FCTUC

Departamento de Engenharia Informática
Faculdade de Ciências e Tecnologia
Universidade de Coimbra

Quality of Service and Mobility Support in WiMAX

(Suporte de Qualidade de Serviço e Mobilidade em WiMAX)

Bruno Miguel de Oliveira Sousa

Master Thesis submitted to the University of Coimbra

Dissertação de Mestrado submetida à Universidade de Coimbra

November 12, 2007

Suporte de Qualidade de Serviço e Mobilidade em WiMAX

Dissertação de Mestrado submetida à Universidade de Coimbra

Autor:
Bruno Miguel de Oliveira Sousa

Orientada por:
Marília Pascoal Curado
Kostas Pentikoutis

Novembro 12, 2007

To a beautiful flower, Florinda,
for inspiring me to reach this day.
I never forget you, grandmother!

Acknowledgements

To make this thesis a reality, it would not have been possible without the passive or active participation of many people. I would like to express my gratitude to all of you, after all, it is the minimum I can do.

When working on a team, the spirit is to fight together, to believe in the partner just close to us. I feel this with LCT team.

Thanks David Palma, the discussions of the WEIRD architecture, the explanations of the NSIS framework have been interesting and useful.

Thanks Luis Conceição and Vitor Bernardo GIST is not the same without you.

Thanks Luis Cordeiro, when things got complicated, you saved the day. Your tips and tricks, your comments, your support have been useful and always in the right moment.

Rui Vilão, WEIRD is not the same without you. Those NSIS attendants have your touch. The configuration of the machines in the testbed was easier with you.

Isidro, we got the synchronization issues. Your support to install DAG cards to synchronize the machines has demonstrated me, that with determination we can suceed.

João Almeida and Filipe Amaral, WEIRD Agent is not the same without you. The application to "stress" the WEIRD system has been a precious tool to perform the performance tests.

Fernando Rocha, ns-2 trace files are familiar to you. It would not be possible to analyse ns-2 traces without your support.

Luis Veloso, the tips about evalvid have been a great help to understand how evalvid framework works.

Pedro Neves from PT Inovação, thanks for performing WEIRD performance tests.

To the WEIRD project and to all the people that make it possible. I learn a lot with all of you.

To my supervisors, Marília Curado and Kostas Pentikousis, whose comments, corrections, tolerance for my delays and support have no words to express my appreciation. Above all, for guiding me in this work, without refusing any request of mine.

I can not end without mention my wife, Célia Simões, for being at my side and believing always in me, even in those moments that I did not believe in myself.

I would not have reach this day without all of you!

Foreword

The work described in this thesis was carried out at the Laboratory of Communication and Telematics of the Centre for Informatics and Systems of the University of Coimbra within the context of the WEIRD project:

- WEIRD - *WiMAX Extension to Isolated Research Networks* - European project about Quality of Service and mobility in WiMAX networks, from June 2006 to May 2008. The evaluation of Quality of Service support in the WiMAX equipment and the performance assessment of the signalling protocols was done in the context of this project.

The work done during this thesis resulted in the following publications:

- Bruno Sousa, Marília Curado, Edmundo Monteiro, "IP and WiMAX coalition", in *IEEE Communications Magazine*. [1]
- Bruno Sousa, Pedro Neves, Gabriela Leão, David Palma, Jorge Sá Silva, Susana Sargento, Francisco Fontes, Marília Curado, Fernando Boavida, "The Cost of Using IEEE 802.16d Dynamic Channel Configuration, submitted to *IEEE International Conference on Communications, (ICC2008)*, Beijing, China, May 19-23, 2008.

The following publications concerning Quality of Service were co-authored by the candidate:

- Gabriela Leão, Bruno Sousa, Marília Curado, Jorge Sá Silva, "End-to-end Signaling with Heterogeneous QoS Models Support", in *International Conference On Late Advances in Networks, (ICLAN'2007)*, Paris, France, December 05-07, 2007.

[1] Under editor review.

The following presentations describing WEIRD were performed by the candidate:

- Bruno Sousa, “WEIRD Project Overview”, in *69th meeting Internet Engineer Task Force, (69th IETF)*, Chicago, USA, July 22-27, 2007.

The candidate also performed contributions to the working documents of the WEIRD project:

- Deliverable D2.1, System Scenarios, Business Models and System Requirements.
- Deliverable D2.3, System Specification.
- Deliverable D3.1, Preliminary Implementation Description.

Abstract

Wireless broadband access standards are evolving to meet current trends, namely the need for more bandwidth and the support for real-time applications. IEEE Std 802.16 is one of the main keys in this development process. By addressing both licensed and license exempt radio frequency bands the adoption of this standard becomes easier.

The WiMAX Forum, an independent organization, is specifying the WiMAX technology based on IEEE 802.16 and ETSI HiperMAN standards to enable interoperability between the equipment of different vendors. The WiMAX network architecture model includes a complete architecture to facilitate the deployment of this technology.

Two major versions of WiMAX have been released, a fixed version supporting cells with higher coverage and a mobile version supporting advanced features like mobility and power saving modes.

Handovers between intra and inter-technology represent also a current trend. IEEE Std 802.21, known as Media Independent Handover (MIH) standard, represents one of the efforts to enable seamless handovers between different technologies. Nowadays, user terminals have more then one interface, for instance, one interface for Wi-Fi networks and other for 3G networks. In this context, the goal of the MIH standard is to enable handovers between different technologies.

WEIRD is an FP6 integrated European project aiming to use WiMAX to provide connectivity to remote and impervious areas. Monitoring volcanoes, seismic activities is easier with WiMAX, also fire prevention with sensors installed in the field allow real-time monitoring and the control of vast areas from a control center. WEIRD integrates these applications in WiMAX networks, and provides extensions that allow to configure WiMAX channels within the applications requirements.

This thesis encompasses an analysis of the state of the art of WiMAX, of the IEEE 802.16 standards, of the MIH standard and a description of the WEIRD architecture and deployed protocols. Moreover the mobility support of WiMAX and the support for Quality of Service (QoS) in WEIRD are evaluated.

keywords: IEEE 802.16, WiMAX, WEIRD, MIH, Handover, Quality of Service.

Resumo

Os standards de redes sem fios de longo alcance têm evoluído para fazer face às necessidades de largura de banda e suportar aplicações em tempo real. O Standard IEEE 802.16 tem um papel de relevo neste processo de desenvolvimento. A sua adopção pela indústria está facilitada dado que suporta bandas de radio frequência licenciadas e não licenciadas.

O WiMAX Forum, uma organização independente, está a especificar o WiMAX baseado nos standards IEEE 802.16 e ETSI HiperMAN para permitir a interoperabilidade entre equipamento de diferentes vendedores. O modelo da arquitectura de rede do WiMAX inclui uma especificação completa para facilitar a instalação.

Foram lançadas duas versões do WiMAX, sendo que a versão fixa suporta células com uma maior cobertura, enquanto a versão móvel suporta funcionalidades avançadas como a mobilidade e modos de poupança de energia.

Os *handovers* entre a mesma e diferentes tecnologias são também uma das correntes actuais. O standard IEEE 802.21, conhecido como Media Independent Handover (MIH), representa um dos esforços para possibilitar *handovers* sem perdas entre diferentes tecnologias. Nos dias de hoje, os terminais de utilizadores têm mais do que um tipo de interface, por exemplo uma para redes Wi-Fi e outra para redes 3G. Neste contexto, um dos objectivos do standard MIH é possibilitar o *handover* entre estes tipos de tecnologia diferentes.

O WEIRD é um projecto europeu do sexto Programa Quadro com o intuito de usar o WiMAX para possibilitar a ligação de áreas remotas ou de difícil acesso. Monitorizar vulcões ou actividades sísmicas é mais simples com o WiMAX, também a prevenção de incêndios, com sensores instalados no campo, é possível monitorizar em tempo real e controlar vastas áreas a partir de um centro de coordenação. O WEIRD integra estas aplicações nas redes WiMAX e introduz extensões que permitem configurar os canais WiMAX de acordo com os requisitos das aplicações.

Este documento inclui uma análise do estado da arte do WiMAX, dos standards IEEE 802.16, do standard MIH e uma descrição da arquitectura do WEIRD e dos protocolos usados na mesma. Para além disto, o suporte de mobilidade no WiMAX e o suporte de Qualidade de Serviço (QoS) no WEIRD são avaliados.

Palavras-Chave: IEEE 802.16, WiMAX, WEIRD, MIH, Handover, Qualidade de Serviço.

Table of Contents

List of Figures

List of Tables

Abbreviations and acronyms

3DES	Triple Data Encryption Standard
3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AC	Admission Control
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
ARQ	Automatic Repeat reQuest
ASN	Access Service Network
ASN-GW	Access Service Network Gateway
ATM	Asynchronous Transfer Mode
BE	Best Effort
BRAN	Broadband Radio Access Networks
BS	Base Station
BWA	Broadband Wireless Access
CBR	Constant Bit Rate
CCoA	Colocated CoA
CDF	Cumulative Distribution Function
CID	Connection Identifier
CIF	Common Intermediate Format
CMIP	Client Mobile IP

CN	Correspondent Node
CoA	Care of Address
CoS	Class of Service
CPE	Customer Premises Equipment
CPS	Common Part Sublayer
CRC	Check Redundancy Check
CS	Convergence Sublayer
CSC	Connectivity Service Controller
CSN	Connectivity Service Network
D-ITG	Distributed Internet Traffic Generator
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DNS	Domain Name Service
DSA	Dynamic Service Addition
DSC	Dynamic Service Change
DSCP	Differentiated Services Code Point
DSD	Dynamic Service Deletion
DSL	Digital Subscriber Line
E2E	End-to-End
ertPS	Extended Real-Time Polling Service
ETSI	European Telecommunications Standards Institute
FA	Foreign Agent
FBWA	Fixed Broadband Wireless Access
FBSS	Fast Base Station Switching
FDD	Frequency Division Duplexing
FMIP	Fast Handovers for Mobile IP

FMIPv6	Fast Handovers for Mobile IPv6
FTP	File Transfer Protocol
GEANT	Pan-European Gigabit Research Network
GIST	General Internet Signaling Transport
GOB	Group of Blocks
GOP	Group of Pictures
GPCS	Generic Packet Convergence Sublayer
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communications
HA	Home Agent
HHO	Hard Handover
HMIP	Hierarchical Mobile IP
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Services
IP	Internet Protocol
IPPM	IP Performance Metrics
ITU	International Telecommunications Union
LAN	Local Area Network
LOS	Line of Sight
MAC	Medium Access Control
MDHO	Macro Diversity Handover
MIB	Management Information Base
MICS	Media Independent Command Service
MIES	Media Independent Event Service

MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIHO	Mobile Node Initiated Handovers
MIIS	Media Independent Information Service
MIP	Mobile IP
MN	Mobile Node
MOS	Mean Opinion Score
MPEG	Moving Pictures Experts Group
MPLS	Multiprotocol Label Switching
MRI	Message Routing Information
MS	Mobile Station
MSTP	Mobility Service Transport Protocol
MTU	Maximum Transmission Unit
NCMS	Network Control and Management System
NDP	Neighbour Discovery Protocol
NIHO	Network Initiated Handovers
NLOS	Non Line of Sight
NMS	Network Monitoring System
nrtPS	Non-Real Time Polling Service
ns-2	Network Simulator 2
NSIS	Next Steps in Signalling
NSLP	NSIS Signalling Layer Protocol
NTLP	NSIS Transport Layer Protocol
NUD	Neighbour Unreachability Detection
PAL	Phase Alternating Line
PDF	Probability Distribution Function
PDP	Policy Decision Point

PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PER	Packet Error Ratio
PF	Policy Function
PHB	Per Hop Behaviour
PHS	Payload Header Suppression
PKM	Privacy Key Management
PLR	Packet Loss Ratio
PMIP	Proxy Mobile IP
PMP	Point-to-Multipoint
PoA	Point of Attachment
PoS	Point of Service
PPP	Point-to-Point Protocol
PSNR	Peak Signal Noise to Ratio
PtP	Point-to-Point
QCIF	Quarter Common Intermediate Format
QNE	QoS NSIS Entity
QNI	QoS NSIS Initiator
QoS	Quality of Service
QSPEC	QoS specification
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RC	Resource Controller
RDF	Resource Description Framework
RF	Radio Frequency
RMF	Resource Management Function
RoF	Radio over Fiber

RS	Router Solicitation
RSVP	Resource Reservation Protocol
RTP	Real-Time Protocol
rtPS	Real-Time Polling Service
SA	Security Association
SAP	Service Access Point
SDU	Service Data Unit
SFA	Service Flow Authorization
SFID	Service Flow Identifier
SFM	Service Flow Management
SID	Service Identifier
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SS	Subscriber Station
TC	Traffic Control
TCP	Transport Control Protocol
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
TLS	Transport Layer Security
TMOD	Traffic Model
ToS	Type of Service

UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
VBR	Variable Bit Rate
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WEIRD	WiMAX Extension to Isolated Research Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network

1 Introduction

This thesis addresses the Quality of Service and the mobility support in WiMAX networks.

The organization of this chapter includes Section 1.2 that presents the motivation for the work developed in the context of the WEIRD project, Section 1.2 that describes the objectives of the work performed and Section 1.3 that presents the structure of this thesis.

1.1 Motivation

The access to Internet services makes part of everybody's life. While more people tend to use one specific service, demands also increase, not only due to the exponential increase of the number of users, but also because users try to explore more deeply the available services.

Nowadays the access to the Internet is done mainly through Digital Subscriber Line (DSL) connections at home or dedicated lines at work places. However on remote areas, DSL networks are not deployed since the return of investment is poor for Internet operators. WiMAX is a wireless broadband access technology that supports wide coverage areas and is rich in the functionalities supported, having the potential to play a role in these situations.

WiMAX is a technology based on the IEEE 802.16 and ETSI HiperMAN standards. To avoid interoperability problems that exist with other technologies, an independent organization was formed by different vendors to specify complete system architectures. This organization is the WiMAX Forum.

Fixed WiMAX is based on IEEE Std 802.16-2004, while mobile WiMAX is based on IEEE Std 802.16e. The major difference between the two releases of WiMAX is the mobility support.

WiMAX completes the IEEE Std 802.16 specifications by defining the mandatory parameters to be implemented within a system, and not leaving optional some features (vendor implementation specific) as happens in IEEE Std 802.16. Furthermore, WiMAX has an architecture which includes IP services and the necessary functional entities in the different network segments, for Mobile IP (MIP). WiMAX also includes primitives to optimize the use of one important characteristic of IEEE Std 802.16, the Quality of Service support. Different classes of applications are defined according to their requirements in terms of bandwidth, delay and jitter allowing the mapping to the classes of service supported by IEEE Std 802.16 (e.g. Unsolicited Grant Services, Real-Time Polling Services, etc).

WEIRD is a FP6 integrated European project that is using WiMAX to provide connectivity to users located in remote and impervious areas. WEIRD delivers the WiMAX potential to different user communities. These user communities use monitoring applications to monitor volcanoes, seismic activities or even for fire prevention. WEIRD software allows the configuration of WiMAX equipment to provide a secure and adequate transport of data from/to remote areas, for instance the data acquired by sensors.

In this context, this work evaluates the QoS support in the WiMAX equipment and the cost of dynamically configuring WiMAX channels for the transport of user data with the adequate level of service. The evaluation of QoS in WiMAX determines the overhead of the WEIRD QoS sinalling.

Mobile WiMAX supports mobility at vehicular speeds (120 Km/h), with low packet losses and with tolerable delay and jitter. Since handovers represent an high cost for mobility, IEEE Std 802.21, known as MIH, is being specified to assist the handover processes in order to achieve seamless intertechnology handovers.

Mobile IP procedures rely on link layer information to determine if a mobile node is attached to a new link. Nevertheless, the way link layer data is gathered depends on the mobile IP protocol, as well as in the respective implementations. The MIH standard, standardizes how link layer information can be gathered for different events such as link down and link up.

The evaluation of mobility aspects in WiMAX and IP encompasses the role of the MIH information.

1.2 Objectives and Contributions

The main objective of this work is to contribute to the deployment of Quality of Service and mobility in WiMAX networks.

The main contributions of this thesis can be grouped in three categories, namely, the contributions to the definition of the WEIRD architecture, the evaluation of software and WiMAX equipment and the standardization.
The contributions of the candidate are summarized bellow:

- Contribute to the definition and implementation of an architecture to allow dynamic reservations in WiMAX channels.
- Contribute to the definition and implementation of a mobility architecture for WEIRD.
- Contribute to the MIH integration in the WEIRD mobility architecture.
- Integrate NSIS framework protocols in the WEIRD architecture.
- Test the performance of the NSIS framework protocols.
- Evaluate RedLine WiMAX equipment performance.
- Contribute to the standardization of QoS mapping between WEIRD domains and non-WEIRD domains.
- Contribute to the standardization of QoS mapping between generic domains and WiMAX domains.

The next section describes the structure of this thesis.

1.3 Structure of the Thesis

This thesis is organized in different chapters, which are briefly summarized in the next paragraphs.

Chapter 2 presents an overview of IEEE 802.16 standards, introducing the main concepts behind this family of standards, as well as the WiMAX technology. A comparison with other wireless broadband standards is also performed.

Chapter 3 overviews the MIH standard. Starting with the evolution of the standard and detailing the Media Independent Handover Function (MIHF) including the network model, the function services and the QoS model. The chapter also contains a section about the use of MIH in association with IEEE Std 802.16.

Chapter 4 introduces the WEIRD project and the QoS protocols deployed in the WEIRD architecture. The chapter also includes a summary of the activities performed by the candidate in the project.

Chapter 5 presents the mobility evaluation in WiMAX and IP. The chapter describes the simulation scenarios which include the combination of WiMAX, IP and MIH information.

Chapter 6 presents the QoS evaluation in a WiMAX testbed. The chapter describes the evaluation of QoS support in WiMAX, as well as in WEIRD.

Each chapter ends with a conclusion section, which represent the comments of the candidate, or conclude the results of the experimentation in the evaluation chapters.

The last chapter of the thesis provides the conclusions of the work performed and the next research steps of the candidate.

2
Last Mile Wireless Broadband Access Standard

This chapter presents IEEE Std 802.16 - the last mile wireless broadband access standard. The standard is being pushed to the market with the commercial name of Worldwide Interoperability for Microwave Access (WiMAX). WiMAX is being standardized by an independent organization, the WiMAX Forum (WiMAXForum, 2007d), formed by different vendors.

This chapter reviews the characteristics of the IEEE 802.16 standards in Section 2.1 and the specifications from the WiMAX Forum in Section 2.2. A comparison between WiMAX and other standards and technologies is presented in Section 2.3.

2.1 IEEE Std 802.16

This section overviews the features of IEEE Std 802.16, including an introduction of the supported features for Quality of Service and mobility and also introduces the evolution of the different IEEE 802.16 standards.

2.1.1 IEEE Std 802.16 Overview

IEEE Std 802.16 is a recent Broadband Wireless Access (BWA) standard. The major versions of the standard, IEEE Std 802.16-2004 (IEEE, 2004) and IEEE Std 802.16e (IEEE, 2005a) support different functionalities. Among these, the operation in Line of Sight (LOS) and Non Line of Sight (NLOS) conditions, the support for different Classes of Service (CoS) enabling diverse services, the mobility support and the extended coverage are the most representative. The cell radius depends on different factors such as modulation schemes and frequency channels.

The key features holding the functionalities aforementioned are summarized, as follows:

- **Flexible and extensible with a common MAC**. The common Medium Access Control (MAC) supports different physical technologies and extensions can be added.

- **Modular**. The physical and the MAC layers include support for different profiles and therefore do not have a rigid specification, they include a set of mandatory and optional features.

- **Multiple network topologies**. The Point-to-Point (PtP), the Point-to-Multipoint (PMP) and mesh topologies are supported. However, the PMP mode has attracted more attention.

- **MAC Convergence Sublayer (CS)**. The MAC layer is able to transport different encapsulated protocol payloads such as Asynchronous Transfer Mode (ATM), Internet Protocol (IP) and Ethernet. The common part of the MAC layer is independent of the payload type, as a result the addition of a new Convergence Sublayer does not require a change in the core MAC.

- **Privacy**. The security mechanisms implemented at the MAC layer (encryption and authentication methods) are separated from the core MAC at a modularized security sublayer.

- **Integrated QoS**. The MAC layer supports multiple types of QoS that can be controlled by higher layers with the support for different Classes of Service. Each CoS is optimized for a specific service.

- **TDD and FDD**: Both Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) are supported. The duplexing mechanism depends on the physical profile deployed.

One of the most promising features of IEEE Std 802.16 is the QoS support. Different scheduling services are defined to allow the transport of different kinds of traffic. IEEE Std 802.16-2004 has introduced Unsolicited Grant Service (UGS), Real-Time Polling Service (rtPS), Non-Real Time Polling Service (nrtPS) and Best Effort (BE) Classes of Service. IEEE Std 802.16e adds also the Extended Real-Time Polling Service (ertPS) class. For instance, Voice over IP (VoIP) applications can use a scheduling service optimized for real-time data transport which envision a minimal delay and a sustainable jitter, such as ertPS.

IEEE Std 802.16e has specified amendments to introduce the mobility support, at vehicular speeds (120 Km/h). New features have been specified, for instance the improved power mode operations and the different association types.

The reference model pictured in Figure 2.1 distinguishes the data/control plane and the management plane and splits MAC and physical layer functionalities. The data/control plane is in the scope of IEEE Std 802.16-2004 and IEEE Std 802.16e, while the management plane is being specified on IEEE Std 802.16g (IEEE, 2007b). The data plane comprehends the means by which the information is encapsulated or decapsulated in the MAC layer and modulated or demodulated in the physical layer, while the control plane includes control functions to support configuration and coordination procedures. The management plane is responsible for the management of classification, security mechanisms, QoS, connection setup, among other functionalities.

The MAC layer is divided into three sublayers: The service-specific Convergence Sublayer, the MAC Common Part Sublayer (CPS) and the security sublayer. The Convergence Sublayer-Service Access Point (SAP) allows upper layer protocols, such as IP, to deliver the protocol Service Data Unit (SDU) for classification in the service-specific Convergence Sublayer.

The MAC SAP represents the interface between the service-specific Convergence Sublayer and the MAC Common Part Sublayers. The MAC SDUs containing the mapping of the external network data are delivered to the MAC Common Part Sublayers to be transformed in MAC Protocol Data Unit (PDU) which includes the MAC SDU plus the headers and an optional Check Redundancy Check (CRC) field.

The Physical SAP is the interface between the MAC Common Part Sublayer and the physical layer. IEEE Std 802.16 supports different physical profiles, nevertheless, MAC Common Part Sublayer is expected to support only one specific physical scheme, since the physical SAP is implementation specific.

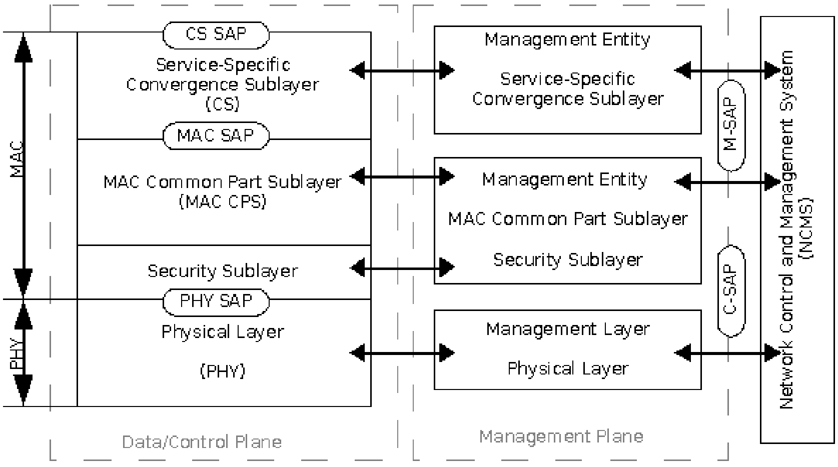

CS SAP
Service-Specific Convergence Sublayer (CS)
MAC SAP
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
PHY SAP
Physical Layer (PHY)
MAC
PHY
Data/Control Plane
Management Entity Service-Specific Convergence Sublayer
Management Entity MAC Common Part Sublayer Security Sublayer
Management Layer Physical Layer
Management Plane
M-SAP
C-SAP
Network Control and Management System (NCMS)

Figure 2.1: IEEE Std 802.16 reference model
Compiled from IEEE Std 802.16-2004 and IEEE Std 802.16g.

The management plane contains different management entities, specified in the IEEE 802.16g (IEEE, 2007b), IEEE 802.16f (IEEE, 2005b) and IEEE 802.16i (IEEE, 2007c) standards. The Management SAP (M-SAP) allows to configure the system to gather statistics, as well as to perform notifications. The M-SAP allows the interaction of the Network Control and Management System (NCMS) with the Management Information Base (MIB) of each 802.16 device.

The Control SAP (C-SAP) allows different functions which may include the notification of handover request by the Mobile Station (MS), the idle mode mobility management, the subscriber session management, and the media independent handover function services.

The management protocol used to interact with the MIB is the Simple Network Management Protocol (SNMP). Both IEEE 802.16f and IEEE 802.16i specifications require a SNMPv2 (Case et al., 1993) support with SNMPv1 (Case et al., 1990) compatibility. The support of SNMPv3 (Case et al., 2002) is optional.

The functional entities depicted in IEEE Std 802.16 architecture are the Subscriber Station (SS) or the MS and the Base Station (BS). SS or MS represent a Customer Premises Equipment (CPE). Either BS and SS have instances of the MAC and physical layers within the respective functions. These entities have a relation of master-slave in the PtP and PMP operation modes, since the SS must obey to all the medium access rules enforced by the BS. The term SS is applied in a fixed context, while the MS is used in a mobile environment, as introduced by IEEE Std 802.16e.

The functions of the BS and SS depend on the operation mode, namely, PMP or mesh. Briefly, the functions of the Base Station are:

- Enforce MAC and physical parameters such as frame size.
- Perform bandwidth allocation for downlink and uplink traffic per SS.
- Perform centralized QoS scheduling based on the QoS parameters configured by the management system and the active bandwidth requests received from the SS.
- Transmit/receive data and control information to/from one or more SSs.
- Provide SS support services like ranging, clock synchronization, power control and handover.

The functions of the Subscriber Station or Mobile Station can be summarized, as follows:

- Identify the BS, acquire physical synchronization, obtain MAC parameters and join the network.
- Establish basic connectivity, setup data and management connections and negotiate parameters as needed.
- Generate bandwidth requests for connections.
- Unless in sleep mode, receive all scheduling and channel information broadcasted and proceed according to the medium access rules provided by the BS.
- Perform specific functions for mobility management, handover and power conservation.

In a 802.16 system, the BS which acts as a central point in the PMP mode, must have additional processing and buffering capabilities to support a reasonable number of Subscriber Stations.

MAC functionalities are specified in a connection-oriented way, thus data communications are associated to transport connections that are linked to service flows containing QoS parameters for PDUs.

Each SS has a unique 48-bit MAC address as defined in IEEE Std 802 (IEEE, 1990). This MAC address is used to identify an SS only during the initial registration or authentication and as part of some management messages. IEEE Std 802.16 uses 16 bit Connection Identifier (CID) to identify all the information exchanged between the BS and SS. Therefore, IEEE Std 802.16 does not rely on MAC addresses to identify source and destination addresses, as employed by other IEEE 802 standards (e.g. IEEE Std 802.3, IEEE Std 802.11).

2.1.2 IEEE 802.16 Service-Specific Convergence Sublayer

Different service-specific Convergence Sublayers are specified in the standard. The ATM Convergence Sublayer and the Packet Convergence Sublayer represent the main types of convergence sublayers defined in IEEE Std 802.16d and IEEE Std 802.16e. Additionally, IEEE Std 802.16g introduces the Generic Packet Convergence Sublayer (GPCS). Multiple Convergence Sublayers can coexist simultaneously and share the same MAC Common Part Sublayer if needed.

The ATM Convergence Sublayer is a logical interface that accepts ATM cells from the upper layers performing classification, and delivers PDUs to the appropriate MAC SAP.

The Packet Convergence Sublayer is able to transport all packet-based protocols such as Internet Protocol (IP) (DARPA, 1981), Point-to-Point Protocol (PPP) (Simpson, 1994), IEEE Std 802.3/Ethernet and IEEE 802.1D, known as Virtual Local Area Network (VLAN).

The GPCS is an upper layer protocol independent packet Convergence Sublayer that supports multiple packet-based protocols.

The service flows support per-connection services, such as different QoS levels and are mapped to a unique CID. The association of higher-layer SDUs to the SIDs and the Service Flow Identifier (SFID) is performed by the Convergence Sublayers.

Convergence Sublayers perform different functions, depending whether it is transmitting or receiving. The Convergence Sublayer functions at the transmitter side are the following:

- Receive the payload protocol PDU from a higher layer protocol.
- Map the payload protocol PDU to the appropriate MAC service flow.
- Compress payload protocol headers.
- Deliver the processed packet to the MAC for transmission.

The Convergence Sublayer functions at the receiver side, are the following:

- Receive the MAC SDU.
- Restore the compressed protocol headers.
- Deliver the payload protocol PDU to the higher layer.

The Convergence Sublayers perform the classification based on the sets of the matching criteria. Through the classification process the MAC SDU is associated with a connection and consequently with the respective service flow characteristics of the connection. If the matching criteria applied to the protocol PDUs entering the 802.16 network are successful, the Convergence Sublayer delivers the MAC SDUs to the MAC SAP on the connection defined by the CID.

The classifiers consist on the following elements: First, a protocol matching criteria; Second, a classifier priority whih is used to distinguish and ordering the several classifiers; and Finally, a reference to CID and PHS rules. There are two types of classifiers, namely downlink and uplink, according to the direction of the traffic. At the BS the downlink classifiers are applied to packets being transmitted to the SS while the uplink classifiers are applied to packets being received from the SS. Figure 2.2 demonstrates the classification and the CID mapping from the Subscriber Station to the Base Station.

The Payload Header Suppression (PHS) allows to suppress repetitive portions of payload headers by the sender and to restore them at the receiving entity. Such compression optimizes the air resources, nonetheless the use of PHS is optional and is negotiated between the BS and the SS when establishing a connection. The PHS rules are managed by different management messages. The Dynamic Service Addition (DSA) and the Dynamic Service Change (DSC) messages allow the creation of PHS rules. The PHS rules may be deleted by the DSC and the Dynamic Service Deletion (DSD) messages.

