Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2006

Pedro Miguel Naia Neves

Qualidade de Serviço em Redes de Acesso IEEE 802.16

Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2006

Pedro Miguel Naia Neves

Qualidade de Serviço em Redes de Acesso IEEE 802.16

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

o júri

presidente	Prof. Dr. Atílio Gameiro professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro
	Prof. Dr. Rui Rocha professor associado do Departamento de Engenharia Electrotécnica e de Computadores do Instituto Superior Técnico
	Prof. Dra. Susana Sargento professora auxiliar convidada do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

agradecimentos

À Professora Susana Sargento, por estar sempre disponível para esclarecer as dúvidas existentes e partilhar os seus conhecimentos. Revelou-se importante o espírito critico demonstrado pela mesma na procura de mais e melhores soluções para os problemas encontrados.

Ao Professor Rui Aguiar pela disponibilidade demonstrada em partilhar os seus conhecimentos e fornecer informação importante para o desenvolvimento da dissertação.

Ao Instituto de Telecomunicações de Aveiro e seus colaboradores por me terem oferecido todas as condições e apoio necessários para o desenvolvimento desta dissertação. Em particular, aos colegas do grupo de redes heterogéneas HNG (Heterogeneous Network Group) que sempre se mostraram disponíveis para discutir as soluções encontradas no decorrer desta dissertação.

À minha esposa, Ana Luísa, e à minha familia pelo incansável apoio, paciência e motivação que sempre me deram durante o desenvolvimento da dissertação.

palavras-chave

IEEE 802.16, IEEE 802.11e, WiMAX, Mobilidade, Qualidade de Serviço, Virtual MAC, MAC Address Translator, 4G, Regras de tradução de pacotes, Fluxos de serviço.

resumo

A procura de serviços e de aplicações com elevadas exigências de largura de banda, e a vontade crescente para aceder a este tipo de serviços em qualquer lugar, torna necessária a integração da Internet actual com as redes móveis de próxima geração. No entanto, existirão sempre àreas remotas onde o acesso à Internet, e nomeadamente a serviços de banda larga, será difícil de conseguir.

O protocolo IEEE 802.16 é uma tecnologia de banda larga sem fios que pode ser usada neste tipo de cenários. Esta dissertação apresenta uma arquitectura de rede capaz de suportar serviços de tempo real com integração de QoS em ambientes IPv6 através da utilização de redes IEEE 802.16. Nomeadamente, a arquitectura definida suporta o acesso dinâmico e rápido por parte dos terminais móveis aos serviços de rede, tal como reservas e modificações dinâmicas de serviços de tempo real, característica essencial para o suporte de alta mobilidade. Para além disto, a solução proposta fornece também suporte IPv6 e diferenciação de serviços direccionados para o mesmo terminal móvel.

Esta dissertação apresenta a arquitectura desenvolvida, os módulos necessários para a integração da tecnologia IEEE 802.16 num ambiente de próxima geração, a implementação desses módulos para a construção de uma rede real, e testes para avaliar o desempenho da rede em termos de QoS num ambiente de rede de acesso mista, composta por IEEE 802.16 e IEEE 802.11. São também efectuados testes de mobilidade para avaliar o desempenho da solução descrita neste tipo de ambientes. Os resultados obtidos com a arquitectura desenvolvida mostram que a arquitectura pode fornecer QoS fim-a-fim sobre a concatenação de redes metropolitanas e locais, com suporte de mobilidade.

keywords

IEEE 802.16, IEEE 802.11e, WiMAX, mobility, Quality of Service, Virtual MAC, MAC Address Translation, 4G, Translation Rules, Service Flows.

abstract

The growing demand of high bandwidth services and applications, and the increasing will of access to these services anywhere, is motivating the requirement to integrate the current Internet with the future mobile networks. However, there will always be remote areas where Internet access will be difficult to achieve. The IEEE 802.16 is an attractive broadband wireless technology for these scenarios, non-withstanding its limitations for dynamic environments.

This Thesis discusses a network architecture able to support IPv6 QoS aware real time services using 802.16 networks. Specifically, this solution supports dynamic and fast access from the Mobile Nodes to the network services, as well as dynamic reservations and modifications of services. These fast and dynamic reservations are crucial to the support of fast mobility approaches. Moreover, the proposed solution is also able to provide IPv6 support and efficient traffic differentiation for services running on the same MN.

This Thesis presents the envisioned architecture, the modules required to provide the integrated QoS approach over the 802.16 network, the implementation of the modules to build a real network, and address main implementation results in terms of QoS performance, and in terms of mobility with QoS support for converged networks comprising WiMAX and Wi-Fi technologies. The obtained results show that our architecture is able to provide end-to-end QoS over the concatenation of metro and local area networks, and that seamless mobility is achieved with high performance measures, thus being able to support real-time services.

Table of Contents

Index of Figures

Index of Tables

Acronyms

	Acronym	Description
	16CP	802.16 Control Protocol
	4G	Fourth Generation Networks
A		
	A4C	Authentication, Authorization, Auditing, Accounting and Charging
	AAA	Authentication, Authorization and Accounting
	AR	Access Router
	ARQ	Automatic Repeat Request
	ATM	Asynchronous Transfer Mode
	AUX-SF	Auxiliar Service Flow
B		
	BE	Best Effort
	BR	Bandwidth Request
	BS	Base Station
	BW	Bandwidth
	BWA	Broadband Wireless Access
C		
	CC	Confirmation Code
	CID	Connection Identifier
	CMS	Central Monitoring System
	COPS	Common Open Policy Service
	CPS	Common Part Sublayer
	CR	Core Router
	CRC	Cyclic Redundancy Check
	CS	Convergence Sublayer
D		
	DAD	Duplicate Address Detection

	DAIDALOS	Designing Advanced Network Interfaces for the Delivery and Administration of Location Independent, Optimised Personal Services)
	DCD	Downlink Channel Descriptor
	DHCP	Dynamic Host Configuration Protocol
	DIUC	Downlink Interval Usage Code
	DL	Downlink
	DL-MAP	Downlink Map
	DOCSIS	Data Over Cable Service Interface Specification
	DSA-REQ	Dynamic Service Addition Request
	DSA-RSP	Dynamic Service Addition Response
	DSA-ACK	Dynamic Service Addition Acknowledgment
	DSC-REQ	Dynamic Service Change Request
	DSC-RSP	Dynamic Service Change Response
	DSC-ACK	Dynamic Service Change Acknowledgment
	DSCP	Differentiated Services Codepoint
	DSD-REQ	Dynamic Service Deletion Request
	DSD-RSP	Dynamic Service Deletion Response
	DSD-ACK	Dynamic Service Deletion Acknowledgment
	DSL	Digital Subscriber Line
	DSx	Dynamic Service Addition, Change or Deletion
E		
	ERTPS	Extended Real Time Polling Service
	ETSI	European Telecommunications Standards Institute
F		
	FA	Foreign Agent
	FBU	Fast Binding Update
	FCH	Frame Control Header
	FDD	Frequency Division Duplexing
	FEC	Forward Error Correction

	FHO	Fast Handover
	FNA	Fast Neighbour Advertisement
	FFT	Fast Fourier Transform
	FTP	File Transfer Protocol
	FSH	Fragmentation Subheader
	FSN	Frame Sequence Number
G		
	GS	Guard Symbol
H		
	HA	Home Agent
	HCS	Header Check Sequence
	HO-DEC	Handover Decision
	HO-REQ	Handover Request
	HO-RSP	Handover Response
	HTTP	Hypertext Transport Protocol
I		
	ICMPv4	Internet Control Message Protocol version 4
	ICMPv6	Internet Control Message Protocol version 6
	ICT	Information and Communication Technology
	IE	Information Element
	IEEE	Institute of Electrical and Electronics Engineers
	IFFT	Inverse Fast Fourier Transform
	IPv4	Internet Protocol version 4
	IPv6	Internet Protocol version 6
	ISP	Internet Service Provider
	ITU	International Telecommunication Union
L		
	LAN	Local Area Network
	LOS	Line of Sight
M		

	MAC	Medium Access Control
	MAN	Metropolitan Area Network
	MANET	Mobile Ad-hoc Networks
	MAT	MAC Address Translator
	MIMO	Multiple Input Multiple Output
	MMSP	Multimedia Service Proxy
	MN	Mobile Node
	MNA-REQ	Mobile Node Access Request
	MNA-RSP	Mobile Node Access Response
	MPEG	Moving Pictures Experts Group
N		
	NA	Neighbour Advertisement
	NDP	Neighbour Discovery Process
	NEMO	Moving Networks
	NLOS	Non Line of Sight
	NRTPS	Non Real Time Polling Service
	NS	Neighbour Solicitation
	NUD	Neighbour Unreachability Detection
O		
	OFDM	Orthogonal Frequency Division Multiplexing
	OFDMA	Orthogonal Frequency Division Multiple Access
P		
	PBNMS	Policy Based Network Management System
	PBR	Piggyback request
	PDP	Policy Decision Point
	PEP	Policy Enforcement Point
	PDU	Protocol Data Unit
	PHY	Physical Layer
	PM	Poll-Me bit
	PMP	Point-to-Multipoint

	PrRtrAdv	Proxy Router Advertisement
	PrRtrSol	Proxy Router Solicitation
	PS	Privacy Sublayer
	PTP	Point-to-Point
Q		
	QAM	Quadrature Amplitude Modulation
	QoS	Quality of Service
	QoSBr	QoS Broker
	QoSM	QoS Manager
	QPSK	Quadrature Phase Shift Keying
R		
	RA	Router Advertisement
	RAN	Radio Access Network
	REG-REQ	Registration Request
	REG-RSP	Registration Response
	RNG-REQ	Ranging Request
	RNG-RSP	Ranging Response
	RS	Router Solicitation
	RSpec	Resource Specification
	RSVP	Resource Reservation Protocol
	RTG	Receive Transition Gap
	RTPS	Real Time Polling Service
S		
	SAP	Service Access Point
	SC	Single Carrier
	SDU	Service Data Unit
	SF	Service Flow
	SF-DEL-REQ	Service Flow Deletion Request
	SF-DEL-RSP	Service Flow Deletion Response
	SF-MOD-REQ	Service Flow Modify Request

	SF-MOD-RSP	Service Flow Modify Response
	SF-RESV-REQ	Service Flow Reservation Request
	SF-RESV-RSP	Service Flow Reservation Response
	SIP	Session Initiation Protocol
	SNMP	Simple Network Management Protocol
	SOFDMA	Scalable Orthogonal Frequency Division Multiple Access
	SPP	Service Provisioning Platform
	SS	Subscriber Station
	SSTG	Subscriber Station Transition Gap
T		
	TCP	Transmission Control Protocol
	TDD	Time Division Duplexing
	TDM	Time Division Multiplexing
	TDMA	Time Division Multiple Access
	TFTP	Trivial File Transfer Protocol
	TLV	Type Length Value
	TSpec	Traffic Specification
	TTG	Transmit Transition Gap
U		
	UCD	Uplink Channel Descriptor
	UDP	User Datagram Protocol
	UGS	Unsolicited Scheduling Service
	UIUC	Uplink Interval Usage Code
	UL	Uplink
	UL-MAP	Uplink Map
	UN	United Nations
V		
	VLAN	Virtual Local Area Network
	VMAC	Virtual Medium Access Control

W		
	WiBro	Wireless Broadband
	WiMAX	Worldwide Interoperability Access
	WLAN	Wireless Local Area Network
	WMAN	Wireless Metropolitan Area Network
	WSIS	World Summit on the Internet Society

Chapter 1: Introduction

1.1. Motivation

After the Second World War, the International Telecommunication Union (ITU) [itu] became the specialized agency for telecommunications of the United Nations (UN) [un]. One of its tasks is to collect statistics on the Information and Communication Technologies (ICTs) penetration, accessibility and use. In 1996, the ITU initiated a project named "*Right to Communicate*" to provide access to the ICTs all around the world. To achieve this aim, the World Summit on the Internet Society (WSIS) [wsis] was created.

The unequal access to the ICTs has been defined by the WSIS as the *Digital Divide*. It refers to the unequal access to the ICTs between the developing and developed countries, rural and urban areas, poor and rich citizens, as well as educated and non-educated population.

Despite the Digital Divide is a characteristic from the developing countries, we can also find it in the developed countries, such as the ones from Europe and North America. In these countries, rural areas have limited access to ICTs, due to the lack of infrastructures and economical conditions. Despite the difference between the developing and the developed countries is decreasing, the gap is still enormous.

Bearing in mind this fact, we can start by analyzing Figure 1, in which the number of fixed telephone subscribers' evolution between 1994 and 2004, in both developed and developing countries, is depicted.

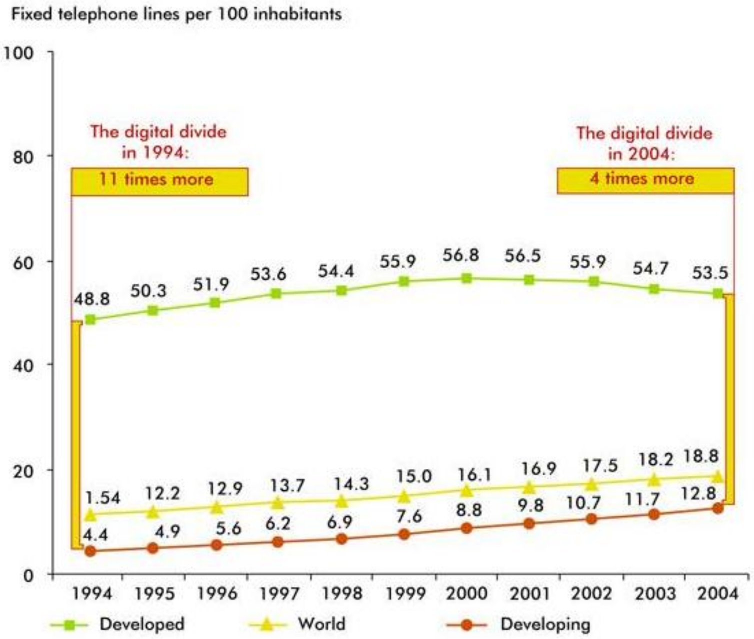

Figure 1: Fixed telephone subscribers' evolution between 1994 and 2004 [wsis]

As we can see, in 1994 the developed countries had eleven times more telephone subscribers than the developing countries, whereas in 2004 the gap decreased to four times. We can notice a significant decrease of the gap in this decade, though it is still not sufficient. For instance, in the African continent, where we find the biggest percentage of developing countries, has an average of 3 % of fixed subscribers, whereas America and Europe have 34 % and 40 % of fixed subscribers, respectively.

Regarding the mobile phone subscribers' evolution, shown in Figure 2, the Digital Divide between developed and developing countries is also seen.

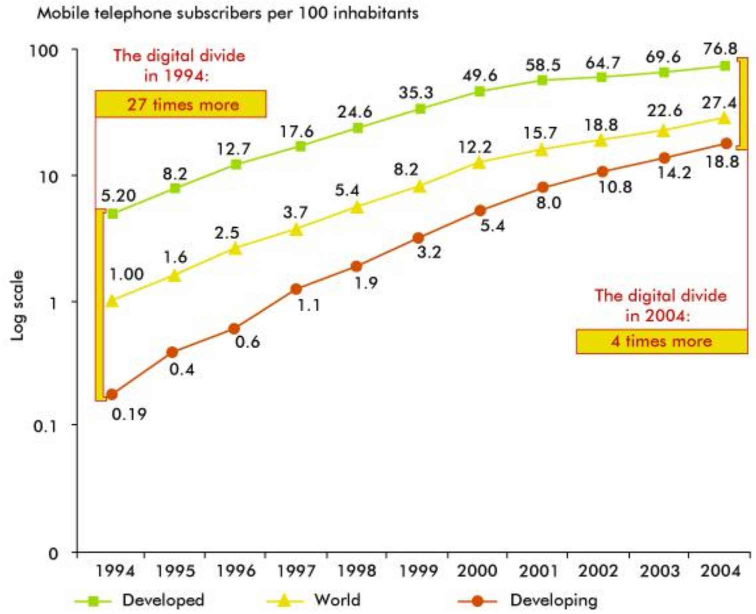

Figure 2: Mobile telephone subscribers' evolution between 1994 and 2004 [wsis]

In this case, the growth was higher comparing to the fixed telephones case shown in Figure 1. In 2004, the developing world had four times fewer mobile subscribers than the developed world, whereas in 1994, the gap was twenty-seven times lower. Just as a remark, the G8 countries population, which is around 14 % of the world population, has 34% of the mobile subscribers in the world.

Finally, Figure 3 depicts the internet users' variation between 1994 and 2004.

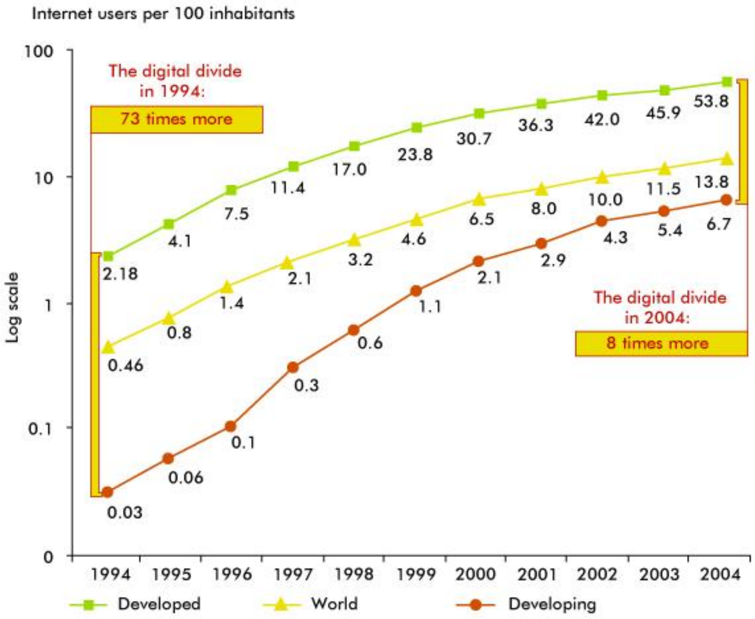

Figure 3: Internet users' subscribers' evolution between 1994 and 2004 [wsis]

In this case, the developing countries' access to the ICTs was remarkably huge. Between 1994 and 2004, the gap decreased from seventy-three times to eight times. Nonetheless, the growth is still too low compared to the internet usage in the developed world. Note that, in 2004, less than 3 % of the Africans had access to the internet, whereas in the G8 countries, 50% of the inhabitants had internet access. Moreover, the total internet users' number is eight times higher in the United States, three in Japan and twice in Germany than in the all African continent, composed by more then fifty countries. Additionally, there are still thirty countries with less than 1 % in internet access.

IEEE 802.16 [ieee802.16-04] [ieee802.16e-05] is an attractive broadband wireless technology that can be used to overcome the previously mentioned limited access to the ICTs, non-withstanding its limitations for dynamic environments. This is a broadband wireless access solution for metropolitan area networks (MANs), reaching maximums of 70 km with very high throughputs (on the hundred Mbps range). Using this access technology, the operators can reach users anywhere, with low installation costs when compared with fibre, cable or DSL (Digital Subscriber Line) [dsl]. Additionally, it is an easy system to install, leading to decreasing costs, which is an important factor in developing countries or rural areas. It also provides a wide coverage that can reach 15 km in Non-Line of Sight (NLOS) environments [gesbcommag02] and 50 km in Line of Sight (LOS) environments, which is extremely important for rural areas. Another important factor is the interoperability effort, which is currently being leaded by the Worldwide Interoperability for Microwave Access (WiMAX) Forum [wimax]. As an outcome of this effort, the equipment prices will decrease, benefiting the developing nations. Furthermore, IEEE 802.16 supports mobile nodes, as defined in the IEEE 802.16e-2005 protocol [ieee802.16e-05], bringing mobility into this MAN scenario. This opens a different set of business opportunities for the operators, turning IEEE 802.16 [eklcommag02] into a viable technology for the so-called "4G" networks [aguiarmobsum04] [janelsev05]. In these environments, users wish for having ubiquitous internet access, with a wide range of possible services while moving (including "triple play": data, voice and video) and with assured QoS guarantees [marqwcom03] [carmobsum05]. These characteristics will lead next generation networks to the ABC (Always Best Connected) paradigm, and as a consequence, the operators will have to cope with a set of extremely challenging requirements [kassecon04] [kasmedhoc05] [kaswadhoc05]. Therefore, the network design, from the core to the access network, should be able to deal with these aspects. Thus, a set of mechanisms must be defined to support an end-to-end (E2E) QoS architecture with fast-mobility and real time services support, in a heterogeneous environment [priorhicss05] [hillcommag04].

1.2. Objectives

The main goal of this Thesis is to design, implement and evaluate a network architecture with E2E QoS and fast mobility support [neviscc06] [nevconftele05]. A special focus will be given to the challenges posed by the IEEE 802.16 technology in the access network [nev16ngps06] [nev16ng06]. More specifically, it will address QoS integration in the access network, including IEEE 802.16 and IEEE 802.11e [ieee802.11e] [ieee802.11-99] technologies. The main goals can be described through the following steps:

- Definition and specification of the access network architecture
- Design of the 802.16 driver (related modules and interfaces), bearing in mind the following requirements:

  - ⇒ E2E QoS
  - ⇒ Real time services
  - ⇒ Fast mobility between 802.11 networks that are backhauled by an 802.16-2004 link
  - ⇒ IPv6
  - ⇒ Two modes of operation: point-to-point (PTP) and point-to-multipoint (PMP)
  - ⇒ Two main scenarios: single-hop scenario (terminal directly connected to the 802.16 system) and two-hop scenario (mobile node connected to an access point that is backhauled by an 802.16 system)
- Implementation of the 802.16 driver with the required functionalities.
- Evaluation of the implemented solution in terms of mobility with QoS support for converged networks comprising 802.16 and 802.11e technologies.

1.3. Document Outline

The present Thesis is organized as follows:

- Chapter 2 provides an overview of the IEEE 802.16 standard, including the MAC and PHY layers, and the QoS support provided by the protocol. A brief comparison between the IEEE 802.16-2004 and the IEEE 802.16e-2005 standards is provided, as well as the main characteristics of the 802.16 equipment used for this Thesis.
- Chapter 3 provides a brief overview about the DAIDALOS project [daid], as well as the network modules and interfaces that have been defined. Additionally, it also describes the open issues related with the IEEE 802.16 integration in a next-generation network.
- Chapter 4 details the novel solutions adopted to overcome the IEEE 802.16 open issues, as well as the developed modules and interfaces. Finally, a detailed overview about the 802.16 driver operation phases is provided, including services reservation, modification and deletion, as well as a fast-mobility case.

- Chapter 5 discusses the measurement results obtained for the implemented solutions. Single-hop and two-hop scenarios, in PTP and PMP modes of operation, are used to perform the required measurements. The obtained times are carefully analyzed.
- Chapter 6 presents the conclusions of this work, as well as the envisaged future work.

Chapter 2: IEEE 802.16 Overview

In the near future, a Broadband Wireless Access (BWA) technology for Metropolitan Area Networks (MANs) will be a requirement. IEEE 802.16-2004 [ieee802.16-04], as one of these technologies, is a serious candidate to fulfil this gap and thus, it is expected to be widely accepted by the telecommunications market.

IEEE 802.16-2004 specifies a Medium Access Control (MAC) layer and several Physical (PHY) layers. Each PHY layer addresses a specific frequency band, providing a very flexible standard. For instance, when operating in the 10 GHz to 66 GHz band, due to the short wavelength, Line of Sight (LOS) is required and multipath is negligible. For frequencies operating in the 2 GHz to 11 GHz band, the wavelength is higher and therefore NLOS scenarios are envisaged. In this case, the multipath effect is not negligible and must be carefully analyzed. The MAC layer is connection oriented and provides Quality of Service (QoS) assurances through the usage of service flows and uplink scheduling services. A set of convergence sublayers are defined to map the upper layer packets into the 802.16-2004 system. The convergence sublayers support packet based protocols, such as Internet Protocol version 4 (IPv4) [rfc791] and Internet Protocol version 6 (IPv6) [rfc2460], as well as cell based protocols, such as Asynchronous

Transfer Mode (ATM) [atmuni94] [atmsig06]. Both point-to-multipoint (PMP) and mesh modes of operation are supported by the standard, despite the mesh mode of operation is optional.

This chapter presents an overview of the IEEE 802.16 standard and its main characteristics. Section 2.1 provides a brief overview of the IEEE 802.16 working group (WG) [16-wg] evolution since its creation in 1998 until the current days. Section 2.2 depicts the basic topology used by the IEEE 802.16-2004 technology whereas section 2.3 introduces its several layers and sublayers. Following, section 2.4 depicts the MAC layer and section 2.5 explains the PHY layer. A comparison between the IEEE 802.16 fixed version, IEEE 802.16-2004, and the mobile one, IEEE 802.16-2005, is provided in section 2.6. The main characteristics of the 802.16 equipment used in this Thesis are depicted in section 2.7. Finally, section 2.8 provides a final summary of the chapter.

2.1. IEEE 802.16 Working Group Evolution

In 1998 the U.S. National Wireless Electronic Systems Testbed (N-WEST) of the U.S. National Institute of Standards and Technology (NIST) [nist] initiated the Institute of Electrical and Electronics Engineers (IEEE) [ieee] 802.16 activities. In November of the same year, a meeting with IEEE 802 occurred, and a study group has been formed with the IEEE 802 approval, being Roger Marks nominated as chairman. The group wrote the Task Group 1 Project Authorization Request (PAR) which was approved on March 18th 1999. In this way, the IEEE project 802 [ieee802], working group 16, often referred as 802.16, was born. Two years later, on December 6th 2001, the **IEEE 802.16-2001** standard [ieee802.16-01] was approved by the IEEE and on April 8th 2002 it was published. This standard specifies the air interface for fixed Line of Sight (LOS) PMP broadband wireless access systems environments utilizing the 10-66 GHz frequency range. A unique, single carrier PHY layer is supported by this standard – the WirelessMAN-SC PHY layer.

On March 15th 2002, the Task Group c PAR was approved by the IEEE 802. This task group was responsible for defining an amendment to the IEEE 802.16-2001 standard. The amendment defines the system profiles for the 10-66 GHz frequency range. The **IEEE 802.16c-2002** standard [ieee802.16c-02] was approved by the IEEE on December 11th 2002 and it was published on January 15th 2003.

On March 30th 2000, the Task Group a PAR was approved by the IEEE 802 group. This task group was responsible for developing the **IEEE 802.16a-2003** standard [ieee802.16a-03], an amendment to the IEEE 802.16-2001 standard. This amendment defines the required enhancements and modifications for the MAC and PHY layers specifications to support the 2 - 11 GHz frequency band. As a result, the IEEE 802.16a-2003 supports non-line of sight (NLOS) environments in opposition to the 10 - 66 GHz case. Besides the PMP topology, this amendment also integrates the mesh topology. Multiple physical layers, single and multi-carrier, are supported, each suited to a particular operational environment. A single carrier PHY layer, named WirelessMAN-SCa air interface, and two multi-carrier PHY layers, that is WirelessMAN-OFDM (256 carriers) and WirelessMAN-OFDMA (2048 carriers), have been defined. On January 29th 2003 the IEEE approved this standard and published it on April 1st 2003.

Finally, on December 11th 2002, the Task Group d (under PAR 802.16d) was approved by the IEEE 802. However, the PAR 802.16d transitioned to the PAR 802.16-REVd on September 11th 2003. This task group was responsible for the development of the **IEEE 802.16-2004** standard [ieee802.16-04]. It revises and consolidates the IEEE 802.16-2001, IEEE 802.16a-2003 and IEEE 802.16c-2002 standards. Additionally, this revision also specifies the profiles for the IEEE 802.16a-2003 standard. This standard has been approved in 24th June 2004 and published in 1st October 2004.

The Task Group e PAR was also approved on December 11th 2002. This task group developed the **IEEE 802.16e-2005** [ieee802.16e-05], an amendment to the IEEE 802.16-2004 standard allowing the Subscriber Stations (SS) to be mobile. This standard has been approved in December 2005.

2.2. Basic Topology

Point-to-multipoint is the basic mode of operation of the 802.16-2004 technology. It is composed by a Base Station (BS) connected to the core network and in contact with fixed wireless SSs. Figure 4 illustrates the 802.16-2004 PMP topology.

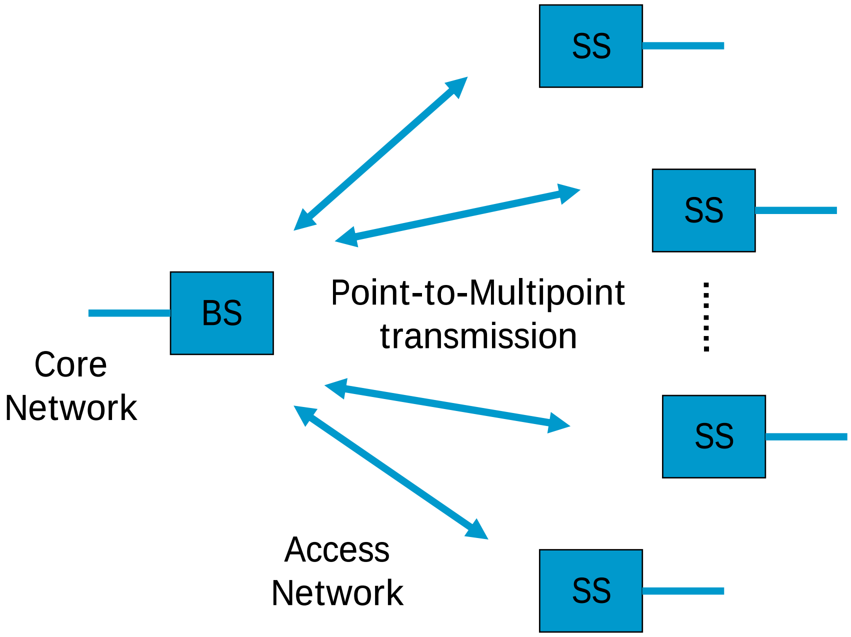

Figure 4: IEEE 802.16-2004 PMP operation mode

Before we analyze Figure 4, it is important to refer that the 802.16-2004 technology is totally connection-oriented. Therefore, all tasks are based on a connection and no packets are allowed to traverse the wireless link without a specific connection allocated. A connection is, by definition, a unidirectional mapping between the BS and the SS MAC layers for the purpose of transporting a service flow's traffic. To uniquely identify a connection, a 16-bit Connection Identifier (CID) is used. More detailed information about the 802.16-2004 connections is provided in section 2.4.2.1.

Going back to Figure 4, all SSs within the same frequency channel receive the same transmission from the BS. The BS sends packets to the SSs multiplexing data in a Time Division Multiplex (TDM) fashion. Since the BS, in a specific frequency channel, is the only transmitter in the downlink direction, it does not have to coordinate with other BSs to transmit in the downlink. Therefore, the downlink subframe is broadcasted to all the SSs. Each SS reads the MAC Protocol Data Units (PDU) inside the downlink subframe and checks if the CID refers to a connection destined for it. If the CID refers to another SS, the SS discards that specific MAC PDU. On the other hand, the uplink channel is shared between the several SSs connected to the BS in an on-demand basis, using Time Division Multiple Access (TDMA). For this purpose, there is a dedicated uplink scheduling service associated to each flow of packets. Four uplink scheduling services are available: Unsolicited Grant Service (UGS), real-time Polling Service (rtPS), non real-time Polling Service (nrtPS) and Best Effort (BE). The usage of the uplink scheduling services determines the rights to transmit in the uplink to each SS, giving the SSs continuing rights to transmit, or the right to transmit may be granted by the BS after the receipt of a bandwidth request message from the user. Also associated with the uplink scheduling services are polling and contention procedures.

Besides the PMP topology, the mesh topology is also specified in the 802.16-2004 standard. While in PMP mode traffic only occurs between the BS and the SSs, in the mesh topology traffic can occur directly between SSs.

2.3. Protocol Layering

The 802.16-2004 protocol defines both the MAC and PHY layers. Figure 5 shows the 802.16-2004 protocol stack.

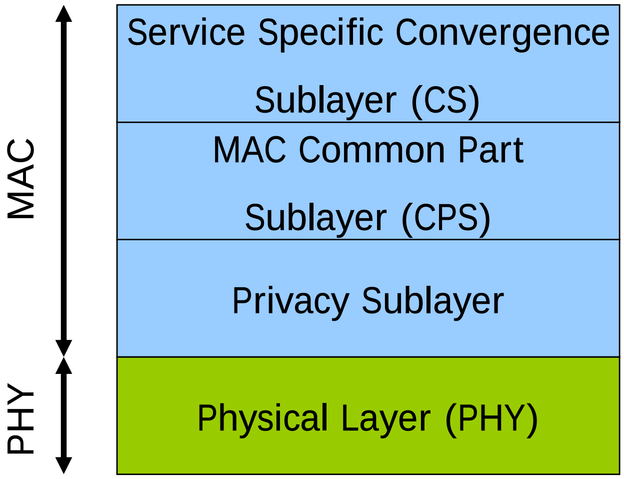
MAC
PHY
Service Specific Convergence Sublayer (CS)
MAC Common Part Sublayer (CPS)
Privacy Sublayer
Physical Layer (PHY)

Figure 5: IEEE 802.16-2004 layers (MAC and PHY)

This section describes in more detail the Service Specific Convergence Sublayer (CS) (see section 2.4.1), the Common Part Sublayer (CPS) (see section 2.4.2) and the Privacy Sublayer (PS) (see section 2.4.3).

2.4. IEEE 802.16-2004 MAC Layer

The MAC layer provides the interface with higher layers through the Service Specific Convergence Sublayer (see section 2.4.1). Below the Service Specific Convergence Sublayer we find the Common Part Sublayer (see section 2.4.2) that is responsible for the most important MAC functions. Finally, under the Common Part Sublayer, there is the Privacy Sublayer (see section 2.4.3).

2.4.1. Service Specific Convergence Sublayer (CS)

As shown in Figure 5, the CS is the first sublayer from the MAC layer. The sending CS is responsible for accepting higher layer MAC Service Data Units (SDU) coming through the CS Service Access Point (SAP) and classifying them to the appropriate CID. The classifier is a set of packet matching criteria applied to each packet. It consists of some protocol-specific fields, such as IP and MAC addresses, a classifier priority and a reference to a particular CID. Each connection has a specific service flow associated providing the necessary QoS requirements for that packet. If no classifier is found for a specific packet, a specific action must be taken. Since the classifier implementation is vendor dependent, the chosen decision is taken by the vendor. For instance, the packet can be discarded, sent on a default connection, or a new connection can be established for it, if enough resources are available. Finally, the CS PDU is delivered to the MAC CPS through the MAC SAP and delivered to the peer MAC CPS. Downlink classifiers are applied by the BS and uplink classifiers are applied by the SS, as shown in Figure 6 and Figure 7, respectively.

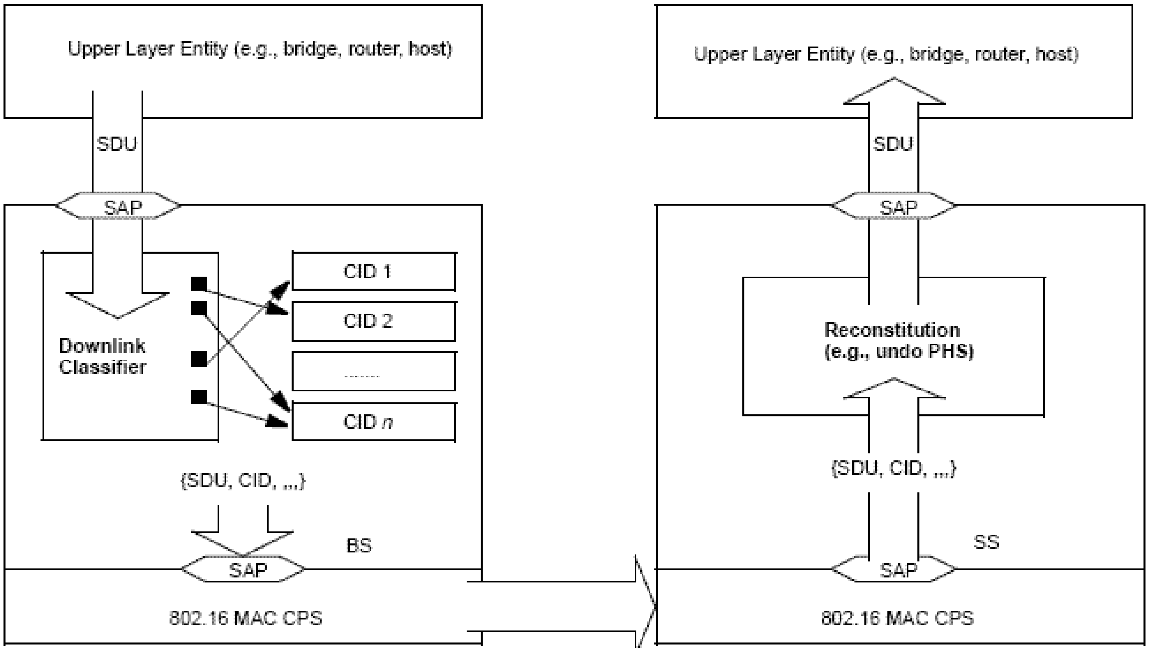
Upper Layer Entity (e.g., bridge, router, host)
SDU
SAP
Downlink Classifier
CID 1
CID 2
....
CID n
{SDU, CID, ,,,}
SAP
BS
802.16 MAC CPS
Upper Layer Entity (e.g., bridge, router, host)
SDU
SAP
Reconstitution (e.g., undo PHS)
{SDU, CID, ,,,}
SS
SAP
802.16 MAC CPS

Figure 6: Downlink classification process

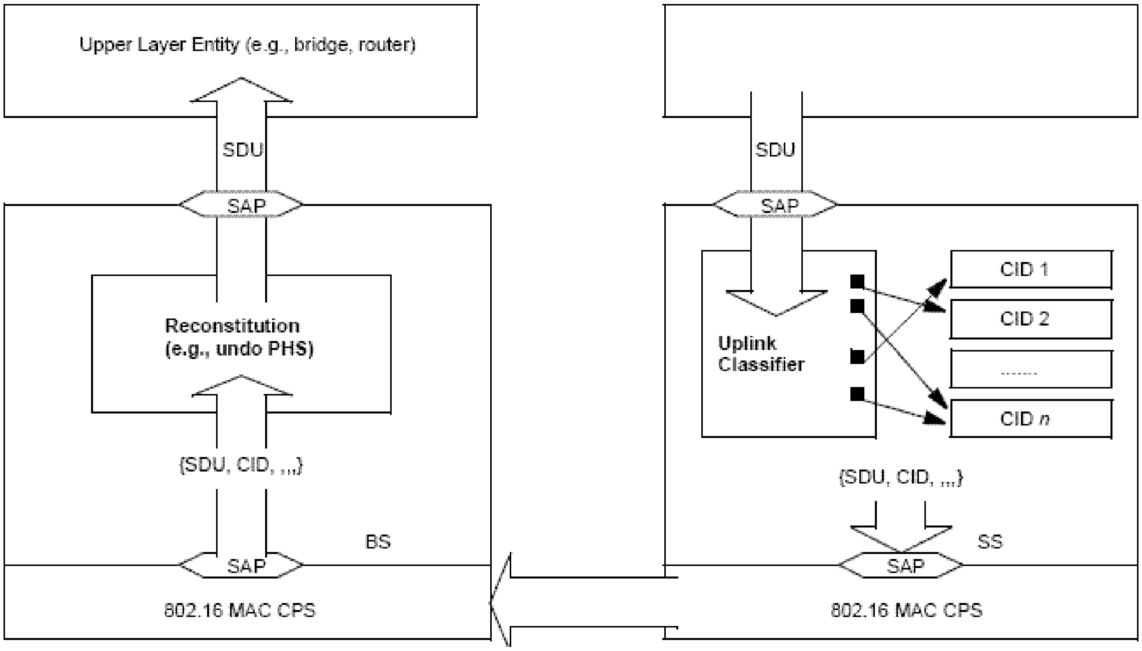

Figure 7: Uplink classification process

The standard defines two general CSs for mapping services to and from the 802.16-2004 MAC connections: the packet-convergence sublayer and the ATM convergence sublayer. The packet-convergence sublayer is defined to support packet-based protocols, and the ATM convergence sublayer is defined to support cell-based protocols.

2.4.2. Common Part Sublayer (CPS)

The CPS is the second sublayer from the MAC layer. It receives packets arriving from the upper sublayer (CS) and it is responsible for a set of functions, such as addressing, construction and transmission of the MAC PDUs, implementing the uplink scheduling services, bandwidth allocation, request mechanisms, contention resolution, among others. The 802.16-2004 MAC is connection oriented since all services are mapped to a connection. Associated with each connection is a service flow (SF). Service flows provide a mechanism for uplink and downlink QoS management.

2.4.2.1. Connections

The SSs are identified by a 48-bit MAC address: the SS MAC address is important during the initial ranging and authentication processes. However, after these processes, the primary addresses used by the system are the connection identifiers. This means that all the remaining tasks from the 802.16-2004 MAC layer, such as requesting bandwidth or providing the QoS mechanisms, are performed based on a connection. As already mentioned in section 2.2, a connection is a unidirectional mapping between the BS and the SS identified by a CID.

During the SS initialization process, three pairs of management connections are established between the BS and the SS: the basic connection, the primary management connection and the secondary management connection. Since each connection provides a different level of QoS, it is easily understood that the three management connections reflect three different QoS requirements for management traffic. The basic connection is used for the transfer of short, time-critical MAC management messages. The primary management connection is used to transfer longer, more delay tolerant management messages. The secondary management connection is used to transfer delay tolerant, standard-based management messages such as Dynamic Host Configuration Protocol (DHCP) [rfc2131] [rfc2132] [rfc3315], Trivial File Transfer Protocol (TFTP) [rfc1350] [rfc2349] and Simple Network Management Protocol (SNMP) [rfc1157] [rfc1441].

Besides the three pairs of management connections, another group of connections is also defined: the broadcast management connection, the multicast polling connection and the transport connection. The broadcast connection is configured by default and is used to transmit MAC management messages to all the SSs. It is important to mention that this broadcast connection is only used for management messages and not for data messages. A multicast polling connection is used by the SSs to join multicast polling groups, allowing them to request bandwidth via polling. Finally, to satisfy the contracted services, transport connections are allocated.

2.4.2.2. MAC PDU Format

The MAC PDU format is depicted in Figure 8. It consists of a fixed-length header, a variable length payload and an optional Cyclic Redundancy Check (CRC). The fixed length header contains the Generic MAC header or the Bandwidth Request header. The payload consists of zero or more subheaders and zero or more MAC SDUs.

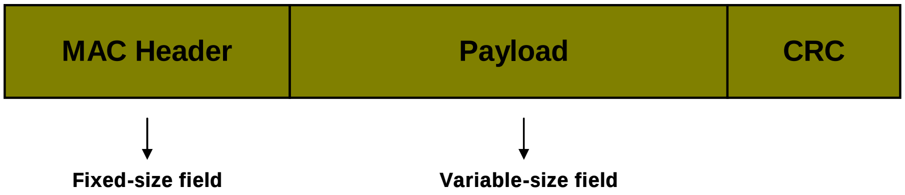

Figure 8: MAC PDU format

Depending on the type of MAC header that is being used, two types of MAC PDUs may exist:

- Generic MAC PDU: uses the Generic MAC header; requires the Payload and the CRC. In this case, the CRC is calculated based on the Generic MAC Header and on the Payload.
- Bandwidth Request PDU: uses the Bandwidth Request header; in this case, nor the payload nor the CRC are required for the PDU. Therefore, the Bandwidth Request header is unprotected.

2.4.2.3. MAC Header

The two possible MAC headers are shown in the next table (Table 1).

Syntax	Size	Notes
MAC Header() {		
HT	1 bit	**Header Type** 0 = Generic MAC header 1 = Bandwidth Request Header
EC	1 bit	**Encryption Control** If (**HT** = 0) then (**EC** = 1)
if (HT = 0) {		Generic MAC Header
Type	6 bits	Indicates included subheaders
Reserved	1 bit	Shall be set to zero
CI	1 bit	**CRC Indicator**
EKS	2 bits	**Encryption Key Sequence**
Reserved	1 bit	Shall be set to zero
LEN	11 bits	**Length**
}		
else {		Bandwidth Request header
Type	3 bits	Bandwidth Request Type
BR	19 bits	**Bandwidth Request**
}		
CID	16 bits	**Connection Identifier**
HCS	8 bits	**Header Check Sequence**
}		

Table 1: MAC header format

The fields from the MAC header shown in Table 1 will be described in the following sections.

