling and data performance of the implemented modules.

1.4 Document Outline

The report is organized in chapters, and each chapter is structured into sections and eventually sub-sections. The document structure is summarized here:

- Chapter 2 presents the background of this thesis, giving an overview of some existent broadband access technologies. The WiMAX technology is either way the main focus, including the key aspects of the PHY and MAC layers while emphasising its QoS features. This chapter also describes the main characteristics of the 802.16 equipment used throughout this thesis and the 802.21 Framework along with IP mobility state of the art.

- Chapter 3 provides a brief overview of WEIRD project architecture, as well as the DAIDALOS II project architecture. The overview is centred in the QoS models adopted, but also depicts the mobility support among other important features.

- Chapter 4 discusses how to accomplish Resource Management in WiMAX, presenting the common architectural aspects among WEIRD and DAIDALOS implemented systems. It details the common steps taken to accomplish this thesis, including the design and specification.

- Chapter 5 illustrates Radio Resource Control architecture in WEIRD, detailing implementation aspects. It also shows and discusses the performance results obtained for the implement solution, considering the PTP and PMP modes of operation, different Convergence Sub layers, and detailed evaluation of WiMAX equipment performance, and modules processing time.

- Chapter 6 presents the WiMAX Radio Resource Control architecture developed under the scope of DAIDALOS and the evaluation of the implemented architecture. Both control and data plane have been assessed.

- Chapter 7 presents the conclusions of the accomplished work, as well as the future work.

2 Chapter 2: Background

This chapter presents the background of this thesis, briefly mentioning some existent broadband access technologies, but evidently focusing the IEEE 802.16 technology and its QoS aspects.

This chapter also presents a small overview of the emergent standard IEEE 802.21, still in draft version and the IP Mobility State of Art, which helps to contextualize the work developed under DAIDALOS scope.

2.1 Broadband Technologies

Today, the Internet is impacting the way we live, work, play and learn. It is a place where we can find the products, services, solutions, shortening the distance of people around the world.

However, to enjoy the complete benefits of the Internet, broadband connections are required. As a consequence, Internet broadband connectivity has become one of the most widespread communications developments ever and the growth in demand for high-speed Internet connections is set to continue.

Most people today experience broadband communications via a PC connected over a fixed line (usually DSL or cable). However, many of the broadband users expect to get online anytime and anywhere. In this case, a fixed line is simply not an option and wireless networks, such as WiMAX, may be their primary broadband access method.

There are a set of technologies competing to deliver commercial mobile broadband services.

The solutions based on radio connections used in the access networks, usually called by WLL (Wireless Local Loop) or FWA (Fixed Wireless Access), facilitate the deployment and allow to serve rapidly a sort of potential clients. However, for long time there was no standardization and consequently no price limitation. This type of scenario is not beneficial, either in economical terms or when considering that a proprietary solution deployment poses the fabricant in negotiable advantage over the operator.

At this point, WiMAX IEEE 802.16 comes to take the lead in terms of broadband wireless networks, widespreading the use of wireless radio access and making this type of solution economically viable.

The massive use of this type of broadband technologies is envisioned. WiMAX is expected to be massively adopted by new operators that do not have any type of access network infrastructure.

By far the most mature broadband wireless access technology at present time is HSPA, which is actually the greatest WiMAX competitor.

2.1.1 HSPA

The third generation WCDMA radio access technology approached 44 million subscribers worldwide in 2005, according to World Cellular Information Service, and is continuing to grow with an accelerated pace. However, to maintain WCDMA competitiveness in the long-term future, it is necessary to further develop today's standard. The first steps of this evolution have already been taken by the 3rd Generation Partnership Project (3GPP) through the additions of High Speed Downlink Packet Access (HSDPA) and Enhanced Uplink to WCDMA
High Speed Packet Access, which is commonly seen as a software upgrade to the 3G network infrastructure, that allows higher data rates. It consists on a collection of *mobile telephony protocols* that extend and improve the performance of existing *UMTS* protocols. Two standards, *HSDPA* and *HSUPA*, have been recognized.
HSDPA refers to High Speed Downlink Packet Access and HSUPA stands for High Speed Uplink packet access. This means that each version corresponds respectively to an improvement of data rates in the downlink direction and in the uplink.
HSPA has a great legacy, coming from the GSM family, which delivers mobile communications to over a third of the world's population. The evolution has seen familiar acronyms such as GPRS (the first packet technology giving around 128kb/s) to EDGE (an enhanced version offering around 240kb/s) and then the introduction of 3G networks increasing the data rate to 384kb/s.
The various enhancements on the HSPA route are as follows:

- HSDPA – High Speed Downlink Packet Access – the ability to receive large files to your mobile device such as email attachments, PowerPoint presentations or web pages. HSDPA 3.6mbps network can download a typical music file of around 3Mbytes in 8.3 secs and a 5Mbps video clip in 13.9 secs. Speeds achieved by HSDPA top 14.4Mb/s but most network operators provide speeds up to 3.6Mbps, with the rollout of 7.2Mbps quickly growing. HSDPA networks have been around for about 2 years and are deployed and offering mobile broadband right across the world. For a full list of HSPA networks, *click here*.

- HSUPA – High Speed Uplink Packet Access – this is a further enhancement to increase the speed by which you communicate from your mobile device – for example, this enables you to upload videos to YouTube in secs so that you can share the experience in real time. The upload speeds which were at 384kb/s with HSDPA are now increased to a maximum of 5.7Mb/s.

Common terms used by mobile network operators to market the service are: 3G+, NextG, 3G Broadband, 3.5G and many more. It is impossible to appoint a certain favourite among WiMAX and HSPA technologies. We can only note that the whole world started using HSDPA earlier than WiMAX. However, in Russia the situation is the opposite - WiMAX is already in use.

2.1.2 IEEE 802.16

Broadband Wireless is a fairly new technology that provides high-speed *wireless internet* and *data network* access over a wide area.

Broadband wireless is about bringing the broadband experience to a wireless context, which offers users certain unique benefits and convenience. There are two different types of broadband wireless services, the fixed wireless broadband and the mobile broadband as defined in [WimaxFund] .

The FWB provides a set of services similar to that of the traditional fixed-line broadband but using wireless as the medium of transmission. On the other hand the *mobile broadband,* offers the additional functionality of portability, nomadicity and mobility.

WiMAX (worldwide interoperability for microwave access) technology, the subject of this thesis, is designed to accommodate both fixed and mobile broadband applications and is currently one of the hottest technologies in wireless, providing high throughput broadband connections over long distance; it's to say, at speeds up to 70 Mbps and average coverage between 5 to10 km.

More technically, WiMAX is a layer 1 (PHY or Physical layer) and layer 2 (MAC or Media Access Control layer) technology that does not define connectivity at the network layer, or layer 3. IEEE leaves 3rd parties to innovate and standardize at the higher layers. The result is that WiMAX is positioned to connect to a wide array of legacy systems, either the IP cores of wireline carriers, or the IP cores of wireless operators. In particular, IP Multimedia Subsystem, or IMS based cores based on 3GPP standards offer a clear opportunity to provide internetwork roaming, compatibility with 3G cellular, IP based Quality of Service and common application while leveraging investments made in existing core networks. Connectivity at the IP layer also makes WiMAX a natural extension of other networks using Seamless Mobility.

2.1.2.1 IEEE 802.16-2004 PHY Layer Short perspective

The WiMAX physical layer is based on orthogonal frequency division multiplexing. OFDM is the transmission scheme of choice to enable high-speed data, video, and multimedia communications and is used by a variety of commercial broadband systems, including DSL, Wi-Fi [Wi-Fi], Digital Video Broadcast-Handheld (DVB-H), and MediaFLO, besides WiMAX. OFDM is an elegant and efficient scheme for high data rate transmission in a non-line-of-sight or multipath radio environment.

OFDM belongs to a family of transmission schemes called multicarrier modulation, which is based on the idea of dividing a given high-bit-rate data stream into several parallel lower bit-

rate streams and modulating each stream on separate carriers, often called subcarriers, or tones.

Multicarrier modulation schemes eliminate or minimize intersymbol interference by making the symbol time large enough so that the channel-induced delays are an insignificant (typically, <10 percent) fraction of the symbol duration.

OFDM is a spectrally efficient version of multicarrier modulation, where the subcarriers are selected such that they are all orthogonal to one another over the symbol duration, thereby avoiding the need to have nonoverlapping subcarrier channels to eliminate intercarrier interference.[WimaxFund].

The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe *channel* conditions — for example, attenuation of high frequencies at a long copper wire, narrowband interference and frequency-selective fading due to *multipath* — without complex equalization filters. Channel *equalization* is simplified because OFDM may be viewed as using many slowly-modulated *narrowband* signals rather than one rapidly-modulated *wideband* signal. Low symbol rate makes the use of a *guard interval* between symbols affordable, making it possible to handle time-spreading and eliminate inter-symbol interference (ISI).

2.1.2.2 IEEE 802.16-2004 MAC Layer

802.16 is a connection-oriented MAC in the sense that it assigns traffic to a service flow and maps it to MAC connection using a CID. In this way, even connectionless protocols, such as IP and UDP, are transformed into connection-oriented service flows. The connection can represent an individual application or a group of applications sending with the same CID [QoSin802.16]. And, the service classes defined in 802.16 are ATM-compatible. Internetworking with ATM is important due to its legacy role in telecom carrier infrastructure and its common use in DSL services.

The WiMAX MAC layer is illustrated on Figure 3. The MAC layer of 802.16 is divided into two sublayers: the convergence sublayer and the common part sublayer.

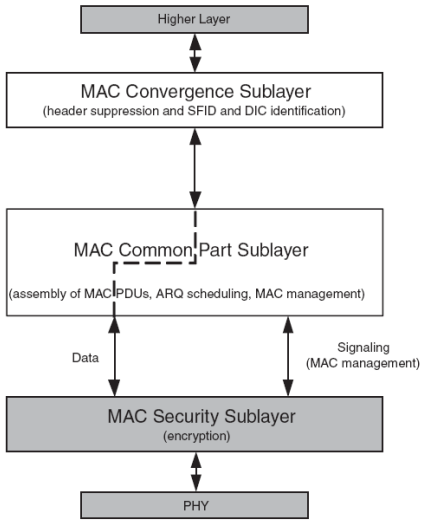

Figure 3: WiMAX MAC Layer [802.16-2004]

The convergence sublayer maps the transport-layer-specific traffic into the core MAC common part sublayer. As the name implies, the convergence sublayer handles the convergence of ATM cells and IP packets, so the MAC layer can support both ATM services and packet services, such as IPv4, IPv6, Ethernet, and VLAN services. The common part sublayer is independent of the transport mechanism, and is responsible for fragmentation and segmentation of the SDUs into MAC protocol data units (PDUs), QoS control, and scheduling and retransmission of MAC PDUs.

The convergence sublayer classifies the incoming Service Data Units (SDUs) by their type of traffic and assigns them to a service flow using a 32-bit SFID. When the service flow is admitted or active, it is mapped to a MAC connection that can handle its QoS requirements using a unique 16-bit CID. A service flow is characterized by a QoS Parameter Set which describes its latency, jitter and throughput assurances. And with Adaptive Burst Profiling, each service flow is assigned a PHY layer configuration (i.e. modulation scheme, Forward Error Correction scheme, etc.) to handle the service.

Once the service flow is assigned a CID, it is forwarded to the appropriate queue. Uplink packet scheduling is done by the BS through signalling to the SS. At the SS, the packet scheduler will retrieve the packets from the queues and transmit them to the network in the appropriate time slots as defined by the Uplink Map Message (UL-MAP) sent by the BS [QoSin802.16]. Figure 4 depicts this process.

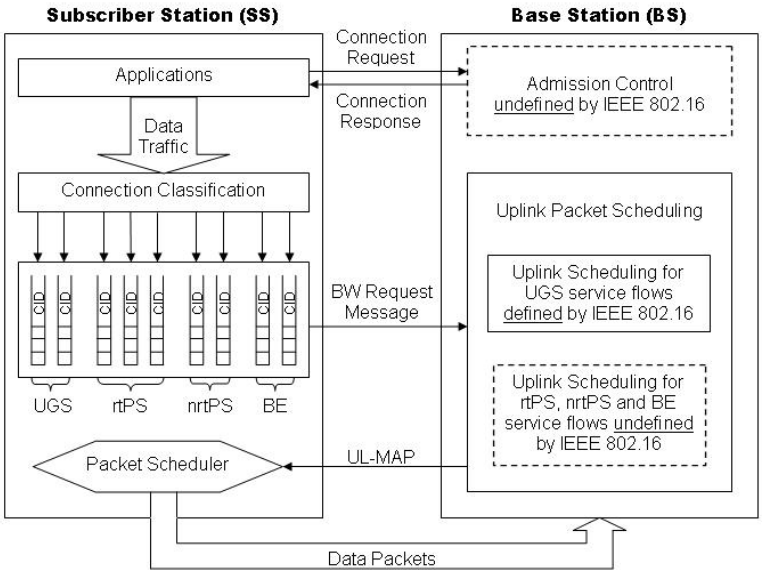

Figure 4: IEEE 802.16 QoS architecture [802.16-2004]

The IEEE 802.16 QoS architecture can handle multiple levels of QoS through its classification, queuing, and control signalling mechanisms.

The common part sublayer is independent of the transport mechanism. It performs the fragmentation and segmentation of MAC service data units (SDUs) into MAC protocol data units (PDUs). MAC PDUs can be concatenated into bursts having the same modulation and coding. The scheduling and retransmission of MAC PDUs is done in this sublayer. The common part sublayer also performs QoS control. The control signalling for the bandwidth request and grant mechanisms are performed in this sublayer.
WiMAX systems were designed at the outset with robust security in mind. Security is handled by a privacy sublayer within the WiMAX MAC (MAC Security Sublayer) that provides key aspects of WiMAX secutiry like: support for privacy by means of AES(Advanced Encryption Standard) or 3DES (Triple Data Encryption Standard), user authentication through an authentication framework based on the Internet Engineering Task Force (IETF) EAP, protection of control messages by means of digest schemes, such as AES-based CMAC or MD5-based HMAC and support for fast handovers(mechanisms of pre-authentication and re-authentication to accelerate the process).

2.1.2.3 IEEE 802.16 Reference Architecture

The network reference model developed by the WiMAX Forum NWG [802.16-WG] defines a number of functional entities and interfaces between those entities. Some of the more important functional entities are illustrated in Figure 5.

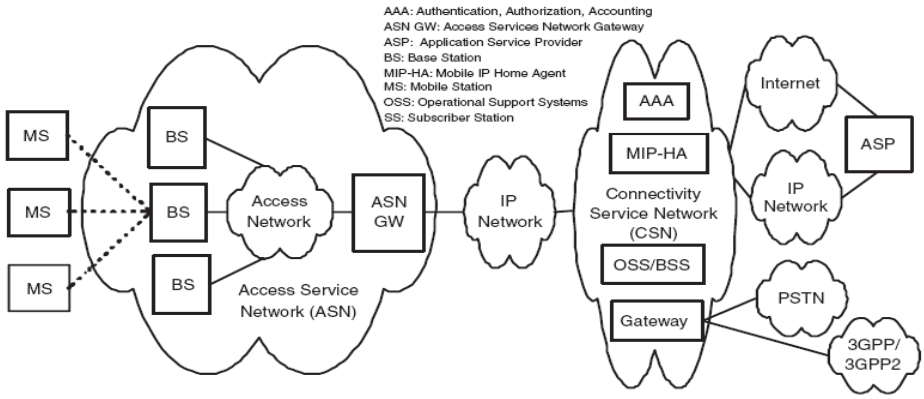

Figure 5: IP based network architecture [802.16-WG]

As defined in [WimaxStg2] the ***BS*** is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micromobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy [RFC2131][RFC3315], session management, and multicast group management.

The ***ASN gateway*** typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management and admission control, caching of subscriber profiles and encryption keys, AAA client functionality, establishment and management of mobility tunnel with base stations, QoS and policy enforcement, foreign agent functionality for mobile IP, and routing to the selected CSN.

The ***CSN*** provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs. Further, CSN can also provide gateways and interworking with other networks, such as PSTN (public switched telephone network), 3GPP, and 3GPP2.

2.1.2.4 QoS and Service Flows management

Per-flow quality of service (QOS) is probably WiMax's strongest differentiator from other wireless access technologies. Wi-Fi has IEEE 802.11e [802.11e], which supports limited prioritization on a single connection between the endpoint and the Wi-Fi access point. WiMax, on the other hand, allows multiple connections between a subscriber station and a base station, and each connection can have its own QOS attributes.

IEEE 802.16 defines four types of QOS:

- ***Unsolicited Grant Service (UGS)***, designed to support constant- bit-rate applications, such as T1 emulation and voice over IP (VOIP) without silence suppression.
- ***Real-Time Polling Service (rtPS),*** for applications that generate periodic variable-size packets, like MPEG and VOIP with silence suppression.
- ***Non-Real-Time Polling Service (nrtPS)***, which supports applications like FTP that generate variable-size packets on a regular basis.
- ***Best Effort (BE) Service***, for low-priority applications like Web surfing.
- ***extended real-time polling service (ertPS)***, a new scheduling service introduced with the IEEE 802.16e standard, builds on the efficiencies of UGS and rtPS.

To implement the QOS levels, the base station polls the subscriber stations for bandwidth requests and schedules the requests it receives. The frequency and regularity of the polling depends on the QOS type of each subscriber station's connections. For example, rtPS connections receive periodic unicast polls, while BE connections are never polled individually, but must respond to multicast "contention request opportunities" or piggyback their requests on data traffic.

2.1.2.4.1 Service Flows

In WiMAX accordingly to [WimaxFund] a Service Flow is basically characterized by:

- *Service flow ID*, a 32-bit identifier for the service flow.
- *Connection ID,* a 16-bit identifier of the logical connection to be used for carrying the service flow. The CID is analogous to the identity of an MS at the PHY layer. As previously mentioned, an MS can have more that one CID at a time, that is, a primary CID and multiple secondary CIDs. The MAC management and signalling messages are carried over the primary CID.
- *Provisioned QoS parameter set*, the recommended QoS parameters to be used for the service flow, usually provided by a higher-layer entity.
- *Admitted QoS parameter set,* the QoS parameters actually allocated for the service flow and for which the BS and the MS reserve their PHY and MAC resources. The admitted QoS parameter set can be a subset of the provisioned QoS parameter set when the BS is not able, for a variety of reasons, to admit the service with the provisioned QoS parameter set.
- *Active QoS parameter set*, the QoS parameters being provided for the service flow at any given time.
- *Authorization module,* logical BS function that approves or denies every change to QoS parameters and classifiers associated with a service flow.

An SF may have one of several statuses: provisioned, admitted or activated.

- Provisioned: A service flow is provisioned by for example a NMS but not resource is reserved yet.
- Admitted: This type of service flow has resources reserved by the BS, but these parameters are not active (its ActiveQoSParamSet is null). Admitted Service Flows may have been provisioned or may have been signalled by some other mechanism.
- Active: This type of service flow has resources committed by the BS for its ActiveQoSParamSet, (e.g., is actively sending maps containing unsolicited grants for a UGS-based service flow). Its ActiveQoSParamSet is non-null.

2.1.2.5 IEEE 802.16e-2005

It is not possible to proceed to next section without summarily mention the IEEE 802.16e-2005 specification, normally referred as mobile WiMAX, which is the mobile version of the 802.16 standard.
This new amendment aims at maintaining mobile clients connected to a MAN while moving across BS's. It supports portable devices from mobile smart-phones and personal digital assistants (PDAs) to notebook and laptop computers. IEEE 802.16e works in the 2.3 GHz, 2.5 GHz and 3.5 GHz frequency bands. It specifies scalable OFDM (OFDMA) for the physical layer and makes further modifications to the MAC layer to accommodate high-speed mobility.

The mobility framework defined in IEEE 802.16e, includes the definition of:

- Signalling mechanisms for tracking stations as they move across one base station to another when active or as they move from one page group to another when idle.
- Protocols to enable seamless handover of ongoing connections from one base station to another.

The IEEE 802.16e specification includes several improvements to the original IEEE802.16-2004, which are following summarized in [YAUNGMobFi]:

- The already referred support for mobility is the major feature of mobile WiMAX, which introduces new MAC messages for handover and allows a MS to maintain a connection when moving from one BS to another. Mobile WiMAX is designed to support mobility applications up to 160 km/h.
- High connection availability in NLOS environments can be supported in mobile WiMAX by using advanced antenna, channel coding, subchannelization, and dynamic modulation technologies to increase link budget.
- New technologies have been introduced in mobile WiMAX. These include support for intelligent antenna technology, such as Multiple-Input Multiple-Output (MIMO) and adaptive antenna system (AAS), high-performance coding, such as turbo coding

(TC), and a Hybrid Automatic Repeat reQuest (HARQ) mechanism for increasing NLOS performance.

- Based on the security features of the fixed WiMAX standard, the mobile WiMAX specification introduces a number of enhancements. For example, the AES as well as 3DES are now a mandatory feature. New high performance coding schemes, such as TC and low-density parity check (LDPC), are included. These features enhance the security of the mobile WiMAX air interface.
- Both the connection and service-type-based QoS are designed to meet the requirements of mobile broadband services. These two QoS mechanisms manage both UL and DL directions and support two-way traffic, such as VoIP. The mobile WiMAX QoS has the features of service multiplexing, low data latency, and varying granularity to support real-time broadband multimedia applications.

For a complete end-to-end system, particularly in the context of mobility, several additional end-to-end service management aspects need to be specified. This task is being performed by the WiMAX Forums Network Working Group (NWG) [WiMAX]. The WiMAX NWG is developing an end-to-end network architecture and filling in some of the missing pieces.

It should be noted that the IEEE 802.16e-2004 and IEEE 802.16-2005 standards specifications are limited to the control and data plane aspects of the air-interface. The generic management procedures and services are defined in IEEE 802.16g [802.16g].

2.1.2.6 RedMAX AN-100U Overview

This section presents an overview of the WiMAX equipment, used throughout this thesis.

2.1.2.6.1 Introduction

The WiMAX equipment RedMAX AN-100U [REDCOM] used in this thesis is a carrier class IEEE 802.16-2004 compliant wireless device for deployment of point-to-multipoint (PMP) and point-to-point (PTP) systems.

It is composed by an indoor terminal (IDU) and outdoor transceiver and antenna (ODU). The WiMAX system is comprised of a RedMAX AN-100U and two WiMAX Forum Certified subscriber stations, used to deploy a point-to-multipoint system. Each subscriber station registers and establishes a bi-directional data link with the AN-100U sector controller.

The RedMAX AN-100U base station enforces the Quality of Service (QoS) settings in the WiMAX segment by controlling all uplink and downlink traffic scheduling providing non-contention based traffic with predictable transmission characteristics.

The AN-100U operates in the frequency 3.4480GHz. The maximum channel size is 7 MHz which allows up to 35 Mbps over the air rate and up to 23 Mbps data rate.

The AN-100U system uses time division duplexing (TDD) to transmit and receive on the same RF channel, or using separate RF channels using half-duplex FDD (HD-FDD). It supports coding rates of 1/2, 2/3, and 3/4 and BPSK, QPSK, 16 Quadrature Amplitude Modulation (QAM), and 64 QAM modulation.
The maximum range is 20 Km LOS or 3 Km none LOS.
One of most relevant features of the RedMAX AN-100U relating this thesis is the SNMP support by standard and proprietary MIBs. In any way, other interfaces are supported, as the HTTP, FTP and Telnet/CLI interfaces.

2.1.2.6.2 Service Flows

Service flows are a key feature of the 802.16 standard. A service flow represents a unidirectional data flow. Transmitting bidirectional traffic requires that two service flows be defined: one for the uplink, and another for the downlink. These service flows can have different QoS settings.

2.1.2.6.2.1 Service Flow Classification

Data packets are forwarded by the AN-100U based on classification rules. Classification rules require examining each packet for pattern matches such as destination address, source address. All classification is defined at the AN-100U and the classification parameters are downloaded to the subscriber.

2.1.2.6.2.2 Dynamic Service Addition

Service flows are defined and stored in the AN-100U. For each service flow to be established, the AN-100U sends a setup message to the subscriber station specifying the required set of QoS parameters. The subscriber station responds to each request by accepting or rejecting the setup message.
A service flow may be pre-provisioned or can be dynamically created and deleted without service outage. This is useful for supporting multiple subscribers in a single sector.

2.1.2.6.2.3 Scheduling

The AN-100U enforces QoS settings for each service flow by controlling all uplink and downlink traffic scheduling. This provides non-contention based traffic model with predictable transmission characteristics. By analyzing the total of requests of all subscriber stations, the AN-100U ensures that uplink and downlink traffic conforms to the current service level agreements (SLAs).
Centralized scheduling increases traffic predictability, eliminates contention, and provides maximum opportunity for reducing overhead.

A regular period is scheduled for subscriber stations to register with the AN-100U. These subscriber stations may be newly commissioned or have been deregistered due to service outage or interference on the wireless interface. This is the only opportunity for multiple subscriber stations to transmit simultaneously.
The 802.16 equipment is restricted in terms of service classes support. Only two classes are supported.

Real-Time Polling Service (rt-PS)
The AN-100U schedules a continuous regular series of transmit opportunities for the subscriber station to send variable size data packets. The grant size is based on the current data transfer requirement. Typical applications include streaming MPEG video or VOIP with silence suppression. This is efficient for applications that have a real-time component and continuously changing bandwidth requirements.

Best Effort (BE)
The AN-100U schedules transmit opportunities for the subscriber station to send traffic based on unused bandwidth after all higher level traffic scheduling requirements are serviced. Typical applications may include Internet access and email.

2.2 Mobility

The new mobile paradigm is enabling a new way of working, playing, and communicating. However, it is also imposing new challenges to the network operators. This section presents the state of art in terms of IP mobility but also recently studies towards localized mobility management and the framework 802.21, which is under development at standardization level to assist mobility management procedures across heterogeneous access technologies.

2.2.1 IEEE 802.21

IEEE 802.21 [802.21D9] is an emerging standard that supports a set of uniform procedures and services to allow smooth interaction and media independent handover between 802 technologies and other access technologies.
The standard provides information to allow handing over to and from *cellular*, *WiFi*, *Bluetooth*, *802.11* and *802.16 networks* through uniform handover mechanisms.
The standard is a power enabler of seamless handover between different network types but it also can be used across homogeneous networks.
The standard, still under development specifies handover-enabling functions within the mobility-management protocol stacks of the network elements and the creation therein of a new entity called the MIH Function (MIHF). These functions facilitate handover decision,

providing link layer state information to MIH users. Enabling low latency handovers across multi-technology access networks. It defines the methods and semantics that facilitate the acquisition of heterogeneous network information and the basic content of this information, thereby enabling network availability detection.

Finally it specifies command procedures that smooth the progress of seamless service continuity across heterogeneous networks.

Summarily IEEE 802.21 offers an open interface that:

- supplies a uniform link state event reporting in real time throughout Event Service
- provides intersystem information, automatically and on demand by means of Information Service
- allows an 802.21 user to control handover through Command Service

Next figure illustrates the IEEE 802.21 Services:

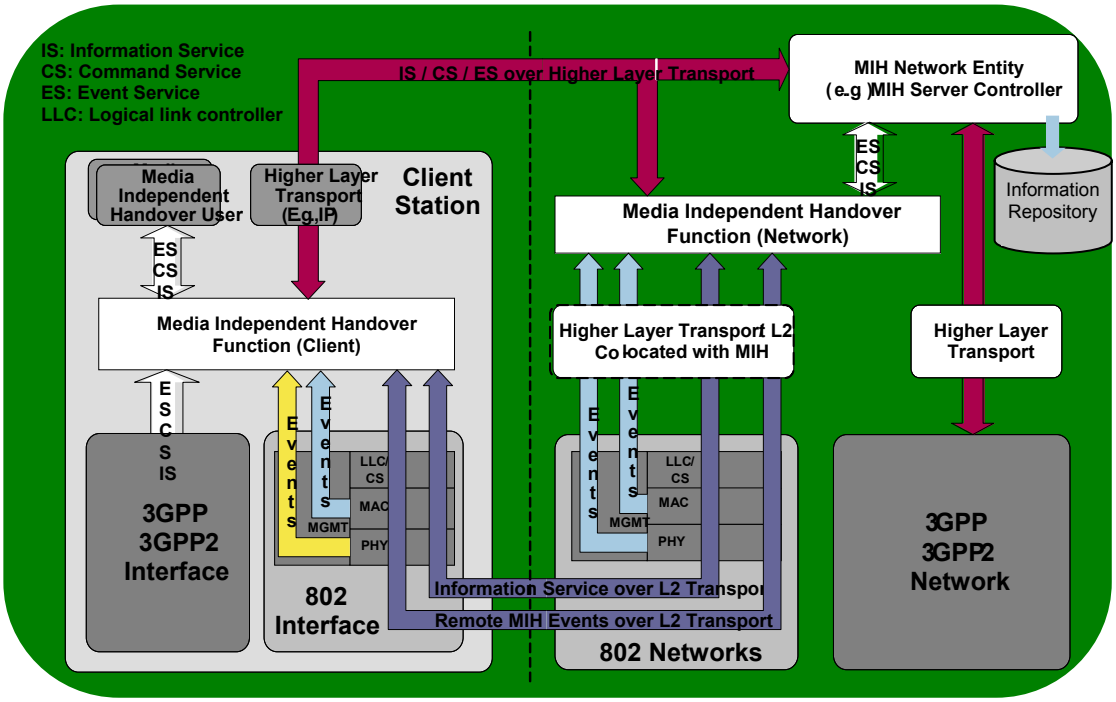

Figure 6: IEEE 802.21 Services

IEEE 802.21 is composed by several entities:

- Media Independent Handover Function (MIHF): MIH is a cross-layer entity that provides mobility support through well defined Service Access Points offering Event, Information and Command services
- MIH User: a local entity that avails of MIHF services through the MIH Service Access Points
- MIH Network Entity: a remote entity that is able to communicate with an MIHF over a transport that supports Media Independent Services

The MIH Function provides three services:

- **Event Service** detects events and delivers triggers from both local as well as remote interfaces (i.e. between terminal and network; e.g. Link_available, Link_up, Link_down, etc.)
- **Command Service** provides a set of commands for the MIH users to control handover (e.g. MIH_Link_Switch, MIH_Configure_Link, MIH_Handover_Initiate, etc.)
- **Information Service** provides the information model and an information server to make more effective handover decisions. The mobile terminal obtains information from the repository using its current network point of attachment or the target point of attachment (e.g. list of available networks, network operator, IP version, neighbour information, etc.)

IEEE 802.21 is a cross-layer entity interaction with multiple layers. It decisively facilitates handover determination through a technology-independent unified interface to MIH users and eases both station initiated and network initiated handover determination. It, also, smoothes the progress of handover determination, providing a technology-independent unified interface for upper layers and MIH users.
It eases both Mobile Initiated and Network Initiated Handovers determination. Both local and remote triggers are supported.

2.2.2 IP Mobility

Nowadays, the network architectures are evidently converging towards all-IP networks. IP networks gained a tremendous popularity for data communications and more recently for voice communications.
It is well known that mobility was not part of the IP protocol fundamentals design, therefore the mobility support only appeared afterwards, conducting to multiple solutions, with particular strengths and weaknesses. At the present time, it was not found yet a unique protocol that can optimally address all types of mobility scenarios, and actually, it is quite improbable that we can find one soon.
Mobile IP was the first suggested mechanism to allow users to change their point of attachment in an IP network, however this protocol has several essential missing features to solve all the requirements of future all-IP networks. This was a fundamental reason to commonly split the mobility issue into two, macro-mobility and micro-mobility.
On one hand, macro-mobility refers to the management of users moving at a large scale, between wide wireless access networks, and normally assumed to be managed through Mobile IP. On the other hand micro-mobility covers the management of users moving at a local level, usually a particular network or domain. In the second case many solutions have been proposed, usually called IP Micro-mobility protocols.

This section presents some of most prominent proposals to handle mobility in IP based networks, focusing only on the IP version 6 guises. Two micro mobility solutions are depicted, Fast Mobile IPv6 [RFC4068] and Hierarchical Mobile IPv6 [RFC 4140]. Also two recent and interesting approaches to micro-mobility, with a distinct perspective of Localized Mobility Management, still under study, are mentioned, the so called NetLMM [RFC 4831][RFC 4830] and PMIPv6.[PMIPv6-Draft]

2.2.2.1 FMIPv6

Mobile IPv6 is a fairly accepted global mobility (macro-mobility) protocol that allows a mobile node to arbitrarily change its location across IPv6 networks while still maintaining existing connections. This is accomplished by handling the change of addresses at Layer 3 by means of Mobile IPv6 messages options and extensions ensuring transparency for transport and above layers, whilst a correct delivery of data regardless of the mobile node's location. Thus, even though the mobile node changes locations and addresses, the existing connections through which the mobile node is communicating are maintained since the connections to mobile nodes are made with a specific address that is always assigned to the mobile node, and through which the mobile node is always reachable. The Mobile IPv6 and its mechanisms are detailed in the RFC [RFC3775].

Fast Handovers for Mobile IPv6 [RFC4068] is an extension to Mobile IPv6. Its main goal is to reduce the number of packets that are lost during a handover by allowing the mobile node to use its previous Care of Address until the mobile node has completed the registration of its new Care of Address at the new access network. This also allows to and to decrease the signalling delay.

This is done by establishing a tunnel between the two involved access routers that allows the mobile node to send packets as if it was connected to its old access point while it is completing its handover signalling at its new access point. At the same time, this alleviates the registration delay, since the mobile node may acquire information needed to join a new link before disconnecting communication at the old link. The approach is based on co-operating access routers which can request information from other access routers that are feasible candidates for a handover.

The protocol consists of several improvements to Mobile IPv6, and the standard [RFC4068] divides the protocol into three phases: handover initiation, tunnel establishment, and packet forwarding. The mobile host uses the received information to prepare itself for the handover, which it can perform in many cases entirely without packet loss, even though connectivity to the network will be lost for a short period of time.

Even though not necessary, the fast handover approach performs even better if the mobile node can be connected at more than one link at any one time, avoiding this way link layer disruption during handovers. This is true for most of the existing protocols.

2.2.2.2 HMIPv6

The Hierarchical Mobile IPv6 Mobility Management standard [RFC 4140] suggests an alternative optimization for Mobile IPv6 which can be seen as complementing the Fast Handovers for Mobile IPv6.

The basis of Hierarchical Mobile IPv6 is to localize the management of the handoffs which reduce the amount of signalling. Simultaneously, it will also improve the effectiveness of MIPv6 in terms of handoff speed. This is typically a good approach to handle mobility across heterogeneous access technologies and well suited to implement access control.