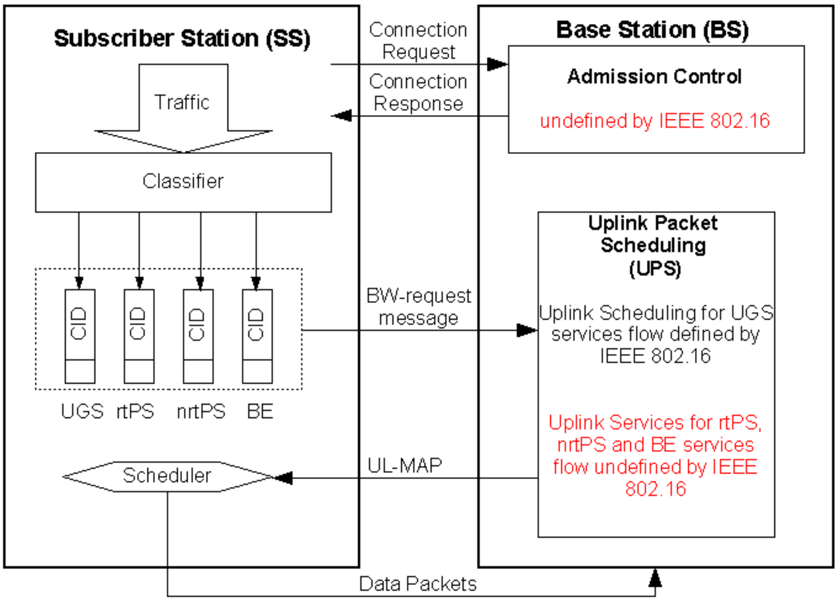


Figure 2.2: IEEE 802.16 QoS architecture
Source Cho et al. (2005).

Packet Convergence Sublayer

The Packet CS is able to transport data of any packet protocol, nevertheless the standard only specifies support for Ethernet and IP. For instance, the standard does not address the support for Multiprotocol Label Switching (MPLS) (Rosen et al., 2001). The Packet Convergence Sublayer includes support for the following packet protocols:

1. **IEEE Std 802.3/Ethernet**. The Ethernet CS, corresponding to IEEE Std 802.3/Ethernet-specific part, includes the source and destination MAC addresses and the Ethertype/SAP fields for the classification process. The Ethernet Convergence Sublayer allows the operation of IP over IEEE 802.3/Ethernet.

2. **IEEE Std 802.1Q/VLAN**. The IEEE 802.1Q classifiers include the MAC addresses parameters, as well as the priority range, defined in IEEE Std 802.1D, and the VLAN ID fields. The IEEE 802.1Q CS allows the operation of IP over IEEE Std 802.1Q.

3. **IP protocol**. The IP specific part, known as IP Convergence Sublayer, al-

lows the classification of IPv4 and IPv6 packets. The IP classifiers are applied to the IP fields defined in RFC 790 (Postel, 1981), in RFC 2460 (Deering & Hinden, 1998) and transport protocols fields. The IP classification parameters include IP source address, IP destination address, IP Type of Service (ToS)/Differentiated Services Code Point (DSCP), IP protocol , IPv6 flow label, source and destination ports defined, for instance, in Transport Control Protocol (TCP) and User Datagram Protocol (UDP) protocols.

The IP Convergence Sublayer is preferable in a mobile context due to the Mobile IP protocols.

Generic Packet Convergence Sublayer

The Generic Packet Convergence Sublayer (GPCS) provides a Convergence Sublayer SAP that is protocol agnostic and therefore does not redefine or replace other convergence sublayers. The upper layers perform the parsing and the classification according to their needs, whilst GPCS only performs the mapping to the 802.16 MAC connections. The GPCS allows the multiplexing of multiple layer protocols types (IPv4, IPv6, Ethernet) over the same connection. Thus, the BS can support GPCS and can communicate with a SS that does not support it. For instance, the BS may use the GPCS for classification while the SS can use the Ethernet specific part or the IP specific part of the packet CS. The negotiation of the supported CS is performed during the connection setup, using the DSx (DSA, DSD, DSC) messages exchange.

The GPCS SAP parameters for the different data path primitives are the following:

- **SFID**. Unique identifier to describe a unidirectional service flow for a Mobile Station. The GPCS performs the mapping to a MAC connection ID based on the SFID and the MAC address of the Mobile Station.
- **MS MAC address**. A 48bit unique identifier of the Mobile Station.
- **Data**. The data delivered by upper layers.
- **Length**. Number of bytes in the data field.

The GPCS defines primitives to allow upper layers to send data and receive data from the GPCS.

2.1.3 IEEE Std 802.16 MAC Common Part Sublayer

This subsection presents the details of the MAC Common Part Sublayer, the core sublayer of IEEE Std 802.16 MAC layer.

The MAC Common Part Sublayer includes the necessary functionalities to control the medium access. The downlink from the BS to the SS operates on a PMP basis, since the downlink data messages are broadcasted, except if the downlink MAP is addressed to a specific SS. In this context, all the SSs listen to the downlink subframe and identify the traffic addressed to them based on CIDs. The SS requests the right to transmit, as a result the uplink to the BS is shared on a demand basis.

In the mesh mode the traffic can be routed via the Subscriber Station and these can communicate directly with others, for instance, there is not a central BS on which on the communications rely as in the PMP mode. In the mesh mode, QoS is provisioned over the links on a message-by-message basis, since there is no service or QoS parameters associated with a link. Thus, the ingress node has the responsibility to perform traffic classification and flow regulation.

The connections, identified by 16-bit CIDs, are unidirectional and different types of CIDs are specified in IEEE Std 802.16e, as follows:

- **Initial ranging CID**. This CID is used to perform the initial ranging, since there is no unique CID available at this moment. If there is a Basic CID, the initial ranging CID is not employed. The initial ranging is reserved in both downlink and uplink.

- **Basic CID**. This CID is assigned in the ranging process, and is used to exchange delay-intolerant and time-critical MAC management messages between the SS and the BS (e.g. RNG-REQ message). The basic CID also identifies the SS in per-SS functions. The basic CID is assigned to both the downlink and uplink connections.

- **Primary Management CID**. CID assigned during the ranging process to both downlink and uplink connections. This CID is used for delay-tolerant MAC management messages between the BS and the SS, for instance, REG-REQ messages.

- **Secondary Management CID**. This CID is applied to transport higher layer management messages such as SNMP, Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP). This CID is

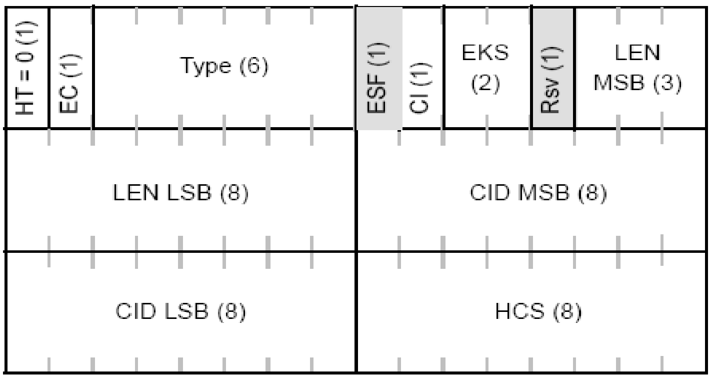


Figure 2.3: Generic IEEE 802.16 MAC header
Source IEEE Std 802.16e.

assigned to the Subscriber Station if it is a "managed SS" (controlled by the network).

- **Transport CID**. Transports the user information. This CID is assigned after ranging and authentication.
- **Broadcast CID**. CID used by the BS to broadcast MAC management information to all the SSs in the downlink. The broadcast CID is not used in the uplink.
- **Multicast CIDs**. CID utilised for the downlink multicast service.

The MAC PDU contains a MAC header, with an optional payload (signalling messages may not contain any payload) and an optional CRC field. The MAC header can have different types, namely, the generic MAC header which corresponds to the downlink MAC header and uplink MAC header and the bandwidth request header, encloses different fields, which are represented in Figure 2.3. IEEE Std 802.16 defines subheaders to extend the functionality of the generic MAC header. The fragmentation subheader is used to transport encapsulated MAC PDUs fragments in a connection. The packing subheader allows the transmission of multiple SDU fragments in a single MAC PDU. Other subheaders are defined, such as mesh subheader which may carry mesh node IDs.

Different MAC management messages are specified for control and management operations. A subset of the MAC management messages defined in IEEE Std 802.16e is presented in Table 2.1.3.

Message Name	Message Description	Connection
UCD	Uplink Channel Descriptor	Fragmentable Broadcast
DCD	Downlink Channel Descriptor	Fragmentable Broadcast
DL-MAP	Downlink Access Definition	Broadcast
UL-MAP	Uplink Access Definition	Broadcast
RNG-REQ	Ranging Request	Initial Ranging or Basic
RNG-RSP	Ranging Response	Initial Ranging or Basic
REG-REQ	Registration Request	Primary Management
REG-RSP	Registration Response	Primary Management
DSx-REQ	Dynamic Service **A**ddition/ **C**hange/ **D**eletion Request	Primary Management
DSx-RSP	Dynamic Service **A**ddition/ **C**hange/ **D**eletion Response	Primary Management
DSx-ACK	Dynamic Service **A**ddition/ **C**hange/ **D**eletion Acknowledge	Primary Management
DSx-RVD	Dynamic Service **A**ddition/ **C**hange/ **D**eletion Received Message	Primary Management
MOB_NBR-ADV	Neighbour advertisement message	Broadcast, primary management
MOB_BSHO-REQ	BS Handover request message	Basic
MOB_MSHO-REQ	MS Handover request message	Basic
MOB_BSHO-RSP	BS Handover response message	Basic

Table 2.1: IEEE 802.16e MAC management messages

The messages are transported on the basic, broadcast and initial ranging connections and never in the transport connections.

2.1.4 IEEE Std 802.16 Network Entry Process

The network entry process allows the Subscriber Station to get connectivity. This process, accomplished by a set of MAC management messages, is performed after a SS/MS power-up or due to an handover process.

The network entry encloses different phases, some optional and others mandatory, which are as follows:

1. **Synchronization with the BS and scan for downlink channel**. The SS performs scan of possible channels of the downlink frequency band operation and performs synchronization on the reception of a DL-MAP message. The DCD messages are used to keep the synchronization active.

2. **Obtain transmit parameters**. The transmit parameters for the uplink chan-

nel are obtained from the UCD messages transmitted by the BS. The uplink parameters can be obtained from the UL-MAP messages, for instance the time slots that the SS can use to transmit.

3. **Perform Ranging**. The ranging represents a process which allows a SS to acquire the correct timing offset and perform power adjustments for an optimal reception at the BS. In the initial ranging, the SS has allocated its basic and primary management CIDs.

4. **Negotiate basic capabilities**. Through the SS basic capability negotiation, the SS informs the BS about the optional functionalities supported, and the BS informs the SS about the options that is allowed to use. This negotiation is done through the SBC-REQ and SBC-RSP messages. Negotiated parameters include MAC and PHY features such as maximum transmit power and modulation schemes.

5. **Authorize SS and perform key exchange**. This is an optional phase in which the SS confirms its entity to the BS. An authorization protocol is used, based on the Privacy Key Management (PKM) messages , to establish the Security Association (SA) between the BS and the SS to secure communications.

6. **Perform Registration**. The SS indicates if it is part of a managed network. If the SS is a managed SS, than a secondary management connection is set, and the IP version and the respective QoS parameters of this connection can be negotiated.

7. **Establish connectivity**. This optional phase uses the DHCP mechanisms to obtain the necessary IP parameters in order to have connectivity. If the SS is using IPv4 than it can use the DHCPv4 mechanisms (Droms, 1997), otherwise, when using IPv6 the SS can use DHCPv6 protocol (Droms et al., 2003) or IPv6 Stateless Address Autoconfiguration (Thomson & Narten, 1998). The IP connectivity mechanisms are transported over the secondary management connections.

8. **Establish time of day**. This optional phase allows the BS and the SS to synchronize the current date and time. The time protocol defined in RFC 868 (Postel & Harrenstien, 1983) is used and transported over the secondary management connections.

9. **Transfer optional parameters**. In this optional phase the SS may download the SS configuration file using TFTP on the secondary management connection.

10. **Set up connections**. The DSA-REQ and DSA-RSP messages are used to set up connections for the preprovisioned service flows belonging to the SS.

In the Mesh mode, the network entry has different phases. First, the SS starts by scanning for an active network and establish a first synchronization with the network. In a second phase, the SS obtains the network parameters for a correct synchronization and builds a list of neighbours from the acquired information. The SS acting as the candidate node, selects the sponsoring node to perform negotiation of the basic capabilities and authentication. In a third phase, and after electing the sponsoring node, the SS opens the sponsor channel in order to establish a temporary schedule in the sponsoring node to allow the candidate node to perform initialization. Figure 2.4 exhibits the network entry process in the PMP mode.

The connection setup can be processed in different modes, namely, it can be BS-initiated or SS-initiated, the last is considered optional in IEEE Std 802.16.

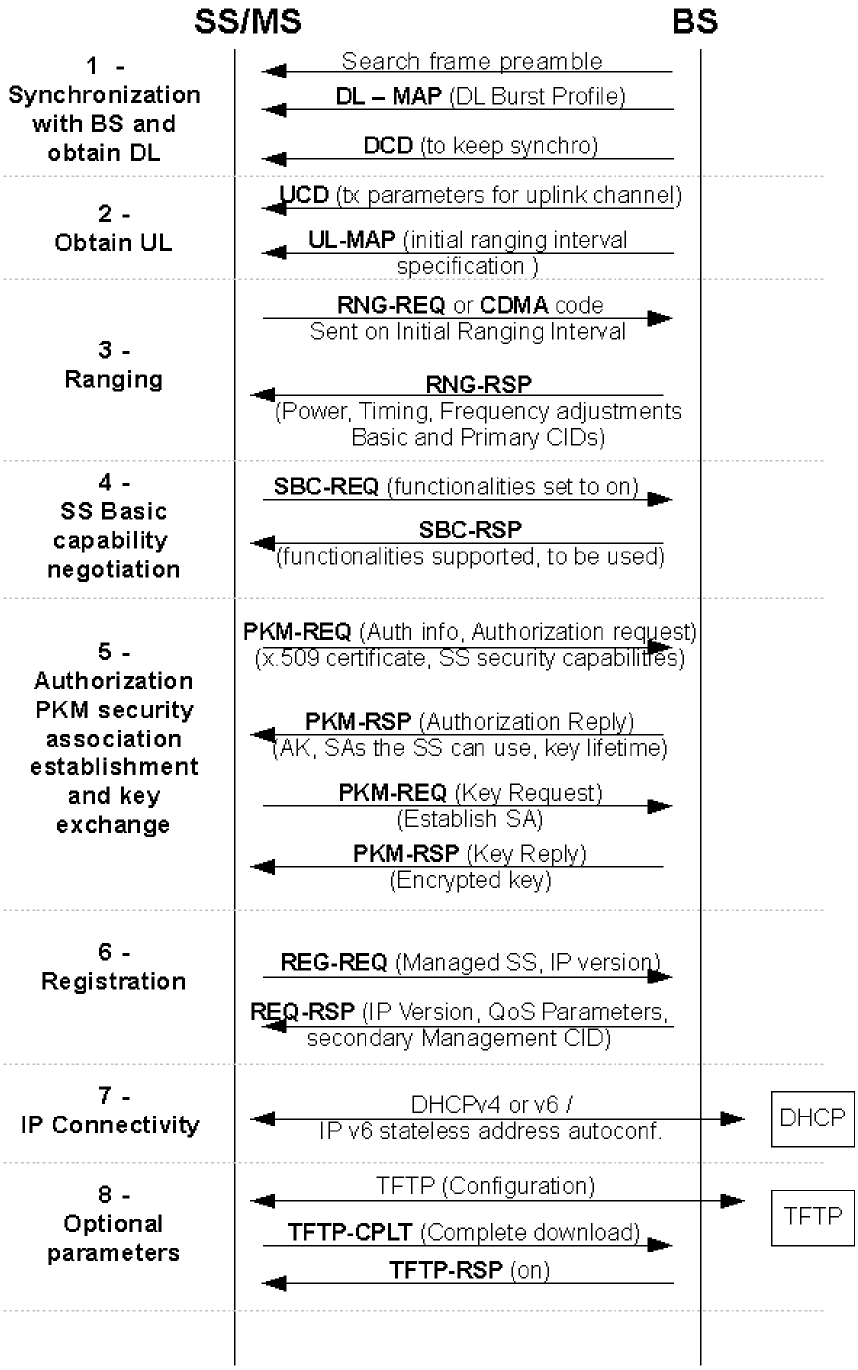

SS/MS
BS
1 - Synchronization with BS and obtain DL
Search frame preamble
DL – MAP (DL Burst Profile)
DCD (to keep synchro)
2 - Obtain UL
UCD (tx parameters for uplink channel)
UL-MAP (initial ranging interval specification)
3 - Ranging
RNG-REQ or CDMA code Sent on Initial Ranging Interval
RNG-RSP (Power, Timing, Frequency adjustments Basic and Primary CIDs)
4 - SS Basic capability negotiation
SBC-REQ (functionalities set to on)
SBC-RSP (functionalities supported, to be used)
5 - Authorization PKM security association establishment and key exchange
PKM-REQ (Auth info, Authorization request) (x.509 certificate, SS security capabilities)
PKM-RSP (Authorization Reply) (AK, SAs the SS can use, key lifetime)
PKM-REQ (Key Request) (Establish SA)
PKM-RSP (Key Reply) (Encrypted key)
6 - Registration
REG-REQ (Managed SS, IP version)
REQ-RSP (IP Version, QoS Parameters, secondary Management CID)
7 - IP Connectivity
DHCPv4 or v6 / IP v6 stateless address autoconf.
DHCP
8 - Optional parameters
TFTP (Configuration)
TFTP
TFTP-CPLT (Complete download)
TFTP-RSP (on)

Figure 2.4: IEEE 802.16 Network entry process
Source IEEE Std 802.16e.

2.1.5 IEEE Std 802.16 Quality of Service Support

IEEE Std 802.16e object model demonstrates the different relations of the main entities focused on the standard. Such relations and entities are depicted in Figure 2.5.

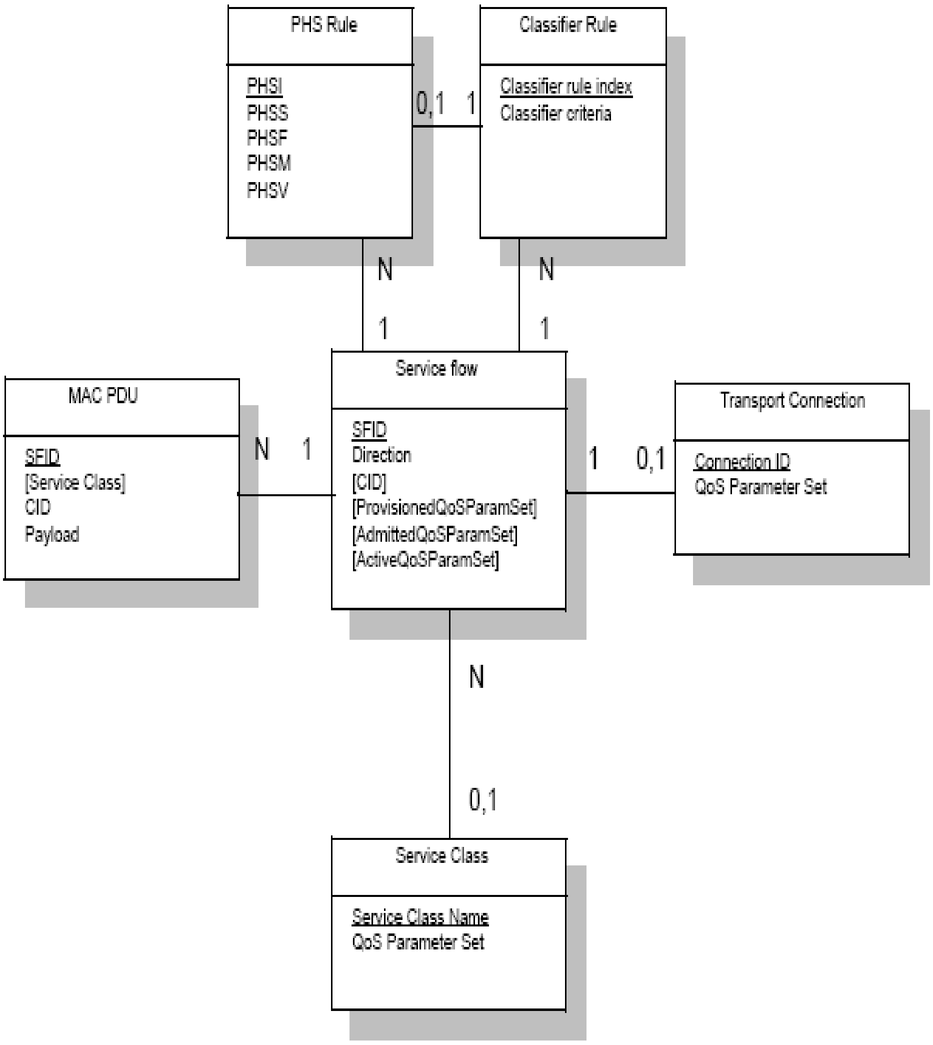


Figure 2.5: Object model of IEEE Std 802.16e
Source IEEE Std 802.16e.

The service flow is a unidirectional flow of packets with a particular set of QoS parameters and is identified by a SFID. The different QoS parameters include traffic priority, maximum sustained traffic rate, maximum traffic burst, minimum reserved traffic rate, minimum tolerable traffic rate, vendor specific QoS parameters, tolerated jitter, maximum latency and request/transmission policy.

The different type of service flows are as follows:

- **Provisioned**. The service flow is provisioned by means not specified in the standard. For instance, it can be specified by the network management system. In this case, the *AdmittedQoSParamSet* and *ActiveQoSParamSet* are both null.

- **Admitted**. This type of service flow has resources reserved by the BS for its *AdmittedQoSParamSet*, but these parameters are not active (i.e., the *ActiveQoSParamSet* is null). Admitted Service Flows may have been provisioned or may have been signalled by other mechanism.

- **Active**. This type of service flow has resources committed by the BS for its *ActiveQoSParamSet*. This service flow may forward packets.

As stated before, the service flows can be BS-initiated or SS-initiated. Figure 2.6 illustrates MAC management messages when service flows are initiated by the MS/SS. In this case the BS sends a DSx-RVD to acknowledge the reception of a DSA-REQ message, since the optional DSx-RVD message allows a faster acknowledging when compared to the DSA-RSP message.

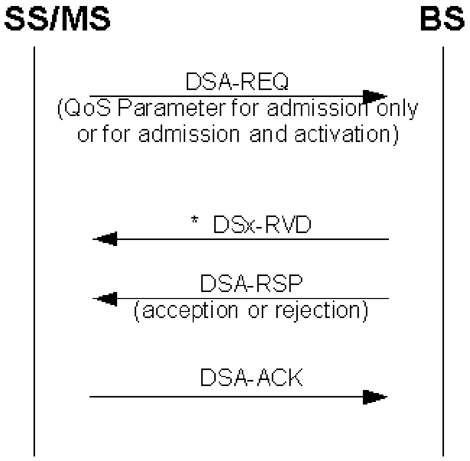

SS/MS
BS
DSA-REQ
(QoS Parameter for admission only
or for admission and activation)
* DSx-RVD
DSA-RSP
(acception or rejection)
DSA-ACK

Figure 2.6: Service flow initiated by the Subscriber Station
Source IEEE Std 802.16-2004.

The BSs are responsible for the one-to-one mapping between admitted and active service flows (32-bit SFID) and the transport connections (16-bit CID).

IEEE Std 802.16-2004 and IEEE Std 802.16e define different scheduling services to support a wide variety of applications. The global service class name supports the configuration of specific QoS parameters by an operator in a given network topology. Table 2.2 depicts the characteristics of the different scheduling services. The ertPS scheduling service class and the global service class are only specified in IEEE Std 802.16e.

Name	**QoS Parameters**	**Applications**
UGS Unsolicited Grant Service	Maximum sustained rate, maximum latency, tolerated jitter and request/transmission policy	Fixed-size data packets transmitted at periodic intervals, Constant Bit Rate (CBR), such as VoIP.
rtPS Real-Time Polling Service	Minimum reserved rate, maximum sustained rate, maximum latency, traffic priority and request/transmission policy	Real-time data streams with variable-sized data packets issued at periodic intervals. For instance, streaming Moving Pictures Experts Group (MPEG) video with Variable Bit Rate (VBR)
ertPS Extended Real-Time Polling Service	Minimum reserved rate, maximum sustained rate, maximum latency and request/transmission policy	Real-time services generating variable size data packets on a periodic basis, such as VoIP with silence suppression
nrtPS Non-Real-Time Polling Service	Minimum reserved rate, maximum sustained rate, traffic priority and request/transmission policy	Delay-tolerant data streams consisting of variable-sized data packets requiring a minimum data rate. For instance, the File Transfer Protocol (FTP)
BE Best-Effort	Maximum sustained rate and request/transmission policy	No QoS guarantees. For instance, data transfer, Web Browsing and others

Table 2.2: The IEEE Std 802.16 scheduling services

Since the QoS model specified in the standard focused on the PMP mode, an algorithm to support QoS in the mesh mode, with low delay and low packet drop rates has been proposed (Liu et al., 2005). The algorithm relies on different fields of CID, such as: probability of a packet being dropped when congestion occurs and reliability of a packet, if the packet is retransmitted on an error situation.

Cho et al. (2005) present the main issues of the IEEE Std 802.16 QoS architecture, being the most relevant the following:

- **No definition of the admission control process**. The standard only defines the connection signalling, the admission control process is not defined to accept or reject new connections.
- **No definition of the uplink scheduler**. The mechanisms that determine the Information Elements in the UL-MAP are not defined, only the UGS scheduling service class is defined.
- **The SS MAC has no scheduler**. Only the BS MAC defines a scheduler. Cicconetti et al. (2006) refer that a SS MAC scheduler could infer more precisely the grant of its connections. The bandwidth requests are done per connection but granted by the BS to the SS as a whole.

The QoS support of IEEE Std 802.16 is an improvement when compared to current wireless standards, because Quality of Service is supported natively and not as an extension and also supports demanding applications, such as real-time applications.

2.1.6 IEEE Std 802.16 Mobility Support

IEEE Std 802.16e introduces power-saving specifications and handover procedures to enable mobility.

The power-saving features are deeply associated with mobility, since mobile devices must operate for long periods without having to recharge. The different power-saving modes are as follows:

- **Sleep mode**. State in which the MS effectively turns itself off and becomes unavailable for predetermined periods. Such periods of absence are negotiated with the serving BS. The support of this operation mode is required by the standard.
- **Idle mode**. With this mechanism the MS can completely turn off and become periodically available for downlink broadcast messages without being registered with any BS. When compared to the sleep mode, the idle mode is more power conservative. However the support of the idle mode is optional.

The sleep mode has three different power saving classes, these are respectively, power saving class type I, type II and type III. The power saving classes describe the context kept by the BS and they are characterized by different parameters, procedures of activation/deactivation and policies of MS availability for data transmission. Power saving class type I is recommended for best-effort and non real-time traffic, while the power saving class type II is recommended for UGS service, and the power saving class type III is recommended for multicast traffic or management traffic.

The handover procedures introduced in IEEE Std 802.16e can be used in the following situations:

- MS moves and needs to change the BS to which it is connected.
- MS can be served with higher QoS at another BS.

Three handover methods are supported in IEEE Std 802.16e. The mandatory handover mode is the Hard Handover (HHO) mode. The HHO mode implies an abrupt transfer of connection from one BS to another. The handover decisions are made by the BS, MS or by a network entity, and the determination of handover is based on the measurements reported by the MS using the MOB_SCN-REP management message. The MS performs scans during the scanning intervals allocated by the BS. The MS uses the MOB_SCN-REQ message to request for allocation of scanning intervals. Afterwards, the BS indicates the allocation result in the MOB_SCN-RSP messages.

The identity of the neighbouring BSs and the frequencies that a MS can use to perform scan are provided in the MOB_NBR-ADV messages, that are broadcasted. During the scanning intervals, the MS is also allowed to optionally perform initial ranging and to associate with one or more neighbouring BSs. Once a handover decision is made, the MS begins synchronization with the downlink transmission of the target BS, performs ranging if it was not done while scanning, and then terminates the connection with the previous BS.

The optional handover modes are the Fast Base Station Switching (FBSS) and the Macro Diversity Handover (MDHO). In these two methods, the MS maintains a valid connection with more than one BS simultaneously. In the FBSS case, the MS maintains a list of the BSs involved, called the active set. The MS continuously monitors the active set, does ranging, and maintains a valid connection ID with each of them. MS communicates only with one BS, called the anchor BS. In the MDHO case, the MS communicates on the downlink and uplink with all the base stations in the active set, called the diversity set. Both the FBSS and MDHO offer better performance when compared to the hard handover mode, but they require synchronization and share of network entry-related information.

Three levels of association are possible during the scanning process.

1. **Association Level 0** *(scan/association without coordination)*. The MS performs contention-based ranging without coordination from the network.

2. **Association Level 1** *(scan/association with coordination)*. The serving BS coordinates the association procedure with the neighbour BS. The MS performs unicast ranging since a ranging code and a transmission interval of each neighbour BS is provided by the network to the MS.

3. **Association Level 2** *(network assisted association with reporting)*. Same as association level 1 but the MS receives the physical offsets of each neighbour scanned from the serving BS in a MOB_ASC_REPORT message which aggregates all the ranging related information, which was sent by the scanned neighbour BS over the backbone.

The handover process, as specified by the hard handover mode, consists on the following stages:

1. **Cell reselection**. The MS performs scanning and association with one or more neighbouring BSs.

2. **Handover decision and initiation**. When the handover decision is taken by the MS, it sends a MOB_MSHO-REQ message to the BS, indicating one or more BSs as handover targets. The BS then sends a MOB_BSHO-RSP message indicating the target BSs to be used for this handover process. The MS sends a MOB_MSHO-IND indicating which of the BSs indicated in MOB_BSHO-RSP will be used for handover.

3. **Synchronization to the target BS**. The MS synchronizes with the downlink transmission of the BS handover target in order to decode the DL-MAP, UL-MAP, DCD and UCD messages to get information about the ranging channel.

4. **Ranging with the target BS**. The MS performs initial ranging to synchronize its uplink transmission with the BS. The MS uses the RNG-REQ message to perform ranging and processes the responses sent by the BS with the RNG-RSP messages. If the association was performed during the cell reselection stage, this stage can be shortened.