2.4.2.3.1 Generic MAC Header

The Generic MAC header is used to transport CS data or MAC management messages. The **Header Type (HT)** field differentiates between the Generic MAC header and the Bandwidth Request header. For the Generic MAC header, the **HT** is set to 0. The **Encryption Control (EC)** field indicates if the payload is encrypted (set to 1) or not (set to 0). The **Type** field indicates the presence of subheaders. The presence or absence of the CRC is indicated through the **CRC Indicator (CI)** field. The **Encryption Key Sequence (EKS)** field is only meaningful if the **EC** is set to one, indicating that the MAC PDU payload is encrypted. The **EKS** indicates the index of the Traffic Encryption Key (TEK) and Initialization Vector (IV) used to encrypt the payload. The length (in bytes) of the MAC PDU, including the MAC header, is indicated by the **Length (LEN)** field. To detect errors in the MAC header, the **Header Check Sequence (HCS)** field is used. The transmitter must calculate the **HCS** value for the first five bytes and insert it in the **HCS** field. Finally, the **Connection Identifier (CID)** is also present.

2.4.2.3.2 Bandwidth Request Header

The Bandwidth Request header is used to request additional bandwidth. In this type of MAC header, the payload is not present in the MAC PDU, and then, the Bandwidth Request header must have a fixed value of bytes. In this case, the **Header Type (HT)** field is set to 1 indicating a Bandwidth Request header. The **Encryption Control (EC)** field is also present as in the Generic MAC header case, but since there is no payload in this situation, this field is always set to zero. The **Type** field indicates whether the bandwidth request is incremental or aggregate. Finally, the **Bandwidth Request (BR)** field indicates the number of uplink bytes requested by the CID indicated in the **Connection Identifier (CID)** field.

2.4.2.4. MAC Subheaders

When necessary, extra information can be carried in the MAC PDUs. To achieve this, MAC subheaders are used. Two main types of MAC subheaders are defined: the per-PDU and per-SDU subheaders. The per-PDU subheaders are used only once in each MAC PDU and inserted following the Generic MAC Header. The per-SDU subheaders are used several times in each MAC PDU, but only once for each MAC SDU. It must be inserted before each MAC SDU.

The Fragmentation subheader and the Grant Management subheader are two of the possible per-PDU MAC subheaders, whereas the Packing subheader is the only per-SDU subheader. The per-PDU subheaders must always precede the per-SDU subheaders in the MAC PDU. Among the several existing subheaders, we just briefly describe the Grant Management subheader.

The Grant Management subheader is used by the SS to tell the BS about its bandwidth needs.

Syntax	Size	Notes
Grant Management Subheader() {		
if (scheduling type == UGS) {		UGS scheduling service
SI	1 bit	**Slip Indicator**
PM	1 bit	**Poll-Me**
Reserved	14 bits	Shall be set to zero.
}		
else {		Non-UGS scheduling service
PBR	16 bits	**PiggyBack Request**
}		
}		

Table 2: Grant management subheader format

As we can see in Table 2, this subheader format depends on the type of uplink scheduling service that is being used. When using the UGS uplink scheduling service, the **Slip Indicator (SI)** bit is set to 1 and indicates that the service flow has exceeded its transmit queue depth. The **Poll-Me (PM)** bit is used by the SS to request a bandwidth poll to non-UGS connections. Finally, in non-UGS connections, the **PiggyBack Request (PBR)** field is used by the SS to specify the number of uplink bytes requested.

2.4.2.5. MAC Management Messages

The MAC management messages are carried in the payload of the MAC PDU. These messages, as shown in Figure 9, are composed by the MAC management message Type and by MAC management message Payload.

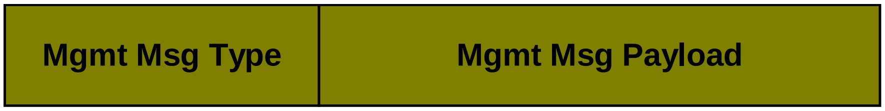

Figure 9: MAC management message format

In the following sections, we will depict some of the most important MAC management messages, such as:

- Downlink Channel Descriptor (***DCD***)
- Downlink Map (***DL-MAP***)
- Uplink Channel Descriptor (***UCD***)
- Uplink Map (***UL-MAP***)
- Dynamic Service Addition Request (***DSA-REQ***)
- Dynamic Service Addition Response (***DSA-RSP***)
- Dynamic Service Addition Acknowledgement (***DSA-ACK***)
- Dynamic Service Change Request (***DSC-REQ***)
- Dynamic Service Change Response (***DSC-RSP***)
- Dynamic Service Change Acknowledgment (***DSC-ACK***)
- Dynamic Service Deletion Request (***DSD-REQ***)

- Dynamic Service Deletion Response (***DSD-RSP***)

2.4.2.5.1 Downlink Channel Descriptor (DCD)

The Downlink Channel Descriptor (***DCD***) MAC management message must be periodically transmitted by the BS to define the downlink channel characteristics. The following table (Table 3) shows the ***DCD*** message format.

Syntax	Size	Notes
DCD Message Format() {		
Type = 1	8 bits	Message Type
Downlink Channel ID	8 bits	
Configuration Change Count	8 bits	
TLV Encoded information	variable	
Begin PHY Specification {		
for (i=1; i<=n; i++){		n is the number of downlink bursts
Downlink_Burst_Profile		PHY specific
}		
}		
}		

Table 3: DCD message format

The **Downlink Channel ID** is used as an identifier for the downlink channel. The **Configuration Change Count** is incremented by the BS when the ***DCD*** message parameters are different from the last message. This way, the SS, by reading this field, is capable to recognize if the remaining parameters are different from the previously received ***DCD*** message. The remaining parameters from the ***DCD*** message are encoded in a Type-Length-Value (TLV) form. Among the encoded values, we emphasize the **Downlink_Burst_Profile** encoding, which is common to all PHY specifications. The **Downlink_Burst_Profile** is a TLV encoding that associates with a particular Downlink

Interval Usage Code (DIUC) the downlink transmission properties, such as the modulation type and Forward Error Correction (FEC) code.

2.4.2.5.2 Downlink Map (DL-MAP)

The Downlink Map (***DL-MAP***) MAC management message must be periodically transmitted by the BS to define the access to the downlink information. Table 4 illustrates the ***DL-MAP*** message format.

Syntax	Size	Notes
DL-MAP Message Format() {		
Type = 2	8 bits	Message Type
PHY Synchronization	variable	PHY specific
DCD Count	8 bits	
Base Station ID	48 bits	
Begin PHY Specification {		
for (i=1; i<=n; i++){		n is the number of downlink bursts
DL-MAP_IE()	variable	PHY specific
}		
}		
}		

Table 4: DL-MAP message format

The **DCD Count** matches the **Configuration Change Count** parameter from the ***DCD*** message. The **Base Station ID** is a 48-bit long field identifying the BS. The encoding of the remaining portions of the ***DL-MAP*** message is carried in Information Elements (**DL-MAP_IE**). Each DL-MAP Information Element (**DL-MAP_IE**) is used to specify one downlink burst. It indicates the start time, in units of symbol duration, of the downlink burst associated with this **DL-MAP_IE**, including the preamble. To indicate the end of the last allocated burst, an **End of Map** burst (DIUC = 14) with zero duration is used. A **DIUC** is also used to identify the downlink burst associated with the **DL-MAP_IE**.

2.4.2.5.3 Uplink Channel Descriptor

The Uplink Channel Descriptor (***UCD***) MAC management message must be periodically transmitted by the BS to define the uplink channel characteristics. The following table illustrates the ***UCD*** message format.

Syntax	Size	Notes
UCD Message Format() {		
Type = 0	8 bits	Message Type
Configuration Change Count	8 bits	
Ranging Backoff Start	8 bits	
Ranging Backoff End	8 bits	
Ranging Request Start	8 bits	
Ranging Request End	8 bits	
TLV Encoded information	variable	
Begin PHY Specification {		
for (i=1; i<=n; i++){		n is the number of uplink bursts
Uplink_Burst_Profile		PHY specific
}		
}		
}		

Table 5: UCD message format

The **Ranging Backoff Start** and the **Ranging Backoff End** parameters specify the initial and the final backoff window size for initial ranging contention, respectively. The **Request Backoff Start** and the **Request Backoff Final** parameters indicate the initial and the final backoff window size for contention bandwidth requests, respectively.

Likewise in the ***DCD*** MAC management message, the remaining parameters from the ***UCD*** message are encoded in a TLV form. One of the encoded values, common to all PHY specifications, is the **Uplink_Burst_Profile**. The **Uplink_Burst_Profile** associates the uplink transmission properties, such as the modulation type and FEC code, to a specific Uplink Interval Usage Code (UIUC).

2.4.2.5.4 Uplink Map (UL-MAP)

The Uplink Map (***UL-MAP***) MAC management message must be periodically transmitted by the BS to define the access to the uplink information. The ***UL-MAP*** message format is demonstrated in Table 6.

Syntax	Size	Notes
UL-MAP Message Format() {		
Type = 3	8 bits	Message Type
Uplink Channel ID	8 bits	
UCD Count	8 bits	
Allocation Start Time	32 bits	
Begin PHY Specification {		
for (i=1; i<=n; i++){		n is the number of uplink bursts
UL-MAP_IE()	variable	PHY specific
}		
}		
}		

Table 6: UL-MAP message format

The **Uplink Channel ID** is the identifier of the uplink channel. The **UCD Count** is used to match the value of the Configuration Change Count of the ***UCD*** message. The **Allocation Start Time** indicates the start time of the uplink allocation defined by the ***UL-MAP***. The remaining parameters of the ***UL-MAP*** message are carried in Information

Elements (**UL-MAP_IE**). Each **UL-MAP_IE** indicates the start time of the uplink burst and its duration.

Several IEs can be used by the BS in the ***UL-MAP*** message to allocate uplink time intervals to the SSs in the uplink subframe. The **Request IE** is used by the BS to allocate an uplink interval in which the SSs may send bandwidth request PDUs. When using the Basic CID of the SS, this request is allocated to that specific SS. On the other hand, if the multicast/broadcast CID is used, the SSs will have to contend to send the bandwidth request PDUs. The BS uses the **Initial Ranging IE** to allocate an uplink interval during which new SSs may join the network. This period of time will be used by the SSs to send a ***RNG-REQ*** message to the BS, after contention. Finally, the **Data Grant IE** is used by the BS to provide an opportunity for a specific SS to transmit uplink PDUs.

2.4.2.5.5 Dynamic Service Addition (DSA)

The Dynamic Service Addition (***DSA***) set of messages are used to create a new service flow. ***DSA*** includes Request (***DSA-REQ***), Response (***DSA-RSP***) and Acknowledgment (***DSA-ACK***) MAC management messages.

The ***DSA-REQ***, illustrated in Table 7, is used by the BS or the SS to create a new service flow.

Syntax	Size	Notes
DSA-REQ Message Format() {		
Type = 11	8 bits	Message Type
Transaction ID	16 bits	
TLV Encoded Information	32 bits	
}		

Table 7: DSA-REQ message format

The **Transaction ID** parameter is used to uniquely identify the service flow creation process between the BS and the SS. The remaining parameters are coded as TLV tuples. For instance, the **Service Flow Parameters** are coded as a TLV tuple. They specify the service flow's traffic characteristics and scheduling requirements. The **Convergence Sublayer Parameters** specify the service flow's CS specific parameters. The service flow creation process can be triggered by the BS (BS-Initiated) or by the SS (SS-Initiated). In the BS-Initiated case, the ***DSA-REQ*** message is sent by the BS to the SS, including the CID and the Service Flow Identifier (SFID). In the SS-Initiated case, the ***DSA-REQ*** message is sent by the SS to the BS without including the CID or the SFID.

The ***DSA-RSP*** is sent by the BS or SS as a response to a received ***DSA-REQ*** message. It includes a **Confirmation Code** to confirm the correction reception of the ***DSA-REQ*** message. The ***DSA-ACK*** message is sent by the BS or SS as a response to a received ***DSA-RSP*** message.

2.4.2.5.6 Dynamic Service Change (DSC)

The Dynamic Service Change (***DSC***) set of MAC management messages is used to change a previously allocated service flow. ***DSC*** includes Request (***DSC-REQ***), Response (***DSC-RSP***) and Acknowledgment (***DSC-ACK***) MAC management messages.

The ***DSC-REQ***, illustrated in Table 8, is used by the BS or the SS to change a previously allocated service flow.

Syntax	Size	Notes
DSC-REQ Message Format() {		
Type = 14	8 bits	Message Type
Transaction ID	16 bits	
TLV Encoded Information	variable	
}		

Table 8: DSC-REQ message format

The **Transaction ID** parameter is used to uniquely identify the service flow modification process between the BS and the SS. The remaining parameters are coded as TLV tuples. For instance, the **Service Flow Parameters** are coded as a TLV tuple, including the

SFID. It specifies the new service flow's traffic characteristics for the previously allocated service flow.

The ***DSC-RSP*** MAC management message is used as a response to a received ***DSC-REQ*** message.

The ***DSC-ACK*** MAC management message is sent by the BS or SS as a response to a received ***DSC-RSP*** message.

2.4.2.5.7 Dynamic Service Deletion (DSD)

The Dynamic Service Deletion Request (***DSD-REQ***) and Response (DSD-RSP) MAC management message are used by the BS or the SS to delete a previously allocated service flow. The ***DSD-REQ*** message format is illustrated in Table 9.

Syntax	Size	Notes
DSD-REQ Message Format() {		
Type = 17	8 bits	Message Type
Transaction ID	16 bits	
Service Flow ID	32 bits	
TLV Encoded Information	variable	
}		

Table 9: DSD-REQ message format

The **Transaction ID** parameter is used to uniquely identify the service flow deletion process between the BS and the SS. The **Service Flow ID** indicates the service flow that must be deleted. The remaining parameters are coded as TLV tuples.

2.4.2.6. Scheduling Services

The scheduling services specify the policy used by the BS and the SSs to manage the poll and grant processes. Four scheduling services are defined to meet the QoS needs of the data flows carried over the air link in the upstream direction. The scheduling service is associated to each connection at connection setup time and, as a consequence, associated to a service flow.

The defined uplink scheduling services are the following:

- Unsolicited Grant Service (UGS)
- Real-Time Polling Service (rtPS)
- Non-Real-Time Polling Service (nrtPS)
- Best Effort (BE)

2.4.2.6.1 Unsolicited Grant Service (UGS)

The Unsolicited Grant Service (UGS) is designed to support real-time service flows that generate fixed size data packets on a periodic basis, such as VoIP. The service offers fixed size unsolicited data grants (transmission opportunities) on a periodic basis. This eliminates the latency and overhead of requiring the SS to send requests for transmission opportunities, and assures that grants are available to meet the flow's real-time needs. Briefly, Data Grant Burst IEs are provided by the BS to the SSs at periodic intervals based on the Maximum Sustained Traffic Rate of the service flow. In this type of scheduling service, the SS is not allowed to use any contention request opportunities. The key parameters for UGS service flows are the following: Maximum Sustained Traffic Rate (equal to the Minimum Reserved Traffic Rate), Maximum Latency, Tolerated Jitter and the Request/Transmission Policy.

2.4.2.6.2 Real Time Polling Service (rtPS)

The Real-Time Polling Service (rtPS) is designed to support real-time service flows that generate variable size data packets on a periodic basis, such as moving pictures experts group (MPEG) video or streaming video. The service offers real-time, periodic, unicast request opportunities, which meet the flows real-time needs and allow the SS to specify the size of the desired grant. In this case, the SS is not allowed to use any contention request opportunities. The SS is periodically polled by the BS to its specific Basic CID to send a bandwidth request. The key parameters for rtPS service flows are the following:

Maximum Sustained Traffic Rate, Minimum Reserved Traffic Rate, Maximum Latency and the Request/Transmission Policy. Comparing to the UGS service, the rtPS requires more overhead but supports variable grant sizes.

2.4.2.6.3 Non Real Time Polling Service (nrtPS)

The Non-Real-Time Polling Service (nrtPS) is designed to support non-real-time service flows that require variable size data grants on a regular (but not strictly periodic) basis, such as high bandwidth FTP. The service offers unicast polls on a periodic basis but uses more space intervals then rtPS. This ensures that the flow receives request opportunities even during network congestion. Additionally, the SS should also be authorized to use contention request opportunities. The key parameters for nrtPS service flows are the following: Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Traffic Priority and the Request/Transmission Policy.

2.4.2.6.4 Best Effort (BE)

The Best Effort (BE) service is intended for traffic where no throughput or delay guarantees are provided. The SS sends requests for bandwidth in either random access slots or dedicated transmission opportunities. The occurrence of dedicated opportunities is subject to network load, and in contrast to the nrtPS, the SS cannot rely on their presence.

The following table (Table 10) shows the scheduling services and the poll/grant options of each one of them.

Scheduling Type	PiggyBack Request	Contention	Polling
UGS	Not allowed	Not allowed	PM bit is used to request a unicast poll for bandwidth needs of non-UGS connections
rtPS	Allowed	Allowed	Scheduling only allows unicast polling
nrtPS	Allowed	Allowed	Scheduling may restrict a service flow to unicast polling via the transmission/request policy; otherwise all forms of polling are allowed
BE	Allowed	Allowed	All forms of polling allowed

Table 10: Uplink scheduling services

2.4.2.7. Bandwidth Allocation and Request Mechanisms

In this section, we will depict the several mechanisms used by the 802.16-2004 SSs to perform bandwidth requests, as well as the mechanism used by the BS to grant the requested bandwidth. Additionally, the polling mechanisms used by the BSs will also be discussed.

2.4.2.7.1 Bandwidth Request

The Bandwidth Request mechanism is used by the SS to indicate to the BS that it needs to allocate more bandwidth in the uplink direction. This mechanism is always done on a connection basis. A bandwidth request may be done using the Bandwidth Request header, as depicted in section 2.4.2.3.2, or using a PiggyBack Request through the usage of a Grant Management subheader. The request must be done in terms of the number of bytes needed for the MAC header and payload, but not taking into account the PHY overhead. The bandwidth request can be incremental or aggregate. When the BS receives an aggregate bandwidth request, it should replace its perception of the bandwidth needs of the connection with the quantity of bandwidth requested. On the other hand, when the BS receives an incremental bandwidth request, it should add the quantity of the bandwidth requested by the SS with its perception of bandwidth needs of the connection. The Bandwidth Request PDU may be transmitted during either the Request IE or during the Data Grant IE, as depicted in section 2.4.2.5.4.

2.4.2.7.2 Bandwidth Grant

Opposite to the bandwidth request process, which is connection basis, the bandwidth grant is addressed to the SSs Basic CID, not to individual CIDs. Therefore, the SS scheduler must decide to which waiting transport CID the available bandwidth is going to be given. If the requested bandwidth is not granted to the SS, it may decide to perform backoff according to the ***UCD*** management message parameters and repeat the bandwidth request, or to discard the SDU.

2.4.2.7.3 Polling

The BSs use the polling process to allocate dedicated bandwidth in the uplink subframe for the SSs to request bandwidth. There is no explicit message sent by the BS to the SSs to perform polling. Several polling methods are available: unicast, multicast/broadcast and the Poll-Me bit. In all these, allocations for polling are done in the uplink subframe as indicated by the ***UL-MAP*** message.

In unicast polling, the allocations are done to individual SSs. In this case, the SS is polled by allocating a Data Grant Burst IE to its Basic CID. The Request IE to the SS Basic CID could also be used for unicast polling. However, it is usually not used in unicast polling to avoid that an SS has to transmit the bandwidth request PDU in a less robust burst profile. In this particular case, even if the SS is able to transmit in a higher burst profile, it has to use the Request IE burst profile.

In multicast/broadcast polling, the allocations are done for a group of SSs. In this case the Request IE to the multicast/broadcast CID must be used. In this case, if more the one SS is trying to send a bandwidth request PDU to the BS, they will collide and the contention resolution algorithm must be used.

The Poll-Me bit is set in a Grant Management subheader, indicating to the BS that the SS needs to be polled to request bandwidth for non-UGS connections. With this mechanism, SSs with UGS connections are not individually polled, unless the PM bit is set. This is useful to save bandwidth avoiding all the SSs to be individually polled.

Briefly summarizing, unicast polling is done on an SS basis by allocating a Data Grant IE to its Basic CID, whereas the multicast/broadcast polling is done through the usage of the Request IE to the multicast/broadcast CID. Finally, the PM bit is used by the SSs to indicate that extra bandwidth is required for non-UGS connections.

2.4.2.8. Network Entry and Initialization

The initial procedure for a SS to entry in the network can be described by the following steps:

- Scan for downlink channel and establish synchronization with the BS
- Obtain downlink and uplink parameters
- Perform ranging
- Negotiate basic capabilities
- Perform Registration
- Establish IP connectivity
- Establish Time of Day
- Establish Provisioned connections

2.4.2.8.1 Scan for downlink channel and establish synchronization

The 802.16-2004 MAC has an initialization procedure to eliminate the need for manual configuration. The SS stores the last channel used and tries to re-acquire this downlink channel. If this process fails, the SS has to scan the possible channels of the downlink frequency band of operation.

2.4.2.8.2 Obtain downlink and uplink parameters

During this phase, the SS has to maintain synchronization and obtain the downlink and uplink parameters. For the SS to be synchronized, a ***DL-MAP*** message must be periodically received. If the reception of a ***DL-MAP*** message fails, the SS looses synchronization with the BS.

After synchronization is achieved, the SS must periodically receive a ***DCD*** message to maintain synchronization. Additionally, this message is used by the SS to obtain the transmission parameters of the downlink channel – modulation and coding schemes. If one of these messages – ***DL-MAP*** and ***DCD*** – is not periodically received by the SS, a downlink channel must be re-scanned.

Likewise the downlink parameters, the uplink transmission parameters must also be acquired by the SS. When the synchronization process is completed, the SS must wait for a ***UCD*** message. After this process is completed, the SS will receive a ***UL-MAP*** message in each frame, which is responsible for the uplink bandwidth allocation.

2.4.2.8.3 Perform Ranging

After the SS is synchronized and the uplink transmission parameters are obtained by the SS, it shall read the ***UL-MAP*** message and try to find an Initial Ranging IE to transmit the Ranging Request (***RNG-REQ***) MAC management message to the BS. When an Initial Ranging IE is found, it will wait a ranging backoff period that is specified in the ***UCD*** message, and then the ***RNG-REQ*** message is sent to the BS using the Initial Ranging IE.

After the BS receives the ***RNG-REQ*** message, it calculates the timing advance value that the SS must use in uplink direction, and sends this information to the SS in the Ranging-Response (***RNG-RSP***) management message. The BS also sends power control information, as well as the CID for the basic management connection and the primary management connection. The BS, in its response, can deny the use of any capability reported by the SS. If the SS does not receive a response, the SS shall resend the ***RNG-REQ*** management message in the next Initial Ranging IE at a higher power level.

2.4.2.8.4 Negotiate Basic Capabilities

When the ranging process is completed, the SS sends an SS Basic Capability Request (***SBC-REQ***) message to the BS with its capabilities - physical parameters supported. The BS receives the message and sends an SS Basic Capability Response (***SBC-RSP***) management message to the SS with the intersection of the SSs capabilities and the BS capabilities.

2.4.2.8.5 Perform Registration

At this moment, the SS is not yet registered in the BS. For registration, the SS sends a Registration Request (***REG-REQ***) message to the BS. The BS responds with a Registration Response (***REG-RSP***) message which has the secondary management CID included. As a consequence, the SS becomes manageable.

2.4.2.8.6 Establish IP Connectivity

At this period of the initialization process, the SS will try to acquire an IP address. To configure an IP address, the DHCP protocol is used through the usage of the secondary management CID.

2.4.2.8.7 Establish Time of Day

For time-stamping management events, the SS and the BS must have the current date and time. The Time Protocol [rfc868], a simple request/response protocol is used to perform this task.

2.4.2.8.8 Establish Provisioned Connections

Finally, the BS must send ***DSA-REQ*** messages to the SS to setup connections for pre-provisioned service flows belonging to the SS. As a response, a ***DSA-RSP*** message is sent by the SS to the BS terminating the service flow allocation.

2.4.2.9. Service Flow Management

As depicted in section 2.3, three sublayers compose the MAC layer. In particular, the MAC CS and the MAC CPS sublayers are the main responsible for the service flow management process. To establish the communication between the MAC CS and the MAC CPS sublayers, a set of primitives have been defined. The communication is established through the MAC SAP allowing the creation, modification and deletion of service flows. Table 11 includes the defined primitives.

Service Flow	Primitives
Creation	*MAC_CREATE_CONNECTION.request* *MAC_CREATE_CONNECTION.indication* *MAC_CREATE_CONNECTION.response* *MAC_CREATE_CONNECTION.confirmation*
Modification	*MAC_CHANGE_CONNECTION.request* *MAC_CHANGE_CONNECTION.indication* *MAC_CHANGE_CONNECTION.response* *MAC_CHANGE_CONNECTION.confirmation*
Deletion	*MAC_TERMINATE_CONNECTION.request* *MAC_TERMINATE_CONNECTION.indication* *MAC_TERMINATE_CONNECTION.response* *MAC_TERMINATE_CONNECTION.confirmation*

Table 11: 802.16-2004 MAC SAP Primitives

A brief overview about the use of the primitives shown in Table 11 is illustrated in Figure 10.

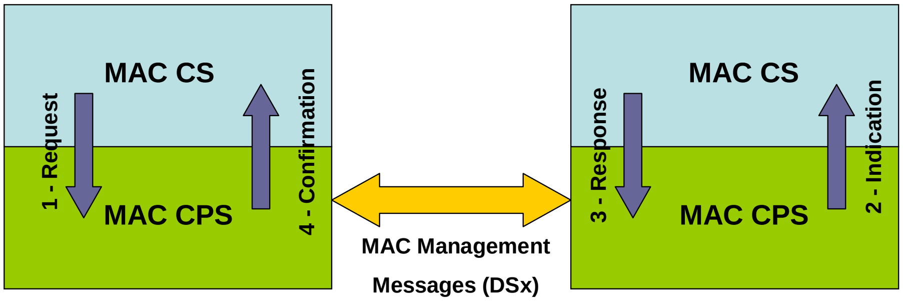

Figure 10: 802.16-2004 MAC SAP Primitives Flow

Initially, the MAC CS issues a *Request* primitive to the MAC CPS below. As a result, the corresponding DSx MAC management message is sent by the MAC CPS to the peer MAC. At the peer MAC, an *Indication* primitive is created by the MAC CPS and sent to the MAC CS. The MAC CS replies with a *Response* primitive to the MAC CPS. Consequently, the correspondent DSx MAC management message is sent to the MAC peer, triggering the *Confirmation* primitive to the MAC CS of the original requesting entity. The service flow creation, modification and deletion process will be described in the following sub-sections.

2.4.2.9.1 Service Flow Creation

The service flow creation process is used to establish a service flow between the BS and the SS with a set of QoS parameters, as well as a classification method. The service flow creation process is illustrated in Figure 11.

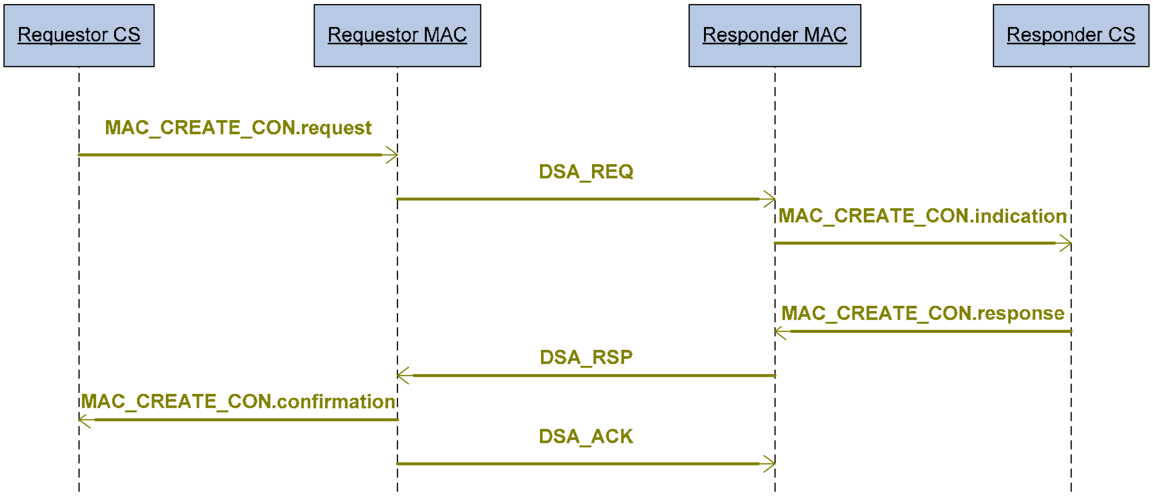

Figure 11: Service flow creation process

The Requestor CS sends a *MAC_CREATE_CONNECTION.request* primitive (see Table 11) to the Requestor MAC. This primitive carries, among other, the set of QoS parameters for the service flow, the CS used to classify the packets for this service flow and the uplink scheduling service. If the Requestor MAC is the BS (BS-Initiated service flow creation), the SFID and the CID for the new service flow are created at this stage. If the Requestor MAC is the SS (SS-Initiated service flow creation), the SFID and CID creation process will be delegated to the Responder MAC. Then, the Requestor MAC sends a ***DSA-REQ*** message to the Responder MAC. The Responder MAC triggers a *MAC_CREATE_CONNECTION.indication* primitive to the Responder CS to indicate the new service flow creation. If the service flow creation has been initiated by the SS, the actions of generating a SFID and a CID are done at this moment. After receiving the

MAC_CREATE_CONNECTION.response primitive from the Responder CS, the Responder MAC sends a ***DSA-RSP*** message to the Requestor MAC. The Request MAC, after receiving the ***DSA-RSP*** message, triggers a *MAC_CREATE_CONNECTION.confirmation* primitive to the Requestor CS. Finally, a ***DSA-ACK*** message is sent by the Requestor MAC to the Responder MAC.

2.4.2.9.2 Service Flow Modification

The service flow modification process is used to update the set of QoS parameters from a previously allocated service flow. The service flow modification process is illustrated in Figure 12.

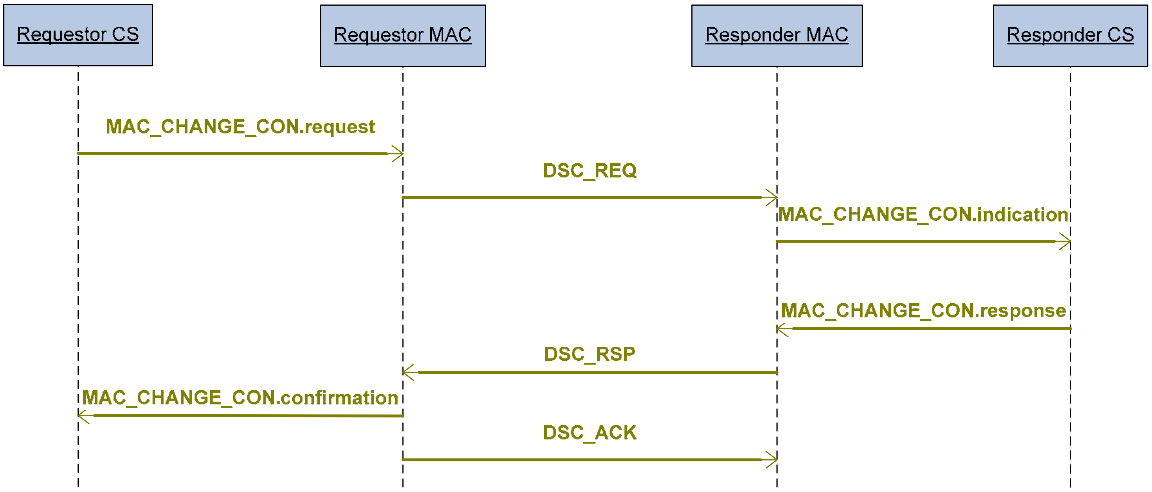

Figure 12: Service flow modification process

The service flow modification process is very similar to the service flow creation process depicted in section 2.4.2.9.1. The only difference is on the primitives that are used: in this case, the *MAC_CREATE_CONNECTION* (*request*, *indication*, *response* and *confirmation*) primitives are replaced by the *MAC_CHANGE_CONNECTION* (*request*, *indication*, *response* and *confirmation*) primitives as presented in Table 11. Besides the primitives, the MAC management messages are also different: instead of using ***DSA-REQ***, ***DSA-RSP*** and ***DSA-ACK***, the ***DSC-REQ, DSC-RSP*** and ***DSC-ACK*** management messages are used.

2.4.2.9.3 Dynamic Service Deletion

Finally, the service flow teardown is used to delete a previously allocated service flow and free its resources. The service flow deletion process is illustrated in Figure 13.

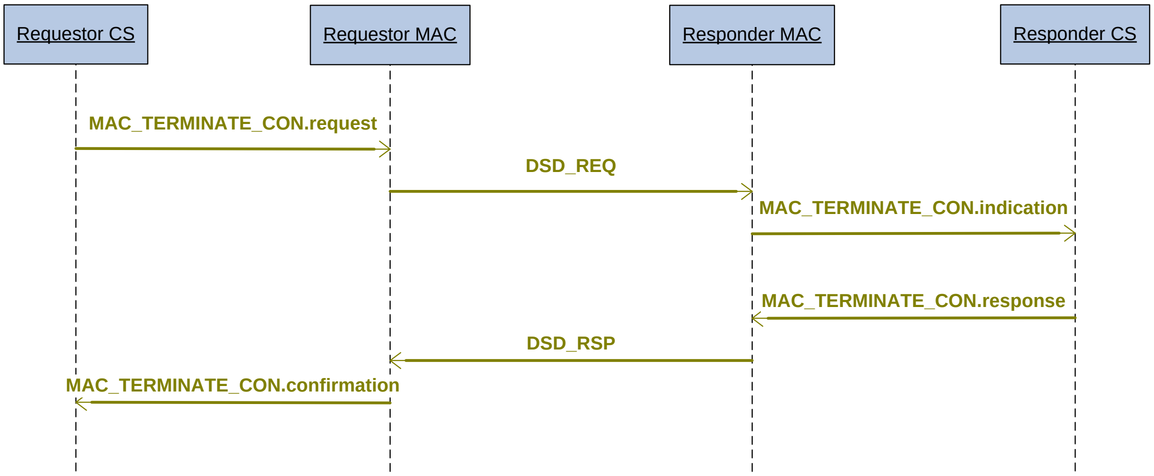
Requestor CS
Requestor MAC
Responder MAC
Responder CS
MAC_TERMINATE_CON.request
DSD_REQ
MAC_TERMINATE_CON.indication
MAC_TERMINATE_CON.response
DSD_RSP
MAC_TERMINATE_CON.confirmation

Figure 13: Service flow deletion process

Once again, this process is similar to the creation and to the service flow modification processes depicted in sections 2.4.2.9.1 and 2.4.2.9.2, respectively. In this case, the used primitives are *MAC_TERMINATE_CONNECTION* (*request, indication, response* and *confirmation*) and the used MAC management messages are ***DSD-REQ*** and ***DSD-RSP***.

2.4.2.10. Broadcast and Multicast Connections

Despite a range of multicast connections is defined for polling purposes, there is no multicast connection dedicated for data. To setup a multicast connection, the BS should setup a multicast group inside the 802.16 network. To accomplish this task, the BS starts to create and associate a unicast transport connection with a specific SS. Then, this same connection shall also be associated with all the SSs that belong to the multicast group. With this process, when multicast data is sent on this connection, all the SSs that belong to the multicast group will be able to decode it.

Figure 14 illustrates a multicast connection creation in the 802.16 network. Suppose a multicast group with four elements is created (1 laptop and 1 PDA in SS#1, 1 laptop and 1 PDA in SS#3). In this case, a unicast transport connection (CID1) is established between the BS and SS#1. After this connection is established, the BS will create a similar unicast transport connection with SS#3 using the same connection identifier (CID1). This way, SS#1 and SS#3 will both start decoding MAC PDUs that are sent with CID1. Thus, we have a multicast connection established between the BS, SS#1 and SS#3.

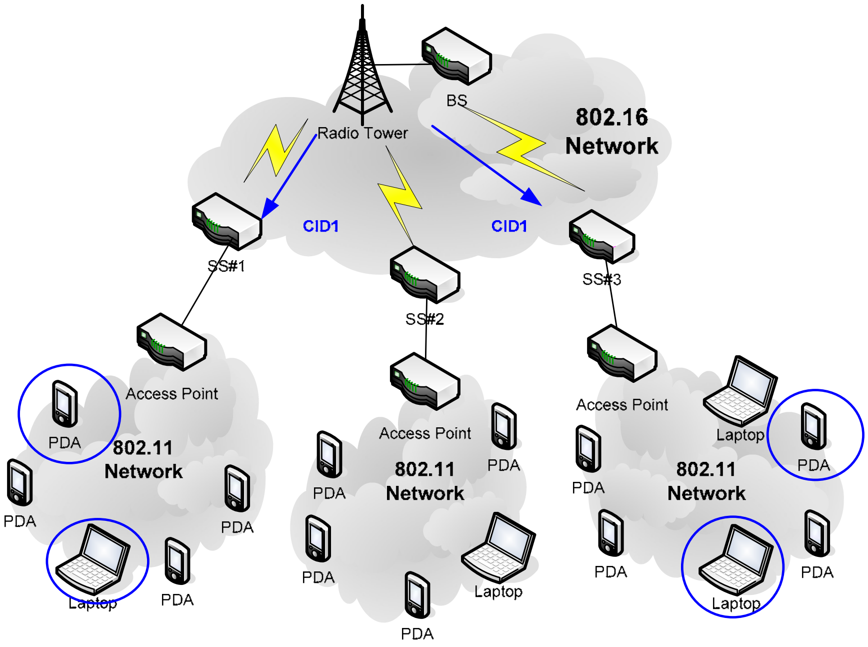

Figure 14: Multicast connection establishment

It is important to mention that an 802.16 multicast connection is only required if the multicast nodes belong to different SSs. This is the situation illustrated in Figure 14. However, if the multicast group elements belong to a single SS, no 802.16 multicast connection would be required in this case. A simple unicast connection would be enough to send data to the multicast group only formed inside the 802.11 network.

Regarding broadcast support, there is no specific CID for broadcast connections. There is a broadcast management CID which is not allowed to send data traffic through it. To create a broadcast connection, the process is the same used to create multicast connections, but it shall be expanded to all the SSs in the downlink channel.

2.4.3. Privacy Sublayer

The Privacy sublayer is the third and last sublayer from the MAC layer. This sublayer provides authentication and data encryption functions.

2.5. IEEE 802.16-2004 PHY Layer

The PHY layer is also defined in the 802.16-2004 standard. Both frequency and time division duplex techniques are defined in the standard. Adaptive burst profiling, including the modulation and coding schemes can be individually adjusted to each SS on a frame-by-frame basis. Several modulation techniques, such as Quadrature Phase Shift Keying (QPSK), 16-state Quadrature Amplitude Modulation (16-QAM) and 64-QAM, are supported, allowing the formation of varying robustness and efficient burst profiles. In this section, besides depicting the Frequency Division Duplex (FDD) and the Time Division Duplex (TDD) techniques, we will also give a brief overview about the different physical layers supported in the standard as well as the downlink and uplink subframes format.

2.5.1. Frequency Division Duplex

When the FDD technique is used, two separate frequency channels are allocated: one uplink channel and one downlink channel. As a consequence of using the FDD technique, full-duplex SSs (can transmit and receive simultaneously) and half-duplex SSs (cannot transmit and receive simultaneously) are supported. The frames duration (uplink and downlink) is fixed, allowing the utilization of different modulation techniques.

2.5.2. Time Division Duplex

When the TDD duplex technique is used, the uplink and the downlink use the same frequency channel. In this case, the uplink and the downlink transmissions must occur in different periods of time sharing the same frequency channel. As a consequence of using this duplex technique, the SSs work in half-duplex. As in the FDD case, the frame has a fixed duration. However, this frame is divided in two subframes. One subframe is used for the uplink transmission and the other subframe is used for the downlink transmission. PS (Physical Slot) is the unit used to divide the TDD frame. This duplex technique is adaptive because the bandwidth allocated to the downlink and to the uplink can vary depending on the needs. The TDD technique is illustrated in the next picture.

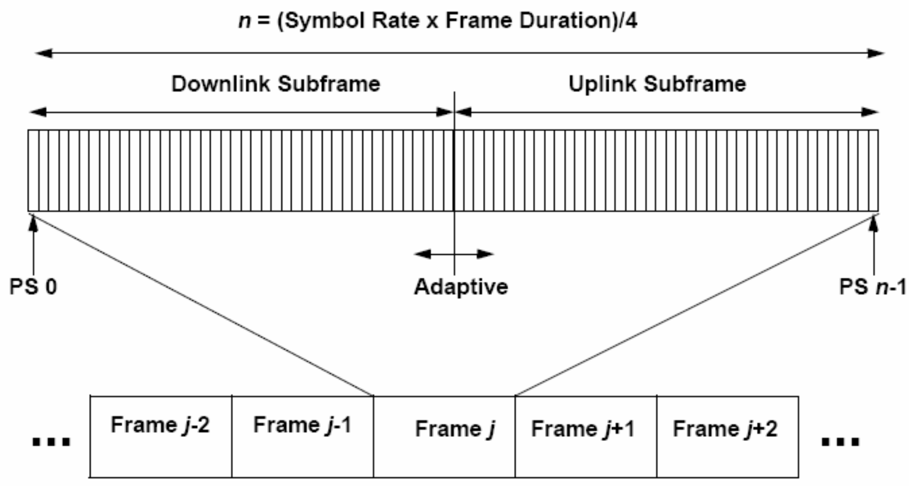

Figure 15: TDD duplex technique

2.5.3. Supported PHY Layers

The 802.16-2004 physical layer supports two different frequency bands. They are:

- 10 – 66 GHz licensed bands (**WirelessMAN-SC**).
- 2 – 11 GHz licensed bands (**WirelessMAN-SCa**, **WirelessMAN-OFDM**, **WirelessMAN-OFDMA**).

The 10 – 66 GHz licensed bands provide a physical environment in which, due to the short wavelength, LOS environment is required. The channels bandwidth used in this physical environment are usually large (25 or 28 MHz). The 10 – 66 GHz licensed bands provide transmission rates of 120 Mbit/s, being a good option for PMP access in LOS environments. This single-carrier modulation air interface is known as **WirelessMAN-SC** air interface.

The 2 – 11 GHz licensed bands provide a physical environment where, due to the longer wavelength, LOS environment is not necessary. By supporting NLOS scenarios, it requires additional PHY functionalities. It provides lower transmission rates (75 Mbit/s) when compared to the 10 – 66 GHz, but it does not require a LOS environment. Three air interfaces are defined in this frequency band:

- **WirelessMAN-SCa**: single carrier air interface.
- **WirelessMAN-OFDM**: multi-carrier air interface using Orthogonal Frequency Division Multiplexing (OFDM) [litofdm] with 256 carriers.
- **WirelessMAN-OFDMA**: multi-carrier air interface using Orthogonal Frequency Division Multiple Access (OFDMA) with 2048 carriers.

2.5.4. Overall TDD Frame Structure

The overall TDD frame structure will be analyzed in this section. In particular, section 2.5.4.1 depicts the downlink subframe structure, whereas section 2.5.4.2 describes the uplink subframe structure. Figure 16 shows the TDD frame.

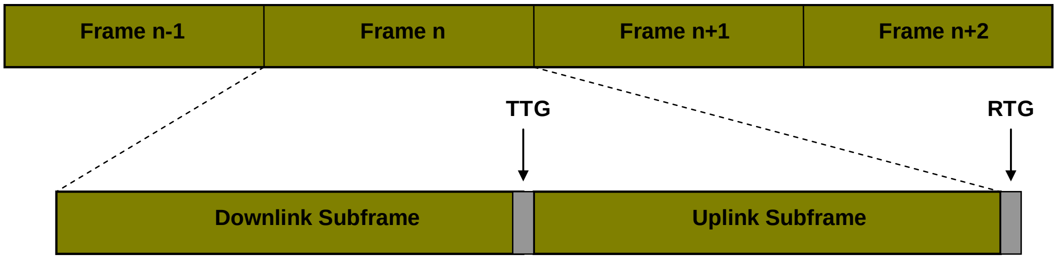

Figure 16: TDD frame structure

2.5.4.1. Downlink Subframe

When the TDD duplex technique is used, the structure of the downlink subframe is as shown in Figure 17.