The HMIPv6 tends to reduce the latency of performing the Binding Update procedure by using a Mobility Anchor Point (MAP) that is located topologically near the current location of the mobile node. The MAP acts as a local home agent. A mobile node that needs to move to a new point of attachment in the network, only needs to register its new care of address at its current MAP. As the MAP should be topologically close to the mobile node, this update procedure can be performed rapidly. The mobile node may also benefit from a decreased number of signalling messages as route optimization may not be needed when Hierarchical Mobile IPv6 is used, and only the current MAP needs to be updated instead of a potentially large number of correspondent nodes.

When the MN moves into MAP coverage, it asks the MAP for a Regional Care-of-Address (RCoA) from which the MAP will forward packets to the MN. Once the MN has obtained an RCoA, it uses this address in its BUs to HA and CNs.

A MAP covers a number of access networks. While a mobile node moves within the coverage of a MAP it need not re-bind its HA or CNs, thus signalling is reduced. Since the MN is generally closer to the MAP than its correspondent nodes, signalling latency is also reduced.

The mobile node sends Binding Updates to the local MAP rather than the HA (which is typically further away) and CNs.

Only one Binding Update message needs to be transmitted by the MN before traffic from the HA and all CNs is re-routed to its new location. This is independent of the number of CNs that the MN is communicating with.

A MAP is essentially a local Home Agent. The aim of introducing the hierarchical mobility management model in Mobile IPv6 is to enhance the performance of Mobile IPv6 while minimising the impact on Mobile IPv6 or other IPv6 protocols. It also supports Fast Mobile IPv6 Handovers to help Mobile Nodes achieve seamless mobility.

2.2.2.3 NetLMM

During the last decade, host-based mobility approach was the only solution for mobility management having in MIP, generically described as the main mobility enabler. Some of its debilities, in terms of performance and functionalities are well known. This lack of functionalities in MIPv6, in particular the inability to handle nodes moving speedily has lead to intensive studies and developments mostly along the lines of local optimization, such as FMIPv6 and HMIPv6.

However these two aforementioned mobility techniques are host-based, where hosts have to handle the signalling and to be aware of local and global signalling protocols.

So in fact, there are a significant number of mobiles nodes without Mobile IPv6 support and it is desirable to support IP mobility for all hosts, independently of the presence or absence of mobile IPv6 functionality. Based on this, new approaches are being developed, shifting the signalling management from the host to the network, where Proxy Mobility [PMIPv6-Draft]is the most emergent and mature scheme.

Related activities are also studying the standardization of Localized Mobility Management (NetLMM) [RFC 4831][RFC 4830], which is under intensive development by IETF group.

New works on global mobility management approaches other than Mobile IPv6 suggests that a localized mobility management approach decoupled from the global mobility management protocol might result in a more modular mobility management system design.

This suggests a design paradigm that could be used to accommodate global mobility management protocols of different types while not increasing software complexity: a network-based, localized mobility protocol with no mobile node software to specifically implement localized mobility management and no requirement for a network interface to change IP address when the mobile node changes to a new router.

The NetLMM protocol is scalable to topologically large networks, but requires no host stack involvement for LMM. This brings relevant advantages such as support for hosts without any mobility management protocol, and avoiding overhead over the air.

Mobility anchor points within the backbone network maintain a collection of routes for individual mobile nodes.

The routes point to the access routers on which mobile nodes currently are located. Packets for the mobile node are routed to and from the mobile node through the mobility anchor point. When a mobile node moves from one access router to another, the access routers send a route update to the mobility anchor point. While some mobile node involvement is necessary and expected for generic mobility functions such as movement detection and to inform the access router about mobile node movement, no specific mobile node to network protocol will be required for localized mobility management itself.

2.2.2.4 PMIPv6

PMIPv6 is one of the most recent localized mobility protocols, based on some of NetLMM design principles. According to [PMIPv6-draft] a proxy mobility agent in the network performs the signalling with the home agent and does the mobility management on behalf of the mobile node attached to the network. Because of the use and extension of Mobile IPv6 signalling and home agent functionality, this protocol is referred to as Proxy Mobile IPv6 (PMIPv6). Figure 7 shows its main components.

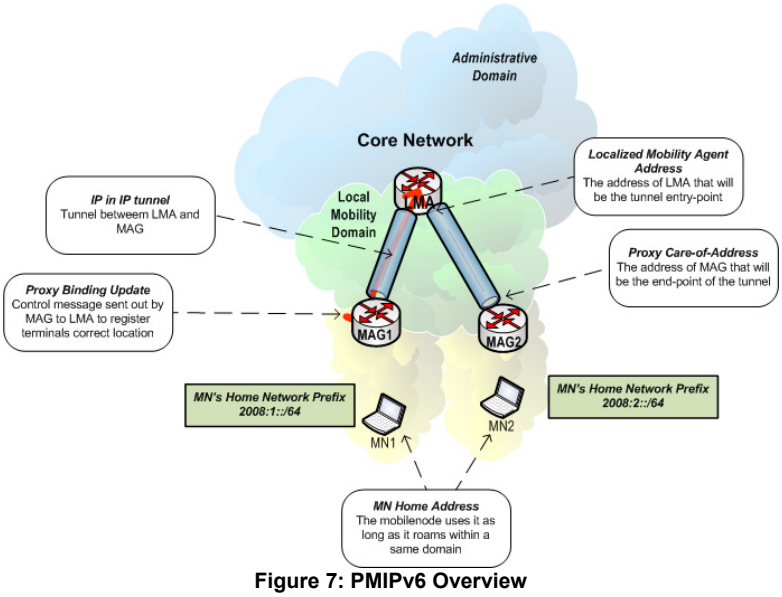

Figure 7: PMIPv6 Overview

PMIPv6 is a network-based mobility management protocol aiming at local mobility support, while reusing when possible MIPv6 entities and concepts.

This protocol differentiates the nodes by means of a MN-ID, with set of associated parameters that are saved in a Policy Store Server (AAA) accessible by PMIP entities.

Thus this protocol assumes that upon MN attachment the node is authenticated, providing the necessary information to ensure that the network can retrieve the Home Network Prefix of the MN and emulating the MN Home Network behaviour.

A typical message sequence chart is illustrated on Figure 8.

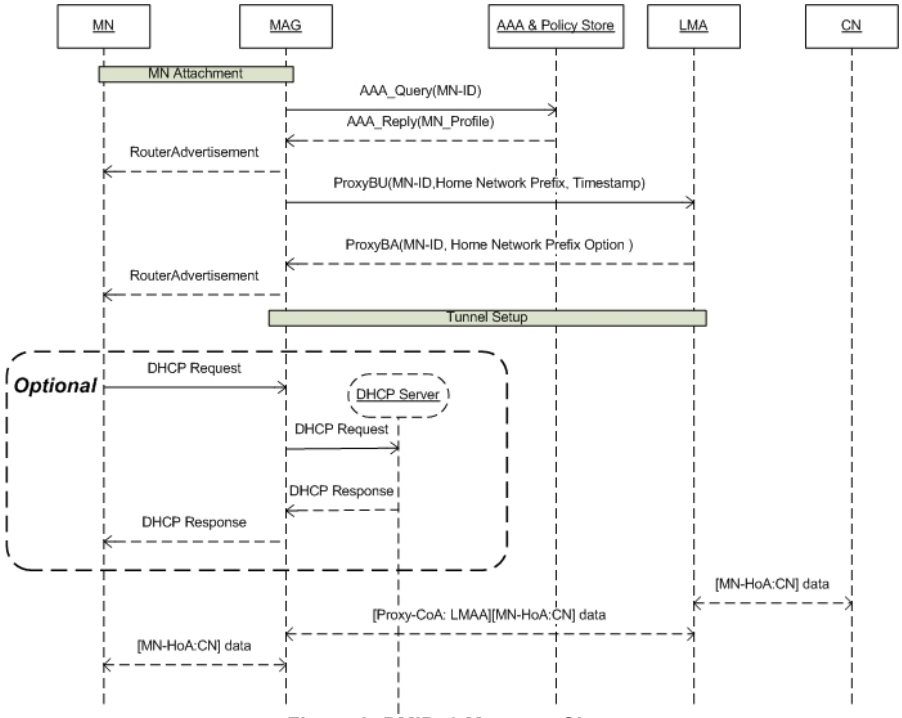

Figure 8: PMIPv6 Message Chart

The MAG manages the mobility related signalling for a mobile node, sending the customized Router Advertisement or DHCP relay functions. It also tracks the mobile node's attachment to the link and for signalling the MN's LMA.

The mobility signalling consists on Binding Updates to the MN's Home Agent.

LMA is basically the Home Agent for the mobile in the PMIPv6 domain. It assign's the MN's home prefix and manages the MN's reachability state.

2.3 Related Work

There are already several proposals in the literature that address the support of QoS and/or mobility in IEEE 802.16 networks. As an example, [Mobility_in_802.16d] addresses the mobility support for IEEE 802.16d wireless networks, proposing techniques to handle connection handoff and correct reception for moving terminals in IEEE 802.16d without any change in the specification. However, its focus is on layer 2, and the presented solution is only micro-mobility, and much centred on WiMAX segment. Moreover, there is no consideration of heterogeneousness or QoS. In [ABC_QoSModel] it was proposed an Always Best Connection (ABC) model in a WLAN and WiMAX heterogeneous network. However, the analysis is only based on simulations and the solution is not extended to other technologies. In [802_21WMAN_WLAN] it is presented a platform to enable interworking between WLAN and WMAN (mobile Wimax), based on IEEE 802.21 framework [802.21]. QoS Adaptation was one of the interesting aspects of this paper; nevertheless the study does not specify how to perform end-to-end QoS neither it considers mobility. [RSVPDynamicManag] studied the

bandwidth allocation of RSVP connections together with the bandwidth management of the layer 2 connections in WiMAX/WLAN environment. This work explored the flexibility of 802.16d [802.16-2004] for dynamic environments. Nonetheless, mobility across heterogeneous environments was not mentioned and the work was focused on bandwidth management and negotiation mechanisms between BS and SS. Moreover, it is well-known that RSVP does not work properly with changing end-point identifiers [RFC 4094].

In terms of real experimental evaluations there is few related work such as [Pentikousis-WiNMee2008]. However, the empirical evaluations conducted on this work do not evaluate the behaviour of real time applications when dynamically adapting the resources of WiMAX segment. Finally, in [Neves-ISCC2006] it is proposed a QoS architecture for 802.16 in heterogeneous scenarios, also able to support mobility. However, it does not consider this close integration of mobility through 802.21 QoS-enabled, as is supported in this thesis.

2.4 Summary

Throughout this chapter the background of this thesis was exposed. A small vision about broadband access technologies was presented, mentioning, HSPA (future LTE), probably the major competitor of the upcoming WiMAX. Afterwards the attention was given to the elucidation of IEEE 802.16 technology characteristics, focusing key aspects of PHY and MAC layers. This chapter also describes the main characteristics of the 802.16 equipment used throughout this thesis. The IEEE 802.21 Framework along with IP mobility state of the art was also referred, describing interesting approaches to network localized mobility management, which inspired DAIDALOS II specification.

3 Chapter 3: WEIRD and DAIDALOS II architecture Overview

This chapter gives a small overview of the WEIRD and DAIDALOS II architecture to contextualize the developed work.
The supplied vision is more focused in the QoS models of the two European projects, but in DAIDALOS case, mobility is also exposed.
WEIRD's architecture is deeply based on the WiMAX Forum reference architecture [WimaxStg2][WiMAXForumStg3] considering the functional entities as Subscriber Station (SS) / MS (Mobile Station), Access Service Network (ASN) and Connectivity Service Network (CSN).
The DAIDALOS architecture goes beyond WEIRD and is doubtless more futuristic and innovative.

3.1 High Level view of the WEIRD Architecture

The architecture considered in WEIRD as described in [WEIRDD2.3] and illustrated in Figure 9 is *vertically* structured into two "macro-layers", '*Application and Service Macro-Layer'* and '*Transport Macro-Layer'*. Horizontally the architecture may be traditionally divided into *Management Plane (MPl)*, *Control Plane (CPl)* and *Transport/Data Plane (DPl)*. This approach follows the recent architectural trends, which aim at decoupling the applications and services from transport technologies, in order to allow heterogeneity in the core and access.

Vertical decomposition:

- *Applications and Service layer* includes the architectural layers and functions performing *management, control* and also *operations of data* (e.g. adaptation, transcoding, etc.) at higher layers, independently of network transport.
- *Transport Macro-Layer* includes the architectural layers and functions performing *management, control* for resources and traffic and also *operations on data* in order to transport the data traffic through various networking infrastructures.

Horizontal decomposition:

- *Management Plane(MPl)*: - performs management functions generally-medium and long term related to service management at the Application and Service Layer macro-layer and resource and traffic management at Transport layer. It provides coordination between all the planes. The following management functional areas identified in ITU-T Rec.M.3010 [M.3010] are performed in the management plane: FCAPS – Fault, Configuration, Accounting, Performance, Security management.

Each architectural layer may have its own layer-manager associated with it; also a general management macro-layer may exist, to coordinate all layer managers.

- *Control Plane (CPl)* includes all layers which perform short term control actions related to higher layers (high level services and applications): through signalling, the control plane sets up and releases high level connections, and may restore a connection in case of a failure; transport layers: CPI performs the short term actions for resource and traffic engineering and control, including routing.

- *Data Plane (DPl) (also Called Transport Plane)* is mainly responsible for transferring the user/ application data. In case of IP architectures the data plane also transports (via unique IP) the control and management related data between the respective entities. The DPl may include functions and mechanisms to act upon the packets transported. In multi-domain environment the transport stratum may be split in inter and intra-domain parts.

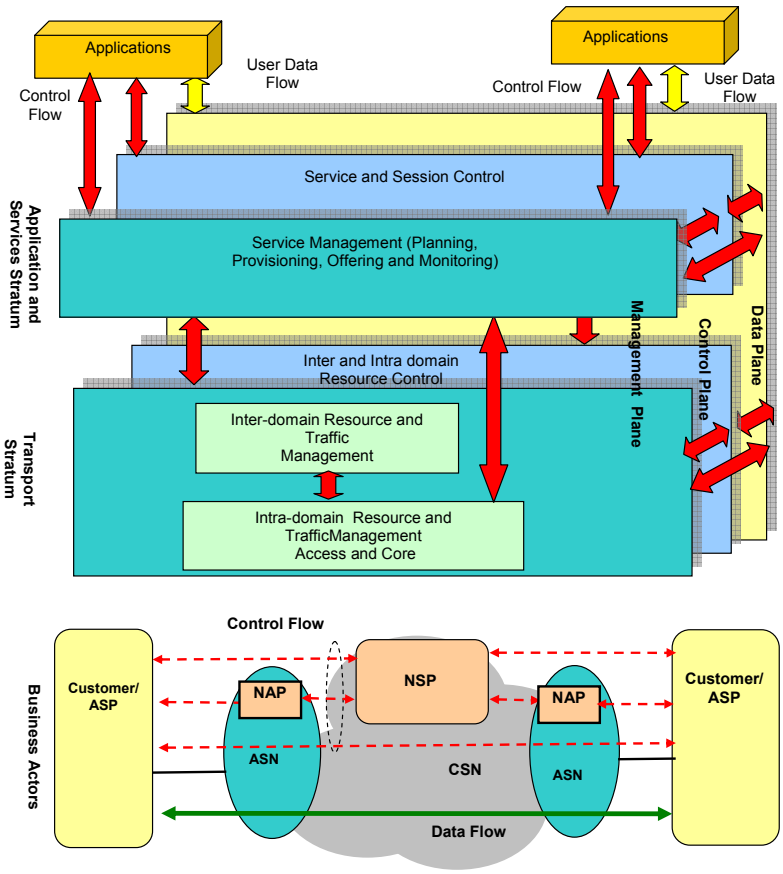

Figure 9: General architectural planes in a multi-domain environment [WEIRDD2.3]

The WEIRD system is layered according to the architecture model described above. The applications are running on the client endpoints and are located in the highest layer of the model. The WEIRD application and service layer contains a signalling control channel to let

applications to ask for services. This control channel lets applications to request QoS in the local AS (including WiMAX channel).

The application service control plane is located at Application and Service Layer providing session and service control to the applications. It communicates upward with applications, either by APIs or application signalling protocol(s), like SIP [RFC3261] or RTSP. It communicates downwards with the WEIRD control plane, which provides Resource and Control functions, by control signalling.

The WEIRD resource control plane is located in the lower vertical macro-layer – Transport Layer and performs typically transport of data and resource control.

3.1.1 WEIRD QoS Model

WEIRD architecture offers different levels of QoS to the high level services/applications while using the IEEE 802.16 classes of services UGS, rt-PS, ert-PS, nrt-PS, BE, contributing this way to end-to-end QoS assurance by appropriate interfaces with CPE and CSN.

Applications have been split according to Table 1:

	Customizable	***Legacy***
SIP-based	Some SIP and/or SDP [RFC3264] extension(s) shall be needed, according to the adopted QoS model and SF triggering scheme.	Off-the-shelf SIP clients, with at least a Best Effort QoS model.
no-SIP-based	Use of WEIRD API on client side.	Use of WEIRD Agent on client side.

Table 1: Applications classification

For the session based services, the WEIRD architecture aims to support two different QoS models, the *QoS assured* and the *QoS enabled.*

The QoS a*ssured* model, specifies that a call can be established only if the requested/required QoS can be set; that is to say, the QoS setup becomes a *precondition* for calls.

In the *QoS enabled* model the availability of QoS resources does not affect the success of a call; it only affects the effective level of QoS associated to the call.

WEIRD considers two QoS triggering models.

*1. QoS triggering and reservation initiation from A*F

An application function (AF) located in the home CSN is the common method to support service flow creation. In this scenario, the SS/MS directly communicates with the AF through application layer control protocols. The AF may request to Resource Control to reserve and allocate resources.

The AF is responsible to trigger WiMAX service flow creation, admission and activation through the service controller (CSC) located in the ASN.

2. QoS triggering from endpoint

The QoS can be triggered by the endpoint using on-path QoS signalling (e.g. RSVP [RFC2205], NSIS [NSIS]) to request activation in the ASN. This is made possible by the use of a suitable WEIRD API on the MS/SS side to let applications request resource reservation.

Table 2 resumes the QoS provisioning modes:

	Customizable	***Legacy***
SIP-based	Triggered from AF or from MS/SS side using WEIRD API	AF triggering only by the use of SIP clients.
No-SIP-based	Use of WEIRD API for Resource Request from SS/MS and QoS-NSLP [NSLP] for resource reservation along the data flow path.	Use of WEIRD Agent on client side.

Table 2: Qos Provisioning modes for the different types of applications

To finish this section we have to distil WEIRD *Control Plane* modules and interfaces, which are presented in Figure 10 are deeply detailed in [Neves-ISCC2008].

The presented architecture is based on WiMAX Forum Network Reference Model, nonetheless new modules have been defined on the *Control Plane* to efficiently support real time services with QoS differentiation. As aforementioned, both SIP [RFC3261] and legacy applications are supported. For SIP-based applications, the *SIP User Agent* (SIP UA) in the MS communicates directly with the *SIP Proxy* at the CSN. For legacy applications, a specific module is specified for the MS – the *WEIRD Agent* – which adapts and configures the QoS parameters as required by legacy applications.

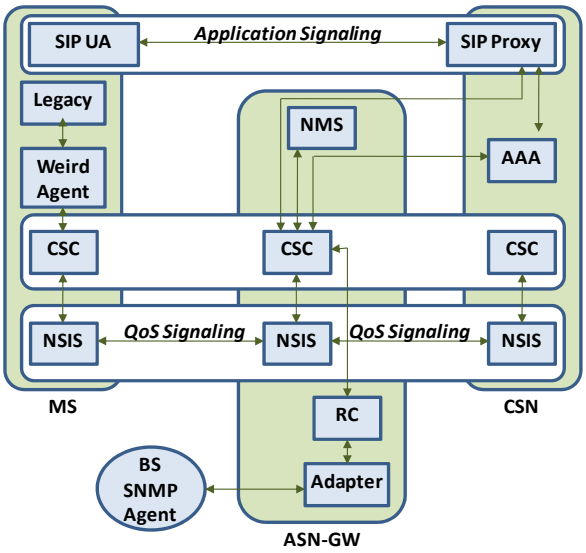

Figure 10: WEIRD Architecture – Control Plane [Neves-ISCC2008]

The *Connectivity Service Controller* (CSC) modules include the most important functions of the system. Since WEIRD is focused on the ASN segment, the CSC at the ASN (*CSC_ASN*) is the main coordination point for QoS functions, such as resource allocation and admission control in the ASN and the WiMAX segments. For SIP applications, the *SIP Proxy* extracts the QoS parameters from the SIP/SDP [RFC3264] messages, performs user authentication and authorization with the AAA server, and forwards the collected QoS information to the *CSC_ASN* using a Diameter (Gq/Gq') [Diameter] interface.

CSC_MS communicates with the *WEIRD Agent* to obtain the QoS parameters required by the legacy applications and provides this information to the main QoS coordination point (*CSC_ASN*). When the *CSC_CSN* receives the QoS reservations requests from the *CSC_ASN,* it establishes the QoS paths on the core network. Moreover, the *CSC_ASN* has an interface with the Network Management System (NMS) for medium- and long-term functions, such as QoS provisioning.

The communication between the several *CSCs* (MS, ASN and CSN) is performed through the usage of the Next Steps in Signalling (NSIS) QoS signalling protocol [NSIS]. *NSIS* decomposes the overall signalling protocol suite into a generic (lower) layer and specific upper layers for each specific signalling application. At the lower layer, General Internet Signalling Transport (*GIST*) [GIST] offers transport services to higher layer signalling applications. Above this layer, the *NSIS* Signalling Layer Protocol (*NSLP*) [NSLP] supports any protocol within the signalling application layer.

All functions related with the WiMAX system are managed and controlled by the *Resource Controller* (RC), which can be seen as the *WiMAX link manager*. The *RC* is responsible for the QoS management in the WiMAX link, including *Service Flows* (SFs) and *Convergence Sublayer* classifiers control (including Ethernet, IPv4 and IPv6 classification), as well as for admission control tasks on the WiMAX link. Furthermore, the *RC* acts as an *abstraction layer* between the upper parts of the architecture and the lower level modules. It hides all WiMAX technology related functionalities from the upper layers, keeping them independent and oblivious of WiMAX-specific QoS characteristics. To enforce the QoS decisions on the WiMAX BS, the *RC* triggers the *Adapter* module that will communicate the decisions to the WiMAX BS through an SNMP interface. The initial proposed model of WiMAX *Adapter* is presented in [NissilaAdapter]. It is split into a *Generic Adapter* (*GA*) component and one or more *Vendor-Specific Adapter* (*VSA*) modules.

With this approach, different WiMAX equipments can be integrated into the WEIRD architecture by developing a *VSA* for each new vendor equipment, if necessary. From all modules defined on the WEIRD architecture, *VSAs* are the only *dependent* on the specific WiMAX equipment used.

3.2 DAIDALOS II - Overview

DAIDALOS II [DAIDALOS-IST] is the second phase of the Integrated Project DAIDALOS that continues the research on beyond 3G architectural concepts and components.
One of the most concerning aspects of DAIDALOS project is the heterogeneous network integration thematic. With the current evolution of network technologies, leading with the heterogeneity assumes an enormous relevance since it is crucial to deal with this fast technological progress, providing usable and manageable communication infrastructures for the future.
The DAIDALOS goal is a seamless, pervasive access to content and services through heterogeneous networks. The project aims at working towards an environment, where the mobility is fully established through scalable and seamless integration of a complementary range of heterogeneous technologies, enabling mobile users to enjoy a diverse range of personalised services, seamless supported by the underlying technology and transparently supplied by the pervasive interfaces.

The DAIDALOS is guided by five 5 key concepts explained on [D2GlobalArch] that are summarily described in next lines:

- ***MARQS*** – consists on bringing together Mobility Management, AAA, Resource Management, QoS and security, supporting this way functional integration for end-to-end services across heterogeneous technologies.
- ***VID*** – aims to separate the user from the device, while keeping the things secure and maintaining the user privacy, providing a Virtual Identity to the user.
- ***USP*** - (Ubiquous and Seamless Pervasiveness) are the capability of enabling pervasiveness across personal and embedded devices, and allowing adaptation to changing contexts, movement and user requests.
- ***SIB*** – (Seamless Integration of Broadcast), which integrates broadcast at both the technology level, such as DVB-S/T/H, and at services level, such as TV and data-cast.
- **Federation** - which will enable network operators and service providers to offer and receive services, allowing users to enter and leave the field in a dynamic business environment.

3.2.1 Main QoS Architecture

This section gives an overview of the QoS architecture [D2_E2E_QoS], presenting and depicting some of its most relevant concepts and components. This architecture has been developed under the framework of the IST-Daidalos project [DAIDALOS-IST]. The QoS

architecture merges a hierarchical organization of data-path network elements with off-path control functions. A hierarchical network topology combined with strategic placement of QoS and mobility control entities allowing support of integrated QoS and mobility over heterogeneous networks was considered.

Figure 11 illustrates the hierarchical approach for the network architecture. It shows an Administrative Domain with three Local Mobility Domains, each connected to two Access Networks.

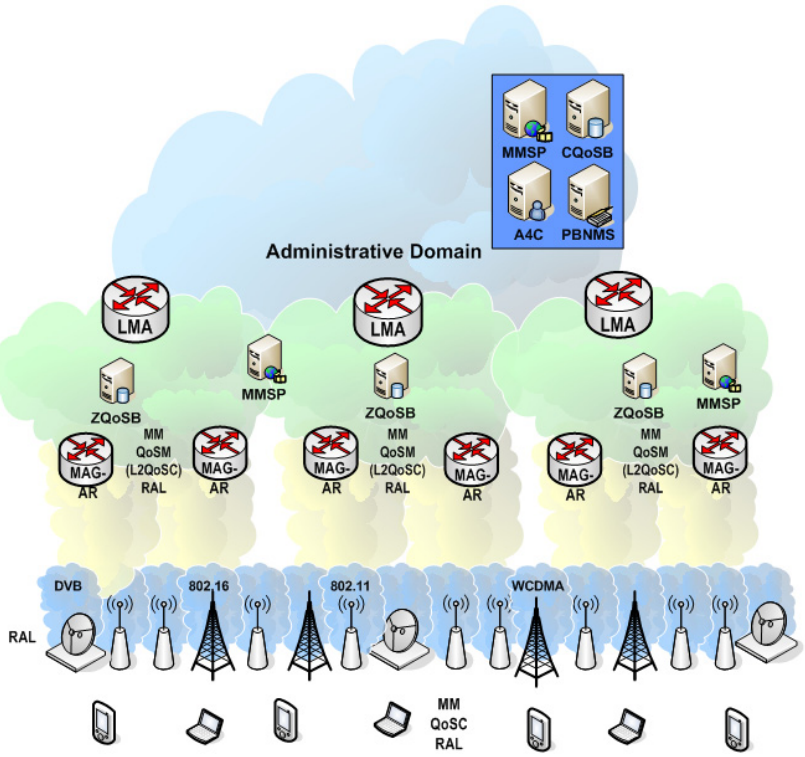

Figure 11: QoS network architecture

The QoS control is achieved separating end-to-end QoS control at layer 3 from link-local (layer 2) QoS control.

The Zone QoS-Brokers (ZQoSBs) manage the layer 3 QoS inside the Local Mobility Domains (LMDs), being responsible for the execution of a wide range of functions, such as resource management inside the Local Domains, per-flow admission control, handover authorization and performance optimization based on both user requirements and network availability. Inside the Core Network (CN) we have Core QoS Brokers (CQoSB) managing the CN and inter-domain functions using Differentiated Services (DiffServ) model of resource management. In the core it is also in place an Authentication, Authorization, Accounting, Auditing and Charging (A4C) server that manages user accounts and interfaces with QoS modules for authorization purposes, a Multimedia Service Proxy (MMSP) bearing multimedia services with inherent QoS, and finally a Policy-based Network Management System (PBNMS), containing the policies to manage the QoS network elements.

Now, highlighting the access network, both Mobile Terminals (MTs) and the Access Routers (AR), here denoted as Mobility Access Gateways – Access Router (MAGs-AR), contain

elements that perform the enforcement of the QoS in the network and trigger the QoS process for admission control and resource reservation: QoS Client (QoSC) and QoS Manager (QoSM), respectively in the MTs and MAGs-AR. The handling of reservations at Layer 2 is performed by a L2 QoS Controller (L2QoSC). The specific characteristics and reservation handling of each technology are executed by a Radio Access Layer (RAL) – WiMAX_RAL for the 802.16 technology.

The stratified QoS network architecture aims at ensuring scalability, making possible per-flow resource management in wireless access where restricted and precious radio resources should be managed effectively.

3.2.2 General Mobility Architecture overview

In terms of mobility, DAIDALOS considers the separation of local and global mobility. Under this concept and referencing Figure 11, each LMD is managed by Local Mobility Anchor (LMA).

The LMA is a representative element, similar to Mobility Anchor Points from HMIP, which localizes the signalling traffic and hence reduces the handoff latency. LMA maintains a collection of routes for individual mobile nodes.

The routes point to the access routers (MAG-ARs) on which mobile nodes currently are located. Packets for the mobile node are routed to and from the mobile node through the LMA.

The most important feature resulting from this hierarchy is that the terminal is not required to reconfigure itself (i.e. obtain a new IP address) each time a handover occurs. Hence independent local mobility schemes are supported in distinct LMDs.

As mentioned above, and proceeding with our high level description, each LMD integrates different ANs which may comprise several technologies. This implies that QoS support over heterogeneous technologies must be in place and mobility mechanisms have to be considered to support seamless mobility across these heterogeneous links.

Under DAIDALOS architecture mobility mechanisms supporting seamless mobility are coupled with QoS provisioning mechanisms.

IEEE 802.21 was adapted as the control plane protocol, covering both vertical and horizontal handovers. This allowed the MIH mechanisms to complement data plane control protocols. In DAIDALOS case, as mentioned before, the MIPv6 is used for GMD, and NetLMM for LMD. Daidalos considers a MIHF at every entity, either network or mobile terminal, allowing for full exploration of all available 802.21 mechanisms considering the precious uniform information to enhance the handover decision.

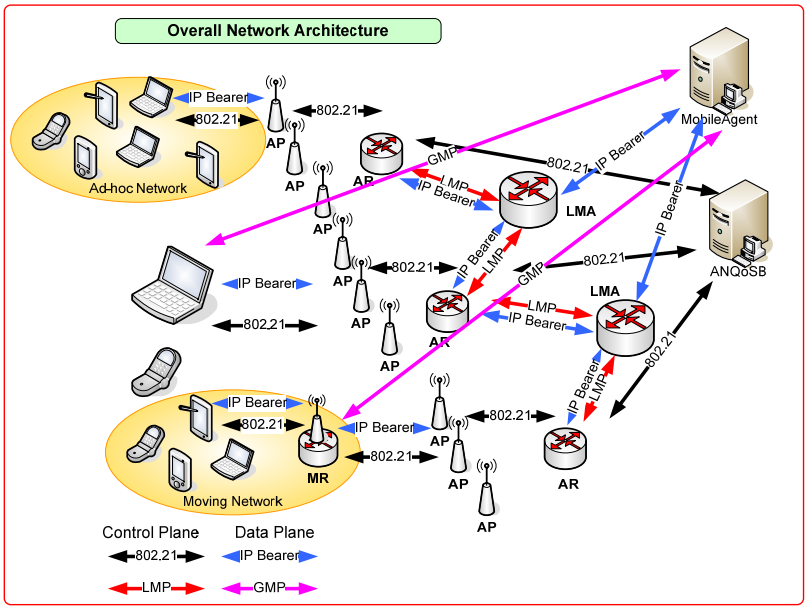

Figure 12: DAIDALOS Mobility Architecture view

Observing the figure we can see how 802.21 communication between all entities that can support Local and Global Mobility Management procedures reach the network decision point (composed by a Mobile Agent and a Access Network QoS Broker), allowing them to be aware of the terminals point of view of the network.

The most relevant aspect about using 802.21 framework is that where in the figure is an AP, it could be any other technology, due to the abstraction capabilities of the MIHF.

3.2.3 IEEE 802.16 Integration Requirements

To successfully integrate the WiMAX systems in the DAIDALOS architecture a set of requirements must be satisfied.

Most of these requirements were previously explored in the past in [WiMaxThesis].

Among the most relevant stipulations are the fast MN network access, dynamic service differentiation, dynamic QoS management, seamless integration of Global Mobility management and Localized Mobility Management, and the IPv6 neighbouring discovery process support [RFC2461].

The ***fast MN network*** consists of supplying fast access to the requested services by a new entity that enters in the network, avoiding initialization delays. This is also in line with mobility requisites, which impose that the mobility schemes with the intention of maintaining a user session even when performing handover. Thus, 802.16 Service Flow reservations should be fast to avoid traffic disruption during handover process.

The QoS management aptitude consists on providing a fast ***dynamic service reservation*** to the end user to access services through the 802.16 systems and allowing **dynamic service modification** without considerable affecting the service that is being used.

The ***dynamic service flow differentiation*** is a crucial requisite since it is mandatory in NGN to distinguish between services initiate by the same MN, in order to achieve a higher performance.

IPv6 support is imperative in next generation networks and therefore IPv6 Neighbour Discovery Process (NDP) [RFC2461]support.

3.3 Summary

In this chapter, it is given a broad view of the conceptual architecture of the European Projects WEIRD and DAIDALOS II, contextualizing the research carried out throughout this thesis.
A high level view of the WEIRD architecture is presented exploiting its vertical and horizontal decomposition. WEIRD QoS Model is also analysed, presenting the distinct ways to trigger QoS sessions and the WEIRD architecture control plane. In which concerns to DAIDALOS, the 5 key concepts that guided DAIDALOS II are summarily described. Furthermore DAIDALOS Global architecture is also revealed, spotlighting its QoS and mobility architecture. In the end of the chapter, the IEEE 802.16 integration requirements are presented, concerning the future demanding DAIDALOS heterogeneous environments.

4 Chapter 4: Resource Management in WiMAX

This chapter discusses how to accomplish Resource Management in WiMAX networks, presenting the common architectural aspects among WEIRD and DAIDALOS implemented systems. It details the research method and the common developed work concerning both two European projects that support this thesis.
The accomplished research process is widely described, including the study of the supported mechanisms by the Redline WiMAX equipment, the evaluation and presentation of the most relevant tools used throughout the implementation, and the description of the generic QoS modules and SNMP interface, developed under the scope of both ventures.

4.1 802.16 QoS supported mechanisms

The first stage of this thesis was to analyse and study the supported QoS mechanisms in vendor specific equipment, in this case, Redline equipment RedMAX AN-100U [REDCOM]. An overview of the RedMAX AN-100U was previously given in chapter 2, section 2.1.2.6. After some familiarization with the equipment HTTP interface and its functionalities, in particular, QoS management capabilities, it was started the revision of the 802.16f standard [802.16f] .
The IEEE 802.16f standard document amends IEEE 802.16-2004 [802.16-2004] by defining a management information base [RFC3418][RFC1213] for the MAC and PHY and associated management procedures. So this section relates the mandatory MIB objects of the 802.16-2004 compliant equipment and presents a management reference model.