5. **Termination of context with the serving BS**. The MS is already connected with the target BS and decides to terminate the connections with the serving BS. The MOB_HO-IND message is sent to the serving BS triggering the activation of timers to expire the MAC state machines and discard MAC PDUs belonging to the MS.

The handover process can be cancelled at any stage, if the MOB_HO-IND message has not been sent.

2.1.7 IEEE Std 802.16 Evolution

IEEE Std 802.16 or the Wireless Metropolitan Area Network (WirelessMAN) standard has evolved through different versions, specified by the IEEE 802.16 Working Group (IEEE, 2007a). Carl Eklund et al. (Eklund et al., 2006) provide a brief history of the IEEE Std 802.16 evolution which is depicted in Table 2.3[1].

IEEE 802.16 Working Group has specified different conformance test standards. The 802.16/Conformance0x documents specify conformance tests to improve interoperability and conformity which can not be assured by the standards alone. IEEE Std 802.16/Conformance01-2003, IEEE Std 802.16/Conformance02-2003, IEEE Std 802.16/Conformance03-2003 and IEEE Std Conformance04-2006 represent the different versions of conformance tests specified so far.

IEEE 802.16 Working Group also provides guidelines to assist operators implementing systems in licensed bands (co-channel and adjacent channel interference). IEEE Std 802.16.2-2001 superceded by IEEE Std 802.16.2-2004, provides recommendations for the design and coordinated deployment of Fixed Broadband Wireless Access (FBWA) systems. The recommendations intend to control the interference and facilitate the coexistence among systems.

The next section presents WiMAX which is based on the IEEE 802.16-2004 and IEEE 802.16e standards.

[1] Status at 2007/11/12. Reference http://wirelessman.org/published.html

Version	Year	Specification	Status
802.16-2001	1999 - 2001	10GHz - 66GHz MAC based on Time Division Multiplexing (TDM)/Time Division Multiple Access (TDMA) and supportting TDD and FDD. The physical layer, *WirelessMAN-SC*, is designed for LOS conditions.	Superceded
802.16c	2002	Designed to allow an easier interoperability since the prior version was complex.	Superceded
802.16a	2000 - 2003	Designed for licensed and license-exempt bands. NLOS support in the physical layer and supporting different physical schemes: *WirelessMAN-OFDM*; *WirelessMAN-OFDMA*.	Superceded
802.16d	2004-2005	Also known as 802.16-2004. Intended to specify profiles for lower frequency bands allowing the operation of indoor CPE. 802.16-2004 made obsolete prior versions.	Active
802.16e	2005	Expand the 802.16 fixed access system into a combined fixed/mobile system allowing a single BS to support both fixed and mobile terminals in licensed bands below 6GHz.	Active
802.16f	2005	MIB specification for fixed systems.	Active
802.16g	2005 -	Defines management plane procedures and services for the management of 802.16 devices.	Under Development
802.16h	2006 -	Defines improved coexistence mechanisms for license-exempt operations for the 802.16-2004.	Under Development
802.16i	2006 -	MIB specification for mobile systems.	Under Development
802.16j	2006 -	Provides the specification for multihop relay stations in order to enhance coverage and system capacity of 802.16 networks.	Pre-Draft Stage
802.16m	2006 -	Provide performance improvements necessary to support future advanced services and applications (described in ITU-R M.2072).	Pre-Draft Stage
802.16k	2006	Provides an amendment to the IEEE 802.1D to support bridging of the IEEE 802.16 medium access control.	Approved

Table 2.3: IEEE 802.16 standard versions

2.2 WIMAX

WiMAX is a technology based on the IEEE 802.16 standards, which aims at providing wireless access over long distances. The WiMAX Forum (WiMAXForum, 2007d) is the entity responsible for the WiMAX specification.

2.2.1 WiMAX Overview

WiMAX is a standard base technology enabling the delivery of the last mile wireless access broadband access as an alternative to cable and Digital Subscriber Line (DSL). WiMAX provides fixed, nomadic, portable and mobile wireless broadband connectivity without the need for direct LOS with a BS. On fixed and portable network deployments, the cell radius can vary between 3 to 10 km and the WiMAX Forum certified equipments can deliver a capacity of 40 Mbps per channel. For mobile network deployments, the cell radius of 3 km can deliver a capacity of 15 Mbps.

The goal of the WiMAX Forum is to promote and certify the compability and interoperability of equipments that conform to IEEE Std 802.16 and the ETSI HiperMAN standards. WiMAX Forum also collaborates with other industry groups to enhance WiMAX features. For instance, a connection with the Wi-Fi Alliance allows the seamless handovers between multiple wireless standards. A connection with 3GPP allows the implementation of IP Multimedia Services (IMS) services in WiMAX networks.

WiMAX is getting popularity, mainly due to the key features supported by the standard. WiMAX interoperability equipment is one of the key strengths of WiMAX. The key features of WiMAX can be summarized as:

- **Flexible Architecture**. Several system architectures are supported, PtP, PMP and mesh. The PtP configuration allows to cover longer distances.
- **High Security**. Different encryption standards are supported. Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) assure the privacy between SS and BS.
- **QoS support**. WiMAX supports different classes of service, each one optimized for a distinct application.
- **Quick deployment**: WiMAX can be deployed in unlicensed bands. As soon as the antennas and the equipment are powered the system is ready to be used.

- **Multi-Lever Service**. Different Service Level Agreement (SLA) can be defined between the network provider and the user.

- **Lower cost**. When compared to the cellular systems, the deployment costs are lower.

- **Wider coverage**. IEEE Std 802.16 is optimized for NLOS conditions. With the NLOS support, wide areas are covered, less BSs are needed as the Radio Frequency planning is simplified and the deployment is facilitated.

- **Higher capacity**. WiMAX allows high throughput rates. The adaptative modulation schemes increase the throughput or reliability.

- **Support fixed and mobile access**. The technology supports, at the same time, fixed and mobile access. The mobility mechanisms include support for idle/sleep modes and handovers at the speeds of 120 km/h.

- **Complete Network Management System**. The network management system is specified to allow the management of the QoS profiles.

WiMAX is designed to address a wide range of applications, such as VoIP, Video conference and streaming media applications. WiMAX can be exploited in different usage scenarios according to the applications. For instance, the quick deployment of WiMAX allows its employment in a military battlefield, while its QoS support allows the deployment of WiMAX for Wireless Service Providers access networks.

The different versions of WiMAX are (WiMAXForum, 2005):

- **Fixed WiMAX**: Also known as 802.16-2004 WiMAX. It is based on IEEE Std 802.16-2004 and on ETSI HiperMAN. Supports fixed and nomadic access in LOS and NLOS conditions.

- **Mobile WiMAX**: Also known as 802.16e WiMAX. It is based on IEEE Std 802.16e and adds support for mobile wireless acccess.

WiMAX Forum conduces different groups of tests, known as plugfest, to determine the interoperability of equipments. The interoperability can be in two flavors, as cited in the second mobile WiMAX Plugfest white paper (WiMAXForum, 2007a):

- **Basic interoperability**. A BS and a MS must interoperate with each other.

- **Advanced interoperability**. A BS and one or more MSs interoperate supporting advanced test scenarios (power control, sleep mode, handover, etc).

The plugfest is conducted with the equipments of different vendors and has different goals:

- Identify misunderstood parts of the standards.
- Identify interoperability problems.
- Prepare the products of a vendor to a certification testing.

The plugfest events are managed by the WiMAX Forum Certification Working Group. This Working Group defines the test scenarios, the system under test, which is formed by a BS and one or more SS/MSs. In the Plugfest, the QoS testing is also assessed in order to emulate the real final user experience (transmitting data according to the QoS parameters defined and checking that the QoS of a service flow is not affected by other best effort data transmissions).

2.2.2 WiMAX Network Architecture

The WiMAX Forum Network Working Group has defined the WiMAX network reference model in the documents (WiMAXForum, 2007b,c). The network reference model is depicted in Figure 2.7.

The WiMAX network architecture encloses different entities. The Network Access Provider is a business entity that provides WiMAX radio resources to one or more WiMAX Network Service Providers and controls the Access Service Network (ASN). The Network Service Provider is a business entity that provides IP connectivity and WiMAX services to the WiMAX subscribers and manages the Connectivity Service Network (CSN).

The Access Service Network includes as network elements the Base Station and the ASN Gateway (ASN-GW), providing network access to the Mobile Stations. The ASN contains the network functions needed to provide radio access to a WiMAX subscriber. These functions include:

- WiMAX Layer 2 connectivity with the WiMAX MS.

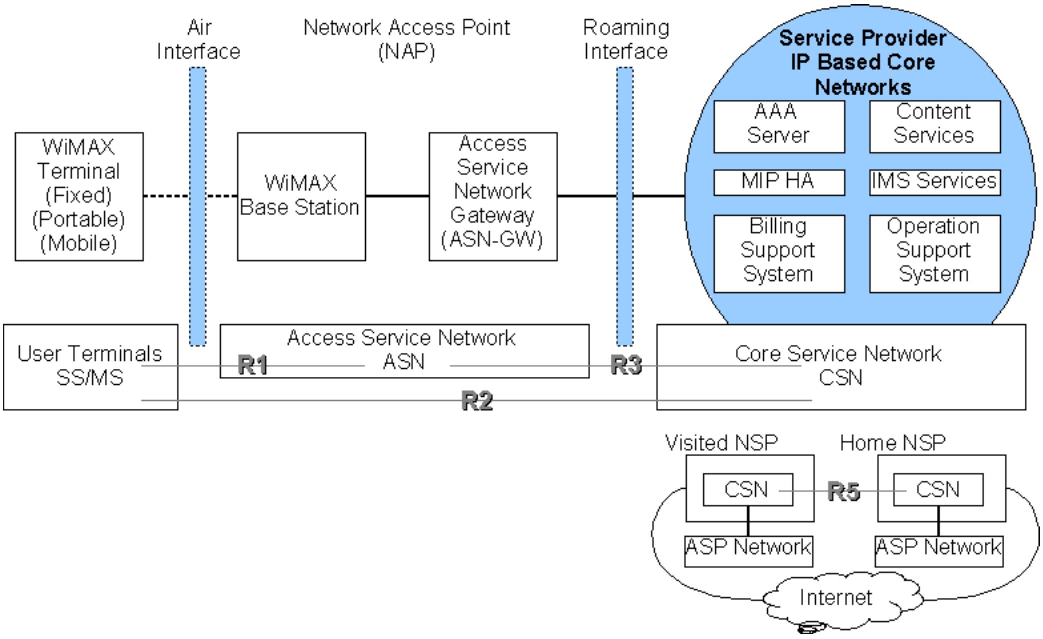


Figure 2.7: WiMAX network architecture
Compiled from the WiMAX network reference model.

- Transfer of Authentication, Authorization and Accounting (AAA) messages to the home network service provider of the WiMAX subscriber for authentication, authorization and session accounting for subscriber sessions.
- Network discovery.
- Relay functions to establish layer 3 connectivity.
- Radio resource management.
- ASN anchored mobility.
- CSN anchored mobility.
- Paging.
- ASN-CSN tunnelling.

The communication between the different elements of the network architecture is performed through the reference points, that are defined for interoperability. The reference points are the following:

- **R1**: This reference point includes protocols and procedures between MS and ASN, such MAC and physical specifications are specified in the IEEE 802.16-2004, 802.16e and 802.16g standards.

- **R2**: This logical reference point consists of protocols and procedures between MS and CSN associated with authentication, services authorization and IP host configuration management.

- **R3**: This reference point contains a set of control plane protocols between ASN and CSN to support AAA, policy enforcement and mobility management capabilities. The bearer plane methods are also included to transfer user data between ASN and CSN.

- **R4**: Reference point containing a set of control and bearer plane protocols between ASN-GWs to coordinate the MS mobility. This reference point allows interoperability between similar or different ASNs.

- **R5**: Reference Point containing a set of control and bearer plane protocols between the CSN operated by the home Network Service Provider and the visited Network Service Provider.

- **R6**: This ASN reference point consists of a set of control and bearer plane protocols for communication between BS and ASN-GW. The bearer plane consists of intra-ASN data path between BS and ASN-GW. The control plane includes protocols for data path establishment, modification and release control according to the MS mobility events.

- **R7**: This ASN reference point is optional and defines a set of control plane procedures between the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP).

- **R8**: This ASN reference point defines the set of control plane message flows and bearer plane data flows between the base stations to ensure fast and seamless handover. The control plane is defined by the IEEE 802.16e and 802.16g standards.

Being responsible for a well defined interface between the WiMAX entities, the reference points of the network reference model play an important role in the interoperability goal of the WiMAX Forum.

The WiMAX Network Working Group defines three different ASN profiles, which exhibit the possible implementations of the ASN. A vendor can implement only one, but must be compliant with the specification of the profile being implemented. The different ASN profiles are the following:

- **Profile A**: This profile includes a ASN-GW and one or more BSs. The handover control and the radio resource control are performed in the ASN-GW. The ASN anchored mobility among BSs is performed through the R6 and R4 reference points.
- **Profile B**: This profile leads to the implementation of the ASN functions into a single device such as an Integrated Base Station network entity. The intra-ASN interfaces are not exposed.
- **Profile C**: The ASN functions are distributed between the ASN-GW and the BS. The handover control and the radio resource control are performed in the BS. The ASN anchored mobility among BSs is performed using the R4 and R6 reference points.

The Connectivity Service Network includes network elements such as routers, AAA proxy/servers, user databases and gateways. The CSN defines a set of network functions that provide IP connectivity services and which include also IP address allocation, Internet access, billing operations, WiMAX and emerging services such as location based services and IP Multimedia Services.

2.2.3 Mobile WiMAX

The Mobile WiMAX is based on IEEE Std 802.16e. The mobility management defined by the WiMAX Forum was designed to accomplish the following set of features (Andrews et al., 2007):

- Minimize packet loss and handover latency and maintain packet ordering to support seamless handover at vehicular speeds.
- Keep handover control and data path control separate.
- Support IPv4 and IPv6 mobility management protocols.
- Support multiple deployment scenarios. For instance rural and urban areas.

The WiMAX architecture supports two types of mobility, as depicted in Figure 2.8, namely, the ASN anchored mobility and the CSN anchored mobility.

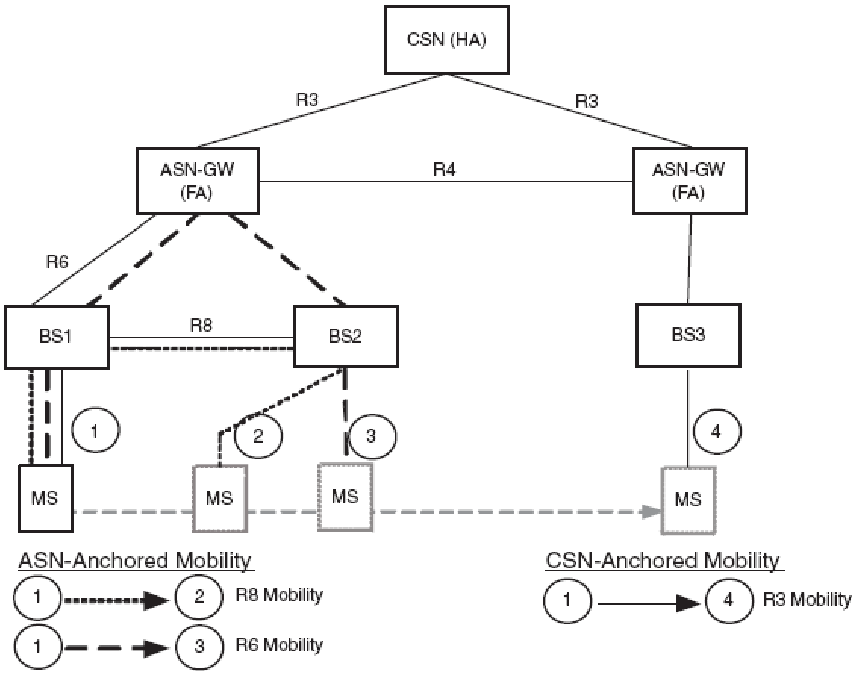


Figure 2.8: WiMAX mobility types
Source Fundamentals of WiMAX.

ASN Anchored mobility

The ASN anchored mobility, also known as intra-ASN mobility, or micromobility is devoted to the mobility procedures that occur without a Care of Address (CoA) update of the MS. In this case, MS moves its point of attachment between BSs within the same ASN network. The micromobility applies to the mobility cases which are not MIP based and all the management messages exchange occurs between R6 and R8 reference points.

The functions that support the ASN-anchored mobility management are:

- **Data Path Function**. Involves the management of the data paths needed for data packet transmission between the functional entities (BSs and ASN-GW). This includes setting up appropriate tunnels between the entities for packet forwarding to ensure low latency and to support multicast and broadcast.

- **Handover Function**. Controls the handover decision operation and signalling procedures.

- **Context Function**. Addresses the exchange of the state information among the network elements involved in the handover process.

There are two types of Data Path Functions, Type 1 and Type 2. The Data Path Type 1 is used for IP or Ethernet packet forwarding using layer 2 bridging or layer 3 routing between two Data Path Functions. The Data Path Type 2 forwards IEEE Std 802.16e MAC SDUs appended with additional information such as CID of the target BS and Automatic Repeat reQuest (ARQ) parameters using layer 2 bridging or layer 3 routing.

The data path is identified via the classification operation which can use different parameters for the classifier, such as MS MAC address, CID, etc. The data path forwarding can be processed in different levels of granularity, such as per service flow, per subscriber or per functional entity. The forwarding of individual streams can be done using tagging supported by different forwarding technologies such as Generic Routing Encapsulation (GRE) (Farinacci et al., 2000), MPLS or 802.1Q.

The Mobile WiMAX specification includes also SFID and CID management. According to IEEE Std 802.16, the SFID does not change during the handover between BSs belonging to the same Network Access Provider. The SFID is set only once (when a layer 2 service flow is originally established) and is not modified by handovers, nevertheless the CIDs must be refreshed whenever the MS moves to a new cell since the CID identifies a logical radio link, while the SFID identifies a layer 2 session.

CSN Anchored mobility

CSN anchored mobility, also known as inter-ASN mobility or macro-mobility considers IP mobility between ASN and CSN across the R3 reference point. In a IPv4 scenario, there is a change of the FA and the inter-ASN mobility is limited to the FAs belonging to the same Network Access Provider.

Different types of Mobile IP implementations are considered to support macro-mobility. The first one is based on MIP-aware clients and the other one is based on clients not MIP-aware, which need some kind of assistance from the network to perform handover. The last approach is based on the Proxy Mobile IP (PMIP) implementation.

With the MIP-aware version, the MS is compliant with the MIP specification as in RFC 3344 (Perkins, 2002) and with some MIP extensions like reverse tunnelling based on RFC 3024 (Montenegro, 2001) and mobile IP vendor-specific extensions based on RFC 3115 (Dommety & Leung, 2001). The client gets a CoA from a FA located in the ASN. As the client moves, it becomes aware of the movement via the agent advertisements, performing a MIP registration with the new FA and obtaining a new CoA from the new FA. In this way, the MS gets the home address from the HA that is located in the CSN network.

With the PMIP variant model, the MIP stack is run on the ASN on behalf of the MS that is not MIP-aware. The PMIP mobility manager is a functional entity that manages multiple PMIP clients. The PMIP client is identified by the Network Access Identifier of the user (the same used for authentication) and performs the MIP registration to set up or update the forwarding path of the MS on the HA. All the mobility management is transparent to the MS. The FA performs sightly different from a standard MIP specification (RFC 3344). The control plane is held between PMIP client and PMIP mobility manager, while user data is sent to the MS over the corresponding R4 or R6 data path.

The mobility management for IPv6 differs from IPv4. For instance, an IPv6 node does not need the Foreign Agent. The route optimization, with a MIPv6-aware client, uses the Colocated CoA (CCoA) obtained via stateless configuration as in RFC 2462 (Thomson & Narten, 1998) or via stateful configuration like DHCPv6 defined in RFC 3315 (Droms et al., 2003)). The CCoA is communicated to the HA and to the CN which updates its binding cache. If the CN does not use a binding cache, it relies on the HA to communicate with the mobile node.

2.2.4 Quality of Service in WiMAX

The WiMAX QoS framework extends IEEE Std 802.16e QoS model by defining various QoS-related entities in the WiMAX network and the mechanisms for provisioning and managing various service flows (Andrews et al., 2007).

The WiMAX QoS framework supports static and dynamic service flow creation. Release 1.0 only envisions the static provisioning of service flows. Also, the QoS mechanisms only focus on the WiMAX radio link connections and no end-to-end QoS guarantees are specified (there is no provision of QoS in the access and core networks).

The WiMAX QoS framework has the following elements in the release 1.0:

- **MS and ASN**. The ASN-initiated creation of service flows must be supported.
- **Policy Function (PF)**. PF and policy database are located in the home Network Service Provider. PF contains the general and application-dependent policy rules of Network Service Provider. PF is responsible for evaluating a service request, which may come from a Service Flow Authorization (SFA) or from an Application Function (AF).
- **AAA server**. This server stores QoS profiles and associated policy rules. This information can be provided in two ways: In the first hand, the user QoS profiles can be downloaded to the SFA at the network entry process as part of the authorization and authentication part. On the other hand, the AAA server can provision the information to the PF.
- **Service Flow Management**. Entity located in the BS and responsible for the creation, admission, activation, modification and deletion of the IEEE 802.16e service flows. It consists of an admission control function and associated local resource information.
- **Service Flow Authorization**. Entity placed in the ASN and with the responsibility of determining if a service flow is allowed in the presence of an incoming service request against the user QoS profile. An anchor SFA exists for each MS for a given session and holds the communication with the PF. The serving SFA communicates directly with the SFM.
- **Application Function (AF)**. Entity that can initiate the service flow creation on behalf of an user (e.g. SIP client).
- **Network Management System**. Allows the administrative provision of service flows.

Within the release 1.0, a set of service flows can be created, admitted, and activated by default, after a subscriber station registers with the WiMAX network and before IP data begins flowing. The description of the service flow, and optionally the user priority, must be given for the service flow creation.

An anchor SFA is assigned to the MS after the registration of the MS with the WiMAX network. If the QoS profile has been downloaded from the AAA server during the authentication part of the network entry process, the SFA initiates the creation, admission and activation of the pre-provisioned service flow. Otherwise, the Policy Function has the responsibility to initiate the creation and activation of the pre-provisioned service flow.

The WiMAX QoS framework includes the definition of abstract messages to convey triggers, initiate service flows actions, request policy decisions, download policy rules and update MS location. Resource Reservation Request is sent by the anchor SFA to the serving SFA and to the SFM to request a reservation of resources for traffic flows from/to the MS. Resource Reservation Response is sent from the SFM to the anchor SFA or to the serving SFA to indicate the result of the reservation request.

Despite current standardization of WiMAX and IEEE Std 802.16, other standards have been specified for wireless broadband access.

2.3 Other Standards and Technologies

This section briefly presents some standards and technologies related with IEEE Std 802.16 and WiMAX, namely the HIPERMAN and the WiBRO standards.

2.3.1 HIPERMAN

The Broadband Radio Access Networks (BRAN) technical committee of the European Telecommunications Standards Institute (ETSI) has specified two wireless standards: the ETSI BRAN HiperAccess and the ETSI BRAN HiperMAN.

The HiperAccess defines the PMP broadband wireless for use in frequency bands between 11 GHz and 66 GHz. It can be compared to the IEEE Std 802.16 WirelessMAN-SC profile since some of the features are shared, such as:

- Single-carrier modulation.
- Basic request/grant scheme.
- Same CoSs and QoS concepts.
- Similar uplink and downlink map structure.

ETSI BRAN HiperMAN specifies PMP and mesh network topologies operating in frequencies below 11 GHz. HiperMAN is specified in different technical documents. ETSI TS 102 178 (ETSI, 2006a) specifies the data link control features and ETSI TS 102 177 (ETSI, 2006b) addresses physical layer characteristics.

The HiperMAN includes specifications for interoperability with IEEE Std 802.16-2004 and IEEE Std 802.16e. The ETSI TS 102 178 defines PDU formats, downlink header formats (similar to the ones covered by IEEE Std 802.16), generic header and bandwidth request header. MAC management messages are specified the same way as in IEEE Std 802.16, for instance *DSx-REQ* and *DSx-RSP* have the same type encoding. Nevertheless, other management messages are modified, for instance *REQ-REQ* message, when including MAC version, maximum power transmitted, amplifier backoffs and current transmitted power parameters.

The HiperAccess standard is easier to implement, when compared to the IEEE Std 802.16 WirelessMAN-SC physical profile, but is less efficient and only focuses on the ATM cell transport.

2.3.2 WiBro

The WiBro is a Wireless Broadband standard (WiBro, 2007) compliant with IEEE Std 802.16e. It is being developed by the Korean telecommunication industry.

The evolution of WiBro and IEEE Std 802.16e leads to an interoperability between the two standards, being the WiBro considered as a service name for Mobile WiMAX in Korea as cited by WiMAX Forum (Forum, 2006). WiBro corresponds to a subset of the IEEE Std 802.16e WirelessMAN-OFDMA profile.

The network architecture of WiBro contains the Access Control Router, which can be compared to the ASN-GW, the Radio Access Station that is similar to the BS and the Personal Subscriber Station.

2.4 Conclusion

IEEE Std 802.16 has interesting characteristics that make it a promising standard, for instance, the simultaneous point to multipoint and mesh modes.

WiMAX Forum is specifying WiMAX based on the IEEE 802.16 standards family. The current efforts of the WiMAX Forum in the specifications and interoperability tests represent a stimulus to the WiMAX adoption as the wireless broadband access technology of the momentum.

The native QoS support of IEEE 802.16 is also an important feature of the standard that is incorporated in WiMAX to support a whole range of applications, going from data transmission to real-time applications.

Recent developments have been concentrated in mobility. The Mobile WiMAX based on IEEE Std 802.16e, supports vehicular speeds and somehow can compete with 3G standards.

3
The Media Independent Handover Standard

The Media Independent Handover (MIH) Standard or IEEE Std 802.21, being specified to enable handovers between heterogeneous networks, is introduced in this chapter.

In the first section an overview of the evolution of IEEE Std 802.21 is presented. The second section presents a description of the standard. The third and fourth sections introduce the Media Independent Handover Function, and the relation between the MIH standard and IEEE Std 802.16, respectively. Finally the current IETF specifications regarding the Media Independent Handovers are introduced.

3.1 IEEE Std 802.21 Evolution

The IEEE 802.21 Working Group (IEEE, 2007f) is developing a standard to enable handover between heterogeneous networks, which include IEEE 802 and non IEEE 802 networks, such as cellular networks. This Working Group has started to work on 2003, according to the Project Authorization Request document (IEEE, 2007e), with the purpose at allowing the handovers between 802 networks, including wired and wireless networks.

Initially the issues identified were:

- Ambiguous indicators of network attachment in 802 Medium Access Control (MAC) layers.
- Lack of information to make an effective handover decision. The 802 standards family do not provide sufficient information to the upper layers.
- No standard mechanism to exchange information in 802 standards between mobile terminals and network attachment points.

The 802.21 Working Group released the first draft of the Media Independent Handover standard in 2005, the P802.21/D00.01. In 2006, the P802.21/D01.00 (IEEE, 2006) was released. The last version published[1] is the P802.21/D07.00 (IEEE, 2007d) draft.

3.2 IEEE Std 802.21 Overview

This section presents the MIH architecture, describing the main goals of IEEE Std 802.21 and how they are achieved.

Vivek G. Gupta (Gupta, 2006) refers that the goal of the MIH standard is improving the handover between heterogeneous technologies, known as vertical handovers. To achieve a seamless handover support, different aspects need to be improved:

- **Network selection**. The target networks are only selected based on signal strength criteria. However other important requirements, such as the need for higher data rates, are not considered, thus leading to underperformant network selection.
- **Support for multihomed nodes**. Nodes have more than one type of interface according to the technologies supported. Nevertheless, the use of the diverse interfaces is not optimized. For instance, if there is no connection for a Wireless Fidelity (Wi-Fi) network, the node does not incur in the use of the 3G interface to have service continuity.
- **Support for L3 mobility protocols**. Distinct mobile IP management mechanisms address the operations at layer 3 to support mobility. Nevertheless, each proposed scheme relies on different kinds of information to perform

[1] August 2007

the handover procedures at IP layer. Therefore, the implementation of 'assisting information' is needed to enable the mobile processes addressed in the Mobile IP specifications, such as MIPv4 and MIPv6, for each technology standard (i.e. 802.16, 802.11 and others).

- **Unstructured L2 information**. The L2 information, which acts as the sustaining information for upper layers, is not provided a standard way. For each new technology standard, L3 mobility protocols must be adapted to the specific media type defined in the corresponding standard. For instance, Fast Handovers for Mobile IPv6 (FMIPv6) (Koodli, 2005) rely on the L2 triggers to provide seamless handovers, since the predictive mode of FMIPv6 is triggered by L2 information. Nonetheless, for each wireless technology, FMIPv6 should be adapted since there is not a common way to provide L2 information.

The handover, the process by which a mobile node obtains air facilities and preserves traffic flows upon link switch events, is specified in the standard. The handovers can be classified as *hard* and *soft*, according to the method by which they are performed. The *hard* handover uses a *break-before-make* approach, leading to the unavailability of the facilities during the link switch process. The *soft* handover uses a *make-before-break* approach which does not cause disruption of the facilities provided.

The handovers are also classified depending whether they are performed between different technologies – vertical handover, or within the same technology – horizontal handover.

Yet another way to classify handovers is based on the control mechanisms performed. Handovers can be Mobile Node (MN) initiated, MN controlled, network-initiated, and network-controlled. With the MN controlled handover, the MN has the primary control over the handover process. While in the MN initiated case, the MN only informs the network that the handover is necessary or is desired.

The handover process, performed in three phases (initiation, preparation and execution), is affected by several factors. The MIH standard addresses them, as follows:

- **Service Continuity**. The continuation of a service during and after the handover, while minimizing data losses and disruption times, must be supported without the user intervention. The MIH standard can supply the information to an application regarding the available Quality of Service (QoS) on a candidate network, and determine if the handover is viable or not, considering the required QoS and the supported on the candidate network.

- **Application class**. The MIH standard can provide the necessary characteristics for the applications which are handover-aware. Such applications can perform the handover decision, for instance, during the pause phase of a conversation, to minimize the service disruption (delay and data loss).

- **Quality of Service**. IEEE Std 802.21 includes mechanisms to define the QoS parameters, which can be considered as part of the handover decision. MIH defines also mechanisms to support a certain level of QoS during the handover process.