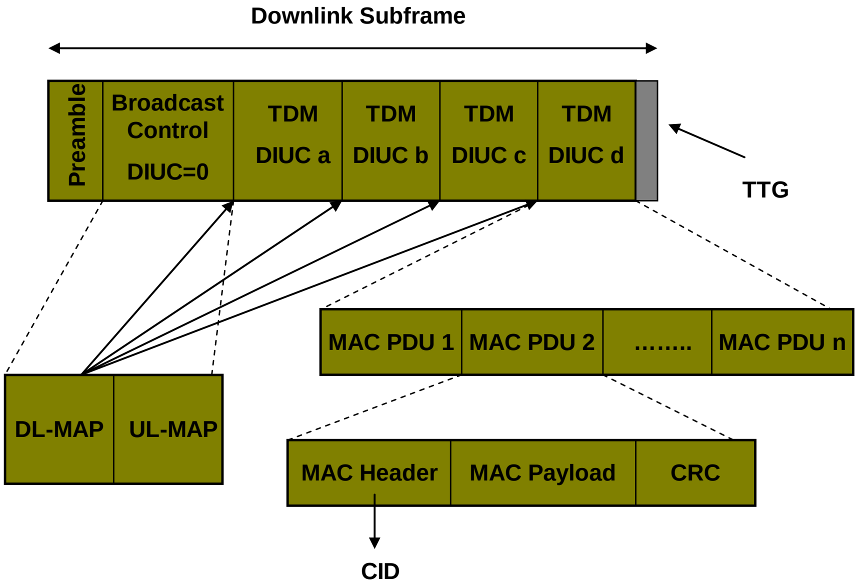

Figure 17: TDD downlink subframe structure

The downlink subframe is composed by a Preamble used for synchronization, followed by the Frame Control Header (FCH). The FCH contains the ***DL-MAP*** and the ***UL-MAP*** management messages, indicating the location and burst profile of each downlink and uplink burst, respectively. Moreover, it contains the downlink and uplink channel descriptors (***UCD*** and ***DCD*** messages). Following the FCH, starts the downlink data bursts section. Downlink bursts are transmitted in order of decreasing robustness – QPSK followed by 16-QAM and 64-QAM. The SSs listen to all bursts that it is capable to receive, including burst with profiles of equal or greater robustness that has been negotiated with the BS at connection setup time. Then, the SS analyses the MAC header of all the MAC PDUs inside each burst to check if the CID is destined to itself. At the end of the frame, the Transmit Transition Gap (TTG) is used to separate the downlink and the following uplink bursts. The TTG allows the SS to switch from receive mode to transmit mode.

2.5.4.2. Uplink Subframe

The uplink subframe is shown in Figure 18.

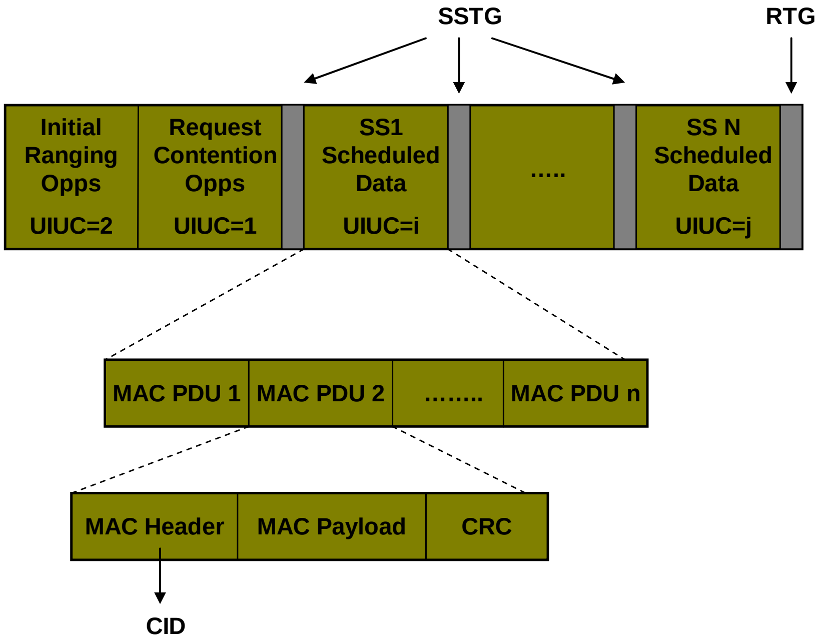

Figure 18: Uplink subframe structure

In the beginning of the uplink subframe there are two contention slots. The first contention slot is used by the SSs for initial ranging (Initial Ranging IE), whereas the second contention slot is used by the SSs to send bandwidth request PDUs to the BS (Request IE). The rest of the transmission slots are grouped by SSs. Each SS has a specific slot allocated for uplink transmission (Data Grant IEs). The Subscriber Station Time Gap (SSTG) is a time interval used to separate the transmissions of the various SSs during the uplink subframe.

2.6. IEEE 802.16e-2005 vs. IEEE 802.16-2004

The IEEE 802.16e-2005 standard, approved in December 2005, envisages the support of voice and data sessions at vehicular speeds up to 120 kilometres per hour. 802.16e-2005 standard is an amendment to the 802.16-2004 standard with a set of enhancements that provide an optimized solution for fixed and mobile broadband wireless access. Among these enhancements, we can find handoff mechanisms, power management functions, channel bandwidth scalability, frequency reuse and better NLOS performance. 802.16e-

2005 will give service providers that deploy an 802.16e-2005 network the possibility to also provide a fixed access to the end users.

The IEEE 802.16e-2005 frequency of operation is limited to licensed bands in the 2 – 6 GHz frequency band. Instead of using OFDM as in the 802.16-2004 standard, the 802.16e-2005 standard uses the Scalable OFDMA (S-OFDMA) technique supporting scalable channel bandwidths from 1.25 MHz to 20 MHz through the usage of different FFT sizes ranging from 128, 512, 1024 to 2048.

Even though OFDMA with 2048 FFTs was already specified in 802.16-2004, it was fixed, whereas S-OFDMA is variable, allowing several FFT sized to be used depending on the bandwidth. Therefore, 802.16e-2005 is not backward compatible with 802.16-2004. Moreover, to enable power conservation and to preserve the battery life for end user devices, power management functions, such as sleep and idle mode are implemented.

Regarding the uplink scheduling services, 802.16e-2005 defines an extra one when compared with 802.16-2004: Extended Real-Time Polling Service (ertPS). It is intended to support real-time services that generate variable size data packets on a periodic basis, such as VoIP with silence suppression. This scheduling mechanism is based on UGS and rtPS. Unicast grants are provided to the MNs in an unsolicited manner like in the UGS system, and therefore the latency of a bandwidth request message is saved. Instead of providing fixed allocations such as UGS, ertPS provides dynamics allocations. The size of the allocation can be changed by either using an extended PiggyBack request field on the Grant Management Subheader or using the bandwidth request PDU.

Table 12 briefly summarizes the main differences between the 802.16-2004 and 802.16e-2005 standards.

	802.16-2004	802.16e-2005
IEEE Approval	June 2004	December 2005
Frequency	2 GHz – 11 GHz	2 GHz – 6 GHz
Scheduling Services	UGS, rtPS, nrtPS, BE	UGS, rtPS, ertPS, nrtPS, BE
Subscribers	Fixed	Fixed / Mobile
Channel Conditions	LOS / NLOS	
Modulation	OFDM	S-OFDMA
Duplexing	TDD / FDD	
Sub-carrier Modulation	QPSK, 16-QAM, 64-QAM	
Data Rate	75 Mbps @ 20 MHz 18 Mbps @ 5 MHz	15 Mbps @ 5 MHz
Cell Range	50+ Km @ rural 15 Km @ urban	3 km @ indoor 5 km @ outdoor
Channel Bandwidth	1,25 MHz – 20 MHz	

Table 12: IEEE 802.16-2004 vs. IEEE 802.16e-2005

802.16-2004 cell range is about 20 km in rural areas and 2 to 5 km in urban areas, whereas in 802.16e-2005 the cell range is around 3 km indoor and 5 km outdoor. Data rates are higher in 802.16-2004 reaching the maximum of 75 Mbps using a 20 MHz channel bandwidth. In 802.16e-2005, with a 5 MHz channel bandwidth, data rates can reach 15 Mbps.

2.7. IEEE 802.16 Equipment Features – Redline Communications AN100

The IEEE 802.16 equipment (Redline Communications AN100) used for this work is compliant with the IEEE 802.16a-2003 version (see section 2.1) and has been acquired from Redline Communications [redcom]. It has a licensed test channel bandwidth of 7

MHz operating at 3.44 GHz, which provides around 24 Mbps of bit-rate in PMP mode. The antennas used for the tests were mounted on the roof of our premises.

Despite demonstrating a good radio performance, the equipment has a set of restrictions which can compromise its successful integration in our envisioned architecture. These restrictions are explained in the following subsections.

2.7.1. Convergence Sublayers

The 802.16 equipment is restricted in terms of available classification methods (Convergence Sublayers). Only two distinct methods are available for traffic classification in the equipment: classification based on the IPv4 protocol (IPv4 CS), or classification based on the MAC address of the MN (Ethernet [ieee802.3-02] CS), either the source (for the uplink traffic) or the destination (for the downlink traffic). Since our aim is to work in a next generation environment, IPv4 is not considered as a valid choice and thus we decided to use the Ethernet CS to perform classification in the 802.16 system. However, using the MN MAC address as the CS raises a service differentiation issue when several services are requested by the same MN.

2.7.2. Service Flow Management

Other major issue is the time taken to perform reservations in the 802.16 equipment. It takes approximately 11 seconds to perform a service flow reservation. Moreover, to modify a previously installed service flow, it takes up to 21 seconds. These high reservation times are not compliant with 4G environments, and a workaround must be found to solve this issue.

2.7.3. 802.16 Equipment Management Interface

SNMP interface has not been provided in time by the vendor. Therefore, reservations in the 802.16 equipment were done using a Hypertext Transfer Protocol (HTTP) [rfc1945] interface with the SS, locally or remotely. Remote reservations are done through the usage of the Access Router (AR) connected to the BS, and the local ones are done using the Access Point (AP) (in the two-hop scenario [see Figure 23]) or the Mobile Node (MN) (in the single-hop scenario [see Figure 22]), connected to the SS. The former mode has been dropped since it brought up access problems to the 802.16 equipment management interface when reservations were made simultaneously with ongoing traffic. In this case, the HTTP management interface stopped responding and connectivity with the 802.16 equipment was lost. Therefore, we decided to use the local mode to establish reservations through the usage of the AP (two-hop scenario) or the MN (single-hop scenario).

2.8. Summary

In this chapter we presented an overview of the IEEE 802.16 networks and their main characteristics. As explained, the 802.16 MAC layer is divided in three sublayers: the Service Specific Convergence Sublayer (CS), the Common Part Sublayer (CPS) and the Privacy Sublayer. The MAC layer is totally connection-oriented, even for connectionless protocols, such as IP. Therefore, a classification mechanism must be used to classify each of the incoming packets in the 802.16 system into one of its specific connections. This task is done by the CS, which classifies the incoming packets and delivers them to the correspondent connection. The CPS is responsible for the addressing and connection creation mechanisms, while the privacy sublayer is responsible for the security-related issues. In the PHY layer, two main groups are defined: the single carrier and the multi carrier physical layers. The multi carrier physical layer can use OFDM with 256 subcarriers or OFDMA technique provides 2048 subcarriers. In this case, NLOS environments are envisaged and the multipath effect should be taken into account.

The 802.16 equipment features and limitations have also been presented. For this specific equipment, we have been able to see that the service flow reservation and modification processes are not instantaneously, no IPv6 CS is provided and no SNMP interface is integrated. Therefore, Ethernet is adopted as the CS and an HTTP interface is used to interface with the equipment.

Chapter 3: IEEE 802.16 in 4G Environments

Ubiquitous Internet access is one of the biggest challenges for the telecommunications industry in the near future. Users access to the Internet all the time and everywhere is growing significantly in the current days and will be a requirement in next generation networks. This is very challenging for the operators that will have to find a way to provide broadband connectivity to the users, independently of their location. Additionally, the demand for high bandwidth services and applications will also be required. IEEE 802.16-2004, deeply explained in chapter 2, is an attractive solution for this type of next generation environments. It is a PMP technology, providing high throughputs, oriented for MANs. Built-in QoS functionalities through the usage of connections and unidirectional service flows between the BS and the SS is an important feature provided by this wireless technology.

The DAIDALOS project defines a next-generation network environment, where the seamless integration of heterogeneous network technologies is envisaged. The DAIDALOS architecture shall provide seamless QoS support, mobility, security and multicast, among other features. In order to achieve this, several European partners came together to define a modular architecture for QoS. It is important to stress that one of these partners was IT-Aveiro, which, in fact, had a relevant and active role in both layer 3 and layer 2 QoS architecture definition. One of the defined modules is the Abstraction Layer, which provides a generic interface to the upper layers and handles the technology independent functionalities. Moreover, it defines an interface for the technology specific modules, namely IEEE 802.11e, IEEE 802.16a and Time Division Code Multiple Access (TD-CDMA). These ones implement the technology related QoS functions. Network initiated and mobile node initiated handovers are also supported. The work carried out in this Thesis comprised the collaboration in the definition of the Layer 2 QoS architecture, the specification and implementation of the IEEE 802.16 QoS driver and the testing of the overall QoS architecture.

This chapter presents the DAIDALOS network architecture with emphasis on the QoS architecture and its integration with mobility. Section 3.1 provides a global overview of the DAIDALOS project, including the QoS and fast-mobility procedures in both the layer 3 and the layer 2. Section 3.2 presents one main module of the architecture – the QoS Abstraction Layer. A detailed explanation of this module is given, including the interfaces between the QoS Abstraction Layer and the layer 3 and layer 2 modules involved. Section 3.3 depicts the requirements that must be integrated for the 802.16 equipment to be fully supported in a real time and dynamic environment such as the DAIDALOS network. Finally, section 3.4 summarizes this chapter.

3.1. DAIDALOS Environment Overview

A brief description about the DAIDALOS environment is given in the following sections. The overview is focused on the QoS part of the architecture, as well as in the mobility process.

3.1.1. DAIDALOS Vision

DAIDALOS (**D**esigning **A**dvanced Network **I**nterfaces for the **D**elivery and **A**dministration of **L**ocation Independent, **O**ptimised Personal **S**ervices) is an Integrated Project funded by the European Commission, composed by 46 partners from industry and academia. Essentially, it addresses the seamless integration of heterogeneous network technologies, wired and wireless, allowing network operators and service providers to offer a wide range of new services to the end users. A global overview about the DAIDALOS vision is shown in the quotation given below.

> *"The project addresses the fact that mobility has become a central aspect of our lives in business, education, and leisure. It deals with rapid technological and societal changes with proliferating technologies and services that have resulted in complex and confusing communications environments for users and network operators. By rethinking fundamental technology and business issues, Daidalos targets usable and manageable communication infrastructures for the future. The goal is a seamless, pervasive access to content and services via heterogeneous networks that supports user preferences and context. The project will use a user-centric, scenario-based and operator-driven approach to effectively cover user and business needs."* [daid]

As an operator-driven project, DAIDALOS must ensure that the architecture provides the network operators with a set of mandatory features, such as network management, network monitoring, performance optimization, user recognition and service control. On the other hand, it must be user-centric, giving the users the capacity to make decisions. This duality requires a strong effort on the design of the architecture.

Since we are working in a next generation environment, a set of demand features are required for the architecture design, namely QoS, fast-mobility, security, multicast and broadcast. QoS is supported in the core network through the usage of *DiffServ* (Differentiated Services) [rfc2475] [rfc2474] [rfc2598], whereas in the access network, an *IntServ-like* (Integrated Services) [rfc1633] approach is used. Fast-mobility support is achieved through the usage of Mobile-IPv6 [rfc3775] and FHO concepts [nunomob], extended from those defined in [rfc4068]. Moreover, the architecture is IPv6 based and multicast-aware [rfc2710]. Broadcast services and security are also supported.

Another innovative concept introduced in the DAIDALOS architecture is the pervasiveness. A pervasive architecture allows the user to benefit from customized services, adapted to its individual preferences and specific context. This is inline with the user-centric concept of the architecture.

3.1.2. Global Architecture

The overall DAIDALOS architecture is significantly complex. In Figure 19 we depict at a high level, a very simple view of the DAIDALOS main components.

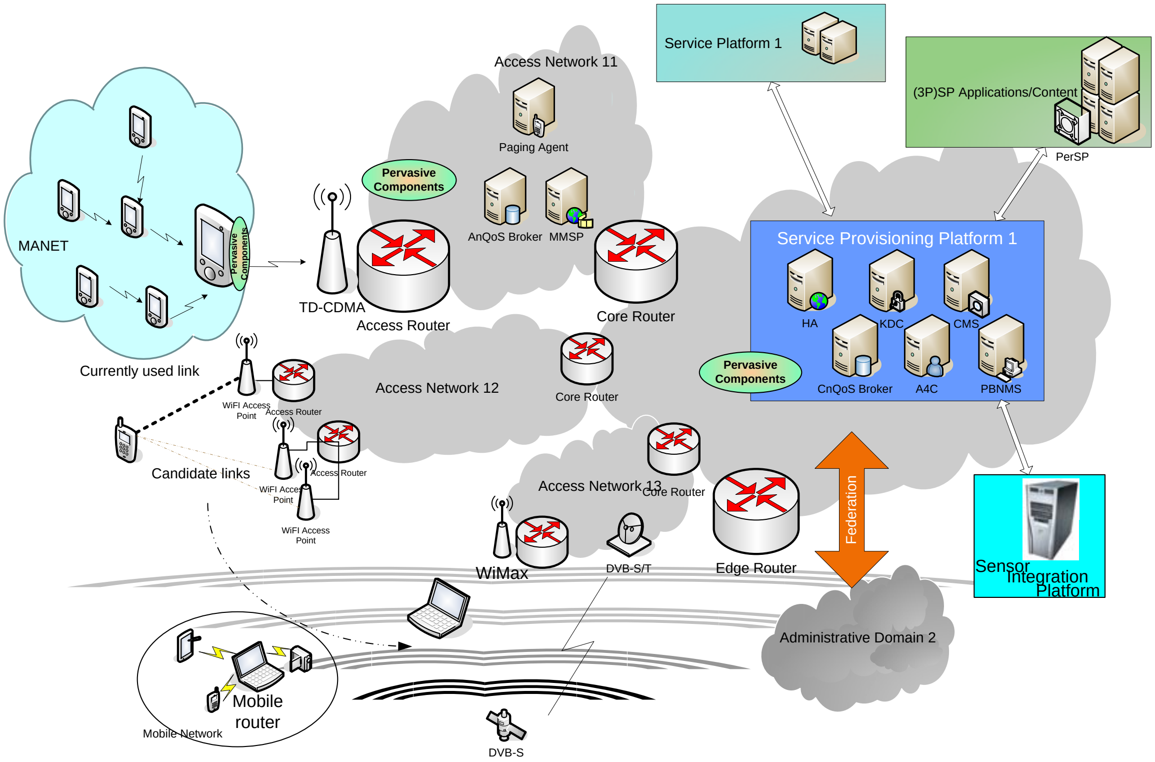

Figure 19: DAIDALOS Architecture Overview

DAIDALOS global architecture is built based on the pervasiveness concept. A pervasive system must be capable of providing a larger number of services everywhere in a personalized manner, based on the user context and preferences. Therefore, the behaviour of the network and the services will be highly dependent on the user profile. In order to achieve a high level of pervasiveness, all entities involved in the architecture must be "pervasive-aware", including the Edge Routers (ERs), the Core Routers (CRs), the Access Routers (ARs) and the Mobile Nodes (MNs).

Despite the fact that the entities represented in Figure 19 belong to a single administrative domain, a federation can be established between two administrative domains. ERs are used to interconnect these two distinct administrative domains. Each administrative domain is composed by a Core Network (CN) and one or more Access Networks (ANs).

The Service Provisioning Platform (SPP) is located in the CN and maintained by the operator. This platform provides a large set of functions required for efficient telecommunication provision, such as:

- Home Agent (HA): provides the functionalities for handover.
- Core Network QoS Broker (CNQoSBr): responsible for resource management in the CN, dealing with aggregates of flows traversing the core, and inter-domain resources.
- Central Monitoring Server (CMS): collects information from probes in multiple entities, providing a central query service for real time monitoring information.
- A4C: centralizes a large set of functions such as, Authentication, Authorization, Auditing, Accounting and Charging
- Key Distribution Center (KDC): provides the crypto information for the A4C [rfc2989] actions. This entity will be interconnected to a global PKI (Public Key Infrastructure).
- Policy Based Network Management System (PBNMS): defines the resource management policies and feeds this information to the QoS Brokers and the A4C.

The CRs are used to interconnect the CNs and the ANs. In Figure 19 several ANs are represented. A set of distinct technologies in the AN are supported – Ethernet, Wireless Fidelity (Wi-Fi) [wifi], Digital Video Broadcast (DVB) [dvb] [etsi] (Satellite and Terrestrial), WiMAX (Fixed and Mobile) and TD-CDMA. Each AN is composed by one or more cells. An AR connects the AN to the specific technology entity in the cell: AP in Wi-Fi [wifi] and BS in WiMAX [wimax], as examples.

The DAIDALOS network also includes Mobile Ad-hoc NETworks (MANET) [rfc2501] and Moving Networks (NEMO) [rfc3963]. Sensors are also a requirement in the DAIDALOS environment. These are integrated in the network through the usage of the Sensor Integration Platform. The (Third-Party) Service Providers provide applications and content to the end-users, either in the domain of the telecom operator or outside (third-party).

In each AN, the following entities are represented:

- Access Network QoS Broker (ANQoSBr): provides the management of the AN resources and per-flow admission controls.
- Multimedia Service Proxy (MMSP): provides the first point of contact for Session Initiation Protocol (SIP) [rfc3261] [rfc3312] based services.
- Paging Controller: provides power saving.

3.1.3. Layer 3 QoS Architecture

The SPP contains the QoS entities in the CN. The SPP contains the CNQoSBr, responsible for resource management in the core, dealing with aggregates of flows traversing the core, and inter-domain resources. Policies for resource management are defined by the PBNMS and sent to the QoS Brokers. The CMS collects statistics and other network usage data from the Network Monitoring Elements (NMEs), performing both passive and active probing. This information is then fed to the PBNMS and the QoS Brokers, which use it for proper network (re)configuration, resource management and admission control.

The ANQoSBr performs admission control, manages network resources and controls the ARs according to the active sessions and their requirements. It also performs load balancing of users and sessions among the available networks (possibly with different access technologies) by setting off network-initiated handovers. This is a rather important feature, since it provides the means to optimize the usage of operator resources and maximize operator's income.

The provision and control of multimedia services is provided by the MMSP; this element is also QoS-aware in the sense that it is able to request appropriate resources and QoS for its services. Terminals may also contain a QoS Client (QoSC) module able to mark the application packets with the corresponding assigned QoS and to request resources to QoS Brokers. Moreover, ARs (through the Advanced Router Mechanism – ARM module) can also trigger QoS for applications running in legacy terminals on behalf of the MNs. Thus, this architecture provides large flexibility in QoS signalling, enabling the use of a diversity of QoS access signalling scenarios, according to defined business cases.

When a user registers in the network, the ANQoSBr retrieves from the A4C a subset of the user profile. This subset, termed Network View of the User Profile (NVUP), contains information on the subscribed network level services (classes of service) that may be provided to the user, reflecting the user's contract (including e.g. bandwidth parameters). A Service View of the User Profile (SVUP), containing higher level information on the application services available to the user (e.g., voice calls, video telephony, and the respective codecs), may also be retrieved by the MMSP from A4C to perform access control to multimedia services.

To enforce the QoS decisions in the AN, a QoS Manager (QoSM) module is implemented in the ARs. To perform the communication between the ANQoSBrs and the QoSM, a Common Open Policy Service (COPS) [rfc2748] interface is used. Within the COPS architecture, the ANQoSBr is implemented as the Policy Decision Point (PDP) and the AR is implemented as the Policy Enforcement Point (PEP). Thus, all the admission control decisions are done in the ANQoSBr which enforces the AR to perform those decisions in the respective AN.

3.1.3.1. QoS Signalling Strategies

The proposed architecture is very flexible in the supported QoS signalling scenarios. These are mainly defined by the entity that triggers the QoS requests to the ANQoSBr. MMSP, ARM and the MN (through the QoSC) are the components able to issue QoS requests. These scenarios are related to specific service models: the MMSP scenario is targeted at application oriented models, whereas ARM and QoSC scenarios are, respectively, more targeted at network service and user oriented models.

Figure 20 illustrates a simplified example of a multimedia session (triggered by MN1) initiation using SIP (this scenario may work with other application level signalling protocol). The figure considers that the terminals are connected to different ANs in the same domain. Notice that some of the SIP messages not relevant for the QoS process were removed.

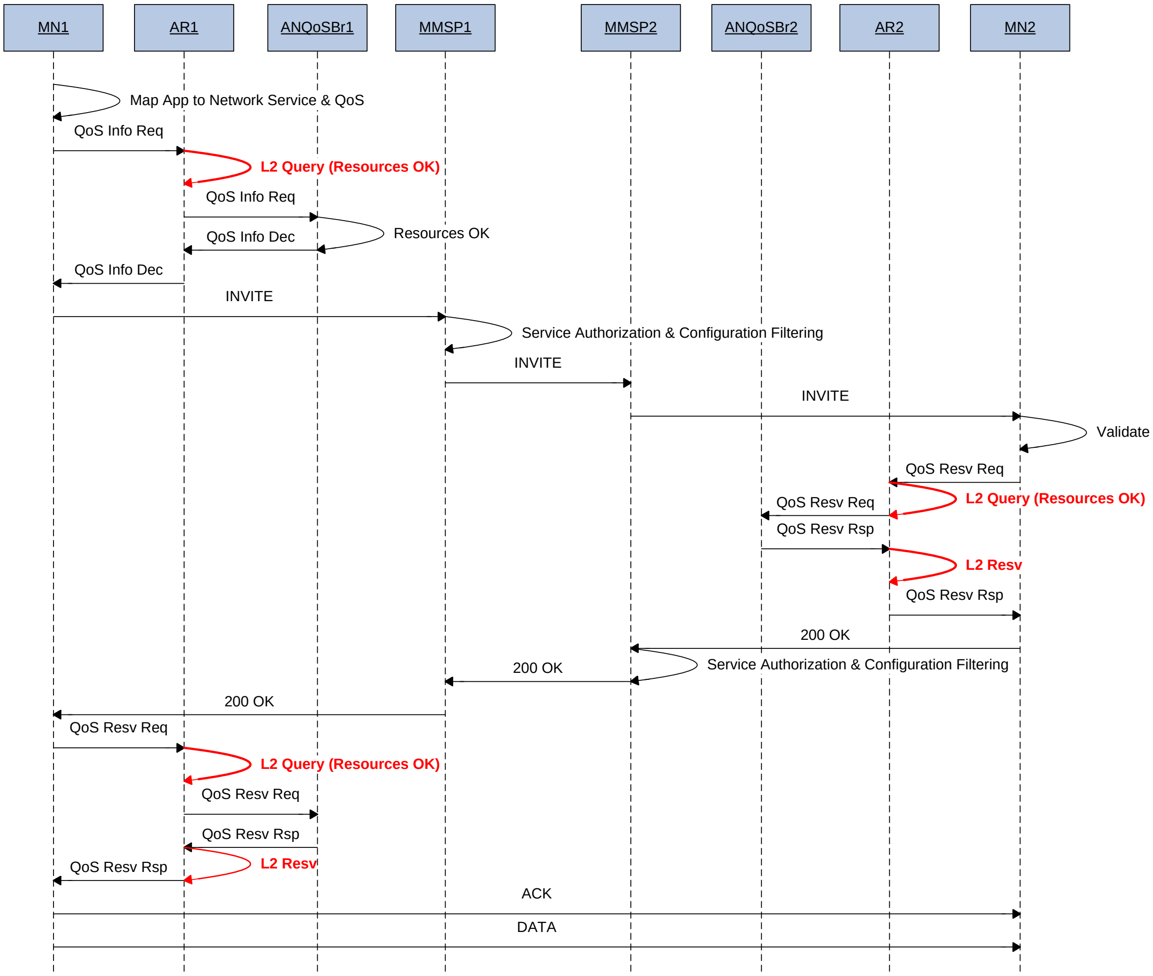

Figure 20: Signalling Strategy – MN scenario

When MN1 wants to start a communication, it starts by mapping the application requirements to network service and QoS requirements (done by the QoSC). Then, it sends a QoS Info Request (***QOS-INFO-REQ***) message to the QoSM entity at AR1. This message carries information about the QoS parameters required for that session. At this moment, the QoSM module checks if there are enough layer 2 resources available to satisfy the session setup requests. To perform this, the QoSM triggers an Abstraction Layer Resource Query (***AL-RESOURCE-QUERY***) message (see section 3.2) from a QoS Layer 2 abstraction layer (QoSAL) protocol in order to verify if enough resources are available in the layer 2 technologies. This layer 2 process between the QoSM and the other layer 2 entities will be explained in section 3.1.5. In this section we are just considering the layer 3 network signalling, which is responsible for triggering the layer 2 process.

Notice that, at this time, the resources are not yet reserved since there is still no information on the session capabilities that will be chosen by both terminals. Meanwhile, the QoSM receives an Abstraction Layer Resource Indication (***AL-RESOURCE-INDICATION***) message (section 3.2) from the QoSAL protocol indicating the result of the query process. If enough resources are available to satisfy the session setup request, the QoSM sends the message to the ANQoSBr1 with information on the required network and QoS parameters for the session. ANQoSBr1 answers with information on the services that may be used according to the user profile and the current network status. This step prevents the terminal from trying to initiate services that cannot be supported by the network, or that the terminal is not allowed to use, in face of the user profile (subscribed services). If allowed by the ANQoSBr1, the MN1 sends an ***INVITE*** message to MN2.

When receiving the ***INVITE*** message with an initial offer of QoS configurations, MMSP1 performs service authorization, filtering any service not allowed by the SVUP. If the service is authorized, the ***INVITE*** is forwarded to the MN2. Based on these QoS parameters, as done in the source entity (MN1) side, the destination entity (MN2) sends a QoS Reservation Request (***QOS-RESV-REQ***) message to the QoSM module in the AR2 querying the necessary resources in layer 2 to perform the session setup between the MN1 and the MN2. The layer 2 query process is similar to the one described in the source network. If resources in layer 2 are available, the AR2 requests ANQoSBr2 for available resources. When AR2 receives the reply from the ANQoSBr2, it triggers a reservation process in the layer 2 technology as will be explained in section 3.2. Since a query was made by the AR2 before the message was sent to ANQoSBr2, the reservation in the access technologies can be securely made since the resources are available. After the reservation is made, the QoSM module in AR2 triggers a QoS Reservation Response (***QOS-RESV-RSP***) message to the MN2 informing him that the reservation was successful.

MN2 generates a counter-offer, included in the ***200 OK*** message. On receiving this message, MMSP2 authorizes the services, filtering those authorized, and the message arrives at MN1. MN1 chooses then the service to use, and sends a ***QOS-RESV-REQ*** to

AR1. Resources in layer 2 are checked, and the message is sent to ANQoSBr1. A response is sent back to AR1, and the layer 2 reservation is triggered. Finally, an ACK message containing the final configuration that will be used is sent to MN2, and data may flow between the two end-points with reserved resources.
The QoS signalling request between the QoSC and the QoSM is implemented through an extension to Resource Reservation Protocol (RSVP) [rfc2205]. Communication between QoSM and ANQoSBr1 is based on COPS.

3.1.4. Fast Mobility Support

Two fast handover mechanisms were proposed: mobile node initiated handover (MNIHO), when the terminal changes network due to mobility or user preferences, and network initiated handover (NIHO), when the terminal is requested to change network due to resource management reasons. In inter-domain mobility, only the former handover type is considered.

Figure 21 illustrates a MNIHO process, integrated with QoS, considering an inter-AN handover, over intra- and inter-technology.

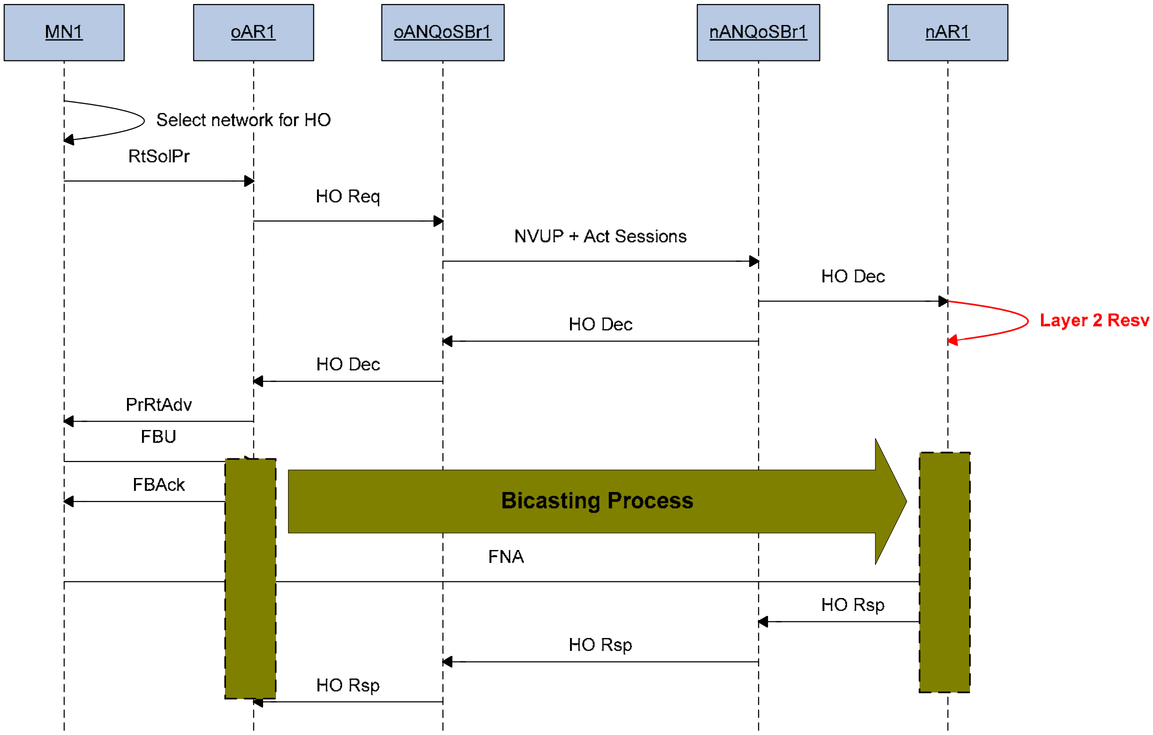

Figure 21: MNIHO process

In the first phase of the handover process, the MN needs to discover the available candidate ARs. This information is provided by Candidate Access Router Discovery (CARD) [rfc4066]. After this information is obtained, the MN sends a Router Solicitation for Proxy (***RtrSolPr***) message request to the old AR1 (oAR1) to handover for the new network. Next, a Handover Request (***HO-REQ***) message is sent by the oAR1 to the old ANQoSBr1 (oANQoSBr1). Immediately, the oANQoSBr1 sends the NVUP and the active sessions to the nANQoSBr1. Assuming that the new ANQoSBr1 (nANQoSBr1) accepts the handover request with the required characteristics, a Handover Decision (***HO-DEC***) message is sent to both oAR1 and nAR1.

In the nAR1, the necessary resources are allocated, including layer 2 resources. Reserving the layer 2 resources requires that the QoSAL process is triggered, as will be explained in section 3.2.

When the ***HO-DEC*** message reaches the oAR1, a Proxy Router Advertisement (***PrRtrAdv***) message is sent to MN1. The terminal then sends a Fast Binding Update (***FBU***) message to the oAR1 confirming the handover. This ***FBU*** message triggers the bicasting process. Thus, each packet sent to MN1 via the oAR1 is duplicated at oAR1 and also sent to nAR1. After MN1 performs the handover, it sends a Fast Neighbour Advertisement (***FNA***) message to the nAR1. This message will populate the nAR1 neighbour cache where buffered packets may be already waiting to be delivered. Finally, both ANQoSBrs are informed that the handover is completed through a Handover Response (***HO-RSP***) message. As a result, the bicasting process stops.

3.1.5. Layer 2 QoS Architecture

The layer 2 QoS architecture has been designed in order to follow a set of main guidelines, outlined as follows:

- A modular architecture to allow the separation of the technology specific and independent parts, which facilitates the future inclusion of new wireless technologies into the architecture.
- The designed architecture is flexible to allow the concatenation of several wireless technologies in the access.
- Automatic learning techniques are used which minimizes the configuration requirements and facilitates operation.
- The architecture is integrated with the CN QoS architecture providing users with end-to-end QoS guarantees.
- A solution integrated with mobility protocols has been designed to ensure that QoS is not disrupted during handoffs.

Technology specific enhancements and configuration algorithms have been developed and designed for the various wireless technologies considered.

3.1.5.1. Supported Scenarios

In DAIDALOS, the layer 2 QoS architecture distinguishes between two main scenarios: the single-hop and the two-hop (concatenated/backhaul) scenarios. The single-hop scenario can be composed with different wireless technologies, such as, IEEE 802.11e, IEEE 802.16 and TD-CDMA. In this type of scenario, the base station of each technology is directly connected to the AR of the wired part of the AN. In our specific case, we consider 802.16 as the technology directly connected to the AR, through the BS, feeding the Terminal that is connected to the SS. This scenario is shown in Figure 22.

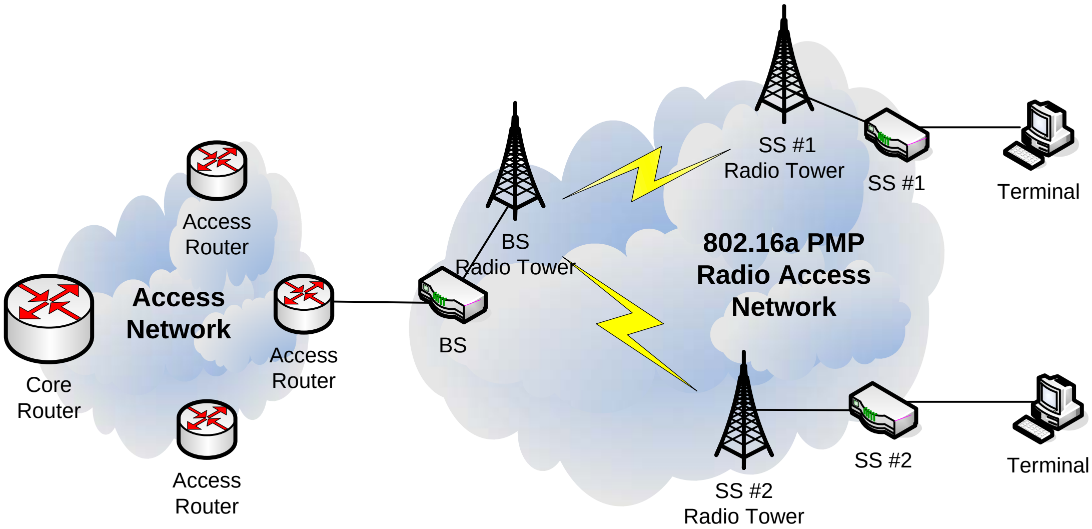

Figure 22: Single-hop scenario (Terminal directly connected)

Figure 23 shows the two-hop (concatenated/backhaul) scenario. This scenario is the concatenation of two wireless technologies, namely, 802.16 in the first hop and 802.11e in the last hop. The 802.16 solution is used as a backhaul link for the 802.11e network. The BS of the 802.16 network is directly connected to the AR and the SS is directly connected to the 802.11e AP.

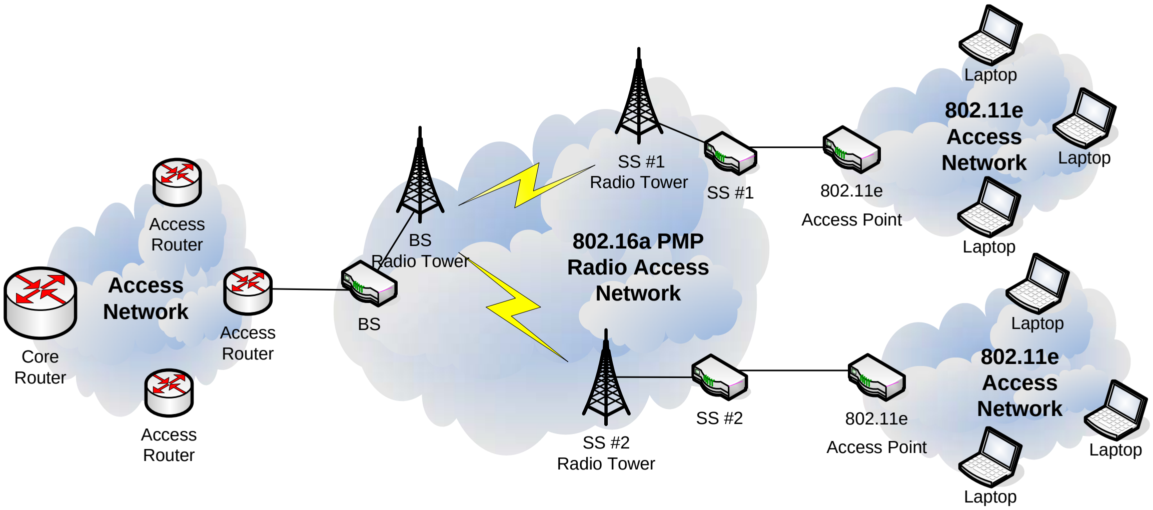

Figure 23: Two-hop or concatenated scenario (Backhaul)

Both scenarios provide end-to-end QoS capabilities. In the single-hop scenario, QoS is provided by the 802.16 system, whereas in the two-hop scenario QoS is achieved through 802.16 and 802.11e technologies. Full details about these scenarios and how they are integrated in the DAIDALOS network will be given in further sections of this document, including all the modules and interfaces involved.

3.1.5.2. High Level L2 QoS Architecture Overview

DAIDALOS QoS main goal is to provide an end-to-end QoS solution with strict guarantees independently of the wireless technology that is being used to access the network. Such a high level of support and transparency implies that strong and reliable integration methods are developed.

To accomplish the demands of a transparent end-to-end QoS architecture, a set of modules and interfaces have been defined and implemented. As we can see in Figure 24, a technology independent module has been defined: QoSAL. The QoSAL module is responsible for the layer 2 signalling part of the AN QoS architecture. It implements the functionality of resource management in the AN, being able to perform QoS reservations, modifications and deletions. Additionally, it is also capable of performing resource querying from the AR to remotely located APs, support for concatenation of multiple wireless technologies, and has the ability to work without requiring a priori centralized knowledge of the AN topology. It is composed of three variations of the same basic module working in the MNs, APs and ARs.

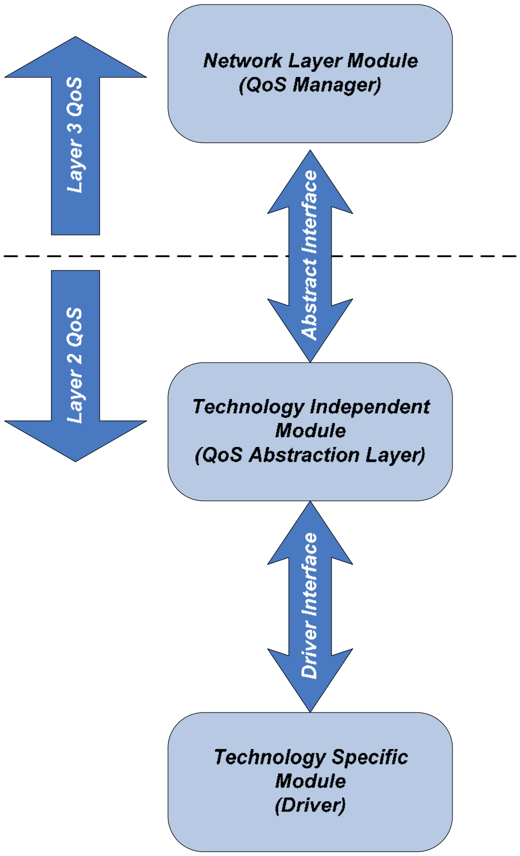

Figure 24: High Level Architecture Overview

Figure 24 also presents the technology specific modules, which are specific technology drivers. These modules are responsible for the QoS support for a particular technology in a single network link. They directly communicates with the specific technology, translating general QoS parameters from the QoSAL, like Traffic Specification (TSpec) and Resource Specification (RSpec), to technology specific QoS parameters.