After the definition of the QoS objects supported by the Redline WiMAX equipment, depicted in detail in section, 4.1.2, the study process of the QoS mechanisms proceeded. This second part of the study is described in section 4.1.3.

4.1.1 Management Reference Model

Figure 13 illustrates the management reference model of fixed Broadband Wireless Access (BWA) networks described in the 802.16f Standard.

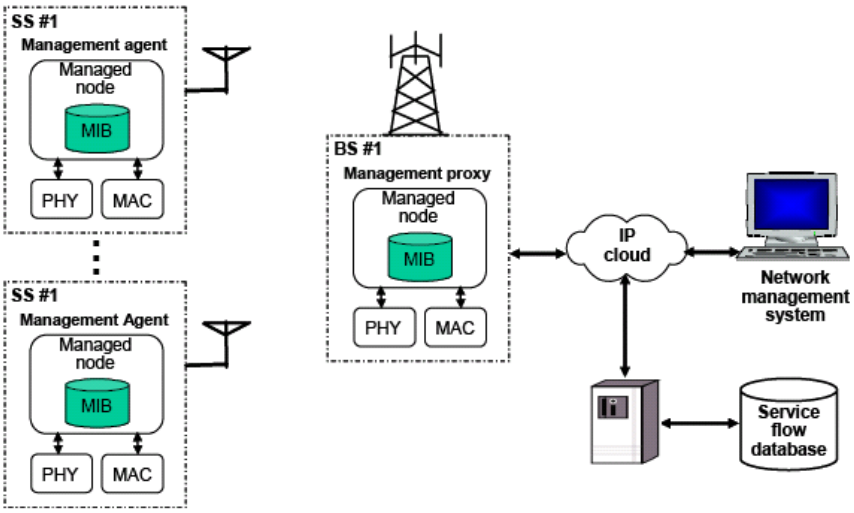

Figure 13: Management Reference Model for BWA networks [802.16f]

As can be observed, the network management model is composed by a Network Management System (NMS), managed nodes and a service flow database. The BS and SS managed nodes collect and store the managed objects in the format of *wmanIfMib* and *wmanDevMib* that are made available to NMSs via management protocols, such as SNMP (Simple Network Management Protocol).

Service Flow Database contains the service flow and the associated QoS information that has to be populated in BS and SS when a SS enters into a BS network.

The management information between SS and BS will be carried over the second management connection for managed SS. If the second management connection does not exist, the SNMP messages shall go through another interface in the customer premise.

4.1.2 Definition of QoS objects supported by WiMAX equipment

As mentioned in the beginning of this chapter in order to define the QoS objects of the WiMAX equipment it was used the document 802.16f/Draft [802.16f/Draft].This document is actually an approved standard 802.16f-2005 [802.16f] and relates the mandatory MIBs [RFC3418][RFC1213] that should be present in the 802.16d equipments. It must be noted that the content of the 802.16f-draft is very close to the approved standard and it was not detected any relevant change in terms of QoS management that could impose a change in the specified QoS management modules addressed in this thesis.

In such a way, the first step consisted on the analysis of the WMAN-IF-MIB. This is, the MIB with the definition of all mandatory objects for 802.16d equipments. Therefore, in this MIB are congregated all the QoS objects.

From this analysis, it was made a compilation of all QoS objects, grouped by OID. All the QoS objects, which directly or indirectly had relevance for the implementation of the QoS management mechanisms, were considered. Subsequently, the focus was turned to the

analysis of WMAN-IF-CONTROL-MIB that excluded the objects that were not supported by the equipment.

The MIBs REDLINE-MIB, REDLINE-WMAN-IF-MIB, REDLINE-BS-MIB, REDLINE-SS-MIB, REDLINE-SYSTEM-MIB were also carefully analysed in order to evaluated the possible existence of proprietary relevant QoS objects.

Finally, the MIBs REDLINE-CONTROL-MIB, REDLINE-WMAN-IF-CONTROL-MIB, REDLINE-BS-CONTROL-MIB, were also verified so that we could have a precise list of supported proprietary objects.

4.1.2.1 QoS objects defined in 802.16f Standard MIBs

The definition of the objects is expressed in SMIv2 [RFC2578], allowing the management through the SNMP protocol [RFC1157]. Management Information Base's for BS and SS are defined as modules ASN.1.

4.1.2.1.1 802.16 objects integration in the MIB II tree

The IANA has assigned the ifType propBWAp2Mp (184) for the point to multipoint operation mode.

The 802.16 MIB can be accessed through

Iso.org.dod.internet.mgmt.mib-2.transmission.ifType (1.3.6.1.2.1.10.184)

Wireless MAN interface table is located under transmission subtree, as follows.

wmanIfMib ::= {transmission 184}-- WMAN interface table

All mandatory QoS objects are defined in WMAN-IF-MIB, shown in Figure 14.

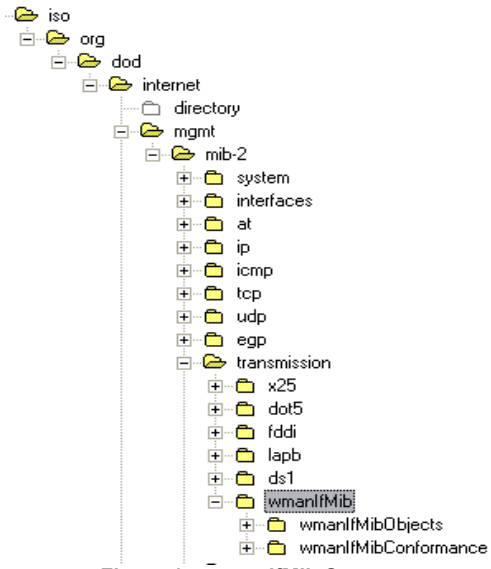

Figure 14: wmanIfMib Structure

The MIB is organized according to the reference model defined by IEEE802.16f standard.

4.1.2.1.2 Redline Proprietary MIB structure

On the MIBs defined by Redline, it was not found any QoS object that could be useful for the QoS mechanisms management implementation, except to the traps support that is depicted in section 4.1.3.

So in this sub-section is just made a little reference to this proprietary MIB by illustrating its structure. Figure 15 shows Redline Management MIB structure.

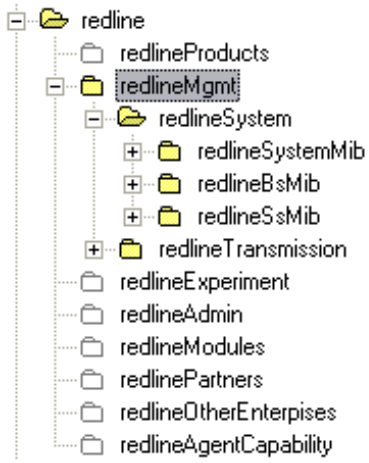

Figure 15: Redline Management MIB Module Structure

The MIB REDLINE-MIB is shown in Figure 16:

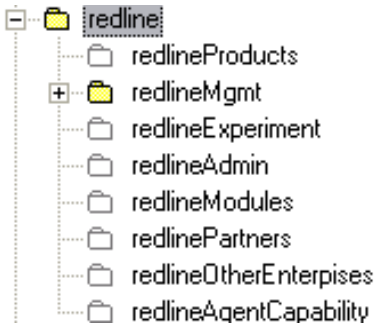

Figure 16: REDLINE-MIB Structure

The MIB REDLINE-BS-MIB structure is shown in Figure 17

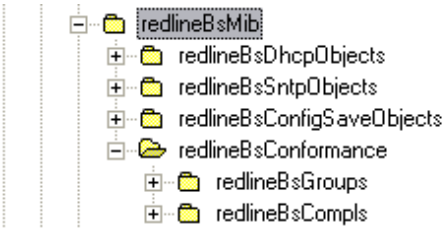

Figure 17: REDLINE-BS-MIB structure

The MIB REDLINE-SS-MIB, presented in Figure 18 does not define any QoS object.

Figure 18: REDLINE-SS-MIB structure

The MIB REDLINE-WMAN-IF-MIB is the largest of the proprietary MIB modules analysed and has the following structure:

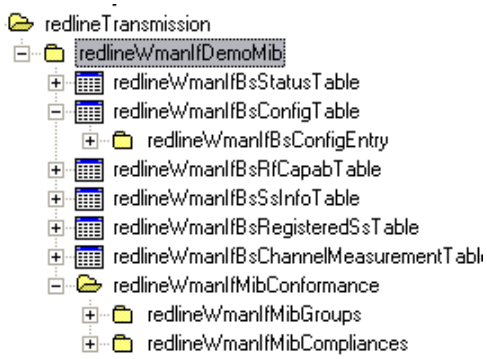

Figure 19: REDLINE-WMAN-IF-MIB structure

The MIB REDLINE-WMAN-IF-CONTROL-MIB excludes the subsequent objects of the REDLINE-WMAN-IF-MIB:

- redlineWmanIfBsConfigTable;
- redlineWmanIfBsRfCapabTable;
- redlineWmanIfBsStatusTable;
- redlineWmanIfBsSsInfoTable;

Although these objects do not have a determinant role at the QoS management level, some of the OIDs of these tables would be useful for a Resource Management solution.
This study, in its first stage, validates the implementation viability of a QoS Management application for the WiMAX network through the SNMP protocol.

4.1.3 Traps, RF, Physical and MAC Parameters support

This section presents the study of the 802.16-2004 equipment parameters that enable an effective WiMAX segment resources management.
A large part of PHY and MAC Parameters are not mapped in MIB OID's. For the no supported ones, alternative ways of gathering this data, using a different interface, but not SNMP, had been proposed.
The objects that will be referred are useful for resources management and admission control, important features to the implementation of a reliable and efficient QoS Model. Nevertheless, it must be mentioned that the traps support is the main focus of this sub-section. Although the support of traps by the equipment is reduced, it is possible to dynamically obtain and build the network topology by capturing asynchronous events generated by SNMP agents of the redline subscribers and base station. This is preponderant to achieve a full dynamic network management.

4.1.3.1 Traps Support

The SNMPv2 [RFC1157] [RFC2578] version used by the agents of the Redline equipment, define traps in a slightly different way, compared to SNMPv1. In a MIB, Version 1 traps are defined as *TRAP-TYPE*, while Version 2 traps are defined as *NOTIFICATION-TYPE*. SNMPv2 also puts away the notion of generic traps; instead, it defines many specific notifications in public MIBs.

The format of the SNMPv2 notification is shown below.

```
NOTIFICATION-TEST-MIB DEFINITIONS ::= BEGIN
      IMPORTS ucdavis FROM UCD-SNMP-MIB;

demonotifs OBJECT IDENTIFIER ::= { ucdavis 991 }

demo-notif NOTIFICATION-TYPE
            STATUS current
      OBJECTS { sysLocation }
            DESCRIPTION "Just a test notification"
      ::= { demonotifs 17 }

END
```

The traps have an important role in a NMS, since a NMS server can react to SNMP traps it receives. For example, when an NMS receives a *linkDown* trap from a router, it might respond to the event by paging the contact person, displaying a pop-up message on a management console, or forwarding the event to another NMS.

The traps supported by the Base Station are in Table 3

Trap Name	***Description***
SNMPv2-MIB::coldStart	*A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered. Counters and Gauges have been reinitialized.*
SNMPv2-MIB::warmStart	*A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered.*
IF-MIB::linkup	*A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state).*
IF-MIB::linkDown	*A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.*
SNMPv2-MIB:: authenticationFailure	*An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.*
WMAN-IF-MIB:: wmanIfBsSsStatusNotificationTrap	*This trap reports the status of a SS. Based on this notification the NMS will issue an alarm with certain severity depending on the status and the reason received. The supported statusValues are*

	ssRegistered(3), ssRegistrationFail(4) and ssDeregistered(5).
REDLINE-SYSTEM-MIB::redlineSWUpgradeStatusTrap	*Notifies a software upgrade.*

Table 3: Supported Traps Description

4.1.3.2 Traps Configuration

In order to receive the traps a TrapReceiver table must be set in the agent, with the information of the eventual trap receivers. This table is illustrated in Figure 20.

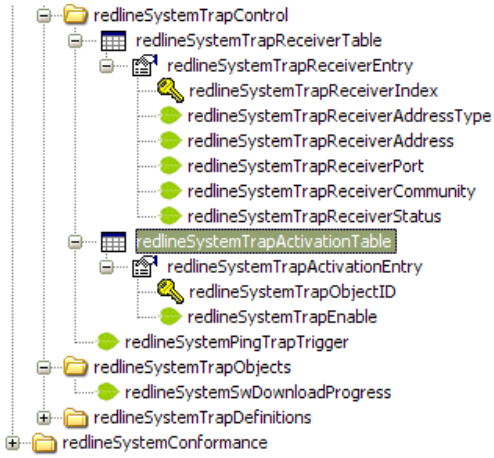

Figure 20: redlineSystemTrapReceiverTable

The entries of this table are indexed by the trap OID, which means that the OIDs of all traps should be known in order to enable/disable them individually.

The next example shows a Net-SNMP request to activate coldStart trap which uses an SNMP Set with single object:

#snmpset -v 2c -c private 192.168.25.3 redlineSystemTrapEnable.1.3.6.1.6.3.1.1.5.1 i 2

Or

#snmpset -v 2c -c private 192.168.25.3 .1.3.6.1.4.1.10728.2.1.1.4.1.2.1.2.1.3.6.1.6.3.1.1.5.1 i 2

and Agent's response

SNMPv2-SMI::enterprises.10728.2.1.1.4.1.2.1.2.1.3.6.1.6.3.1.1.5.1 = INTEGER: 2

To enable/disable the• snmpEnableAuthenTraps object we can also use this set command

#snmpset -v 2c -c private 192.136.93.61 snmpEnableAuthenTraps.0 i 1

Or

#snmpset -v 2c -c private 192.136.93.61 .1.3.6.1.2.1.11.30.0 i 1

and Agent's response

SNMPv2-MIB::snmpEnableAuthenTraps.0 = INTEGER: enabled(1)

Finally to enable *wmanIfBsSsStatusNotificationTrap*, it is necessary to set the *wmanIfBsTrapControlRegister* and *wmanIfBsStatusTrapControlRegisterobjects* of WMAN-IF-MIB.

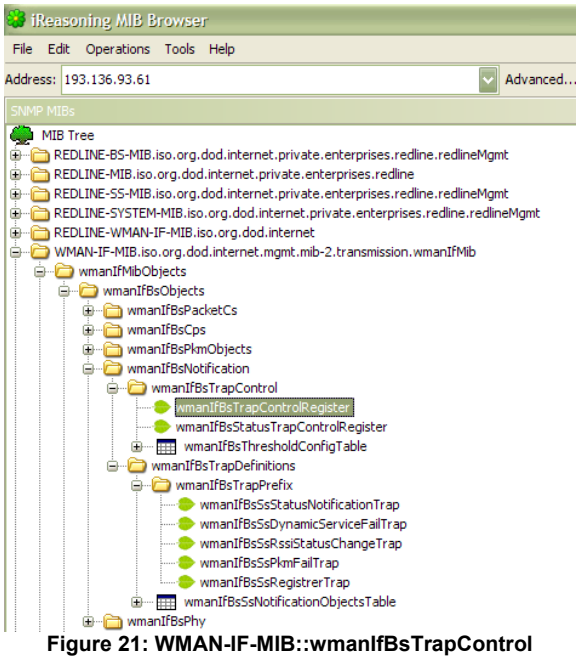

Figure 21: WMAN-IF-MIB::wmanIfBsTrapControl

Only wmanIfBsSsStatusNotificationTrap trap can be enabled/disabled using this method.

Below is an example of a Net-SNMP request to activate *wmanIfBsSsStatusNotificationTrap* to report only "ssRegistered" events:

#snmpset -v 2c -c private 192.168.25.3 wmanIfBsTrapControlRegister.0 x "80" wmanIfBsStatusTrapControlRegister.0 x "1000"

Or

#snmpset -v 2c -c private 192.168.25.3 .1.3.6.1.2.1.10.184.1.1.4.1.1.0 x "80" .1.3.6.1.2.1.10.184.1.1.4.1.2.0 x "1000"

and Agent's response

SNMPv2-SMI::transmission.184.1.1.4.1.1.0 = Hex-STRING: 80
SNMPv2-SMI::transmission.184.1.1.4.1.2.0 = Hex-STRING: 10 00

The same can be achieved through Trap Activation Table and following command:

#snmpset -v 2c -c private 192.168.25.3 redlineSystemTrapEnable.1.3.6.1.2.1.10.184.1.1.4.2.0.1 i 1

The equipment has set to send a notification when a new SS registers or deregisters with the Base Station.

4.1.4 RF Physical and MAC Parameters mapping into OID

The following tables list the RF Physical and MAC Parameters, which contain relevant information to realize an effective resource control, mapping to OID. When a parameter is not

mapped on the MIB, an alternative to obtain its value is proposed, using other available equipment interfaces.

The unsupported SNMP objects by Redline WiMAX 802.16d equipment are highlighted in gray bold colour. Each table corresponds to a Resource Management primitive; these primitives are listed in Annex A, section B.

Parameter Name	***Object Name***	***Alternative Support - Telnet and/or HTTP***
bs_mac_addr	ifPhysAddress	
bs_ipv4_mgmt_addr	redlineSystemIpAddress	
sector_avail_dl_bw	**redlineWmanIfBsStatusDlBandwidthMargin**	Available via CLI Telnet and HTTP (BS Status Info)
sector_avail_ul_bw	**redlineWmanIfBsStatusUlBandwidthMargin**	Available via CLI Telnet and HTTP (BS Status Info)
tx_power	redlineWmanIfBsCurrentTxPower	
channel_bw	**redlineWmanIfBsConfigPhyImode**	Available via CLI Telnet and HTTP (Wireless Interface Configuration)
freq_oper	**redlineWmanIfBsConfigRfDlChannel**	Available via CLI Telnet and HTTP (Wireless Interface Configuration)
Guard_interval	**redlineWmanIfBsConfigPhyCp**	Available via CLI Telnet and HTTP (Wireless Interface Configuration)
Frame_dur	**redlineWmanIfBsConfigMacFrameDurationCode**	Available via CLI Telnet and HTTP (Wireless Interface Configuration)
dl_ratio	**redlineWmanIfBsConfigMacAdaptiveDlUlRatio**	Available via CLI Telnet and HTTP (Wireless Interface Configuration)
vendor_id	**wmanIfBsSsVendorIdEncoding**	Can be extracted from the MAC address of BS (first 3 bytes)

Table 4: ADAPTER_NEW_BS parameters mapped into MIB Objects

bs_mac_addr	ifPhysAddress	

Table 5: ADAPTER_DEL_BS parameters mapped into MIB Objects

ss_mac_addr	wmanIfBsSsMacAddress	
ss_ipv4_mgmt_addr	redlineWmanIfBsSsIpAddress	
Assoc_bs_mac_addr	ifPhysAddress	We can obtain all BS MAC addresses associated with this SS via CLI – bsIdTable
ss_avail_dl_bw		Available the DL Rate and UP rate via CLI.
Ss_avail_ul_bw		Available the DL Rate and UP rate via CLI.
mod_type		Available via CLI Telnet and HTTP (SS Status Info) / There's 4entries in wmanIfBsRegisteredSsTable from which can be deduced the modulation type that is being used, this entries are wmanIfBsSsMaxTxPowerBpsk, wmanIfBsSsMaxTxPowerQpsk, wmanIfBsSsMaxTxPower16Qam, wmanIfBsSsMaxTxPower64Qam. But the CLI interface facilitates the access to this information.
tx_Power	**wmanIfBsSsMaxTxPowerBpsk, wmanIfBsSsMaxTxPowerQpsk, wmanIfBsSsMaxTxPower16Qam, wmanIfBsSsMaxTxPower64Qam**	The access to this information is not direct in the MIB, so it's more viable use the Telnet CLI interface.
Dist	**redlineWmanIfBsSsInfoDistance**	Available via CLI Telnet and HTTP (SS Status Info)
vendor_id	**wmanIfBsSsVendorIdEncoding**	Can be extracted from the MAC address of BS (first 3 bytes)

Table 6: ADAPTER_NEW_SS parameters mapped into MIB Objects

ss_mac_addr	wmanIfBsSsMacAddress	
bs_mac_addr	ifPhysAddress	

Table 7: ADAPTER_DEL_SS parameters mapped into MIB Objects

bs_mac_addr	ifPhysAddress	
ss_mac_addr	wmanIfBsSsMacAddress	
Cinr	**wmanIfBsMeanCinrReport**	Available via CLI Telnet - from diagStatistics (Diagnostic Statistics Commands)
Rssi	**wmanIfBsMeanRssiReport**	Available via CLI Telnet - from diagStatistics (Diagnostic Statistics Commands)
if_status	ifOperStatus	

Table 8: ADAPTER_CSI_INFO parameters mapped into MIB Objects

ss_mac_addr	wmanIfBsSsMacAddress	
bs_mac_addr	ifPhysAddress	

Table 9: ADAPTER_RESOURCES_REQ parameters mapped into MIB Objects

bs_mac_addr	ifPhysAddress	
ss_mac_addr	wmanIfBsSsMacAddress	
ss_used_dl_bw		**CLI Interface**
ss_used_ul_bw		**CLI Interface**

Table 10: ADAPTER_RESOURCE_RESP parameters mapped into MIB Objects

4.2 QoS Design Principles and Mechanisms

To achieve end-to-end QoS, mechanisms are required in both the control plane and the data plane. Control plane mechanisms are needed to allow the users and the network to negotiate and agree on the required QoS specifications, identify which users and applications are entitled to what type of QoS, and let the network appropriately allocate resources to each service. Data plane mechanisms are required to enforce the agreed-on QoS requirements by controlling the amount of network resources that each application/user can consume.

In which refers to control plane mechanisms, the *QoS policy management*, *signalling,* and *admission control take important roles.*

- QoS policy management defines and provisions the various levels and types of QoS services, as well as manages which user and application gets what QoS.
- *Signalling* is defines how a user communicates QoS requirements to a network. Signalling mechanisms may be either static or dynamic.
- *Admission control* is another important control plane function that consists on the ability of a network to control admission to new traffic, based on resource availability.

Admission control is necessary to ensure that new traffic is admitted into the network only if such admission will not compromise the performance of existing traffic. Admission control may be done either at each node on a per-hop basis, or just at the ingress-edge node, or by a centralized system that has knowledge of the end-to-end network conditions.

The data plane mechanisms are responsible to enforce the agreed-on QoS by classifying the incoming packets into several queues and allocating appropriate resources to each queue. Classification is done by inspecting the headers of incoming packets; resource allocation is done by using appropriate scheduling algorithms and buffer-management techniques for storing and forwarding packets in each queue. In such a way, this type of mechanisms is covered inherently by the QoS capacities of the WiMAX equipment.

On the basis of the QoS Model architecture of WEIRD and DAIDALOS II, a set of primitives has been delineated to trigger the resources allocation in the WiMAX equipment and, at the same time, to get a sort of topological information of the WiMAX network, its elements and resources. In DAIDALOS II case, the Resource Control in WiMAX, is mainly done by the WiMAX Radio Access Layer, this is, we have a centralized control entity. In WEIRD's case, the Resource Management is distributed across different components, Resource Controller, Network Management System.

To implement Wimax Resource Control system, in both evolved projects (WEIRD and DAIDALOS), according to the Redline equipment limitations (unsupported important MIB objects for resources management, only two service classes: best effort and rtPs,…) it was necessary to carefully specify the systems architecture in order to achieve highest level, as possible, of transparency, openness, scalability and robustness [Distr_Systems].

These goals express the following concerns:

- The developed architecture should be transparent: it should hide its complexity, hiding how a resource is accessed, that a resource is replicated or may be shared by several competitive users, or hide whether a resource is in the memory or in the disk.
- Another important goal is the system openness, so it must be a fact to lead in account, that the modules should be specified through interfaces offering its services and increasing at the same time the readability of the system.
- The designed architecture should take into account that it should be easy to add more resources and users to the system maintaining the agreed QoS level.
- The robustness is the fault tolerance of the system, that is, if an error occurs, the system should act accordingly, ignoring it or informing other entities, but should remain functional.

When considering all these aspects it is possible to reach a good abstraction level and build a better application, which can be easily modified /updated or integrated with other applications. All these premises were taken into account when specifying and implementing the modules for WEIRD and DAIDALOS. Part of the developed modules for WEIRD were reused and seamlessly adapted to work with DAIDALOS architecture, for instance the QoS Management functionalities and the SNMP interface.

4.3 NET-SNMP API Overview

This section gives an overview of NET-SNMP API functions that were used in both projects, WEIRD and DAIDALOS, to implement the interaction with the WIMAX systems, through SNMP protocol, supporting the 802.16f MIB.

Using the C API to develop SNMP applications is appreciably more difficult and time consuming than using the PERL and CLI interfaces. Nevertheless, the advantages of being able to integrate with other native C modules to build complex applications are obvious [NET-SNMP].

The SNMP C API has different structures which are used to store information needed by different phases of a SNMP dialog. The basics steps to implement an SNMP dialog are:

1. Initialize an SNMP session (snmp_session_init() function was created to easy this step)
2. Define attributes for the session
3. Add MIBs to the current MIB tree if necessary
4. Create a PDU (Primary Data Unit)
5. Pack OIDs into the PDU for GET MESSAGE or packs OIDs, Types and Values into the PDU for SET MESSAGE
6. Send the request and wait for response
7. Do something with the returned values
8. Free the PDU
9. Close the session

Main methods of NET-SNMP API:

init_snmp()

SNMP session initialization method. When a new SNMP session is initialized, a snmp_session structure will be initialized with default values. We can then modify the elements (community version, peername, snmp version) of that structure to match our needs.

snmp_open()

Opens a snmp session with the previous defined parameters by init_snmp(). This returns another snmp_session struct as a handle.

add_mibdir()

Defines the location of the MIB we want to load into the MIB tree.

read_mib()

Loads a MIB into the MIB tree used by the library.

snmp_pdu_create()

Creates a packet data unit according to its type (GET, SET, GETNEXT, GETBULK,…)

read_objid()

Reads the OID from the MIB

snmp_add_null_var()

Adds that OID as a variable to the variable list used by the PDU. The variable bindings are null.

snmp_add_var()

Similar to snmp_add_null_var but used to populate a SET PDU, that needs to know the types and values of the OIDs to process the packet.

snmp_synch_response()

Sends the PDU and expects a response that is inserted into a new PDU structure with both the OIDs and the values. This function passes the open session handle, the PDU to send, and an empty PDU structure to accept the response which includes the populated values for each OID in the variable list.

At this point, the returned data can be extracted and manipulated either by utilizing built in functions such as print_value() or by simply directly accessing the structures.

snmp_free_pdu()

Free the PDU(s)

snmp_close()

Close the sessions

4.4 Summary

Throughout this chapter, the most prominent common architectural aspects shared between WEIRD and DAIDALSO have been mentioned. An extensive study has been carried out discussing means to accomplish Resource Management in WiMAX networks.

Initially, the supported QoS mechanisms have been studied. This point embraces the definition of the supported QoS objects by the used WiMAX equipment, the revision of Physical, MAC, RF and asynchronous events that could be useful to implement the Resource Control Architecture. In this chapter, QoS design principles and mechanisms, and a set of implementation guidelines have been trailed. The NET-SNMP API, used to implement the SNMP interface with WiMAX equipment and indifferently used in both projects, was depicted.

This chapter detailed the research method and the common developed work concerning both two European projects that support this thesis.

5 Chapter 5 - Architecture for Resource Control in WEIRD

This chapter presents a brief overview of Radio Resource Control architecture in WEIRD and details implementation aspects. It also shows and discusses the performance results obtained in a first phase, for the implemented solution, considering the PTP and PMP modes of operation and different Convergence Sub layers. In a second phase, more exhaustive tests have been carried out, using micro-seconds precision, which allowed for a more comprehensive exposition of the time distribution among tasks among the WiMAX Resource Control architecture, developed under scope of WEIRD project.

5.1 Developed architecture for Resource Control (WEIRD)

In section 3.1 it was described the high level WEIRD architecture. Now, the WEIRD architecture for resources control is introduced in more detail, presenting how it offers QoS access/transport facilities to applications through WiMAX.

The Resource Control features of the WiMAX network are mainly concentrated in the ASN-GW. Figure 22 illustrates the ASN-GW architecture.

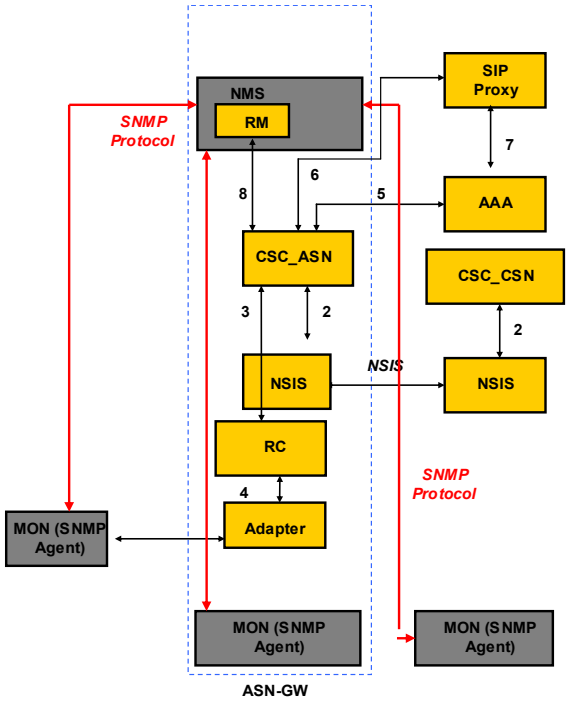

Figure 22: ASN-GW Architecture [WEIRDD2.3]

A small summary of the ASN-GW modules functionalities is given below:

CSC

The Connectivity Service Controller (CSC) acts as a QoS coordination point, processing both requests for static resource pre-provisioning and requests for resource allocation from SIP

Proxy and NSIS. It coordinates QoS signalling towards the WiMAX segment through the Resource Controller and towards the CSN and the Core Network through NSIS [NSIS]. It also controls the resource in the ASN through traffic control and PHB Enforcement.

NMS

The NMS has two main functions and consequently is composed of two subsystems:

- *Conventional Network Management Systems* (CNMS) having "classical" functions such as network static provisioning, network monitoring, alarm collection and management
- *Resource* Manager which is responsible to manage reservation and allocation of connectivity resources in the ASN and WiMAX segments.

RC

The Resource Controller (RC) has the capability to differentiate among 802.16d and 802.16e requests and trigger the correspondent interface with the appropriated Adapter module (using the AI).

Adapter

The Adapter (AD) module interfaces with the resource controller (RC) in ASN-GW and the SNMP Agent module in the BS.

Adapter uses, if supported, the SNMP protocol, when communicating with the SNMP Agent module.

To deal with the different Vendor equipment, the Adapter is split into a common part (called Generic Adapter) and a set of Vendor specific libraries to provide a differentiated SNMP request processing for each Vendor BS.

The implementation work of this thesis was mainly focused on this module, the Adapter module. Initially, it was not specified that the Adapter would be separated in two sub-modules, so it was started the development of a Global Adapter. This development was abandoned lately because of the WEIRD specification redefinition concerning the Adapter. So, the Adapter was divided in two sub-modules, the Generic Adapter module that, basically, abstracts which vendor specific adapter is being used and the Vendor Specific Adapter module, in this case Redline Adapter, that interfaces with the WiMAX Redline equipment.

5.1.1 Adapter Functionalities in WEIRD

The Adapter developed under the scope of WEIRD implements all the service flow management primitives and resources and topology information primitives (that can be found in Annex A, section A and B) had been implemented, contributing this way with important features to accomplish the proposed WEIRD QoS model architecture, in which concerns the ASN.

Figure 23 illustrates the simplified network topology will be referring to in the next paragraphs.

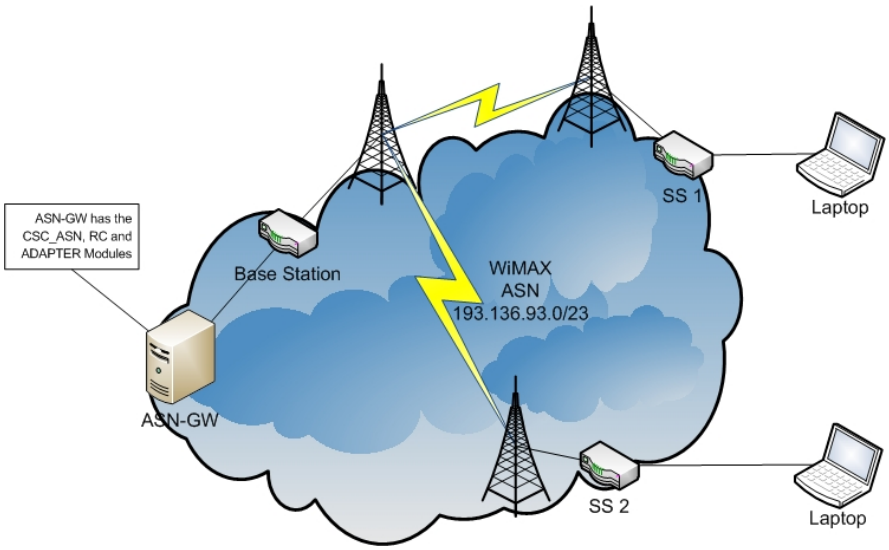

Figure 23: Access Service Network Topology

The Adapter has the ability to detect new Subscribers and Base Stations that join to the ASN-GW, building the complete network topology in WiMAX segment in a dynamic way and supplying at the same time relevant Physical and MAC parameters for the NMS and RC. This WiMAX network discovery feature is implemented over the SNMP traps support by the equipment.

The Adapter is also prepared to respond upon resources requests, including downlink and uplink available bandwidth for the SS.

And the last but not the least, that is to say, the most important features, are the capacity to enforce the QoS reservations, modifications and deletions requests, received from the upper modules in the Redline WiMAX equipment, using IPv4 or 802.3 Ethernet as CS.

It should be mentioned that only Service Flow management primitives implementation was mandatory in the first stage of WEIRD.

But considering the study that was accomplished relatively to the support of the other primitives, it was decided to implement them all, as a way to improve the developed work.

5.1.2 Implemented modules

This sub-section presents the 802.16 Adapter modules architecture, presenting the interaction between different modules.

The Adapter Architecture, part of the ASN-GW, is illustrated in Figure 24.