- **Network Discovery**. The standard defines the information and the means to assist the network discovery.

- **Network Selection**. The MIH users or higher layers employ the MIH information, such as link quality and link capabilities, to perform the network selection.

- **Security**. The standard specifies the security mechanisms to set up secure connections. For instance, all the message exchange between the MIH services of the MN and the Point of Attachment (PoA) must be secured until the MN has a secure connection with the PoA.

- **Power Management**. The MIH standard provides media dependant information to higher layers, without having to use particular media specifications to obtain it, thus allowing an efficient optimization of power.

- **Mobile Node Movement**. The standard simplifies the vertical and horizontal handovers by providing information about link conditions.

To address all these factors, the MIH standard defines different services to retrieve information either dynamically or statically.

3.3 Media Independent Handover Function

This section details the MIH Function, a logical layer in the mobility management protocol stack, providing MIH services to upper layers.

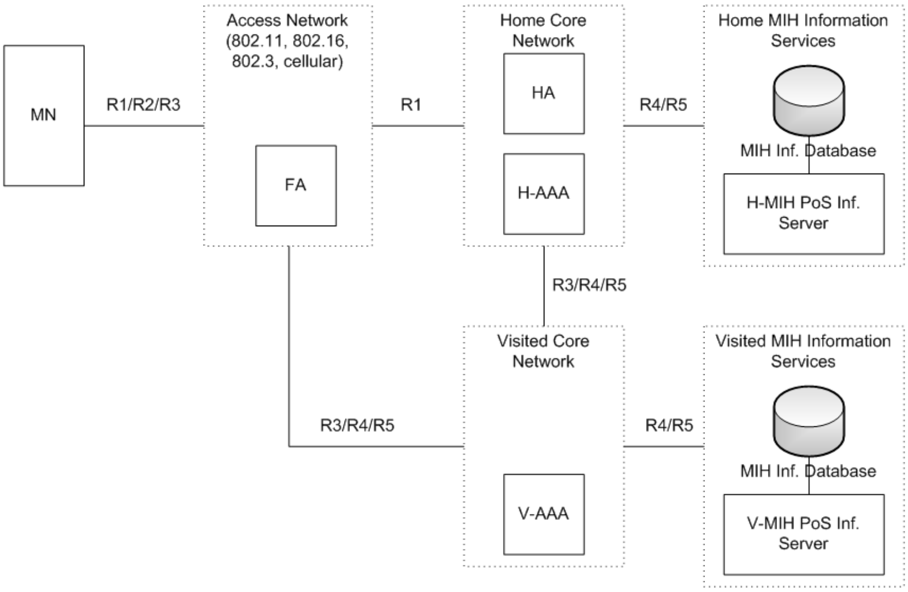


Figure 3.1: Network model with MIH services
Figure compiled from IEEE Std 802.21.

3.3.1 MIH Network Model

The MIH framework defines several reference points over which the control and data information is exchanged. Figure 3.1 depicts a network model with MIH services deployed. The Mobile Node, located at the client side, represents a MIH-capable mobile node. In the access network, the Point of Attachment MIH-capable facilitates heterogeneous handovers. Each access technology advertises its MIH capabilities or responds to MIH service discovery. The access networks have access to the MIH Point of Service (PoS) nodes, which can provide the MIH services during the MIH capabilities discovery. The location of the PoS is operator deployment dependent. It can be co-located with the PoA node in the access network or can reside in the core network.

The reference points, over which entities with a Media Independent Handover Function (MIHF) communicate, are:

- **R1**. Refers to MIHF procedures between the MIHF on the MN and the MIH PoS on the network entity of its serving PoA. The transport of MIH related messages can occur with layer 2 or layer 3 mechanisms.
- **R2**. Refers to the MIHF procedures between the MIHF on the MN and the MIH PoS on the network entity of a candidate PoA. The MIHF messages can be transported using layer 2 or layer 3 protocols.

- **R3**. Refers to the MIHF procedures between the MIHF on the MN and the MIH PoS on a non-PoA network entity. The transport of messages, within this interface, occurs at layer 3 aiming at technology independence. Nevertheless, layer 2 communication is possible in some cases, such as Ethernet bridging, or Multiprotocol Label Switching (MPLS).
- **R4**. Related to the MIHF procedures between an MIH PoS in a network entity and an MIH non-PoS instance in another network entity. Layer 3 communication is defined for this reference point to allow technology independence.
- **R5**. Related to the MIHF procedures between two MIH PoS instances in distinct network entities. This reference point encloses layer 3 facilities for communication.

The MIH entity of the MN can communicate with the MIH network entities using the reference points R1, R2, and R3 of any of the available access networks. R4 and R5 are used for the access to other MIH services, such as the MIH information server, as well as to allow the communication between distinct network entities like the visited and the home network.

The MIH information server holds information in a database which is used by a MN to obtain roaming lists, costs, provider information and supported services.

3.3.2 MIH Function Services

The MIH services supported by the MIH Function, assisting the handover process and the mobility management process, are:

- **Media Independent Event Service (MIES)**. Provides event classification, event filtering and event reporting corresponding to dynamic changes in link characteristics, link status and link quality.
- **Media Independent Command Service (MICS)**. Enables MIH users to control and manage the link behaviour associated with handovers and mobility.
- **Media Independent Information Service (MIIS)**. Provides details of the network characteristics and supported services. Such information allows the effective choice of the target network.

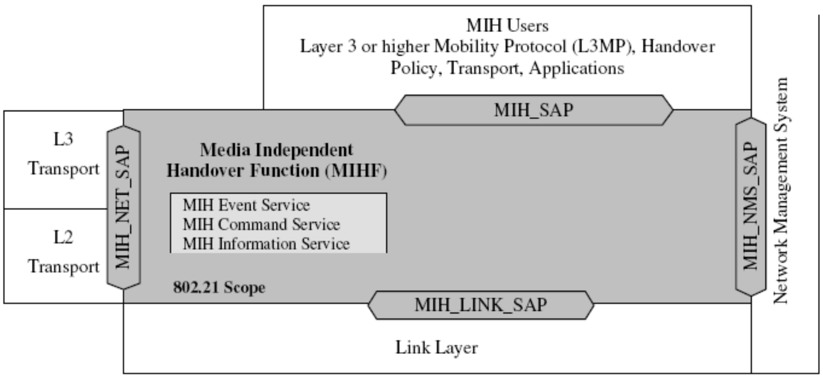


Figure 3.2: MIH general reference model
Source IEEE Std 802.21.

The MIH Function provides asynchronous and synchronous services, through well defined Service Access Point (SAP) for link layers and MIH users. The MIH users represent higher layers protocols (e.g. IP) or user applications. The reference model, depicted in Figure 3.2, illustrates the position of the MIH Function in a protocol stack and its interaction with other elements of the system.

All the information exchanged between the MIHF and other functional entities occurs through the SAPs, which include the following:

- **MIH_SAP**. Allows the interaction of the MIH users with the MIH Function. For instance, to send commands to the local MIHF. The MIH users must be registered in order to obtain access to the MIH generated events and the Link Events.
- **MIH_LINK_SAP**. Interface of the MIHF with the lower layers of the media-specific protocols.
- **MIH_NMS_SAP**. Allows the interaction of the MIH Function with the Network Monitoring System (NMS), which is responsible for retrieving and configuring MIHF parameters, such as the maximum packet transfer delay and the packet loss rate.
- **MIH_NET_SAP**. Interface to enable the transport services over the data plane on the local node, supporting the exchange of MIH messages with remote MIH Functions.

When the MN is connected to an IEEE 802 network, it can use layer 2 or layer 3 mechanisms to exchange MIH signalling messages. When connected to Third

Generation Partnership Project (3GPP) (3GPP, 2007)/3GPP2 (3GPP2, 2007) networks, the mobile node may use layer 3 mechanisms to perform the MIH signalling.

IEEE Std 802.21 defines the MIHF reference model for each media-specific standard. This includes specifications to the MIH_LINK_SAP to interact with IEEE Std 802.3, IEEE Std 802.11, IEEE Std 802.16, 3GPP and 3GPP2 standards.

MIH Service Management

The MIH services availability requires configuration of the MIH entities. To perform such configuration, the standard defines distinct service management functions, which are defined as follows:

- **MIHF Discovery**. To discover the peers supporting the MIH Function. The pre-configuration of MIH peers can also be performed.
- **MIH Capability Discovery**. To find out the MIH services supported by a MIH peer.
- **MIH Registration**. To register and deregister with a MIH peer. For instance, the registration is needed for a notification of the event occurrence.
- **MIH Event Subscription**. To receive notifications about one or more MIH events which occurred locally or remotely.

The MIHF Discovery can be performed at layer 2 and layer 3, although the standard only specifies the procedure over the control plane using media specific broadcast control messages and over the data plane using MIH protocol messages. The IEEE 802.16 Downlink Channel Descriptor messages constitute an example of media specific broadcast messages which allow the discovery of MIH peers. The capabilities of a MIH peer are characterized in terms of the MIH services supported, namely the events in the Media Independent Event Service, the commands in the Media Independent Command Service and the information in the Media Independent Information Service.

The MIH registration provides a mechanism for two peer MIH Functions to identify and communicate with each other. The registration may be necessary for MIH network entities to provide MIH services to the MN. Figure 3.3 depicts the MIH registration flow. First, the source MIH node performs a MIH discovery to determine the address of the peer MIHF. Second, a MIHF capability discovery is

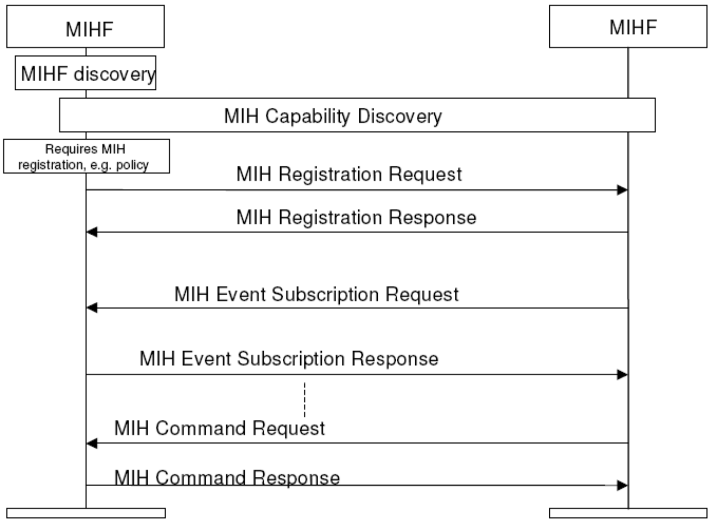

MIHF
MIHF
MIHF discovery
MIH Capability Discovery
Requires MIH registration, e.g. policy
MIH Registration Request
MIH Registration Response
MIH Event Subscription Request
MIH Event Subscription Response
MIH Command Request
MIH Command Response

Figure 3.3: MIH registration flow
Source from IEEE Std 802.21.

executed to determine the MIHF services supported by the MIH peer. If the registration is required, the source MIH node performs a MIH registration request. On a successful registration, the MIHF entities can send requests for specific event subscriptions or send other MIHF commands to request particular actions.

The MIH event subscription allows the subscription of a MIH User for a particular set of events originated at a local or remote MIHF peer.

MIH Events Services

The events indicate a change in a state and transmission behaviour of the physical, and MAC layers, or, with a certain confidence level, predict changes in these layers. Events can be classified in MIH events and Link events, according to their origin. The MIH events are provided by the MIH Function while the Link events are triggered by lower layers. Figure 3.4 depicts the origin and the destination of the different event types.

The events can also be local or remote. The local events are propagated across layers within the local stack of a single device, whereas the remote events traverse a network from a MIH Function to a peer MIHF.

The event registration allows a MIH user to indicate which events it is interested to receive. The registration is performed with a local or remote MIHF entity,

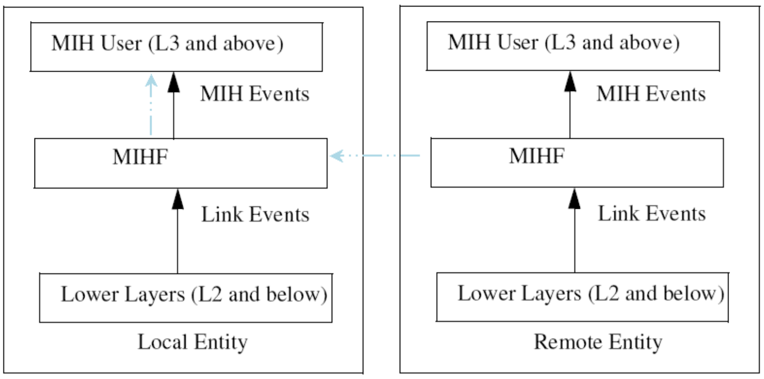


Figure 3.4: Local and remote MIH events
Compiled from IEEE Std 802.21 D07.

to receive MIH events notification.

The Media Independent Event Service supports several types of link events, which are depicted in Table 3.1.

Link Event Name	**Description**
MAC and physical state changes	Correspond on changes in the MAC and physical layers.
Link Parameters	Events triggered due to change in link layer parameters.
Predictive	Events reporting the likelihood of a future change in a certain property. The predictive events have a confidence level, since the prediction is based on past and present events.
Link Synchronous	Events providing indications of precise timing of L2 handover events that are useful to upper layer mobility management protocols.
Link Transmission	Events indicating the transmission status of the higher layer Protocol Data Unit (PDU) by the link layer. These events are useful for upper layers to improve the buffer management in order to achieve low-loss or no loss handovers.

Table 3.1: Types of Link events

Table 3.2 specifies the Link events that are originated by lower layers, for instance, MAC layer of IEEE Std 802.16.

The MIH events are defined based on the link layer events in order to notify the registered MIH user of the respective events occurrence.

Event Type	Event Name	Description
State Change	Link Up	L2 connection is successfully established and ready to be used. Can be delivered by the lower layer of a MN or a PoA.
State Change	Link Down	L2 connection is not available.
State Change	Link Detected	A new link has been detected.
State Change	Link Event Rollback	The previous link event predicted in a Predictive event is no longer expected and needs to be rolled back.
Predictive	Link Going Down	L2 connection is expected to go down (Link_Down) within a certain time interval.
Link Parameters	Link Parameters Report	Link parameters have crossed preconfigured threshold levels.
Link Transmission	Link PDU Transmit Status	Indicate the status of a higher layer PDU.
Link Synchronous	Link Handover Imminent	A link layer handover decision has been made and its execution is imminent.
Link Synchronous	Link Handover Complete	The L2 link handover to a new PoA has been completed.

Table 3.2: Link Layer Events

MIH Command Services

The Media Independent Command Service allows higher layers to configure, control and get information from lower layers. The MIH user may issue commands to the local or remote MIH Function. The information provided by the MIH commands has a dynamic nature when compared to the information provided by the MIIS. The first, includes link parameters like signal strength and link speed while the second has a static nature due to the nature of the comprised parameters, such as network operators and higher layer information. Therefore, the combination of the MICS and MIIS information facilitates handover.

The commands can be classified in two categories: The MIH commands and the Link commands. The MIH commands can be issued by the MIH user to request specific actions from the remote or local MIH Function entity. The Link commands are issued by the MIH Function to request specific actions from the lower layers. The complete list of commands, as specified in IEEE Std 802.21, is exhibited in in Appendix A and Appendix B, respectively.

The classification of the MIH handover commands can be based on the functionality: First, Mobile Node to network; Second, Network to Mobile Network;

Lastly, Network to Network. The Mobile Node to network commands are originated from the Mobile Node towards the destination point, (e.g. *MIH_MN_HO_** commands). The network to Mobile Network commands are originated at the network and are destined to the mobile node (e.g. *MIH_NET_HO_** commands).

MIH Information Services

The Media Independent Information Service provides a framework that allows the MIH Function to discover and obtain network information within a geographical area in order to facilitate network selection and handovers. The information for network selection and handover decisions is provided in the Information Elements.

With Media Independent Information Service, a MN is able to get information about all IEEE 802 and 3GPP networks in a geographical area, even if it only has a IEEE 802.11 interface. The most relevant of the functions of the MIIS are the following:

- Provide information about the availability of access networks in a geographical area.
- Provide static link layer information parameters to assist the MN in the selection of the appropriate access network. For instance, if QoS and security are supported on a particular access network.
- Provide information about the capabilities of different PoA within a geographical area. This information can be supplied in the neighbour reports used to assist radio configuration (channels used by the PoAs).
- Provide indication of the higher layer services supported by different access and core networks. This information may aid in making the handover decision.

The Information Elements can be classified into three major groups, as follows:

- **General information and access network specific information**. Provide a general overview of the different networks offering coverage within an area. The information can include network security, the cost of connecting to the network and the supported QoS level.

- **Information about PoAs**. Provide information about different PoAs for each access network. This information includes PoA addresses, location, supported data rates, the type of physical and MAC layers and channel parameters.

- **Other Information**. Vendor specific information.

The different schemes to represent the Information Elements are the Type Length Value (TLV) representation and the Resource Description Framework. The Media Independent Information Service schema can be classified in two major categories: First, the basic schema that must be supported by each MIHF; and second, the extended schema that is vendor specific. Appendix C exemplifies a subset of the defined Information Elements. The TLV representation of the Information Elements includes the type field, which has four bytes and describes the Information Element ID; the length field and the value field which contains the value of the Information Elements.

Different Information Element containers are defined to represent the neighbourhood information in a TLV format. These include List of Neighbouring Access Networks container, Access Network container and the PoA container. The containers group both optional and non-optional IEs.

The RDF schema is based on the Extensible Markup Language (XML) syntax. The RDF schema has some advantages when compared to the TLV format, such as the support of hierarchical and non-hierarchical information structure, support of flexible data query, and the distribution of the schema definitions.

3.3.3 Quality of Service Model for MIH

This section highlights the QoS specification of the MIH standard, which are conformant to the ITU-T recommendation Y.1540 (ITU, 2002).

IEEE Std 802.21 provides examples of mapping the MIH QoS parameters to the media-specific QoS supported parameters. Such mapping is relevant since the QoS specification within each standard is very particular and different among them. Table 3.3 exhibits the mapping between the MIH QoS parameters and the IEEE 802.16 QoS parameters.

The parameters that allow the accurate characterization of the channel information transfer include minimum packet transfer delay, average packet transfer

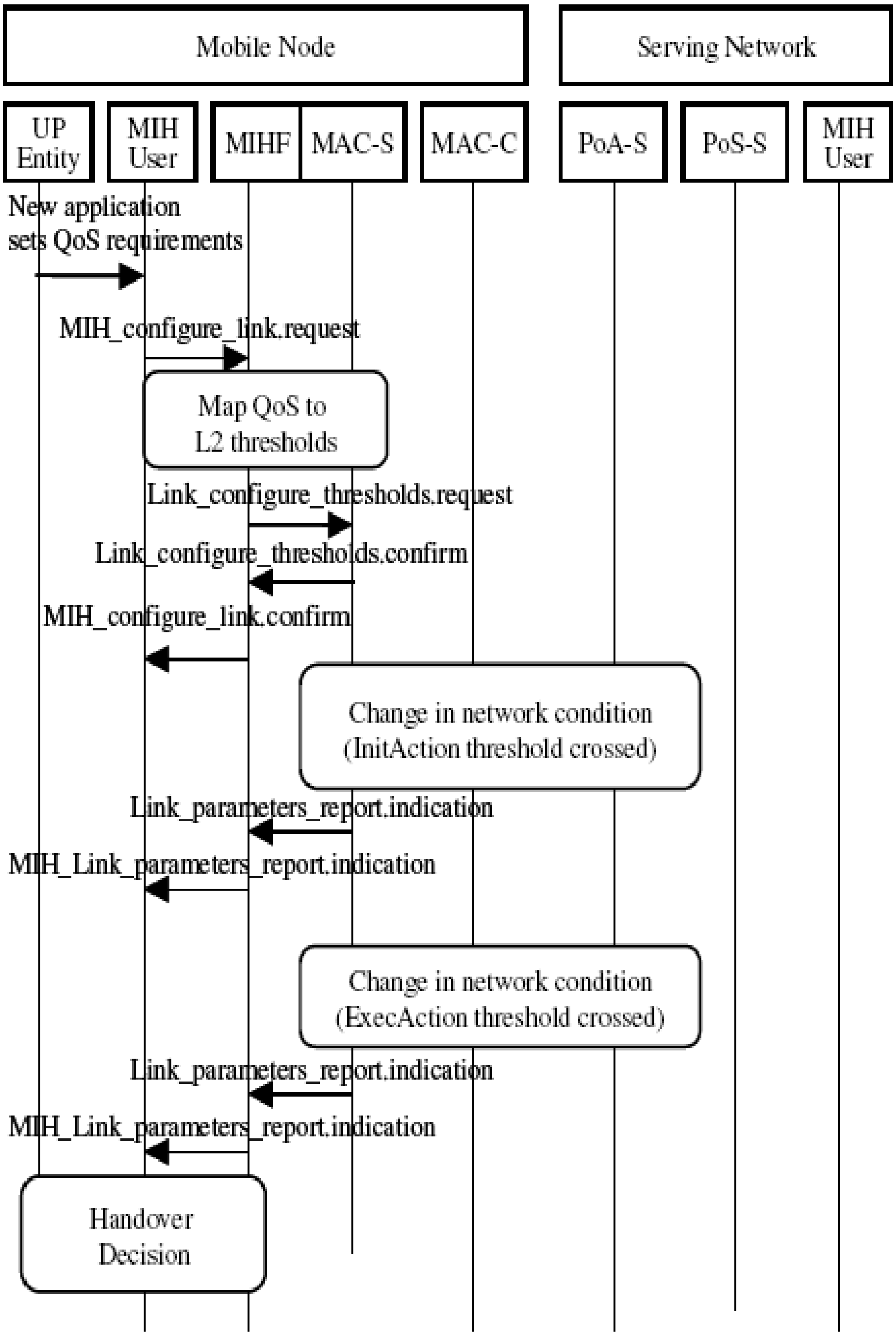

Mobile Node
Serving Network
UP Entity
MIH User
MIHF
MAC-S
MAC-C
PoA-S
PoS-S
MIH User
New application sets QoS requirements
MIH_configure_link.request
Map QoS to L2 thresholds
Link_configure_thresholds.request
Link_configure_thresholds.confirm
MIH_configure_link.confirm
Change in network condition (InitAction threshold crossed)
Link_parameters_report.indication
MIH_Link_parameters_report.indication
Change in network condition (ExecAction threshold crossed)
Link_parameters_report.indication
MIH_Link_parameters_report.indication
Handover Decision

Figure 3.5: MIH QoS flow
Source IEEE Std 802.21.

MIH QoS Parameters	802.16 QoS Parameters
Throughput	Maximum Sustained Traffic Rate
Packet Loss Rate	-
Packet Error Rate	Packet Error Rate
CoS Minimum packet transfer delay	-
CoS Average packet transfer delay	-
CoS Maximum packet transfer delay	Maximum Latency
CoS packet transfer delay jitter	Tolerated jitter

Table 3.3: QoS mapping between MIH QoS and IEEE 802.16 QoS parameters

delay, maximum packet transfer delay, jitter, packet loss rate and packet error rate.

Some technologies, such as IEEE Std 802.16 support Class of Service (CoS) differentiation per link. The parameters to characterize the information transfer of a multi-CoS include link throughput (maximum data rate achievable), link packet error rate, supported classes of service, class minimum packet transfer delay, class average packet transfer delay, class maximum packet transfer delay, class packet delay jitter and class packet loss rate.

Figure 3.5 depicts an example of the QoS message flow to set the requirements of an application. The application informs the MIH user about the QoS requirements, and a MIH request is issued towards the MIHF, thus the mapping between MIH QoS parameters and Layer 2 parameters is performed and a link request is issued by the MIH Function to the respective MAC specification.

The MIH standard also specifies the calculation of the different QoS parameters and the mapping to other technologies, such as, 3GPP and IEEE 802.11.

3.3.4 MIH Protocol

This section overviews the MIH protocol which includes the specifications of the MIH messages.

The MIH protocol defines the format of the messages that are exchanged between remote MIH entities and the transport mechanisms ensuring messages delivery. The transport mechanism depends on the access technology connecting the Mobile Node to the network and on the location of the MIH PoS. The two kind of transport mechanisms considered in the MIH standard are: Lower layer transport (layer 2), and the Higher layer transport (layer 3). Within layer 2, the transport can be assured in the data and management planes. For instance, the MIH messages can be carried in management messages of IEEE Std 802.16, while other standards, like Ethernet, only support the transport in data frames. Whenever the Mobile Node can not reach the MIH PoS via layer 2 mechanisms, then the layer 3 transport mechanisms must be employed.

The MIH protocol provides several services, such as the following:

- **MIH Function discovery**. To discover the MIHF entity that provides MIHF services in the access network.
- **MIH capability discovery**. To discover the capabilities of a peer MIH Function entity in the network.
- **MIH registration**. To register with a peer MIHF to establish a new MIHF pairing.
- **MIH event subscription**. To subscribe to a particular set of events.
- **MIH message exchanges**. To exchange MIH messages between the peer MIHFs.

The MIH protocol messages require reliability to ensure the receipt of data by the destination. The reliability can be maintained with optional acknowledgement mechanisms, which are needed when the underlying transport protocol does not ensure reliable services. The source MIHF, transmitting MIH messages, can use the MIH ACK message to acknowledge the successful receipt of a MIH protocol message at the destination MIH Function. If the MIH ACK is lost, and after the expiration of the ACK timer, the source retransmits the MIH message that was being acknowledged.

The MIH protocol frame is constituted by the MIH protocol header and the respective MIH payload. Table 3.4 contains a detailed description of the header fields.

The messages of the MIH protocol use the MIH Function ID and Transaction ID identifiers. The MIH Function ID is a identifier required to uniquely identify MIH Funciton end points to deliver the MIH services. The MIH Function ID is used during the MIH registration and in all messages that are required to identify end points. The broadcast MIH Function ID (value zero) can be used when the destination is not known. The Transaction ID is an identifier used to match a request message with the corresponding response message. The identifier is required to match each request, response or indication message and the respective

Field Name	**Size (bits)**	**Description**
Version	4	To specify the version of the MIH protocol. Value 1 is the current specification.
ACK-Req	1	To request the acknowledgement of a message.
ACK-Rsp	1	To respond to the request for an acknowledgement.
Unauthenticated Information Request	1	To indicate if the protocol message is sent before an authentication or an association. This limits the length of the response message.
Reserved	9	Not used, filled with zeros.
MIH Message ID (MID)	16	Combines the Service Identifier (SID), 4 bits identifying the different MIH services (1-Service management, 2-Event service, 3-Command service, 4-Information service); the Operation Code, 2 bits establishing the type of operation of the respective SID (1-Request, 2-Response, 3-Indication); and the Action Identifier (AID), 10 bits indicating the action to be taken regarding SID.
Transaction ID	16	To match Request and Response, as well as matching Request, Response and Indication to an ACK.
Variable Load Length	16	Indicates the length of the variable part embedded in the MIH protocol frame. The length of the MIH protocol header is not included.

Table 3.4: MIH protocol header

acknowledgement. It is set by the node initiating the transaction and is carried over the fixed part of the MIH protocol frame. The transaction ID is a 16 bit identifier.

The MIH standard does not specify the support for the transport of the MIH messages at layer 3. Such support is being addressed by other entities, such as the Internet Engineering Task Force (IETF).

3.4 IEEE Std 802.21 and IEEE Std 802.16

This section provides a general overview on the relations of the MIH standard and IEEE Std 802.16 also known as Wireless Metropolitan Area Network (WMAN).

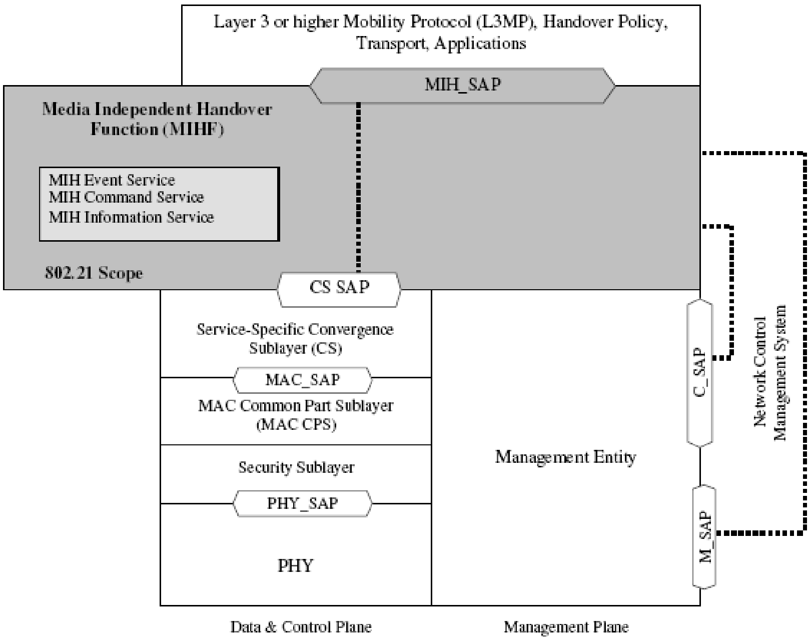

Layer 3 or higher Mobility Protocol (L3MP), Handover Policy, Transport, Applications
MIH_SAP
Media Independent Handover Function (MIHF)
MIH Event Service
MIH Command Service
MIH Information Service
802.21 Scope
CS SAP
Service-Specific Convergence Sublayer (CS)
MAC_SAP
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
PHY_SAP
PHY
Management Entity
C_SAP
M_SAP
Network Control Management System
Data & Control Plane
Management Plane

Figure 3.6: MIH reference model for IEEE Std 802.16
Source IEEE Std 802.21 D07.

3.4.1 MIH Specifications for IEEE Std 802.16

The MIH standard uses the MIH_LINK_SAP to interface with the media-dependent lower layers. The Control (C_SAP) and the Management (M_SAP) SAPs are employed to interface with the control and management planes of the IEEE 802.16 networks, respectively. Both the C_SAP and the M_SAP are defined by IEEE Std 802.16g (IEEE, 2007b). Figure 3.6 depicts the MIH reference model for IEEE Std 802.16.

The Convergence Sublayer SAP, defined in IEEE Std 802.16, provides the interface between the MIH Function and the Service-Specific Convergence Sublayer and is used to transport the MIH messages over the data plane.