To allow the communication between the QoSAL module and the technology specific drivers, an interface – Driver Interface - has been defined. The Driver Interface is used to translate abstract QoS to technology specific QoS parameters.

The Abstract Interface is responsible to provide the communication between the QoSAL and the layer 3 QoS entities, in both, the AR and the MN. In the AR, the communication is done with the QoSM and in the MN with the QoSC. The Driver and Abstract Interface primitives are described in section 3.2.

A unique identifier in the AN is used to identify each service – connection identifier (*CnxID*). The *CnxID* is carried in the IPv6 Flow Label field, allowing the involved technologies in the AN to classify the traffic based on this field.

3.2. QoS Abstraction Layer

As already depicted in a high-level way, the QoSAL is the technology independent part of the AN QoS architecture. The QoSAL, as a layer 2 signalling protocol, works only in the control plane level. A set of services are offered by the QoSAL, such as:

- QoS flows management
- Resource querying
- L2 QoS notifications

3.2.1. QoS Flows Management

This is the main service offered by the QoSAL. It consists in the creation, modification and deletion of *QoS connections*. A QoS connection is a virtual channel between a MN and an AR, provisioned with QoS guarantees. Since it is a control plane module, no additional header is inserted into the IPv6 data packets transported in some layer 2 frame. The IPv6 Flow Label field is reused in a context local to an AN, and each value identifies uniquely a service in a given AN.

The service of QoS reservation is offered at the AR by the primitive *AL-CNX-ACTIVATE-REQ*, which takes as parameters, among others, the L2 address of the destination end-point and the desired QoS attributes. The QoS parameters include a TSpec and an RSpec. The ***AL-CNX-ACTIVATE-REQ*** primitive is sent by the QoSM entity to the QoSAL through the Abstract Interface (Figure 24), triggering the reservation process in the AN. As a consequence, a ***CNX-ACTIVATE-REQ*** message is sent by the QoSAL to the MN. All the QoSAL messages are intercepted by the intermediate APs that implement the QoSAL protocol, before forwarding the messages again to the original destination. Finally, the QoSAL message (***CNX-ACTIVATE-REQ***) reaches the MN and a reply message (***CNX-ACTIVATE-RESP***) is sent back to the AR in the reverse path.

During the reverse path, the QoSAL module running in the APs or ARs intercepts the ***CNX-ACTIVATE-RESP*** message, and triggers a reservation in the specific technology driver (by sending an ***ALD-CNX-ACTIVATE-REQ*** primitive to the specific technology driver through the Driver Interface – Figure 24). The Driver performs admission control, by checking if its available resources are enough to perform the reservation, performs the requested reservation, and sends an ***ALD-CNX-ACTIVATE-RESP*** to the QoSAL module through the Driver Interface. After this process is completed, the ***CNX-ACTIVATE-RESP*** message is sent again until it reaches the AR. When the message finally reaches the QoSAL module running in the AR, a *CnxID* is returned to the QoSM in an ***AL-CNX-ACTIVATE-RESP*** primitive through the Abstract Interface. This identifier is used to mark the IPv6 flow label field of the data packets that will be associated to the connection, and to modify and delete the QoS connections.

After a reservation is done in the AN, it can be modified or deactivated. The modification process is similar to the reservation case depicted above; only the primitives and messages are slightly different. For this process, the ***AL-CNX-MODIFY-REQ*** and the *AL-**CNX-MODIFY-RESP*** primitives are used in the Abstract Interface; for the Driver Interface, the ***ALD-CNX-MODIFY-REQ*** and the ***ALD-CNX-MODIFY-RESP*** primitives have been defined. The ***CNX-MODIFY-REQ*** and the ***CNX-MODIFY-RESP*** are the messages used between the AR and the MN.

To deactivate a reservation, an ***AL-CNX-DEACTIVATE*** primitive is sent by the QoSM to the QoSAL in the AR. Immediately after, the ***CNX-DEACTIVATE*** message is sent and the ***ALD-CNX-DEACTIVATE*** primitive is used in the Abstract Interface to notify the specific drivers.

3.2.2. Resource Querying

There is a primitive to request a report of the available resources in the AN, the ***AL-RESOURCE-QUERY***. Its only parameter is the identifier of the path for which resources are to be queried. This parameter can be the MN MAC address (request a single report for all APs in the path towards the given MN), or an AP (request a single report for all APs in the path towards the given AP, including the destination AP itself). As a reply, the ***AL-RESOURCE-INDICATION*** primitive has been defined. This primitive carries the available resources in the queried technology.

3.2.3. Layer 2 QoS Notifications

The primitive ***AL-CNX-INDICATION*** can be triggered in the QoSAL from the AR, the AP or the MN to indicate that the QoS parameters from a specific connection have been modified. The primitive includes the connection identifier and the modified RSpec as parameters.

3.3. IEEE 802.16 Integration Requirements

For the successful integration of the 802.16 system in the DAIDALOS architecture, a set of mandatory requirements must be satisfied. These requirements have an important influence in the overall design of the 802.16 technology dependent module, which will be depicted in chapter 4. The next sub-sections depict these requirements and the issues originated by them.

3.3.1. Fast MN Network Access

In real-time environments, users must have fast access to the requested services without having to wait long periods for the services initialization. As mentioned in sections 2.2 and 2.4, no packets are allowed to traverse the 802.16 link if no appropriate reservation has been established. Since we have adopted Ethernet as the CS, a reservation must be performed using the MN MAC address to allow the packets to flow in the 802.16 system. However, to perform the service flow reservation, the AR must be aware of the MN MAC address. For instance, in the two-hop scenario shown in Figure 23, the MN MAC address must be provided to the AR when the MN associates with the AP. The MN MAC address can only be discovered as soon as the MN gets connected. This lack of information about the MN MAC address is time consuming and breaks the fast MN network access. Therefore, it is not a trivial process for the 802.16 system to provide a fast network entry for the MN.

3.3.2. Dynamic Service Reservation

In next generation environments, QoS reservations must be dynamic and fast. Uplink and downlink service reservations have to be supported without delaying the data packets while service flows are being established in the 802.16 system. For instance, if the MN launches a specific service, the respective data packets must be able to traverse the 802.16 air link, even if the service flow establishment in the 802.16 system is not completed. Since 802.16 is connection oriented, no packets are allowed to traverse the 802.16 link without a dedicated reservation. Thus, it is required that a reservation is performed. However, as mentioned in section 2.7.2, a service flow allocation is not an instantaneous process. Therefore, a workaround must be done to allow the packets to flow in the network before the completion of the service flow reservation. Section 4.3.3 depicts the solution for this issue.

3.3.3. Dynamic Service Modification

Dynamic service modifications are also mandatory. Users must be able to dynamically modify the set of QoS parameters from a previously allocated reservation, without interrupting the service that is being used. The user must not notice that changes are being made in its service flow; otherwise, no dynamic service flow modification is provided. However, service flow modifications take large periods of times, as depicted in section 2.7.2. The developed solution to overcome this problem is presented in section 4.3.4.

3.3.4. Dynamic Service Differentiation

Another open issue is related to the traffic differentiation granularity. If the MN is running more then one service, the 802.16 system is not able to differentiate between the two services. This is due to the fact that we are using Ethernet as the CS, as depicted in section 2.7.1, and each MN has only one MAC address to identify it. Even if the MN is running only one service, signalling packets and data packets should be sent in different service flows in order to achieve high performance. Thus, a problem is identified on how to differentiate different services in the 802.16 wireless link for the same MN, using Ethernet CS. For next generation network environments, a solution for this problem must be found providing per service QoS guarantees, where QoS differentiation should be done based on each service instead of each the MN. Section 4.3.5 illustrates the developed solution for this issue.

3.3.5. Fast-Handover Support

In the two-hop scenario, shown in Figure 23, fast handovers between the MNs connected to the APs must be supported. Therefore, 802.16 service flow reservations in the new SS (nSS) must be dynamic and fast in order to avoid traffic disruption during the fast-handover process. This implies that immediately after the MN handoffs from the old AP (oAP) to the new AP (nAP), reservations in the old SS (oSS) are teardown and reservations in the nSS are established. If the service flow allocation in the nSS is slow, the handover latency will be high and thus, service(s) running in the MN will be degraded during this period of time. Therefore, fast service flow reservation in the nSS is crucial. Since service flow allocations in 802.16 systems are not fast enough to support fast-handover, how can this feature be fully supported in this scenario, without the MN noticing service interruption? A solution for this issue is presented in section 4.3.6 allowing network operators, service providers and users to benefit from such scenario.

3.3.6. IPv6 Neighbour Discovery Process (NDP) Support

IPv6 support is mandatory in next generation networks. Specifically, the IPv6 Neighbour Discovery Process (NDP) [rfc2461] support, which is multicast-based, is fundamental. As we have already mentioned, 802.16 is connection-oriented, even for non-connection protocols such as IPv6. Therefore, a solution must be found to support the IPv6 NDP over 802.16 networks. This issue is discussed in section 4.3.7.

3.4. Summary

In this chapter, the DAIDALOS project environment has been presented. The QoS architecture developed in the framework of the Daidalos project aims at providing an end-to-end QoS solution under a heterogeneous access environment. In the framework of the Layer 2 QoS architecture, a QoS Abstraction Layer module has been defined as the technology independent part of the architecture and is responsible for the layer 2 signalling of the access network QoS environment. It performs service flow reservations, modifications and deletions, as well as resource queries in the access network. Besides the QoS Abstraction Layer module, a technology specific module has also been defined for each one of the technologies from the access network. This module is responsible to enforce the QoS requests in the access technologies, including the 802.16 system.

Finally, some of the main requirements for the successful integration of the 802.16 technology in the DAIDALOS environment, such as dynamic service flow reservation and modification, service differentiation and fast-mobility support, have been introduced.

Chapter 4: IEEE 802.16 QoS Modules Specification

To integrate the 802.16 technology in a next-generation environment, as outlined in chapter 3, a set of modules had to be specified and developed. These modules should provide full QoS functionalities, as well as fast-mobility procedures.

Despite the built-in QoS feature provided by 802.16, the support of IPv6 QoS aware real-time services is not straightforward. Real-time environments require that the technologies being used are very fast in the reservation process. For example, the MN access to the network services and applications must be fast and dynamic. Since the 802.16 system is connection-oriented, a service flow must be allocated to allow the MN to access the network services. This is a constraint in real-time and dynamic environments. Additionally, dynamic service reservations and modifications must also be supported, as well as traffic differentiation, IPv6 support and fast-mobility. These issues have been pointed out in section 3.3.

Since the service flow allocation takes some time to be performed, and because the users and services cannot wait that amount of time, we have designed a solution to allow the packets to flow in a default connection, which is already setup, until the specific flow allocation is in place. Moreover, packet classification in the 802.16 link is based on the MAC address. Since service differentiation in the same terminal is required, the usage of this classification process has strong limitations. Therefore, we based our solution on the Virtual MAC (VMAC) concept. We adopted Ethernet as the CS and used the VMAC address concept to build our solution. A MAC Address Translator (MAT), based on a set of translation rules, has been implemented. The translation rules are responsible for the replacement of the original MAC addresses by the VMAC addresses and vice-versa. A set of building blocks and a new protocol (802.16 Control Protocol) have been defined to control the QoS and fast-mobility processes in the AN entities.

This chapter is divided into six main sections. Section 4.1 details the novel adopted solutions that have been implemented to overcome the open issues previously presented. Section 4.2 depicts the developed architecture to integrate the 802.16 technology in the DAIDALOS environment. The presented architecture is mainly focused on the layer 2 part of the DAIDALOS system, including all the modules and interfaces that have been implemented. Section 4.3 presents the several operation phases of the developed driver, including the dynamic service flow reservation/modification and fast handover support. Section 4.5 describes the 802.16 Control Protocol, whereas section 4.4 details the implemented modules and interfaces. Finally, section 4.6 provides a brief summary of this chapter.

4.1. Proposed Solutions

To successfully integrate the 802.16 technology in the DAIDALOS environment, a set of integration requirements have been described (see section 3.3). To fulfil these requirements, several issues were raised due to the limitations associated with the 802.16 technology, as described in section 2.7. To overcome these open issues, original solutions have been specified and developed. Following sections depict these solutions and their operation mode.

4.1.1. Virtual Medium Access Control (VMAC) Address

As mentioned in section 2.7.1, the 802.16 equipment has some restrictions with respect to classifiers (no IPv6 CS is available). This forced us to develop a new classification mechanism based on the MN MAC addresses, either the source (for the uplink traffic) or the destination (for the downlink traffic). Since classification is done based on the MN MAC address, this can raise a problem when several services are requested by the same MN. This will create an issue concerning the requirement pointed in section 3.3.4 – Dynamic Service Differentiation. Therefore, a novel solution was developed to overcome this issue, based on the concept of ***Virtual MAC (VMAC) addresses***. Each MN will have a number of flow reservations in the 802.16 equipment equal to the number of different QoS services that it is using; each one will be identified by a different VMAC address in the 802.16 system, with its specific QoS parameters associated, instead of being identified by the MN MAC address.

The VMAC addresses are generated based on the original MAC address, but changing higher order bits, exploiting the IEEE MAC number scheme structure. This strategy allows us to perform service differentiation between services that are being used by the same MN and not only to differentiate and to provide QoS to services running on different MNs. Detailed information about the service differentiation solution will be provided in section 4.3.5.

4.1.2. MAC Address Translator (MAT)

Due to the usage of the VMAC address, an efficient translation process is required before data packets reach the 802.16 system (downlink/uplink). Additionally, the reverse translation process after the packets leave the 802.16 network (downlink/uplink) is also necessary. To perform these translations, a MAC Address Translator (MAT) has been implemented in both the AR (BS side entity) and in the AP/MN (SS side entity). For the single-hop scenario (Figure 22), the SS side entity is the MN, whereas in the two-hop scenario it is the AP (Figure 23). The MAT is responsible for the translation rules management (install, delete, block and unblock), as well as for the adequate translation of the MAC addresses to the correspondent VMAC addresses, according to the IPv6 Flow Label field. The reverse translation process, which translates the VMAC address to the original MAC address, is also done by the MAT. The MAT operation is based on a set of translation rules that indicate the specific VMAC address that must be used for a particular MAC address.

4.1.2.1. Downlink MAT Operation

In the downlink direction, before reaching the BS, the destination MAC address of the packets must be translated to the correspondent VMAC address, according to the IPv6 Flow Label field. This downlink translation process is performed by the MAT in the BS side entity (AR), in both single-hop and two-hop scenarios shown in Figure 22 and Figure 23, respectively. After traversing the 802.16 air link, packets reach the SS side entity (AP/MN) with the downlink VMAC address as the destination MAC address. Therefore, the reverse translation process is also necessary to guarantee that the packets are correctly delivered to the MN. This way, the downlink VMAC address must be replaced by the original destination MAC address. This translation process is done by the MAT in the SS side entity (AP/MN) when packets arrive from the SS in the downlink direction.

4.1.2.2. Uplink MAT Operation

In the uplink direction, a similar process is implemented. The original source MAC address of the packets is replaced by a specific VMAC address according to the IPv6 Flow Label field. This translation is done by the MAT in the SS side entity (AP/MN). After the translation process is completed, packets are sent to the 802.16 link and classified by the later according to the source MAC address. Finally, packets reach the AR with the VMAC address as the source MAC address.

4.1.2.3. VMAC Address Synchronization Requirements

For both downlink and uplink directions, using the VMAC address requires that a high level of synchronization is achieved between the MAT located in the BS side entity (AR) and the MAT located in the SS side entity (AP/MN). This means that the translation rules installation in the BS and in the SS side entities must be synchronized. For this task, we use a set of messages from a new defined protocol named 802.16 Control Protocol (16CP) (see section 4.4). Detailed information about how and when to apply the translation rules combined with the 16CP messages is explained in section 4.3.

4.1.3. Auxiliary Service Flow (AUX-SF)

Other major issue is the time taken to perform 802.16 reservations, as described in section 2.7.2. Although it varies between equipment vendors, it is usually not a fast process. In our case, the 802.16 equipment took about 11 seconds and 21 seconds to perform a service flow reservation and modification, respectively. Meanwhile, traffic is queued waiting for the reservation process to be completed. This is not acceptable in advanced scenarios and therefore, to overcome this problem, we used a permanent ***backup data channel***, effectively creating one ***auxiliary service flow (AUX-SF)*** in the 802.16 network. This channel, typically of very good quality and already created as backup, does not use its bandwidth unless required. If a specific service flow being used has to suffer a modification (e.g. of the QoS parameters), the data traffic is immediately redirected to the auxiliary service flow and its packets do not suffer any delay related to the 802.16 reservation process. After that, the QoS parameters of the original service flow can be changed, without affecting the traffic; when completed, the traffic is returned to the original service flow. The auxiliary service flow will stay active waiting for other modification requests, once again without traffic. Note that, all this is achieved by fast processing on the VMAC address in the AR and in the AP/MN, changing the MAC addresses appropriately through the usage of the MAT and the 16CP. Note that, besides the stable bandwidth provided, the developed solution also guarantees that there are no losses of data packets when these are redirected to the backup service flow or to the original service flow.

4.2. Developed Architecture

The single-hop (Figure 22) and two hop scenario (Figure 23) have been successfully integrated in the DAIDALOS environment. To achieve this level of integration, a set of modules and interfaces have been defined and integrated in both scenarios, as depicted in the following sections.

4.2.1. Single-hop scenario

Figure 25 depicts how the developed modules interact in the single-hop scenario. In this case, the 802.16 BS is connected to an AR (BS side entity), whereas the 802.16 SS is directly connected to a MN (SS side entity).

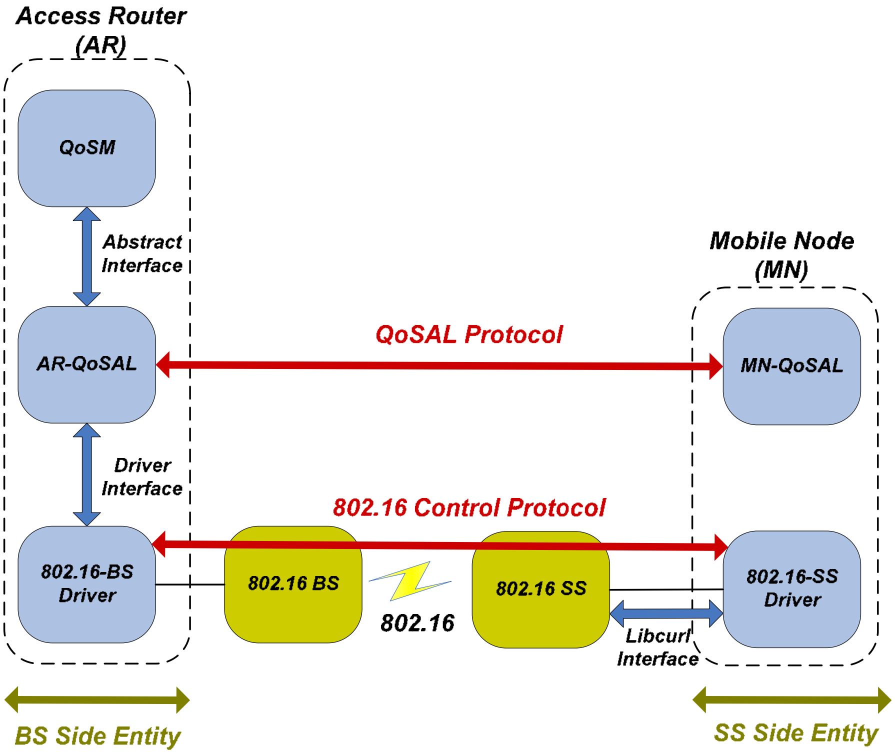

Figure 25: QoS architecture - single-hop scenario

In this particular scenario, the MN (SS side entity) is directly connected to the 802.16 SS. Therefore, a technology dependent module (802.16-SS Driver) that is responsible to control the 802.16 SS must be installed in the MN. To manage all the 802.16 system, a technology dependent module (802.16-BS Driver) is also located in the AR (BS side entity). It provides the communication with the upper layers (AR-QoSAL) and with the 802.16-SS Driver using the 16CP. The QoSAL, depicted in section 3.2, has been developed to establish the communication between the access technologies and the layer 3 architecture. A module of the QoSAL is located in the AR, called AR-QoSAL, and another one is installed in the MN, named MN-QoSAL. For the communication between these two modules, the QoSAL protocol is implemented. Finally, a layer 3 QoS entity is located in the AR, the QoS Manager (QoSM), to provide the communication with the AR-QoSAL and map the incoming requests to layer 2 specific requests.

4.2.2. Two-hop scenario

In the two-hop scenario it is required to integrate 802.16 and 802.11e technologies. For the successful integration of both wireless technologies, different control modules had to be defined in the different physical elements. Figure 26 depicts the modules and interfaces defined in the architecture for the integrated 802.16 control. The overall objective was the assurance of end-to-end QoS support on the compounded wireless links, and thus different control entities had to be implemented.

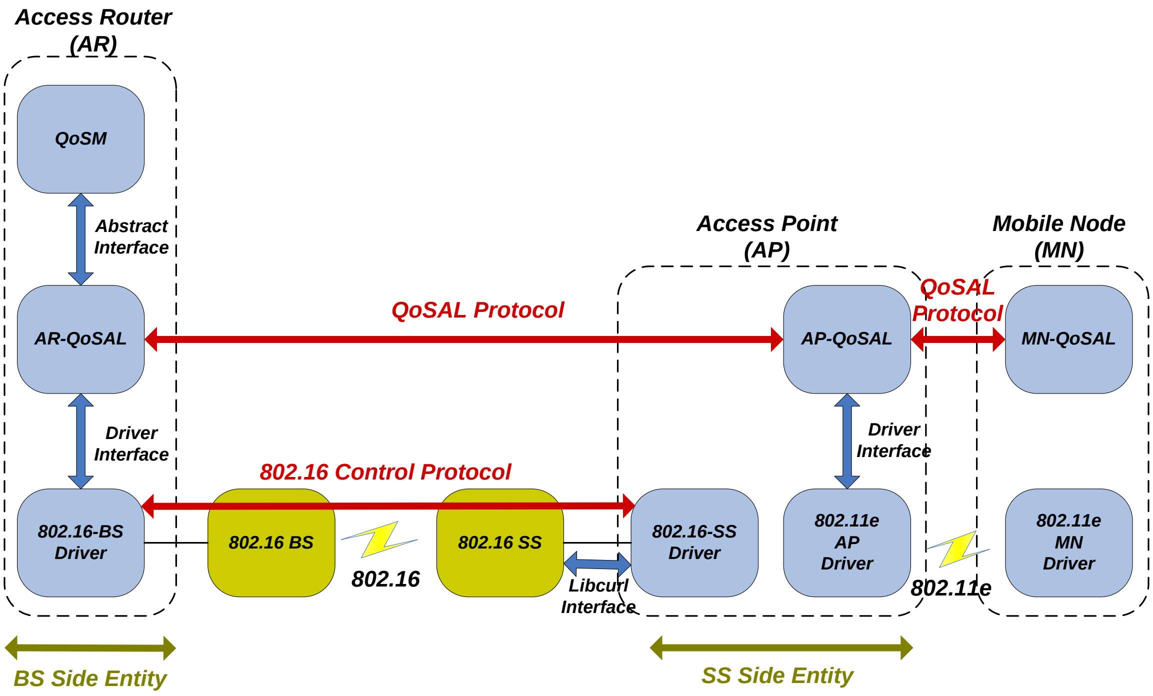

Figure 26: QoS architecture - two-hop scenario

When compared with the single-hop architecture, there is an additional entity in this scenario which is the AP. In this case, instead of using the MN as the responsible entity to perform the communication and control of the 802.16 SS, the AP (SS side entity) is directly in charge of this responsibility. Therefore, the modules that are required to control the 802.16 SS are installed in the AP, instead of running in the MN as in the single-hop scenario. Since we are in a compounded environment with an 802.16 and an 802.11e network, the AP also has a technology dependent module, the 802.11e AP Driver, to control the 802.11e network. Besides the 802.11e AP Driver located in the AP, an 802.11e Driver is also located in the MN (802.11e MN Driver). As a consequence of having a technology dependent module in the AP, it is mandatory to have a QoSAL module to interface with the 802.11e AP Driver and enforce the QoS policies in the 802.11e network.

4.2.3. Access Network QoS Reservation

In both single-hop and two-hop scenarios, the layer 2 QoS architecture communicates with the layer 3 QoS architecture through the usage of the Abstract Interface (AI) in the AR. The AI provides the communication between the QoSM and the AR-QoSAL using the primitives described in section 3.2. Therefore, all the QoS enforcement in the access technologies is done through this interface. The QoSM receives the COPS messages from the QoSBr and enforces these decisions in the network. When this information reaches the AR-QoSAL, depending on the received request, the correspondent action is taken. For instance, if a QoS reservation request is sent by the QoSM to the AR-QoSAL, an ***AL-CNX-ACTIVATE-REQ*** message from the QoSAL signalling protocol is sent from the AR-QoSAL towards the MN. If we are using the single-hop scenario, the ***AL-CNX_ACTIVATE-REQ*** message is sent directly to the QoSAL module running in the MN (MN-QoSAL). On the other hand, if the two-hop scenario is being used, the ***AL-CNX-ACTIVATE-REQ*** message is sent to the QoSAL module running on the AP (AP-QoSAL) and then forwarded to the MN-QoSAL. In both cases, the MN-QoSAL receives the ***AL-CNX-ACTIVATE-REQ*** message and sends the response message (***AL-CNX-ACTIVATE-RESP***) back to the AR-QoSAL module in the reverse path. In the single-hop scenario, the ***AL-CNX-ACTIVATE-RESP*** message is directly sent to the AR-QoSAL. In the two-hop scenario, the ***AL-CNX-ACTIVATE-RESP*** message is intercepted by the AP-QoSAL.

When the AP-QoSAL receives the message, it triggers the reservation process in the 802.11e technology. For this purpose, an ***ALD-CNX-ACTIVATE-REQ*** primitive is sent by the AP-QoSAL to the 802.11e AP Driver indicating the reservation parameters for the required connection. If enough resources are available in the 802.11e wireless link, the reservation is done by the 802.11e AP Driver and an ***ALD-CNX-ACTIVATE-RESP*** primitive is sent to the AP-QoSAL indicating that the reservation is complete. After receiving the reservation response primitive, the AP-QoSAL forwards the ***AL-CNX-ACTIVATE-RESP*** message to the AR-QoSAL. Independently of the scenario being used, when the ***AL-CNX-ACTIVATE-REQ*** message reaches the AR-QoSAL, the reservation process for the 802.16 technology is triggered. Thus, an ***ALD-CNX-ACTIVATE-REQ*** primitive is sent by the AR-QoSAL module to the 802.16 Driver running in the AR (802.16-BS Driver), triggering the service flow reservation in the 802.16 system (if enough resources are available in the 802.16 link). When the service flow reservation in the 802.16 link is completed, the 802.16-BS Driver sends an ***ALD-CNX-ACTIVATE-RESP*** primitive to the AR-QoSAL module indicating the success of the reservation. Finally, the AR-QoSAL notifies the QoSM that the layer 2 connections are reserved and traffic can start being forwarded in the AN.

4.3. 802.16 Driver Operation Phases

After the brief overview that has been given in the previous section about the 802.16 Driver, a deep explanation about its operation mode for the two-hop scenario will be given in the following sections.

4.3.1. System Setup

Since we are dealing with a connection oriented technology, during system setup we must prepare the 802.16 system to support all the possible scenarios. To allow the communication between the 802.16-BS Driver and the 802.16-SS Driver, two service flows are defined during the system boot up phase for this purpose:

- **AP-DL-SF** (**Access Point Downlink Service Flow**): Allows the 16CP downlink packets to be forwarded from the 802.16-BS Driver to the 802.16-SS Driver. This service flow is created using the AP MAC address as the classification parameter.
- **AP-UL-SF** (**Access Point Uplink Service Flow**): Allows the 16CP uplink packets to be forwarded from the 802.16 SS Driver to the 802.16 BS Driver. This flow is allocated using the AP MAC address as the classification parameter.

Considering the 802.16 equipment restrictions pointed in section 2.7, the successful support of real-time environments requires that two auxiliary service flows (see section 4.1.3) are also defined:

- **AUX-DL-SF** (**Auxiliary Downlink Service Flow**): Defined using a specific VMAC address for the downlink direction – *VMAC_AUX_DL* address.
- **AUX-UL-SF** (**Auxiliary Uplink Service Flow**): Defined using a specific VMAC address for the uplink direction – *VMAC_AUX_UL* address.

Despite these service flows are installed during the system setup phase, they will only be used when a MN connects to the network and the associated translation rules are installed. Anyway, they are installed in this phase to avoid wasting this extra time when the MN connects to the network. More details about this specific part of the process will be explained in the MN network access phase, depicted in section 4.3.2.

When the MN connects to the network it is necessary to install the correspondent translation rules in the AR and in the AP. Despite the translation rules installation period is very small, the MN can start sending/receiving data packets in that interval of time and consequently, these data packets will be lost. To avoid loosing these packets, and consequently allowing data packets to be sent to/from the MN during this period of time, two service flows are defined:

- **DEF-DL-SF** (**Default Downlink Service Flow**): Since we are in a point-to-multipoint environment, the BS must be aware of the SS to which the packets should be sent. This depends on the point of attachment of the MN. Since, at this early stage of the process, the AR is not yet aware of the MN location, the downlink packets should be sent to all the SSs that are associated with the BS. Thus, we use the broadcast MAC (*BC_MAC*) address to classify the packets sent in the **DEF-DL-SF** service flow.
- **DEF-UL-SF** (**Default Uplink Service Flow**): In the uplink direction, the SS should always send the packets to the associated BS. Therefore, in this case a regular VMAC address is used to establish the service flow – *VMAC_DEF_UL*.

For the **DEF-UL-SF** and **DEF-DL-SF** service flows to be correctly used, the following translation rules must be installed during the system setup phase:

- **DEF-UL-SS-RL** (**Default Uplink Rule – SS side**): Defined in the AP to translate the original source MAC address of the packets to the *VMAC_DEF_UL* address when the dedicated translation rules for the MN are not yet installed. As a consequence, the uplink packets are redirected to the **DEF-UL-SF** service flow.
- **DEF-DL-BS-RL** (**Default Downlink Rule – BS side**): Installed in the AR to replace the original destination MAC address of the packets by the broadcast MAC address (*BC_MAC*). Consequently, the downlink packets are sent in the **DEF-DL-SF** service flow.

During the system setup phase, we must allow that Router Advertisement (RA) messages from the IPv6 Neighbour Discovery Process (NDP) are sent through the incoming MNs. This allows the MNs that will attach to the network to immediately configure an IPv6 global address. RA messages must be received by all the MNs immediately after they access the network. For this reason, we create the **RA-DL-SF** (Router Advertisement Downlink Service Flow) service flow using the broadcast MAC address as the classification parameter. Since the RA destination MAC address is the all-nodes multicast MAC address (33:33:00:00:00:01), we must install the **RA-DL-BS-RL** (**Router Advertisement Downlink Rule**) translation rule in the BS side entity to translate the all-nodes multicast MAC address to the broadcast MAC address (*BC_MAC*).

The remaining messages from the IPv6 NDP, in particular, the Router Solicitation (RS), the Neighbour Solicitation (NS), and the Neighbour Advertisement (NA) messages, are only sent when the MN is already connected to the network. Thus, the support of these messages by the 802.16 system will be depicted in section 4.3.7.

To summarize, Table 13 shows the group of service flows established during the system setup phase.

Service Flow	Classification	Type of traffic	Direction
AP-DL-SF	AP_MAC	16CP signalling	Downlink
AP-UL-SF	AP_MAC	16CP signalling	Uplink
AUX-DL-SF	VMAC_AUX_DL	IPv6 NDP signalling QoSAL signalling (RA not included)	Downlink
		Data (backup case)	
AUX-UL-SF	VMAC_AUX_UL	IPv6 NDP signalling QoSAL signalling (RA not included)	Uplink
		Data (backup case)	
DEF-DL-SF	BC_MAC	IPv6 NDP signalling QoSAL signalling (RA not included) (default case)	Downlink
		Data (default case)	
DEF-UL-SF	VMAC_DEF_UL	IPv6 NDP signalling QoSAL signalling (RA not included) (default case)	Uplink
		Data (default case)	
RA-DL-SF	BC_MAC	IPv6 NDP signalling (RA only)	Downlink

Table 13: Service flows created during the system setup phase

Table 14 illustrates the translation rules installed during the system setup phase.

Translation Rule	Filter	Direction	Entity
DEF-DL-BS-RL	NO_RULE → BC_MAC	Downlink	AR
DEF-UL-SS-RL	NO_RULE → VMAC_DEF_UL	Uplink	AP MN
RA-DL-BS-RL	ALL_NODES_MAC → BC_MAC	Downlink	AR

Table 14: Translation rules installed during the system setup phase

4.3.2. Fast MN Network Access

Immediately after the MN connects to the network, the AP is notified and the MN network access process begins. At this point, the following translation rules must be installed:

- **AUX-UL-SS-RL** (**Auxiliary Uplink Rule – SS side**): Defined in the SS side entity (AP) to translate the original source MAC address of the packets by the *VMAC_AUX_UL* address. Allows uplink packets to be sent in the **AUX-UL-SF** service flow.
- **AUX-DL-BS-RL** (**Auxiliary Downlink Rule – BS side**): Defined in the BS side entity (AR) to translate the destination MAC address of the packets by the *VMAC_AUX_DL* address. Downlink packets will be sent in the **AUX-DL-SF** service flow after this rule is applied.
- **AUX-DL-SS-RL** (**Auxiliary Downlink Rule – SS side**): Installed in the SS side entity (AP) to perform the reverse translation from the *VMAC_AUX_DL* address to the original destination MAC address. As a result, downlink packets can be delivered to the MN without packet loss.

After the **AUX-UL-SS-RL** and the **AUX-DL-SS-RL** translation rules are installed in the SS side entity (AP), the MN MAC address must be sent to the AR. A Mobile Node Access Request (***MNA-REQ***) message, from the 16CP, containing the MN MAC address, is sent by the AP to the AR. The **AP-UL-SF** service flow, which has been created during the system setup phase with the AP MAC address as the classification parameter, is used to send the message to the AR, as shown in Figure 27. The AR receives the ***MNA-REQ*** message and installs the associated translation rule – **AUX-DL-BS-RL**. This rule replaces the original destination MAC address of the packets by the *VMAC_AUX_DL* address. Packets can then be sent in the downlink direction using the **AUX-DL-SF**. When these packets reach the AP, they are reverse translated by the previously installed **AUX-DL-SS-RL** translation rule and delivered to the MN. Notice that in Figure 27, the two-hop scenario message charter is illustrated.

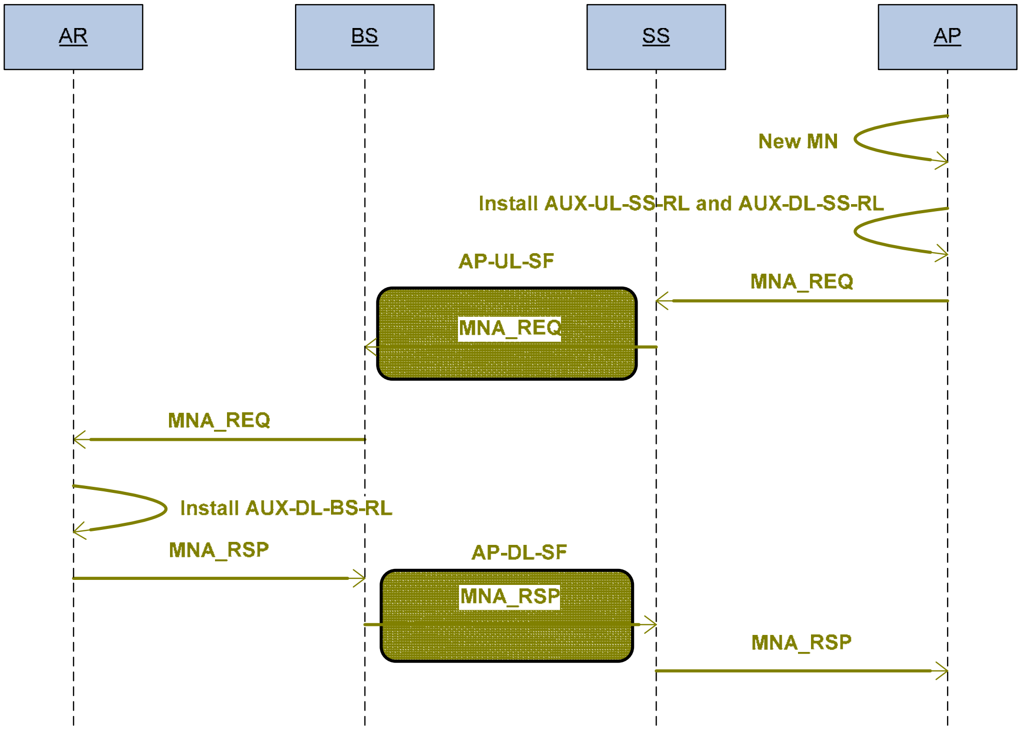

Figure 27: MN access network phase (two-hop scenario)

Finally, a response is sent to the AP using the ***MNA-RSP*** message indicating that the MN MAC address has been received and the correspondent translation rule has been installed (**AUX-DL-BS-RL**).

While the previously mentioned translation rules are being installed, the MN can start sending/receiving packets. In this specific situation, the auxiliary service flows are not ready to be used while the translation rules are not installed. Therefore, the default service flows are used – **DEF-UL-SF** and **DEF-DL-SF**. In the downlink direction, the destination MAC address of the packets is translated in the AR to the broadcast MAC address (*BC_MAC*), using the **DEF-DL-BS-RL** translation rule, and sent in the **DEF-DL-SF** service flow in the wireless link. This process is demonstrated in Figure 28.

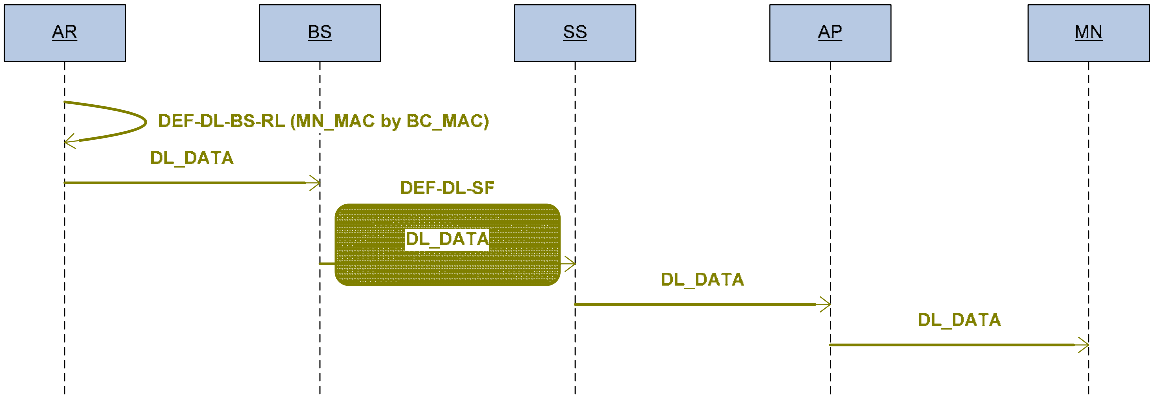

Figure 28: Downlink default service flow (two-hop scenario)

The uplink direction scenario is shown in Figure 29. In this case, the source MAC address of the packets is translated in the AP to the *VMAC_DEF_UL* address, using the **DEF-UL-SS-RL** translation rule, and sent in the **DEF-UL-SF** service flow in the 802.16 system.

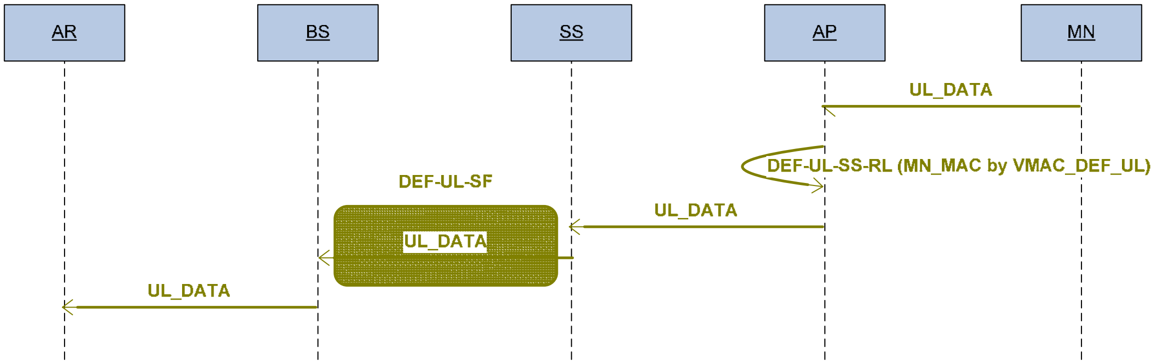

Figure 29: Uplink default service flow (two-hop scenario)

Table 15 shows the translation rules installed during the MN network access phase.

Translation Rule	Filter	Direction	Entity
AUX-DL-BS-RL	MN_MAC → VMAC_AUX_DL	Downlink	AR
AUX-DL-SS-RL	VMAC_AUX_DL → MN_MAC	Uplink	AP
AUX-UL-SS-RL	MN_MAC → VMAC_AUX_UL	Uplink	AP MN

Table 15: Translation rules during the MN network access phase

4.3.3. Dynamic Service Reservation

Our approach for the classification process is to use Ethernet as the CS. Therefore, all packets for the MN will be classified based on the MN MAC address. However, instead of using the MN MAC address to classify the packets, we use a VMAC address, allowing each service to have a dedicated service flow, with a specific VMAC address. Nevertheless, the establishment of a service flow in the 802.16 equipment is time consuming. Thus, a workaround must be found to allow packets to traverse the wireless link while the service flow is being reserved. Sections 4.3.3.1 and 4.3.3.2 depict the adopted solutions for the uplink and downlink service reservations, respectively.

4.3.3.1. Dynamic Uplink Service Reservation

Suppose that the MN starts running service S1. The S1 data packets must cross the 802.16 system in the uplink direction and reach the AR. When the data packets reach the AR, a new flow is detected and the layer 3 QoS reservation process is triggered. Thus, despite no reservation for the launched service S1 has been allocated in the 802.16 system, the data packets sent by the MN must be able to traverse the air link and reach the AR. To allow uplink data packets to be delivered to the AR without a dedicated service flow allocated, we use the **AUX-UL-SS-RL** translation rule in the AP created during the MN network access phase. This translation rule replaces the source MAC address of the S1 data packets (MN MAC address) by the *VMAC_AUX_UL* address. As a result, these packets are redirected to the **AUX-UL-SF** service flow. Figure 30 illustrates this process.