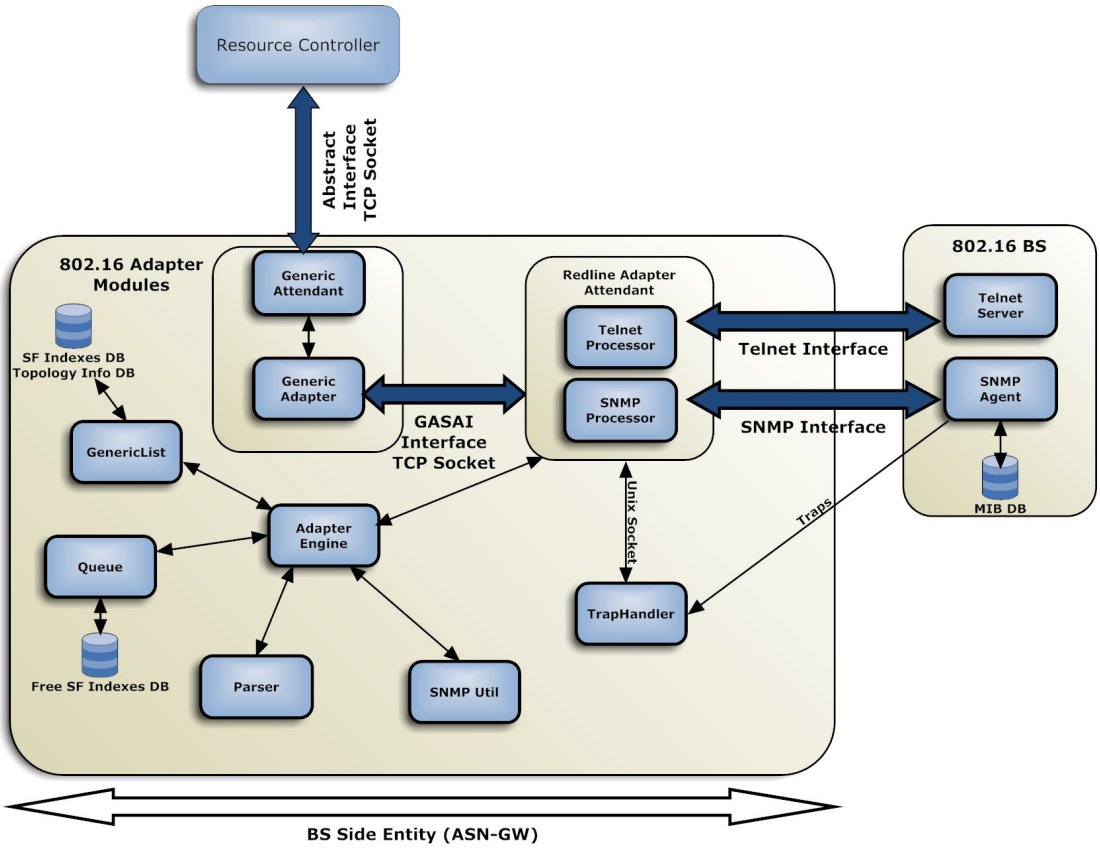

Figure 24: Adapter Architecture

The Adapter is composed by several modules and some interfaces. The AI (Abstract Interface) is the interface defined between the Resource Controller and the Generic Adapter. The Generic Adapter is composed by the Generic Attendant and Generic Engine that abstracts the vendor specific adapter which is being used; this module was developed by Tuomas from VTT. It interfaces with the Specific Vendor Adapters through the GASAI Interface.

All the remaining modules belong to the Redline Adapter and are depicted following:

RedlineAdapterAttendant

Here is where all the communication takes place. This module is responsible to maintain the communication between the Generic Adapter, the Base Station and the TrapHandler module. It multiplexes all the message requests by the use of a select function.

This is also the module that launches the needed instances in order to setup the system and process all the requests that are sent to the RedlineAdapterAttendant.

More specifically, it can be referred that the RedlineAdapterAttendant implements a Unix Socket Server [UNIX_SOCKS] (A Unix domain socket or IPC socket is a virtual socket, similar to an *internet socket* that is used in *POSIX operating systems* for *inter-process communication*) that is listening for asynchronous events that can be generated by the WiMAX network elements, BS or SSs, it is to say, trap messages. It should be understood

that, as we could have several Subscribers connected to one BS, or managing several Base Station, two trap messages could be sent at the same time to the RedlineAdapterAttendant, which imposed a thread based implementation. If RedlineAdapterAttendant receives a trap, it processes it (converts the trap_info message into GASAI, more details in TrapHandler module explanation) and sends the GASAI primitive to the generic.
In the same way, the Redline Attendant implements a TCP Socket Client that is expecting for Generic Requests. Accordingly to the request received, it uses the SNMP or the TELNET interface to interact with the equipment, and send back the response to the Generic.

AdapterEngine

It concentrates the main intelligence of the application. Almost all the processing work is done here. It processes the GASAI messages and the Trap Messages that are sent to the Redline Attendant.
The processing work, among other things, does the conversion of GASAI primitive into SNMP messages (GET, SET) and vice-versa. It also converts the trap MESSAGES into GASAI primitives.
As occurs with almost all the modules error checking is done here in order to maintain the robustness and consistency of the application, assuring for example that the AI Primitive values are between the limits supported by the equipment.
Moreover, this module implements the initialization functions like the TrapReceiverConfiguration and other useful functions to get performance measures.

TrapHandler

This module implements a thread that interacts with the NET-SNMP TrapHandler. The NET-SNMP trapHandler (snmptrapd) receives a trap and redirects the trap Information to the STDIN. The RedlineTrapHandler is basically monitoring the STDIN and according to the trap type received, it parses the STDIN, saves the trap information into the struct trap_info and sends it to Unix Socket Server, it is to say, the Redline Attendant.

The trap_info Message is shown in the next table.

```
trap_info MESSAGE{
        type;              /* trap message type */
        ipv4_addr;         /* source ipv4 of the agent that generates the asynchronous event */
        varbinds List;     /* variable binding list with the trap information */
};
```

```
varbinds{
        oid;
        value;
};
```

SnmpUtil

This module implements the low level primitives that interact with the BS, using the SNMP protocol. The NET SNMP API [snmpAPI] was used in order to implement the snmp_set and snmp_get primitives that interact with the 802.16 equipment through the SNMP Protocol.

It was also implemented one method for snmp session initiation that supports both the SNMPv2 and SNMPv3, regarding this way, future evolution of the SNMP agent and other useful functions.

Two types of snmp_get primitives were implemented here. One that gets a unique object identifier value by session, and other one, the multi_get, that can be used to resquest multiple variables in one single session, packing the requested OIDs into the same PDU. As disadvantage, if the return values must be saved, it forces the programmer to know the exact order in which he requests the OID values, so that the response values could be associated with the correspondent object identifiers.

Parser

The Parser module is the one that makes possible to get the primitive parameters that are not mapped in the BS SNMP Agent MIB, through the Telnet Protocol.

To implement this feature exist quite a few alternatives. One would be the utilization of a telnet java API, but this would increase the integration difficulties, and pose performance problems. Moreover it would be necessary to serialize the data, which implies a considerable effort. At the time of decision it was not found a reasonable Telnet C API, and the problem was solved in a different way, considering that for network resources monitoring, the operations are not as time sensitive as occurs with QoS management operations.

The found solution was to automate telnet sessions through the use of expect scripts. The telnet session information was then wrote to stdout and redirected to a file that was parsed after the telnet session finishing.

Following is an example of an expect script that automates a telnet session with the Base Station. Argv is a script argument that represents the BS address.

```
#!/usr/bin/expect

spawn telnet $argv
expect "Login:"
send "admin\r"
expect "Password:"
send "admin\r"
expect "AN100U#>"
send "show status\r"
expect "#>"
send "interfaces wireless show\r"
expect "#>"
send "logout\r"
expect " (press 'Y' to confirm)"
send "Y"
```

Queue
Implements a FIFO of integer values that is used to save the SF indexes that are set free when a Service Flow is deleted.

GenericList
Implements a Generic and dynamic List module that can handle all kinds of data needed by the Redline Adapter. This module defines the SF Indexes structures and Topology Info Structures that save, respectively, all the associated indexes needed to modify or delete a previous allocated service flow, and all the topology Information (BS's information and SS's information). The SF Indexes track is necessary because when we do a set on a MIB table we need to index the columns and rows of that table, and generally several indexes are needed.

5.1.2.1 Redline Adapter Initialization Procedure

In order to execute the Redline Adapter, it is necessary to launch the Generic Adapter before, otherwise when the Redline Adapter tries to connect to TCP Server, the connection will be refused.
We can open three terminals and execute the Generic Adapter

```
#./GenericAdapter
```

Launch the RedlineAdapter in the other terminal executing,

```
#./RedlineAdapter GenericAddr BsAddr TrapReceiverAddr TrapReceiverPort
```

The Redline Adapter needs all these parameters. The GenericAddr is the address of the Generic Adapter it will connect to in order to receive and send GASAI (Generic Adapter Specific Adapter Interface) messages.
All other parameters are needed to configure the TrapReceiver in the BS MIB. After we start the program, the trapReceiver must be configured and for that, it is necessary to send a SNMPSET message to the BS agent. This is the reason why the actual BS IPv4 address is needed in advance. The other parameters are the Trap receiver address and the trap receiver port in which it will be listening for traps. By default the snmptrad is listening in all ports so we can define the port we want, to filter the information.
The trap community and the IP address type are set by default, hardcoded, since the equipment doesn't allow in the actual firmware version to change this values.
Finally, we can launch the snmptrapd

```
#snmptrapd –f –Lo
```

This command will force the snmptrapd to print the received trap messages to the stdout. As mentioned before, the snmptrad will call the Redline TrapHandler to threat the trap messages accordingly to its type and the definitions of the snmptrapd.conf file. In its time our

TrapHandler after parsing the trap message will send it to the Redline Adapter that will in turn process it accordingly.

In the initialization phase of the system, the network topology information of the WiMAX network is dynamically built: the SF indexes structures are also initialized, the Resources information and Physical and MAC parameters info are obtained. This information is saved in the RedlineAdapter cache and also sent to the Resource Controller and Connectivity Sector Controller in order to allow an effective Resource Management and Admission Control.

The sequence diagrams shown below describe the initialization procedure of the system in which refers to the NEW_BS (Figure 25) and NEW_SS detection (Figure 26).

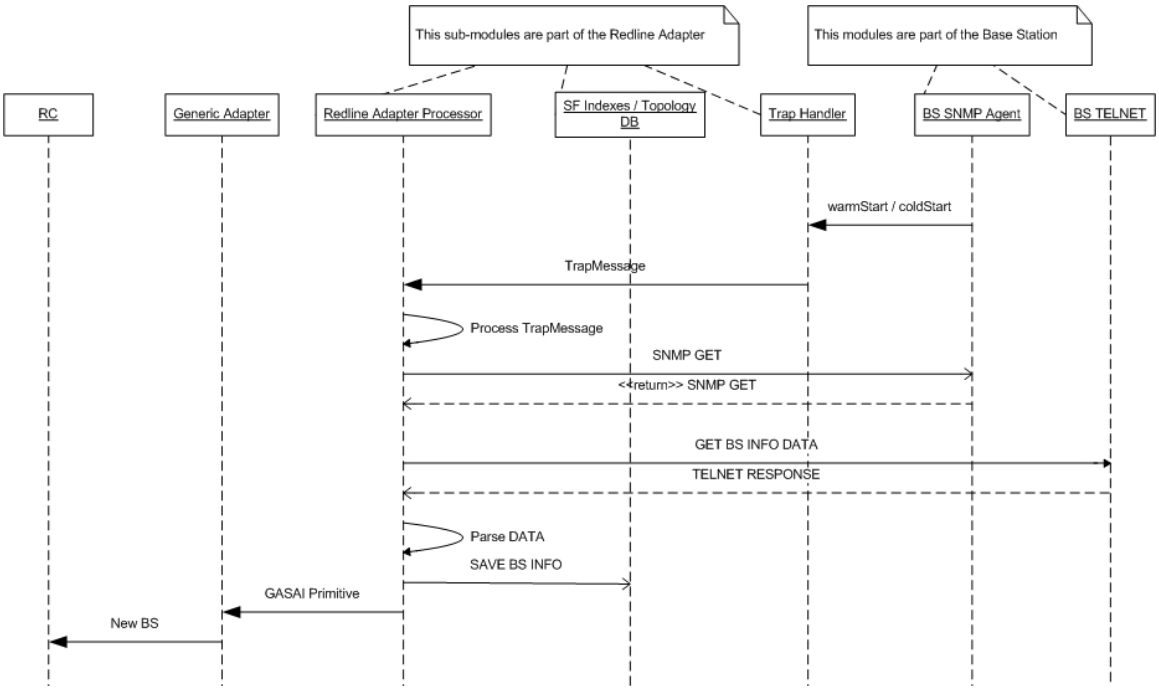

Figure 25: NEW_BS sequence diagram

As we can observe, when the Redline TrapHandler receives a warmStart or coldStart trap, it packs the important information into a trap_info Message previously described and sends it to the Redline Adapter Processor. In this case, the values of the downlink and uplink available bandwidth are obtained, and other physical and MAC parameters as the channel bandwidth, the transmission power, the frequency of operation; this information is packed into a GASAI primitive and sent to the Generic that forwards it to the upper modules.

Figure 26 shows how a NEW SS is detected.

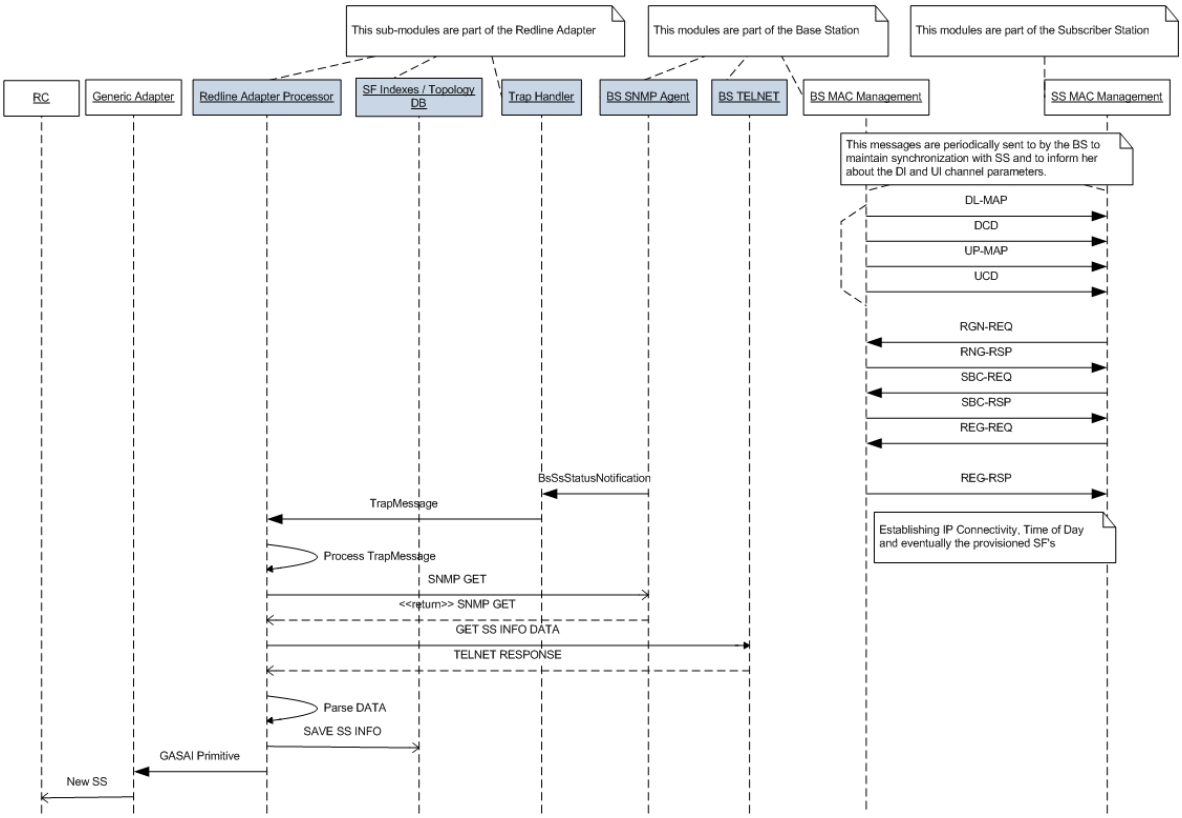

Figure 26: New SS sequence diagram

In which concerns NEW_SS sequence diagram, the MAC messages exchanged between the BS and the SS are also illustrated. The SS register process includes the exchange of several MAC Management messages between the BS and the SS. The sequence of messages is illustrated in order to contextualize all the process. The main steps to a SS entry in the WiMAX network are:

- scan and synchronize the Downlink Channel
- obtain the uplink parameters
- perform ranging
- negotiate basic capabilities
- register and establish IP connectivity
- establish service flow

When the SS registers with the BS, an asynchronous event is generated by the BS SNMP agent and a *wmanIfBsSsStatusNotificationTrap* is sent to the TrapHandler.
The TrapHandler packs the important info into a trapMessage previously described and sends it to the Redline Adapter Processor. Then it proceeds, executing a similar process as the NEW_BS, in order to obtain the needed parameters, such as SS available downlink/uplink bandwidth, the modulation type, the transmission power and the distance.

There are two important details considered in the implementation related with these primitives. The first one is that, after a SS registers with the BS, it has to establish the IP connectivity, besides the modulation type and other parameters that are saved in the BS internal modules. This takes a few seconds to be negotiated and assigned after the SS registers. This time can vary according to the distance and environment conditions, so a ten seconds limit was considered here. This is an important detail, because if we do not expect this period of time, the BS will not have any information about the Subscribers and will send erroneous values to the Generic, RC and CSC. Since this 10 seconds period only occurs in the initialization process, it did not affect the performance of the system, because the delay is not denoted by the other modules. In the initialization process the SS's info is loaded into the Redline Adapter Cache, so when a SS deregisters, the information is kept and only the status is changed to inactive. This way, if the same SS re-enters the WiMAX network again, it is avoided the 10 seconds period wait.

In a mobility scenario on which a MS would be regularly joining the system this would introduce a delay that would not be acceptable. But, since the deployed scenario does not include mobility at the Subscribers level, this does not introduce any restriction to the system. The only thing that can occur is that a subscriber station can deregister because of environment conditions or power supply problems, and for this situation the system is prepared.

The other aspect that was considered at the implementation time, was that since the SNMP runs over the UDP transport layer protocol, we can receive SNMP traps out of order, that is, we can receive a *BsSsStatusNotificationTrap* signalling that a SS has register in the system, before we receive a coldStart or warmStart trap signalling that a new BS is in the system. This situation may occur frequently and was foreseen by the Redline Adapter (802.16 System Manager).

A simple capture was done illustrating this situation (Figure 27)

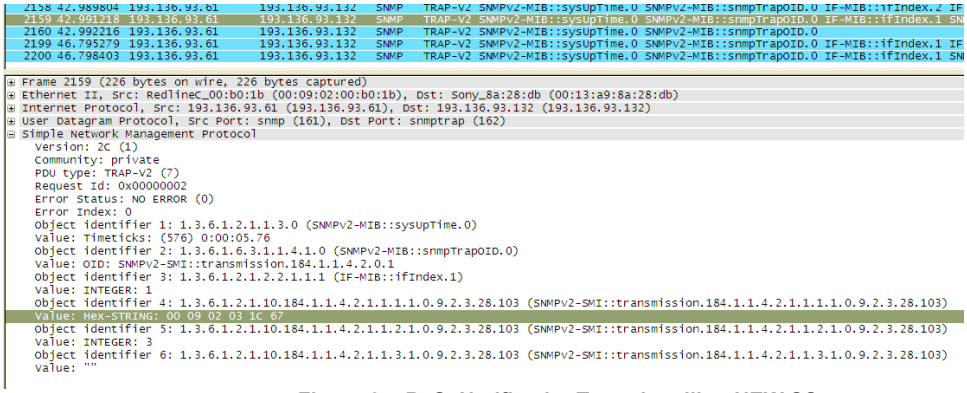

Figure 27: BsSsNotificationTrap signalling NEW SS

As we can observe the SS with the MAC Address 00:09:02:03:1c:67 is received and only in the next trap message is received the notification of a new BS (Figure 28).

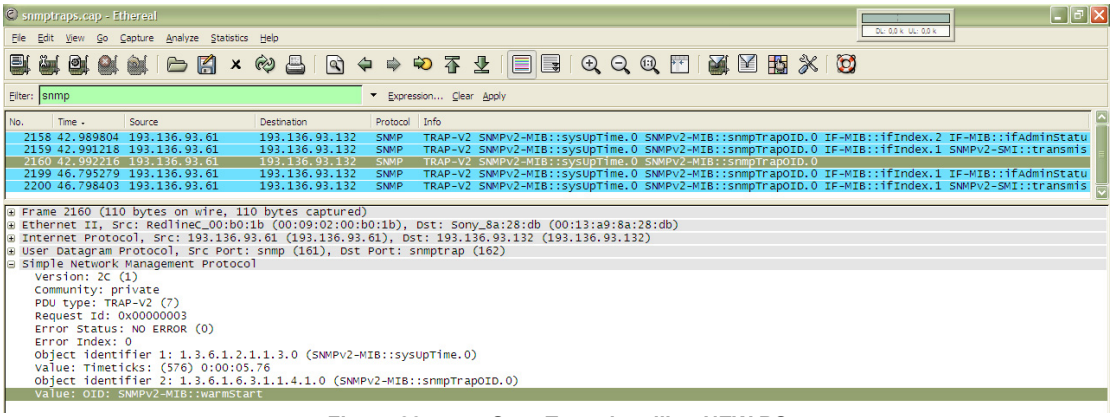

Figure 28: warmStart Trap signalling NEW BS

After this initialization procedure the CSC and RC obtain the WiMAX network topology information and the available resources and can start to send requests to the Adapter.
The next pages present the primitives that are supported by the Redline Adapter and describe the message flow charts across ASN-GW modules.

5.1.2.2 Redline Adapter Resource Control

After depicting the initialization messages sequence across ASN-GW modules, it is shown how the RedlineAdapter leads with the distinct resources requests.

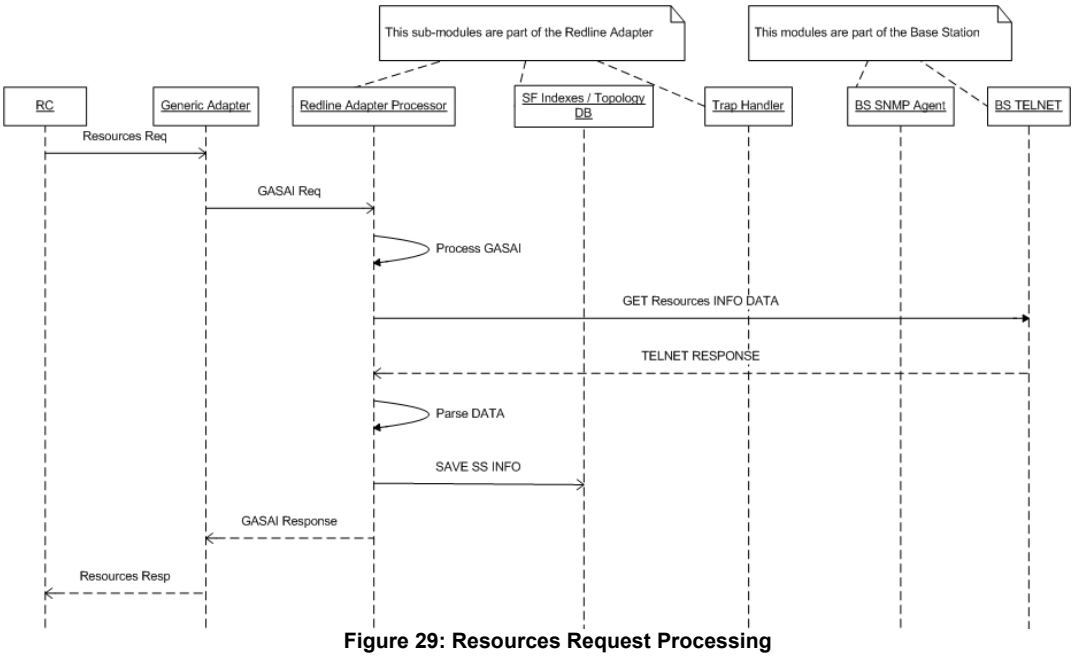

Figure 29: Resources Request Processing

This sequence diagram (Figure 29) presents how the Resources Request message triggered by the Resource Controller is processed by the Redline Adapter. The processing is very similar as the previous depicted NEW_SS and NEW_BS primitives, since the requested information, SS available uplink/downlink bandwidth is not supported in the MIB of the BS agent. Thus, it has to be obtained via Telnet. So, the expect scripts are used to automate a telnet session, the session information is parsed and saved into the SS info struct and the

GASAI primitive is built and sent to the Generic. The Generic forwards the message to the RC.

5.1.2.3 Redline Adapter Service Flow Management

Finally, the processing of the Service Flow Management requests is portrayed in Figure 30.

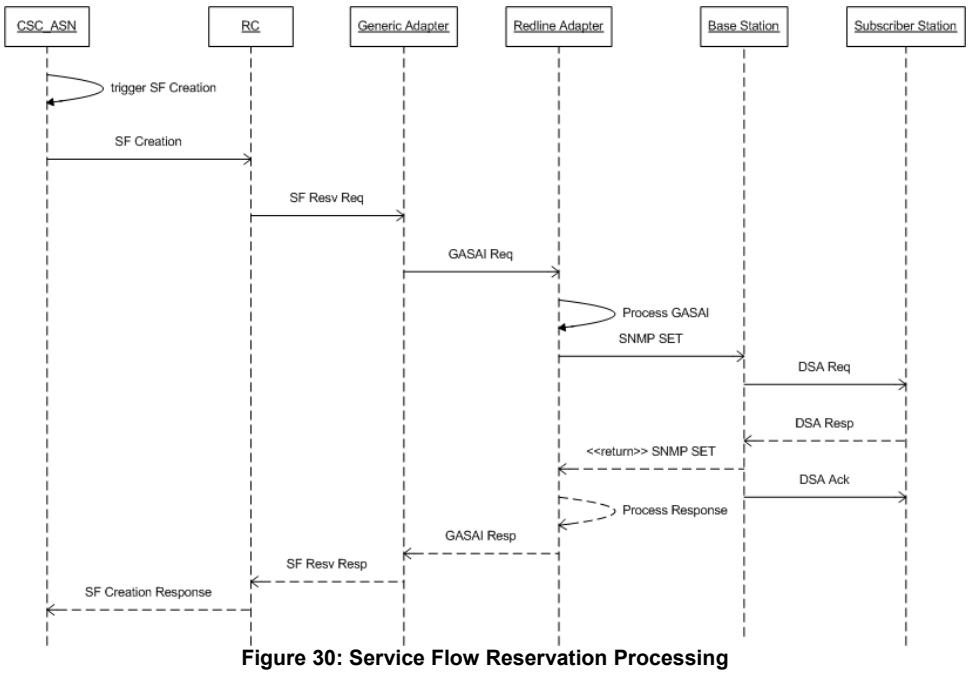

Figure 30: Service Flow Reservation Processing

The service flow creation is triggered by the AF or from the SS side. The CSC_ASN is the module responsible to manage the SF triggering. When it receives a Service Flow request, it maps the QoS parameters into 802.16 QoS parameters and triggers the SF creation in the 802.16 network. The service flow creation is sent to the RC. The RC does some processing and sends a SF Reservation Request to the Generic; the Generic transforms the request into a GASAI primitive and forwards it to the Redline Adapter.

With the purpose of making a SF reservation in the 802.16 equipment, the SNMP protocol is used, and consequently SNMP SET messages must be created, packing the 802.16 QoS parameters. The SNMP_SET Message illustrated in the Service Flow Reservation Request sequence diagram doesn't correspond to a single SNMP SET message, but four. There's a special function in Redline Adapter Engine to process the SF Requests (Create, Modification and Delete).

The most delicate type is the SF creation. To enforce a reservation in WIMAX equipment using the SNMP protocol is necessary to SET four MIB Tables by this order:

- ***wmanIfBsServiceClassTable*** (This table is provisioned and is indexed by wmanIfBsQoSProfileIndex. Each entry of the table contains corresponding service flow characteristic attributes)

- ***wmanIfBsProvisionedSfTable*** (This table contains service flow profiles provisioned by NMS. The service flow should be created with SS(s) following instruction given by wmanIfBsSfState object.

  1. The QoS parameters of the service flow are provisioned in wmanIfBsServiceClassTable and referenced by wmanIfBsServiceClassIndex.

  2. The classifier rules of the service flow are provisioned in wmanIfBsClassifierRuleTable, where they refer to SF via wmanIfBsSfId.

  The MAC addresses of SSs the service flow is created with are provisioned in wmanIfBsSsProvisionedForSfTable, where they refer to SF via wmanIfBsSfId.)
- ***wmanIfBsSsProvisionedForSfTable*** (This table maps the MAC addresses of SSs to the service flows provisioned in wmanIfBsProvisionedSfTable.)
- ***wmanIfBsClassifierRuleTable*** (This table contains packet classifier rules associated with service flows.)

This logical order is respected by the Redline Adapter. This order should be kept because of the association between the tables. We first need to set a row to the Service Class Table, in order to obtain the QoSProfileIndex. This way, when we set the Provisioned SF Table, we can associate the SF with a set of QoS Parameters. The next step is set the Provisioned For SF Table that maps the MAC Addresses of the SS's to the service flows, and that uses as index the previous SFID employed in the Provisioned SF Table. The last table to set is the Classifier Rule Table that associates the classifier rule with the SF trough the SFID previously defined.

For each table row set, it is sent a SNMPSET PDU to the BS 802.16 Agent with OIDs, types and values. Each table has a rowStatus parameter which assures that the set to the row in the table is atomic. To create a new row the value createAndGo(4), should be used and to delete we use the destroy(6). If it is intended to modify a table row, we don't use the rowStatus, we just access the parameters and change them. After all this processing work is done, a GASAI Response is filled and we can send it to the Generic that forwards the data to the RC, which in turn sends the response to the CSC. The MAC Messages exchanged between the BS and SS when a service flow is created are also illustrated.

The SF deletion process is similar to the SF creation, but in this case we only need to exchange two SNMPSET Messages between the Redline Adapter and the Base Station. One is for setting the wmanIfBsProvisionedSfTable rowStatus value to 6, and other for setting up the wmanIfBsServiceClassTable rowStatus to 6.
When we delete a wmanIfBsProvisionedSfTable row entry, we are in fact deleting, at the same time, all the associated entries with that SFID in wmanIfBsSsProvisionedForSfTable and wmanIfBsClassifierRuleTable. This is, the entries on wmanIfBsSsProvisionedForSfTable

and wmanIfBsClassifierRuleTable are automatically erased too. This is the reason why the deletion process is very simplified. All the process can be clearly observed in Figure 31

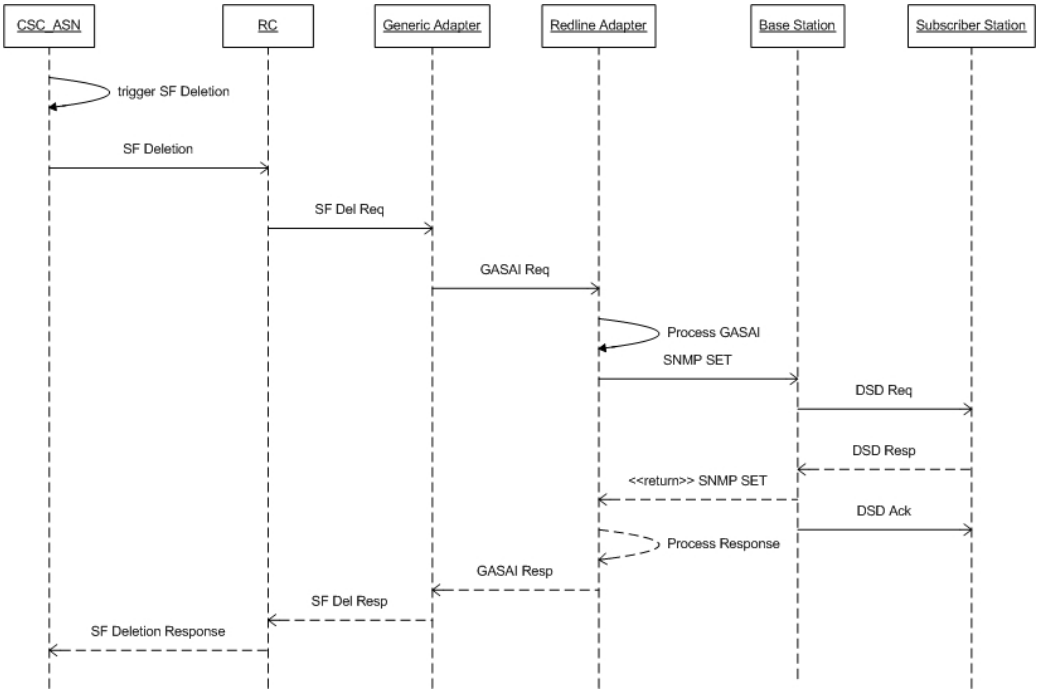

Figure 31: Service Flow Deletion Processing

To finish this section we have to illustrate the SF modification processing in the WiMAX segment, show in Figure 32.

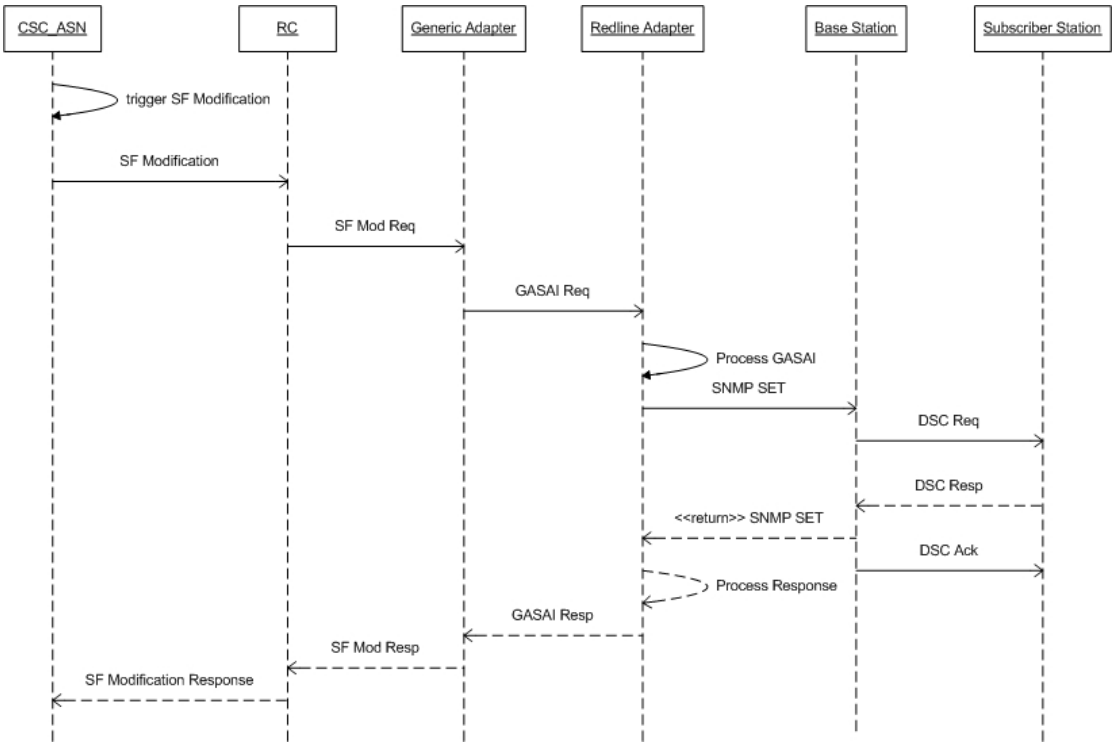

Figure 32: Service Flow Modification processing

To modify the QoS Parameters of a determined SF, the process is also relatively simple. The Redline Adapter only needs to search for the QoSProfileIndex associated with the requested SFID and set the parameters with the new values: a SNMPSET PDU is packed with the new service flow priority, max rate, min rate, jitter and max latency values and sent to the BS Agent. The BS and the SS uses the DSC messages to change the Service Flow parameters. When the Redline Adapter receives the response it builds the GASAI response and sends it to the Generic and from there, the message is forward to the RC and lately from the RC to the CSN_ASN.