The MIH standard also includes specification for the mapping of the MIH primitives to the IEEE Std 802.16 primitives. For instance, the MIH_LINK_SAP primitive Link_Detected corresponds to the C-HO-RSP primitive of the IEEE 802.16 C_SAP.

3.4.2 IEEE Std 802.16 support for MIH messages

The MIH protocol messages can be conveyed through the MOB_MIH_MSG management message, between 802.16 entities, as defined in IEEE Std 802.16g (IEEE, 2007b).

During the network entry, if the MIH query capability is enabled, the Privacy Key Management (PKM) messages can be used to exchange MIH Frames. The Mobile Station submits an MIH query by sending a PKM-REQ message with code 31. The Base Station, when receiving the MIH query, acknowledges the request with a PKM-RSP message with code 32 (MIH ACK). The message from the BS is not the response to the MIH query, thus when the BS receives the MIH response, it allocates bandwidth for the MS in the UL-MAP, if using unicast delivery method. The BS then uses a PKM-RSP message with the code 33 (MIH Comeback Response) to deliver the MIH response to the MS. Whenever the broadcast delivery method is employed, the MIH Frames are carried, from the BS to the MS, in the Service Identity Identification Advertisement (SII-ADV) messages. Figure 3.7 illustrates the unicast delivery method.

The MS and BS supporting the MOB_MIH_MSG management message shall use the MIH Capability Supported TLV in the Subscriber Station (SS) Basic Capability Request (SBC-REQ) and SS Basic Capability Response (SBC-RSP) management messages. This one byte TLV indicates the supported MIH services and is also used by the BS in the DCD messages to indicate the MIH service capabilities in the BS.

IEEE Std 802.16g specifies support for the MIH control protocol procedures. The Control SAP is extended to support the C-MIH-IND primitive, which is used to indicate the reception of a MOB_MIH-MSG on the air interface. This SAP also allows the Network Control and Management System (NCMS) to request the transmission of MOB_MIH-MSG messages containing the MIH frames.

IEEE Std 802.16g is completing the specification of IEEE Std 802.16-2004 and IEEE Std 802.16e. The support of transport of the MIH messages is an example of such extension.

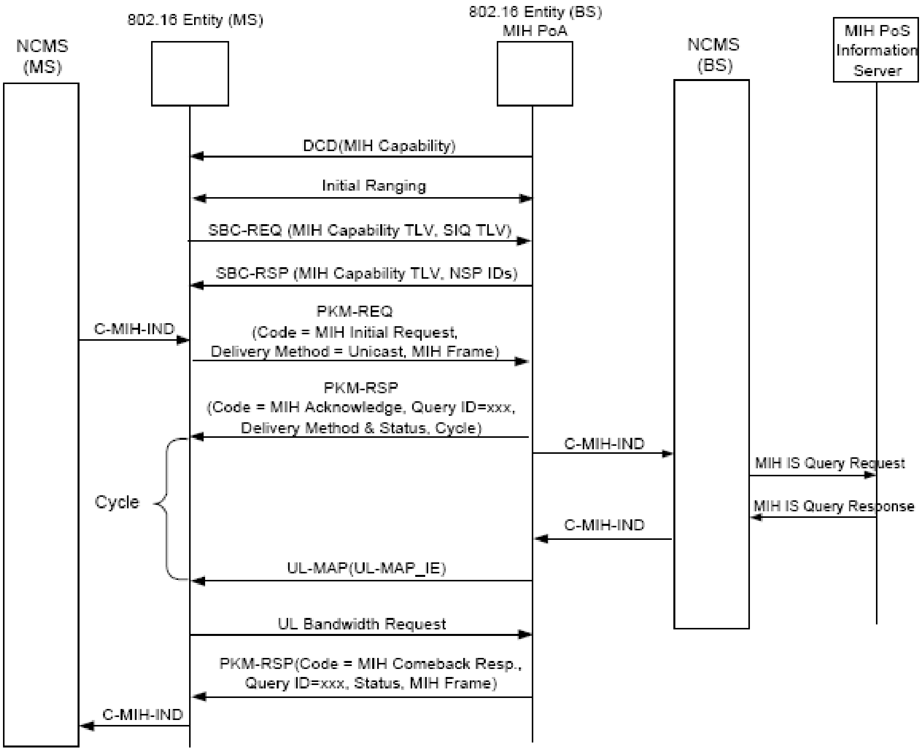

NCMS (MS)
802.16 Entity (MS)
802.16 Entity (BS) MIH PoA
NCMS (BS)
MIH PoS Information Server
DCD(MIH Capability)
Initial Ranging
SBC-REQ (MIH Capability TLV, SIQ TLV)
SBC-RSP (MIH Capability TLV, NSP IDs)
C-MIH-IND
PKM-REQ (Code = MIH Initial Request, Delivery Method = Unicast, MIH Frame)
PKM-RSP (Code = MIH Acknowledge, Query ID=xxx, Delivery Method & Status, Cycle)
C-MIH-IND
MIH IS Query Request
MIH IS Query Response
Cycle
C-MIH-IND
UL-MAP(UL-MAP_IE)
UL Bandwidth Request
PKM-RSP(Code = MIH Comeback Resp., Query ID=xxx, Status, MIH Frame)
C-MIH-IND

Figure 3.7: MIH exchange using unicast deliver method of IEEE Std 802.16
Source IEEE Std 802.16g.

3.5 IEEE Std 802.21 and IETF

This section presents the different connections between the IEEE 802.21 Working Group and the different Working Groups, composing IETF, such as the MIPSHOP Working Group [2] and the IP over IEEE 802.16 Networks (16ng)[3].

The MIPSHOP Working Group is addressing the development of solutions to aid IP handover mechanisms between heterogeneous wired and wireless access systems, including IEEE Std 802.21. The MIPSHOP Working Group identifies the issues related with transport and security of messages containing different sets of information to aid in IP handover mechanisms in heterogeneous environments

[2] The MIPSHOP stands for Mobility for IP: Performance, Signalling and Handoff Optimization. The description of this working group can be found at `http://www.ietf.org/html.charters/mipshop-charter.html`

[3] The 16ng Working group is available at `http://www.ietf.org/html.charters/16ng-charter.html`

(Melia et al., 2007). The MIH layer 3 problem can be divided in two parts:

1. **Information**. The information elements being exchanged. The messages can be different in nature, such as the Information, Command and Event Services.

2. **Transport**. The transport mechanism to support the exchange of information elements, which includes discovery of peers and security of messages over the network.

As mentioned before, IEEE Std 802.21 does not define a higher layer transport mechanism for the MIH protocol. The Mobility Services correspond to the different functions to support MIH management, namely Information, Event and Command Services.

The transport layer provides container capability to support mobility services, as well as any required transport and security operations necessary to provide communication. The Mobility Service Transport Protocol (MSTP) contains a transport header and an opaque payload (no inspection performed). The MSTP must support a number of requirements to enable the transport of MIH messages. For instance, MSTP should enable node and service discovery, establish security association, and provide secure and reliable delivery of information.

Rahman et al. (2007) propose the use of User Datagram Protocol (UDP) as a mechanism to transport MIH messages between nodes. UDP is preferred over Transport Control Protocol (TCP), since this transport protocol is already widely used due to its simplicity and the fast transport mechanisms supported.

Jang et al. (2007) on the specification of FMIPv6 protocol over IEEE 802.16 networks, explore the MIH primitives, like *Link_Detected* and *Link_Going_Down*. Such use allow to inform upper layers of the link layer events in a standard form.

3.6 Conclusion

The MIH standard is filling a missing gap in the current standards to enable seamless handovers, especially handovers performed between heterogeneous technologies.

To achieve the goal of supporting handovers between heterogeneous networks, current standards are including the MIH specification, namely, the mechanisms to transport MIH messages at the link layer. IEEE STd 802.16g introduces such support for the IEEE 802.16 standards family.

The current versions of the different standards (802.3, 802.11) which do not support the transport of MIH messages at the link layer, can use the transport of MIH messages at layer 3.

4

WiMAX Extension to Isolated Research Network Areas

This chapter describes the WEIRD research project. WEIRD explores the WiMAX technology to overcome the limitations of current wireless standards.

Section 4.1 presents the WEIRD project description, the testbeds and the system scenarios. Section 4.2 describes the WEIRD architecture. Section 4.3 presents the signalling protocols to enable Quality of Service. Section 4.4 presents the mobility protocols used in WEIRD. The chapter ends with the description of the work performed by the candidate in the project.

4.1 WEIRD - Project Description

This section introduces the WiMAX Extension to Isolated Research Network (WEIRD) project, highlighting the goals and the characteristics of the project.

WEIRD, as described in the Description of Work document (WEIRDConsurtium, 2006), is a 24 month integrated project aiming at implementing research testbeds using the Worldwide Interoperability for Microwave Access (WiMAX) technology. Therefore isolated or impervious areas are able to get connection to the Pan-European Gigabit Research Network (GEANT) (GÉANT, 2007). WEIRD results are demonstrated in four European testbeds connected through the GEANT network. The testbeds comprise environmental applications to monitor volcanic and seismic activities, and for fire prevention. It also includes tele medicine applications transmitting data in real-time from remote locations to central offices (e.g. hospitals).

The system scenarios which include environmental monitoring, tele medicine and fire prevention are described with more detail in Appendix E. The WEIRD Testbeds associated to the system scenarios are also presented in Appendix E.

4.2 WEIRD - Architecture

This section details the WEIRD architecture engineered to deploy the different scenario applications targeted by WEIRD, such as fire prevention and tele medicine.

The system specification is defined in deliverable D2.3 (WEIRDConsurtium, 2007). The WEIRD architecture is compatible with the IEEE 802.16d and IEEE 802.16e standards, with the WiMAX Forum network architecture, with the diverse protocols of Internet Engineering Task Force (IETF)[1], as well as with European Telecommunications Standards Institute (ETSI)[2] and 3GPP standards. The WEIRD architecture is vendor independent and offers to applications different levels of QoS based on the IEEE Std 802.16 classes of service.

The WEIRD architecture includes support for Quality of Service (QoS) and mobility. An overview of the WEIRD Architecture is described in Appendix F.

4.2.1 WEIRD - QoS Architecture

This subsection highlights the aspects related with QoS in the WEIRD architecture.

The applications of the WEIRD project have different QoS requirements, in terms of delay and bandwidth. The applications can communicate their requirements to the appropriate entities using the Session Initiation Protocol (SIP) (Rosen-

[1] http://www.ietf.org

[2] http://www.etsi.org

berg et al., 2002), using the WEIRD Agent or via the WEIRD Application Programming Interface (API). SIP-aware applications use the Session Description Protocol (SDP) (Handley et al., 2006) to describe the multimedia sessions characteristics, such as, the codec negotiation. WEIRD-aware applications use the WEIRD API to communicate the QoS requirements such as jitter, delay and maximum bandwidth.

The QoS models supported by the WEIRD architecture for session based services are:

- **QoS assured**. A call can only be established if the requested/required QoS can be guaranteed. These applications require all the QoS setup (media stream specific parameters) before the call. With this model, the call can only start after the successful setup of the resource reservation. The signalling and the resource reservations are controlled by preconditions, that must be verified by one or more users. The SIP applications use this model.
- **QoS enabled**. A call can be set, independently the availability of the QoS resources. With this model, the call setup and the resource reservation are not coupled and may proceed concurrently. The availability of resources does not affect the success of the call but only the effective level of QoS. In a reservation failure situation, the caller can be notified and continue the call in the Best Effort (BE) service. The Enhanced WEIRD Agent uses this model.

The Application Function located in the Connectivity Service Network (CSN) allows the Subscriber Station (SS) to request allocation of resources for SIP applications. The Application Function triggers the service flow creation, admission and activation using the Connectivity Services Controller in the Access Service Network (ASN).

Non SIP-aware applications (e.g. customizable or legacy applications) perform the resource reservation requests through the WEIRD API or with the WEIRD Agent. The Next Steps in Signalling (NSIS) framework protocols are used to perform the signalling of the Quality of Service requests. The QoS-NSIS Signalling Layer Protocol (NSLP) (Manner et al., 2007) performs the reservation in the different nodes traversed by the data flows. The NSIS framework protocols are present in all the segments of the network and communicates with the Connectivity Services Controller (CSC) modules to manage and allocate resources. The CSC engines (e.g. CSC_MS, CSC_ASN and CSC_CSN) act as the Resource Management Function (RMF), in the perspective of NSIS, acting as an interface to the resource manager to perform the requested reservations. Therefore the CSC engines build the denominated QoS specification object (QSPEC) and then inform the QoS-NSLP about the necessary QoS settings.

4.2.2 WEIRD - Mobility Architecture

This subsection introduces the mobility architecture of WEIRD, focusing on the protocols and the different entities to enable mobility.

The mobility architecture of WEIRD is implemented in different phases. The first corresponds to the micro-mobility supported by the IEEE 802.16e equipment, with no enhancements to the off-the-shelf mobility supported by vendors. The second considers macro-mobility schemes such as standard Mobile IPv4 (MIPv4) (Perkins, 2002) or Mobile IPv6 (MIPv6) (Johnson et al., 2004). The macro-mobility schemes can also be based on the improved mobility management protocols, such as Hierarchical Mobile IP (HMIP) (Soliman et al., 2005) and Fast Handovers for Mobile IP (FMIP) (Koodli, 2005), (Koodli & Perkins, 2007). The mobility architecture is based on IPv4 since the support of IPv6 in the WiMAX equipment vendors is still embryonic[3].

The WiMAX Forum Network Working Group classifies applications based on the support of mobile IP mechanisms (Forum, 2007). The applications can be classified as follows:

- **Client Mobile IP (CMIP)**. For applications that are MIP-aware. The Mobile Station (MS) supports MIPv4 defined in RFC 3344 and/or MIPv6 specified in RFC 3775.
- **Proxy Mobile IP (PMIP)**. For applications that do not support MIP and need transparent Mobile IP assistance, defined for IPv4 (Wakikawa & Gundavelli, 2007) and for IPv6 (Gundavelli et al., 2007).

The WEIRD architecture considers two levels of mobility, according to the WiMAX Forum specifications (Forum, 2007):

- **Micro-mobility** or **Access Service Network (ASN) anchored mobility**. The handover functions, context transfer and data path registration only occurs between BS and Access Service Network Gateway (ASN-GW) and/or

[3] At the date of this writting

between BS. This kind of mobility is provided mainly by the mobility support of the mobile WiMAX profile[4], since there is no change of the Foreign Agent (FA).

- **Macro-mobility** or **Connectivity Service Network (CSN) anchored mobility**. This level occurs when the MS changes to a new FA and mobile IP facilities are required. This level of mobility aggregates the mobility support of IEEE Std 802.16e and the mobility support of Mobile IP.

The WEIRD micro-mobility is related to the mobility inside the ASN domain. The MS starts the handover process, although it can also be triggered by the network.

The WEIRD macro-mobility is based on the mobility support from WiMAX, bundled with Mobile IP protocols. The Mobile IPv4, MIPv4, is the core mobile network management protocol in the WEIRD mobility architecture. The functional elements in the WEIRD macro-mobility are:

- **Mobile Node (MN)**. The MN represented by the Mobile Station which changes its point of attachment from the home network/subnetwork to another network/subnetwork.
- **FA**. The FA is performed by the ASN-GW which provides routing services to the registered MN.
- **Home Agent (HA)**. This element is installed in the CSN network, where IP connectivity is assured. The HA forwards (via tunnels) the packets to a mobile node when it is away from its home network/subnetwork.
- **Correspondent Node (CN)**. It represents a node with which the MN communicates.
- **AAA Servers**. The Authentication, Authorization and Accounting (AAA) servers perform authentication and authorization of nodes.

The WEIRD mobility architecture is compliant with IEEE Std 802.21 (IEEE, 2006), known as Media Independent Handover (MIH) standard and which specifies 802 media independent mechanisms to assist the handover process between 802 systems and between different 802 systems and cellular systems. The Media

[4] WiMAX profile based on IEEE Std 802.16e.

Independent Handover Function (MIHF) provides different services to upper layers, such as Information services, Command services and Events services.

The WEIRD mobility architecture is based on the MIPv4 protocol. The MS performs handover between different BSs controlled by different ASN-GWs. After performing the networking entry, as defined in IEEE Std 802.16e, the MS receives information from the FA, which allows the determination of the Care of Address (CoA), that is used by the MS to register with its HA.

4.3 WEIRD - QoS Protocols

This section introduces the QoS protocols implemented in WEIRD. These protocols deal with signalling for admission control, resource control and resource management.

4.3.1 NSIS Framework

The NSIS framework specified in the RFC 4080 (Hancock et al., 2005) splits the signalling protocol stack into two layers: the signalling transport layer that is a generic layer, and the signalling application layer which may support functionalities such as QoS signalling. The NSIS Transport Layer Protocol (NTLP) is referred as the NSIS protocol component supporting lower-layer functions to allow the transport of signalling. Whilst NSIS Signalling Layer Protocol (NSLP) is defined as the NSIS protocol component that supports specific signalling applications.

NSIS may operate in one of the following manners: *on-path* or *off-path*. In the *path-coupled* or *on-path* signalling approach, the signalling messages are routed through the entities that are on the data path. In the *path-decoupled* or *off-path* signalling approach, the signalling messages are routed to nodes that are not on the data path, but that are aware of it. In this case the signalling endpoints may not be related with the ultimate data sender or receiver. The path-decoupled mechanisms have the advantage of an easier deployment, since the upgrade of routers on the data path is not required Cordeiro et al. (2007).

Figure 4.1 depicts NSIS two-layer protocol model. The General Internet Signaling Transport (GIST) (Schulzrinne & Hancock, 2007) is the NSIS transport layer protocol specified to allow routing and transport of upper layer signalling.

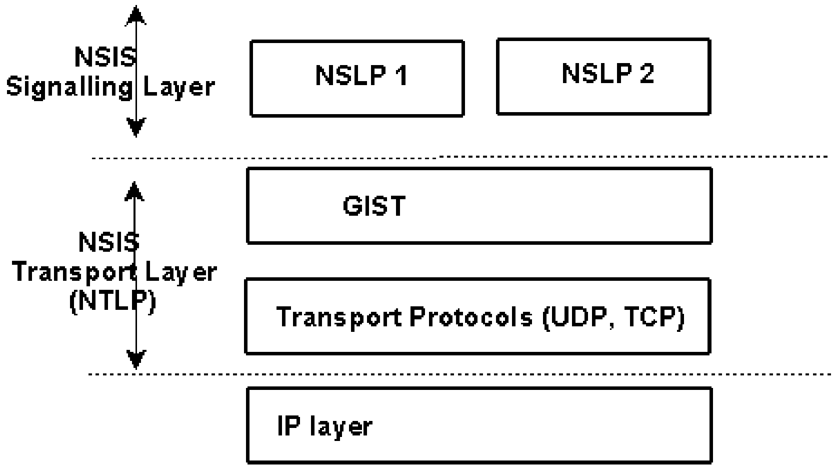


Figure 4.1: NSIS two-layer protocol model
Source RFC 4080 (Hancock et al., 2005).

The QoS-NSLP (Manner et al., 2007) is used for signalling QoS reservations in the network and to maintain the signalling at the application level.

There is also another NSLP specified in the NSIS working group, the Network Address Translator and Firewall (NAT/FW) NSLP (Stiemerling et al., 2007), which allows hosts behind NATs to obtain public reachable addresses and hosts behind firewalls to receive data traffic. However, the NAT/FW NSLP is not used in WEIRD.

The QoS specification (QSPEC) (Ash et al., 2007) characterizes the general QoS parameters of a QoS-enabled domain in a object, the QSPEC.

4.3.2 NSIS QSPEC

A QoS-enabled domain supports a particular QoS model, which incorporates QoS provisioning methods and a QoS architecture, such as Differentiated Services (DiffServ) or Integrated Services (IntServ).

The QoS model specification defines how QoS resources requested are described and how they are managed by the RMF. The QSPEC object contains the necessary information for a QoS model.

Figure 4.2 depicts the local QSPEC processing in a QoS-enabled domain. The QoS NSIS Initiator (QNI) signals its QoS requirements in the initiator QSPEC

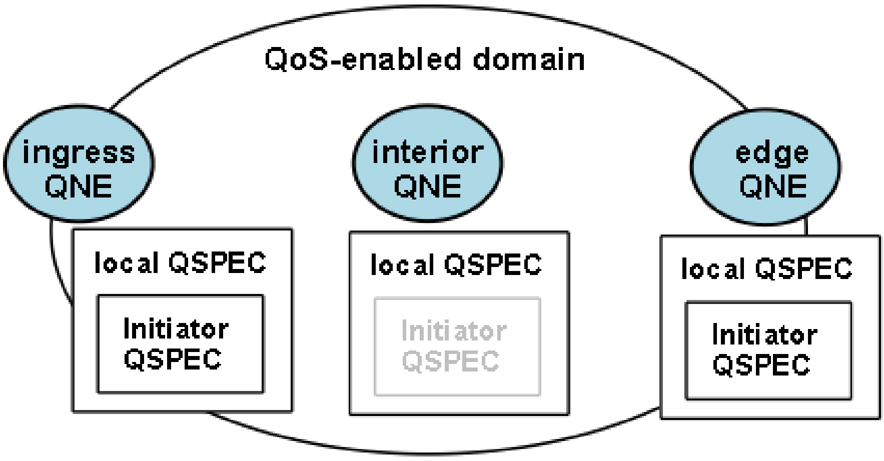


Figure 4.2: Local QSPEC processing

object, the ingress QoS NSIS Entity (QNE) in the local domain translates the initiator QSPEC parameters into the local QSPEC which includes equivalent parameters that are understood in the local domain. Interior QNEs only interpret the local QSPEC objects, while edge QNE interprets local and initiator QSPEC objects. The QSPEC processing at the edge QNE can be performed in one of two ways:

- Translate the initiator QSPEC into a local QSPEC and encapsulate the initiator QSPEC in a *RESERVE* message.
- 'Hide' the initiator QSPEC through the local domain and reserve resources by generating a new *RESERVE* message.

The QSPEC information includes the QSPEC version number and QSPEC objects that can include up to four types of QSPEC objects, which are as follows:

- **QoS Desired**. QSPEC representing the desired QoS specification for a reservation. Included in the *RESERVE* message and is not modified by the different QNEs (it is a read-only object). QNEs must support this type of QSPEC.
- **QoS Available**. QSPEC describing the available resources. QNEs must support also this type of QSPEC object. This QSPEC can be included in the *RESERVE* and *QUERY* messages, in the last case, QSPEC can be updated if resources for a specific parameter are less than those specified in the QSPEC object transported in the messages.

- **QoS Reserved**. QSPEC representing the reserved resources and related QoS parameters. It is not updated by QNEs along the path (read-only) and must be supported by QNEs.
- **Minimum QoS**. This QSPEC is not required to be supported by QNEs, but if supported it represents a lower bound of QoS specification to be supported.

A QSPEC object, as specified in the QSPEC protocol (Ash et al., 2007), includes different parameters, such as:

- **Traffic Model (TMOD)**. The TMOD parameter provides a description of traffic for which resources are reserved. This must be included by the QNI and interpreted by all the QNEs of the QoS-enabled domain. The TMOD parameter includes four mandatory sub-parameters: *rate (r)*, *bucket size (b)*, *peak rate (p)* and *minimum policy unit (m)*.
- **Constraint parameters**. These include Path Latency, Path Jitter, Path Packet Loss Ratio (PLR), Path Packet Error Ratio (PER) and Preemption Priority.
- **Traffic handling directives**. For instance, the excess treatment parameter that indicates how QNE processes the excess traffic that is out-of-profile.
- **Traffic classifiers**. For instance, Per Hop Behaviour (PHB) classes used in DiffServ domains.

The QSPEC include fields to indicate if the QSPEC object is describing Sender-Initiated Reservations or Receiver-Initiated Reservations, as well as flags to depict if the QSPEC object is a Initiator or Local QSPEC.

4.3.3 NSIS QoS-NSLP

This subsection introduces Quality of Service (QoS) NSIS Signalling Layer Protocol (NSLP) protocol, known as the QoS-NSLP.

The QoS-NSLP (Manner et al., 2007) is a protocol to maintain state at nodes along the path of a data flow, with the purpose of providing forwarding resources for a flow. The protocol is conceptually similar to the Resource Reservation Protocol (RSVP) defined in RFC 2205 (Braden et al., 1997). QoS-NSLP uses a soft-state and a peer-to-peer refresh messaging approach as the primary state management mechanism instead of an end-to-end mechanism, as in RSVP.

The QoS request, received by QoS-NSLP, is handled by the RMF, which coordinates the activities required to grant and configure the resources. RMF also handles policy-specific aspects of QoS signalling. The grant process involves the following decision modules:

- **Policy Control**. This module determines whether the user is authorized to make the reservation.

- **Admission Control**. Determines if the node has sufficient available resources to supply the requested QoS.

QoS-NSLP has one interface with RMF and another with GIST to send and receive messages. The interface with RMF allows to request for resource provisioning and receiving information (e.g. monitoring, resource availability and topology) from the RMF.

QoS-NSLP delivers messages and additional information to GIST, such as the identifier of the QoS-NSLP, the session identifier (used by GIST to provide unique session IDs), the Message Routing Information (MRI) object and the indication of the intended direction of the message (towards data sender or receiver).

QoS-NSLP protocol supports both Sender-initiated and Receiver-initiated reservations. In the Sender-initiated reservations, *RESERVE* messages are forwarded in the same direction as the data flow. For a Receiver-initiated reservation *RESERVE* messages travel in the opposite direction of the data flow. In this case the receiver has the responsibility of requesting resources and of maintaining the reservation state.

Figure 4.3 depicts an example of the sender-initiated reservation. In this case, the *QUERY* message is optional and can be used to gather information from the QNEs along the path, in order to find out what are the resources available. The example of Figure 4.3 assumes that the *QUERY* message want sent with the request identification information object which is used to request explicit confirmation (*RESPONSE* message).

An interesting feature supported by QoS-NSLP concerns the bidirectional reservations. There are two special cases in the bidirectional reservations:

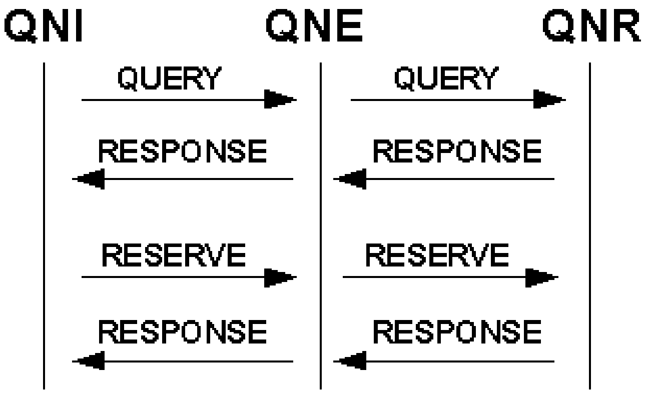


Figure 4.3: Sender-initiator reservation

1. **Binding two sender initiated reservations together**. For instance, one-sender initiated reservation from QNE-A to QNE-B and another from QNE-B to QNE-A.

2. **Binding a sender-initiated and a receiver-initiated reservation together**. For instance, a Sender-initiated reservation from QNE-A towards QNE-B and a Receiver-initiated reservation from QNE-A towards QNE-B. This case is useful when, at least, one of the edges nodes communicating has all the required information to set up both sessions.

Figure 4.4 depicts the bidirectional reservation for the second case. In this case, the response messages are optional, for instance the *QUERY* message was not sent with the request identification information object. The *QUERY* message is sent with the Reserve Init flag set to trigger receiver-initiated reservation (1). The sender-initiated reservation is represented in (2).

Table 4.1 presents the different types of the QoS-NSLP messages and their usage. QoS-NSLP messages are sent peer-to-peer and contain three types of objects:

- **Control information**. General information affecting Qos-NSLP processing (e.g. if response is required).

- **QoS Specification**. QSPECs describe the actual QoS resources desired.

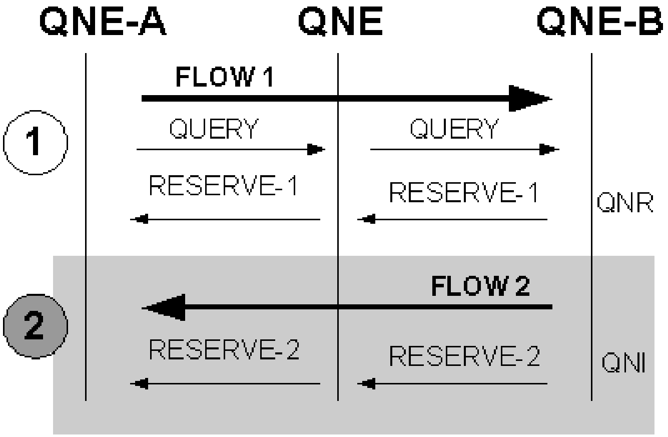


Figure 4.4: Bidirectional reservation process

Type	Description	Flags	Information
RESERVE	create, refresh, modify and remove reservations.	(T) TEAR - reservation to torn down. (R) REPLACE - replace an existing reservation.	Includes reserve sequence number.
QUERY	request information about data path.	(R) RESERVE-INIT - trigger receiver-initiated reservations	Includes QPSEC object.
RESPONSE	provide information about result of a previous message.	- no flags -	Include INFO-SPEC to indicate success or error of operation.
NOTIFY	convey information to a QNE.	- no flags -	Include INFO-SPEC to indicate reason of notification.

Table 4.1: QoS-NSLP messages

- **Policy Objects**. Object with policy data to authorize the reservation of resources.

QoS-NSLP is decoupled from the QoS model, since the QSPEC is opaque to QoS-NSLP.

4.3.4 NSIS QoS-NSLP Authentication

The NSLP auth draft (Manner et al., 2007) specifies a generic model for session authorization within the NSIS Signalling Layer Protocol (NSLP). The session authorization allows to exchange information between network elements in order to authorize the use of resources for a service. A NSLP session authorization policy object (*AUTH_SESSION*) conveys the authorization information for the request. Such information for authorization is provided by the user and is inserted into the NSLP message in the policy object part. The session authorization attributes can be diverse and are identified by an attribute type. For instance, authentication data of the session or the source IP address (IPv4 or IPv6).

The NSLP auth specification also supports different mechanisms of authentication, such as Public key based mechanisms and shared symmetric keys.

The *AUTH_SESSION* object can be used in the QoS-NSLP *QUERY* and *RESERVE* messages to authorize the query operation and the reservation request, respectively. Moreover, it can be present in the *RESPONSE* message to indicate that the authorizing entity changed the original request.