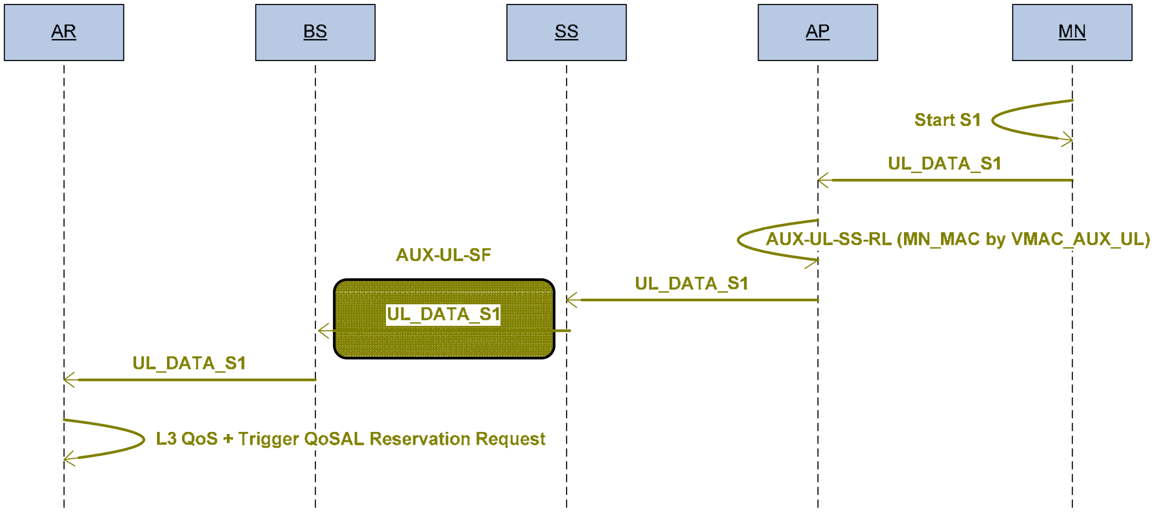
AR
BS
SS
AP
MN
Start S1
UL_DATA_S1
AUX-UL-SS-RL (MN_MAC by VMAC_AUX_UL)
AUX-UL-SF
UL_DATA_S1
UL_DATA_S1
UL_DATA_S1
L3 QoS + Trigger QoSAL Reservation Request

Figure 30: Uplink pre-reservation phase (two-hop scenario)

When the uplink data packets reach the AR, the layer 3 reservation process in the AR for service S1 is triggered. Following, the QoSM provides the QoS parameters that must be used for the requested connection to the QoSAL through the Abstract Interface (AI). After the QoSAL module is triggered, an ***AL-CNX-ACTIVATE-REQ*** message is sent to the MN, and the MN replies with an ***AL-CNX-ACTIVATE-RESP*** message to the AR. For a deep overview about the QoSAL process, please refer to section 3.2. The QoSAL messages are sent in the 802.16 system through the auxiliary service flows (**AUX-DL-SF** and **AUX-UL-SF**) defined for the MN during the network access phase. To redirect the QoSAL packets to the auxiliary service flows, the associated translation rules are used (**AUX-DL-BS-RL** in the AR and the **AUX-DL-SS-RL** and **AUX-UL-SS-RL** in the AP). Figure 31 illustrates this process.

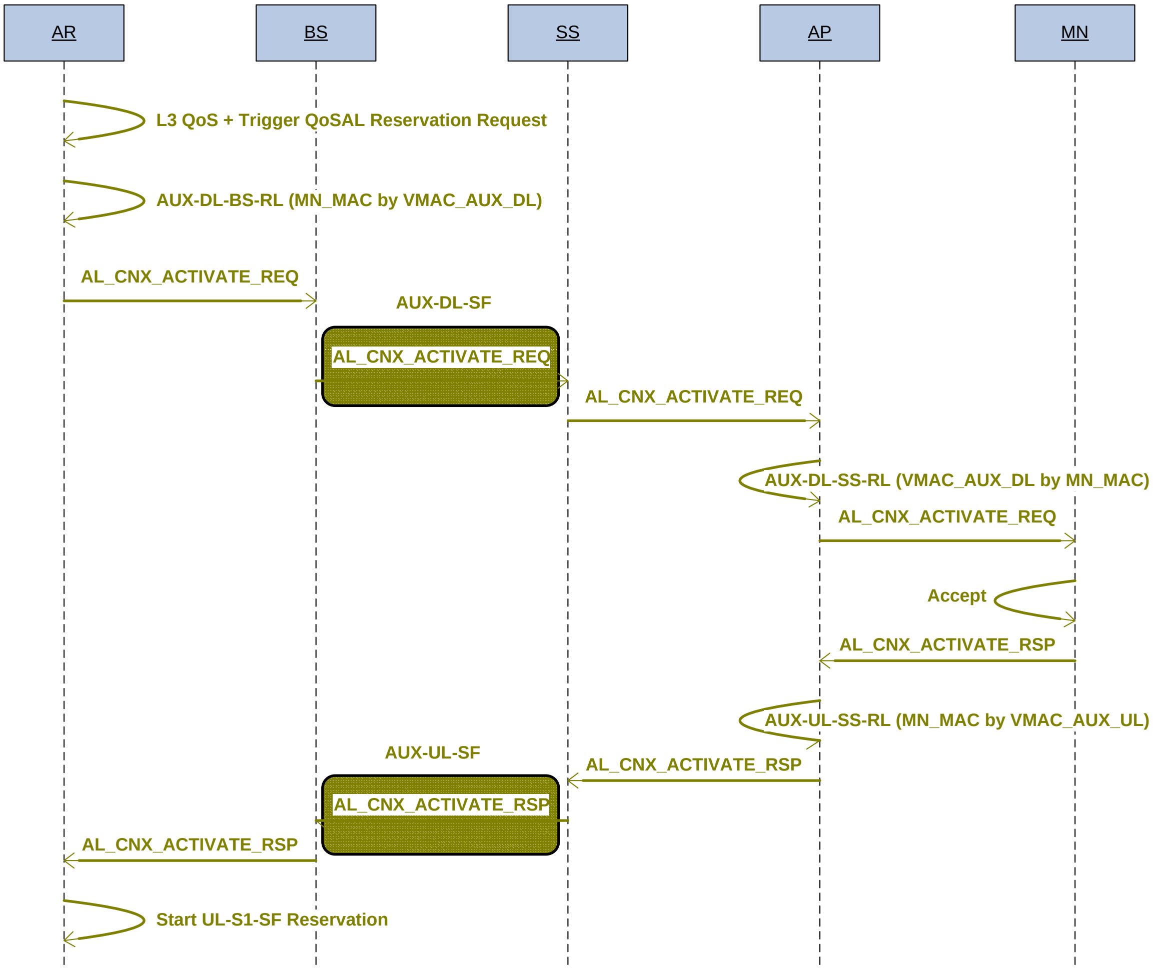

Figure 31: QoSAL uplink connection reservation (two-hop scenario)

When the ***AL-CNX-ACTIVATE-RESP*** message reaches the AR, an ***ALD-CNX-ACTIVATE-REQ*** primitive is sent to the 802.16-BS Driver through the Driver Interface (DI). As a consequence, the 802.16-BS Driver will verify if enough resources are available to satisfy the requested QoS parameters and, if the resources are enough, establish a service flow in the 802.16 air link for service S1 – **UL-S1-SF** service flow. Instead of using the MN MAC address as the classification parameter, this service flow uses a dedicated VMAC address (*VMAC_S1_UL*) to perform service S1 packets classification. To establish the **UL-S1-SF** service flow in the 802.16 equipment, a ***SF-RESV-REQ*** message (see section 4.4.2) from the 16CP is sent to the AP. The message is received by the AP and starts the installation of the service flow in the 802.16 system through the SS. When the dedicated uplink service flow reservation is completed (**UL-**

S1-SF), the AP sends a ***SF-RESV-RSP*** message (see section 4.4.2) to the AR. The explained service flow reservation process is shown in Figure 32.

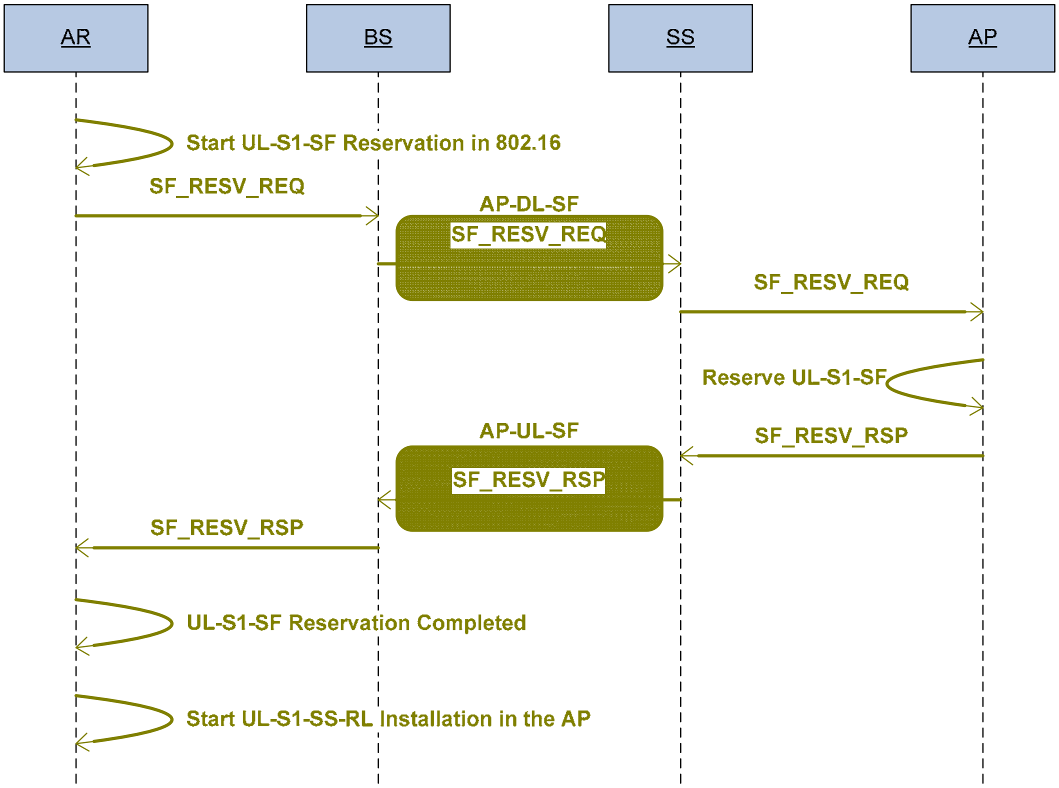
AR
BS
SS
AP
Start UL-S1-SF Reservation in 802.16
SF_RESV_REQ
AP-DL-SF
SF_RESV_REQ
SF_RESV_REQ
Reserve UL-S1-SF
AP-UL-SF
SF_RESV_RSP
SF_RESV_RSP
SF_RESV_RSP
UL-S1-SF Reservation Completed
Start UL-S1-SS-RL Installation in the AP

Figure 32: Uplink service flow reservation (UL-S1-SF) (two-hop scenario)

The AR receives this information and is able to start the **UL-S1-SS-RL** translation rule installation in the AP. For this process, the AR sends a ***TR-INST-REQ*** message (see section 4.4.5) to the AP using the **AP-DL-SF** service flow. The **UL-S1-SS-RL** translation rule states that uplink packets from service S1 already have a dedicated service flow allocated (**UL-S1-SF**) and must be sent through it. Therefore, the source MAC address of the S1 packets is replaced by the *VMAC_S1_UL* address from the **UL-S1-SF** service flow. After the rule is installed, a ***TR-INST-RSP*** message (see section 4.4.5) is sent to the AR through the **AP-UL-SF** service flow. This process is shown in Figure 33.

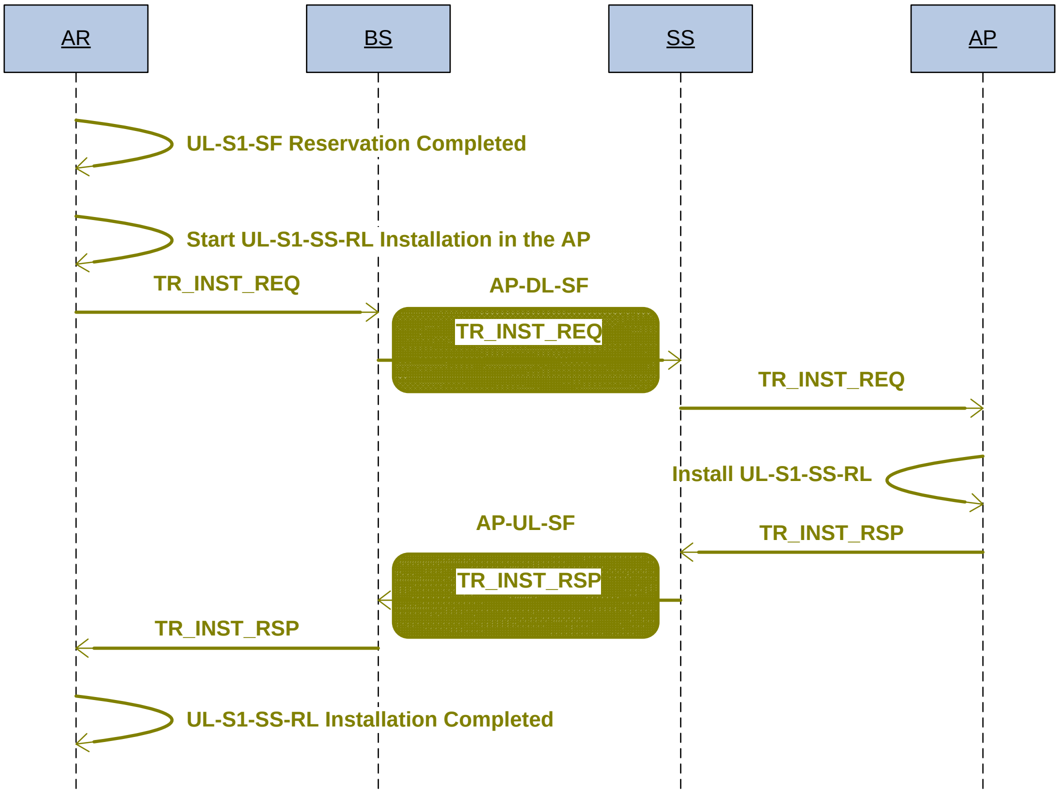

Figure 33: Uplink translation rule installation (UL-S1-RL) (two-hop scenario)

Finally, S1 packets can be sent in its dedicated service flow – **UL-S1-SF**, using the requested QoS parameters. Figure 34 illustrates S1 packets flowing from the MN to the AR through the **UL-S1-SF** service flow.

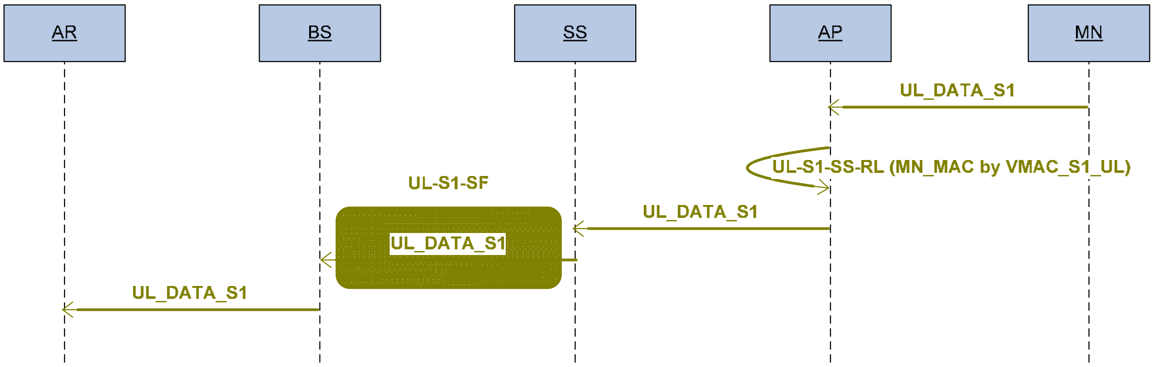

Figure 34: Uplink S1 data packets (two-hop scenario)

Briefly summarizing, Table 16 and Table 17 illustrate the created service flow and the installed translation rule during the uplink service reservation phase.

Service Flow	Classification	Type of traffic	Direction
UL-S1-SF	VMAC_S1_UL	Service S1 Data	Uplink

Table 16: Service flow created during the uplink service reservation

Translation Rule	Filter	Direction	Entity
UL-S1-SS-RL	MN_MAC → VMAC_S1_UL	Uplink	AP MN

Table 17: Translation rules installed during the uplink service reservation phase

4.3.3.2. Dynamic Downlink Service Reservation

In the previous section, we illustrated the uplink service reservation scenario. In this section, we will depict the downlink service reservation scenario.

Suppose that the AR receives an incoming packet from service S2 whose destination is the MN. The QoS reservation process is started. However, as mentioned in the previous section, the service flow reservation is not an instantaneous process. Therefore, during the QoS reservation process, packets will traverse the air link through the **AUX-DL-SF** service flow, through the usage of the **AUX-DL-BS-RL** and **AUX-DL-SS-RL** translation rules. This process is illustrated in Figure 35.

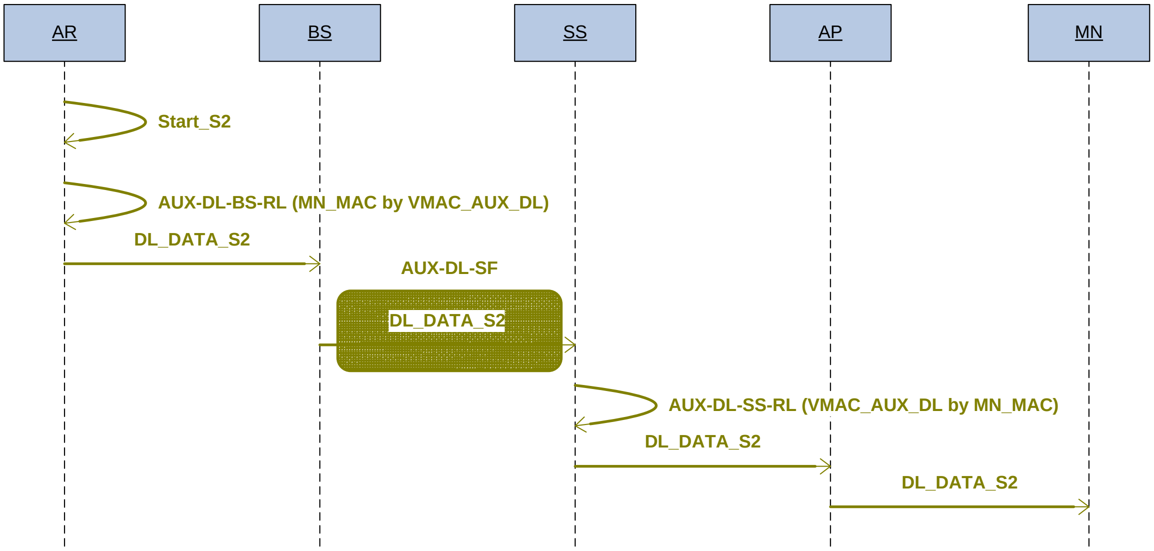
AR
BS
SS
AP
MN
Start_S2
AUX-DL-BS-RL (MN_MAC by VMAC_AUX_DL)
DL_DATA_S2
AUX-DL-SF
DL_DATA_S2
AUX-DL-SS-RL (VMAC_AUX_DL by MN_MAC)
DL_DATA_S2
DL_DATA_S2

Figure 35: Downlink pre-reservation phase (two-hop scenario)

As a consequence of the QoS process, the 802.16-BS Driver receives a QoSAL message indicating a QoS reservation request. The 802.16 dedicated service flow creation for service S2 (**DL-S2-SF**) is triggered. Instead of using the MN MAC address as the classification parameter, this service flow uses a specific VMAC address (*VMAC_S2_DL*) to perform the packets classification. To establish the **DL-S2-SF** service flow in the 802.16 equipment, a ***SF-RESV-REQ*** message is sent to the AP. The AP receives the message and starts the installation of the service flow in the 802.16 system through the SS. Figure 36 provides detailed information about the **DL-S2-SF** service flow installation. When the dedicated downlink service flow reservation is over, a ***SF-RESV-RSP*** message is sent to the AR.

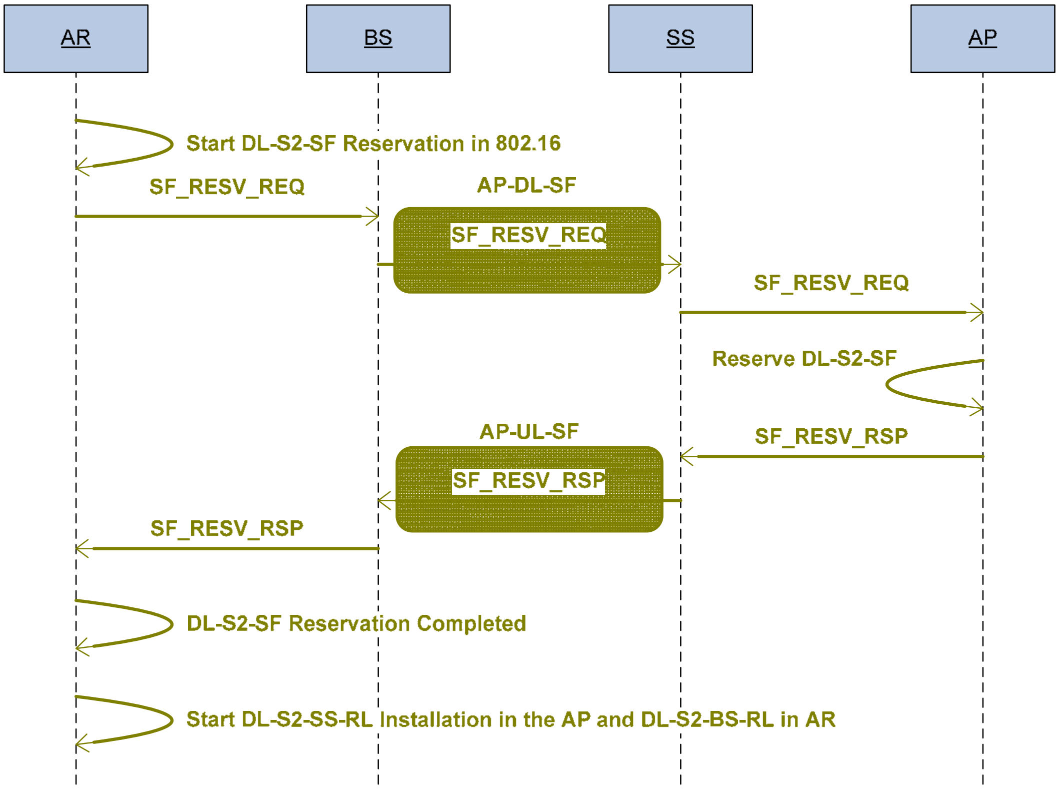
AR
BS
SS
AP
Start DL-S2-SF Reservation in 802.16
SF_RESV_REQ
AP-DL-SF
SF_RESV_REQ
SF_RESV_REQ
Reserve DL-S2-SF
AP-UL-SF
SF_RESV_RSP
SF_RESV_RSP
SF_RESV_RSP
DL-S2-SF Reservation Completed
Start DL-S2-SS-RL Installation in the AP and DL-S2-BS-RL in AR

Figure 36: Downlink service flow reservation (DL-S2-SF) (two-hop scenario)

After the **DL-S2-SF** service flow installation is completed, the translation rules in the AR and in the AP can be installed. Basically, a rule must be installed in the AR to replace the original destination MAC address of the downlink packets by the *VMAC_S2_DL* address. This way, downlink packets from service S2 are sent in the **DL-S2-SF** service flow. When these packets reach the AP, the reverse translation must be applied – replace the destination MAC address of the packet (*VMAC_S2_DL* address) by the MN MAC address (original destination MAC address). We start by installing the **DL-S2-SS-RL** translation rule in the AP, guaranteeing that we have no packet loss during the translation rules installation period. To install the **DL-S2-SS-RL** translation rule, the AR sends a ***TR-INST-REQ*** message to the AP using the **AP-DL-SF** service flow. After the **DL-S2-SS-RL** translation rule is installed, a ***TR-INST-RSP*** message is sent to the AR. The AR receives the ***TR-INST-RSP*** message and starts the installation of the **DL-S2-BS-RL** translation rule. Figure 37 shows the translation rules installation process.

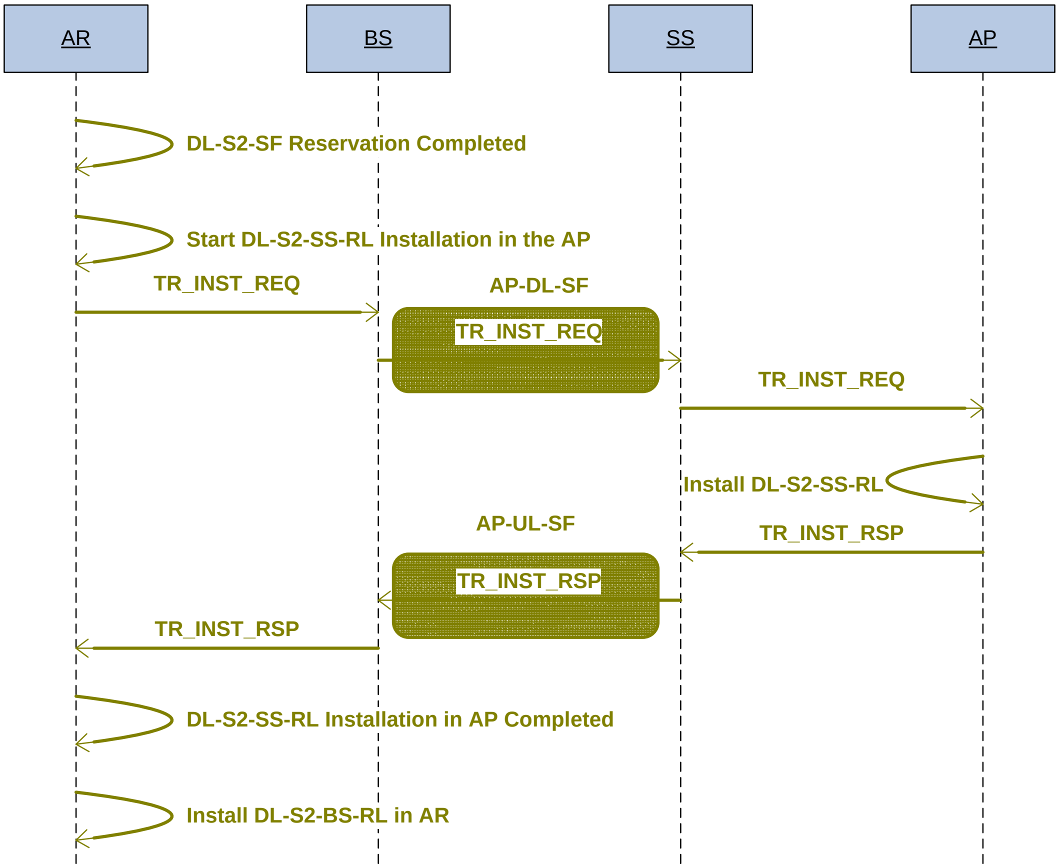
AR
BS
SS
AP
DL-S2-SF Reservation Completed
Start DL-S2-SS-RL Installation in the AP
TR_INST_REQ
AP-DL-SF
TR_INST_REQ
TR_INST_REQ
Install DL-S2-SS-RL
AP-UL-SF
TR_INST_RSP
TR_INST_RSP
TR_INST_RSP
DL-S2-SS-RL Installation in AP Completed
Install DL-S2-BS-RL in AR

Figure 37: Downlink translation rule installation (DL-S2-RL) (two-hop scenario)

Finally, downlink packets start flowing through the **DL-S2-SF** service flow as seen in Figure 38.

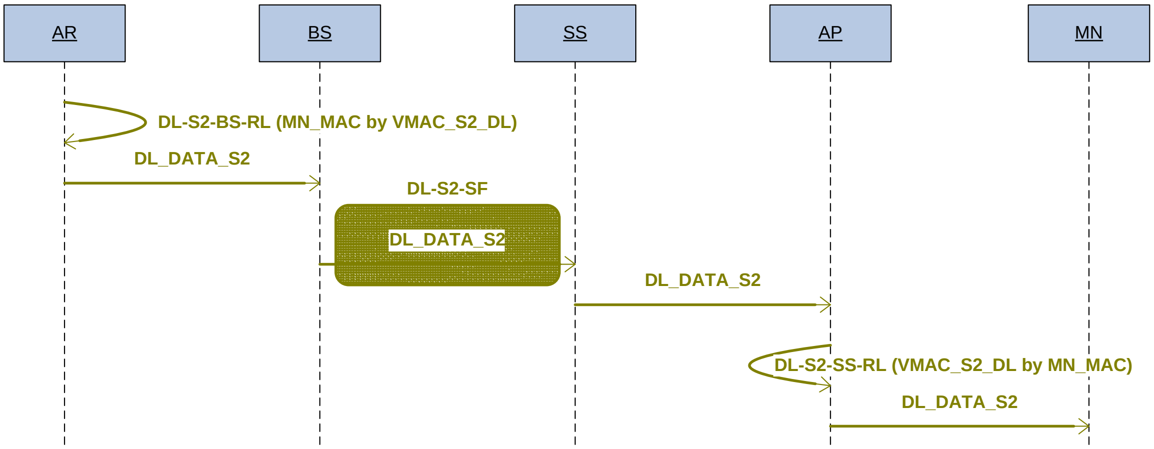
AR
BS
SS
AP
MN
DL-S2-BS-RL (MN_MAC by VMAC_S2_DL)
DL_DATA_S2
DL-S2-SF
DL_DATA_S2
DL_DATA_S2
DL-S2-SS-RL (VMAC_S2_DL by MN_MAC)
DL_DATA_S2

Figure 38: Downlink S2 data packets (two-hop scenario)

Table 18 and Table 19 illustrate the created service flow and the installed translation rules during the downlink service reservation phase.

Service Flow	Classification	Type of traffic	Direction
DL-S2-SF	VMAC_S2_DL	Service S2 Data	Downlink

Table 18: Service flow created during the downlink service reservation

Translation Rule	Filter	Direction	Entity
DL-S2-BS-RL	MN_MAC → VMAC_S2_DL	Downlink	AR
DL-S2-SS-RL	VMAC_S2_DL → MN_MAC	Downlink	AP MN

Table 19: Translation rules installed during the downlink service reservation phase

4.3.4. Dynamic Service Modification

Already allocated services, in the downlink and uplink directions, must support dynamic modifications of the QoS parameters, avoiding traffic disruption during the modification process. Sections 4.3.4.1 and 4.3.4.2 present the adopted solution to support services modification in the downlink and in the uplink directions, respectively.

4.3.4.1. Dynamic Downlink Service Flow Modification

In this case, suppose that service S2 has to be modified. After the downlink reservation process is completed, a dedicated service flow (**DL-S2-SF**) for service S2 is allocated (process explained in section 4.3.3.2). The associated translation rules (**DL-S2-BS-RL** and **DL-S2-SS-RL** translation rules) are also installed.

Suppose that a modification message is sent to the AR with a set of QoS parameters to replace the existing ones of the **DL-S2-SF** service flow. It is mandatory that the QoS parameters of the **DL-S2-SF** service flow are changed without interrupting the data packets that are flowing through the service flow. However, we must not forget that the modification process of a service flow in the 802.16 system is not instantaneous. For this to be possible, we will have to send the downlink data packets in the **AUX-DL-SF** service flow during the modification period instead of using the **DL-S2-SF** service flow. To achieve this, we must block the previously installed **DL-S2-BS-RL** translation rule in the AR. After the translation rule is blocked, the data packets are automatically redirected to the **AUX-DL-SF** service flow and we can perform the QoS parameters modifications in the **DL-S2-SF** service flow without interruptions. To perform the service flow modification, a ***SF-MOD-REQ*** message (see section 4.4.3) is sent to the AP. As a reply, the AR receives a ***SF-MOD-RSP*** message (see section 4.4.3) indicating that the service flow modification is completed. Figure 39 illustrates this process.

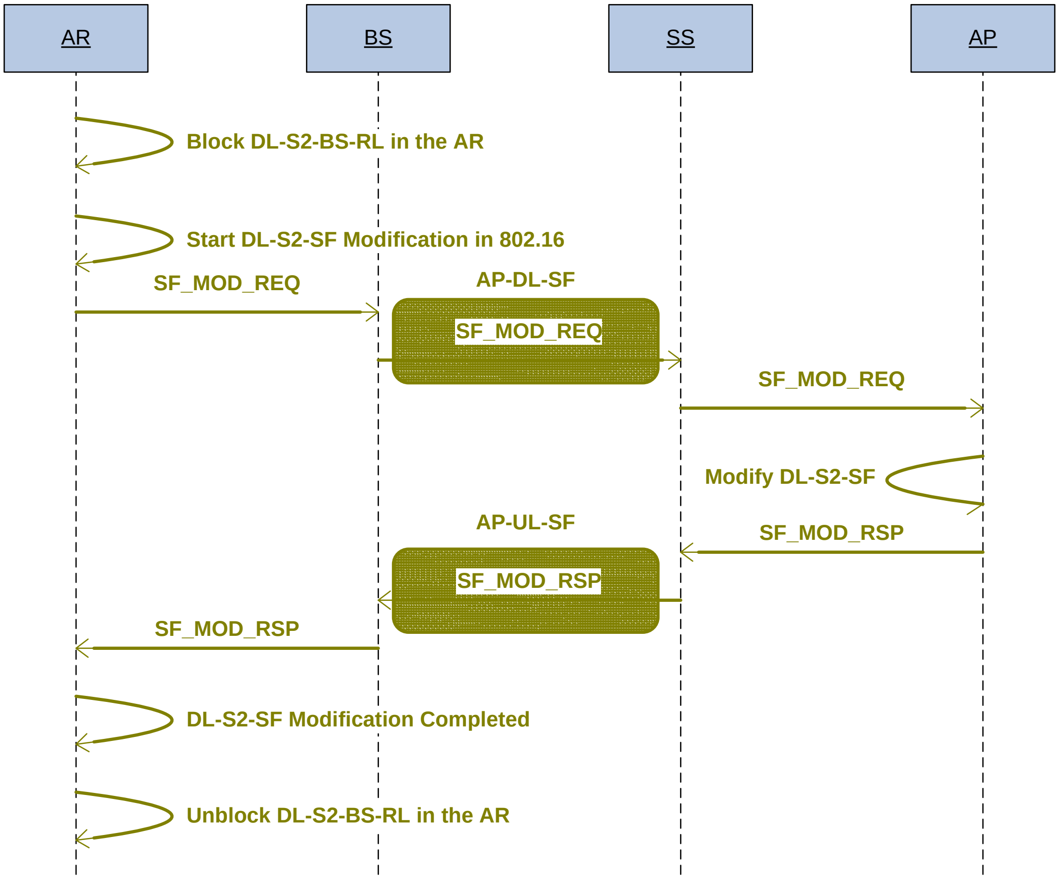
AR
BS
SS
AP
Block DL-S2-BS-RL in the AR
Start DL-S2-SF Modification in 802.16
SF_MOD_REQ
AP-DL-SF
SF_MOD_REQ
SF_MOD_REQ
Modify DL-S2-SF
AP-UL-SF
SF_MOD_RSP
SF_MOD_RSP
SF_MOD_RSP
DL-S2-SF Modification Completed
Unblock DL-S2-BS-RL in the AR

Figure 39: Downlink service flow modification (DL-S2-SF)

When the **DL-S2-SF** service flow QoS parameters modification is finished, data packets can be sent again in the **DL-S2-SF** service flow. To redirect service S2 packets to the **DL-S2-SF,** we must unblock the **DL-S2-BS-RL** translation rule in the AR.

4.3.4.2. Dynamic Uplink Service Flow Modification

In this case, an uplink service (service S1) is being used by the MN. The dedicated service flow (**UL-S1-SF**) and the translation rules are created as explained in section 4.3.3.1. If the QoS parameters of the **UL-S1-SF** service flow have to be modified, it must be performed without affecting the uplink data packets that are traversing the service flow. To achieve this, the uplink data packets must be sent in the **AUX-UL-SF** instead of being sent in the dedicated service flow for service S1 (**UL-S1-SF**). To redirect the packets to the **AUX-UL-SF** service flow during the modification period, we must block the **UL-S1-SS-RL** translation rule in the AP. Therefore, a ***TR-BLK-REQ*** message (see section 4.4.6) is sent by the AR to the AP, indicating the translation rule that must be blocked. After the translation rule is blocked, a ***TR-BLK-RSP*** (see section 4.4.6) message is sent to the AR as a response to the translation rule block request. This process is shown in Figure 40.

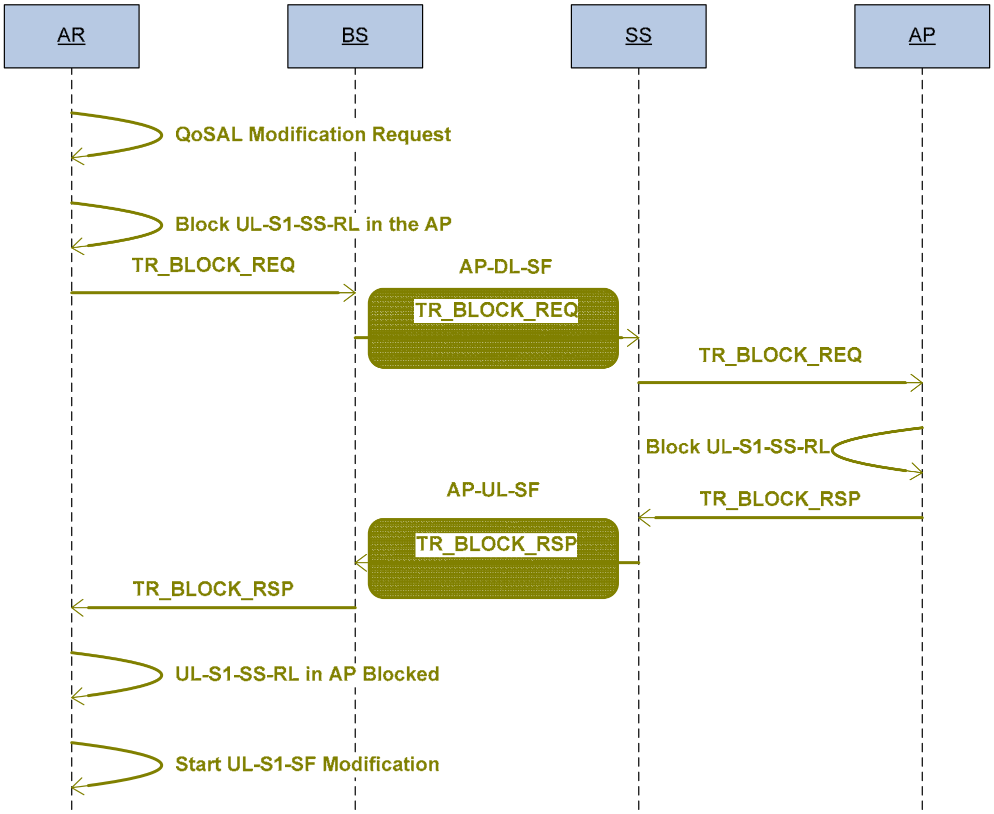

Figure 40: Uplink translation rule block (UL-S1-RL) (two-hop scenario)

At this moment, the service flow can be modified without affecting the service S1 packets. The AR sends a ***SF-MOD-REQ*** message to the AP to modify the QoS parameters of the service flow. While the **UL-S1-SF** service flow QoS parameters are being modified, the uplink data packets from service S1 are sent in the **AUX-UL-SF** service flow. This redirection process is very useful since it avoids any traffic losses of incoming packets from the MN. The service flow modification process is shown in Figure 41.

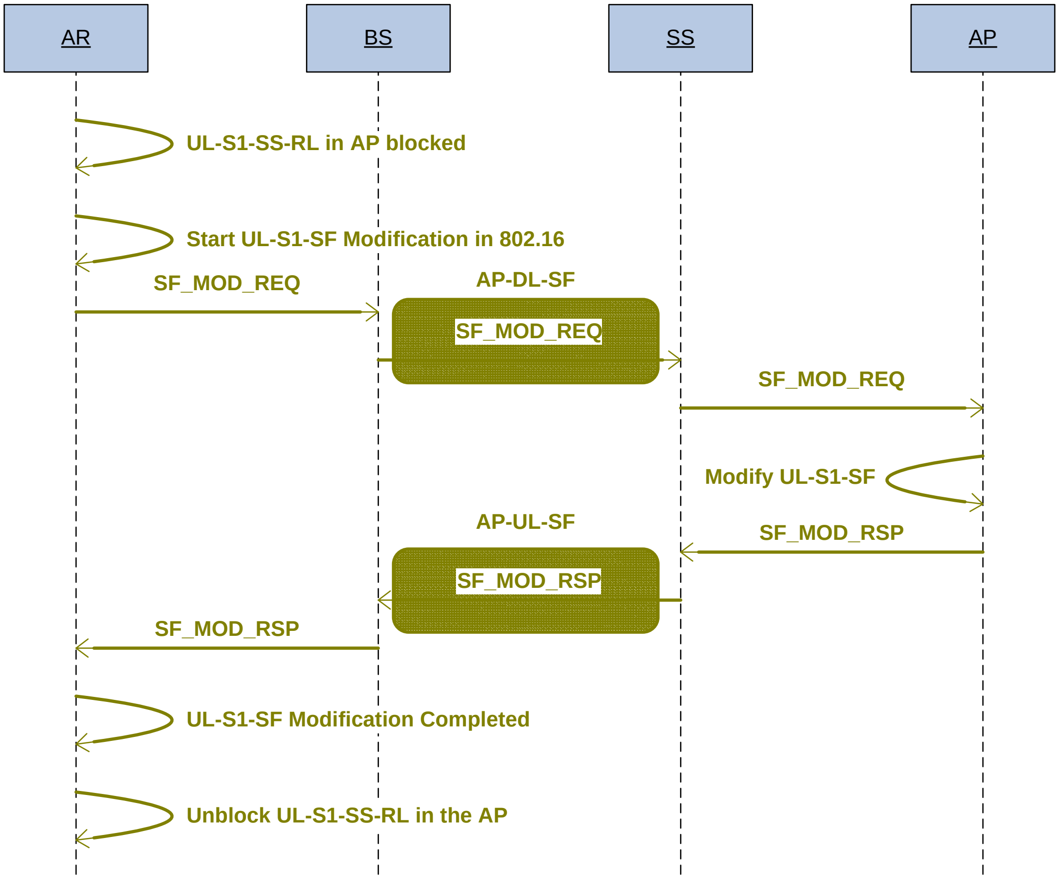
AR
BS
SS
AP
UL-S1-SS-RL in AP blocked
Start UL-S1-SF Modification in 802.16
SF_MOD_REQ
AP-DL-SF
SF_MOD_REQ
SF_MOD_REQ
Modify UL-S1-SF
AP-UL-SF
SF_MOD_RSP
SF_MOD_RSP
SF_MOD_RSP
UL-S1-SF Modification Completed
Unblock UL-S1-SS-RL in the AP

Figure 41: Uplink service flow modification (UL-S1-SF) (two-hop scenario)

When the modification period is over, an ***SF-MOD-RSP*** message is sent to the AR. As a result, uplink data packets from service S1 must be redirected again to the dedicated **UL-S1-SF** service flow. To achieve this, we must unblock the **UL-S1-SS-RL** translation rule in the AP by sending a ***TR-UNBLK-REQ*** (see section 4.4.7) message from the 16CP. The AP unblocks the **UL-S1-SS-RL** translation rule and sends a ***TR-UNBLK-RSP*** message to the AR through the **AP-UL-SF** service flow, indicating that the translation rule is already installed. Figure 42 illustrates this scenario.