5.2 Results and Performance Tests in WEIRD

In this chapter the accomplished debug and performance tests are illustrated and discussed. All the implemented Adapter functionalities had been tested several times with varied parameters in order to prove the implemented solutions. The performance tests were accomplished for two distinct modes of operation, the Point-to-Point and the Point-Multi-Point.

5.2.1 Integration tests of the ASN-GW modules

Figure 33 shows the network topology used to test the WEIRD ASN-GW gateway modules, and consequently the Redline Adapter module.

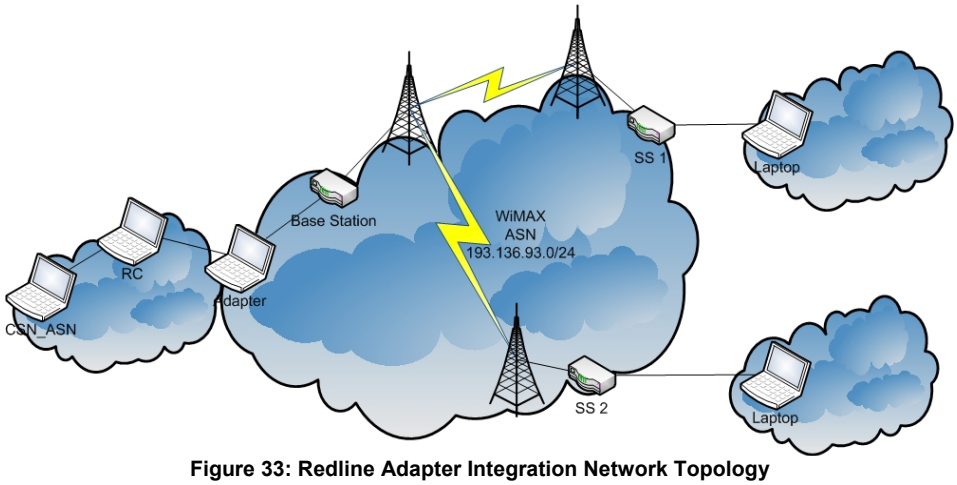

Figure 33: Redline Adapter Integration Network Topology

All the ASN-GW modules add been successfully integrated. A considerable amount of tests had been carried out. In the following, we describe an example.

In the presented situation, the CSC_ASN sends four Service Flow creation messages and two service flow deletion messages. The flow of information along the ASN-GW modules was described in section 5.1.2.

Note that the Redline Adapter debug messages are colored to simplify its analysis. The SF Reservation message is green, the SF Modification message is yellow and the SF Deletion message is red. The trap messages are violet. All the other prints are normally white, or blue.

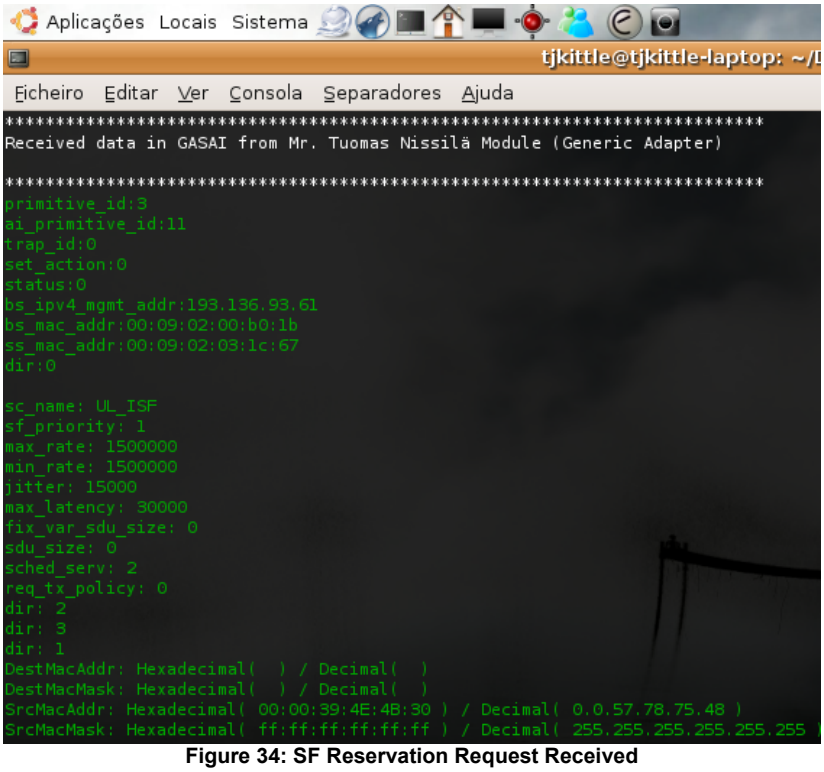

Figure 34: SF Reservation Request Received

In Figure 34 we receive a SF reservation request from the Generic Adapter. The received parameters are listed. The 802.3 Ethernet CS will be used to set the classifier.

We start to process the request by setting the rows in four tables, the Service Class Table, Service Flow Provisioned Table, Service Flow For Provisioned Table and Classifier Rule Table.

All set response values are shown below, in Figure 35.

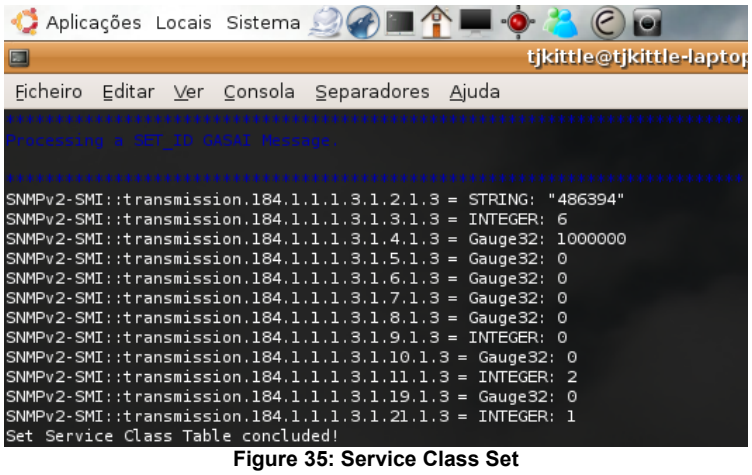

Figure 35: Service Class Set

It can be observed the Service Class Table set, and below (Figure 36) the Provisioned SF Table, Provisioned For SF table and the Classifier Rule Table ones.

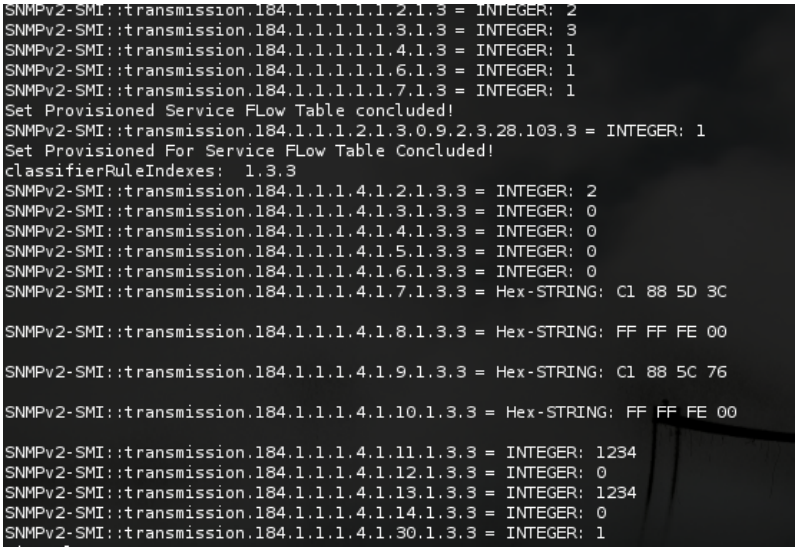

Figure 36: Provisioned SF Table, Provisioned For SF Table and Classifier Rule Table Set

In the next figure it is shown a received delete message and its processing.

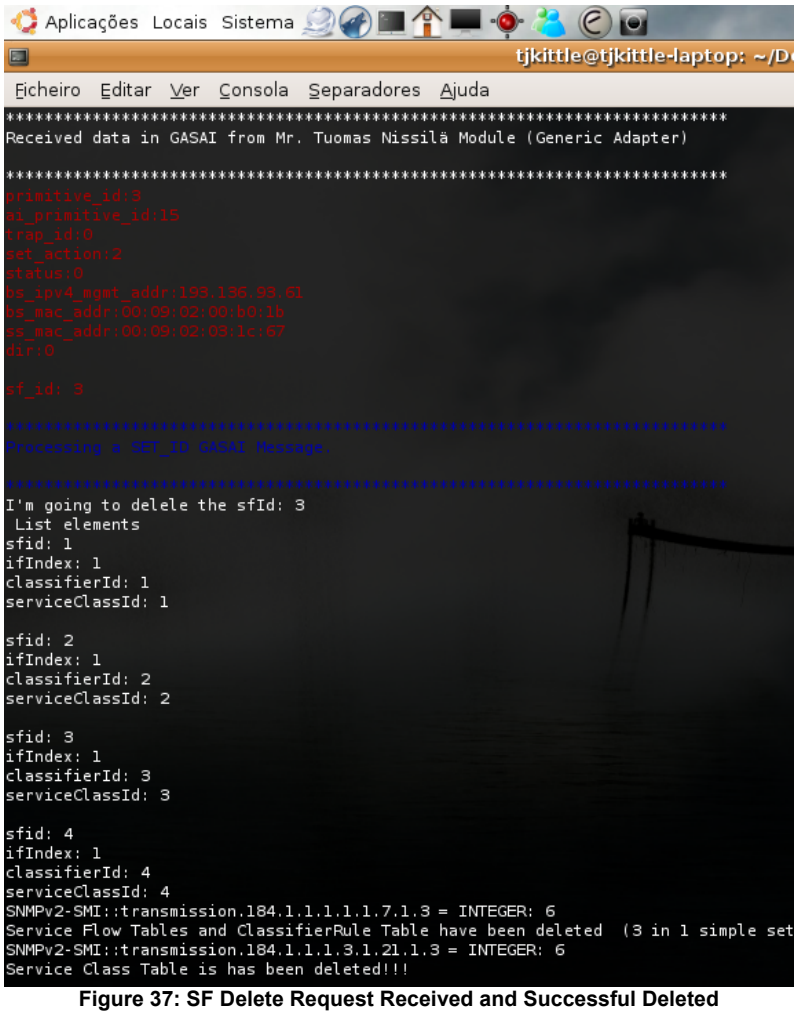

Figure 37: SF Delete Request Received and Successful Deleted

The HTTP interface of the Redline AN100U (Figure 38) proves that the SETs were correctly made.

SFID	SS Mac	SS Name	Direction	SC Name	SF State	Prov. Time	CS Specification	Enable/Disable
1	00:09:02:03:1c:67	Subscriber1	downstream	DL_ISF	active	2 days 02:04:50	802.3 Ethernet	Enabled
2	00:09:02:03:1c:67	Subscriber1	upstream	UL_ISF	active	2 days 02:04:50	802.3 Ethernet	Enabled
4	00:09:02:03:1c:67	Subscriber1	downstream	616858	active	2 days 02:04:59	IpV4	Enabled

Figure 38: SF Table (http interface)

As illustrated above, there are three Service Flows since the SFID 3 was deleted.

The Service Class QoS Parameters and the Classifier Rule have the correct values. Moreover the entries in the Service Class and Classifier Rule tables associated with the deleted SFID were also erased (respectively, Figure 39 and Figure 40).

SC Name	Traffic Prio.	MaxSTR	MinRR	MaxLat	Fixed vs Var. Sdu	Sdu Size	Sched. Type	ReqTxPol
DL_ISF	1	1500000	1500000	30000	Variable	0	BE	
UL_ISF	1	1500000	1500000	30000	Variable	0	BE	
616858	6	1000000	0	0	Variable	0	BE	

Figure 39: Service Class Table (http interface)

SFID.ClsID	State	Prio.	DstMac Addr/Mask	SrcMac Addr/Mask	Enet Type/Prot	UserPri Low-High	VlanID	Ip Prot.	Tos Low-High/Mask	DstIp Addr/Mask	SrcIp Addr/Mask	DstPort Start-End	SrcPort Start-End
1.1	active	1		00:13:a9:a6:28:15 ff:ff:ff:ff:ff:ff		-			- /				
2.2	active	1		00:00:39:4e:4b:30 ff:ff:ff:ff:ff:ff		-			- /				
4.4	active	2				-		0	0 - 0 / 0	193.136.93.60 255.255.254.0	193.136.92.118 255.255.254.0	1234 0	1234 0

Figure 40: Classifier Rule Table (http interface)

This demonstrates the correct operation of the develop application. As can be observed in the following ethereal capture, the Adapter exchanges SNMP SET Messages with the BS and receives SNMP Response messages with the assigned values for each requested OID.

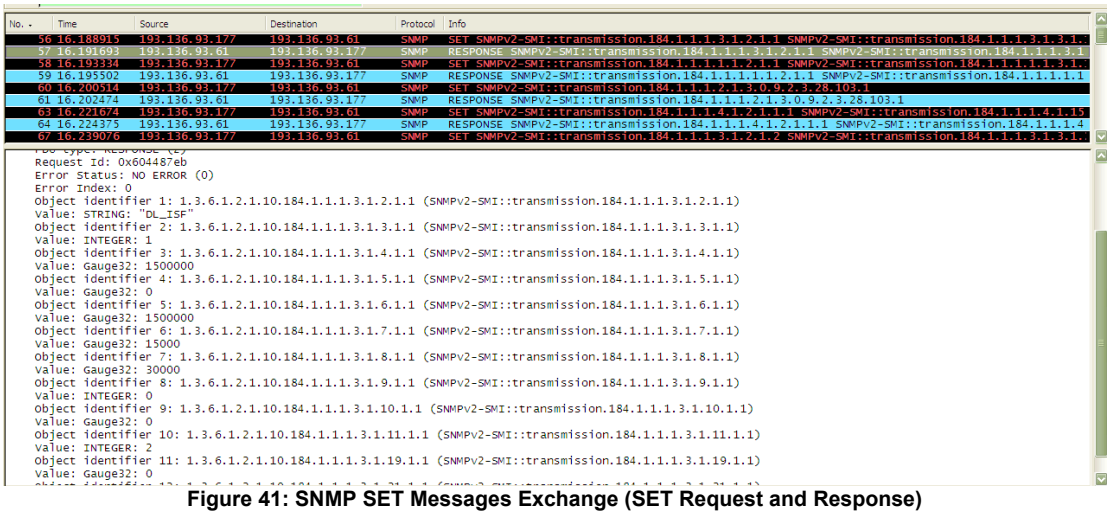

Figure 41: SNMP SET Messages Exchange (SET Request and Response)

5.2.2 Performance Tests

After a slightly demonstration of the SNMP application capabilities, a few performance tests have been accomplished in order to attest the Adapter efficiency.

When there is a Service Flow Reservation in the WiMAX equipment, four tables need to be set. Besides, to add a row to the Service Class table, it is required to set twelve objects; to the Provisioned Service Flow Table it is required five objects; one object for the Provisioned Service Flow Table; for the Classifier Rule Table, this number of objects depends on the

Convergence Sub layer that is in use. When using IPv4 as CS fourteen objects are assigned, when using the 802.3 Ethernet only six objects are set.

For the Service Flow Deletion we just set one object in two different tables, the Service Class Table and the Provisioned Service Flow Table.

The modification is also fairly simply when compared with the Service Flow reservation. In this case are just re-assigned five objects of the Service Class Table in order to carry out the modification.

Following is presented a table (Table 11) indicating the number of objects that must be set in order to accomplish the service flow reservation, modification and deletion having into account the different Convergence Sub layers.

***Service Flow type*/CS**	**IPv4**	**802.3 Ethernet**
Service Flow Reservation	32	24
Service Flow Modification	5	5
Service Flow Deletion	2	2

Table 11: Number of OIDs to set for the different SF Resv/Mod/Del

It must be noted that the clock used in this first set of performance tests has got a +-10 ms precision, it is to say that if the processing time goes under the 10 ms two distinct values can be returned. If the processing time is in the interval [0,5[ms the return value is 0 ms, otherwise if the processing time is between [5,10] the value returned will be 10ms.

Since the Service Flow Modification and Service Flow Deletion implies that just 5 or 2 MIB objects had to be set, the processing time obtain was generally 0.0 ms, which didn't allow to perceive the differences when doing several service flow modifications or deletions. So it's just concluded, that the time consumed by a service flow modification or deletion, goes under 5 ms, which is an excellent result, when compared with the 21 seconds taken for a modification when using the previous 802.16a equipment.

So, only the reservation process was considered in the sections 5.2.2.1, 5.2.2.2, 5.2.2.3 and 5.2.2.4.

These results were obtained for a 256K bandwidth allocation request. Half of the samples are in the downlink direction and the other in the uplink direction. The time values represent the round-trip delay of SNMP request via Ethernet link in milliseconds.

5.2.2.1 PTP scenario performance measurements using IPv4 as CS

The Point-to-Point mode of operation in which the Service Flow reservation process is always done for the same SS is shown below (Figure 42)

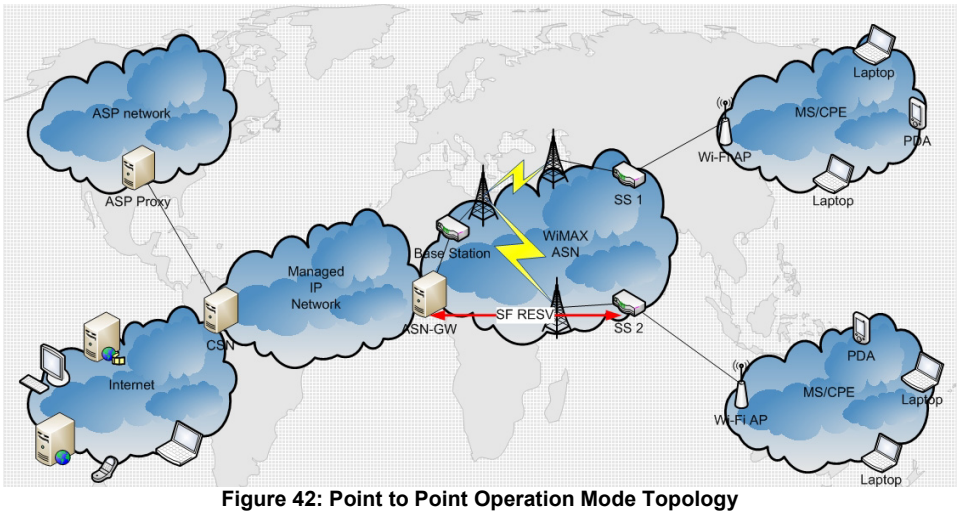

Figure 42: Point to Point Operation Mode Topology

Table 12 illustrates the downlink and uplink performance measurements for the reservation requests.

Service Flow Reservations Number	Total Time (ms)	Time (s)	Mean Reservation Time per flow (ms)
1	10	0.01	10,81395349
5	60	0.06	
10	110	0.11	
20	230	0.23	
50	520	0.52	
100	720	0.72	10,6
500	5640	5.64	

Table 12 : Downlink/Uplink performance measurements for reservation requests

It was not distinguished considerable variations of time with the increment of requests amount. Additionally, it was noticed that WiMAX equipment stayed quite stable with a sequential 500 reservation requests.

This means that the Adapter and the WiMAX equipment are able to deal with a high number of sequential requests. The average round trip is 10.8 ms, a good performance time.

5.2.2.2 PTP scenario performance measurements using 802.3Ethernet as CS

When using the 802.3 Ethernet Convergence Sublayer, it is expected that the round trip times are comparatively under the values illustrated on previous table (Table 12).

Service Flow Reservations Number	Time taken (ms)	Time (s)	Mean Reservation Time per flow (ms)
1	20	0.02	10,58139535
5	60	0.06	
10	110	0.11	
20	210	0.21	
50	510	0.51	

Table 13: Downlink/Uplink performance measurements for reservation requests

Like we were waiting for the mean reservation time per flow in this situation is around 10.6 ms, which is less that the mean reservation time when requesting a Service flow reservation using the IPv4 CS. This occurs, apparently, because of the distinct amount of OIDs two be set in the two situations. In any way the variation is quite small.

5.2.2.3 PMP scenario performance measurements using IPv4 as CS

The Point-Multi-Point mode of operation in which the Service Flow reservation process is done for more than one SS is shown in Figure 43.

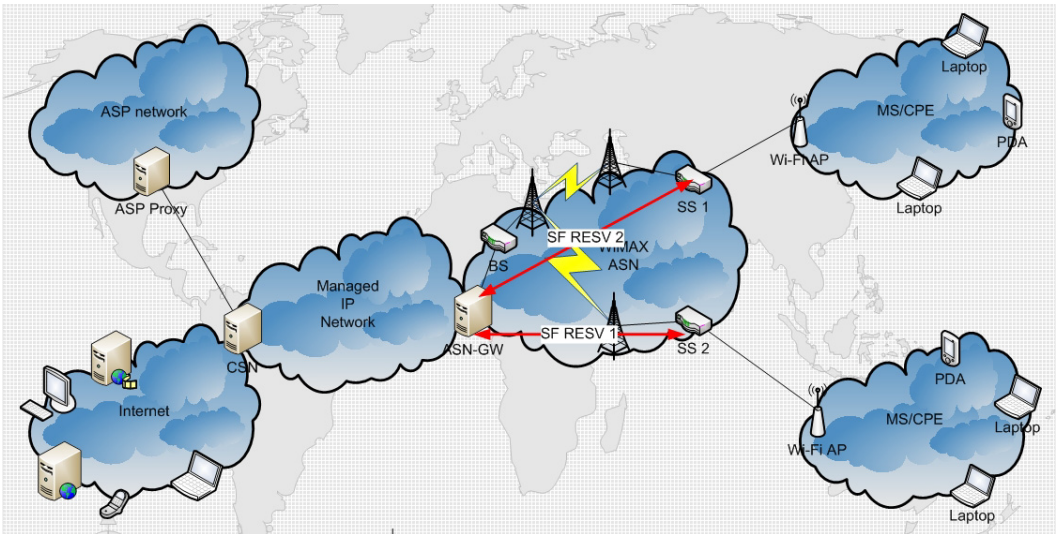

Figure 43: Point-Multi-Point operation mode topology

In our tests, the even requests where done for one Subscriber and the odd requests for another. Table 14 resumes the results.

Service Flow Reservations Number	Time taken (ms)	Time (s)	Mean Reservation Time per flow (ms)
2	30	0.03	11,8852459
10	110	0.11	
20	210	0.21	
40	590	0.59	
50	510	0.51	

Table 14: Downlink/Uplink performance measurements for reservation requests

Unsurprisingly, using the PMP mode of operation, the mean reservation time slightly increases, in this case it is 11.9 ms. Once again, the variation time is very small when compared to the PTP tests and can be almost irrelevant.

5.2.2.4 PMP scenario performance measurements using 802.3Ethernet as CS

Service Flow Reservations Number	Time taken (ms)	Time (s)	Mean Reservation Time per flow (ms)
2	30	0.03	10,24590164
10	100	0.10	
20	200	0.20	
40	410	0.41	
50	510	0.51	

Table 15: Downlink/Uplink performance measurements for reservation requests

The performance measures when using 802.3Ethernet as CS in the PMP operation mode were surprisingly better than the ones when using the PTP mode. This only comes to confirm that the equipment can efficiently manage several subscribers. In fact the variations of round trip times are very small, and the times are extremely close to each other even when varying the mode of operation. The mean reservation time in this situation was 10.2 ms.

5.2.2.5 Comparison between the PTP and the PMP Scenarios

Figure 44 presents a comparison between the mean reservation time obtained in PTP and PMP operation modes while also varying the WiMAX Convergence Sub-layers (IPv4 and 802.3).

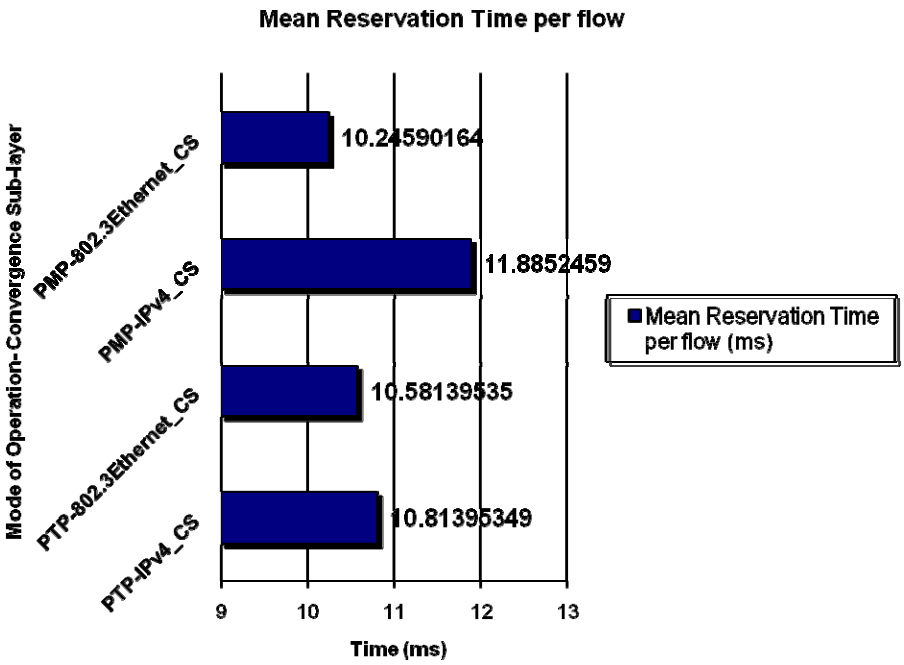

Figure 44: Mean Reservation Time per flow

The results show that the performance is independent of the number of requests or the mode of operation being used in the 802.16 network. Varying the CS and requesting a considerable amount of sequential service flows reservations do not interfere noticeably with the

performance. Besides the reservation times, the implemented solution has shown that the service flows modifications and deletions stay under the 5 ms. The variations are so small that they practically can be considered as insignificant. To finish this section, it must be mentioned that it would be of tremendous interest, to realize the above measures having a more realistic scene in which the subscriber station is distanced from the BS in the range of km.

5.2.2.6 WEIRD Resource Control architecture signalling tests

The above sections illustrate and discuss the obtained results in a first phase. In spite of the significant interest of those tests, some points remain unclear, for instance, the mean reservation times were estimated and include de internal processing time of the Redline Specific Adapter (RSA), and the modification and deletion times, are highly imprecise. Furthermore the presented values are estimated round trip times relative to the Adapter interaction with WiMAX segment and the exact time distribution over RSA tasks is not known. It is valuable to know (using a more precise clock) the internal RSA processing time, the time spent in each interaction with WiMAX system, it is to say, the time spent when performing individual SNMP SET requests.

This section is devoted to the discussion and analysis of more detailed Redline Specific Adapter (RSA) performance results. A considerable array of times was collected in order to analyze the time distribution across the different tasks accomplished by RSA. The RSA, as described on subsection 5.1, is the module that interacts with the WiMAX equipment. Thus, the total time spent from the reception of a request (SF Reservation / SF Modification / SF Deletion) to the sending of the correspondent answer to the GA was obtained; the partial times were also gathered, in order to distinguish between the internal processing time of the RSA module and the time it takes to set each SNMP MIB table. Figure 45 illustrates the RSA performance times. The RSA Resv/Mod/Del Total Path blocks show the total time used up by RSA to process each request, that is, the entire path since it receives a request from the GA, until it sends back the response to the latter. The RSA Resv/Mod/Del Total SNMPSET blocks represent the sum of all SNMPSET times needed, respectively, for a SF reservation, modification, or deletion. Finally, the RSA Resv/Mod/Del Internal Processing blocks represent the internal processing time of RA routines.

As can be observed in Figure 45, the RSA internal processing time is so small that the total path time is almost not affected, and therefore unseen on the graphic bars. In the worst case, the internal processing time is less than 55 us. This case occurs when 256 SFs are deleted, which causes the module to deal with considerable processing work when looking for the associated indexes to set the SNMP MIB tables.

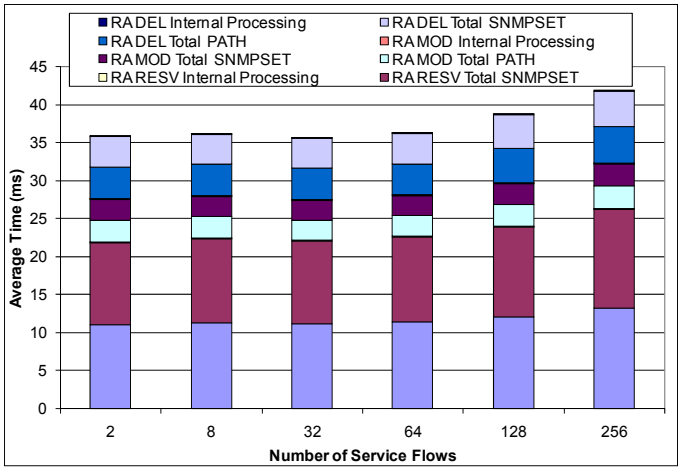

Figure 45: RSA performance times

Another important fact that can be concluded from the graphic is that QoS session's establishment takes more time than the deletion ones, and these, in turn, are more time consuming than the modification requests. Furthermore, we can also perceive that there is a slight increase of time when the number of SFs increases. Nevertheless, these values are kept stable, showing that the RSA and the WiMAX equipment are prepared to deal efficiently with a large number of sequential requests. Finally, the differences between the RSA Resv/Mod/Del Total SNMPSET processing times are due to the different amount of Object IDs (OIDs) that have to be set on the WiMAX MIB, which is larger for the reservation requests when compared to modifications or deletion ones.

Table 16details all the SNMP MIB Tables, and the correspondent OIDs number that are assigned when performing a SF Reservation, Modification and Deletion using the IPv4 CS.

SF Request: MIB Tables	***Functionality***	***OIDs***
DEL : ServiceClassTable	Contains the SF QoS parameters	1
MOD : ServiceClassTable		5
RESV : ServiceClassTable		12
DEL : ProvisionedSfTable	Contains the SF profiles provisioned by NMS	1
RESV : ProvisionedSfTable		5
RESV : ProvisionedForSFTable	Maps the MAC addresses of SSs to the provisioned SFs	1
RESV :ClassifierRuleTable	Contains packet classifier rules associated with SFs	14

Table 16: WiMAX QoS MIB Tables

Figure 46 shows the time spent by every single SNMP MIB table set.

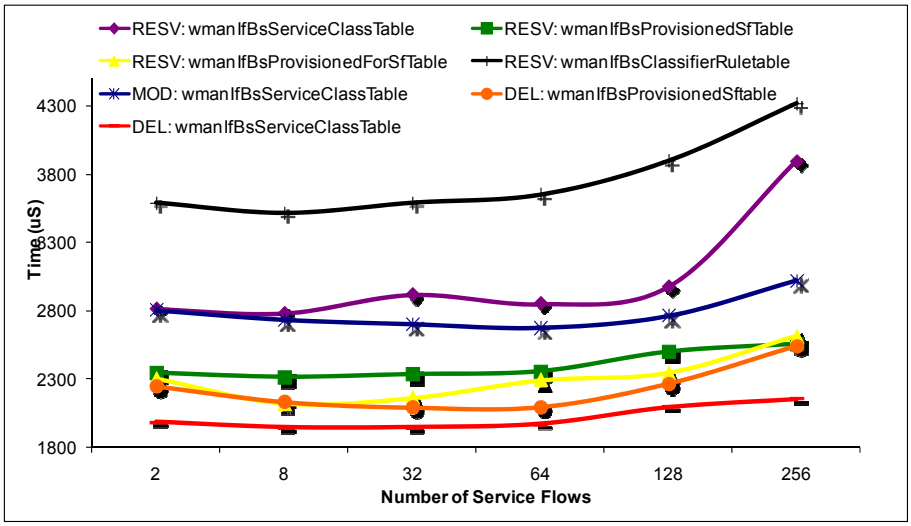

Figure 46: Single SNMPSET performance times

Once again, the inherent processing time is coupled with the increased number of SFs requests, staying a little higher as we increase the number of sequential requests. Furthermore, the time taken to process each SNMPSET is also strictly related with the number of OIDs that must be set in each operation – the greater the number of OIDs to assign, more time is spent on performing this task by the equipment. The differences that occur when setting distinct SNMP MIB tables with the same OIDs number are due to the inherent processing time of WiMAX equipment for those tasks. For instance, erasing an existing SF by the WiMAX equipment is more time consuming than just doing some amendment to the QoS parameters of an existing one. Moreover, when deleting a ProvisionedSfTable row entry, we are in fact deleting, at the same time, all the associated entries in ProvisionedForSfTable and ClassifierRuleTable. For that reason the deletion process when erasing elements of ServiceClassTable is smaller than when deleting elements from ProvisionedSfTable.

5.3 Conclusions

This chapter presented a novel solution for the dynamic resource control in WiMAX environments, motivating the use of the IEEE 802.16f MIB standard. The presented system architecture was developed in the WEIRD project, and comprises Resource Controller and WiMAX Adapter modules for the support of QoS reservations, modifications and deletions, and resources management. Furthermore, interesting functionalities, such as Dynamic Network Discovery, implemented over SNMP traps, have been depicted.

In order to validate the QoS resource management support of Redline Specific Adapter, QoS measurements have been performed in a WiMAX certified testbed, varying the mode of operation and the Convergence Sublayers. The achieved results have shown that the

processing times for the QoS reservations, modifications and deletions are very small, enabling the use of the WiMAX based architecture in NGN real-time environments without traffic disruptions.