The QNI must fill the *AUTH_SESSION* object in the policy object part of the NSLP message. QNEs receiving messages, must proceed according to the QoS-NSLP specification (Manner et al., 2007) and as follows:

- If the QNE is policy unaware it must ignore the policy data objects and continue processing the NSLP message. Otherwise, the QNE can use Diameter QoS application or RADIUS QoS protocol to communicate with the Policy Decision Point (PDP).

- If the response from a PDP is negative, the request must be rejected, therefore the QNE must send a *RESPONSE* message with the status of the authorization failure. The INFO-SPEC object is used to describe the result of the authorization process.

The NSLP auth is filling a gap in the NSLP specifications regarding authorization of resources.

4.3.5 NSIS GIST

GIST is an on-path protocol for the transport of signalling messages, being the current solution for the NSIS Transport Layer Protocol (NTLP).

The transport of signalling messages requires:

- **Routing**. GIST must determine the adjacent signalling node, since it uses a 'hop-by-hop' approach.

- **Transport**. Deliver the signalling information to the peer identified in the routing process.

The three-way handshake used by GIST supports the establishment of the necessary routing state between adjacent peers. To assure transport, GIST uses two approaches[5]: the "*easy*" which is handled by GIST internally, and the "*hard*" which requires assistance from other protocols. The first, is for "*easy*" messages with a size lower than the Maximum Transmission Unit (MTU) of a path or do not cause congestion and do not need any security or guaranteed delivery. The last, is for "difficult" messages. GIST uses the assistance of transport protocols, such as Transport Control Protocol (TCP) or User Datagram Protocol (UDP) for such cases.

GIST uses two modes of operation, the Datagram mode (D-mode) and the Connection mode (C-mode). The D-mode uses UDP to encapsulate the messages and is used for small and infrequent messages. The C-mode uses TCP or any other stream or message oriented protocol and allows GIST to support reliability and security, if Transport Layer Security (TLS) is employed.

GIST defines four primary messages types: *QUERY*, *RESPONSE*, *CONFIRM* and *DATA*. The *ERROR* message indicates error conditions at the GIST level and the Message Association Hello (*MA-Hello* can be used as a keepalive mechanism for associations. A detailed description of the primary messages of GIST is depicted in Appendix D.

[5] The terminology "*easy*" and "*hard*" are employed in the GIST specification.

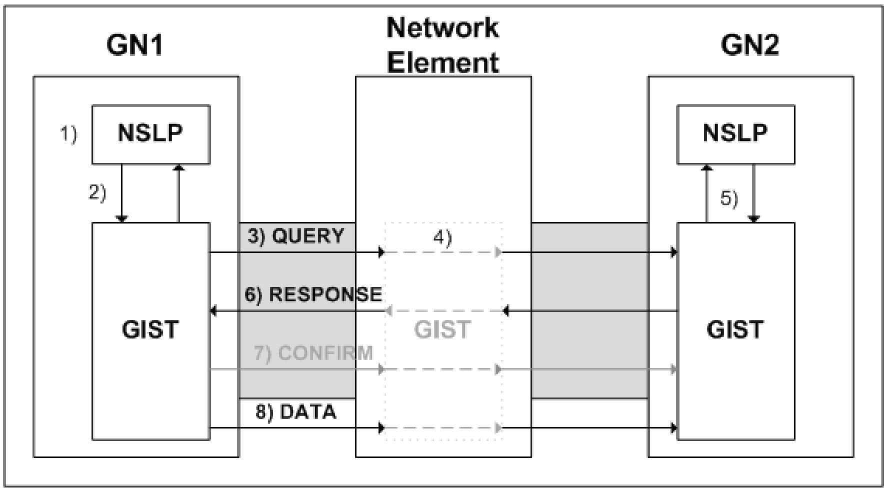


Figure 4.5: GIST operation

Figure 4.5 depicts an example of the GIST operation assuming *GN1* as the sender and *GN2* as the receiver. The network element (e.g. a router) represents a node that is not GIST aware or does not support the NSLP of this domain. The operation proceeds as follows:

1. NSLP processes the signalling message. After checking security and transport requirements, NSLP sends the message to GIST and provides the MRI which contains the needed routing information.

2. GIST receives the message from NSLP, which contains the NSLP payload, control information that expresses how the message should be routed, as well as the session identifier. GIST determines if the message requires fragmentation and checks if it has knowledge for the flow.

3. GIST constructs a *QUERY* message carrying the NSLP payload and additional information at the GIST level to initiate the message association. The *QUERY* is encapsulated in a UDP datagram and addressed towards the flow destination. Every router, along the path of the message checks the *QUERY* message.

4. The network elements forward the message.

5. The message is intercepted at *GN2* by the GIST layer, which passes the NSLP payload upwards to the NSLP layer. The NSLP layer has the responsibility to accept the peering with *GN1*.

6. *GN2* will send a *RESPONSE* message. If an association already exists between *GN1* and *GN2* this message identifies *GN2* as the peer for the flow.

Otherwise, *GN2* sends the *RESPONSE* message in D-mode to proceed with the association setup.

7. This step is only verified if the association does not exist between *GN1* and *GN2*. *GN1* sends a *CONFIRM* message to finish the set up of the association with *GN2*.

8. The signalling message, transmitted by the NSLP of *GN1* and that originated the association between *GN1* and *GN2*, is transported in a *DATA* message.

Figure 4.5 also depicts the three-way handshake process, which occurs in three steps, each one represented by the respective type of message: *QUERY*, *RESPONSE* and *CONFIRM*. The three-way handshake is necessary for each session, but the associations that result from the handshake process can be re-used if the peer and the association characteristics are the same.

GIST uses states for each action occurred in the system and associates a timer to each state. Each time the state is updated, the timer is restarted. If the state is not updated the timer expires and the state is removed. GIST has mainly two state tables: Message Routing State and Message Association State. The Message Routing State is responsible for managing individual flows while the Message Association State is responsible for managing the association between individual peers.

4.4 WEIRD - IPv6 Protocols

IPv6, also known as IP Next Generation (IPng) overcomes some of the limitations of IPv4, providing a better support for mobility. Besides the increased mobility support, IPv6 nodes have a higher routing performance, since IPv6 headers are simplified and only the necessary fields for routing are specified in a general header. The extensions headers are employed to support new functionalities.

The complete IPv6 specification introduces new protocols that concentrate some of the functionalities that were spread in different protocols such as Internet Control Message Protocol (ICMP) and Address Resolution Protocol (ARP) in IPv4. For instance, Neighbour Discovery Protocol (NDP) allows IPv6 to be decoupled from ARP.

4.4.1 IPv6 Neighbour Discovery

The NDP specified in RFC 2461 (Narten et al., 1998) addresses different problems that are related to the interaction between nodes attached to the same link, therefore different procedures are specified. These include Neighbour Unreachability Detection (NUD) specification, employed to determine if a neighbour is no longer reachable, and Duplicate Address Detection (DAD) that allows a node to check if an address it wishes to use is not already in use by other nodes.

NDP operation is based on four type of messages, which are as follows:

- **Router Solicitation (RS)**. This type of message is used by hosts when interfaces are activated to request routers to generate router advertisements messages immediately. Message sent to the all-routers multicast address, which is listened by all routers.

- **Router Advertisement (RA)**. Messages sent by routers containing prefixes that are used for on-link determination and/or address configuration. This message also informs hosts how to proceed with address configuration, which can be performed via stateful mechanisms like Dynamic Host Configuration Protocol (DHCP), or stateless mechanisms, like IPv6 autoconfiguration.

- **Neighbour Solicitation**. Messages sent by a node to determine the link-layer address of a neighbour or to verify if a neighbour is still available, therefore employed by DAD procedure. Message sent to solicited-node multicast address.

- **Neighbour Advertisement**. Message sent in unicast in response to a neighbour solicitation.

The exchange of messages allow hosts to determine the routers that are present on a link, and other information, such as neighbours and next hops. For instance, the neighbour cache allows the node to retain information about neighbours and their reachability, and the prefix list, allows the storage of prefixes received in the Router Advertisement messages sent periodically by routers.

Nodes acting as routers must be explicitly configured to act as a router, such configuration includes the ability to send RAs, since, by default, nodes must not send RAs at any time. The configuration of nodes to process router advertisement messages is performed within different parameters, which include :

- **MaxRtrAdvInterval**. Represents the maximum time allowed to before sending unsolicited RA. Default value is 600 seconds and the allowed values are in the range between 4 and 1800 seconds.

- **MinRtrAdvInterval**. Represents the minimum time allowed before sending unsolicited RA. Default value is 0.33x*MaxRtrAdvInterval* and allowed values vary between 3 and 0.75x*MaxRtrAdvInterval*.

- **AdvDefaultLifeTime**. Represents the Lifetime of a RA. If a value of zero exists, then the router sending such message must not be used, otherwise the values vary between *MaxRtrAdvInterval* and 9000 seconds. Default value is 1800 seconds.

Other important parameters to the protocol operation are related to the Prefixes announced. Prefixes have a lifetime associated (*AdvValidLifeTime*) with a default value of 2592000 seconds (30 days).

4.4.2 Mobile IPv6

Mobile IPv6 (MIPv6) is a protocol specifying mobility support for IPv6. Such specification is addressed in RFC 3775 (Johnson et al., 2004).

Without the mobile assistance, a MN can change its IP address each time it moves to a new link but would not be able to maintain transport and higher-layer connections when changing location. MIPv6 allows hosts to change between links without changing the mobile home address.

Mobility support is also specified for IPv4 (MIPv4) in RFC 3344 (Perkins, 2002). Nevertheless MIPv6 has the following benefits when compared to MIPv4:

- There is not the need to have Foreign Agents.

- Supports route optimization natively.

- Less overhead. Packets addressed to a MN are sent using IPv6 routing header rather than being encapsulated, as in IPv4.

- It is decoupled from any particular link layer since it uses IPv6 Neighbour Discovery protocol instead of ARP.

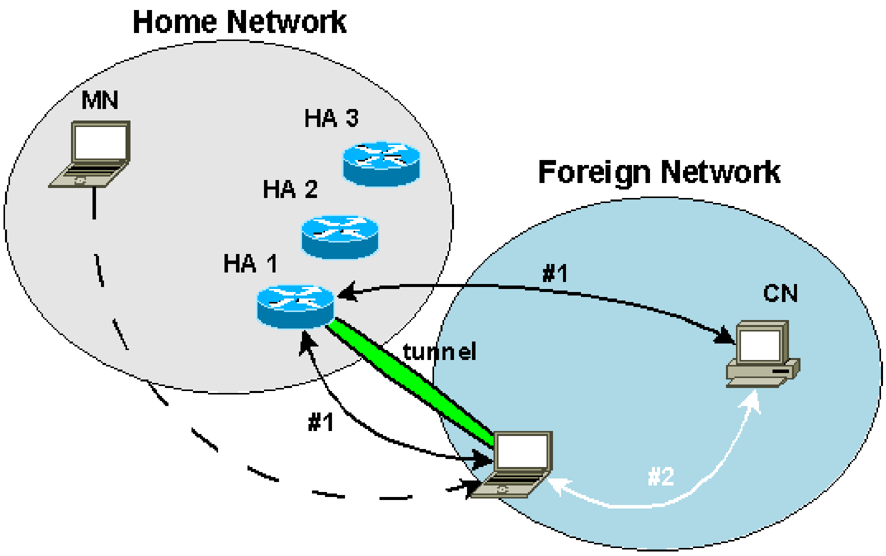


Figure 4.6: MIPv6 Operation

Figure 4.6 highlights MIPv6 operation. While the MN is in its home link, packets addressed to its home address (used as the permanent address of the MN) are routed to the home link of the MN using conventional routing mechanisms.

At a foreign link, the MN is addressable at the Care of Address, which is used as a temporary address while in a foreign link. The CoA is associated with the subnet prefix of a particular foreign link and is obtained using stateless or stateful IPv6 mechanisms. The MN can receive several subnet prefixes, forming diverse CoAs respectively, but the one registered with the Home Agent (HA) is the primary CoA. HA is a router giving assistance to the MN while away from its home network.

After receiving a CoA, the MN performs a binding, an association between the home address and the Care-of Address. The MN registers its CoA with the HA using the binding registration. The MN sends a *Binding Update* message to the HA and the HA replies with a *Binding Acknowledgement* message.

The node with which the MN can communicate is denominated the Correspondent Node and the communication with the CN can be performed in two modes.

- **Bidirectional tunnelling**. This mode does not require MIPv6 support by the CN. Packets from CN are routed to the HA and then tunnelled to the mobile node. Packets to the CN are tunnelled from MN to HA (reverse tunnelled). HA intercepts IPv6 packets addressed to the home address of the MN. This mode corresponds to (#1) as Figure 4.6 exhibits.

- **Route Optimization**. The MN registers its current location at the CN. Packets from CN can be routed directly to the CoA of the MN. This mode has the advantage of using the shortest path and avoids also congestion on the home link of the Mobile Node. This mode is represented by (#2) in Figure 4.6.

It is possible to have more than one HA in the home link, and subnet prefixes may change overtime. MIPv6 defines dynamic home agent address discovery to allow MN to discover IP addresses of HA.

MIPv6 specifies security mechanisms to protect the integrity and authenticity of binding registration messages exchanged between Mobile Node and Home Agent. The Correspondent Node uses the return routability procedure to assure the authenticity of the MN sending the binding registration messages for a route optimization mode. With return routability procedure, the configuration of security associations is not required. This procedure makes CN to send initial messages (Home Address test and Care-of Address test) to the CoA and home address of the MN with keygen tokens. If the MN receives both messages (sent for the different addresses) than the MN is authentic and is not forging the binding registration messages.

MIPv6 defines the mobility header as an extension header of IPv6. This header is used by MIPv6 messages, which are the following:

- **Binding Refresh Request Message**. Message sent to request a MN to update its mobility binding.

- **Home Test Init Message**. Message used to initiate the return routability procedure and is used to test the home address of the MN.

- **Care-of Test Init Message**. Message used to initiate the return routability procedure and is used to test the CoA of the MN.

- **Home Test Message**. Message sent in response to a *Home Test Init* message.

- **Care-of Test Message**. Message sent in response to a *Care-of Test Init* message.

- **Binding Update Message**. Message used to notify other nodes (e.g. HA, CN) of a new binding triggered by the new CoA formation. The message includes information about the home address of the MN, CoA and lifetime for the binding.
- **Binding Acknowledgement Message**. Message employed to acknowledge the reception of the binding update.
- **Binding Error Message**. Message employed by CN to signal an error related to mobility, such as an inappropriate attempt to use home address destination without an existing binding.

MIPv6 defines also modifications to the IPv6 NDP (Narten et al., 1998), which focus on router advertisements procedures, therefore the Router Advertisement (RA) messages include new or modified options such as:

- **Prefix Information**. Option modified to allow routers to advertise their global address instead of link-local address as supported in the standard IPv6 NDP.
- **Advertisement Interval**. Option used to inform the MN about the advertisement interval of unsolicited router advertisement messages.
- **Home Agent Information**. Option related to the HA functionality, such as HA lifetime.

RA messages are used by the Mobile Node to detect movement, thus the detection of movement in a timely fashion determines MIPv6 performance for handovers. MIPv6 decreases the limits of *MinRtrAdvInterval* and *MaxRtrAdvInterval* to allow a router to send unsolicited router advertisements more frequently. The values specified are 0.03 seconds for the *MinRtrAdvInterval* and 0.07 seconds for the *MaxRtrAdvInterval*.

The advertisement lifetime is also reviewed in MIPv6 since the maximum value for *AdvDefaultLifetime* is set to *MaxRtrAdvInterval*. MIPv6 specifies a minimum of one second, to avoid zero values for the lifetime of router advertisements.

4.5 WEIRD - Participation

This subsection highlights the role of the candidate in the WEIRD project.

The participation of the candidate can be summarized according to the different work packages of the project:

- **Work Package 2000**
  - Contribution to the WEIRD architecture definition.
  - WEIRD interfaces specification. Included in the system specification, this task involved the analysis of the signalling processes and the necessary messages exchange between the different modules of the architecture.
  - WEIRD mobility architecture definition. Contributions to the documents addressing mobility were made.
- **Work Package 3000**
  - Software architecture definition. Tasks involving technical documentation to assist the development process.
  - Software modules implementation and testing. For instance, the WEIRD Agent and the NSIS framework modules.
  - Coordination of the development team.
  - Integration of software. The candidate attended to implementation meetings where integration and troubleshooting of software was performed.
- **Work Package 5000**
  - Configuration of equipments and software. Tasks including installation of WEIRD and non-WEIRD software.
  - Preparation of demonstrations and first year audit.
  - Performance tests between the different testbeds.
- **Work Package 6000**
  - Presentation of the WEIRD project.
  - ‘Bridging’ with IETF, namely with the 16ng working group[6]. The candidate has presented the WEIRD project and contributed to the specifications of the 16ng Working Group on behalf of WEIRD.

[6] http://www.ietf.org/html.charters/16ng-charter.html

The WEIRD architecture definition was the very first contribution carried out in the scope of the project. The analysis of the documents involving WiMAX, vendors specifications and related protocols was the base to this contribution. The network reference model, from the WiMAX Forum, exemplifies the complete specification of profiles and network elements necessary to deploy WiMAX. The functions of each entity were investigated to identify the necessary elements to the WEIRD system, in order to make this one compatible, as much as possible, with the network reference model of the WiMAX Forum. When identified the principle entities, the different relations with the QoS-NSLP (Manner et al., 2007) and GIST protocols (Schulzrinne & Hancock, 2007) (protocols integrated in the NSIS framework) was a matter of study. This study included the primitives with the necessary data to make the signalling.

The WEIRD mobility specification includes the micro-mobility supported by IEEE Std 802.16e, as well as the macro-mobility solutions based on MIPv4 and MIPv6. The macro-mobility specification in WEIRD was based on the mobility specifications from WiMAX Forum, covering clients with Mobile IP support, as well as, clients not MIP-aware. The candidate work considered the integration of the specifications from the WiMAX Forum, the Mobile IP protocols into the WEIRD architecture to enable mobility. A study of the Media Independent Handover (MIH) standard was conducted in order to "empower" the mobility convergence layer introduced in the WEIRD architecture.

The link information provided by the MIH standard, like *Link UP*, *Link Down* and *Link Going Down* has been demonstrated and analysed to assist Mobile IP protocols. The message flow associating the MAC management messages from IEEE Std 802.16; the MIH triggers and the management messages of Mobile IPv4 and Mobile IPv6 has demonstrated the relation with these standards and protocols to provide seamless handover support.

In the Mobile Station, different modules were designed to trigger WEIRD reservations. The WEIRD Agent allows the user to make reservations for the different types of traffic, such as voice, video conference and video streaming. The specification of the WEIRD Agent included the internal architecture of the WEIRD Agent and the interface with the CSC_MS, known as WEIRD API. All the interaction with the WEIRD Agent and the overall system was addressed with NSIS signalling. The signalling for a dynamic instauration of a service flow was exhibited in message flows diagrams. Therefore, different scenarios were envisioned in the diagrams, including successful reservations, error situations and non sufficient resources for a reservation such as AAA failure or no WiMAX resources.

The DiffServ mechanisms were also object of study and configuration. Such mechanisms considered the extension of the QoS support in the non-WiMAX segments, for instance between ASN and CSN. Nowadays, many applications do not set the value of the DSCP field in the IP header. The DiffServ mechanisms implemented with Traffic Control (TC)[7], led us to classify the traffic accordingly the recommendations of several entities, for instance the International Telecommunications Union (ITU). The classification mechanism was implemented at the boundaries of the WEIRD domain, SS and CSN.

Other step to realize the WEIRD architecture was the integration of the different software modules developed by the diverse partners of the project. The candidate has been the responsible to manage the team implementing NSIS in WEIRD and other software modules such as the WEIRD Agent.

4.6 Conclusion

WEIRD, by employing the WiMAX technology, fulfils a missing gap to interconnect research networks. The applications assessed in the testbeds have different QoS requirements and WEIRD provides the necessary mechanisms to support the different services explored by such applications.

The WEIRD mobility architecture also adds functionalities to the WEIRD architecture to enable the mobility between different networks.

[7] TC - traffic control, is a Linux QoS control tool (Stanic, 2007)

5
Evaluation of Mobility in WiMAX

The evaluation of mobility in WiMAX, assisted with MIH standard and MIPv6 procedures is presented in this chapter. Mobility evaluation is performed through simulation using the ns-2 simulator installed and configured with the NIST mobility package.

This chapter is organized as follows: Section 5.1 introduces the tool used to perform the evaluation of mobility. Section 5.2 describes the different elements of the mobility scenario. Section 5.3 introduces the parameters used to evaluate the mobility performance of WiMAX. Finally, the discussion of the results of the evaluation of mobility in WiMAX is presented in Section 5.4.

5.1 Introduction

Mobile WiMAX is based on IEEE Std 802.16e (IEEE, 2005a). The WiMAX Forum (WiMAXForum, 2007d) is specifying a complete network architecture for WiMAX deployment. The architecture includes the required elements for the Access Service Network (ASN) and for Connectivity Service Network (CSN) to provide IP connectivity.

The mobility scenario configured for the Network Simulator 2 (ns-2) (NS-2, 2007) includes the mandatory elements of the WiMAX network reference model, namely, the Mobile Station (MS), Base Station (BS) and Access Service Network Gateway (ASN-GW). Since ns-2 does not include, natively, IEEE Std 802.16 features, an extension is used to provide the Medium Access Control (MAC) and physical functionalities of the standard. NIST add-on for ns-2 (Rouil, 2007) combines IEEE Std 802.16 features, IEEE Std 802.21 (IEEE, 2006) functionalities and Mobile IPv6 (Johnson et al., 2004) into a mobility package. Appendix H includes a description of the features supported by the NIST extension. A comparison with other extensions and the reason to choose the NIST extension are also introduced.

5.2 Simulation Setup

This section describes the simulation setup, introducing a description of the mobility scenario and the respective configuration.

5.2.1 Mobility Scenario

This section describes the mobility scenario configured for ns-2.

The simulation scenario, as depicted in Figure 5.1, is based on the WiMAX Forum network architecture (WiMAXForum, 2007b) and includes the following entities:

- **Mobile Station**. Represents a CPE device with an IEEE 802.16 interface.

- **Base Station**. Represents a device that provides the connectivity to the IEEE 802.16 network.

- **Access Service Network gateway**. Represents a device that manages the BSs, and provides IP functions, such as Foreign Agent (FA) in the case of mobile IPv4. In the scenario under study, this node represents a router to which all the BSs are connected.

- **Servers in the Connectivity Service Network network**. Different servers are located in the CSN network, for instance the Authentication, Authorization and Accounting (AAA) and Dynamic Host Configuration Protocol (DHCP) servers. In the scenario under evaluation, the video server and the voice peer node are located in the CSN.

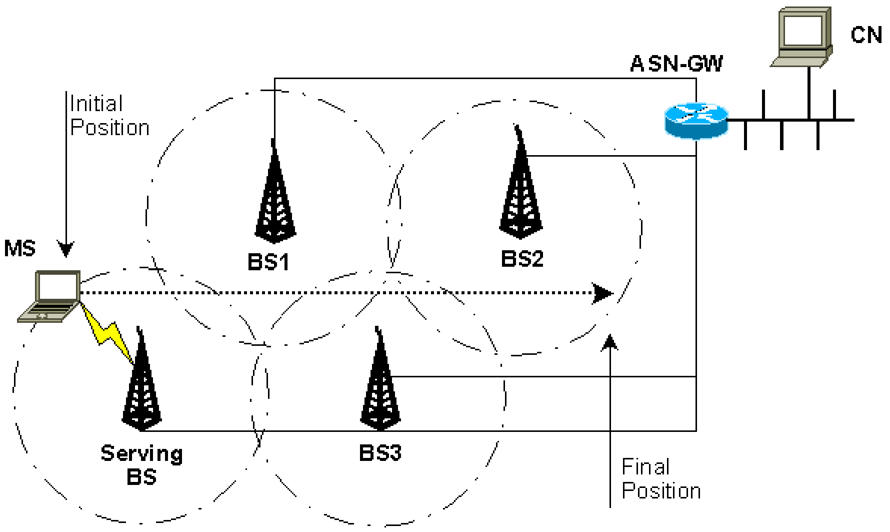


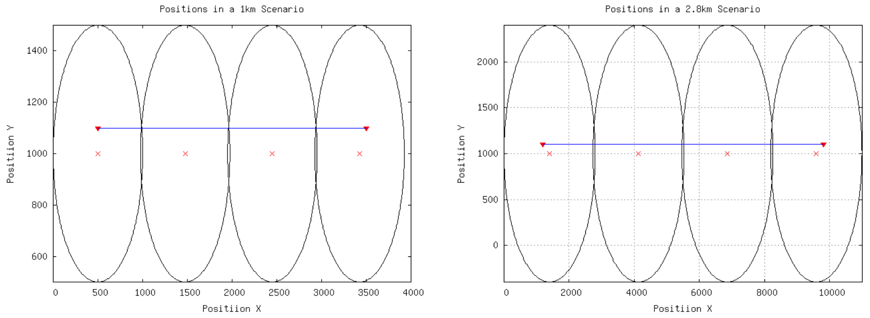
Figure 5.1: Simulation scenario

The BSs are connected to the ASN-GW, representing a domain under the same administrative entity. Under ns-2, each BS represents a different domain for which layer 3 routing and mobile IP procedures are required to assure IP connectivity to the mobile nodes.

The layout of the simulation scenario depends on different factors, the distance between the BS represents the most significative characteristic. Therefore, Figure 5.2(a) and Figure 5.2(b) depict the positions of the MS and the BSs for different scenarios. Such positioning graphics have been built using Octave[1]. The 1km and 2.8km distance between Base Stations are determined to simulate the urban macrocell and the urban microcell, respectively (WiMAXForum, 2006a).

The characteristics of video and voice applications, which are employed to evaluate the mobility performance in WiMAX, are described in Appendix I. The voice traffic includes Constant Bit Rate (CBR) streams with the packetization interval of 20ms and packets with 206bytes. The video traffic is based on real video files in the H.264 format and which are parsed with the tools of the Evalvid framework in order to be used in the simulation process (Klaue et al., 2003).

[1] GNU Octave is a high-level language, primarily intended for numerical computations. It provides a convenient command line interface for solving linear and nonlinear problems numerically, and for performing other numerical experiments using a language that is mostly compatible with Matlab. Source http://www.gnu.org/software/octave/



(a) Positions in the urban microcell scenario (b) Positions in the urban macrocell scenario

Figure 5.2: Layout of the simulation scenarios

5.3 Configuration and Evaluation Parameters

This subsection describes the configured parameters and the items observed in the simulation.

The simulation configuration parameters can be grouped in three categories: Media Independent Handover (MIH) layer, layer 3 and generic parameters. The MIH layer activates or deactivates the use of IEEE Std 802.21 assisting information for handovers. The layer 3 parameters describe the different addressing and Mobile IP mechanisms. The generic parameters include global parameters, such as the distance between the BS and the overlapping areas.

The MIH layer includes the type of handover. The values specified are 1, 2, 3 and correspond to the events being subscribed, with the following meanings: 1- No events and no predictive triggers (e.g. no *Link Down* and no *Link Going Down*); 2- *Link Down* trigger; and 3- *Link Going Down* trigger.

Layer 3 parameters configured in the simulation include the following:

- **Addressing**. Hierarchical addressing schemes supported by ns-2.
- **Router Advertisement (RA) interval**. RA interval is configured with *3s* as in the RFC 2461 Neighbour Discovery Protocol (NDP) (Narten et al., 1998) or configured with *3ms* as recommended on the MIPv6 protocol defined in RFC 3775 (Johnson et al., 2004).

The generic parameters include:

- **Cell Size**. Encompasses the urban macrocell, with 2.8km between BS, and the urban microcell, with less than 1km of distance between BSs.
- **Velocity of the MS**. Consider the different speeds specified in the ITU Vehicular A profile (ETSI, 2003) with velocities of 30 and 120 Km/h.
- **Overlap area coverage**. Two adjacent cells have 5% overlap in the coverage area (Leung et al., 2005). The overlapping areas are employed to avoid non covered areas and to improve the handover performance.

Table 5.1 summarizes the values for different parameters used in the tests.

Speed of MS	**BS Distance**	**MIH Level of Confidence**	**RA interval (NDP or MIPv6)**	**MIH Scenario case**
30	1 km / 2.8 km	60% / 80%	0 (NDP) / 1 (MIPv6)	1 / 2 / 3
120	1 km / 2.8 km	60% / 80%	0 (NDP) / 1 (MIPv6)	1 / 2 / 3

Table 5.1: Simulation Settings

To determine voice quality, different features are evaluated from the ns-2 trace files. These evaluation features include:

- **Packet Loss Ratio (PLR)**. Evaluates the number of packets lost during the simulation and is measured according to Equation 5.1.

$$PLR = \frac{Number of packets received in the MN}{Number of Packets generated in the CN} \tag{5.1}$$

- **One way delay**. Propagation time of a packet from the source to the destination. This parameter is determined as recommended by IP Performance Metrics (IPPM) group[2] in RFC 2679 (Almes et al., 1999a).
- **Jitter**. Jitter corresponds to the variation of delay on the transmission of consecutive packets. Jitter is determined as recommended by IPPM in RFC 3393 (Demichelis & Chimento, 2002) and as referenced in Equation 5.2, where *T1* represents the instant when it is send the first packet and *T2* represents when the second packet is sent.

$$Jitter = DelayT2 - DelayT1 \tag{5.2}$$

[2] IPPM is an IETF working group devoted to the metrics applied to quality, performance and reliability of Internet data delivery services. *http://www.ietf.org/html.charters/ippm-charter.html.

- **Throughput**. Throughput of the received packets at the mobile node during the simulation.

The quality of video is evaluated based on the Evalvid framework. The following metrics can be gathered by Evalvid tools:

- **Packet/Frame loss**.
- **Delay and Jitter**. These parameters are determined based on probabilistic values of Probability Distribution Function (PDF) or Cumulative Distribution Function (CDF).
- **Peak Signal Noise to Ratio (PSNR)**. Compares the maximum possible signal energy to the noise.
- **Mean Opinion Score (MOS)**. The 5-point scale for user perceived video quality.

The next section discusses the simulation results.

5.4 WiMAX Mobility Evaluation

This section presents the results achieved in the WiMAX mobility evaluation using video and voice traffic.

Results are presented and compared for the two major scenarios, 1km and 2.8km, as well as for the velocities of 30Km/h and 120Km/h.

5.4.1 Voice Tests

This subsection provides and comments the simulation results of the voice applications achieved in the simulation.