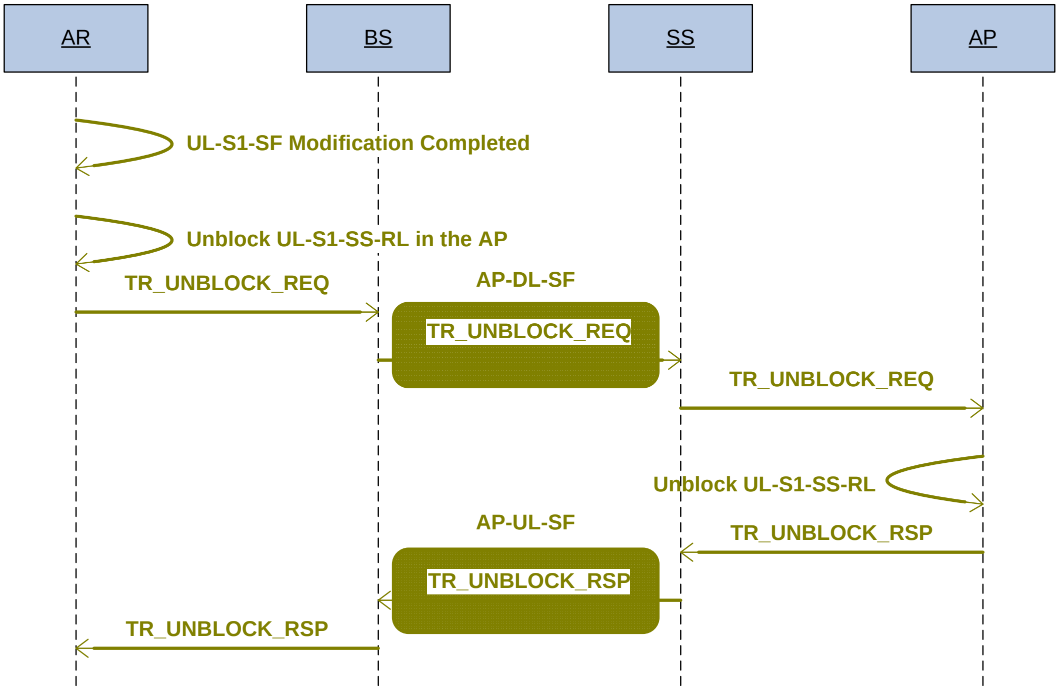

Figure 42: Uplink translation rule unblock (UL-S1-RL) (two-hop scenario)

After the **UL-S1-SS-RL** translation rule is unblocked, the original source MAC address (MN MAC address) of the uplink packets from service S1 is automatically replaced by the *VMAC_S1_UL* address. Therefore, the uplink service flow modification process is completed and the packets start being sent in the **UL-S1-SF** service flow.

4.3.5. Dynamic Service Differentiation

Service differentiation is achieved through the usage of the VMAC addresses. If we assign each service a specific VMAC address in the 802.16 link, a different connection will be used and therefore different QoS parameters will be applied for each service data packets. Differentiation is successfully achieved under these conditions.

4.3.5.1. Dynamic Downlink Service Differentiation

Services S3 and S4 are used to demonstrate the differentiation process. The reservation process for services S3 and S4 is similar to the downlink reservation process already explained in section 4.3.3.2. When the downlink reservation processes are completed, the dedicated service flows **DL-S3-SF** and **DL-S4-SF** are allocated. The associated downlink translation rules for service S3 (**DL-S3-BS-RL** and **DL-S3-SS-RL**) and for service S4 (**DL-S4-BS-RL** and **DL-S4-SS-RL**) are also installed. This way, packets belonging to different services will be sent in different service flows in the 802.16 link even if they are sent to the same MN. Figure 43 shows the services S3 and S4 being used simultaneously by the MN and with QoS differentiation through the usage of dedicated VMAC addresses.

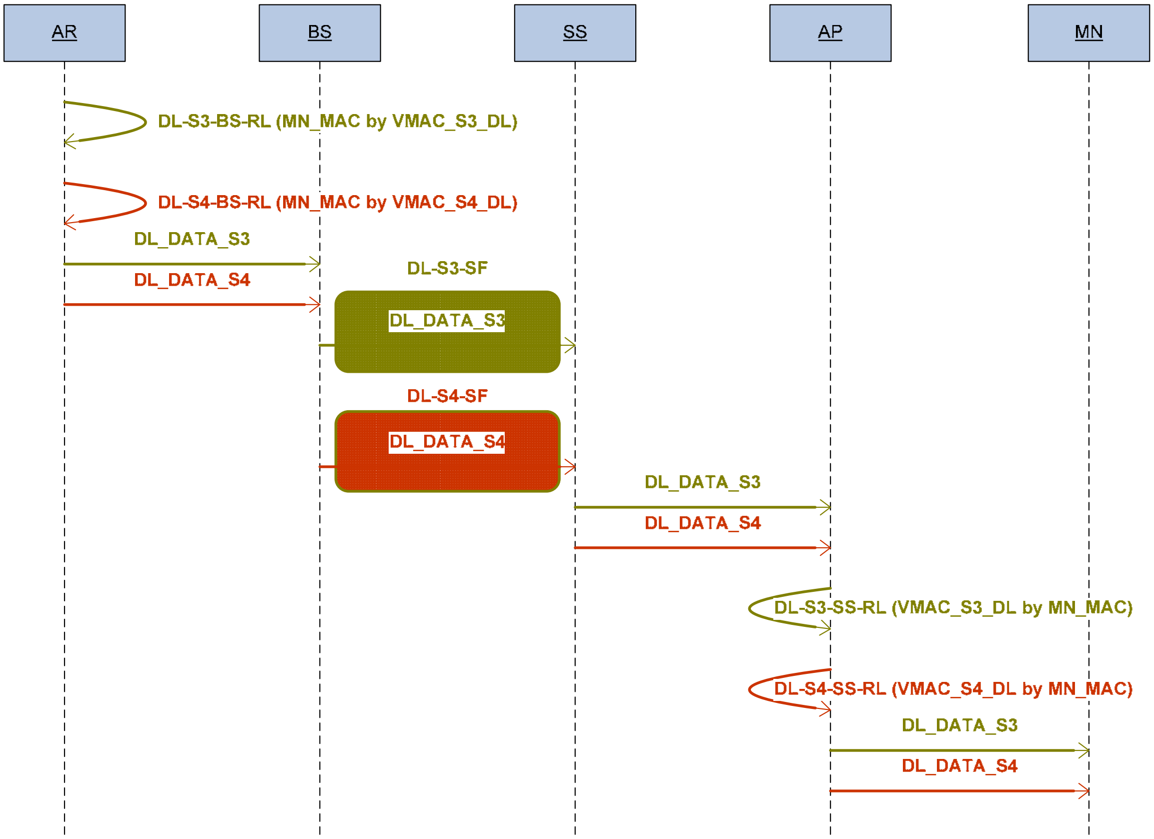
AR
BS
SS
AP
MN
DL-S3-BS-RL (MN_MAC by VMAC_S3_DL)
DL-S4-BS-RL (MN_MAC by VMAC_S4_DL)
DL_DATA_S3
DL_DATA_S4
DL-S3-SF
DL_DATA_S3
DL-S4-SF
DL_DATA_S4
DL_DATA_S3
DL_DATA_S4
DL-S3-SS-RL (VMAC_S3_DL by MN_MAC)
DL-S4-SS-RL (VMAC_S4_DL by MN_MAC)
DL_DATA_S3
DL_DATA_S4

Figure 43: Downlink dynamic service differentiation (two-hop scenario)

The **DL-S3-BS-RL** translation rule is applied in the AR to the downlink data packets from service S3. As a consequence, the original destination MAC address of the packets

(MN MAC address) is replaced by the *VMAC_S3_DL* address. These data packets are classified by the BS and sent to the air link in the **DL-S3-SF** service flow. When they are delivered to the AP, the reverse translation rule **DL-S3-SS-RL** is applied. This rule replaces the destination MAC address of the packets (*VMAC_S3_DL*) by the MN MAC address. Finally, packets are delivered to the MN. The same process is applied to the data packets from service S4. The **DL-S4-BS-RL** translation rule is applied in the AR, replacing the original destination MAC address (MN MAC address) by the *VMAC_S4_DL* address. Packets are classified by the BS and sent in the **DL-S4-SF** service flow to the AP. The AP applies the **DL-S4-SS-RL** translation rule, and the destination MAC address of the packet (*VMAC_S4_DL*) is replaced by the MN MAC address. After the translation rule is applied in the AP, data packets can be delivered to the MN without losses or delays.

4.3.5.2. Dynamic Uplink Service Differentiation

The uplink process is similar to the downlink process explained in the previous section. Two services are used to illustrate the uplink service differentiation – services S5 and S6. In the AP, the **UL-S5-SS-RL** translation rule is applied to the uplink data packets from service S5. That is, the original source MAC address of the incoming packets (MN MAC address) is replaced by the *VMAC_S5_UL* address. As a consequence, packets are classified by the SS and sent in the **UL-S5-SF** service flow to be delivered to the AR. The **UL-S6-SS-RL** translation rule is also applied in the AP to the service S6 packets. Original source MAC addresses (MN MAC addresses) are replaced by the *VMAC_S6_UL* addresses, and sent in the **UL-S6-SF** service flow through the AR. Figure 44 presents this scenario.

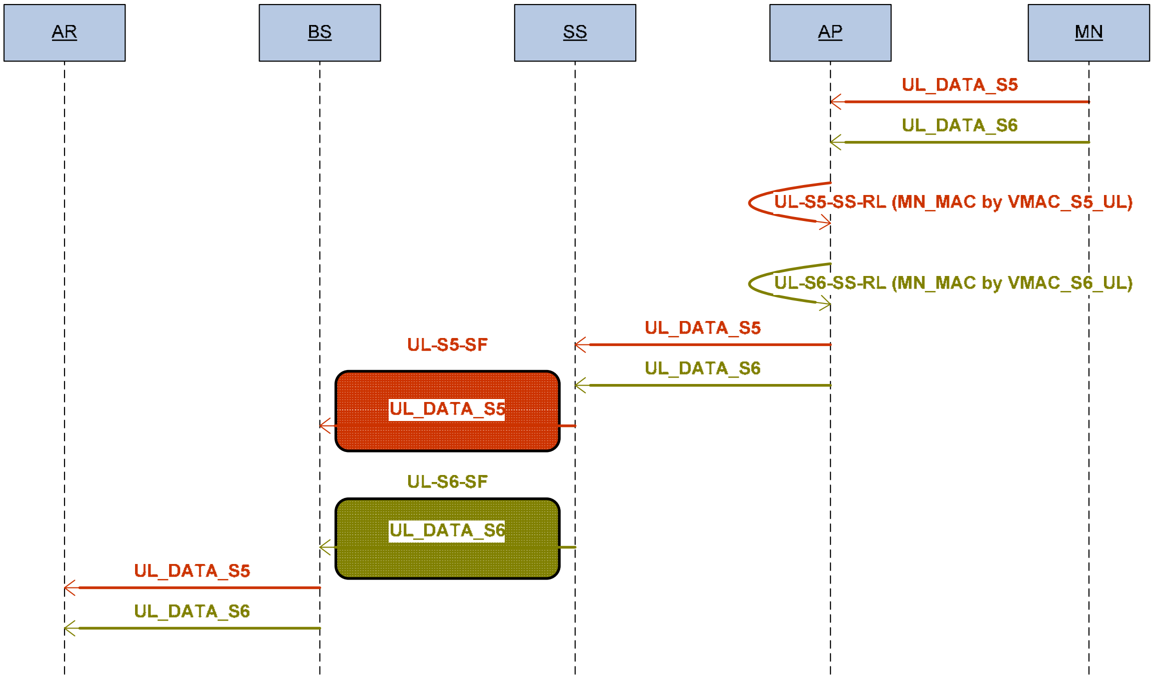

Figure 44: Uplink dynamic service differentiation (two-hop scenario)

4.3.6. Fast Handover Support

When a FHO process occurs, the FHO modules provide the new AR (nAR) information about the MN MAC address, the MN CoA (Care of Address) and the new AP (nAP) MAC address. This information is provided to the nAR before the FHO is done.

During the system setup, the **DEF-DL-SF** and **DEF-UL-SF** service flows have been defined to allow the communication between the AR and the MN, while the MN network access process is being performed. In this case, when the MN moves between the old AR (oAR) and the new AR (nAR), these service flows are used to allow the communication between the MN and nAR while the MN network access process is not completed.

When the MN performs the handover to the nAR, despite the auxiliary service flows (**AUX-DL-SF** and **AUX-UL-SF**) have already been established during the system setup phase, the associated translation rules (**AUX-DL-BS-RL**, **AUX-DL-SS-RL** and **AUX-UL-SS-RL**) are not installed yet. For these translation rules to be allocated, the MN network access process must be completed. During the translation rules installation, uplink and downlink data packets must be able to traverse the 802.16 link, avoiding traffic disruption during the FHO process. These packets are able to traverse the air link using the **DEF-DL-SF** service flow for downlink packets and the **DEF-UL-SF** service flow for uplink packets. This is the main purpose of these service flows – assist the FHO process by allowing the downlink and uplink packets to traverse the 802.16 air link while no translation rules are defined.

Therefore, the first action to take after the nAR receives information that a FHO will occur, is to install the **AUX-DL-BS-RL**, **AUX-DL-SS-RL** and the **AUX-UL-SS-RL** translations rules allowing packets to be sent to/from the MN.

The **AUX-DL-BS-RL** translation rule replaces the original destination MAC address (MN MAC address) of the downlink packets by the *VMAC_AUX_DL* address. This way, when packets reach the nAR to be delivered to the MN, the **AUX-DL-BS-RL** translation rule is applied and the packets are sent to the BS with the *VMAC_AUX_DL* as the destination MAC address. These packets are classified by the BS according to the destination MAC address they are carrying. In this case, the destination MAC address is the *VMAC_AUX_DL* address, therefore the packets are sent in the **AUX-DL-SF** service flow. Additionally, when packets reach the AP, another translation rule must be applied in order to deliver the packets to the MN. The packets reach the AP with the *VMAC_AUX_DL* as the destination MAC address and the **AUX-DL-SS-RL** translation rule must be applied to perform the reverse translation.

The same procedure must exist for the uplink packets during the FHO process. Besides downlink packets, the MN might start sending uplink packets towards the nAR while the MN network access process is not completed. In this case, packets are sent in the **DEF-UL-SF** service flow while the **AUX-UL-SS-RL** translation rule is not installed. Therefore, uplink packets that reach the SS during the MN network access process are sent in the **DEF-UL-SF** service flow using the **DEF-UL-SS-RL** translation rule.

After the **AUX-DL-BS-RL**, **AUX-DL-SS-RL** and **AUX-UL-SS-RL** translation rules are installed, the packets are redirected to the **AUX-DL-SF** and **AUX-UL-SF** service flows instead of being sent trough the **DEF-DL-SF** and **DEF-UL-SF** service flows.

At this stage of the process, the MN is already initialized in the system and is able to receive/send signalling and data packets through the usage of the MN auxiliary service flows (**AUX-DL-SF** and **AUX-UL-SF**). If new service reservations are requested by the

MN, the procedure is exactly the same as depicted in section 4.3.3.1 for uplink service reservations, and in section 4.3.3.2 for downlink service reservations.

4.3.7. IPv6 NDP Support

IPv6 support is mandatory in next generation environments. With our architecture, IPv6 data packets (unicast packets) support is trivial since we are using Ethernet as the CS. Besides the IPv6 data packets support, the IPv6 NDP must be supported as well.

The IPv6 NDP is composed of several processes, namely, the Router Discovery process, the Address Resolution process, the Duplicate Address Detection process, the Neighbour Unreachability Detection process and the Redirect process.

The Router Discovery process is used for the nodes to discover the routers in the link and acquire a prefix in order to configure an IPv6 address. Router Solicitation and Router Advertisement messages are used to support the Router Discovery process in our system. The support of these messages in our system is explained in section 4.3.7.1 and section 4.3.7.2, respectively.

The Address Resolution process is used to discover the link-layer address of the next-hop on-link for a specific destination address, when the neighbour cache does not have an entry for the later. Neighbour Solicitation messages and Neighbour Advertisement messages are used to support this process in our system. Detailed information about the support of these messages in our system is depicted in section 4.3.7.3 and in section 4.3.7.4, respectively.

Duplicate Address Detection process is used for the detection of a duplicated address in the link. Neighbour Unreachability Detection process is important to detect if a specific address is reachable. Finally, the Redirect process is used by the routers to inform the nodes that a new route for a specific network must be used.

4.3.7.1. ICMPv6 Router Solicitation

Router Solicitation messages are sent from the unicast nodes MAC address to the all-routers multicast MAC address (33:33:00:00:00:02). This way, we must allow the RS packets to reach the AR, traversing the 802.16 link. For this purpose, we use the **AUX-UL-SF** service flow that has been created during the MN network access phase.

4.3.7.2. ICMPv6 Router Advertisement

Router Advertisements messages are periodically sent, or as a response to the RS messages, from the routers to the all-nodes multicast MAC address (33:33:00:00:00:01). Therefore, these packets must be sent to all the SSs that are connected to the BS. Thus, as mentioned in section 4.3.1, we established the **RA-DL-SF** service flow during the system setup phase. This service flow uses the broadcast MAC address as the classification parameter, and therefore requires the installation of the **RA-DL-BS-RL** translation rule in the AR. This translation rule replaces the all-nodes multicast MAC address of the RA messages by the broadcast MAC address.

4.3.7.3. ICMPv6 Neighbour Solicitation

Neighbour Solicitation messages are sent by an IPv6 host to discover the next-hop on-link link-layer address. Thus, the 802.16 system must allow these messages to traverse the air link in both, uplink and downlink directions. In the uplink case, a Neighbour Solicitation message is sent by the MN to the solicited-node multicast destination MAC address to discover the link-layer address of the destination. The **AUX-UL-SF** service flow created during the MN network access process is used to forward these packets. In the downlink case, a Neighbour Solicitation message is sent by the AR to the solicited-node multicast MN MAC address to discover the link-layer address of the MN. The auxiliary service flow (**AUX-DL-SF)** is also used to transport these messages.

4.3.7.4. ICMPv6 Neighbour Advertisement

Neighbour Advertisement messages are sent by an IPv6 host as a response to a Neighbour Solicitation. The **AUX-DL-SF** service flow is used to transport the Neighbour

Advertisement messages in the downlink direction, whereas in the uplink direction, the **AUX-UL-SF** service flow is used.

4.4. 802.16 Control Protocol

The 802.16 Control Protocol (16CP) defines a set of messages that are used to manage the translation rules and the service flows in both the BS side entity and the SS side entity.

4.4.1. Mobile Node Access (MNA)

MNA messages are sent when a new node joins the network. ***MNA Request*** (***MNA-REQ***), depicted in Table 20, is sent by the AP/MN to the AR.

Syntax	Notes
MNA-REQ Message Format() {	
Type = 0	Message Type
MN MAC Address	MN MAC address
AP MAC Address	MN Point of attachment MAC address
}	

Table 20: MNA-REQ message

It carries the AP MAC address as well as the MN MAC address. The MN MAC address is provided for the MAT located in the AR to trigger the translation rules installation (see section 4.3.2).

The ***MNA Response*** (***MNA-RSP***) message, as illustrated in Table 21, is sent by the AR to the AP/MN as a response to the ***MNA-REQ*** message.

Syntax	Notes
MNA-RSP Message Format() {	
Type = 1	Message Type
MN MAC Address	MN MAC address
AP MAC Address	MN Point of attachment MAC address
Result	Mobile Node access result
}	

Table 21: MNA-RSP message

The **Result** field provides the AP/MN the translation rules installation result.

4.4.2. Service Flow Reservation (SF-RESV)

SF-RESV message triggers the service flow reservation process in the 802.16 equipment. Table 22 illustrates the ***SF-RESV-REQ*** message, which is sent by the AR to the AP/MN.

Syntax	Notes
SF-RESV-REQ Message Format() {	
Type = 2	Message Type
QoS Parameters	Maximum and Minimum Bandwidth, Priority, Scheduling Service, Maximum Latency
Classification Parameters	MAC and VMAC address, 802.16 Service Flow index
ID	Service Flow Identifier
CnxID	Service Identifier
}	

Table 22: SF-RESV-REQ message

The **QoS Parameters** field carries the service flow QoS characteristics: maximum and minimum bandwidth, priority, scheduling service and maximum latency. The **Classification Parameters** include the VMAC address that will be used to classify the packets, as well as the service flow index of the 802.16 equipment. The **ID** is used to identify this specific service flow, whereas the **CnxID** is the service identifier for which this service flow will be used.

The ***SF-RESV-RSP*** message, illustrated in Table 23, is sent by the AP/MN to the AR in response to the ***SF-RESV-REQ*** message.

Syntax	Notes
SF-RESV-RSP Message Format() {	
Type = 3	Message Type
ID	Service Flow Identifier
CnxID	Service Identifier
Result	Service Flow Reservation Result
}	

Table 23: SF-RESV-RSP message

The **Result** field informs the AR if the reservation was successful or not.

4.4.3. Service Flow Modification (SF-MOD)

The ***SF-MOD-REQ*** message, sent by the AR to the AP/MN, is used to modify a previously allocated service flow in the 802.16 equipment. Table 24 illustrates this message.

Syntax	Notes
SF-MOD-REQ Message Format() {	
Type = 4	Message Type
New QoS Parameters	Maximum and Minimum Bandwidth, Priority, Scheduling Service, Maximum Latency
ID	Service Flow Identifier
CnxID	Service Identifier
}	

Table 24: SF-MOD-REQ message

The **New QoS Parameters** field indicates the new set of QoS characteristics of the service flow.

The ***SF-MOD-RSP*** message is sent by the AP/MN to the AR as a response to the ***SF-MOD-REQ*** message.

4.4.4. Service Flow Deletion (SF-DEL)

The ***SF-DEL*** messages are used delete a previously allocated service flow in the 802.16 equipment. Table 25 illustrates the ***SF-DEL-REQ*** message.

Syntax	Notes
SF-DEL-REQ Message Format() {	
Type = 6	Message Type
ID	Service Flow Identifier
}	

Table 25: SF-DEL-REQ message

4.4.5. Translation Rule Installation (TR-INST)

The ***TR-INST*** messages trigger a translation rule installation. Table 26 depicts the ***TR-INST-REQ*** message, which is sent by the AR to the AP/MN.

Syntax	Notes
TR-INST-REQ Message Format() {	
Type = 8	Message Type
Translation Rule	MAC and VMAC address
ID	Translation Rule Identifier
CnxID	Service Identifier
}	

Table 26: TR-INST-REQ message

The **Translation Rule** indicates the MAC address that will be translated, as well as the VMAC address that will be used. The **ID** identifies this translation rule and the **CnxID** indicates the data packets that will be translated.

4.4.6. Translation Rule Block (TR-BLOCK)

Before a service flow is modified, the associated translation rule must be blocked allowing the packets to flow through the auxiliary service flow (see section 4.3.4). This is triggered by the ***TR-BLOCK-REQ*** message, illustrated in Table 27.

Syntax	Notes
TR-BLOCK-REQ Message Format() {	
Type = 10	Message Type
ID	Translation Rule Identifier
CnxID	Service Identifier
}	

Table 27: TR-BLOCK-REQ message

The **ID** parameter indicates the translation rule that must be blocked.

4.4.7. Translation Rule Unblock (TR-UNBLOCK)

The ***TR-UNBLOCK*** message is used to unblock a previously blocked rule. ***TR-UNBLOCK-REQ*** message is presented in Table 28.

Syntax	Notes
TR-UNBLOCK-REQ Message Format() {	
Type = 12	Message Type
ID	Translation Rule Identifier
CnxID	Service Identifier
}	

Table 28: TR-UNBLOCK-REQ message

The **ID** parameter identifies the rule that should be unblocked.

4.4.8. Translation Rule Deletion (TR-DEL)

To delete a translation rule in the AP/MN, a ***TR-DEL*** message is sent. Table 29 presents a ***TR-DEL-REQ*** message.

Syntax	Notes
TR-DEL-REQ Message Format() {	
Type = 14	Message Type
ID	Translation Rule Identifier
CnxID	Service Identifier
}	

Table 29: TR-DEL-REQ message

The translation that must be deleted is identified by the **ID** parameter.

4.5. Implemented QoS Modules and Interfaces

As stated before, the service flow reservation in the 802.16 link is done through the usage of the 802.16 Driver. As shown in Figure 25 and Figure 26, the 802.16 Driver has two instances:

- **802.16-BS Driver**: Instance of the 802.16 Driver running in the BS side entity (AR) in both single-hop and two-hop scenarios.
- **802.16-SS Driver**: Instance of the 802.16 Driver running in the SS side entity. For the single-hop scenario, the SS side entity is the MN, whereas for the two-hop scenario the SS side entity is the AP.

The 802.16-BS Driver is very important, since it concentrates the main intelligence of our system. This module is responsible for receiving the layer 3 requests and enforcing them in the 802.16 wireless link; it works as an 802.16 manager entity for the control of the BS and the 802.16 wireless resources. Focusing all the intelligence on the 802.16-BS Driver, allows us to control all the SSs connected to that specific BS and to easily support the two envisaged scenarios. Since we are in a point-to-multipoint shared wireless environment, this allows us to efficiently perform admission control and manage the overall resources.

However, the reservations in the 802.16 technology must be done locally in the SS. Thus, another instance of the 802.16 Driver must be installed in the SS side entity. In the single-hop scenario, the 802.16-SS Driver is located in the MN directly connected to the SS. For the two-hop scenario, the 802.16-SS Driver is implemented in the AP directly connected to the SS. This way, the 802.16-BS Driver must convey the QoS policies (resource reservation, modification or deletion) to the 802.16-SS Driver. This information is sent through the usage of the 16CP. Finally, the service flow reservation in the equipment can be established with the requested QoS parameters through the usage of the 802.16-SS Driver.

Figure 45 illustrates the two implemented drivers with their modules and interfaces. C programming language has been used to perform the implementation.

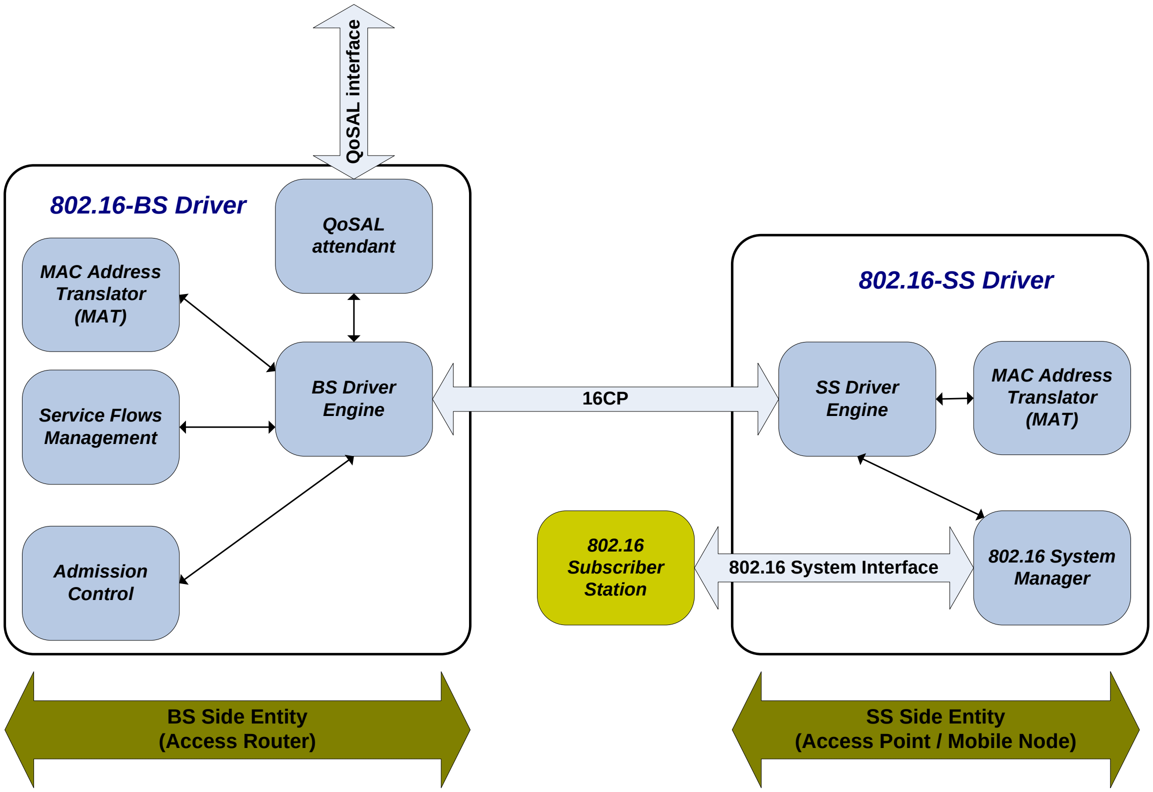

Figure 45: Implemented modules and interfaces

On the left side of Figure 45 we illustrate the 802.16-BS Driver, whereas on the right side we present the 802.16-SS Driver. The communication between the drivers is established through the 802.16 Control Protocol (16CP) (see section 4.4).

The **802.16-BS Driver** comprises the following modules:

- QoSAL Attendant
- Admission Control
- Service Flows Management
- MAC Address Translator (MAT)

The following modules are implemented in the **802.16-SS Driver**:

- MAC Address Translator (MAT)
- 802.16 System Manager

The **QoSAL attendant** interfaces with the QoSAL through a UNIX socket (Driver Interface). It is a very important interface since it provides the communication with the upper layers.

The **Admission Control** module is used to verify if the available resources in the 802.16 link are enough to satisfy the requirements of the new service flow. If enough resources are available, the service reservation is accepted. On the other hand, if resources are not available to satisfy the requested QoS parameters, the Admission Control module will have to analyze the Service Class and the Priority parameters from the new service flow and compare it with the already existent service flows in the 802.16 link. The action taken by the Admission Control module will depend on the result of this evaluation.

The **Service Flows Management** module is responsible for the service flow creation, modification and deletion in the 802.16 equipment, depending on the received QoSAL primitive. Since the interface with the 802.16 equipment is done in the SS, the service flow management policies must be sent to the AP through the usage of the 16CP.

The **802.16 System Manager** module is responsible to enforce the received requests in the 802.16 system. This is done through the usage of an HTTP interface using *Libcurl*. *Libcurl* is a client-side URL transfer library which supports, among others, the HTTP and the File Transfer Protocol (FTP) protocols.

A state machine has been implemented in the AR to control the service flow management process. The following states have been defined:

- **RESV_INIT**: Initial state of the service flow creation.
- **WAIT_RESV**: The 802.16 equipment is already performing a reservation and therefore the service flow is queued waiting for an opportunity to trigger the reservation process.
- **RESERVING**: Service flow is being reserved in the 802.16 equipment.
- **RESERVED**: Service flow reservation is completed.
- **WAIT_MOD**: The 802.16 equipment is already performing a reservation and therefore the service flow is queued waiting for an opportunity to trigger the modification process.
- **MODIFYING:** Service flow is being modified in the 802.16 equipment.

- **WAIT_DEL:** The 802.16 equipment is already performing a reservation and therefore the service flow is queued waiting for an opportunity to trigger the deletion process.
- **DELETING**: Service flow is being deleted in the 802.16 equipment.

Figure 46 illustrates the service flows state machine.

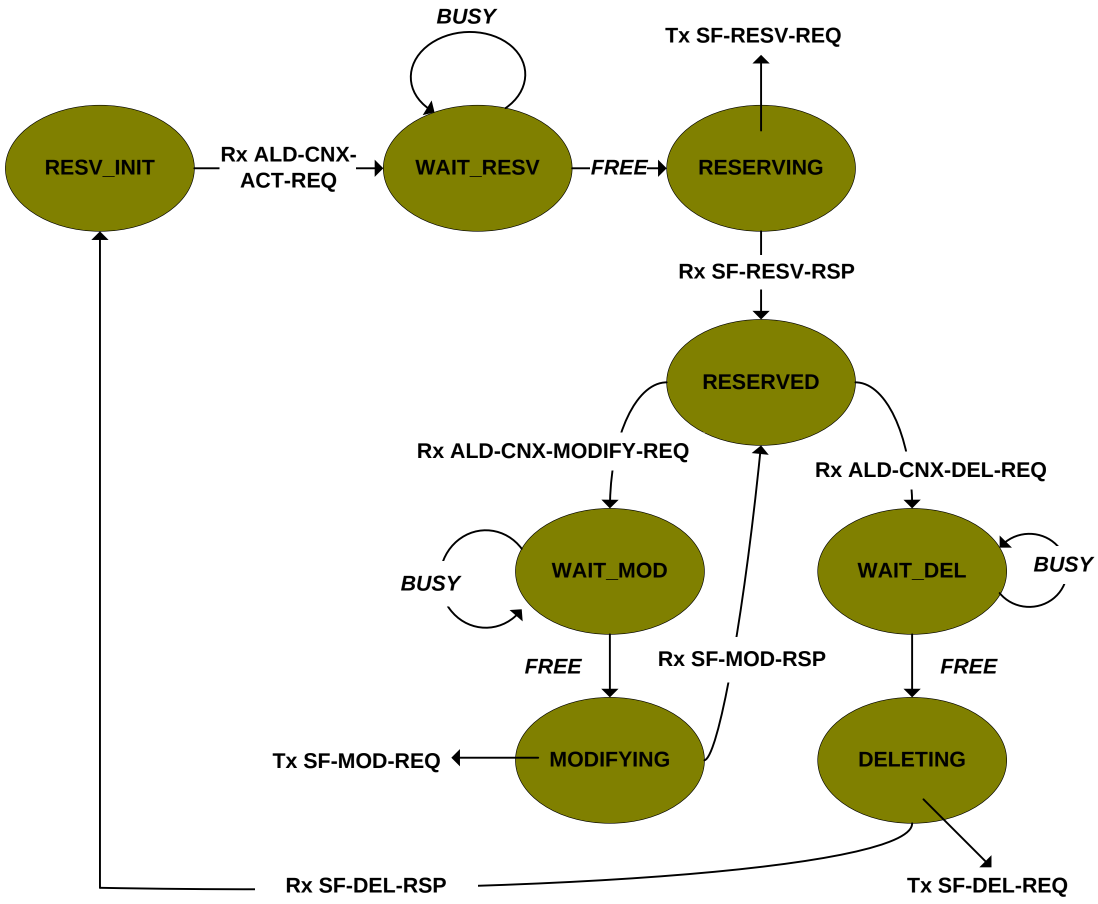

Figure 46: Service Flow State Machine

When an ***ALD-CNX-ACTIVATE-REQ*** is received from the QoSAL, the service flow state changes from **RESV_INIT** to **WAIT_RESV** (service flow waiting for reservation). If the 802.16 equipment is making a reservation, then the service flow will stay in this state. When the 802.16 equipment is free, it changes to the **RESERVING** (service flow reservation process in the AP/MN will take place) state. As a consequence the AR sends

a ***SF-RESV-REQ*** message to the AP/MN and the service flow is reserved in the 802.16 equipment. Following, a ***SF-RESV-RSP*** message is sent by the AP/MN to the AR and the service flow state is changed to **RESERVED** (service flow is reserved).
If an ***ALD-CNX-MODIFY-REQ*** message is sent from the QoSAL, the service flow state changes to **WAIT_MOD** (service flow waiting for modification) while the 802.16 equipment is busy. After the equipment is free, the state changes to **MODIFYING** (service flow modification process in the AP/MN will take place) and an ***SF-MOD-REQ*** message is sent to the AP/MN. When the service flow modification is over, an ***SF-MOD-RSP*** message is sent to the AR and the service flow state changes to **RESERVED** (service flow modification is completed).
If an ***ALD-CNX-DEL-REQ*** primitive is received from the QoSAL, the service flow state will change to **WAIT_DEL** (service flow waiting for deletion) until the equipment is free. Then, the service flow state changes to **DELETING** (service flow will be deleted) and an ***SF-DEL-REQ*** message is transmitted to the AP/MN. When the service flow is deleted, the AP/MN sends a ***SF-DEL-RSP*** message to the AR, and consequently, the service flow state changes to **RESV_INIT**.

The **MAT** module performs the translation rules management (install, delete, block and unblock), as well as the MAC addresses translation and the VMAC addresses management. Specifically, the MAT in the 802.16-BS Driver installs and translates the destination MAC addresses of the packets in the downlink direction to the specific VMAC address that will be used to classify the packets. In the downlink direction, the MAT in the 802.16-SS Driver replaces the VMAC address (that has been used by the MAT in the 802.16-BS Driver to classify the packets) by the original destination MAC address. In the uplink direction, the MAT in the 802.16-SS Driver is responsible to translate the source MAC addresses of the uplink packets to the VMAC addresses, which will be used by the SS to perform the classification. The MAT in the AR communicates with the MAT in the AP/MN through the 16CP messages.

A state machine for the translation rules has been implemented in both the AR and the AP/MN. The defined states were the following:

- **RULE_INIT**: Initial state of the translation rule creation.
- **INSTALLED**: The translation rule is installed.
- **BLOCKED**. The translation rule is blocked for service flow modification.

The translation rules state machines for the AP/MN and for the AR are shown in Figure 47 and Figure 48, respectively.

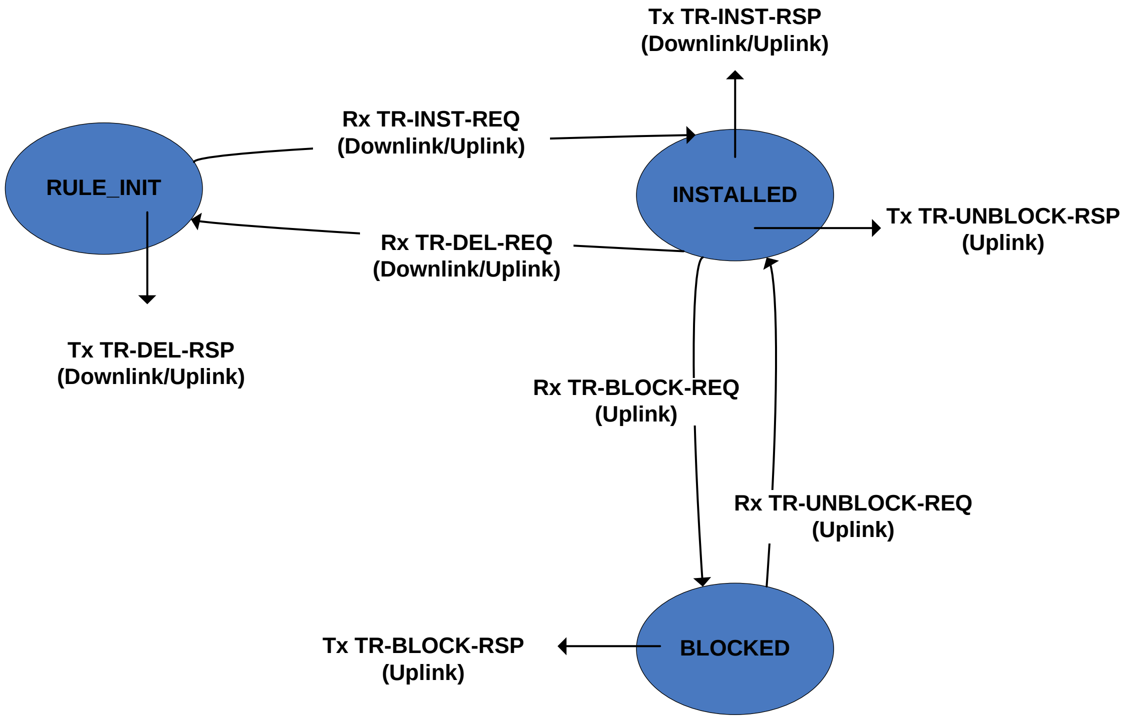

Figure 47: AP/MN Translation Rules State Machine

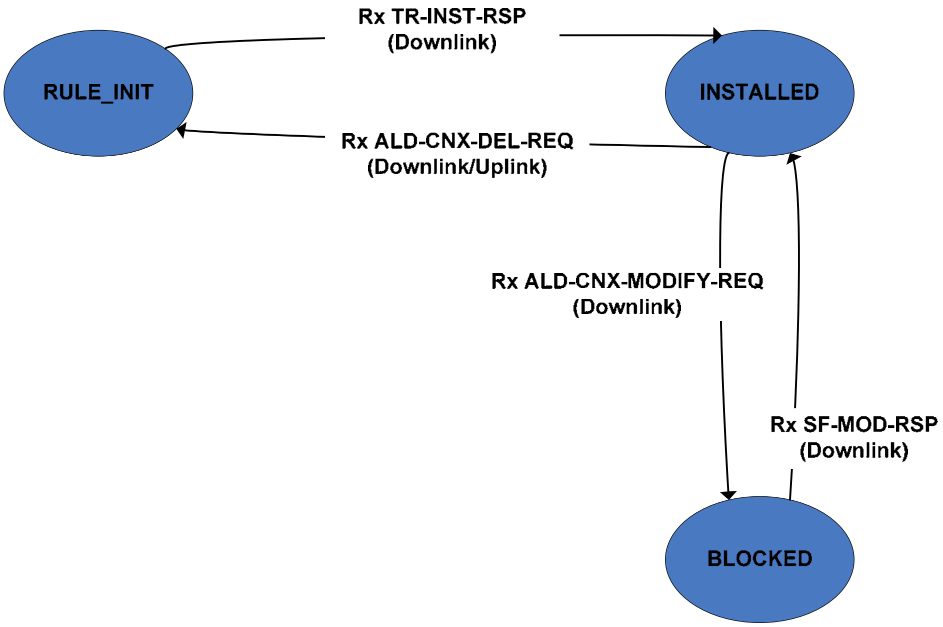

Figure 48: AR Translation Rules State Machine

Immediately after a downlink service flow is established in the 802.16 link, a translation rule has to be installed in the AP/MN to start translating the packets (refer to section 4.3.3.2). Therefore, a ***TR-INST-REQ*** message is transmitted by the AR to the AP/MN to start the translation rule installation in the AP/MN (Figure 47). When the translation rule is installed in the AP/MN, the state changes from **RULE_INIT** to **INSTALLED** (translation rule is installed). Following, the AP/MN sends a ***TR-INST-RSP*** message to the AR (Figure 48) and the translation rule in the AR is installed. As a result, the translation rule state machine in the AR changes from **RULE_INIT** to **INSTALLED** (Figure 48).

If there is an uplink service flow reservation (refer to section 4.3.3.1), there is no translation rule installation in the AR (Figure 48).

If a downlink service flow modification request is received by the AR (***ALD-CNX-MODIFY-REQ*** primitive in Figure 48), the translation rule state changes to **BLOCKED** (service flow will be modified). When the service flow modification is completed, the state changes to **INSTALLED**.

If an uplink service flow modification is received by the AR, a ***TR-BLOCK-REQ*** message is sent to the AP/MN and the translation rule state is changed to **BLOCKED** (service flow will be modified) (refer to Figure 47). The AP/MN replies with a ***TR-***

BLOCKED-RSP message to the AR. When the service flow modification is over, the AP/MN receives a ***TR-UNBLOCK-REQ*** message and changes the state to **INSTALLED** (Figure 47).

4.6. Summary

Novel solutions to overcome the open issues raised in section 3.3 have been depicted. One of the adopted solutions is the usage of a MAT (MAC Address Translator) in the AR and in the AP/MN as well. The MAT is responsible to translate the original MAC address of the packets to a specific VMAC (Virtual MAC) address. Besides the MAT, an auxiliary service flow (AUX-SF) is also defined to allow data to be forwarded in the 802.16 system while reservations and modifications are being done in the original service flows.

A complete description of the AN architecture is presented, including the interfaces between the technology specific modules (equipment drivers) and the technology independent modules (QoSAL module). A detailed description of the different operation phases of the developed driver is also given, as well as the description of its implementation.

Chapter 5: Performance Measurements

To test the performance of the specified and implemented solutions, a set of tests, divided in two major groups has been performed: the single-hop scenario tests and the two-hop scenario tests. For each one of these groups, a set of parameters has been varied to check for the consistency of the implemented solutions. We have tested both, the point-to-point and the point-to-multipoint topologies for each scenario. Additionally, the number of flows and the number of terminals has also been varied, as well as the bandwidth associated in order to check if the requested QoS is guaranteed. Likewise, fast-mobility tests have also been performed to verify the support of this capability in the developed architecture.

This chapter is divided in two main sections. Section 5.1 provides a full description of the performance tests that have been done for the single-hop scenario, shown in Figure 22. The tests developed for the two-hop scenario, shown in Figure 23, are described in section 5.2. Section 5.3 briefly summarizes the performance measurements chapter.

5.1. Single-Hop Scenario QoS Tests

Figure 49 illustrates the implemented demonstrator for the QoS tests in the single-hop scenario. In the Radio Access Network (RAN), two SSs are connected to the BS creating an 802.16 PMP scenario. Terminal 1 (T1) is directly connected to SS1, whereas terminal 2 (T2) is connected to SS2. The 802.16 BS is directly connected to AR1, establishing the link between the RAN and the AN. AR2 is connected to a Correspondent Node (CN) that will be responsible to receive and send data packets in the uplink and downlink directions, respectively.