6 Chapter 6 Architecture for Resource Control and Mobility support in DAIDALOS II

This chapter presents a description of the specified and developed Radio Resource Control architecture in DAIDALOS II, detailing the most relevant implementation characteristics.
The implemented solution was extensively evaluated both in control and data plane, and the performance results are presented and discussed throughout section 6.2. In the control plane, results concerning signalling performance over the modules responsible for the management/transport of Layer 2 (L2) Quality of Service have been gathered. In the data plane, a traffic generator was used, JTG [JTG], measuring the aptitude of WiMAX segment to adapt to dynamic environments, even when under stressful conditions. Moreover, the WiMAX segment was afterwards concatenated to a WiFi cloud, and more reliable end-to-end QoS results have been carried out.

6.1 Developed architecture for Resource Control with mobility support by means of 802.21

In section 3.2 an overview of QoS and Mobility architecture on DAIDALOS was given. Now, DAIDALOS II architecture is more detailed from WiMAX technology point-of-view, presenting the relevant integration points of the IEEE 802.16 technology on DAIDALOS network heterogeneous environment.

6.1.1 IEEE 802.16 Integration in End-to-End QoS Architecture

This section depicts the process for QoS in IEEE 802.16 technology integrated in the end-to-end QoS architecture. It is presented a L3 session setup scenario, depicting the steps to perform the session establishment.
IEEE 802.16, as a Broadband Wireless Access (BWA) technology, is provided by a backhaul platform (through the Base Station – BS – and the Subscriber Station – SS) where the access network and the wireless access technologies (WiMAX-WiFi) are bridged together Figure 47.

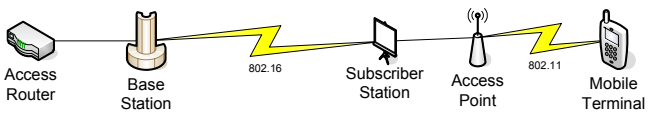

Figure 47: Scenario using 802.16-2004 as a backhaul

To perform end-to-end QoS setup, the Next Steps In Signalling (NSIS) protocol suite [NSIS] is used. As mentioned previously, the MT and the AR contain elements that perform the

enforcement of the QoS in the network and trigger the QoS process for admission control and resource reservation, namely the QoS Client (QoSC) and the QoS Manager (QoSM). Figure 48 depicts this process.

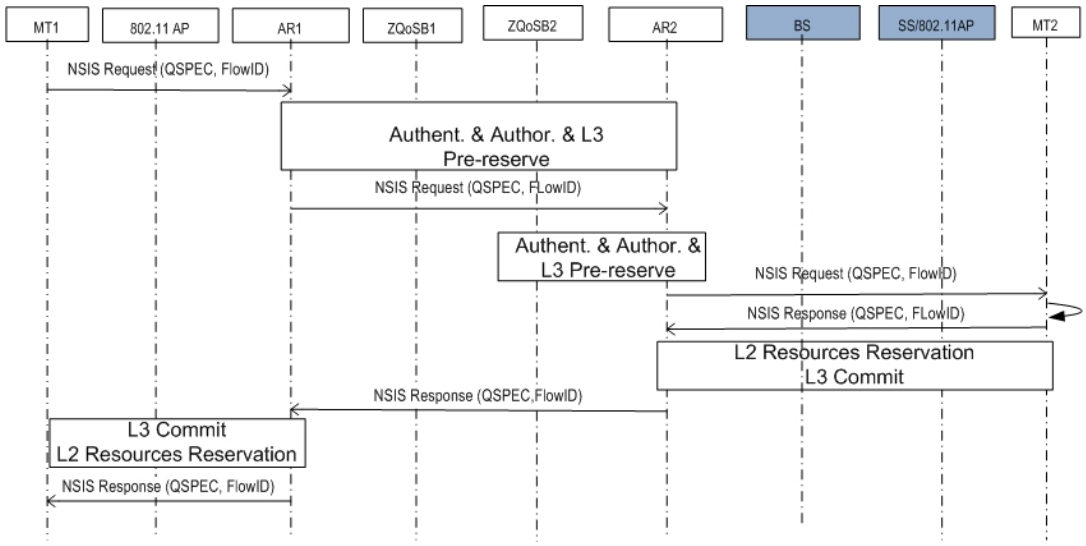

Figure 48: QoS Session Setup scenario End-to-End

The QoSC module running in MT1 is triggered to reserve resources with specified QoS for new sessions. Upon the detection of a new session, the QoSC triggers an NSIS message. The NSIS message carries a QoS Specification (QSPEC) object describing the QoS session. This message will be captured by the serving AR1 that will mediate the communication with the ZQoSB, performing a set of actions, such as authentication (resorting to an A4C), authorization and pre-reservation of L3 resources in the AR. Here we assume the successful achievement of these actions.

After access granted, the AR will forward the NSIS message to the flow termination point. The destination AR2 checks, equally, authorization with its local ZQoSB2 and delivers the message to the destination terminal, MT2. The MT2 is attached to a WLAN AP that is bridged with an 802.16 Subscriber Station (SS). The layer 3 signalling stated in this stage is transparent for the WiMAX network, in the sense that a signalling Service Flow is previously allocated, in both traffic directions, uplink and downlink. If the destination terminal accepts the request, a backwards response is sent. When the NSIS response message reaches both ARs, they reserve L3 resources and signal the downstream L2 entities to create reservations according to the specific technologies, afterwards L2 reservations proceed. The layer 2 process is depicted in more detail in the next section. Only after the end of the L2 QoS Control, the Layer 3 process is considered complete.

6.1.2 IEEE 802.21 and QoS Extensions For QoS and Mobility Integration

The presented architecture considers the upcoming standard IEEE 802.21 Media Independent Handovers (MIH) as the mean to implement protocol operations for handover execution. The IEEE 802.21 [802.21] is the common denominator that abstracts the heterogeneity of the access technologies. We used it to join together QoS provisioning and mobility. A common framework like this contributes for a clean network design and a new set of simplified network operations.

For this purpose, it was necessary to extend IEEE 802.21 draft with a new set of functionalities to cope with the requirements for tightly coupled QoS integration for session setup and handover scenarios. It must be noted that the reference IEEE 802.21 draft [802.21] used during DAIDALOS II specification phase has been updated, and consequently some of its nomenclature has also changed since then.

6.1.2.1 QoS Extensions for 802.21 and mobility

As previously referred, L2 QoS management is executed at the ARs by the L2QoSC. It interacts with the MIH Function as a high level entity thus becoming an MIH-user. The Layer 2 entities may supply topology information and link layer events (such as signal strength, available bandwidth) through 802.21 mechanisms, to the QoSM, as well as to the ZQoSB. As it is well known, IEEE 802.21 considers the separation of the handover procedure in two phases: a preparation phase that comprises the preparation and query of available resources in the handover target, and commit phase that embraces the activation of the pre-provisioned resources. This is in fact very important, depending on the technology in place, since it may require some time to request a certain QoS level from the technology, creating a noticeable impact in the user experience. In spite of conceptually considered in DAIDALOS II specification, the adoption of the *MIH_Handover_Prepare.request* command used to prepare the link in the handover target and to query for available resources (and furthermore, extended with specific QoS parameters, to allow the preparation of QoS reservations), was abandoned. In fact, considering federation (inter-domain) signalling, the handover preparation in two cycles, would impose a great penalty in terms of delay, attending for instance to the large amount of messages that would be needed to be exchange, between ARM, QoSBroker, A4C's. For this reason, the implementation was slightly changed to use only one of the phases. This process does not penalise the WiMAX technology, since the QoS reservation and modification process is relatively fast as will be following verified.

Taking this approach into account, the following primitive has been extended in the handover scenarios:

- ***MIH_Handover_Commit.request*** was extended to include QoS specific parameters

which allow the execution of QoS reservations;

Once the handover execution imposes the exchange of two commands, *MIH_Handover_Initiate.request* and *MIH_Handover_Commit.request,* a new command set, *MIH_Resource_Activate.request/response*, was created in order to reduce session setup time, combining the functionality of the *Initiate* and *Commit* messages in a single message exchange. This new command is the one used to provide the 'L2 Resources Reservation' process in Figure 48.

Specific parameters are also required to supply information for QoS provisioning. The QoS parameters consist of a list that ranges from 1 to 16 *FlowSpec* objects describing the resources for allocation of a specific micro-flow, and containing the following information:

- *Direction*: direction of the flow, upstream or downstream;
- *TSpec*: describes (using standard token bucket parameters) the traffic envelope to be transported;
- *RSpec*: describes the actual *bitrate* and class of service for allocation at layer 2. The class identifier is used to classify packets belonging to a flow, as well as the class of service to be applied;
- *FilterSpec*: containing the IPv6 five tuple information, used to classify the packets in the IEEE 802.16 link.

Figure 49 illustrates the proposed process of reservation of L2 resources in the compound 802.16 and 802.11 networks, as a reaction to a mobility trigger. This process integrates 802.21 handover messages, extended with QoS information, having the Simple Network Management Protocol (SNMP) [RFC1157] to trigger the addition of a new Service Flow (this will be better explained in the next section), by means of 802.16 messages (e.g. Dynamic Service Addition/Change/Deletion – DSA/C/D).

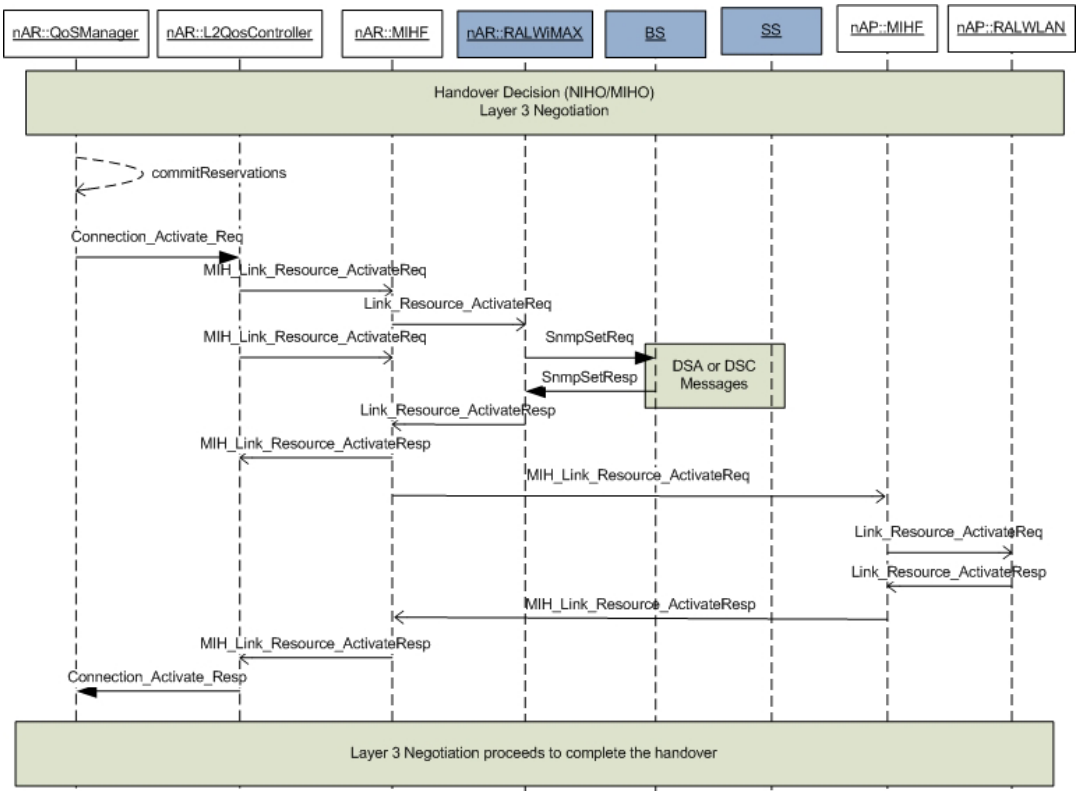

Figure 49: Handover Scenario

This scenario requires the handover to the WiMAX/WLAN technology. It is of vital relevance to reserve resources in the handover target preserving the QoS level. Assuming that the ZQoSB triggered a *MIH_Handover_Initiate.request* (in this case, the network triggered the handover), after receiving the correspondent terminal response, it can start the QoS reservation process at the handover target. Thus, it sends a *MIH_Handover_Commit.request* to the QoS Manager (QoSM) module existing in the AR of the local domain containing the handover target network. Following, the QoSM will reserve L3 QoS resources and then forwards a *connection activate* message to the L2QoSC, which will in its turn perform L2 resources allocation in the WiMAX segment and in the concatenated WLAN network. Hence, L2QosController sends two *MIH_Link_Resource_Activate.request's* to the MIHF, one to RAL_WiMAX (Radio Access Layer in WiMAX) and another to RAL_WLAN. MIHF translates the received request to the respective technology, forwarding the *Link_Resource_Activate.request* to the RAL_WiMAX and to the RAL_WLAN. The RAL_WiMAX will interface with the WiMAX equipment via SNMP, sending *SNMPSET* messages. These messages are translated into 802.16 *Dynamic Service* Messages, accordingly, *Dynamic Service Addition/Change/Deletion* (DSA/C/D). After receiving the *SNMPSET* response, the RAL_WiMAX answers to the MIHF that will forward the response to the L2QoSC. The same happens with the RAL_WLAN, when it allocates the channel in the 802.11 segment (802.11e-2005). When L2QoSC receives both *MIH_Resource_Activate.response's*, it sends a *Connection_Active_Req* to QoSM. The

ZQoSB is now able to send *MIH_Handover_Commit.response* to the terminal for handover commitment. The terminal is now able to execute the handover. When this handover is complete, a *MIH_Handover_Complete.req* message is sent to the ZQoSB, which initiates the release of resources in the previous link.
Considering the presented solution, the IEEE 802.16 technology, seamlessly supports mobility. From L2 QoS point of view, handover reservations are performed in the same way as in the session setup process. In this sense, the 'L2 Resources Reservation' process in Figure 48 is similar to this process in Figure 49. Considering that the architecture assures the preparation of resources in advance, the mobility support is seamless. Moreover, using this framework, it is able to provide a seamless process for different technologies and integrate 802.16 in a heterogeneous environment. However this point, concerning mobility support, will be explored in more detail in forwarding sections.

6.1.2.2 Mobility Management in DAIDALOS

DAIDALOS II realizes a partitioning between Global Mobility and Localized Mobility Management. The Control Plane as aforementioned is based on IEEE 802.21 framework, combining mobility and QoS signalling and covering both vertical and horizontal handovers.
In DAIDALOS, the mobility management comprises control plane protocols for GMD (Global Mobility Domain) and LMD(Local Mobility Domain). Global Mobility is implemented through MIPv6 protocol whilst, Local Mobility is based on a NetLMM draft proposal [NETLMMProto].
The use case scenario involving WiMAX network, comprises an intra-technology, LMD (Local Mobility Domain) handover, from WLAN1 to WLAN2+WiMAX. WiMAX network is used as a backhaul to a Wireless LAN network. Despite the fact of this scenario is not exploiting PMP capabilities of WiMAX, the developed architecture totally supports this mode of operation. Thus, it is viable to perform handovers, from WLAN1+WiMAX to WLAN2+WIMAX. Even more, though the involved handover is intra-technology, since, from the terminal point of view it corresponds to an handover from Wireless LAN to Wireless LAN, considering DAIDALOS environment the WLAN1 technology could be any other technology.
Mobility in DAIDALOS can be initiated from the terminal side, hereinafter referred as (Mobile Initiated Handover) MIHO or from the network side, hereinafter referred as NIHO (Network Initiated Handover).
In order to allow a clean design and deployment of IEEE 802.21 to the whole access network, access points and access routers implement the MIH layer. The design also allows easy integration of functionalities such as QoS thus enabling QoS driven NIHO operations.

In this architecture, a network entity decides upon handover based on all information available when, how and where to mobile terminals should execute handovers.
In order to take such a decision, the decision entity needs accurate and up-to-date information. This information can be generally classified into static and dynamic information.

Static information, such as cost, QoS capabilities or mobility protocols supported by certain network, can be obtained upon request to an information database. However, dynamic information, such as load in certain network nodes or networks perceived by the terminal, is rather obtained based on event triggering.

Events can be triggered either by end mobile terminals or by other network nodes involved in the communication path.

The execution of the handover will be dependent on the scenario where it is happening. In scenarios with a high density of heterogeneous networks and overlapping, handover might be originated to improve the current connection or better satisfy user's preferences (e.g. cheaper networks preferred). In these cases, handover is not time critical and the decision can be taken with a complete set of information. On the other hand, in scenarios where overlapping areas are not large enough, handovers must be performed as fast as possible in order to maintain ongoing sessions. In such cases, the decision to handover might be based on a partial set of information, possibly leading to not optimal handover decisions but assuring user session continuity.

Figure 50 depicts how mobility can be seamless handled by WiMAX network system when performing a Mobile Initiated Handover, inside the same domain and concerning a handover from a WLAN1 network to a WLAN2 network backhauled by a WiMAX network. This sequence is largely simplified, since they do not contain detailed terminal and network modules.

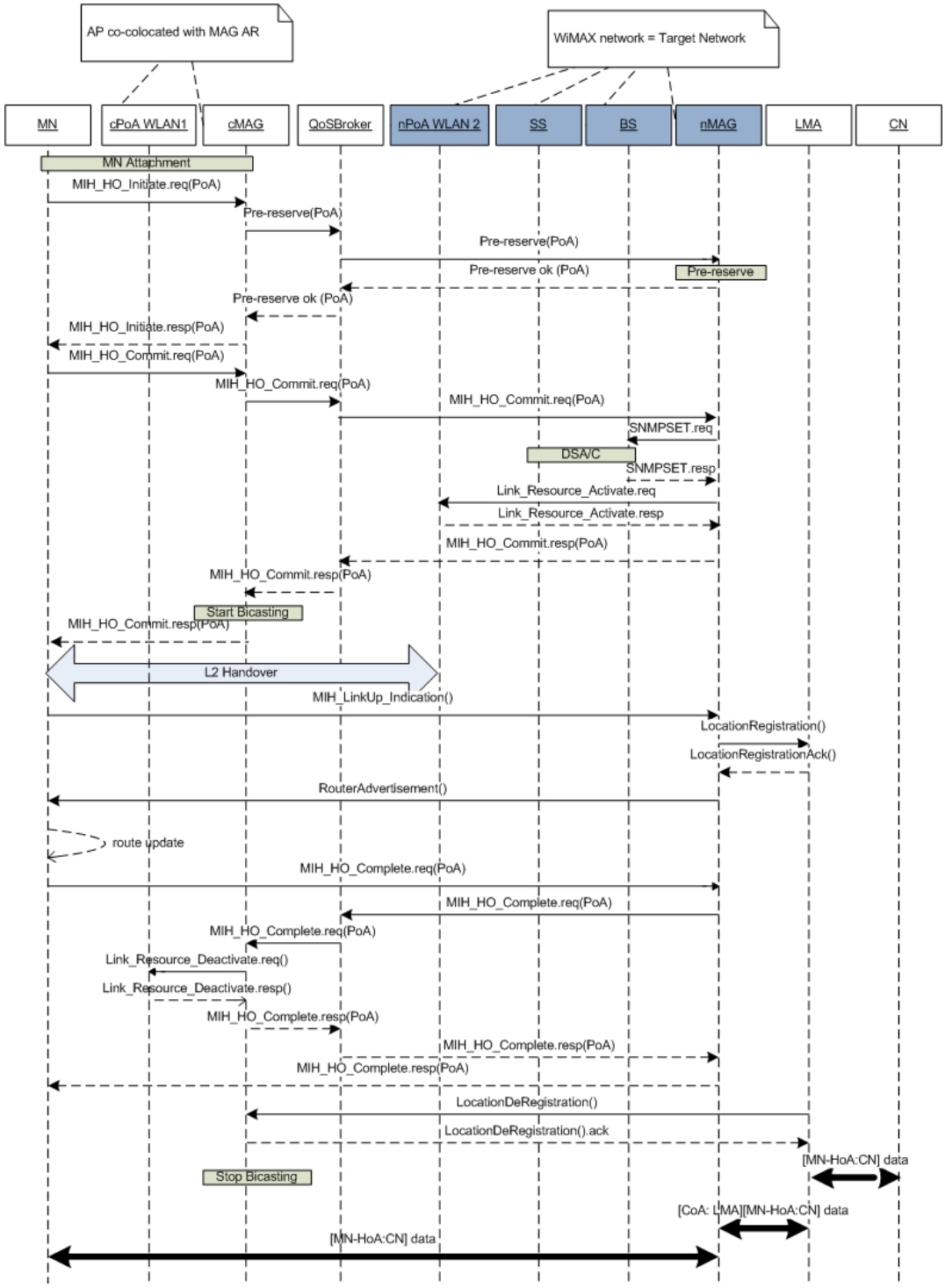

Figure 50: Intra-Domain, intra-tech, MIHO handover Scenario

When the handover decision module residing in the mobile terminal has selected the candidate target point(s) of attachment, this selection will be sent to the current point of attachment, through the primitive *MIH_Handover_Initiate.request*. The current AR will then perform the layer 3 resources pre-reservation before replying back to the mobile node with the result of the performed operations.

According to this result, the mobile node will continue the procedure by committing the handover to a specific point of attachment. This is done by means of a *MIH_Handover_Commit.request.* Upon the reception of this primitive, the new MAG AR will trigger the L2QoSCtrl, which will in turn, trigger the reservations across the layer 2 concatenated networks, in the case, the WiMAX segment and the WLAN segment. Considering the success of this operation the new AR, will send back to the terminal a *MIH_Handover_Commit.response*. After this, the mobile device will try to set a L2 connection with the new point of attachment, using the information obtained previously (e.g. BSSID - Basic Service Set Identifier, channel, etc.). If the attachment succeeds, the MN generates a *MIH_LinkUP_Indication* event, which is sent to the new MAG. This MAG will perform the mobility management operations, registering the new MN in the LMA. The LMA associates mobile nodes by its identifier with its address information, moreover, associating the mobile node with its serving MAG.
After this, a *RouterAdvertisement* is sent back to the MN, updating the route for its address. Finally the MN will send a *MIH_Handover_Complete.request* to the new MAG that forwards this message to the ZQoSBroker, so that the resources reserved in the old path are released to be used by other users. The LMA sends then a *LocationDeregistration* to the old MAG to remove the state it has which is related to the MN.

In the case of a NIHO, the network selection is performed by the mobility manager located in the network. This entity will be in charge of initiating the handover by providing the target point(s) of attachment to the mobile node, which will reply with a subset of possible point(s) of attachment in case some criteria can be applied.
At this point, the network entity will commit a handover to the proposed point of attachment, after reserving the convenient resources. The subsequent procedure will then be same as for the MIHO case, where a L3 connection is established after the L2 link is completed.

6.1.3 RAL WiMAX and Driver WiMAX implemented architecture

The developed work under DAIDALOS scope was accomplished after WEIRD project involvement. So, part of the functionalities of RALWiMAX and DriverWiMAX are common to the ones present on RSA and RALWiMAX/DriverWiMAX. Anyway, as aforementioned, DAIDALOS II goes beyond WEIRD requirements, which imposed a redefinition and special add-ons in terms of functionalities. DAIDALOS II requirements are depicted on section 3.2.3.
Figure 51illustrates the typical Access WiMAX network topology (802.16-2004) will be referring to in next paragraphs.

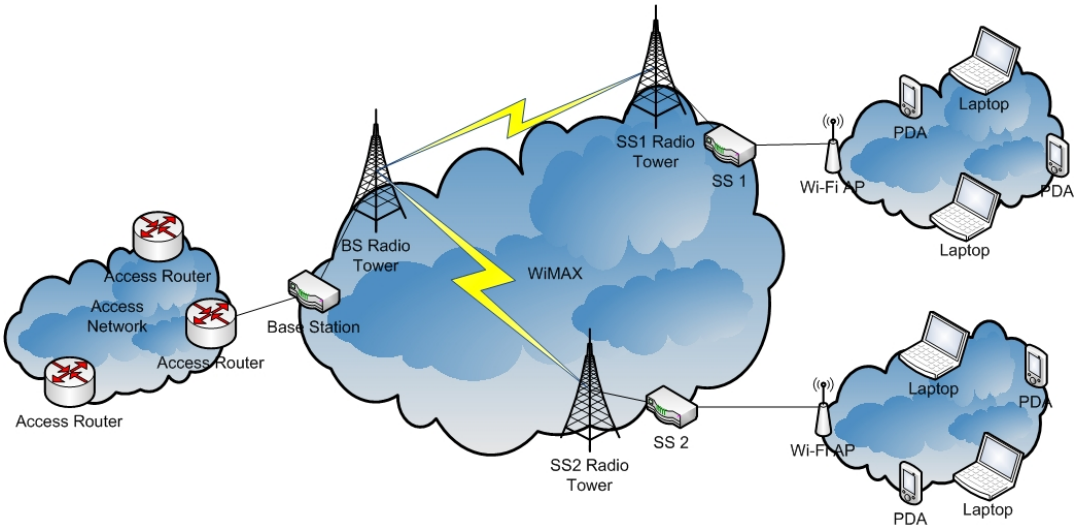

Figure 51: WiMAX network topology in DAIDALOS II

The shown WiMAX network architecture is composed by WLAN clouds, which are collocated with the CPE (Subscriber Stations). The BS will be in the operator side of the network, connected typically to a layer three entity, in the case an Access Router. The BS manages the associated Subscriber Stations in a Point-Multi-Point mode of operation. The eventual mobile users connected via Wi-Fi AP have the ability to handover across Access Points, and across different subscribers. In spite of the developed system adaption capabilities to PTP or PMP mode of operation, in DAIDALOS II scenario, only PTP was considered.

The RAL_WiMAX (Radio Access Layer WiMAX) and the Driver_WiMAX (Driver WiMAX) are the components that deal with the specificities of the IEEE 802.16 technology. These two modules are able to control the behaviour of 802.16 network entities, namely the BS and SS and are located in the AR.

Figure 52 shows the resource management architecture in both BS and SS. The implementation work has been developed with a 802.16-2004 compliant equipment, supplied by Redline Communications [REDCOM], using the SNMP protocol. The Redline BS SNMP agent implements the IEEE 802.16f [802.16f], an amendment to IEEE 802.16-2004 that defines a Management Information Base (MIB) for the MAC and PHY layers. Due to equipment vendor restrictions, the entities that manage and control the 802.16 technology, RAL_WiMAX and Driver_WiMAX, are located in the AR.

As can be observed from the figure, the Driver_WiMAX is an integral part of RAL_WiMAX. Therefore, henceforth, we will refer to the RAL_WiMAX as a whole that necessarily includes the Driver_WiMAX. In a broad sense, the main functionalities of RAL_WiMAX are: QoS Management, Admission Control, IEEE 802.16 Network Discovery and IPv6 Traffic Classification to/from nodes interconnected via 802.16 backhaul.

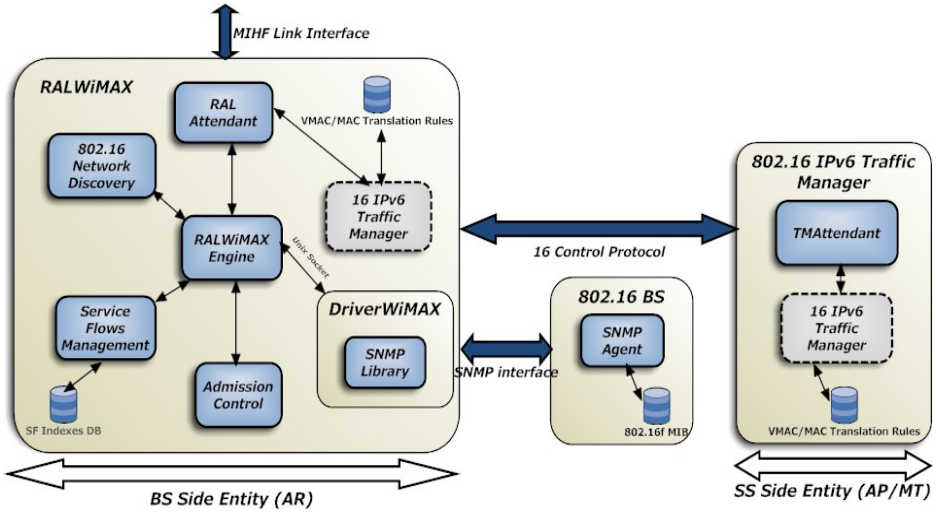

Figure 52: WiMAX Resource Management Architecture

QoS management consists on the aptitude to enforce the received QoS requests in the Redline WiMAX equipment via SNMP, and to collect information from the 802.16 network such as RF, Physical and MAC parameters, including downlink and uplink available bandwidth, to better manage the 802.16 link.

The QoS Management features are very similar to the ones developed under WEIRD scope. But now, in spite of the distributed WiMAX management system, across RSA and RC, this functionality is centred on the RALWiMAX component.

The Admission Control allows the effective control of the 802.16 link resources, either providing a fast answer upon upper modules in case of unavailable resources, accelerating eventual handover decisions, or allowing better and fairly distribution of resources by flows with higher priorities; it is integrated with the QoS Management feature.

The 802.16 Network Discovery (16ND) detects new SSs and BSs that join the WiMAX network, building the complete network topology of the WiMAX segment in a dynamic way, and supplying at the same time relevant information during bootstrap, such as available downlink/uplink bandwidth on the BS sector controller and on the surrounding SSs. This WiMAX network discovery feature is implemented over the SNMP traps support of the Redline Communications WiMAX equipment and is also very close to the depicted functionalities developed for RSA in section 5.1.2.1. The only difference is that now the data is only saved in RALWiMAX and not in forward to the upper module.

The 802.16 IPv6 Traffic Manager (16TM) is the entity responsible for the IPv6 traffic classification in the 802.16 segment. It associates the packets with allocated Service Flows and offer per-flow handling of IPv6 packets in the WiMAX links; it also operates in the control plane, exchanging 16 Control Protocol (16CP) messages. The need for IPv6 Traffic Manager comes from the lack of Convergence Sublayers (CS) bear by the Redline WiMAX equipment, which only supports 802.3 Ethernet and IPV4 Convergence Sublayers. Two instances of this module are deployed, one in the AR and another simple module in the AP, although in this

last case, the module is completely independent from the rest of the architecture of the AP. Per-flow handling in the access segment enhances the experienced quality, since a given session is granted resources independent of other sessions. The efficiency of the implemented solution is assured by a lookup-table and an efficient hash function implementation for computing the IPv6 five tuple key.

It must be noted that the separation of RAL_WiMAX general functionalities from the more specific ones, such as the WiMAX equipment interface implementation (accomplished by Driver_WiMAX), allows to seamlessly integrate other vendor equipments that do not necessarily implement the 802.16f MIB. On the other hand, since the Driver_WiMAX enforces QoS requests from the upper layer modules in the 802.16 network, respecting completely the 802.16f standard, this solution may be used with other vendor equipments without any modifications in the implementation.

The architecture also contains the RALAttendant that interfaces with the MIHF, through a LinkSAP, the TrapHandler via Unix Socket, and the AP 802.16 IPv6 Traffic Manager, by means of a connectionless IPv6 socket. It also interfaces with all IPv6 packets that traverse the AR, by means of ebtables netlink sockets implementation. The RALEngine concentrates the main intelligence of the application, implementing important methods to efficiently handle requests. The processing work includes the conversion of the MIHF messages into SNMP messages (GET, SET) and vice-versa, and the conversion of trap messages for topology information. The SnmpLibrary defines the low level primitives that interact with the BS, using the SNMP protocol. The NET SNMP API was used in order to implement the methods that interact with the 802.16 equipment through the SNMP Protocol. Finally, the IPv6 Traffic Manager performs the IPv6 traffic classification and differentiation in the WiMAX link (its purpose will be detailed in the next section).

6.1.4 RAL_WiMAX operation details

Due to the lack of existent Convergence Sublayers in the Redline equipment, we decided to use the 802.3 Ethernet convergence sublayer to classify the traffic from the BS to the SS and vice-versa, fundamentally because 802.3 CS is independent of the IP protocol that is running above, which allows a certain grade of flexibility. However, considering this solution as it is, we are not able to differentiate the traffic that is running on the same MT: if the same terminal is running for instance, two distinct services, with different QoS requirements, we are not able to differentiate them in the WiMAX link. In order to allow per-flow basis differentiation in the WiMAX link, we developed the IPv6 Traffic Manager module, previously referenced. The classification of the packets is based on the IPv6 five tuple (IPv6 Source/Destination Address, Protocol, Source Port/Destination Port). A different Virtual MAC is generated to each service flow request and is associated with the real MAC and the classification parameters, composing a so-called translation rule. This process was already proposed and used in [Neves-ISCC2006] and uses the same concepts and protocol: 16 Control protocol, for the

setup of the default and new service flows, as well as for the translation between real and virtual MACs. Figure 53 depicts the data plane operation of the RAL_WiMAX, which is tightly related with the control plane.

When the system is initialized, a default downlink and uplink channel is allocated in the WiMAX segment for signalling purposes and to assist and avoid packet losses and delays when dynamically creating/modifying Service Flows as will we forward confirm when discussing data plane results. It must be noted that this is a channel of very good quality, which all traffic, without classifier rules entries, may exploit. The referred initialization and setup procedure is named bootstrap.