The test cases are identified by the velocity (30Km/h or 120Km/h) and by the Router Advertisements (according to NDP or MIPv6) configured. For instance, the *30kmh_NDP* case represents a test configured with 30Km/h and with Router Advertisements distributed in intervals of 3s. The tests are also identified by the use of the MIH information. The *NoEvents* cases correspond to the test cases configured without MIH information, while the *LinkDown* cases correspond to the test cases using *Link Down* triggers, and the *LinkGDown* cases comprise test cases using predictive information, such as *Link Going Down* trigger. The last test cases, have a confidence level associated, namely 60% and 80%.

Test Case	**BS Distance**	**Packet Loss**
30kmh_NDP	1km	**70.55%**
30kmh_MIPv6	1km	**0.75%**
120kmh_NDP	1km	**3.40%**
120kmh_MIPv6	1km	**15.28%**
30kmh_NDP	2.8km	**21.84%**
30kmh_MIPv6	2.8km	**0.67%**
120kmh_NDP	2.8km	**55.41%**
120kmh_MIPv6	2.8km	**0.89%**

Table 5.2: Packet loss of test cases with a confidence level of 80% (*LinkGDown*)

Table 5.2 depicts the values of packet loss with a confidence level of 80%, while Figure 5.3 and Figure 5.4 depict packet loss for test cases with a confidence level of 60% for urban microcell and urban macrocell, respectively. The test cases with the highest packet loss ratio correspond to the tests configured with the NDP sets (router advertisements in intervals of 3s) and with the tests that do not use the assisting information of MIH (identified in the graphics with *NoEvents* term).

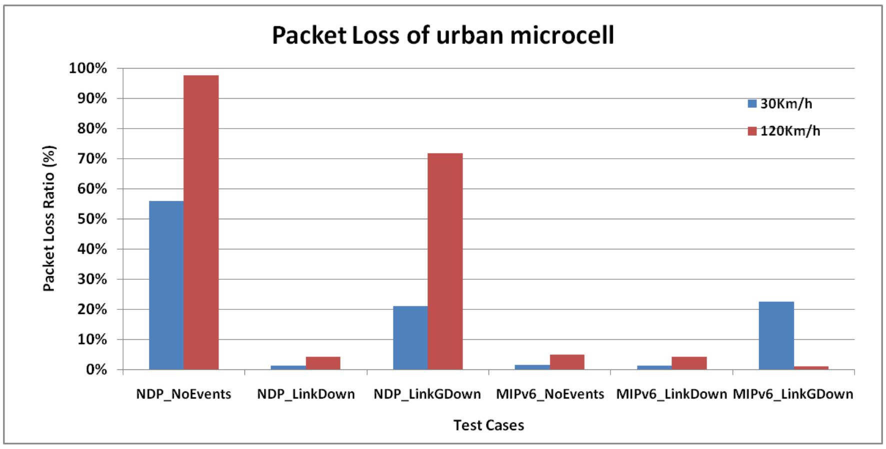


Figure 5.3: Packet loss of urban microcell scenario with a confidence level of 60%

In the *LinkDown* test cases, the packet loss ratio is reduced since the mobile node detects a new link immediately after handover and sends a Router Solicita-

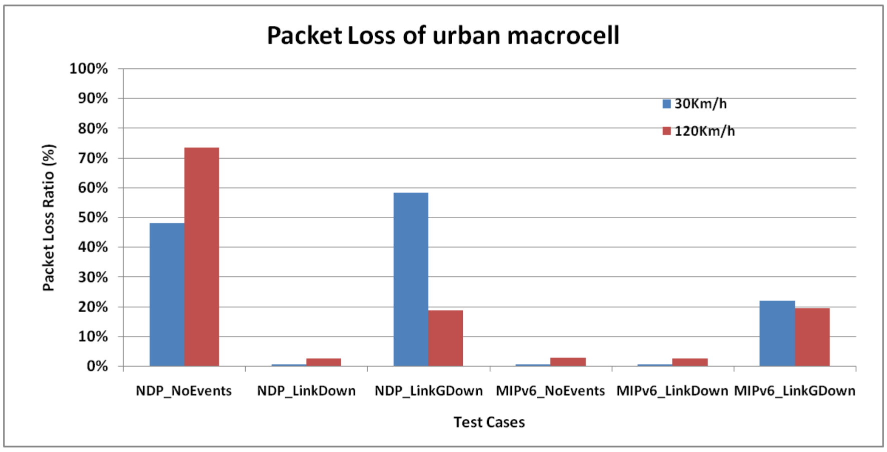


Figure 5.4: Packet loss of urban macrocell scenario with a confidence level of 60%

tion. Such functionality does not happen when MIH triggers are not used since the mobile node relies on the router advertisement messages to detect movement. And if the router advertisement interval is set too high (3s) the detection of movement is low and not accurate. For instance, with high velocities (120Km/h) the mobile node moves too fast without being able to detect a new link in a timely fashion, thus preventing IP connectivity.

The performance of *Link Down* test cases, in terms of packet loss, is the best when compared to the *Link Going Down* test cases (*LinkGDown*). The main difference between these cases is that *Link Going Down* test cases are based on predictive information associated with a certain level of confidence expressing that within a certain amount of time the link will go down (for instance due to loss of signal quality). NIST add-on fakes a link down as the level confidence (60% or 80%) is achieved, causing a variation in the delay, since the mobile node is scanning the network to determine neighbours and a possible target BS. The mobile node only performs handover when it receives a reply to the scans performed. While scanning, packets are buffered at the serving BS (configured a maximum of 50 packets). However, if the scan takes too long, packets are lost due to buffer overflows. Figure 5.5 and Figure 5.6 detail the values of delay during handover, for the urban microcell and urban macrocell test cases, respectively. The fluctuation of delay occurs only on the predictive test cases.

One way delay during non handover instants, when connected to a BS without disruption, is around 4ms. The difference, in terms of delay, between the several test cases is on the handover moments. For instance, Figure 5.7 shows the vari-

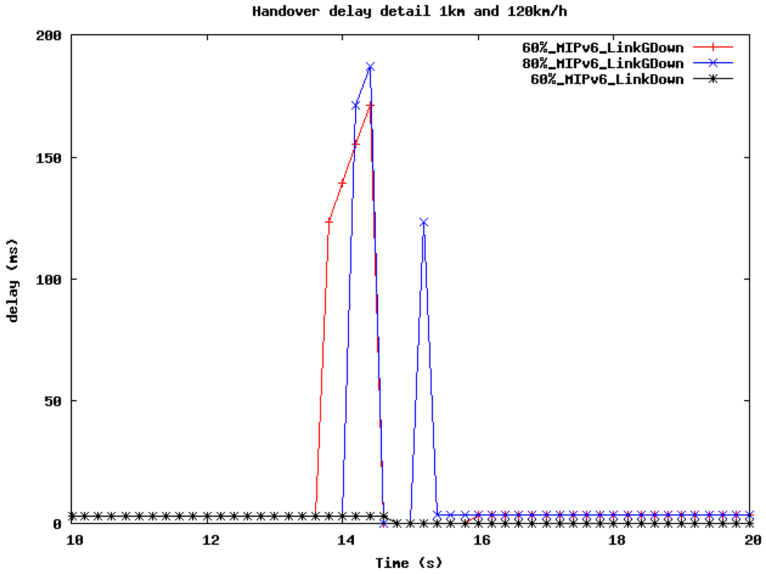


Figure 5.5: Delay during handover (distance 1km, velocity 120km/h)

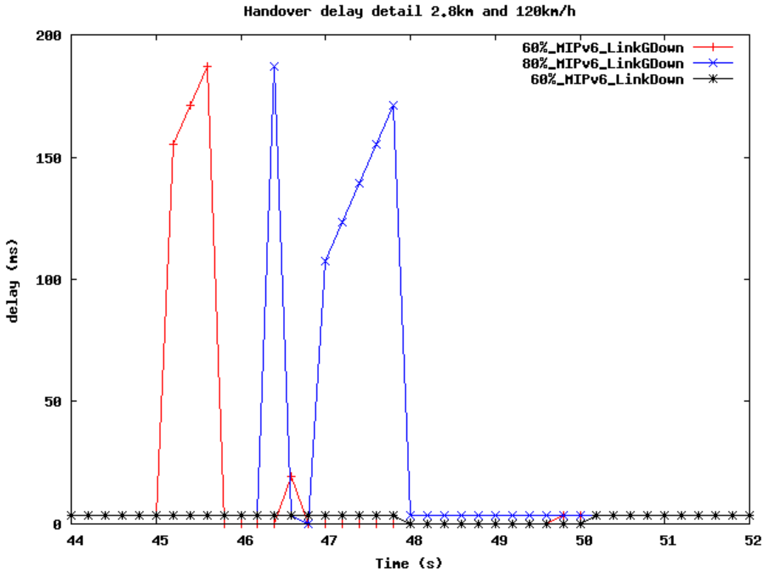


Figure 5.6: Delay during handover (distance 2.8km, velocity 120kmh)

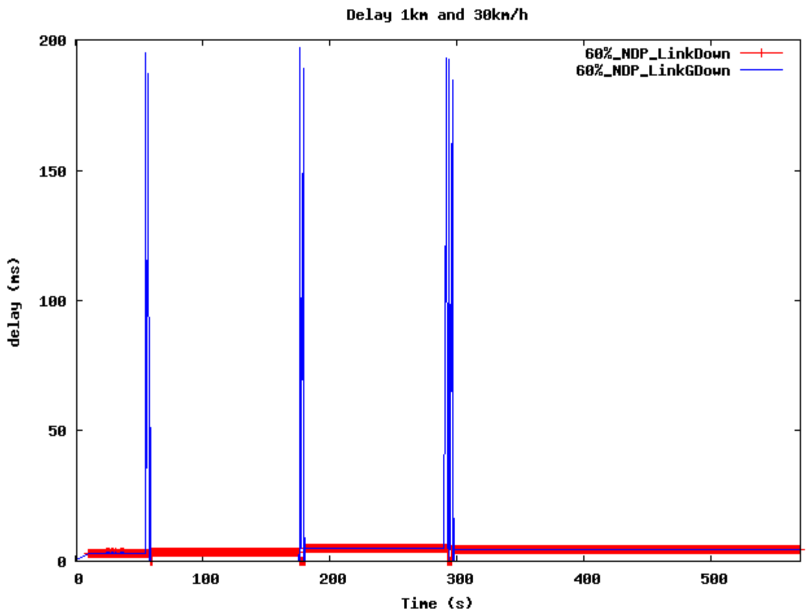


Figure 5.7: Delay during simulation

ation of delay during the simulation time. The delay in the *Link Down* trigger case varies between 0 and 6ms, while the *Link Going Down* case can reach almost 200ms during the predictive moments of a handover.

High values of delay occur in the predictive test cases and the variation of delay in these cases depends on the confidence level configured. For instance, within the test cases with a confidence level of 60% delay achieves high values sooner since the level of confidence is low. This delay is due to the buffering of packets at the serving BS and scanning activities of the MN.

Throughput is around 1030bytes/s during the periods when the Mobile Station is connected to a BS and receiving traffic. The achieved throughput is due to the characteristics of the CBR traffic that was configured with the G.711 parameters. Which include 20ms of packetization interval and packets with 206bytes (contains WiMAX frame header plus IP, UDP and RTP headers and G.711 codec data).

5.4.2 Video Tests

This subsection presents video performance in mobile WiMAX assisted with the MIH protocol for seamless handovers. All the results are based on the measurements performed by the Evalvid framework tools.

The test cases use the same identification nomenclature as the voice tests. For instance, the *60%_NDP_NoEvents* case correspond to a test case configured with a confidence level of 60%, with the Router Advertisements in intervals of 3s as in NDP and does not use the assisting information of MIH standard (*NoEvents*).

(a) Distance 1km, velocity 30Km/h

Test Case	**MOS**
60%_NDP_NoEvents	**1.64**
60%_NDP_LinkDown	**3.59**
60%_NDP_LinkGDown	**3.53**
60%_MIPv6_NoEvents	**3.58**
60%_MIPv6_LinkDown	**3.59**
60%_MIPv6_LinkGDown	**2.58**
80%_NDP_LinkGDown	**3.58**
80%_MIPv6_LinkGDown	**3.56**

(b) Distance 1km, velocity 120Km/h

Test Case	**MOS**
60%_NDP_NoEvents	**1.47**
60%_NDP_LinkDown	**3.38**
60%_NDP_LinkGDown	**2.51**
60%_MIPv6_NoEvents	**3.36**
60%_MIPv6_LinkDown	**3.38**
60%_MIPv6_LinkGDown	**3.38**
80%_NDP_LinkGDown	**2.53**
80%_MIPv6_LinkGDown	**2.75**

(c) Distance 2.8km, velocity 30Km/h

Test Case	**MOS**
60%_NDP_NoEvents	**2.70**
60%_NDP_LinkDown	**4.38**
60%_NDP_LinkGDown	**4.26**
60%_MIPv6_NoEvents	**4.38**
60%_MIPv6_LinkDown	**4.38**
60%_MIPv6_LinkGDown	**3.48**
80%_NDP_LinkGDown	**4.35**
80%_MIPv6_LinkGDown	**4.34**

(d) Distance 2.8km, velocity 120Km/h

Test Case	**MOS**
60%_NDP_NoEvents	**2.04**
60%_NDP_LinkDown	**3.98**
60%_NDP_LinkGDown	**3.92**
60%_MIPv6_NoEvents	**3.98**
60%_MIPv6_LinkDown	**3.98**
60%_MIPv6_LinkGDown	**2.53**
80%_NDP_LinkGDown	**3.96**
80%_MIPv6_LinkGDown	**3.98**

Table 5.3: MOS of Video Highway

The Mean Opinion Score, with the 5-point scale is used to determine the user perceived video quality. With the Evalvid tools, MOS is determined by comparing the PSNR of the transmitted video with the PSNR of the original video file, which is used as reference.

Table 5.3 depicts the MOS classification of the highway video for 1km and 2.8km scenarios. The test cases without the MIH triggers and with the configured sets of NDP have the worst classification, in all the scenarios. The average MOS classification in these test cases is around 2 points, which corresponds to a very annoying video quality.

The predictive cases (*Link Going Down*) underperform when compared to *Link*

Down cases. The predictive test cases can 'infer' packet loss during the handover and during the scanning activities of MS, since NIST add-on fakes a *Link Down* trigger when the level of confidence is achieved.

(a) Distance 1km, velocity 30Km/h

Test Case	**Loss**
60%_NDP_NoEvents	**83.77%**
60%_NDP_LinkDown	**3.43%**
60%_NDP_LinkGDown	**34.64%**
60%_MIPv6_NoEvents	**3.62%**
60%_MIPv6_LinkDown	**3.44%**
60%_MIPv6_LinkGDown	**32.00%**
80%_NDP_LinkGDown	**33.25%**
80%_MIPv6_LinkGDown	**33.59%**

(b) Distance 1km, velocity 120Km/h

Test Case	**Loss**
60%_NDP_NoEvents	**96.68%**
60%_NDP_LinkDown	**5.62%**
60%_NDP_LinkGDown	**64.51%**
60%_MIPv6_NoEvents	**6.78%**
60%_MIPv6_LinkDown	**5.64%**
60%_MIPv6_LinkGDown	**4.88%**
80%_NDP_LinkGDown	**44.28%**
80%_MIPv6_LinkGDown	**19.80%**

(c) Distance 2.8km, velocity 30Km/h

Test Case	**Loss**
60%_NDP_NoEvents	**55.57%**
60%_NDP_LinkDown	**1.08%**
60%_NDP_LinkGDown	**2.84%**
60%_MIPv6_NoEvents	**1.30%**
60%_MIPv6_LinkDown	**1.08%**
60%_MIPv6_LinkGDown	**57.90%**
80%_NDP_LinkGDown	**1.16%**
80%_MIPv6_LinkGDown	**1.16%**

(d) Distance 2.8km, velocity 120Km/h

Test Case	**Loss**
60%_NDP_NoEvents	**74.75%**
60%_NDP_LinkDown	**5.10%**
60%_NDP_LinkGDown	**4.09%**
60%_MIPv6_NoEvents	**5.57%**
60%_MIPv6_LinkDown	**5.07%**
60%_MIPv6_LinkGDown	**54.54%**
80%_NDP_LinkGDown	**24.64%**
80%_MIPv6_LinkGDown	**1.44%**

Table 5.4: Video Highway Packet Loss

Table 5.4 depict the packet loss for 1km and 2.8km test cases. The test cases without MIH and with Router Advertisements configured in intervals of 3s have the worst performance in terms of packet loss. The packet loss increases with velocity. This behaviour stems from the dependency of the movement detection from the Router Advertisements on the new link. Therefore, if the frequency of the Router Advertisements is low, a high packet loss will occur.

In the 2.8km test cases, packet loss ratio is lower than in the 1km test cases. In these test cases, the *LinkGDown* test cases with the highest confidence level have the best performance. This is due to the fact that the scanning activities of the Mobile Node occur faster than in the test cases with a lower confidence level, and therefore the probability of packet loss is decreased.

The delay in the Evalvid framework is determined based on probabilistic values calculated by the PDF or by the CDF for cumulative values. Figure 5.8 and Figure 5.9 compare the delay determined by the PDF for the different confidence levels in the 1km and 2.8km scenarios. Values with 0 ms correspond to lost packets, which are lost during handovers. The delay values, as determined by the PDF, can vary in the interval between 3ms and 18ms. In the 1km scenario there is not a clear distinction between the different MIH confidence level tests, delay in 3-18ms interval has almost 5% of probability for each value inside the interval.

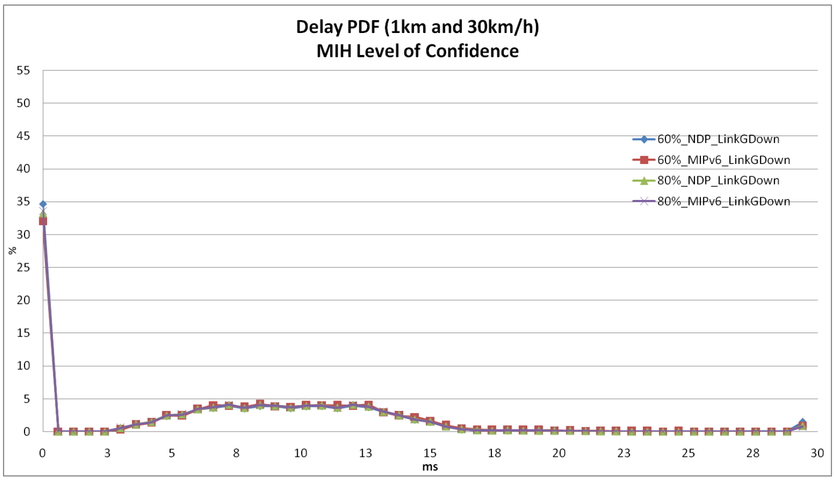


Figure 5.8: Delay determined by PDF for the 1km scenario

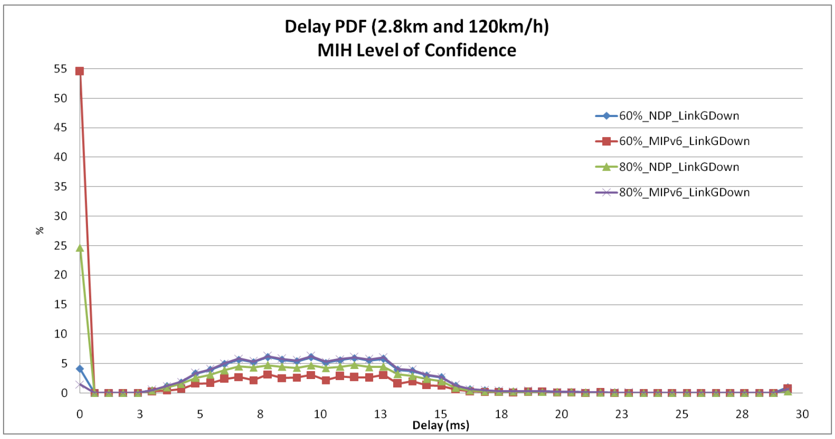


Figure 5.9: Delay determined by PDF for the 2.8km scenario

In the 2.8km scenarios there is a distinction between the different confidence levels of the *Link Going Down* test cases. Delay has a probability about 5% for values inside the 3-18ms interval, nevertheless with a confidence level of 80% and with MIPv6 Router Advertisements test cases, the probability is above 5%. These results mean that the delay, in these cases, has a stronger probability of varying between 3 and 18ms.

5.5 Conclusion

This section summarizes the conclusions for the evaluation of voice and video applications in mobile WiMAX scenario.

Voice quality is determined by packet loss and one way delay measurements between the source and the destination. The packet loss, as verified in all the tests, is due to the handovers at the link and IP layers. When the Mobile Station is connected to a Base Station without service disruption there is no packet loss. The one way delay is around 4ms, despite the fluctuation in the handovers. The one way delay measured is bellow 150ms, as recommended by ITU in the G.114 recommendation (ITU-T, 2003) for voice conversations. In the predictive cases this handover exceeds the 150ms limit and reaches values around 200ms, which is also bellow the 400ms maximum limit specified in the ITU G.114 recommendation. In the remaining cases, without MIH configured and *Link Down*, the delay varies between values of 0 and 6ms.

The packet loss is the main feature influencing voice quality. The 0.1% of packet loss recommended for Classes 0 and 1 in the Y.1541 recommendation[3] (ITU-T, 2006) is not verified. The most performant cases, *Link Down* configured with MIPv6 Router Advertisements, have a packet loss ratio around 1%, which is very low when compared to other cases with high packet losses (cases without MIH information).

The velocity has also an impact in the packet loss ratios, since in both main scenarios (1km and 2.8km) packet loss ratios are greater with higher vehicular speeds (120Kmh).

In the cases where the packet loss is moderate, the video quality is medium and not questionable. Nevertheless, in all the cases the handover moment is perceptible, the effect in the final video quality is different depending on the handover duration time. Figure 5.10 shows the video in the handover moment of a *Link Down* test case, since the packet loss is small, the video is perceptible despite the

[3] The Classes 0 and 1 of the Y.1541 recommendation characterize voice and video traffic.

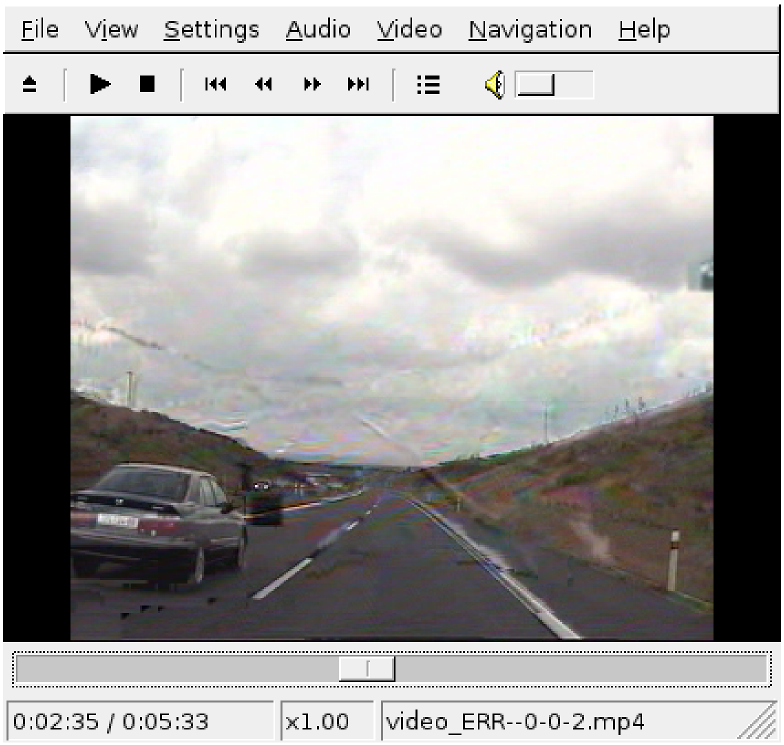


Figure 5.10: Image of the video transmitted in a Link Down test case

‘refresh problem’.

In other cases there is a clear identification of packet loss, since there is an interruption in the video, which can be detected by the user. In the test cases without MIH and with the Router Advertisements configured as in NDP, these interruption times take an excessive amount of time, lasting at least 3s in some cases.

In the predictive cases the handovers are identified by missing frames in the image, Figure 5.11 depicts such example. In this case the ‘slogans’ in the bridge and some parts of the brigde are not perceptible, such fact makes the video quality annoying and questionable.

Mobile WiMAX seems to support vehicular speeds providing adequate throughput rates to video and voice applications. The handover impact in voice and video quality does not depend solely in the handover at layer 2, but relies also on layer 2.5 information (if MIH is employed) and IP information such as Mobile IP facilities.

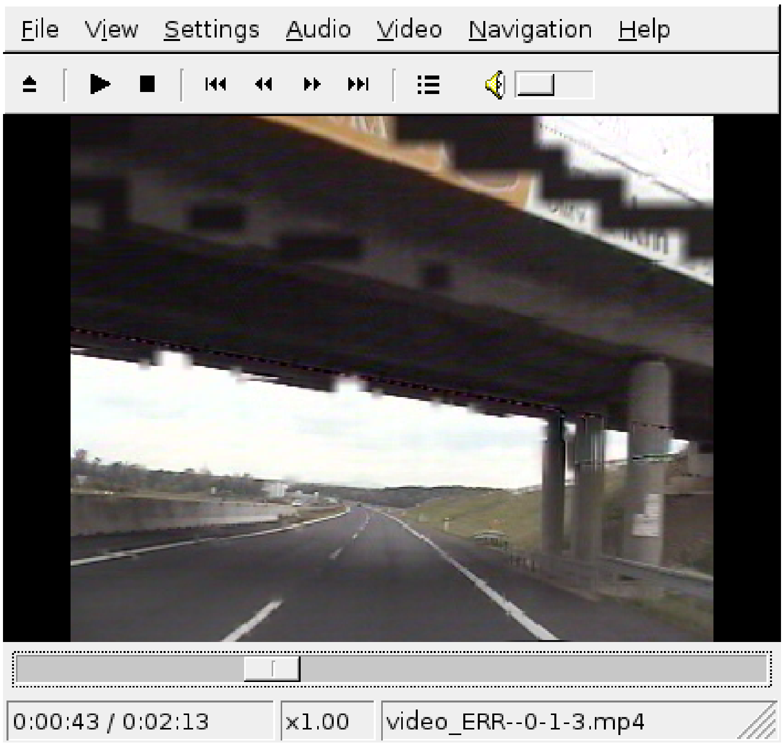


Figure 5.11: Image of the video transmitted in a Link Going Down test case

A correct configuration of the system is important, for instance, the Router Advertisement interval determines the performance in terms of IP handover, IPv6 aware nodes rely on such periodic messages to detect new links and configure the new prefix accordingly. If prefixes are not announced frequently, IPv6 nodes may not be-aware of the new link.

The MIH standard is important, since the detection of movement is not only performed via IP messages (Router Advertisements), but is done more precisely with link layer data. Although not verified in the tests, predictive triggers enable a MIH user to perform seamless handovers (e.g. *make-before-break* approach) since the predictive information allows the MIH user to prepare for handover, for instance to scan for neighbours to collect L2 information and IP prefixes of the possible targets while still connected to the serving Base Station.

6
Evaluation of QoS in WiMAX

The evaluation of Quality of Service depicted in this chapter includes the evaluation of signalling protocols and the experimentation of voice and video applications in WiMAX links.

Section 6.1 describes the different sets of tests and the respective conditions. Section 6.2 introduces the evaluation of WEIRD, namely the NSIS framework protocols. The Section 6.3 depicts the behaviour of video and voice applications in WiMAX links with and without the QoS support.

6.1 Tests Description

This section introduces the testbed layout and the configured parameters for the different tests performed.

6.1.1 Testbed Layout

This subsection presents the layout of the testbeds for the tests assessing the performance of the WEIRD signalling protocols, as well as the performance of voice and video applications in WiMAX.

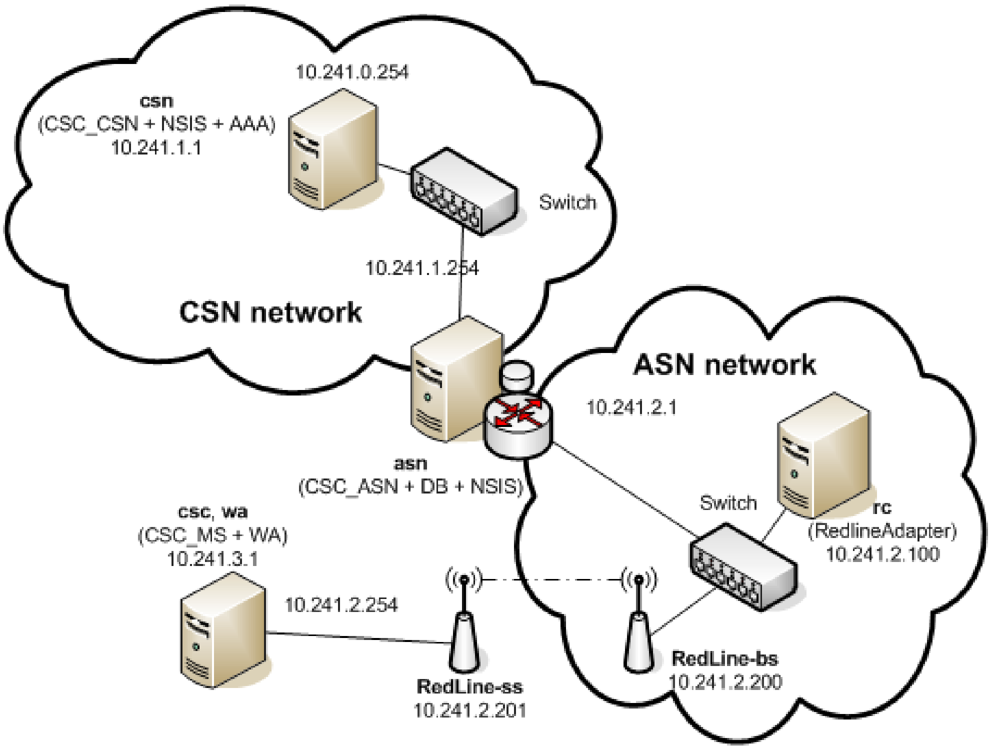


Figure 6.1: WEIRD testbed

WEIRD Signalling Protocols Testbed

The tests with the signalling protocols were performed in a testbed of WiMAX Extension to Isolated Research Network (WEIRD). The testbed layout is depicted in Figure 6.1.