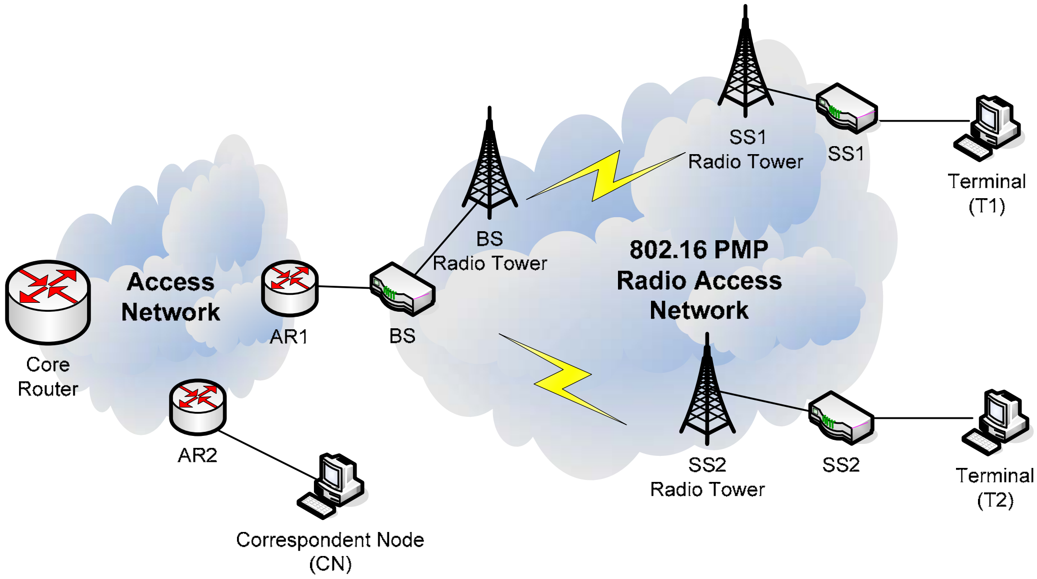

Figure 49: Implemented demonstrator for single-hop scenario QoS tests

QoSM and QoSAL modules are running in all ARs. The QoS Broker is running in another machine, which is accessible by the ARs. QoSAL is also running in the terminals. To load the network with flows of packets, we used the Multi-Generator (MGEN) traffic measurement tool, generating User Datagram Protocol (UDP) packets. The MGEN tool is running in the CN and in the terminals T1 and T2.

5.1.1. Downlink Point-to-Point Scenario

The first set of tests considers the transport of information in the downlink direction in a point-to-point topology. The 802.16 point-to-point (PTP) link will be created between the BS and SS1 (see Figure 49).

5.1.1.1. SH – D – PTP – Test 1

In this test, Single Hop (SH) Downlink (D) and Point-to-Point (PTP), a single terminal (T1) is connected to SS1. One flow (F1) is created and sent from the CN to terminal T1 using the MGEN tool. The bandwidth of the generated flow ranges from 64 kbps to 2 Mbps. Figure 50 illustrates the test procedures just described.

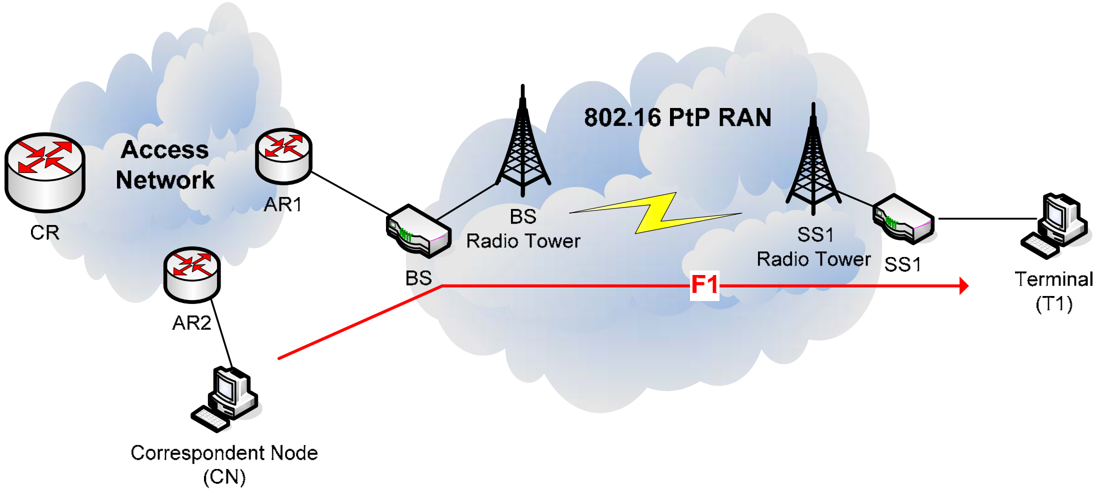

Figure 50: SH – D – PTP – Test 1 implemented demonstrator

5.1.1.1.1. Service Flow Reservation

This test comprises the measurement of the time required to perform a QoS reservation in the 802.16 system using a single flow (F1) in the downlink direction. For detailed information about the QoS reservation process, please refer to section 4.3.3.

The QoS reservation performance measured values, for each one of the tested bandwidths, are illustrated in Table 10. The first column identifies the flow, its source and destination – in this case, F1 is sent from the CN (connected to AR2) to terminal T1 (see Figure 50). Since several bandwidth values are used to perform the tests, each row of the table indicates the results for a specific bandwidth value. The bandwidth value is identified in the second column of the table.

The third column (Δ**T1**) is the time, in microseconds (**µsec**), that the 802.16 driver takes to perform admission control and accept or deny the reservation request. Basically, the 802.16-BS driver, located in the AR, receives an ***AL-CNX-ACTIVATE-REQ*** message from the QoSAL, performs admission control and replies with an ***AL-CNX-ACTIVATE-RESP*** message. Δ**T2** is the time, in seconds (**sec**), taken by the 802.16 driver to perform a service flow reservation. This includes the time spent by the 802.16-BS driver, after receiving the QoSAL reservation request, to send a ***SF-RESV-REQ*** message to the 802.16-SS driver. It also includes the amount of time taken by the 802.16-SS driver to send, after the service flow reservation in the 802.16 equipment is completed, the ***SF-RESV-RSP*** message to the 802.16-BS driver, indicating that the reservation process is over. After the service flow reservation is completed, packets must stop being sent in the backup service flow and start being sent in the dedicated service flow. Consequently, the adequate translation rules must be installed in both the AR and in the terminal T1, as explained in section 4.3.3.2. Δ**T3** is the time, in milliseconds (**msec**), taken by the system to install the translation rule in the terminal T1. To achieve this, the AR sends a ***TR-INST-REQ*** message to terminal T1; terminal T1 installs the translation rule and replies back to the AR with a ***TR-INST-RSP*** message. After the translation rule in terminal T1 is installed, the correspondent translation rule in the AR must be installed. The time taken, in microseconds (**µsec**), to install the translation rule in the AR is given by Δ**T4**.

Flow	BW (bps)	ΔT1 (μsec)	ΔT2 (sec)	ΔT3 (msec)	ΔT4 (μsec)
F1: CN → T1	64 K	96	11	39	31
F1: CN → T1	128 K	92	13	39	28
F1: CN → T1	256 K	92	11	39	27
F1: CN → T1	512 K	90	10	39	32
F1: CN → T1	1 M	87	11	39	29

Table 30: F1 reservation performance measurements (DL PtP single-hop scenario)

As we can see in Table 30, Δ**T1** is always below 100 microseconds. This value is very low and does not compromise the real-time services usage in this environment. It is crucial that Δ**T1** is very low since the packets are queued in the AR during this amount of time. On the other hand, Δ**T2**, which is the amount of time spent by the 802.16 driver to establish the service flow reservation, is very high (approximately 11 seconds). This was expected since the 802.16 equipment is not prepared to work with dynamic services. Despite Δ**T2** is very high, packets are not lost since they are sent in the backup service flow during this period of time. Δ**T3** and Δ**T4** are the periods of time to install the translation rules in terminal T1 and in the AR, respectively. As expected, these periods are also low and do not influence on the QoS process. Despite these values are low, Δ**T3** is higher than Δ**T4**, since Δ**T3** is the time taken to install a translation rule in the AP (remote), whereas Δ**T4** is the time taken to install a translation rule installed in the AR (local). Additionally, as we can see in Table 30, the obtained values are independent of the bandwidth that is being requested. Summarizing, during the whole reservation process, packets flow in the network, bandwidth is stable and no packets are lost.

5.1.1.1.2. Service Flow Modification

This test comprises the measurement of the time required to perform a QoS modification in the 802.16 system. We will keep using the same test setup to verify the consequences when we modify the QoS parameters of the previously reserved service flow. In this case, F1, that is being sent from the CN to terminal T1 with a specific data rate, will be modified at t = 100 seconds. At this moment, it starts sending packets at a higher data rate, simulating a user that wants to upgrade its QoS parameters in terms of bandwidth. The QoS modification process is depicted in section 4.3.4.1.

Table 31 shows the obtained results for this test. The second column specifies the bandwidth upgrade that has been done. For instance, the cell in the second column and second row means that, at t = 100 seconds, F1 bandwidth is modified from 64 kbps to 128 kbps. Comparing to the reservation process shown in section 5.1.1.1.1, the only difference is that the QoSAL, instead of sending the ***AL-CNX-ACTIVATE-REQ*** message and receiving the ***AL-CNX-ACTIVATE-RESP*** message, sends the ***AL-CNX-MODIFY-REQ*** message and receives the ***AL-CNX-MODIFY-RESP*** message. Additionally, the AR translation rule must be blocked during this period to redirect the F1 packets from the dedicated service flow to the backup service flow. This process is completely dynamic and the user does not notice any service degradation while the modification of the flow is occurring. **ΔT5** is the time, in microseconds (**µsec**), that this process takes until it is completed. **ΔT6** is the time, in seconds (**sec**), taken by the 802.16 driver to perform the service flow modification. It includes the time spent by the 802.16-BS driver to send a ***SF-MOD-REQ*** message to the 802.16-SS driver. Moreover, it includes the amount of time taken by the 802.16-SS driver to send, after the service flow modification in the 802.16 equipment is completed, the ***SF-MOD-RSP*** message to the 802.16-BS driver. When the service flow modification process is completed, the packets that were being sent in the backup service flow are redirected to the dedicated service flow. To achieve this, the translation rule in the AR must be unblocked. **ΔT7** indicates this period of time.

Flow	**ΔBW (bps)**	**ΔT5 (µsec)**	**ΔT6 (sec)**	**ΔT7 (µsec)**
F1: CN → T1	64 K → 128 K	185	22	21
F1: CN → T1	128 K → 256 K	179	20	20
F1: CN → T1	256 k → 512 K	190	22	19
F1: CN → T1	512 K → 1M	199	22	20
F1: CN → T1	1 M → 2M	192	21	20

Table 31: F1 modification performance measurements (DL PtP single-hop scenario)

As in the reservation process, the Δ**T5** period is very low. Despite this, it is higher then Δ**T1**. This is due to the fact that, when the 802.16-BS driver receives the ***AL-CNX-MODIFY-REQ*** message from the QoSAL, it must block the translation rule installed in the AR that was responsible for redirecting the packets to the dedicated service flow. Only after the translation rule is blocked, the ***AL-CNX-MODIFY-RESP*** message is sent to the QoSAL. This way, after the translation rule is blocked, the packets start flowing in the backup service flow and the dedicated service flow can be changed without leading to traffic disruption. Also similar to the reservation request case shown in Table 30, we can see that the service flow modification process in the 802.16 equipment (Δ**T6**) is very high – approximately 22 seconds. In this case, the modification is even higher than the reservation time. This is due to the fact that the 802.16 technology, to modify a previously allocated service flow, deletes it and creates a new one. The sum of the deletion time plus the reservation time equals the modification time.

A service flow reservation and modification example is shown in Figure 51. In this case the bandwidth is modified from 512 kbps to 1 Mbps at t = 100 seconds.

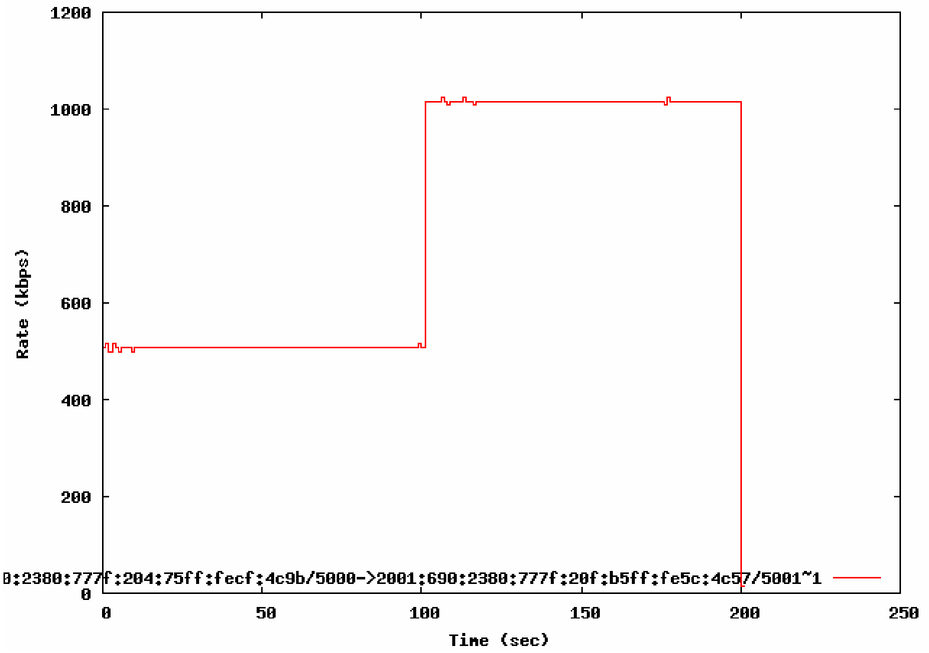

Figure 51: F1 Reservation and modification process for 512 kbps → 1 Mbps (Rate vs Time)

Figure 51 shows that when the service flow is modified, at t = 100 seconds, the bandwidth is stable. Figure 52 proves that no packets are lost during this process.

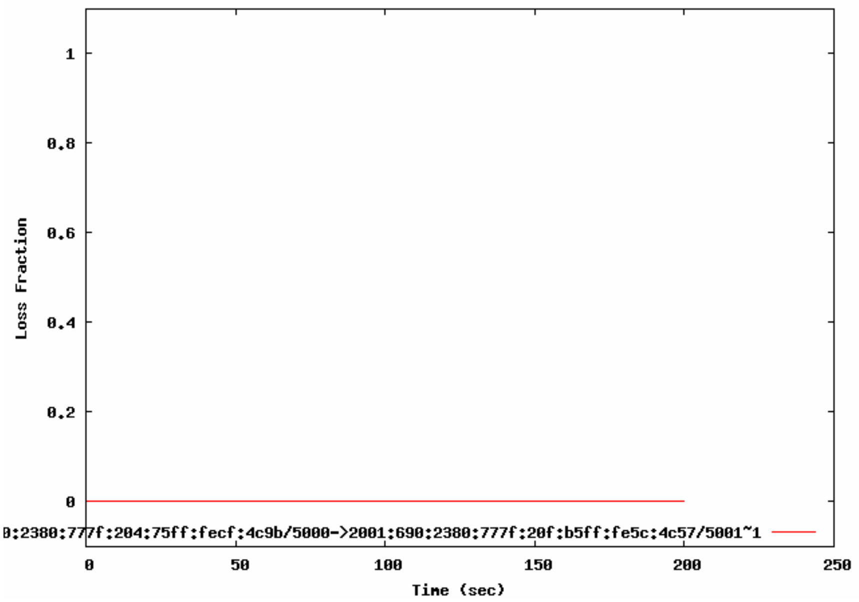

Figure 52: F1 Loss fraction for 512 kbps → 1 Mbps (Loss fraction vs Time)

Finally, in Figure 53, it is possible to analyse the latency during the whole process – reservation and modification.

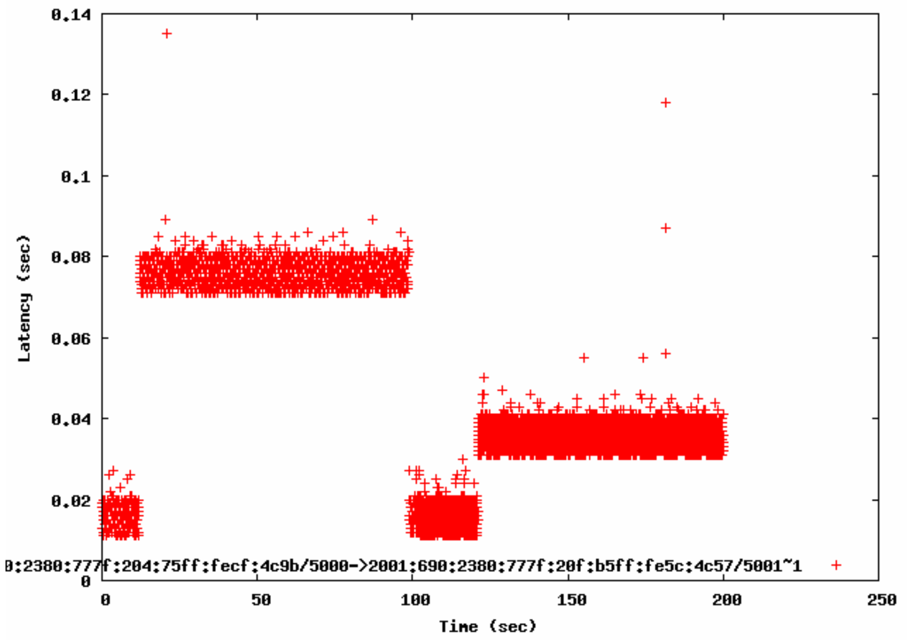

Figure 53: F1 latency for 512 kbps → 1 Mbps (Latency vs Time)

The latency illustration is very useful since it gives a clear view about the service flows that are used by F1 during the whole process (reservation and modification). As we can see, the latency varies during the process. Four different phases are identified in Figure 53:

- Phase 1: After the reservation request is received from the QoSAL, the backup service flow (2 Mbps bandwidth reservation) is used by F1 during the interval [0s, 11 s] (Δ**T2**). During this period, the dedicated service flow is being reserved in the 802.16 equipment. Latency is approximately 20 milliseconds.
- Phase 2: The dedicated service flow reservation is completed (512 kbps reservation) and thus it is used to forward F1 packets during the interval [11 s, 100 s]. Since the dedicated service flow bandwidth is less then the reserved bandwidth in the backup service flow (2 Mbps), the latency increases to 80 milliseconds. Resuming, the dedicated service flow bandwidth is four times lower (512 kbps) then the backup service flow bandwidth (2 Mbps).

- Phase 3: F1 data-rate is upgraded from 512 kbps to 1 Mbps; the backup service flow is used during the interval [100 s, 121 s] (Δ**T6**). During this period, the dedicated service flow is being modified. In this case, the backup service flow bandwidth is the same as in phase 1 (backup service flow is used in both phases) and therefore the latency is the same – 20 milliseconds.
- Phase 4: The service flow modification is completed. Therefore, the new dedicated service flow (1 Mbps reserved bandwidth) is used for F1 packets during the interval [121 s, 200 s]. Summarizing, the dedicated service flow bandwidth is half (1 Mbps) the backup service flow bandwidth (2 Mbps). Therefore the latency is twice (40 milliseconds) the phase 3 latency (20 milliseconds).

5.1.1.2. SH – D – PTP – Test 2

This test is similar to the test depicted in section 5.1.1.1 but in this case four flows (F1, F2, F3 and F4) are used instead of only one. The CN is responsible to send these flows to terminal T1. This test is illustrated in Figure 54.

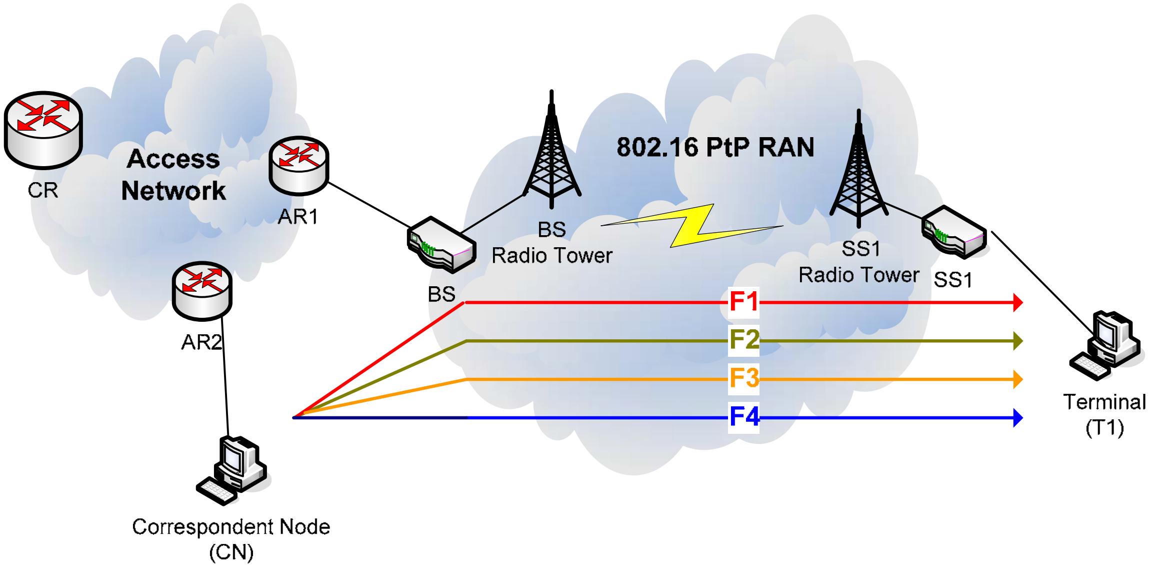

Figure 54: SH – D – PTP – Test 2 implemented demonstrator

5.1.1.2.1. Service Flow Reservation

In this case, four reservations are requested by the QoSAL to the 802.16-BS driver – one for each flow. The obtained results for the multiple flows reservation are illustrated in Table 32.

Flow	BW (bps)	ΔT1 (µsec)	ΔT2 (sec)	ΔT3 (msec)	ΔT4 (µsec)
F1: CN → T1	64 K	93	11	39	28
F2: CN → T1	64 K	94	21	39	31
F3: CN → T1	64 K	84	31	39	28
F4: CN → T1	64 K	89	42	39	29
F1: CN → T1	128 K	85	10	39	29
F2: CN → T1	128 K	85	21	39	30
F3: CN → T1	128 K	96	31	38	29
F4: CN → T1	128 K	87	41	40	29
F1: CN → T1	256 K	93	11	38	29
F2: CN → T1	256 K	92	22	40	32
F3: CN → T1	256 K	94	32	39	28
F4: CN → T1	256 K	88	42	39	28
F1: CN → T1	512 K	92	10	39	31
F2: CN → T1	512 K	91	21	39	30
F3: CN → T1	512 K	91	33	39	30
F4: CN → T1	512 K	90	43	39	31

Table 32: F1, F2, F3 and F4 reservation performance measurements (DL PtP single-hop scenario)

As shown in Table 32, since we have more then one service flow reservation, the **ΔT2** increases directly with the number of service flow reservation requests. This behaviour was expectable since the 802.16 equipment does not support concurrent service flow reservations. Therefore, despite the flow reservation requests are sent simultaneously from the QoSAL, the 802.16-BS driver will queue and serialize these requests.

Consequently, the period of time that the packets will traverse the backup service flow (**ΔT2**) will significantly increase – it is composed by the amount of time that the reservation is queued in the 802.16-BS driver plus the reservation process procedures. The F1, F2, F3 and F4 behaviour during the reservation process is illustrated in Figure 55.

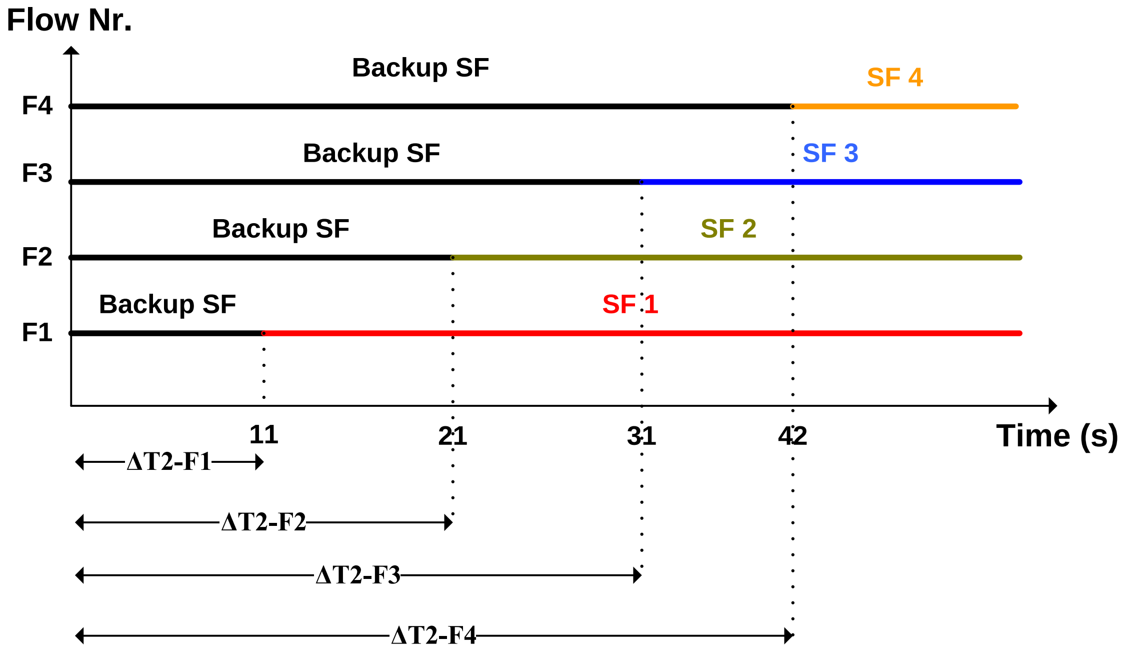

Figure 55: F1, F2, F3 and F4 behaviour during the reservation process (Flow vs Time)

Initially, the F1 reservation is requested by the QoSAL to the 802.16-BS driver; the 802.16-BS driver performs admission control and replies to the QoSAL indicating that F1 packets are allowed to traverse the 802.16 link using the backup service flow. This period of time is indicated by **ΔT1** in Table 32; to simplify, since it is related with F1, we will name it **ΔT1-F1**. Immediately after the QoSAL receives the F1 reservation confirmation, it requests the reservation for F2. This process is repeated for the four flows. As a result, four reservation requests are queued in the 802.16-BS driver until F1 reservation is over (**ΔT2-F1**). At **ΔT2-F1**, as we can see in Figure 55, F1 packets are redirected from the backup service flow to the dedicated service flow (SF1) and F2 reservation process is allowed to start. During the F2 reservation process, F2, F3 and F4 will use the backup service flow, whereas F1 is already using SF1 (Figure 55). At **ΔT2-F2**, the F2 reservation process is completed and its packets are redirected to the correspondent dedicated service flow (SF2). This process is repeated until the four service flows reservations are completed – one for each flow (SF1, SF2, SF3 and SF4).

5.1.1.2.2. Service Flow Modification

In this test, the four previously reserved service flows bandwidth are upgraded to a higher bandwidth at t = 100 seconds. The obtained results are shown in Table 33.

Flow	ΔBW (bps)	ΔT5 (µsec)	ΔT6 (sec)	ΔT7 (µsec)
F1: CN → T1	64 K → 128 K	198	21	20
F2: CN → T1	64 K → 128 K	190	43	19
F3: CN → T1	64 K → 128 K	193	64	21
F4: CN → T1	64 K → 128 K	199	86	20
F1: CN → T1	128 K → 256 K	179	22	20
F2: CN → T1	128 K → 256 K	187	45	20
F3: CN → T1	128 K → 256 K	184	66	19
F4: CN → T1	128 K → 256 K	190	88	21
F1: CN → T1	256 k → 512 K	189	22	18
F2: CN → T1	256 k → 512 K	185	44	22
F3: CN → T1	256 k → 512 K	190	65	19
F4: CN → T1	256 k → 512 K	192	86	20
F1: CN → T1	512 K → 1M	192	22	18
F2: CN → T1	512 K → 1M	199	43	21
F3: CN → T1	512 K → 1M	184	67	21
F4: CN → T1	512 K → 1M	187	89	20

Table 33: F1, F2, F3 and F4 modification performance measurements (DL PtP single-hop scenario)

As demonstrated by **ΔT6** in Table 33, the behaviour of the system is similar to the one observed in the four flows reservation process (depicted in section 5.1.1.2.1). The only difference resides on the fact that, in this case, the time that the packets use the backup service flow is longer. This is due to the fact that the service flow modification period in the 802.16 equipment is longer (actually twice) then the service flow reservation period.

In Figure 56 we can see the modification process. From [0 s, 100 s] the flows are sent with 512 kbps. At t = 100 seconds, as a consequence of the flow modification request received from the QoSAL, the bit-rate is duplicated to 1 Mbps without service interruption.

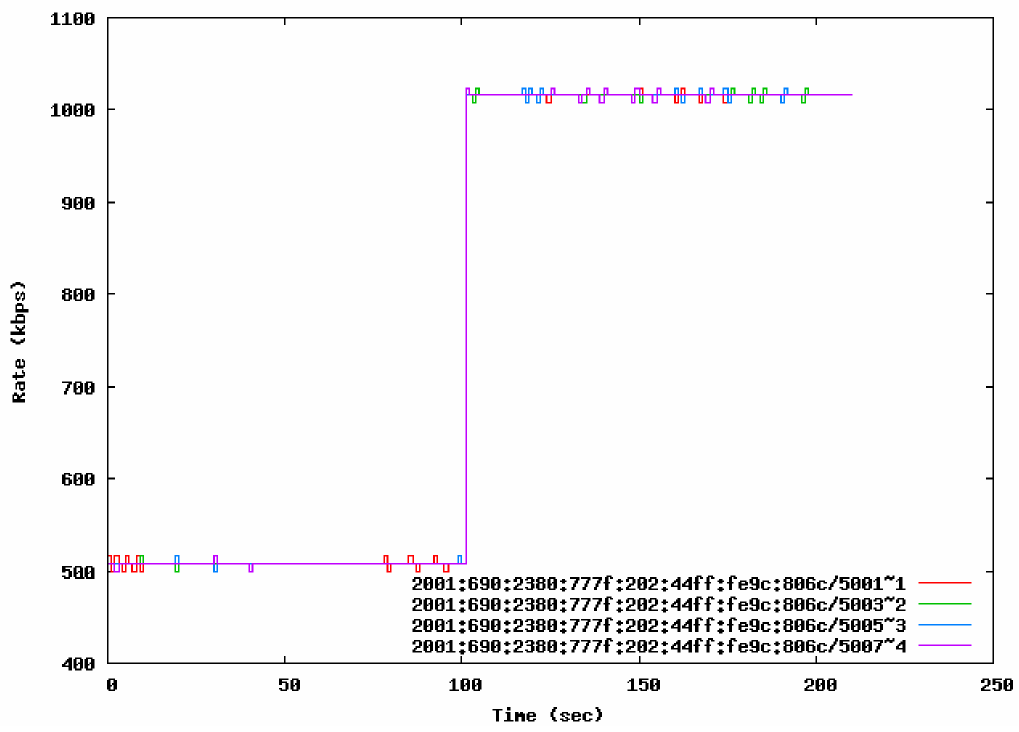

Figure 56: F1, F2, F3 and F4 reservation and modification process (Rate vs Time)

5.1.1.3. SH – D – PTP – Test 3

In this test we saturated the 802.16 link and triggered a QoS reservation in these conditions. The CN (connected to AR2) creates and sends an attacking flow (F1) to terminal T1, flooding the 802.16 link. A second flow (F2), also sent by the CN to terminal T1, will be responsible to study the behaviour of the 802.16 system under saturation. Figure 57 illustrates this test.

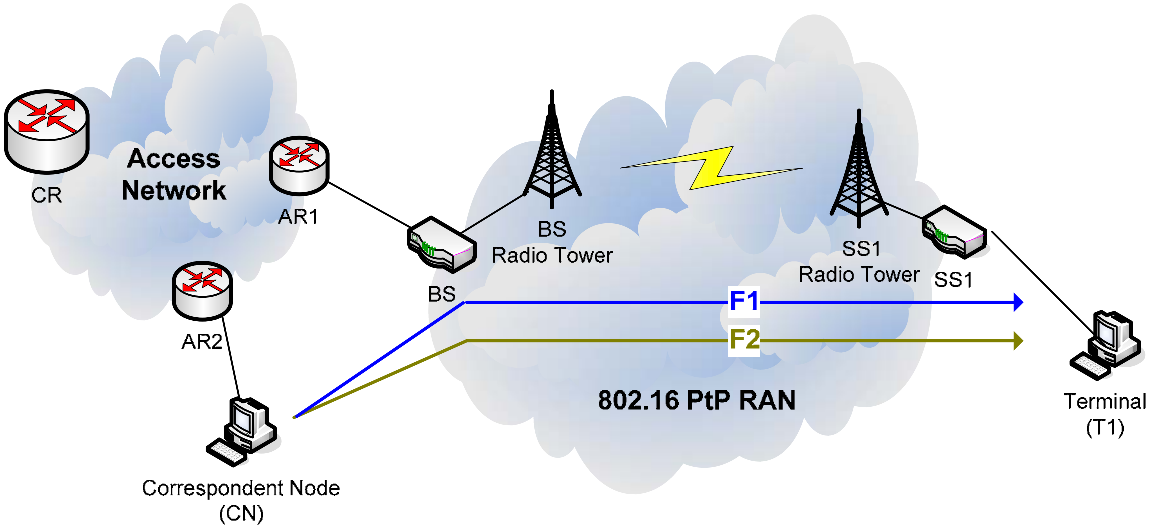

Figure 57: SH – D – PTP – Test 3 implemented demonstrator

5.1.1.3.1. Service Flow Reservation

Different combinations have been used for F1 and F2. These combinations are illustrated in Table 34. The second column of Table 34 represents the bandwidth of F1, before the reservation of F2, and represents the bandwidth that F2 is trying to request. The third column is the service class of each flow, the fourth column is the priority and the fifth column represents the final bandwidth allocated to F1 and F2 depending on the values in the third and fourth column. The last column is the status of each one of the flows after the reservation is completed. Note that, two different service classes may be used: UGS and BE. Inside each service class, we can differentiate among the different flows through the usage of the priority field. The priority field values vary from a minimum of 1 to a maximum of 7.

Flow		Requested BW (Mbps)	Service Class	Priority	Accepted BW (Mbps)	Status
E1	**F1: CN → T1**	15,5	BE	3	9,0	Downgraded
	F2: CN → T1	1,0	BE	7	1,0	Accepted
E2	**F1: CN → T1**	15,5	BE	3	15,0	Downgraded
	F2: CN → T1	1,0	UGS	1	1,0	Accepted
E3	**F1: CN → T1**	15,5	UGS	3	15,5	Unchanged
	F2: CN → T1	1,0	BE	6	0,5	Partially Accepted
E4	**F1: CN → T1**	15,5	BE	4	15,5	Unchanged
	F2: CN → T1	1,0	BE	4	0,5	Partially Accepted
E5	**F1: CN → T1**	16,0	UGS	3	16,0	Unchanged
	F2: CN → T1	1,0	BE	7	0,0	Rejected
E6	**F1: CN → T1**	16,0	BE	3	15,0	Downgraded
	F2: CN → T1	1,0	UGS	7	1,0	Accepted

Table 34: 802.16 admission control module behaviour when saturated

Since we are using a DL/UL ratio of 75%/25%, 16 Mbps is the maximum throughput we can achieve in the downlink direction, and thus, we created F1 (attacking flow) with a data rate of 15.5 Mbps. In the first experiment (E1), F1 belongs to service class BE (Best Effort) and has a low priority – 3 (priority values vary from the minimum of 0 to the maximum of 7). This way, only 500 kbps were left available for reservations in the 802.16 link. We made a reservation request of 1 Mbps with a priority of 7 for F2 (see test **E1** in Table 34). The Service Class of both flows is the same, and therefore the priority parameter is used to differentiate the reservations. In this case, F2 has a priority higher then F1. This way, the reservation for F2 is accepted, downgrading F1. As a result, after the reservation is completed we will have F1 with 15 Mbps (it was downgraded by 500 kbps) and F2 with 1 Mbps. To downgrade F1, a service flow modification process is triggered, as depicted in section 5.1.1.1.2.

The second test (**E2**) is similar to test T1 expect that the differentiation is made by the service class and not by the priority parameter. Since the service classes are different, the priority parameter is not even verified. UGS is the F2 service class and therefore it gets the desired bandwidth. Once again, F1 is downgraded to 15 Mbps.

In the third test (**E3**) F1 belongs to service class UGS with priority 3. The new reservation (F2) belongs to service class BE with priority 6. In this case, since F1 belongs to a higher service class then F2, F1 will not be affected. F2 will be provided with the available bandwidth – 500 kbps. As a result, F2 is partially accepted since it gets only half of the desired bandwidth.

The fourth test (**E4**) is performed to study the behaviour of the admission control module when both flows have the same QoS parameters (service class and priority). In this case, the reserved flows are not changed and the incoming requests should only be provided with the available bandwidth. Therefore, F2 is partially accepted with the available bandwidth.

In the fifth test (**E5**), all the downlink available bandwidth is reserved by F1 using the UGS service class. F2 makes a reservation request of 1 Mbps and, as a result, it is rejected. This result is expected since no bandwidth is available. On the other hand, as shown in the sixth test (**E6**), F1 reservation belongs to BE and F2 to UGS. In this case, F1 is downgraded and F2 is accepted.

The obtained results are according to the expected behaviour of the 802.16 driver, and show that our QoS architecture is able to operate according to the specificities of the technology.

5.1.2. Downlink Point-to-Multipoint Scenario

The Point-to-point tests have been performed in section 5.1.1. In this section, a point-to-multipoint test in the downlink direction will be performed. The 802.16 point-to-multipoint link is created between the BS, the SS1 and SS2 (see Figure 58), and the flows have different destinations, respectively in SS1 and SS2.

5.1.2.1. SH – D – PMP – Test 1

Four flows (F1, F2, F3 and F4) are used in this test. F1 and F2 are sent from the CN to terminal T1 (connected to SS1), whereas F3 and F4 are sent from the CN to terminal T2 (connected to SS2). Figure 58 illustrates this test.

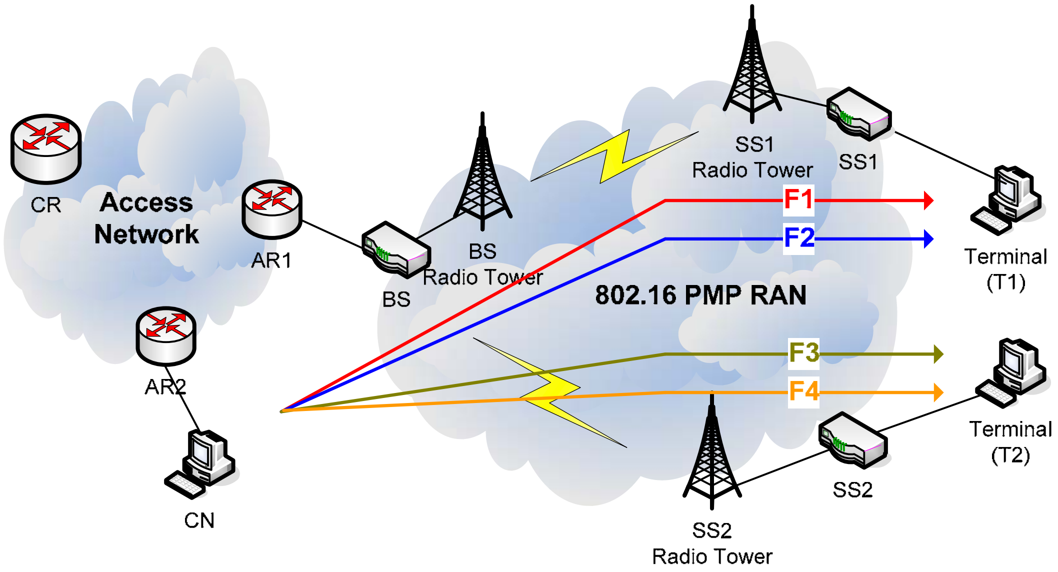

Figure 58: SH – D – PMP – Test 1 implemented demonstrator

5.1.2.1.1. Service Flow Reservation

The results obtained for the reservation process of the four flows (F1, F2, F3 and F4) are shown in Table 35.

Flow	BW (bps)	ΔT1 (µsec)	ΔT2 (sec)	ΔT3 (msec)	ΔT4 (µsec)
F1: CN → T1	64 K	95	11	39	28
F2: CN → T1	64 K	96	22	39	28
F3: CN → T2	64 K	97	10	39	28
F4: CN → T2	64 K	90	21	39	30
F1: CN → T1	128 K	89	12	39	31
F2: CN → T1	128 K	91	22	39	28
F3: CN → T2	128 K	85	11	39	29
F4: CN → T2	128 K	87	21	39	30
F1: CN → T1	256 K	89	10	39	28
F2: CN → T1	256 K	88	22	39	31
F3: CN → T2	256 K	92	10	39	30
F4: CN → T2	256 K	93	20	39	32
F1: CN → T1	512 K	87	11	39	29
F2: CN → T1	512 K	88	21	39	28
F3: CN → T2	512 K	82	12	39	28
F4: CN → T2	512 K	93	23	39	31

Table 35: F1, F2, F3 and F4 reservation performance measurements (DL PMP single-hop scenario)

In this test, flows F1 and F2 are sent to terminal T1 (connected to SS1), whereas flows F3 and F4 are sent to Terminal T2 (connected to SS2). Therefore, two independent reservation processes occur simultaneously – one for SS1 (F1 and F2) and the other for SS2 (F3 and F4). This is demonstrated by the times illustrated in Table 35. The **ΔT2-F1** and the **ΔT2-F2**, as shown in Table 35, are around 11 seconds and 22 seconds, respectively. Similarly, the **ΔT2-F3** and the **ΔT2-F4** are also around 11 and 22 seconds. This demonstrates that the reservation processes in each one of the SSs are completely independent and can be performed at the same time, even though they are connected to the same BS.

If we compare the obtained results in this point-to-multipoint test (Table 35) with the results collected in the point-to-point test (Table 32), we can see that in the point-to-point case, the ΔT2-F3 and the ΔT2-F4 took, approximately, 31 and 42 seconds. This is due to the fact that the service flow reservations had all to be done (sequenced) in the same SS.

5.1.2.1.2. Service Flow Modification

The timing measurements results of the service flows upgrade are shown in Table 36.

Flow	ΔBW (bps)	ΔT5 (µsec)	ΔT6 (sec)	ΔT7 (µsec)
F1: CN → T1	64 K → 128 K	199	21	20
F2: CN → T1	64 K → 128 K	201	42	19
F3: CN → T2	64 K → 128 K	188	20	21
F4: CN → T2	64 K → 128 K	193	41	18
F1: CN → T1	128 K → 256 K	191	21	19
F2: CN → T1	128 K → 256 K	187	42	20
F3: CN → T2	128 K → 256 K	190	22	20
F4: CN → T2	128 K → 256 K	199	42	18
F1: CN → T1	256 k → 512 K	198	20	22
F2: CN → T1	256 k → 512 K	197	41	21
F3: CN → T2	256 k → 512 K	200	21	20
F4: CN → T2	256 k → 512 K	192	42	19
F1: CN → T1	512 K → 1M	199	21	23
F2: CN → T1	512 K → 1M	190	42	22
F3: CN → T2	512 K → 1M	187	21	22
F4: CN → T2	512 K → 1M	201	43	20

Table 36: Two flows per terminal modification performance measurements (DL PMP single-hop scenario)

For the service flow modification case (Table 36), the results are also different from the ones obtained in the point-to-point scenario (Table 33). The reason for this behaviour is similar to the one explained for the reservation case and depicted in section 5.2.1.1.1.

Briefly summarizing, the reservation and modification processes measurements in the point-to-multipoint test, using two flows per SS (section 5.1.2.1), are different when compared to the measurements obtained for the point-to-point test, using four flows (section 5.1.1.2). This is due to the fact that, in the point-to-multipoint case, the service flows reservations are done at the same time for both SSs, whereas in the point-to-point test, the service flows reservation had all to be done (sequenced) in the same SS.