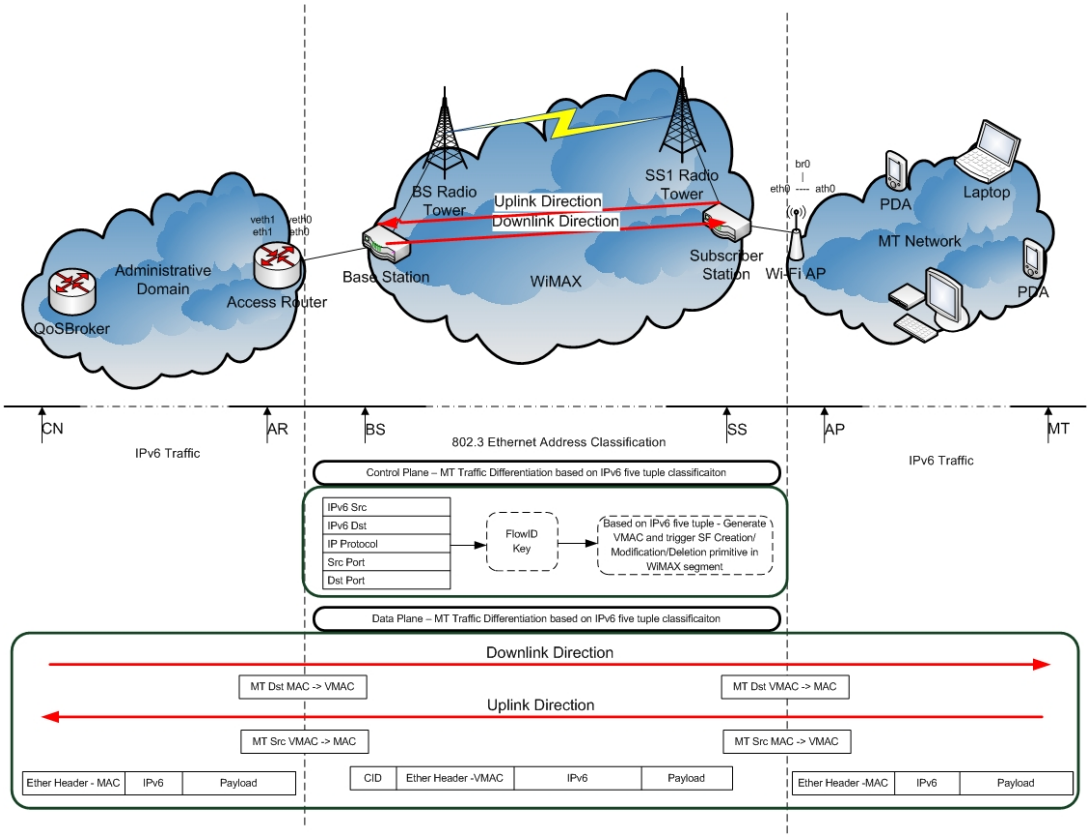

***Figure 53: RALWiMAX* Control and Data Plane interworking**

For sending QoS requests, the L2QoSC sends a command to MIHF, MIH_Handover_Prepare which is translated to the respective technology, in our case, an MIH_Link_ActivateRequest that is sent to the RAL_WiMAX. It must be noted, as already mentioned, that these primitives are QoS extensions to IEEE 802.21. Upon the reception of this message, assuming that it is admitted by the Admission Control module, the RAL_WiMAX will generate a Virtual MAC, and perform the eventual Service Flow reservations. While performing the reservation, a translation rule, with the MAC/VMAC association, and the classification parameters (IPv6 five tuple), is installed in the AR and a Classifier_v6_Rule_Installation_Request is sent to the AP, that will install the same translation rule, and answer to the AR, signalling the correct operation accomplishment.

In the data plane, all the IPv6 traffic is captured by ebtables tool and processed by the 16 IPv6 Traffic Manager. It looks at the IPv6 five tuple, performs a hash, and tries to find the installation rule in the lookup table.

If a Classification rule is found, occurs a MAC translation accordingly, a VMAC to MAC or vice-versa, to allow the packets to reach its source or destination in the layer 2 (L2) cloud. The packets are re-injected by means of a Packet Socket RAW.

6.2 Results and Performance tests in DAIDALOS

We tested the proposed L2 QoS architecture, comprising L2QoSC, MIHF and RAL_WiMAX, focusing, obviously, on the RAL_WiMAX and the WiMAX segment results. The testbed used is illustrated in Figure 54: it comprises a Redline REDMAX fixed WiMAX BS, two SSs (SS1 and SS2), creating a point-to-multipoint topology, and three PC's. The AR is attached to the BS and has been installed with the L2 QoS modules (L2QoSC, MIHF and RAL_WiMAX). The WiMAX configuration parameters are listed in next table.

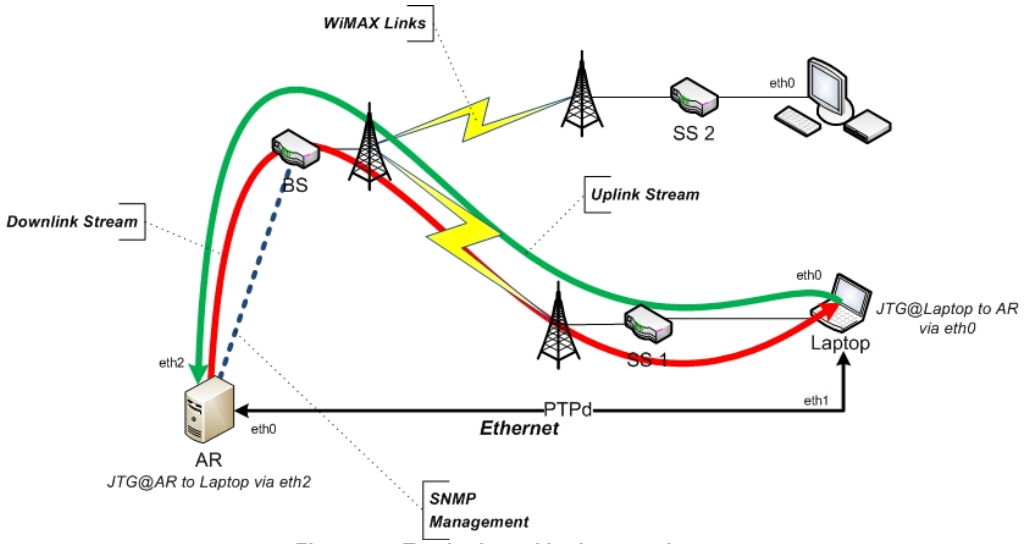

Figure 54: Testbed used in the experiments

Frequency band	***3.5GHz***
Channel Bandwidth	***7 MHz***
BS and SS Tx power	***1.0 dBM***
SS1 Uplink/Downlink modulation :: Distance	***64 QAM (3/4) :: 20m***
SS2 Uplink Downlink modulation :: Distance	***64 QAM (3/4) :: 20m***

Table 17 : Testbed Configuration parameters

It must be noted that the illustrated testbed does not comprise WiFi, since in this first round of tests the intention was to measure only the impact that WiMAX system might have in the whole architecture.

The RAL_WiMAX functionalities have been tested with varied parameters in order to validate the implemented work. The performance tests were accomplished for two distinct modes of

operation, the point-to-multipoint when examining the control/management plane and point-to-point when performing data plane tests with dynamic QoS management.

6.2.1 Signalling Performance in WiMAX System

Figure 55 depicts the Layer 2 QoS architecture that supports the following experiments. A python script was used to trigger the QoS requests in L2QoSC. The QoS requests sent by L2QoSC are translated by MIHF to the RAL_WiMAX, which will in turn process the correspondent commands and interface with the WiMAX equipment through the SNMP interface implemented in Driver_WiMAX.

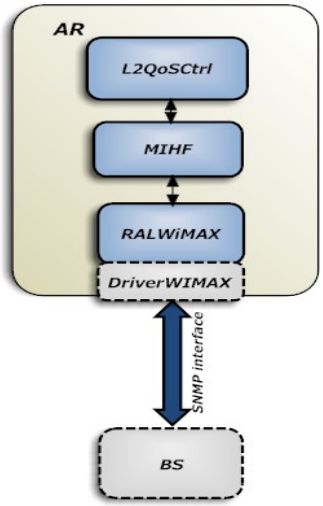

Figure 55: Layer 2 QoS architecture

The QoS requests triggered by the L2QoSC may pack a variable number of Service Flow (SF) requests, ranging from 1 to 16. These QoS requests may be translated in MIH_Link_ActivateRequests (MIH_AR) or MIH_Link_DeactivateRequests (MIH_DR) primitives. The RAL_WiMAX is the one responsible to unpack the messages and perform the eventual SF reservations accordingly to the SF requests of MIH_AR. Moreover, RAL_WiMAX needs to determine whether the primitive MIH_AR corresponds to a request for a new reservation or to a modification.

The following results were obtained for a 512K bandwidth allocation request, in case of SF reservations. For SF modifications, it was varied the allocated bandwidth from 512K to 1024K. Half of the samples were accomplished in the downlink direction and the other half in the uplink direction. These performance tests comprise the point-to-multipoint mode of operation, thus performing SF reservations/modifications/deletions on both SSs.

Figure 56 presents the results of L2 QoS reservations, modifications and deletions with 16 SF requests, but varying the number of SFs packed in each L2 QoS primitive (MIH_AR or MIH_DR), and consequently, varying the number of L2 QoS requests for the 16 SF requests. For the simplification sake, the MIHF is not presented.

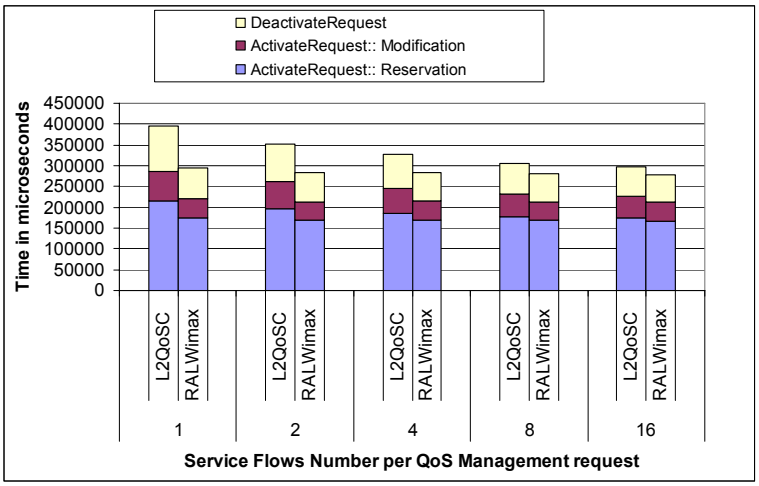

Figure 56: Time spent to perform 16 SF reservations in the WiMAX system while varying SFs aggregation per QoS Management Primitive

For each action, the yy axis represents the cumulative average time (in microseconds) to enforce a specific action on the WiMAX system. The xx axis represents the number of SFs aggregated in each QoS Management primitive (1, 2, 4, 8, 16) that have been used for each test.

Comparing the results, we experience considerable gains in terms of performance when aggregating various SFs in the same L2 QoS request, as was expected. In fact, the messages overhead between modules, are slightly reduced when aggregating diverse SFs Requests, which decisively contributes to the mentioned gains. Moreover, the obtained results show that the needed time to establish a QoS reservation is the most time consuming operation, more than 50% of the total time. Moreover, the RAL_WiMAX is the most time consuming module, mainly because it includes the negotiation of the QoS parameters between the BS and the SS through the usage of Dynamic Service Addition/Change/Deletion, as defined in the IEEE 802.16-2004 standard. The time spent by the remaining modules is due to the message flow and internal processing.

The next test intends to verify how RALWiMAX deals with a considerable amount of sequential QoS management requests. Each QoS management primitive packs two SF requests. We show the total time spent from the reception of a request (MIH_AR::Reservation/Modification/MIH_DR) to the correspondent answer is sent back to the MIHF, being represented by the Total Path illustrated in Figure 57.

The lines represent the average time spent to create/modify/delete the two SFs, carried by MIH_Link_ActivateRequest/MIH_Link_DeactivateRequest commands.

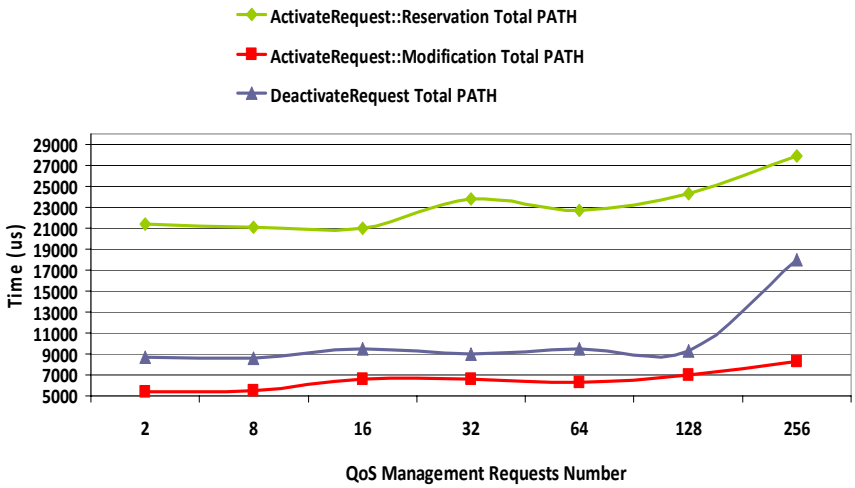

Figure 57: RALWiMAX QoS Management Primitives Total Path

The results show that there is a slight increase of time when the number of SFs increases. However, these values are kept stable, showing that the architecture is prepared to deal efficiently with a large number of sequential requests. The observed differences between SF reservation/modification/deletion are due to the distinct amount of SNMP MIB tables that must be set and to the higher amount of operations the equipment needs to perform during reservations, when compared with the modifications or deletions.

The following whisker-box-plot in Figure 58 shows the time taken to set each SNMP MIB table while performing a reservation/modification/deletion.

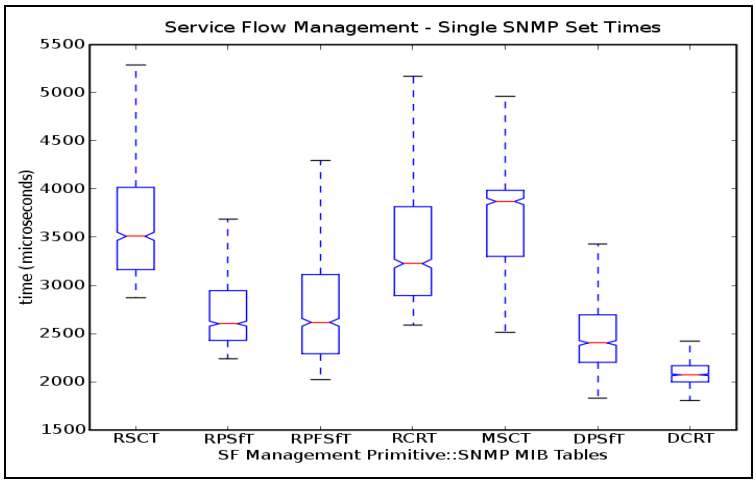

Figure 58: Single SNMP Table Set Times

When performing a reservation, it is necessary to set 4 SNMP tables. The names of the SNMP MIB tables are abbreviated in the graphic and are described in Table 18. Furthermore they are preceded by an “R” in case of a reservation, an “M” for the modification and a “D” for deletion.

SF Request: MIB Tables	Functionality
(SCT) ServiceClassTable	Contains the SF QoS parameters
(PSfT) ProvisionedSfTable	Contains the SF profiles provisioned by NMS
(PFSfT) ProvisionedForSFTable	Maps the MAC addresses of SSs to the provisioned SFs
(CRT) ClassifierRuleTable	Contains packet classifier rules associated with SFs

Table 18: SNMP MIB Tables for QoS Management in 802.16-2004

The box in each figure contains the middle 50% of the measured values. The line in the middle represents the median, the top and the bottom of the box correspond to Q3 and Q1, respectively. Values outliers are not presented in this graph. These results clarify the differences observed in Figure 57. In fact, when performing a reservation in the WiMAX system we need to set 4 MIB tables, while the modification process only requires a set to 1 SNMP MIB table, and the deletion procedure requires 2 MIB Table sets.

Finally, we performed a set of sequential requests triggered by the L2QoSC, varying the class of service parameter (Figure 59). Each QoS management request groups two SF requests, one for uplink direction and another for downlink.

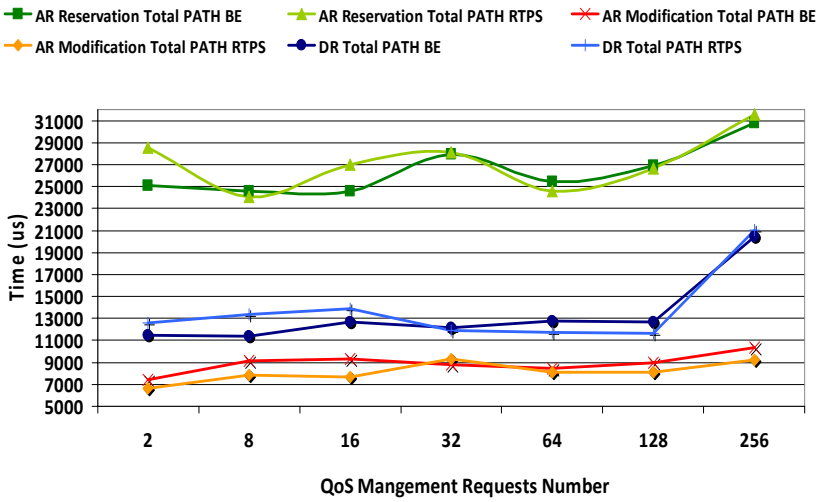

Figure 59: L2QoSCtrl QoS Management Performance

The results show that the QoS Management requests are not class of service dependent. The observed differences are very small. These results also match the ones of Figure 57, in the sense that, as we increase the number of QoS requests, the average time taken to perform each request slightly increases, especially when performing 256 QoS management requests. Anyway, the timing values are small (on the order of 10 to 30 msec) and do not compromise the real-time requirements.

6.2.2 Data and performance results in WiMAX network

The data plane results presented in this section measure the capacity of the architecture to handle a variable number of unicast point-to-point video streams while performing dynamic

resource allocation and reallocation (control plane) isolating the WiMAX network. They are meant to illustrate the behaviour of real-time IP applications running over WiMAX with the proposed QoS architecture. In the case, IPTV A/V streams were used.

Streaming Video traffic is typically characterized by low tolerance delay and packet loss. For video streaming, the following QoS criteria was used for proposal evaluation: packet loss ratio lower than 5%, and one way delay average in WiMAX segment lower than 30 ms.

The IPTV traffic is based on real traffic: we used the Jugi's Traffic Generator, a Linux traffic generator that allows to emulate IPTV A/V streams based on existing packet traces. The packet traces replicate a real IPTV stream. The video stream was captured in H.264/AVC format and the accompanying audio stream was encoded in MPEG-1 Audio Layer 2. The video was streamed at 512 kbps (VBR) and the audio at 192 kbps (CBR). The executed runs last for 60 seconds, and 7 distinct packet traces were used to replicate the real stream, starting from random points. The audio application throughput remains very close to 178 kbps and the video throughput ranges between 490 kbps and 512 kbps, mainly due to the random starting points in the video. These values must be taken into account when analyzing the results. The Precision Time Protocol daemon (PTPd) was used to synchronize clocks of the senders and receivers, allowing the time inference with significant accuracy (the clocks drift was fluctuating between 10 and 100 microseconds).

The performed tests consider that, at a specific time (usually around 10 seconds after the beginning of the video stream), during the IPTV stream execution, the L2QoSC triggers a QoS reservation/modification/deletion. Each QoS management request groups two SF requests, one for the downlink direction and another for the uplink. The scheduling type was varied, nevertheless, due to equipment restrictions, only best effort (BE) and real-time polling service (RTPS) were exploited.

Table 19 presents the performed tests. The values presented in the following box plots, correspond to average values of delay, jitter and losses, calculated by means of jtg_calc [JTG]. For each test, at least five executions have been accomplished.

One Downlink Stream from AR to Laptop	
Test 1	***Static SFs Reservation : 1024 kbps***
Test 2	***Dynamic Modification of SFs : 1024 kbps → 2048 kbps***
Test 3	***Dynamic Allocation of SFs after deletion : 1024 kbps → 0 kbps → 1024 kbps***
Several Uplink/Downlink streams competing for the WiMAX Resources	
Test 4	***Dynamic modification of SFs (2048--> 4096)***

Table 19: Executed experiments legend

Figure 60 illustrates the one way delay measured at the SS1, for tests 1, 2 and 3. This figure is divided in two subplots, one showing the performance results while using RTPS scheduling service, and other one when BE scheduling service is applied.

As may be observed, no substantial differences between the two scheduling services jump in sight. This is mainly because the background traffic was not sufficiently heavy. Moreover, results show how the average delay varies on tests 1, 2 and 3. Test 1 refers to static pre-provisioned allocations, while test 2 refers to a session re-adaptation, finally, test 3 exploits the behaviour expected in a worst case situation, when a running session does not have, at a certain moment, any SF allocated in the WiMAX channel.

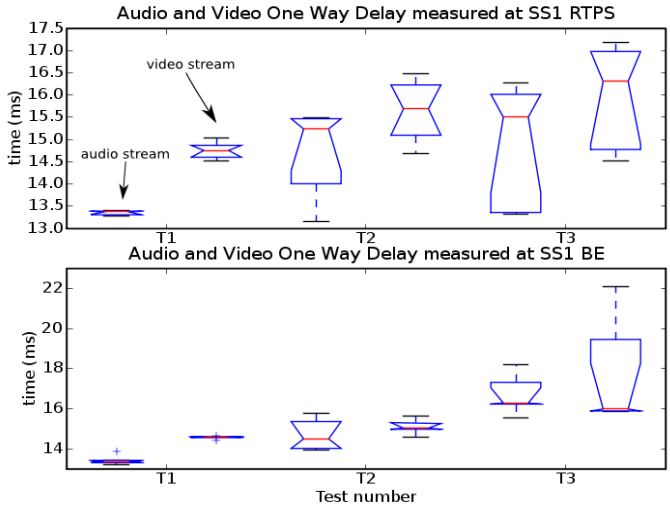

Figure 60: (a)Audio and Video One Way Delay RTPS; (b) Same for BE

As may be observed in terms of delay, even when performing dynamic QoS Management, the IPTV A/V stream maintains very acceptable values, under the previous defined QoS criterion. The same happens in terms of packet loss as can be observed in Figure 61. All the samples, in the worst case situation cause less than 2.5% of packet loss.

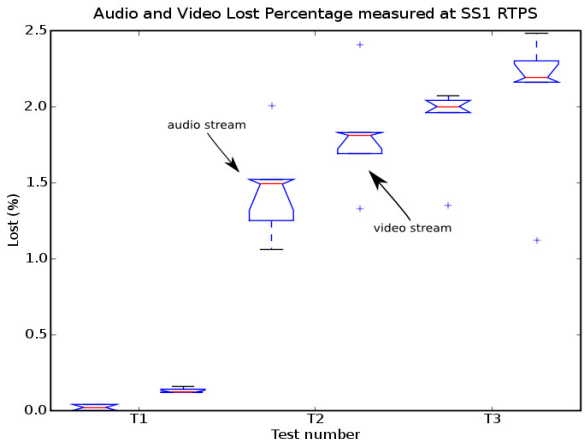

Figure 61: Audio and Video Lost Percentage RTPS

As expected the loss rate increases slightly when dynamically performing allocations and reallocations. Even though, the application loss rate is kept under acceptable values.

Figure 62 represents a sample of the several executed runs, showing how the audio one-way-delay, jitter and the lost packets percentage vary during an IPTV stream emulation. This is an example of the samples that have been collected to plot the whisker boxes. In this case it presents the audio behaviour along the experimental time. Test 1 is the reference. No packet loss is observed and the delay and jitter remain stable until the end of the execution.

When performing a SF modification (Test 2) or SF deletion followed by a SF reservation (Test 3), the delay increases, reaching the value of 28 ms in the first case and 48 ms in the second one, but this happens only momentarily. It is also noted that, when performing Test 3, the delay requires more time to stabilize than in Test 2. The jitter, strictly correlated with the delay, has the same behaviour, showing some peaks when performing the dynamic QoS Management. During the transition periods, it is experienced a considerable packet loss, since the queue is not capable of saving all the packets on it, during the transition phase. On the other hand, the transition periods are relatively small and acceptable, especially in the case of SF modifications (around 1 sec in Test 2 and 2 secs in Test 3).

It should be observed also that each QoS request packs two SF requests, either modifications or deletions/creations, which may also contribute to a large transition period.

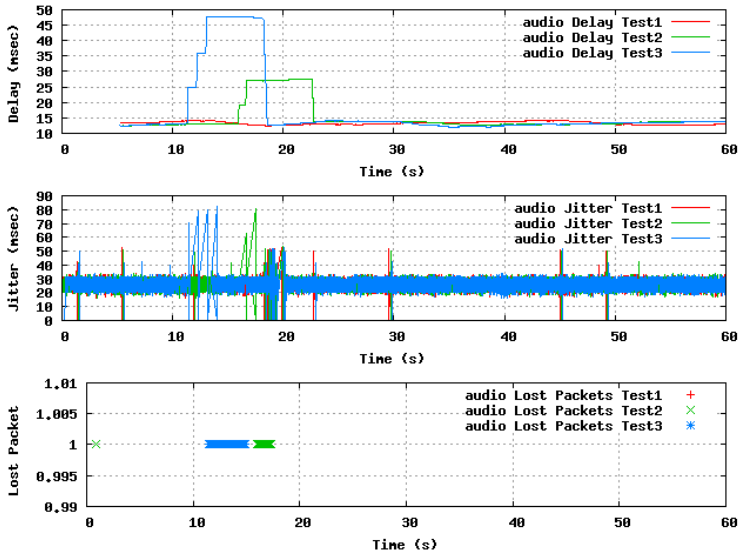

Figure 62: Audio delay during the tests experiments

The graphic below, Figure 63, illustrates Test 4 results, showing that the architecture is able to handle several IPTV streams in the same channel, while executing dynamically SF reservations/modifications/deletions. As presented, the delays stay under the QoS criterion proposal. However when generating 5 simultaneous streams in the uplink and in the downlink direction (10 in total), more than 5 % of packet loss is achieved. This is as expected, considering the traffic overload introduced in the network.

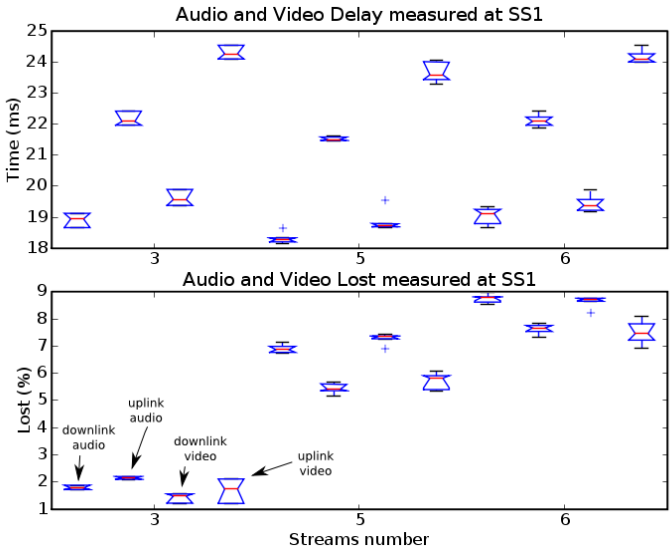

Figure 63: Multiple Uplink/Downlink Streams competing for WiMAX resources

Finally, to end this section, a test was accomplished considering heavy load background traffic. In this case, 200 VoIP streams, with 64 kbps were used. The scheduling type associated with the allocated channel for IPTV A/V traffic was varied. The results are presented in the next figure.

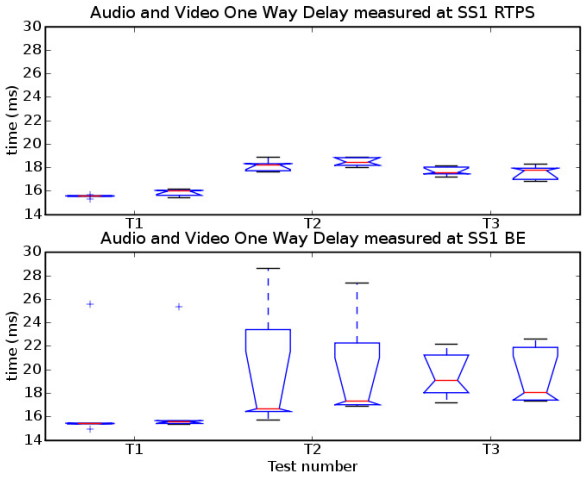

Figure 64: One-Way-Delay measure at MT, under heavy traffic conditions

As can be seen the average one-way-delay even under heavy load conditions and using BE classifier is under the 30 ms. Logically the RTPS has a better behaviour when compared to the BE scheduler. In spite of the stable performance when using RTPS as scheduling type, the difference is not very high. This test shows that the WiMAX system deals under heavy loads of traffic, not compromising the Quality of Experience to the end-user.

6.2.3 Data performance in concatenated WiMAX/WLAN networks

The results gathered on this section complement the ones retrieved on the previous one. This gives a more realistic view of the results, illustrating also the impact that the WLAN network may have in terms of Quality of Service level in the end-to-end QoS path.

The testbed used is illustrated in Figure 65: it comprises a Redline REDMAX fixed WiMAX BS, and one SS (SS1) concatenated with a WiFi AP. The MT is associated with the AP via ath0 interface. The AR is attached to the BS and has been also installed with L2QoSC, MIHF and RAL_WiMAX. The WiMAX and WiFi AP configuration parameters are listed in Table 20.

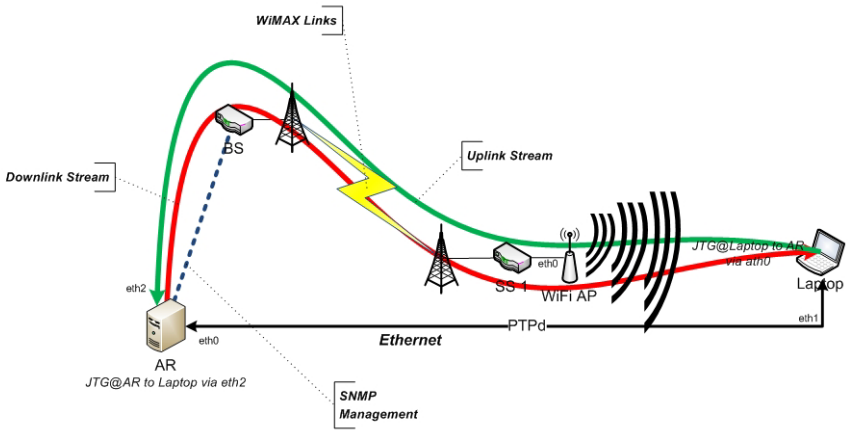

Figure 65: Testbed used in WiMAX/WiFi tests

Frequency band	***3.5GHz***
Channel Bandwidth	***3.5 MHz***
BS and SS Tx power	***1.0 dBM***
SS1 Uplink/Downlink modulation :: Distance	***64 QAM (3/4) :: 20m***
SS2 Uplink Downlink modulation :: Distance	***64 QAM (3/4) :: 20m***
Distance between AP and MT	***2m***

Table 20: Testbed configuration in WiMAX/WiFi testbed

Figure 66 shows the audio (left boxplot of each test) and video (right boxplot of each test) one way delay measured at the MT in the WiMAX/WiFi scenario, exemplifying how system behaves with or without the default service flow.

Surprisingly the one-way-delay, when considering concatenated WiMAX/WiFi networks is slightly smaller comparing to results shown on Figure 60. Even though, it must be noted that due to laboratory restrictions, the MT was considerably near WiFi AP, thus not penalizing significantly the total one-way-delay. Furthermore, the outdoor environment conditions, may justify this little difference in the one-way-delay.

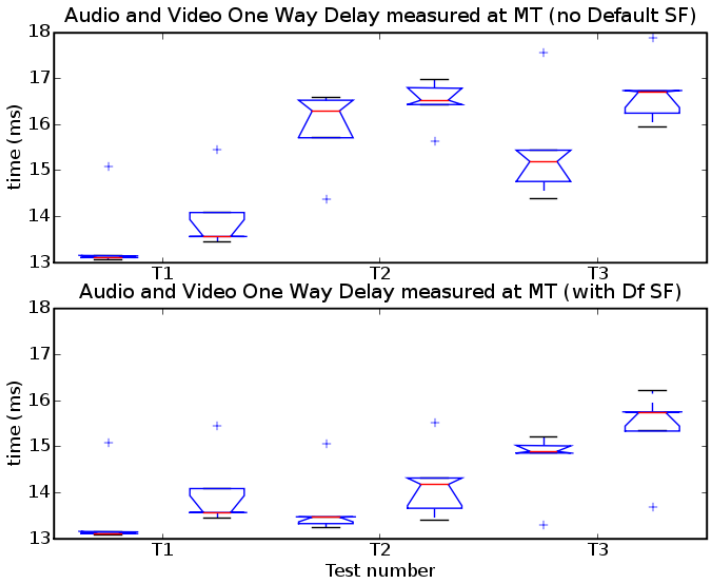

Figure 66: One-Way-Delay measure at MT

The figure is divided in two subplots, the first one showing the performance results when no default SF is allocated and the other one considering the existence of a Default SF, to assure an excellent system behaviour when accomplishing QoS sessions creation and re-adaptation. As may be observed, no substantial differences exist between the two subplots, but the existence of a default SF contributes to soften the transitions and reduce a little one-way-delay when performing QoS management operations.

The average jitter executions distribution is also very similar when considering or not the Default Service Flow. Nonetheless the values distribution interval is very tight which is exactly what is desired when using real-time applications, which have very strict jitter requirements.

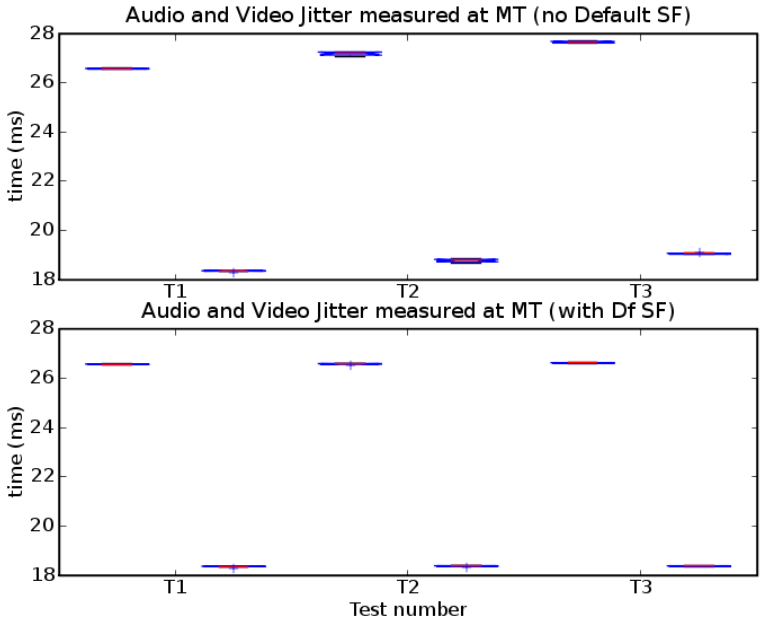

Figure 67: Jitter measured at MT

The lost percentage is the measured parameter that most improves, when considering the Default Service in the WiMAX system. The lost packet rate is almost around zero % even in the Worst Case, that is, Test 3. Thus in this situation the DF SF really softens the impact induced by QoS Management operations over the network.