5.2. Two-Hop Scenario QoS Tests

In this section we study the QoS behaviour of the 802.11e and the 802.16 networks. Figure 59 illustrates the implemented demonstrator for the two-hop scenario QoS tests. In this case, 802.11e APs are directly connected to the SSs, providing a concatenated access network. Two MNs are connected to each AP. The 802.16 BS is directly connected to AR1, establishing the link between the RAN and the AN. The CN that will be responsible to receive and send data packets in the uplink and downlink directions, respectively, is connected to AR2 via 802.11e.

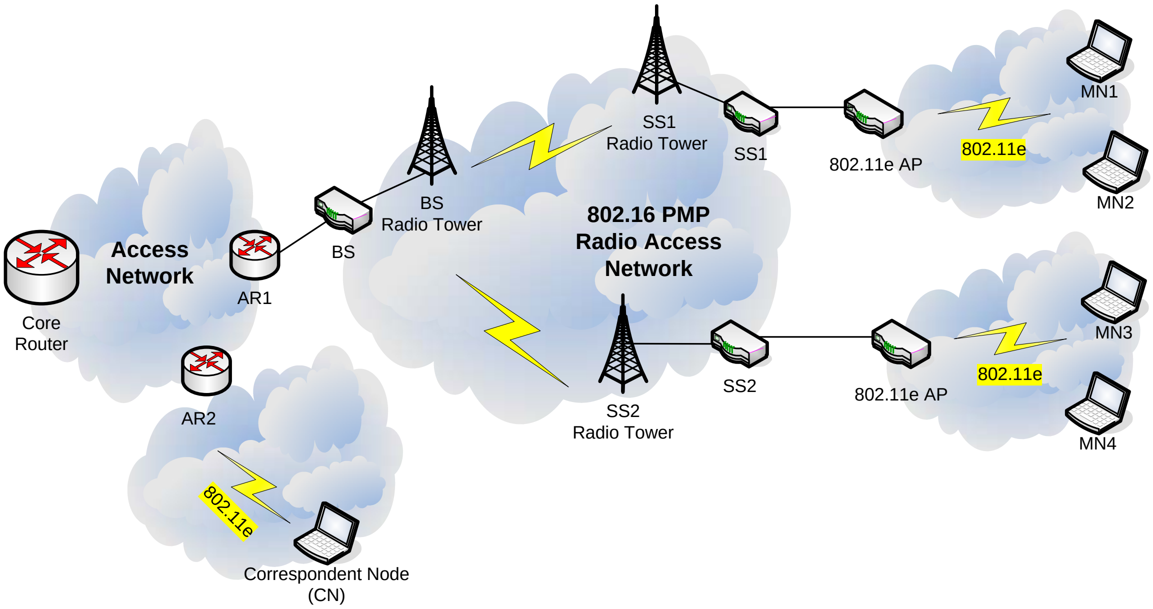

Figure 59: Implemented demonstrator for the two-hop scenario

As in the single-hop scenario tests, QoSM and QoSAL are running in the ARs. The QoSAL is also running in the MNs and in the 802.11e APs. The MGEN tool is running in the CN and in the MNs.

5.2.1. Downlink Point-to-Point Scenario

We started by performing point-to-point tests in the downlink direction. The 802.16 point-to-point link is created between the BS and SS1 (see Figure 60).

5.2.1.1. TH – D – PTP – Test 1

This test is performed in a Two-Hop (TH), Downlink (D) Point-to-Point (PTP) scenario. Two flows (F1 and F2) are used in this test. F1 and F2 are sent from the CN to MN1 and MN2, respectively. Figure 60 depicts this test.

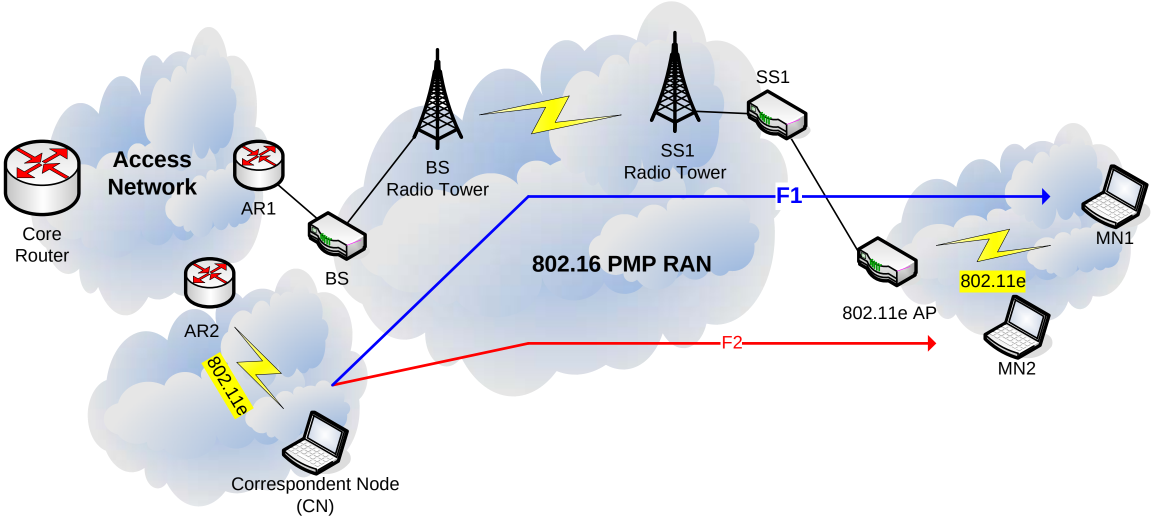

Figure 60: TH – D – PTP – Test 1 implemented demonstrator

5.2.1.1.1. Service Flow Reservation

In this case, two QoS reservations are requested by the QoSAL module. Table 37 presents the individual results of the time necessary to perform a reservation in the two-hop network composed by the 802.16 technology and by the 802.11e technology. **ΔT8**, in microseconds (**µsec**), represents the amount of time that the 802.11e technology takes to perform a service flow reservation in the air link.

Flow	BW (bps)	ΔT1 (µsec)	ΔT2 (sec)	ΔT3 (msec)	ΔT4 (µsec)	ΔT8 (µsec)
F1: CN → MN1	64 K	96	10	38	28	360
F2: CN → MN2	64 K	104	20	41	32	138
F1: CN → MN1	128 K	97	11	43	31	452
F2: CN → MN2	128 K	93	21	40	30	157
F1: CN → MN1	256 K	98	11	39	30	433
F2: CN → MN2	256 K	99	21	42	29	147
F1: CN → MN1	512 K	92	10	36	31	586
F2: CN → MN2	512 K	95	21	41	28	229

Table 37: F1 and F2 reservation performance measurements (DL PtP two-hop scenario)

Regarding the 802.16 service flow reservation period (**ΔT2**), no changes are noticed comparing to the previous tests. The amount of time required to perform the QoS reservation in the 802.11e technology is always below 500 microseconds. We can also calculate the amount of time needed to perform a reservation in the composed heterogeneous RAN. As we can easily see from the obtained results (802.16 results and 802.11e results), the total amount of time is always below 5 milliseconds, which is a good result for next generation environments.

5.2.1.1.2. Service Flow Modification

In this section we analyse the service flow modification in this scenario. The obtained measurements are shown in Table 38. **ΔT9**, in microseconds (**µsec**) is the amount of time taken by the 802.11e driver to perform a service flow modification in the 802.11e technology.

Flow	ΔBW (bps)	ΔT5 (µsec)	ΔT6 (sec)	ΔT7 (µsec)	ΔT9 (µsec)
F1: CN → MN1	64 K → 128 K	201	21	20	160
F2: CN → MN2	64 K → 128 K	199	42	19	146
F1: CN → MN1	128 K → 256 K	193	20	21	170
F2: CN → MN2	128 K → 256 K	189	41	18	145
F1: CN → MN1	256 k → 512 K	197	21	19	167
F2: CN → MN2	256 k → 512 K	196	41	20	145
F1: CN → MN1	512 K → 1M	203	22	24	190
F2: CN → MN2	512 K → 1M	199	43	21	184

Table 38: F1 and F2 modification performance measurements (DL PtP two-hop scenario)

Analysing the 802.16 related times (**ΔT5, ΔT6** and **ΔT7)** in Table 38, we can see that no significant changes occurred comparing to previously presented tests, such as OD – PMP – Test 1 depicted in section 5.1.2.1. Regarding the modification process in the 802.11e network, the obtained times are always below (or approximately) 200 microseconds. This easily shows that real-time services support is not compromised in the two-hop scenario.

5.2.2. Downlink Point-to-Multipoint Scenario

In this section, we will study the downlink point-to-multipoint scenario performance. The 802.16 point-to-multipoint link is created between the BS, the SS1 and the SS2 (see Figure 59).

5.2.2.1. TH – D – PMP – Test 1

In this test four flows (F1, F2, F3 and F4) are created in the CN. F1 and F2 are sent to MN1, through SS1, whereas F3 and F4 are sent to MN3, through SS2. This test is illustrated in Figure 61.

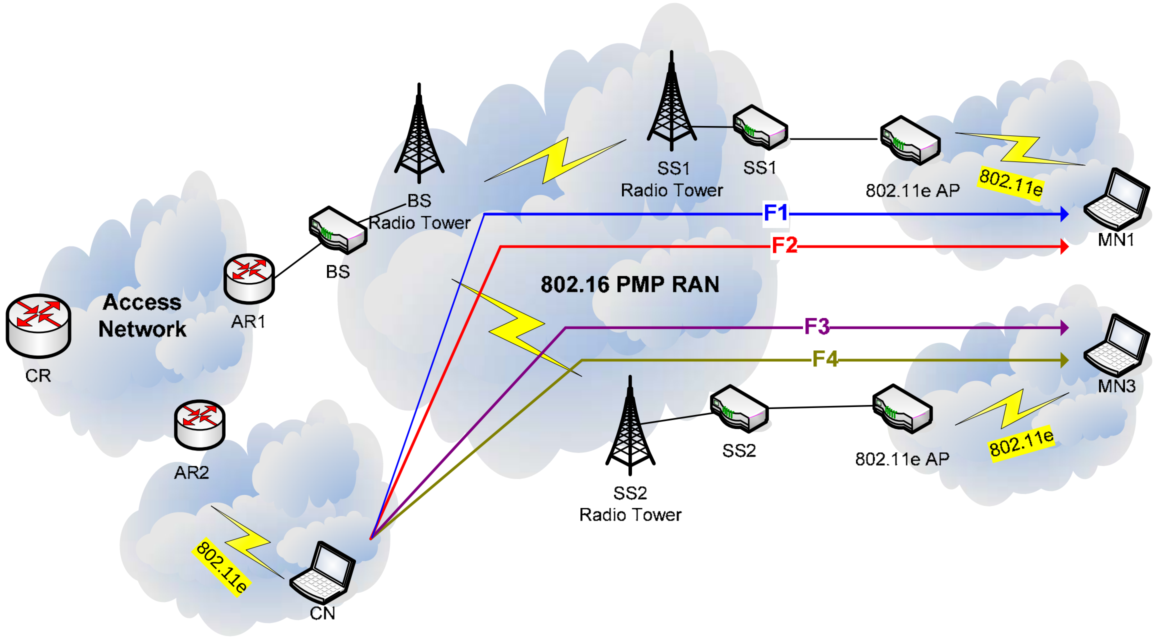

Figure 61: TH – D – PMP – Test 1 implemented demonstrator

5.2.2.1.1. Service Flow Reservation

The reservation process for the four flows involved (F1, F2, F3 and F4) is presented in the following table (Table 39).

Flow	BW (bps)	ΔT1 (µsec)	ΔT2 (sec)	ΔT3 (msec)	ΔT4 (µsec)	ΔT8 (µsec)
F1: CN → MN1	64 K	99	10	39	29	512
F2: CN → MN1	64 K	101	21	38	32	213
F3: CN → MN3	64 K	95	10	39	31	441
F4: CN → MN3	64 K	92	22	39	30	156
F1: CN → MN1	128 K	96	11	39	28	483
F2: CN → MN1	128 K	99	22	41	34	256
F3: CN → MN3	128 K	89	10	39	29	390
F4: CN → MN3	128 K	90	20	39	28	184
F1: CN → MN1	256 K	101	11	39	29	452
F2: CN → MN1	256 K	95	22	39	31	193
F3: CN → MN3	256 K	97	12	39	31	542
F4: CN → MN3	256 K	85	22	38	30	210
F1: CN → MN1	512 K	99	10	37	34	490
F2: CN → MN1	512 K	88	20	39	32	270
F3: CN → MN3	512 K	90	11	38	34	378
F4: CN → MN3	512 K	93	22	39	29	146

Table 39: F1, F2, F3 and F4 reservation performance measurements (DL PMP two-hop scenario)

The obtained results for the point-to-multipoint environment do not vary comparing to the point-to-point results obtained in TD – PTP – Test 1 in section 5.2.1.1.

5.2.2.1.2. Service Flow Modification

The results for the modification process are shown in Table 40.

Flow	ΔBW (bps)	ΔT5 (µsec)	ΔT6 (sec)	ΔT7 (µsec)	ΔT9 (µsec)
F1: CN → MN1	64 K → 128 K	195	21	19	173
F2: CN → MN1	64 K → 128 K	183	42	21	141
F1: CN → MN2	64 K → 128 K	172	20	22	184
F2: CN → MN2	64 K → 128 K	189	41	18	143
F1: CN → MN1	128 K → 256 K	198	21	21	156
F2: CN → MN1	128 K → 256 K	203	42	20	152
F3: CN → MN1	128 K → 256 K	193	20	22	182
F1: CN → MN2	128 K → 256 K	183	40	22	155
F1: CN → MN1	256 k → 512 K	199	21	24	183
F2: CN → MN1	256 k → 512 K	178	41	19	156
F1: CN → MN2	256 k → 512 K	192	21	21	195
F2: CN → MN2	256 k → 512 K	183	42	18	188
F1: CN → MN1	512 K → 1M	202	22	18	177
F2: CN → MN1	512 K → 1M	189	43	16	135
F3: CN → MN1	512 K → 1M	193	22	21	205
F1: CN → MN2	512 K → 1M	198	44	19	169

Table 40: F1, F2, F3 and F4 modification performance measurements (DL PMP two-hop scenario)

As well as in the service flow reservation process discussed in section 5.2.2.1.1, the service flow modification performance measurements are similar to the ones obtained in the point-to-point case, and illustrated in section 5.2.1.1.2.

5.2.3. Uplink Point-to-Point Scenario

Until now, all the presented tests have been done in the downlink direction. This section analyses the performance of the 802.16 driver in the uplink direction on a point-to-point topology. In this case, the 802.16 point-to-point link is created between the SS1 and the BS (see Figure 59).

5.2.3.1. TH – U – PTP – Test 1

As illustrated in Figure 62, a single flow (F1) is sent by the MN1, through SS1, to the CN.

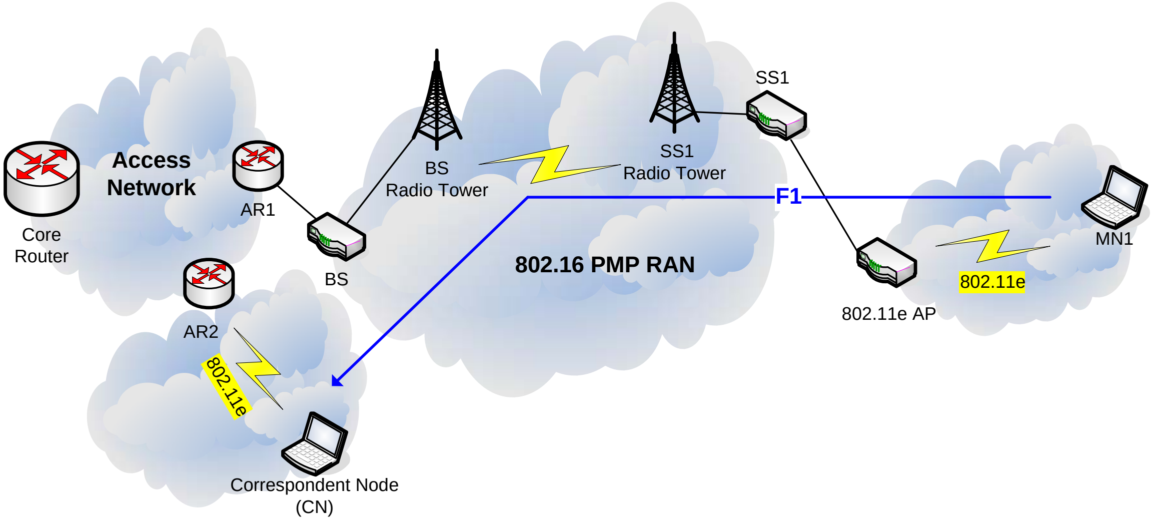

Figure 62: TH – U – PTP – Test 1 implemented demonstrator

5.2.3.1.1. Service Flow Reservation

In the downlink direction, after the service flow is installed in the 802.16 equipment (**ΔT2**), two translation rules, one in the AR and the other one in the AP/MN, must be installed (refer to section 4.3.3.2). The translation rule in the AR (**ΔT3**) allows the destination MAC address of the packets to be changed to the appropriated VMAC address, whereas the translation rule in the AP/MN (**ΔT4**) performs the reverse translation process before the downlink packet is delivered to the MN. In the uplink direction the process is similar. The only difference resides on the fact that only one translation rule is necessary to install in the AP/MN. This translation rule is responsible to translate the source MAC address of the uplink packets to the appropriated VMAC address. The time taken by the system to install this translation rule is given, in milliseconds (**msec**), by **ΔT10**. Detailed information about the uplink service flow reservation is given in section 4.3.3.1.

Flow	BW (bps)	ΔT1 (μsec)	ΔT2 (sec)	ΔT10 (msec)	ΔT8 (μsec)
F1: CN → MN1	64 K	82	11	39	586
F1: CN → MN1	128 K	90	11	39	565
F1: CN → MN1	256 K	85	11	39	596
F1: CN → MN1	512 K	83	12	38	570
F1: CN → MN1	1 M	88	11	41	582

Table 41: F1 reservation performance measurements (UL PtP two-hop scenario)

As illustrated in Table 41**, ΔT10** is approximately 40 milliseconds. Despite this time is high, it does not affect the QoS performance of the system since the packets are using the backup service flow while it is not completed. Regarding the other values in Table 41, they are similar to the service flow reservation values obtained in previous tests for the opposite direction.

5.2.3.1.2. Service Flow Modification

In the downlink direction, when the ***AL-CNX-MODIFY-REQ*** message is received by the 802.16 driver, admission control is performed and a translation rule in the AR is blocked to redirect the downlink packets from the dedicated service flow to the backup service flow (**ΔT5**). Then, the service flow modification in the 802.16 equipment is performed (**ΔT6**). Finally, the translation rule in the AR must be unblocked to redirect packets from the backup service flow to the modified and dedicated service flow (**ΔT7**). In the uplink direction, when the ***AL-CNX-MODIFY-REQ*** message is received, a translation rule must be blocked in the AP to redirect the uplink packets from the dedicated service flow to the backup service flow before they reach the SS. The amount of time required by the 802.16 driver to block the translation rule in the AP and reply with an ***AL-CNX-MODIFY-RESP*** message is given, in milliseconds (**msec**), by **ΔT11**. Only after the translation rule is blocked in the AP, the service flow can be modified. After the service flow is modified, the translation rule in the AP must be unblocked to redirect the uplink packets from the backup service flow to the dedicated service flow. This time is given, in milliseconds (**msec**), by **ΔT12**. Results for the uplink service flow modification are presented in Table 42.

Flow	ΔBW (bps)	ΔT11 (msec)	ΔT6 (sec)	ΔT12 (msec)	ΔT9 (µsec)
F1: CN → MN1	64 K → 128 K	46	21	38	189
F1: CN → MN1	128 K → 256 K	46	21	42	184
F1: CN → MN1	256 k → 512 K	42	21	38	220
F1: CN → MN1	512 K → 1 M	45	22	38	246
F1: CN → MN1	1 M → 2 M	46	21	36	207

Table 42: F1 modification performance measurements (UL PtP two-hop scenario)

Table 42 shows that **ΔT11** (used for the uplink) is higher then **ΔT5** (used for the downlink). This is due to the fact that, in this case (uplink modification), the translation rule that must be blocked is located in the AP. Therefore, a ***TR-BLK-REQ*** message must be sent to the AP, and the AP must reply with a ***TR-BLK-RSP*** message, both over the air. As a result, the time spent in this process is much higher then the time spent to block a translation rule in the AR. After the service flow is modified, the translation rule must be unblocked in the AP; the time spent to unblock the translation rule in the AP is given by **ΔT12**. This time is low and does not compromise the service flow modification process.

5.2.4. Intra-SS Communication

In this section, the communication between MNs that are connected to different SSs, within the same BS, is going to be analysed.

In this case, the MGEN tool will be running only in MN1 and MN3. MN 1 will be used as the sending node, whereas MN3 is utilised as the receiving entity. Two flows (F1 and F2) are used in this test. As illustrated in Figure 63, F1 and F2 are sent by the MN1, through SS1, to the MN3, connected to SS2.

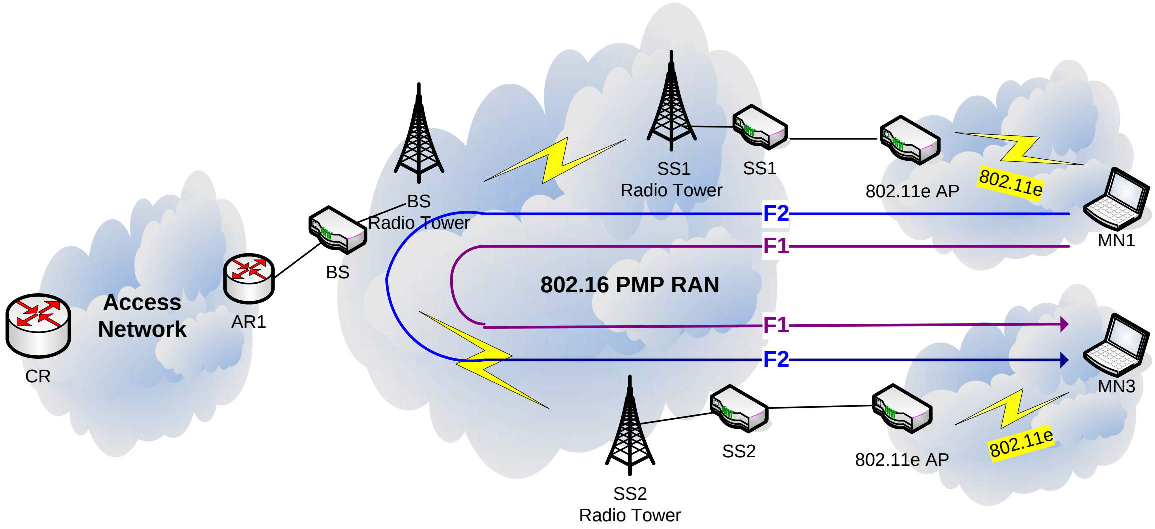

Figure 63: Intra-SS implemented demonstrator

5.2.4.1. Service Flow Reservation

In this scenario we must perform two different service flow reservations: an uplink service flow is reserved from SS2 to the BS, and a downlink service flow reservation is performed from the BS to SS1. The uplink reservation allows the packets sent from MN3 to reach the AR, whereas the downlink reservation allows the packets to be sent from the AR towards its final destination – MN1. Table 43 provides the uplink service flow reservation (from MN3 to the AR).

Flow	BW (bps)	ΔT1 (µsec)	ΔT2 (sec)	ΔT10 (msec)	ΔT8 (µsec)
F1: MN1 → MN3	64 K	97	10	38	489
F2: MN1 → MN3	64 K	86	21	39	256
F1: MN1 → MN3	128 K	82	11	39	573
F2: MN1 → MN3	128 K	93	21	39	331
F1: MN1 → MN3	256 K	99	10	41	512
F2: MN1 → MN3	256 K	89	20	38	213
F1: MN1 → MN3	512 K	88	11	39	488
F2: MN1 → MN3	512 K	92	22	39	155

Table 43: F1 and F2 uplink reservation performance measurements (PMP two-hop scenario)

The downlink service flow reservation (from the AR to MN1) is depicted in Table 44.

Flow	BW (bps)	ΔT1 (μsec)	ΔT2 (sec)	ΔT3 (msec)	ΔT4 (μsec)	ΔT8 (μsec)
F1: MN1 → MN3	64 K	96	11	39	27	423
F2: MN1 → MN3	64 K	87	22	39	31	198
F1: MN1 → MN3	128 K	104	10	38	29	367
F2: MN1 → MN3	128 K	103	21	40	29	143
F1: MN1 → MN3	256 K	99	11	40	28	588
F2: MN1 → MN3	256 K	86	21	39	26	261
F1: MN1 → MN3	512 K	93	11	39	29	512
F2: MN1 → MN3	512 K	91	22	39	31	312

Table 44: F1 and F2 downlink reservation performance measurements (PMP two-hop scenario)

As demonstrated in Table 43 and Table 44, the results obtained in this scenario are inline with the previous obtained results for a service flow reservation in the uplink (section 5.2.3.1.1) and downlink directions (section 5.2.2.1.1).

5.2.5. Fast Mobility

A set of tests involving both QoS and mobility have been performed in this section. The main goal is to prove that, despite the 802.16 equipment limitations, it is perfectly capable of supporting mobility scenarios. In these mobility scenarios, 802.16 can be used as the source or the destination network without compromising the behaviour of the system.

As we can see in Figure 64, the MGEN tool is running in the CN and in MN5. To analyse the fast-mobility process, a flow (F1) is sent by the CN to the MN5, initially connected to AR3. While the MN5 is physically moving away from AR3, the coverage will decrease and, as a consequence, the MN5 will handover to AR1, through SS1.

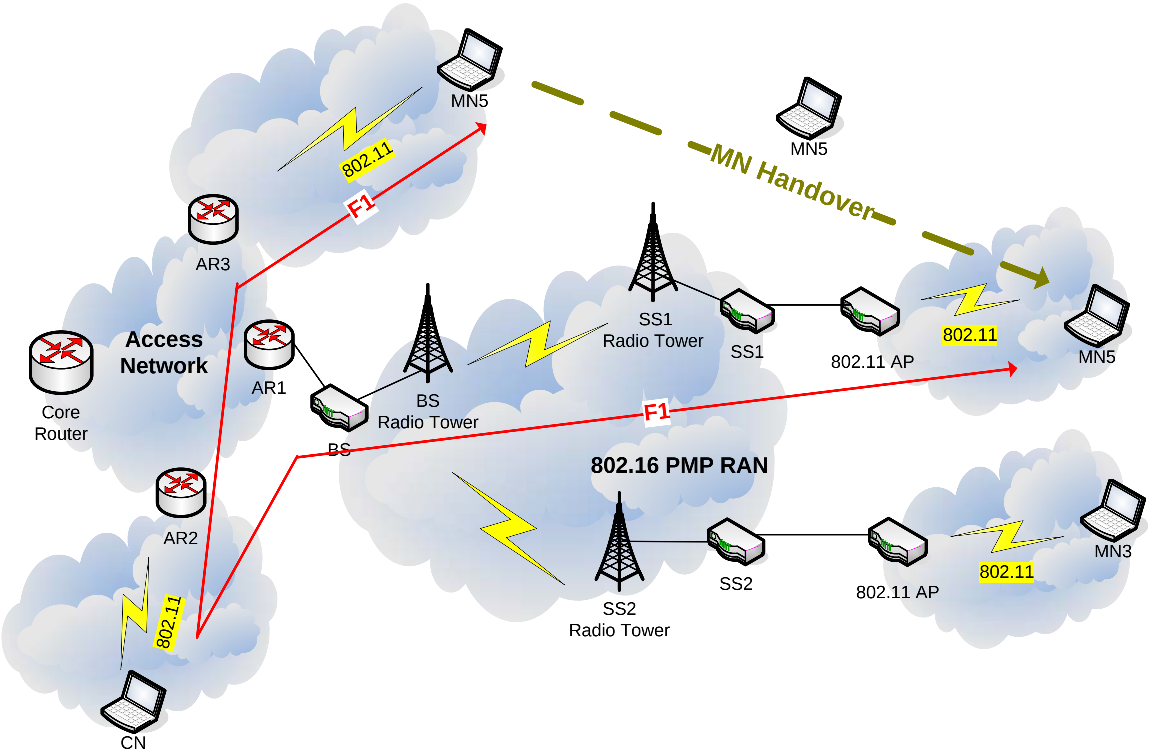

Figure 64: Fast mobility implemented demonstrator

5.2.5.1. Service Flow Reservation

During the handover process, the reservations in the old AR (AR3) must be teardown and the resources released. Simultaneously, new reservations in the new AR (AR1) must be established. In this case, new reservations must be created in the 802.16 link between BS and SS1. The service flow reservation measurements in the new AR during the fast-mobility process are depicted in Table 45.

Flow	BW (bps)	ΔT1 (µsec)	ΔT2 (sec)	ΔT3 (msec)
F1: CN → MN5	64 K	82	10	39
F1: CN → MN5	128 K	103	10	38
F1: CN → MN5	256 K	92	11	39
F1: CN → MN5	512 K	95	10	39

Table 45: F1 downlink reservation performance measurements (Fast-mobility scenario)

As expected, the measured times are totally compliant with a fast handover scenario. The amount of time taken by the 802.16 driver to reply to the QoSAL (**ΔT1**), and consequently, the time required for the data packets to start flowing in the backup service flow is very low. On the other hand, the time necessary to perform a service flow reservation in the 802.16 equipment is high (**ΔT2**). However, packets are redirected through the backup service flow during this period and therefore traffic disruption is avoided.

5.3. Summary

We analyzed the QoS performance of the developed 802.16 Driver in both, the single-hop scenario and the two-hop scenario. A deep evaluation of the driver capabilities has been done, including QoS and fast-mobility tests. Concerning the QoS performance tests, we have demonstrated that a dynamic service flow reservation took about 100 µs using the developed solution while more then 10 seconds were taken without the developed solution. Likewise, a service flow modification took about 190 µs with the implemented solution whereas more than 20 seconds were spent using the original solution. Additionally, we have also demonstrated that the admission control developed module is working and efficiently controlling the available resources. Considering mobility, a set of tests has been done by moving a MN between an 802.11 AP connected to an 802.16 SS and an 802.11 AP collocated with an AR. As expected, during fast-mobility scenarios, the amount of time taken to perform a service flow reservation in the 802.16 system was very small, not compromising the fast-mobility process. With the obtained results we demonstrated that it is perfectly possible to integrate 802.16 in next generation networks, such as DAIDALOS.

Chapter 6: Conclusions

The work presented in this Thesis addressed key aspects of an architecture which is able to bring 802.16 technologies into play for the future 4G networks in compounded wireless environments. A modular architecture, which provides seamless QoS support over different wireless technologies, MANs and LANs, for the access network is described. Furthermore, an interface with the core network is also provided to perform end-to-end QoS.

The designed layer 2 QoS architecture is a modular architecture composed by two main modules: the technology independent module (QoSAL) and the technology dependent module (technology drivers). The QoSAL module is responsible for the layer 2 signalling part of the access network QoS architecture and for the communication with the core network QoS entities. It implements the functionality of resource management in the access network, being able to perform QoS reservations, modifications and deletions. Additionally, if necessary, it performs resource queries to the technologies that compose the access network. The technology dependent modules are responsible for the QoS support for a particular technology in a single network link. They directly communicate with the specific technology, translating general QoS parameters from the QoSAL, such as TSpec and RSpec, to technology specific QoS parameters.

The work developed and implemented in this Thesis is focused on the technology dependent module for the 802.16 technology – the 802.16 Driver. This allows the separation between the network and technology parts of the architecture, providing a seamless way for other technologies integration. Thus, scalability is provided just by adding the correspondent technology dependent module, whereas flexibility is achieved through the support of complex scenarios. Besides the single-hop scenario, the designed architecture is enhanced by adding the two-hop scenario capability, allowing the concatenation of two different technologies to extend the access network. For this Thesis, we have exploited both solutions. In the single-hop scenario, the MN is directly connected to the 802.16 SS, whereas in the two-hop scenario, the MN is associated with an 802.11e AP connected to the 802.16 SS. Besides the single-hop and two-hop scenarios support, the developed and implemented architecture also supports two different modes of operation for the 802.16 system: point-to-point and point-to-multipoint. Thus, combining the two supported scenarios with the two different modes of operation, several tests with different characteristics were exploited.

Our architecture supports fast mobility in the two-hop scenario. In this case, the MNs associated with the 802.11e APs are able to handoff without traffic disruption. This feature allows the operators to provide ubiquitous internet access and thus envisage the challenging ABC (Always Best Connected) philosophy for next generation environments. The architecture overcomes the shortcomings of the 802.16 technology, allowing real-time services to be used in a dynamic environment, where users roam across 802.11 APs. For reaching this aim, both virtual MAC addresses and auxiliary channels had to be used, implying novel functionalities inside the 802.16 network. A mechanism to filter and translate all the packets that are sent to the 802.16 network has also been developed and implemented – MAC Address Translator (MAT) mechanism. The proposed methodology addresses the dynamic problems, by temporary allowing traffic to flow in a reserved channel, thus providing temporary better QoS assurances to traffic flows. Naturally, the quality of this reserved channel can be configured according to the network operator policy.

A field demonstrator has been developed with a commercial 802.16 equipment, as part of a larger 4G architecture demonstrator developed under the scope of the DAIDALOS project. Experimental results for the wireless access have been obtained. The results demonstrated that reservation times are very small and perfectly capable to be integrated in 4G environments, providing QoS differentiation in such a heterogeneous environment. Besides the reservation times, the implemented solution has shown that the service modification measured times are also very low and traffic disruption is avoided. Moreover, we have demonstrated that the obtained measures are independent of the scenario or mode of operation being used in the 802.16 network. Additionally, using a single or several flows, one or two MNs, or even uplink or downlink traffic does not interfere in the measured times. Performance measurement tests have also been done for fast mobility. In this case, with the implemented functionalities, we have seen that no packet losses or delays are noticed during the fast handover process.

As future work, we intend to implement the required functionalities and integrate the solution presented in this Thesis in other 802.16 commercial equipments. Moreover, an SNMP or COPS interface is envisaged for the communication with the 802.16 equipment, instead of the HTTP interface currently employed. Furthermore, we plan to address and study the future mobile and mesh 802.16 networks.

References

	[16-wg]	IEEE 802.16 Working Group (WG). URL: http://www.ieee802.org/16/
A		
	[aguiarmobsum04]	R. L. Aguiar et al, “Designing Networks for the Delivery of Advanced Flexible Personal Services: the Daidalos approach” Proc. IST Mobile & Wireless Telecommunications Summit, Lyon 2004.
	[atmsig06]	ATM Forum Specification af-sig-0061.000, ATM User-Network Interface (UNI) Signalling Specification, Version 4.0, July 1996.
	[atmuni94]	ATM Forum Specification af-uni-0010.002, ATM User-Network Interface Specification, Version 3.1, September 1994.
C		
	[carmobsum05]	Gustavo Carneiro, Carlos Garcia, Pedro Neves, Zhikui Chen, Michelle Weterwald, Manuel Ricardo, Pablo Serrano, Susana Sargento, Albert Banchs, “The DAIDALOS Architecture for QoS Over Heterogeneous Wireless Networks”, Mobile Summit 2005, 14th IST Mobile & Wireless Communications Summit, Dresden, Germany, June 2005.
D		
	[daid]	IST-DAIDALOS project. URL: http://www.ist-daidalos.org
	[docsis]	SCTE DSS 00-05, “Data-Over-Cable Service Interface Specification (DOCSIS) SP-RFIv1.1-I05-000714, Radio Frequency Interface 1.1 Specification", July 2000.

	[dsl]	DSL Forum. URL: http://www.dslforum.org
	[dvb]	Digital Video Broadcasting; EN 301 192, DVB specification for data broadcasting; European Telecommunication Standards Institute, European Broadcasting Union; 1994 – 1998.
E		
	[eklcommag02]	Carl Eklund, Roger B. Marks, Kenneth L. Stanwood and Stanley Wang, "IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access", IEEE Com. Mag., June 2002.
	[etsi]	European Telecommunications Standards Institute (ETSI). URL: http://www.etsi.org
G		
	[gesbcommag02]	D. Gesbert et al., "Technologies and Performance for Non Line-of-Sight Broadband Wireless Access Networks", IEEE Commun. Mag., vol. 40, no. 4, Apr. 2002, pp. 86–95
H		
	[hillcommag04]	Joachim Hillebrand et al, "Quality-of-Service Signalling for Next-Generation IP-Based Mobile Networks", IEEE Communications Magazine, June 2004, pp 72-79.
I		
	[ieee]	Institute of Electrical and Electronics Engineers (IEEE). URL: http://www.ieee.org
	[ieee802]	IEEE Std 802-2001, "IEEE Standards for Local and Metropolitan Area Networks: Overview and

		Architecture”, 2001.
	[ieee802.3-02]	IEEE Std 802.3-2002, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
	[ieee802.11-99]	IEEE Std 802.11-1999, “IEEE 802.11 Standard for Wireless LAN: Medium Access Control (MAC) and Physical Layer (PHY) Specification”, New York, IEEE Inc., 1999.
	[ieee802.11e]	IEEE Std 802.11e, “IEEE Standard for Local and Metropolitan Area Networks, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications – Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements”, IEEE Standard 802.11e, November 2005.
	[ieee802.16-01]	IEEE Std 802.16-2001, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems", IEEE Standard 802.16-2001, April 2002.
	[ieee802.16c-02]	IEEE Std 802.16c-2002, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 1: Detailed System Profiles for 10-66 GHz", IEEE Standard 802.16c-2002, January 2003.
	[ieee802.16a-03]	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.
	[ieee802.16-04]	IEEE Std 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems", IEEE Standard 802.16-2004, October 2004.
	[ieee802.16e-05]	IEEE Std 802.16e-2005, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", IEEE Standard 802.16e-2005, February 2006.
	[itu]	International Telecommunication Union (ITU). URL: http://www.itu.int
J		
	[janelsev05]	J. Jähnert, et al, "The 'pure-IP' Moby Dick 4G architecture", Elsevier, Computer Communications, Vol. 28, Issue 9, 2nd June 2005, ISSN –140-3664.
K		
	[kassecon04]	Andreas Kassler, Pedro Neves, Susana Sargento, Rui L. Aguiar, Sérgio Crisóstomo, "QoS and Multicast aware Integration of Ad-Hoc Networks with Infrastructure Networks based on 802.11 and 802.16", IEEE Secon 2004, 1st IEEE International Conference on Sensor and Ad-Hoc Communications and Networks, Santa Clara - California, EUA, October 2004.
	[kaswadhoc05]	Andreas Kassler, Pedro Neves, Susana Sargento, Rui L. Aguiar, Sérgio Crisóstomo, "Integration of Ad-Hoc Networks with Infrastructure Networks – a QoS perspective", Ad-Hoc 2005, 5th Scandinavian Workshop on Wireless Ad-hoc Networks, Stockholm, Sweden,

		May 2005.
	[kasmedhoc05]	Andreas Kassler, Susana Sargento, Adel Ben Mnaouer, Chen Lei, Pedro Neves, Rui L. Aguiar, Pedro M. Ruiz, “Supporting Multicast in Ad-Hoc networks in a Hotspot Context”, In Proc. 4th Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2005), 21-24, Île de Porquerolles, France, June 2005.
L		
	[litofdm]	L. Litwin, Michael Pugel, “The Principles of OFDM”
M		
	[marqwcom03]	V. Marques et al., “An IP-Based QoS Architecture for 4G Operator Scenarios”, IEEE Wireless Comm., June 2003.
N		
	[nevconftele05]	Pedro Neves, Susana Sargento, Rui L. Aguiar, “Implementation of QoS Support in IEEE 802.16 Access Networks”, Conftele 2005, 5th Conference on Telecommunications, Tomar, Portugal, April 2005.
	[nev16ngps06]	Pedro Neves, Susana Sargento, Rui L. Aguiar, “IPv6 Real-Time Usage of IEEE 802.16: Problem Statement”, IETF 16ng WG draft document, February 2006.
	[nev16ng06]	Pedro Neves, Susana Sargento, Rui L. Aguiar, “QoS Aware Real-Time Support for IPv6 in IEEE 802.16 Backhaul Scenarios”, IETF 16ng WG draft document, February 2006.
	[neviscc06]	Pedro Neves, Susana Sargento, Rui L. Aguiar, “Support of Real-time Services over Integrated 802.16 Metropolitan and Local Area Networks”, ISCC 2006, IEEE Symposium on Computers and Communications, Cagliary, Italy, June 2006.

	[nist]	National Institute of Standards and Technology (NIST). URL: http://www.nist.gov
	[nunomob]	Nuno Sénica, Justino Santos, Susana Sargento, Rui L. Aguiar. "Mobility Between Heterogeneous Networks: Integration and Evaluation", Special Issue on Mobile and Ubiquitous Computing of The Mediterranean Journal of Computers and Networks. (accepted for publication)
P		
	[priorhicss05]	Rui Prior et al, "Heterogeneous Signalling Framework for End-to-end QoS support in Next Generation networks", HICCS-38, Hawaii International Conference of System Sciences, Hawaii, January 2005.
R		
	[redcom]	Redline Communications. URL: http://www.redlinecommunications.com
	[rfc791]	Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.
	[rfc868]	Postel, J. and K. Harrenstien, "Time Protocol", RFC 868, May 1983.
	[rfc1157]	Case, J., M. Fedor, M. Schoffstall and J. Davin, "The Simple Network Management Protocol", RFC 1157, May 1990.
	[rfc1350]	Sollins, K., "The TFTP Protocol (Revision 2)", RFC 1350, July 1992.
	[rfc1441]	Case, J., et al., "Structure of Management Information for version 2 of the SNMP (SNMPv2)", RFC 1441, 1993.
	[rfc1633]	Braden, R., D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: an Overview", RFC 1633,

		June 1994.
	[rfc1945]	Berners-Lee, T., R. Fielding and H. Frystyk, “Hypertext Transfer Protocol”, RFC 1945, May 1996.
	[rfc2131]	Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
	[rfc2132]	Alexander, S., and R. Droms, “DHCP Options and BOOTP Vendor Extensions”, RFC 2132, March 1997.
	[rfc2205]	Braden, R., Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, “Resource Reservation Protocol”, RFC 2205, September 1997.
	[rfc2349]	Malkin, G., A. Harkin, “TFTP Timeout Interval and Transfer Size Options,” RFC 2349, May 1998.
	[rfc2460]	Deering, S., 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]	Nichols, K., 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.
	[rfc2501]	Corson, S., J. Macker, “Mobile Ad-hoc Networking”, RFC 2501, January 1999
	[rfc2598]	Jacobson, V., K. Nichols, “An Expedited Forwarding PHB”, RFC 2598, June 1999.
	[rfc2710]	Deering, S., W. Fenner, B. Haberman, Multicast Listener Discovery (MLD) for IPv6, RFC 2710, October 1999.

	[rfc2748]	Durham, D., Ed., J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, “Common Open Service Protocol”, RFC 2748, January 2000.
	[rfc2989]	Aboba, B. et al, "Criteria for Evaluating AAA Protocols for Network Access", RFC 2989, April 2000.
	[rfc3261]	Rosenberg, J., et al., “SIP: Session Initiation Protocol”, RFC 3261, June 2002.
	[rfc3264]	Rosenberg, J., H. Schulzrinne, “An Offer/Answer Model with Session Description Protocol (SDP)”, RFC 3264, June 2002.
	[rfc3312]	Camarillo, G., et. al., “Integration of Resource Management and Session Initiation Protocol (SIP)”, RFC 3312, October 2002.
	[rfc3315]	Droms R., 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.
	[rfc3963]	Devarapalli, V., R. Wakikawa, “Network Mobility Basic Support Protocol”, RFC 3963, January 2005
	[rfc4066]	Liebsch, M., “Candidate Access Router Discovery (CARD)”, RFC 4066, July 2005.
	[rfc4068]	Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.
U		
	[un]	United Nations. URL: http://www.un.org
W		
	[wimax]	WiMAX Forum. URL: http://www.wimaxforum.org

	[wifi]	WiFi Forum. URL: http://www.wi-fi.org/
	[wsis]	World Summit on the Information Society. URL: http://www.itu.int/wsis