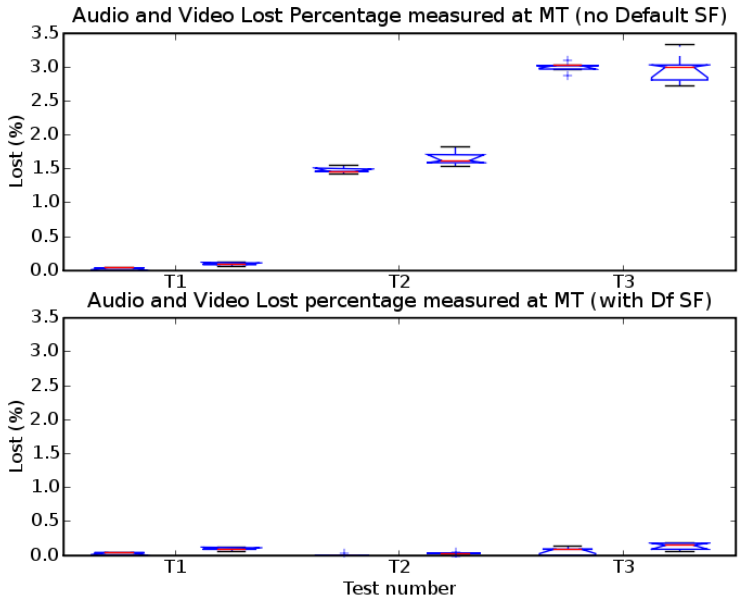

Figure 68: Lost percentage measured the MT

The following two figures represent a sample of the several executed runs, showing how audio one-way-delay, jitter and lost packets vary during an IPTV stream emulation, respectively, when no Default Service Flow is used, and when a DF SF is previously allocated. The audio behaviour along the experimental streaming period is considerably more unstable when no DF SF is used. When using a DF SF (Figure 69) the lost packets are almost inexistent, the jitter variation has only some peaks, not strictly related to dynamic QoS management operations, and the delay variation is also softened with a very small transition (period between peaks and the typical behaviour).

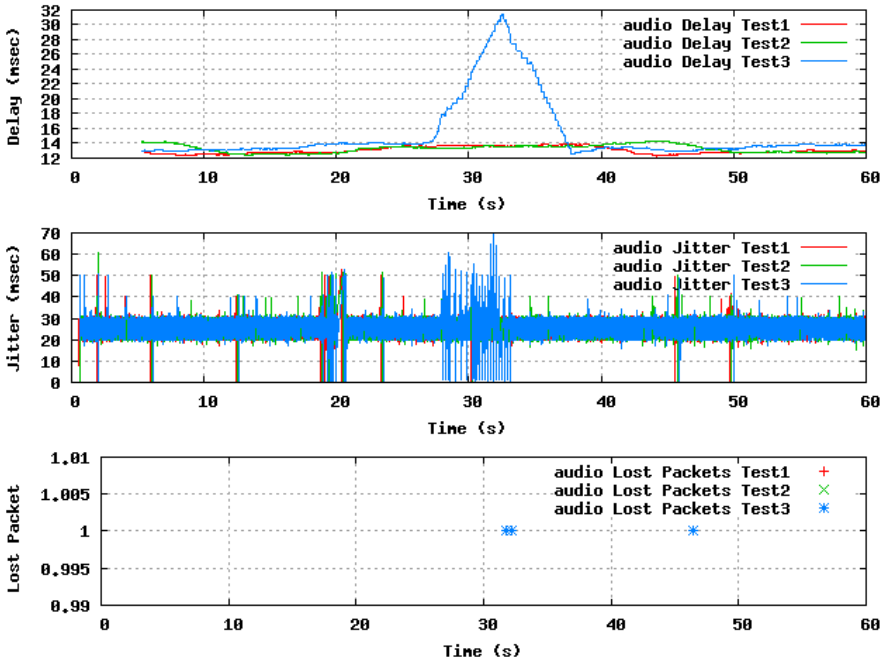

Figure 69: Audio behaviour during streaming period of 60 seconds using a DF SF

It was also noticed that jitter and delay variation, degrade noticeably when using the WiFi network connected the WiMAX backhaul (Figure 70) when comparing to the results achieve when only using WiMAX. This is mainly justified by the fact that 802.11 network was not using any QoS mechanisms, thus not offering any type of Quality of Experience to the end user applications.

In fact, as it was seen before, when only using the WiMAX system, the delay and jitter variations were less accentuated.

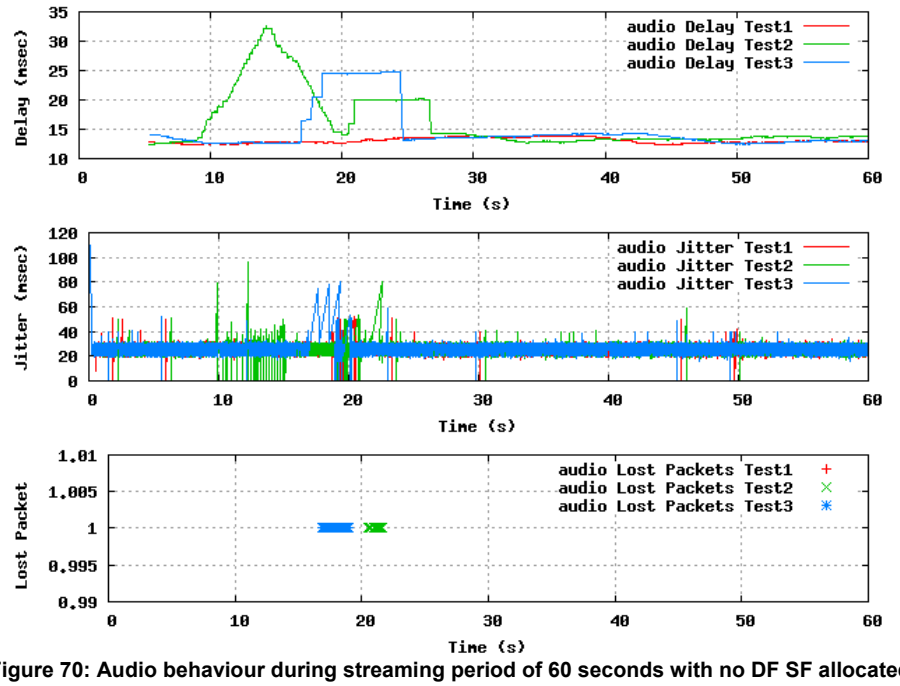

Figure 70: Audio behaviour during streaming period of 60 seconds with no DF SF allocated

Finally, to finish the results analysis, the Video and Audio jitter distribution was plotted (Figure 71), when using the DF SF, and also with no DF SF allocated. As it is well known, an IPTV stream has low tolerance of delay and packet loss, but it also has tight jitter requirements. The following plots show that when using the DF SF, the jitter fluctuation is almost imperceptible, over Test 1, 2 and 3. When no DF SF is used, the dynamic QoS Management operations (Test 2 and 3) create some jitter fluctuation.

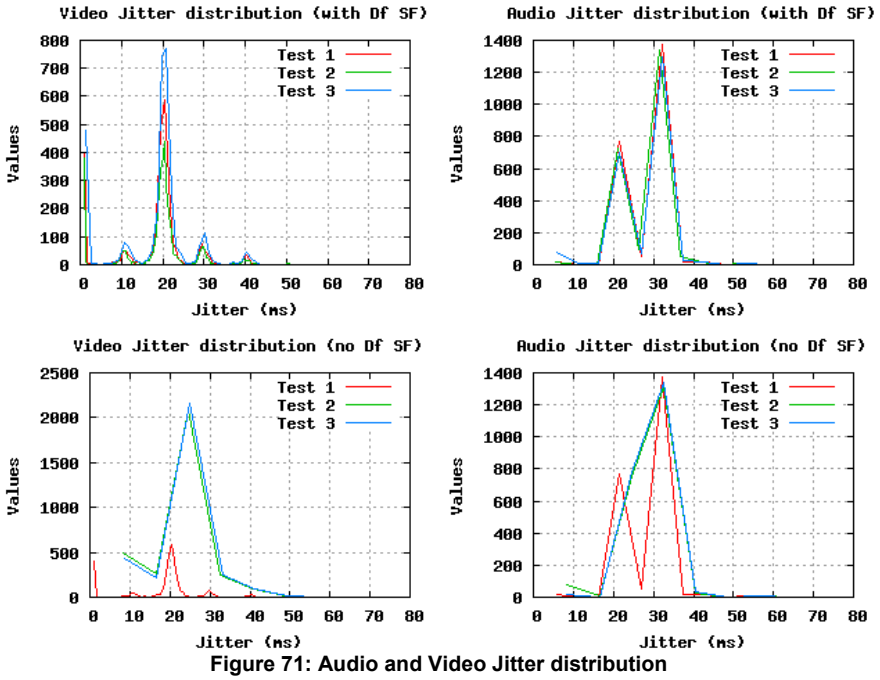

Figure 71: Audio and Video Jitter distribution

6.3 Conclusions

This chapter described the developed work under DAIDALOS scope, addressing the real-time and dynamic support of QoS in the IEEE 802.16 technology, presenting an architecture that seamless integrates QoS and mobility, enabling the support of 802.16 in heterogeneous networks.

A new solution for the dynamic resource control in 802.16 environments, motivating the use of the IEEE 802.16f MIB standard, and integrating the WiMAX Resource Management System with an implementation of the IEEE 802.21 MIHF is proposed.

The designed and implemented WiMAX Resource Management System automates service flow and resources management in the WiMAX network.

This architecture was implemented and integrated in a real testbed. The obtained results of the tests show that, with respect to the signalling performance, the processing times for the QoS reservations, modifications and deletions are significantly small; with respect to the data plane, results showed that real-time applications are not significantly affected while

dynamically managing the WiMAX system, enabling the use of the WiMAX systems under dynamic, demanding, heterogeneous network environments.

7 Chapter 7: Conclusion

This chapter states the final conclusions relating all the work carried out throughout this thesis. It also addresses future work related with the themes this thesis is centred on.

7.1 Final Conclusion

This Thesis addressed the IEEE 802.16 technology with emphasis in the Quality of Service and Mobility support. Some of the key aspects of next generation networks were depicted in the WEIRD and DAIDALOS II projects and have been matter of concern all along the project.
This Thesis developed, implemented and evaluated part of a network architecture with E2E Quality of Service and mobility support, in both European projects. Two Resource Control applications were implemented with the purpose of dealing with WiMAX specificities while respecting the defined network architectures of both projects.
The Adapter Application in WEIRD was enhanced with topology and resources management primitives. This part of the implementation was the materialization of the study that was done on the QoS mechanisms. Ways of overcome the limitation to implement functionalities without the SNMP protocol, using other viable interfaces were also depicted. Moreover, it was demonstrated the correct functionality and flexibility of the WiMAX Resource Control.
In DAIDALOS case, it was proposed a novel solution for the dynamic resource control in 802.16 environments, motivating the use of the IEEE 802.16f MIB standard, and integrating the WiMAX Resource Management System with an implementation of the IEEE 802.21 MIHF for media independent mobility. The designed and implemented WiMAX Resource Management System automates service flow and resources management in the WiMAX network.
These architectures were implemented and integrated in a real testbed. The obtained results of the tests show that, with respect to the signalling performance, the processing times for the QoS reservations, modifications and deletions are significantly small; with respect to the data plane, real tests were effectuated emulating IPTV A/V streams. The results showed that real-time applications are not significantly affected while dynamically managing the WiMAX system.
The experiments accomplished along the thesis confirm expectations relating the 802.16 technology in terms of performance (allowing high quality audio and video communications, tele-medicine) and a variety of usage scenarios.
The combination of these capabilities makes WiMAX attractive for a wide diversity of people: fixed operators, mobile operators and wireless ISPs (Internet Service Provider), but also for many vertical markets and local authorities.

7.2 Future Work

As a future work, it is aimed the integration of IEEE 802.16-2005, mobile WiMAX, in the same DAIDALOS II architecture.

In which concerns the WEIRD's Adapter, it can be updated and be slightly improved considering the still more demanding requirements of the 802.16e standard [802.16-2005].

The WIMAX mesh theme is also intended to be exploited soon.

8 References

[802.21] IEEE P802.21/D01.09 Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services

[802.16-2004] IEEE 802.16 Working Group, *IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE Std. 802.16-2004, October 2004

[802.16-2005] IEEE 802.16 WG, *IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. Amendment 2: Physical and Medium Access Control Layer for Combined Fixed and Mobile Operation in Licensed Bands*, IEEE Std. 802.16e, December 2005.

[802.16f] IEEE 802.16 Working Group, IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 1: Management Information Base, IEEE Std. 802.16f-2005, December 2005

[WimaxStg2] WiMAX Forum, WiMAX End-to-End Network Systems Architecture Stage 2: Architecture Tenets, Reference Model and Reference Points, Release 1.1.0, June 2007.

[802.16g] IEEE 802.16g-07, December 2007, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access SystemsAmendment to IEEE Standard for Local and Metropolitan Area Networks - Management Plane Procedures and Services

[WEIRDD2.3] WEIRD Deliverable D2.3, System Specification, April 2007

[802.11e] IEEE 802.11e Standard, November 2005

[802.16-WG] IEEE 802.16 Working Group (WG), URL: *http://www.ieee802.16.org/16*

[D2GlobalArch] DAIDALOS II Deliverable DII – 121, “Daidalos II Global Architecture including scope of five key concepts”, January 2007

[D2_E2E_QoS] Miguel Almeida et al., *An End-to-End QoS framework for 4G mobile heterogeneous networks*, QoSWinet, 2007.

[DSLForum] DSL Forum, URL: *http://www.dslforum.org*

[IEEE] Institute of Electrical and Electronics Engineers (IEEE).URL: *http://www.ieee.org*

[ITU-T] International Telecommunication Union - Telecommunication *Standardization* Sector.

URL: *http://www.itu.int/ITU-T/index.phtml*

[REDCOM] Redline Communications. URL:*http://www.redlinecommunications.com*

[WiMAX] WiMAX Forum. URL: *http://www.wimaxforum.org*

[Wi-Fi] Wi-Fi Forum. URL: *http://www.wi-fi.org*

[RFC1157] Case, J., M. Fedor, M. Schoffstall and J. Davin, "The Simple Network Management Protocol", RFC 1157, May 1990.

[RFC2578] K. McCloghrie, D. Perkins, J. Schoenwaelder, *Structure of*

Management Information version 2, IETF RFC 2578, April 1999

[RFC1633] Braden, R., D. Clark, S. Shenker, “Integrated Services in the Internet Architecture: an Overview”, RFC 1633, June 1994.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC1213] K.McClghrie, M.Rose, “MIB-II: Management Information Base for network management of TCP/IP based Internets”, RFC 1213, March 1991

[RFC1443] J.Case, K.McCloghrie, M.Rose, “Textual Conventions for SNMPv2”, April 1993

[RFC3418] R. Presuhn, J.Case, K.McCloghrie, M.Rose “MIB for the SNMP”, December 2002

[RFC2205] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, “Resource Reservation Protocol”, RFC 2205, September 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2461] Narten, T., E. Nordmark, W. Simpson, “Neighbour Discovery for IP Version 6”, RFC 2461, December 1998.

[RFC2474] K. Nichols, S. Blake, F. Baker, D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” RFC 2474, December 1998.

[RFC2475] Blake, S., D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, “Architecture for Differentiated Services”, RFC 2475, December 1998.

[RFC3261] J. Rosenberg et al., “SIP: Session Initiation Protocol”, RFC 3261, June 2002.

[RFC3264] J. Rosenberg, H. Schulzrinne, “An Offer/Answer Model with Session Description Protocol (SDP)”, RFC 3264, June 2002.

[RFC3315] R. Droms, Ed., J. Bound, et. Al., Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, July 2003.

[RFC3775] Johnson, D., C. Perkins, J. Arkko, “Mobility Support for IPv6”, RFC3775 June 2004.

[RFC4068] R. Koodli, "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[Wikipedia] The Internet Encyclopedia. URL: *http://wikipedia.org*

[NET-SNMP] URL: *http://net-snmp.sourceforge.net/*

[snmpWiki] URL: *http://net-snmp.sourceforge.net/wiki/index.php/Main_Page*

[snmpAPI] URL: *http://net-snmp.sourceforge.net/dev/agent/*

[WimaxFund] Jeffrey G.Andrews, Arunabha Ghosh, Rias Muhamed, „Fundamentals of WiMAX”, Prentice HALL, February 2007

[WiMaxThesis] Neves Pedro, “Quality of Service and Mobility support in WiMAX Networks”, November 2006

[DigitalDivide] Guy Cayla, Stephane Cohen and Didier Guigon, “WiMAX an efficient tool to bridge the digital divide”, November 2005

[802.16f/Draft] Draft Amendment to IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems -Management Information Base,

August 2005

[Distr_Systems] Andrew Tanembaum, “Distributed Systems Principles and Paradigms”, Prenctice Hall, 2004

[UNIX_SOCKS] http://www.ecst.csuchico.edu/~beej/guide/ipc/usock.html

[802.16a] IEEE Std 802.16a-2003, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz", IEEE Standard 802.16a-2003, April 2003.

[QoSin802.16] Kitti Wongthavarawat, Aura Ganz, Packet scheduling for QoS support in IEEE 802.16 broadband wireless access systems, Wiley, c2003

[JTG] Jugi's Traffic Generator, website: *http://hoslab.cs.helsinki.fi/savane/projects/jtg/*.

[PTPd] Precision Time Protocol daemon website: *http://ptpd.sourceforge.net/*.

[DAIDALOS-IST] *Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised Personal Services (DAIDALOS) project: www.ist-daidalos.org*.

[Neves-ISCC2006] *P. Neves et al., Support of Real-time Service over Integrated 802.16 Metropolitan and Local Area Networks, 11th IEEE Symposium on Computers and Communications (ISCC), 2006.*

[Neves-ISCC2008] P. Neves et al., *Vendor-Independent Resource Control Framework for WiMAX*, 13th IEEE Symposium on Computers and Communications (ISCC), 2008.

[Pentikousis-WiNMee2008] K. Pentikousis et al., *An Experimental Investigation of VoIP and Video Streaming over Fixed WiMAX*, 4th International workshop on Wireless Network Measurements (WiNMee), 2008.

[RFC 4094] J. Manner, X. Fu, *Analysis of Existing Quality-of-Service Signalling Protocols*, IETF RFC 4094, May 2005.

[RSVPDynamicManag] Y.-W. Chen et al, *Dynamic Bandwidth Management for Handoffs with RSVP in 802.16/WLAN Environment*, 21st International Conference on Advanced Information Networking and Applications Workshops, 2007.

[802_21WMAN_WLAN] T. Yahiya et al, *A Case Study: IEEE 802.21 Framework Design for Service Continuity across WLAN and WMAN*, IFIP International Conference on Wireless and Optical Communications Networks, 2007.

[ABC_QoSModel] Jackson et al, *Always Best Connected QoS integration model for the WLAN, WiMAX Heterogeneous Network*, International Conference on Industrial and Information Systems (ICIIS) 2006.

[Mobility_in_802.16d] K. Leung et al., Mobility Support for IEEE 802.16d Wireless Networks, IEEE Wireless Communications and Networking Conference (WCNC), 2005

[WEIRD-IST] WiMAX Extension to Isolated Research Data networks project (WEIRD): *http://www.ist-weird.eu/*

[NSIS] R. Hancock et al, *Next Steps in Signalling (NSIS): Framework*, IETF RFC 4080, June 2005.

[NSLP] J. Manner, G. Karagiannis, *NSLP for Quality-of-Service Signalling*,

IETF NSIS WG Internet-Draft, July 2007.

[NGNPrinciples] K. Knightson, N. Morita, T. Towle, *NGN Architecture: Generic Principles, Functional Architectures and Implementation*, IEEE Communications Magazine, p. 49-55, October 2005.

[WiMAXForumStg3] WiMAX Forum, WiMAX End-to-End Network Systems Architecture Stage 3: Detailed Protocols and Procedures, Release 1.1.0, June 2007.

[RFC 4140] H. Soliman, Flarion, C.Castelluccia, K. El Malki, L. Bellier, Hierarchical Mobile IPv6 Mobility Management (HMIPv6), August 2005

[RFC 4831] J. Kempf, Ed., Goals for Network-Based Localized Mobility Management (NETLMM), April 2007

[RFC 4830] J. kempf, Ed., Problem Statement for Network-Based Localized Management (NetLMM), April 2007

[PMIPv6-Draft] S. Gundavelli, K.Leung, V. Davaparalli, K. Chowdhury, B. Patil, Proxy Mobile IPv6 draft-ietf-netlmm-proxymip6-18.txt, December 2008

[WiMAXAppl] http://www.trackcom-sys.ca/apps/

[QoSMobilityin4G] Vitor Jesus, Susana Sargento, Integration of QoS and Mobility in 4G scenarios, *International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, 2007*

[YAUNGMobFi] Yaung Xiau, WiMAX/MobileFi Advanced Research and Technology, Auerbach Publications, 2008

[RosenbergSIP] J. Rosenberg, G. Camarillo, *SIP: Session Initiation Protocol*, IETF RFC 3261, June 2002

[Diameter] P. Calhoun, J. Loughney, *Diameter Base Protocol*, IETF RFC 3588, September 2003

[GIST] H. Schulzrinne, R. Hancock, *GIST: General Internet Signalling Transport*, IETF NSIS WG Internet-Draft, July 2007.

[NissilaAdapter] T. Nissilä, J. Huusko, I. Harjula, and M. Katz, *Adapter Implementation between WiMAX Specific Layers and Network/Application Layers*, 1st BWA Workshop, Cardiff, Wales, September, 2007, pp. 328-333

[802.21D9] IEEE P802.21/D09 Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services

[M.3010] PRINCIPLES FOR A TELECOMMUNICATIONS MANAGEMENT NETWORK, ITU-T Recommendation M.3010, 1996

[NETLMMProto] H. Levkowetz, G. Giaretta, et al., The NetLMM Protocol draft-giaretta-netlmm-dt-protocol-02, expired April 8, 2007

Annexes

This last chapter is composed by additional, but also relevant information where can be found the implemented interfaces in WEIRD's project.

Annex A – WEIRD annexes

A Service Flows Management primitives

In order to trigger the service flows creation, deletion and modification were defined the following primitives between the Resource Controller and Generic Adapter.

A.1 ADAPTER_RESV_REQ Primitive

This primitive is sent by the RC to the Adapter to trigger a service flow reservation in the SS (*ss_mac_addr*). A service class (*sc_name*), a service flow and the correspondent classifier (*cs_classifier*) must be created.

Source	Destination	Parameter Name	Parameter Description
RC	**Adapter**	*primitive_id*	*An unique ID for each primitive.*
		Bs_ipv4_mgmt_addr	*BS IPv4 management address*
		Bs_mac_addr	*Associated BS MAC address*
		Ss_mac_addr	*Subscriber Station to establish the service flow*
		Sc_name	*Service Class Name*
		sched_serv	*Scheduling Service:* *UGS* *rtPS* *nrtPS* *BE*
		max_rate	*Maximum Sustained Bandwidth*
		min_rate	*Minimum Reserved Bandwidth*
		max_latency	*Maximum Latency*
		sf_priority	*Flow Priority*
		Jitter	*Tolerated Jitter*
		fix_var_sdu_size	*Fixed vs Variable SDU size:* *Fixed* *Variable*
		sdu_size (if fix_var_sdu_size=fixed)	*SDU size in bytes*
		req_tx_policy	*Request and Transmission Policy:* *SF shall not use broadcast BW Req. Opportunities (uplink only)* *SF shall not piggyback requests with data (uplink only)* *SF shall not fragment data* *SF shall not perform PHS* *SF shall not pack SDUs* *SF shall not include CRC*
		cs_classifier	*Classification information:* *ToS Low/High/Mask*

			Src/Dst IP addr *Src/Dst IP Mask* *Src/Dst Port Start/End*
		classifier_priority	*classifier_priority*
		cs_spec	*Convergence-Sublayer specification (IPv4(1), Ethernet 802.3 (3))*
		service_flow_state	*Service Flow State (active, admitted or provisioned)*
		Dir	*Service Flow Direction* *Downlink* *Uplink*

Table 21: ADAPTER_RESV_REQ Primitive

A.2 ADAPTER_RESV_RESP Primitive

This primitive is sent by the Adapter to the RC indicating the result of the reservation process. The service flow identifier (*sf_id*) is included to identify the reserved service flow for a further modification/deletion.

Source Module	Destination Module	Parameter Name	Parameter Description
Adapter	**RC**	*primitive_id*	*An unique ID for each primitive.*
		result	*Reservation Request Result in the WiMAX equipment*
		sf_id	*Service Flow Identifier used in the WiMAX link*

Table 22: ADAPTER_RESV_RESP Primitive

A.3 ADAPTER_MOD_REQ Primitive

This primitive is sent by the RC to the Adapter to modify a service flow that has been previously created. The service flow that must be modified is identified by the *sf_id* parameter.

Source Module	Destination Module	Parameter Name	Parameter Description
		primitive_id	*An unique ID for each primitive.*
		bs_ipv4_mgmt_addr	*BS IPv4 management address*
		bs_mac_addr	*Associated BS MAC address*
		ss_mac_addr	*SS MAC address*
		max_rate	*Maximum Sustained Bandwidth*
		min_rate	*Minimum Reserved Bandwidth*
		max_latency	*Maximum Latency*
		sf_priority	*Flow Priority*
		Jitter	*Tolerated Jitter*
		sf_id	*Service Flow Identifier used in the WiMAX link*

Table 23: ADAPTER_MOD_REQ Primitive

A.4 ADAPTER_MOD_RESP Primitive

This primitive is sent by the Adapter to the RC indicating the result of the service flow modification process. The service flow identifier (*sf_id*) is included to identify the modified service flow.

Source Module	Destination Module	Parameter Name	Parameter Description
Adapter	**RC**	*primitive_id*	*An unique ID for each primitive.*
		result	*Modification Request Result in the WiMAX equipment*
		sf_id	*Service Flow Identifier used in the WiMAX link*

Table 24: ADAPTER_MOD_RESP Primitive

A.5 ADAPTER_DEL_REQ Primitive

This primitive is sent by the RC to the Adapter to delete a specific service flow. The service flow that must be deleted is identified by the *sf_id* parameter.

Source	Destination	Parameter Name	Parameter Description
RC	**Adapter**	*primitive_id*	*An unique ID for each primitive.*
		bs_ipv4_mgmt_addr	*BS IPv4 management address*
		bs_mac_addr	*Associated BS MAC address*
		ss_mac_addr	*SS MAC address*
		sf_id	*Service Flow Identifier used in the WiMAX link*

Table 25: ADAPTER_DEL_REQ Primitive

A.6 ADAPTER_DEL_RESP Primitive

This primitive is sent by the Adapter to the RC indicating the result of the service flow deletion process. The service flow identifier (*sf_id*) is included to identify the deleted service flow.

Source	Destination	Parameter Name	Parameter Description
Adapter	**RC**	*primitive_id*	*An unique ID for each primitive.*
		Result	*Deletion Result in the WiMAX equipment*
		sf_id	*Service Flow Identifier used in the WiMAX link*

Table 26: ADAPTER_DEL_RESP Primitive

For the Generic Adapter and Specific Adapter interaction was defined a generalised primitive with the fields being filled optionally.

Source	Destination	Parameter Name	Parameter Description
Generic Adapter/ Specific Adapter	**Specific Adapter/ Generic Adapter**	*primitive_id*	*An unique ID for each primitive.*
		AI_primitive_id	*An Abstract Interface primitive identifier.*
		trap_id	*"trap_id" is used for TRAPs. The value is one of the AI primitive IDs.*
		Set_action	*"set_action" is used for SET to tell whether a create(0), modification(1) or delete(2) operation is to be made.*
		status	*Used in response primitves to indicate the allocated sf_id or the get process status.*
		bs_ipv4_mgmt_add	*BS IPv4 Address*

		bs_mac_addr	*BS MAC Address*
		ss_mac_addr	*SS MAC Address*
		Dir	*SF Direction*
		value_binding_list	*variables list containing the remaining parameter values of the Abstract Interface Primitive.*

Table 27: Generic and Specific Adapter Interface

It must be mentioned that this primitive is also used between the Generic Adapter and the Specific Adapter for the exchange of topological and resources information.

B Resources and topology information primitives

The resources allocation in WiMAX network had to be efficiently managed. Having this in mind, the topology information and the resources information in the 802.16 network has a farthest relevance for admission control and proficient traffic distribution. In order to allow the upper layer entities to have a detailed picture of the WiMAX segment, the following primitives were defined.

B.1 ADAPTER_NEW_BS Primitive

This primitive is sent by the Adapter to the RC to inform the RC that a new BS, identified by the *bs_mac_addr* parameter, is connected. This primitive must be sent to the RC immediately after a new BS is connected. This will allow the RC to have a complete and updated topology of the WiMAX network, as well as the CSC_ASN.

Source	Destination	Parameter Name	Parameter Description
Adapter	**RC**	*primitive_id*	*An unique ID for each primitive.*
		bs_mac_addr	*BS MAC address*
		bs_ipv4_mgmt_addr	*BS IPv4 management address*
		sector_avail_dl_bw	*Total available downlink bandwidth for the sector*
		sector_avail_ul_bw	*Total available uplink bandwidth for the sector*
		tx_power	*Transmission Power*
		channel_bw	*Channel size of the WiMAX link*
		freq_oper	*BS sector Frequency of operation*
		guard_interval	*OFDM guard interval*
		frame_dur	*Frame Duration*
		vendor_id	*Vendor Identification*

Table 28: ADAPTER_NEW_BS Primitive

B.2 ADAPTER_NEW_SS Primitive

This primitive is sent by the Adapter to the RC to inform the RC that a new SS, identified by the s*s_mac_addr* parameter, is connected to the BS, identified by the *bs_mac_addr* parameter. This primitive must be sent to the RC immediately after a new SS associates with the BS.

Source	Destination	Parameter Name	Parameter Description
Adapter	RC	*primitive_id*	*An unique ID for each primitive.*
		ss_mac_addr	*SS MAC address*
		ss_ipv4_mgmt_addr	*SS IPv4 management address*
		assoc_bs_mac_addr	*Associated BS MAC address*
		ss_avail_dl_bw	*Total available downlink bandwidth for the SS*
		Ss_avail_ul_bw	*Total available uplink bandwidth for the SS*
		mod_type	*Modulation Scheme being used*
		tx_Power	*Transmission Power*
		Dist	*Distance between the SS and the associated BS*
		vendor_id	*Vendor Identification*

Table 29: ADAPTER_NEW_SS Primitive

B.3 ADAPTER_DEL_SS Primitive

This primitive is sent by the Adapter to the RC to inform the RC that the SS (*ss_mac_addr*) connected to the BS (*bs_mac_addr*) has been removed.

Source	Destination	Parameter Name	Parameter Description
Adapter	RC	*Primitive_id*	*An unique ID for each primitive*
		ss_mac_addr	*SS MAC address*
		bs_mac_addr	*Associated BS MAC address*

Table 30: ADAPTER_DEL_SS Primitive

B.4 ADAPTER_RESOURCES_REQ Primitive

This primitive is sent by the RC to the Adapter to check the amount of available bandwidth in a specific SS (*ss_mac_addr*).

Source Module	Destination Module	Parameter Name	Parameter Description
RC	Adapter	*primitive_id*	*An unique ID for each primitive.*
		bs_ipv4_mgmt_addr	*BS IPv4 management address*
		ss_mac_addr	*SS MAC address*
		bs_mac_addr	*Associated BS MAC address*

Table 31: ADAPTER_RESOURCES_REQ Primitive

B.5 ADAPTER_RESOURCES_RESP Primitive

This primitive is sent by the Adapter to the RC as a reply to the ADAPTER_RESOURCES_REQ primitive, including the available (downlink/uplink) bandwidth for the SS.

Source Module	Destination Module	Parameter Name	Parameter Description
Adapter	RC	*primitive_id*	*An unique ID for each primitive.*
		Bs_mac_addr	*Associated BS MAC address*
		Ss_mac_addr	*SS MAC address*
		Ss_used_dl_bw	*Total used downlink bandwidth for the SS.*

		Ss_used_ul_bw	*Total used uplink bandwidth for the SS.*

Table 32: ADAPTER_RESOURCES_RESP Primitive

B.6 ADAPTER_CSI_INFO Primitive

This primitive is sent by the Adapter to the RC to provide the Channel State Information.

Source	Destination	Parameter Name	Parameter Description
Adapter	**RC**	*primitive_id*	*An unique ID for each primitive.*
		bs_mac_addr	*Associated BS MAC address*
		ss_mac_addr	*SS MAC address*
		Cinr	*Carrier to Interference-plus-Noise Ratio*
		Rssi	*Received Signal Strength Indicator*
		if_status	*Interface operational status*

Table 33: ADAPTER_CSI_INFO Primitive

Annex B – DAIDALOS II annexes

A RALWiMAX Supported Primitives (MIHF::RALWiMAX)

Primitives exchanged between MIHF and RALWiMAX.

Source	Destination	Primitive	Parameters
A22_AR_MIH_Function	A21_AR_RAL_WIMAX	LINK_RESOURCE_PREPARE_REQUEST (not implemented, refer to section 6.1.2.1 for details)	- LinkID - FlowID - QoSParameters
A21_AR_RAL_WIMAX	A22_AR_MIH_Function	LINK_RESOURCE_PREPARE_RESPONSE (not implemented, refer to section 6.1.2.1 for details)	- LinkID - FlowID - ResourceStatus - AvailableResources
A22_AR_MIH_Function	A21_AR_RAL_WIMAX	LINK_RESOURCE_ACTIVATE_REQUEST	- LinkID - FlowID
A21_AR_RAL_WIMAX	A22_AR_MIH_Function	LINK_RESOURCE_ACTIVATE_RESPONSE	- LinkID - FlowID - ResourceStatus
A22_AR_MIH_Function	A21_AR_RAL_WIMAX	LINK_CONFIGURE_THRESHOLD_REQUEST	- LinkID - LinkParameterList
A21_AR_RAL_WIMAX	A22_AR_MIH_Function	LINK_CONFIGURE_THRESHOLD_CONFIRM	- LinkID - Result
A22_AR_MIH_Function	A21_AR_RAL_WIMAX	LINK_GET_PARAMETERS_REQUEST	- LinkID - LinkParameterList
A21_AR_RAL_WIMAX	A22_AR_MIH_Function	LINK_GET_PARAMETERS_CONFIRM	- LinkID - LinkParameterResult

Table 34: MIHF and RALWiMAX interface

B RALWiMAX and DriverWiMAX interface primitives

Source	Destination	Primitive	Function
A21_AR_RAL_WIMAX	A21_AR_DRIVER_WIMAX	CNX-ACTIVATE-REQ	Reservation Request
A21_AR_DRIVER_WIM	A21_AR_RAL_WIMAX	CNX-ACTIVATE-RESP	Reservation Response
A21_AR_RAL_WIMAX	A21_AR_DRIVER_WIMAX	CNX-MODIFY-REQ	Reservation Modify Request
A21_AR_DRIVER_WIM	A21_AR_RAL_WIMAX	CNX-MODIFY-RESP	Reservation Modify Response
A21_AR_RAL_WIMAX	A21_AR_DRIVER_WIMAX	CNX-DELETE-REQ	Reservation Teardown Request
A21_AR_DRIVER_WIM	A21_AR_RAL_WIMAX	CNX-DELETE-RESP	Reservation Teardown Response

Table 35: RALWIMAX and DriverWiMAX interface