The tests with the WEIRD signalling protocols are performed between the Mobile Station (MS) and the Connectivity Service Network (CSN), bidirectionally. This means, the reservations are triggered in the MS by the Weird Agent, for downlink traffic (from the CSN towards the MS) and uplink traffic (from the MS towards the CSN). The CSN represents the end of the signalling path, while the Access Service Network Gateway (ASN-GW) is the node controlling the WiMAX resources.

The signalling is performed between the MS and the CSN, traversing the ASN-GW and the signalling path has the following characteristics:

- **MS-ASN**. WiMAX link, powered by a Redline RedMAX AN-100U Base Station (BS) (Communications, 2006a) and a Redline RedMAX Subscriber

Unit - outdoors (Communications, 2006b). This link has a default bandwidth of 1.20Mbytes[1].

- **ASN-CSN**. Ethernet link.

The next subsection details the testbed for the voice and video applications.

Voice and Video Applications Testbed

The tests of the voice and video applications use the same WiMAX hardware as the tests with the signalling protocols. The testbed layout for the evaluation of voice and video applications is different from the WEIRD signalling protocols due to the need of synchronization between the sender and the receiver.

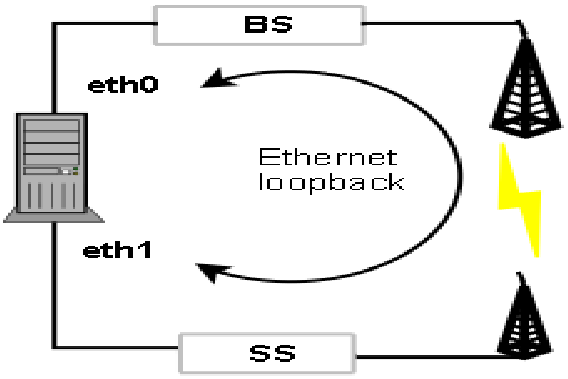


Figure 6.2: Deployment of the testbed for voice and video evaluation

Figure 6.2 depicts the testbed layout employed to measure the performance of voice and video applications. This testbed is based on a Ethernet loopback which requires a Linux patched kernel[2].

6.1.2 General Parameters Description

This subsection describes the general parameters that were configured for the tests. Subsection 6.2.1 describes the evaluated parameters for the WEIRD signalling protocols tests, while Subsection 6.3.1 describes the parameters evaluated to

[1] With the best modulation scheme it is possible to have 2.9Mbytes for downlink and 2.9Mbytes for uplink

[2] The Linux 2.6.22 kernel was patched with the self-to-self patch (Anastasov, 2007).

asses voice and video performance.

Table 6.1 describes the physical parameters, like Radio Frequency (RF) for the Downlink (DL) channel, which were configured once for all the tests. The physical parameters are outside the scope of the evaluation and have been configured according to the output from the tests performed during the project.

Description	**Value**
RF DL Channel [KHz]	3488000
Tx Output Power	0
Channel size	7 MHz
Cyclic Prefix	1/16

Table 6.1: Physical parameters configured

The general Medium Access Control (MAC) layer parameters are depicted in Table 6.2.

Description	**Value**
Frame Duration [ms]	10
DL Ratio [%]	56
Synchronization Mode	No Synch
Cell Range [Km]	5

Table 6.2: MAC parameters configured

To achieve more accuracy in the results of the tests performed, each test included three runs.[3]

6.2 Evaluation of WEIRD Signalling Protocols

This section introduces the protocols and the WEIRD software modules under evaluation.

The goal of the tests described is to evaluate the protocols of the Next Steps in Signalling (NSIS) framework, which include QoS-NSIS Signalling Layer Protocol (NSLP) (Manner et al., 2007), QoS-NSLP authentication (Manner et al., 2007) and General Internet Signaling Transport (GIST) (Schulzrinne & Hancock, 2007).

[3] To achieve 95% of confidence each test must include hundreds of runs. Such recommendation is done by the IP Performance Metrics (IPPM) group in RFC 2681 (Almes et al., 1999b) and RFC 2679 (Almes et al., 1999a). The IPPM is an IETF working group devoted to the metrics applied to quality, performance and reliability of Internet data delivery services. *http://www.ietf.org/html.charters/ippm-charter.html.

The results were obtained with the specification of version 11 [4].

QoS-NSLP interacts with the Resource Management Function (RMF), represented by the Connectivity Service Controller (CSC) modules, in the WEIRD architecture (WEIRDConsurtium, 2007). The performance of the CSC modules is also evaluated to assess the performance of the end-to-end reservation process.

6.2.1 Tests Specification

The performance of the QoS signalling protocols is evaluated for an increasing number of reservations. Table 6.3 depicts the number of reservations and their respective characteristics, while Table 6.4 summarizes all the evaluated parameters per protocol.

N. Reservations	**Characteristics**
2	DL 9 Mbytes / UL 9 Mbytes
32	DL 36.6 Kbytes / UL 36.6 Kbytes
64	DL 18.3 Kbytes / UL 18.3 Kbytes
256	DL 4 Kbytes / UL 4 Kbytes

Table 6.3: General characteristics of reservation

In the NSIS perspective, all the reservations were Sender-initiated with the MS acting as the data sender and the CSN as the receiver. The downlink reservations perform an exchange between source IP and destination IP to allow downlink classifiers to classify packets addressed to the MS.

Also, a pre-configured service flow with 0.1Mbytes for downlink and 0.1Mbytes for uplink was used with the Best Effort (BE) scheduling service, to allow all the transport of the signalling messages over WiMAX.

6.2.2 Quality of Service NSLP Performance

This subsection describes the QoS-NSLP and the Resource Management Function performance results.

[4] QoS-NSLP version 15, QSPEC version 18, GIST version 14 at 02 of November 2007

Protocol	Description
GIST	1. Message Association time. 2. Receiving messages from NSLP. 3. GIST internal processing (e.g. decision of tranport mode). 4. Sending messages to peer GIST.
QoS-NSLP	1. Processing time of *RESERVE* messages. 2. Processing time of *QUERY* messages. 3. Processing time of *RESPONSE* messages. 4. Processing time of *NOTIFY* messages.
QoS-NSLP AUTH	1. Processing authentication time of *QUERY* messages. 2. Processing authentication time of *RESERVE* messages.

Table 6.4: Evaluated parameters

QoS-NSLP deals with application signalling, and has a northbound interface (RMF interface) with the CSC modules and a southbound interface with GIST. The processing in each QoS-NSLP aware node includes two main features. The first, is message parsing (*QUERY*, *RESERVE*, and *RESPONSE*), needed to request to the CSC the policy and admission control functions. The second, concerns state maintenance, in order to verify if reservations should be refreshed. Figure 6.3 depicts the processing time of QoS-NSLP, Authentication, Authorization and Accounting (AAA) and RMF. The results show that the processing time increases with the number of reservations, due to the amount of reservations states, as well as the processing load needed to handle signalling messages. For instance, the single QoS-NSLP processing for 2 reservations presents a low value, approximately 83ms, which increases to 105ms in the case of 256 reservations.

QoS-NSLP AUTH adds extensions to QoS-NSLP to allow the authentication of *QUERY* and *RESERVE* messages. The *QUERY* messages are authenticated based on a trust relation between CSC and QoS-NSLP, whereas the *RESERVE* messages require AAA authentication (included in the QoSNSLP+RMF+AAA item) since the grant of resources needs user authentication and authorization.

Therefore, when QoS-NSLP receives a *QUERY* message, the message is sent back to the RMF in order to be authenticated. The impact of using AAA functions,

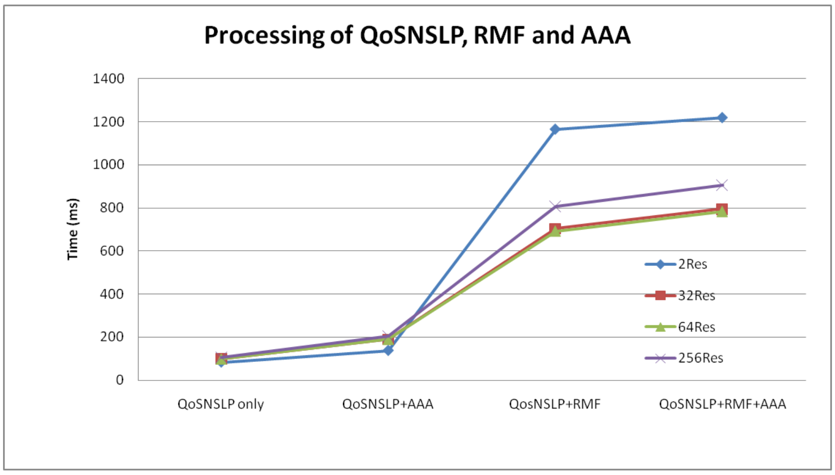


Figure 6.3: Performance of QoS-NSLP, RMF and AAA

both with QoS-NSLP alone (QoSNSLP+AAA), and with QoS-NSLP plus RMF functions (QoSNLP+RMF+AAA) is also illustrated. For instance, the QoS-NSLP processing time is 83ms while the processing time including AAA functions is 137ms.

Regarding the number of reservations, the processing time of QoS-NSLP is minimum when compared to the RMF processing time. The average values of the processing time of QoS-NSLP and RMF include the processing in all the functional entities of the WEIRD architecture, namely the MS, the ASN and the CSN. The 2 reservations case represents the worst performance case due to the necessary setup of sessions in the RMF. The remaining cases have an higher performance since the session is already established.

6.2.3 GIST Performance

This subsection presents GIST performance over WiMAX and Ethernet segments.

GIST provides the transport mechanisms for the applications signalling. The main processing roles of GIST are to handle QoS-NSLP messages (for instance, to decode the Message Routing Information (MRI) in order to create the association with the next GIST-peer), to perform state management and to decide the transport mode (for instance, C-Mode, if guarantees are needed).

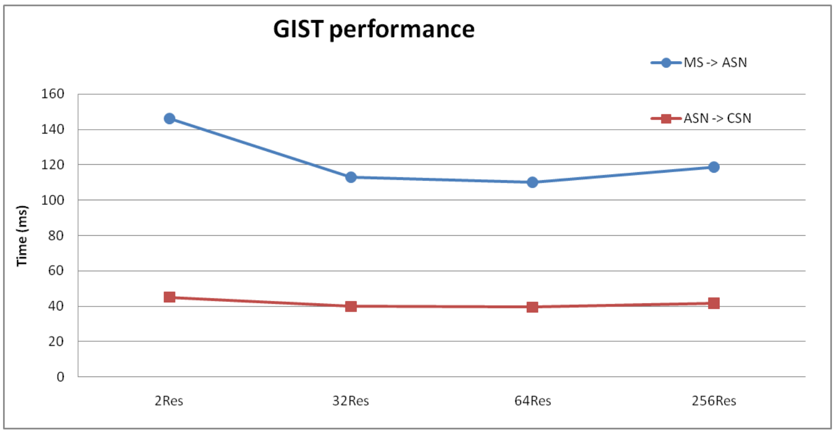


Figure 6.4: GIST performance in different network segments

Figure 6.4 depicts the comparison of GIST processing time in the WiMAX segment (between MS and ASN) and in the Ethernet Segment (between ASN and CSN). GIST establishes associations with peers that are GIST aware and that are in the data path. Therefore GIST in the MS associates with GIST in the ASN and than the ASN associates with the CSN. The values measured include association time, time required to transport QoS-NSLP data messages, and decision on the transport mode, according to the message received and the session state.

When there are 2 reservations only, the processing time is higher, approximately 146ms in the MS-ASN segment since such processing includes the message association setup between GIST peers.

GIST processing time increases slightly with the number of reservations, for instance, with 256 reservations cases the GIST processing time is approximately 118ms while in the 64 reservations cases, the GIST processing time is around 110ms.

The difference found between MS-ASN (line with dots) and ASN-CSN (line with squares) segments result from the delay introduced by the WiMAX air link on the former case.

6.2.4 Overall Assessment

This subsection highlights the conclusions achieved with tests of the WEIRD signalling protocols.

The evaluation of the WEIRD signalling protocols was done in association with the related modules, namely, the CSC_MS, CSC_ASN, CSC_CSN, the Resource Controller (RC) and the Redline adpater. For instance, the CSCs act as the RMF for QoS-NSLP while the Resource Controller manages the service flow creation through adapters that communicate with WiMAX equipment via Simple Network Management Protocol (SNMP).

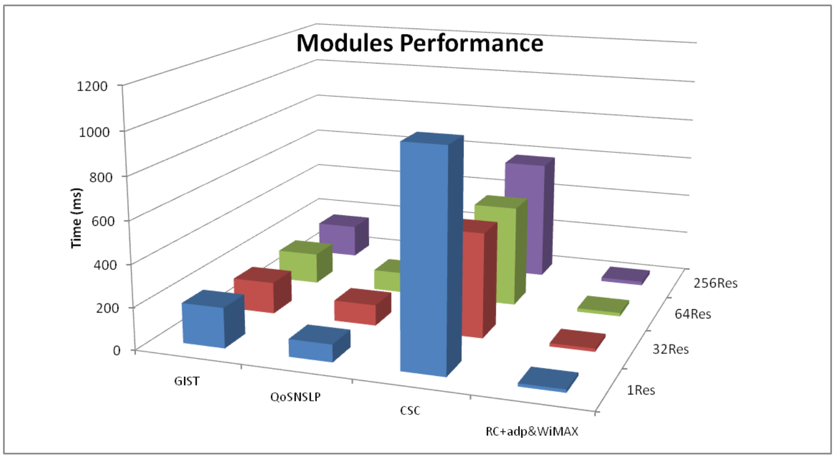


Figure 6.5: Performance of the signalling modules

Figure 6.5 depicts the performance of each software component, which leads to the conclusion that the processing overhead introduced by the CSC modules has the highest impact in the reservation process. For instance, in the 32 reservations case the total processing time of CSC_MS, CSC_ASN and CSC_CSN is around 500ms. GIST is the second software component to introduce more overhead. The necessary message setup association and state maintenance for routing QoS-NSLP data messages justifies the GIST performance values.

Another important aspect that differentiates the modules performance is the coding language. All the modules are coded in JAVA with the exception of RC and adapters. The functionalities performed by each software module is also a criteria affecting the performance. For instance, the processing time of the CSCs is higher when compared to the remaining modules, since the CSCs perform several functionalities such as admission control, session management, policy control, QoS specification (QSPEC) serialization and deserialization and MRI serialization.

The performance of GIST in WEIRD is inline with the GIST implementation of the University of G*ö*ttingen (Fu et al., 2006). This implementation of GIST in C++ presents a performance time around 26ms, including message association re-use and message processing, while the implementation of GIST in WEIRD is around 40ms.

6.3 Voice and Video Evaluation

This section presents the evaluation of voice and video applications in the WiMAX links, in order to determine the WiMAX support for real-time applications.

Voice has been evaluated using the Distributed Internet Traffic Generator (D-ITG) (University, 2007) while video has been evaluated using the Evalvid framework tools (Klaue et al., 2003). The characteristics of voice and video applications are described in Appendix I. Such characteristics have been employed to configure the traffic flows of the respective applications.

6.3.1 Tests Description

This subsection presents the parameters configured and the procedures used to perform the tests with voice and video applications.

The common measurements for video and voice evaluations are:

1. **Packet Loss**. Determine the ratio of packets lost during the transmission of voice or video traffic.
2. **Delay**. Determine one way delay (from the source towards destination).
3. **Jitter**. Determine the variation of delay.

The maximum latency parameter (considered the delay parameter in the tests), according to IEEE Std 802.16d (IEEE, 2004), specifies the maximum latency between the reception of a packet by the BS or SS on its network interface and the forwarding of the packet to its RF interface. If defined, this parameter represents a service commitment (or admission criteria) at the BS or SS and shall be guaranteed. A BS or SS does not have to meet this service commitment for service flows that exceed their maximum reserved rate.

The Evalvid tools add other metrics for video applications, such as Mean Opinion Score (MOS), the 5-point scale for user perceived video quality.

To determine the WiMAX equipment performance in different bandwidth conditions and to assess the effectiveness of WiMAX QoS mechanisms, each test accommodates two distinct scenarios:

1. **Underrated**. A given set of tests are performed with low bandwidth values (less than the required).

2. **Overrated**. Other tests are performed with high bandwidth values (more than the required).

The following sections detail the tests performance with voice and video applications over WiMAX.

6.3.2 Voice Tests

This subsection details the evaluation process of voice applications, which considers two variants that are as follows:

- **One client**. A single flow is created to determine the QoS differentiation of the different scheduling services, for instance Best Effort and Real-Time Polling Service.

- **Multiple clients**. Different flows, each one representing a client, are created to determine the support of simultaneous users in aggregated service flows.

All the voice sessions have a duration of sixty seconds, which describes sufficiently the patterns of Voice over IP (VoIP) traffic. The voice codec configured was G.711 (ITU-T, 1972) with no voice activity detection and with one sample per packet. Although, a codec compliant with G.711 is characterized with a bit rate of 64Kbytes, the D-ITG traffic generator creates packets with 80Kbytes which include the Real-Time Protocol (RTP) header but not the IP header (Stefano Avallone & Ventre, 2004). The VoIP traffic is generated from the Mobile Station towards the Access Service Network.

Table 6.5 summarizes the different tests for the single flow cases. Each test is identified by the reserved bandwidth (160Kbytes or 80Kbytes), by the maximum delay (when applicable) and by the scheduling service configured. For instance, the *160kb_2_rtPS* test has 160Kbytes of bandwidth, a configured delay of 2ms and uses the rtPS scheduling service. The Best Effort test cases do not have delay configured.

The test cases with 80Kbytes represent the underrated cases, since the minimum required bandwidth, for the generated traffic, is 100Kbytes. Whilst the

Test Case	**Bandwidth** (Kbytes)	**Delay** (ms)	**Scheduler**
160Kb_2_rtPS	160	2	rtPS
160Kb_100_rtPS	160	100	rtPS
160Kb_150_rtPS	160	150	rtPS
160Kb_300_rtPS	160	300	rtPS
160Kb_na_BE	160	na	BE
80Kb_2_rtPS	80	2	rtPS
80Kb_100_rtPS	80	100	rtPS
80Kb_150_rtPS	80	150	rtPS
80Kb_300_rtPS	80	300	rtPS
80Kb_na_rtPS	80	na	BE

Table 6.5: Voice application: Tests with one flow

160Kbytes represent the overrated cases.

Table 6.6 exhibits the different combinations for the multiple client tests. In these cases, the tests are identified by the number of simultaneous users, by the configured delay (when applicable) and by the respective scheduling service. All the tests have pre-configured service flow with 1Mbyte of bandwidth. In the multiple clients tests, 25, 50 and 75 test cases represent the overrated cases since only 0.30, 0.60 and 0.90Mbytes are required. Whilst 100 and 180 represented the underrated cases with 1.20 and 2.15Mbytes.

The different values for the delay parameter are based on the ITU G.114 recommendation (ITU-T, 2003), which specifies 150ms for one way delay between sender and receiver of voice applications and defines a maximum bound of 400ms for an acceptable one way delay.

Voice Tests Results

The different results achieved with the tests are presented and discussed bellow.

Figure 6.6 exhibits delay of the single flow voice test. As expected, one way delay increases with the configured bandwidth of 80Kbytes, since there is not the required bandwidth for the flow. With the 160Kbytes bandwidth cases, the delay between the different classes is almost equal, with an average value of 10ms.

With the underrated test cases (80Kbytes of reserved bandwidth) the delay with the BE scheduling service is higher than the delay with rtPS scheduling service. The test cases configured with the rtPS scheduling service and with a config-

Test Case	**Number of flows**	**Delay** (ms)	**Scheduler**
25_2_rtPS	25	2	rtPS
25_100_rtPS	25	100	rtPS
25_150_rtPS	25	150	rtPS
25_na_BE	25	na	BE
50_2_rtPS	50	2	rtPS
50_100_rtPS	50	100	rtPS
50_150_rtPS	50	150	rtPS
50_na_BE	50	na	BE
75_2_rtPS	75	2	rtPS
75_100_rtPS	75	100	rtPS
75_150_rtPS	75	150	rtPS
75_na_BE	75	na	BE
100_2_rtPS	100	2	rtPS
100_100_rtPS	100	100	rtPS
100_150_rtPS	100	150	rtPS
100_na_BE	100	na	BE
180_2_rtPS	180	2	rtPS
180_100_rtPS	180	100	rtPS
180_150_rtPS	180	150	rtPS
180_na_BE	180	na	BE

Table 6.6: Voice Application: Tests with multiple flows

ured delay of 300ms have the best performance. Such fact is due to a non stringent value of delay (2ms or 100ms).

Figure 6.7 shows jitter of the single flow voice tests. The jitter in the 160Kbytes bandwidth test cases has an average value of 1.20ms. In the roll of the underrated test cases configured with the rtPS scheduling service, the test cases with a delay of 100 and 150ms have the best value for jitter. Such fact is due to the stringent criteria of 2ms and to the high value of the allowed delay in the 300ms test cases.

Figure 6.8 presents the packet loss of the different test cases of the single flow voice tests. With the underrated test cases (80Kbytes) there is an average of 28% of packet loss. In these cases, the BE test case has not an high packet loss as some test cases of rtPS, such as, the 2ms test case. This behaviour is due to their rigorous criteria of the allowed 2ms delay in the rtPS. In the test cases configured with the BE scheduling service such criteria does not exist.

Another important aspect within the voice application tests is the support for simultaneous clients in a pre-defined service flow, that can aggregate *n* clients.

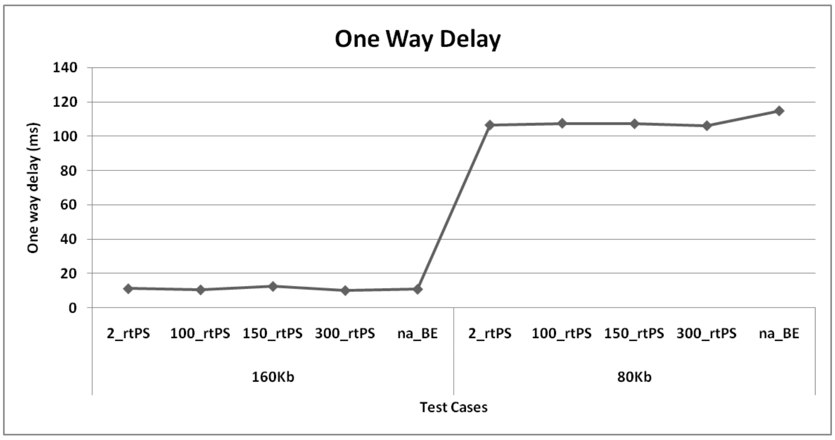


Figure 6.6: One way delay in the case of a single voice flow

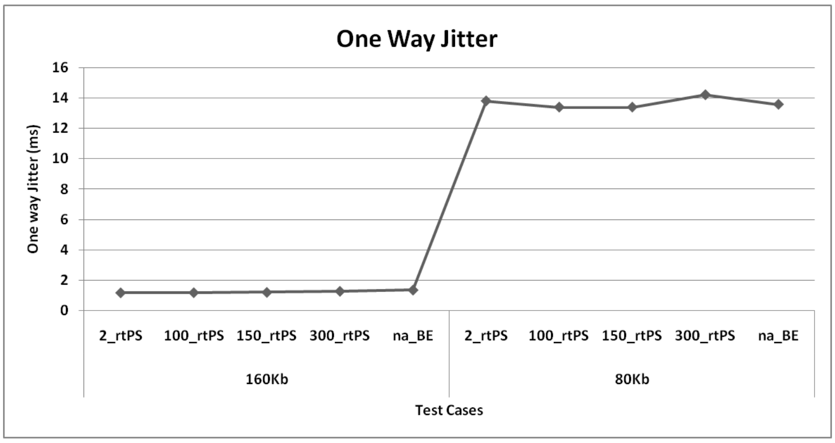


Figure 6.7: One way jitter in the case of a single voice flow

The determination of this number, for a service flow with 1Mbyte is the goal of the multiple voice flows tests.

Figure 6.9 demonstrates the delay for the different test cases in the multiple voice flows tests. Delay increases as the number of simultaneous voice flows increments. For instance, delay has an average of 19ms with the 25 voice flows and an average of 35ms with 180 voice flows. The rtPS scheduling service has a better performance in terms of delay when compared to the BE scheduling service. The 150ms test cases has an improved performance, since it has not a stringent criteria (2ms or 100ms).

Figure 6.10 depicts jitter for the different multiple voice flows tests. As with

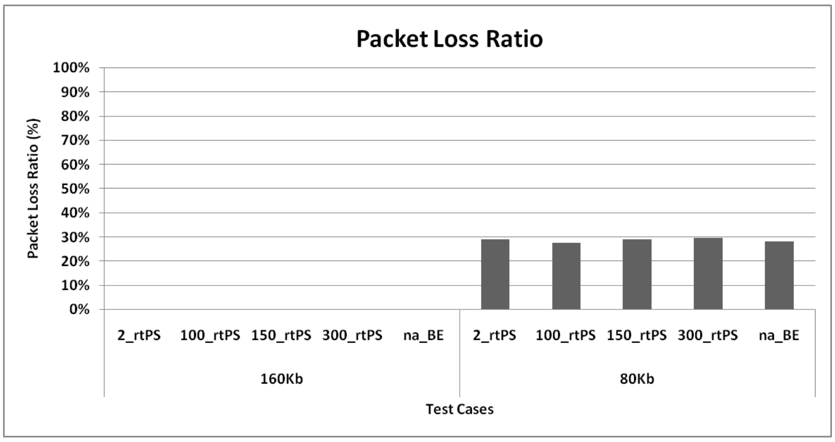


Figure 6.8: Packet loss ratio in the case of a single voice flow

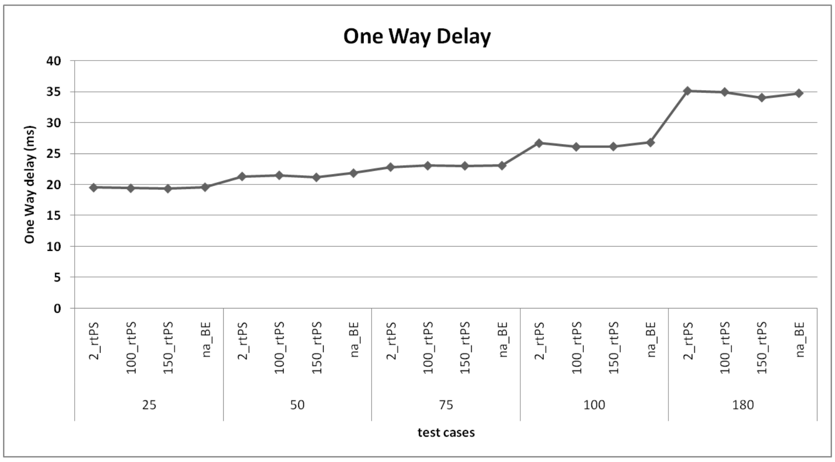


Figure 6.9: One way delay in the case of multiple voice flows

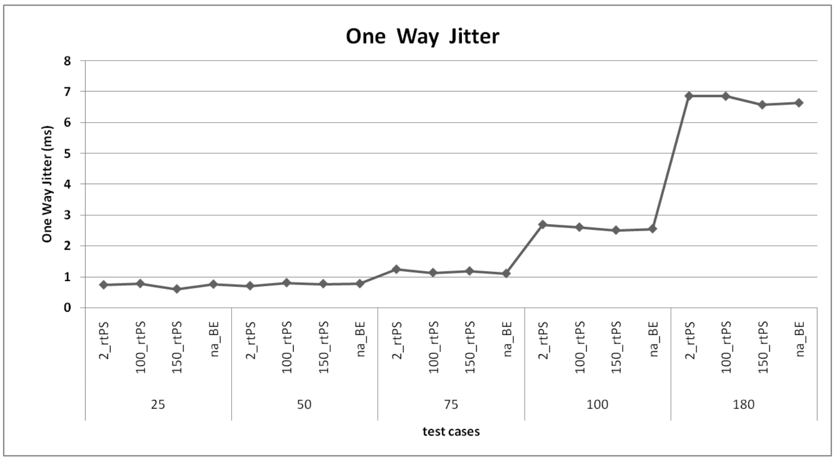


Figure 6.10: One way jitter in the case of multiple voice flows

delay, jitter increases with the number of simultaneous voice flows. For instance, jitter has a minimum value around 1ms in the overrated cases and has a maximum value of 7ms with the 180 voice flows tests.

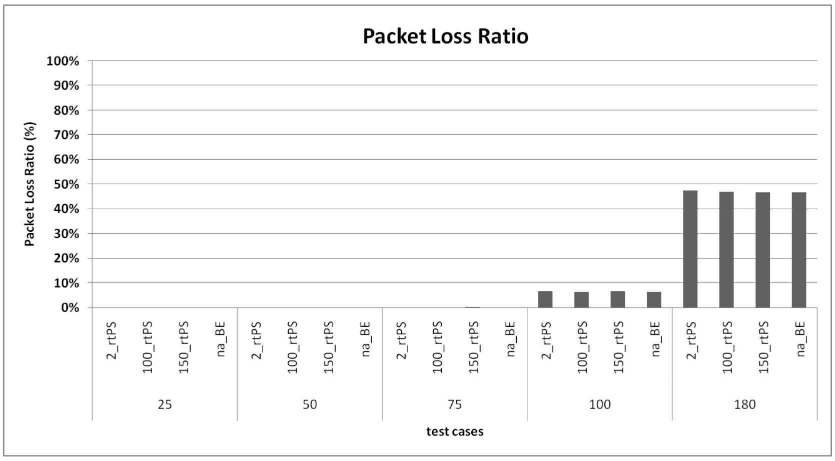


Figure 6.11: Packet loss ratio in the case of multiple voice flows

Figure 6.11 shows the packet loss for the different test cases in the multiple voice flows tests. The packet loss behaviour is similar to the jitter behaviour, high packet loss values with the increased number of simultaneous voice flows. For instance, in the overrated test cases the packet loss is very small (practically non existent). While in the underrated test cases packet loss can achieve ratios of 46%.

Voice Tests Assessments

This subsection summarizes the results obtained with the voice applications.

In the overrated test cases, the WiMAX performance is inline with ITU G.114 (ITU-T, 2003) and ITU Y.1541 (ITU-T, 2006) recommendations. The G.114 recommendation specifies a bound of 150ms for one way delay of voice conversations, while the Y.1541 recommendation presents different QoS classes and for each one defines different values for the network performance parameters. The Y.1541 classes 0 and 1 characterize voice traffic and define the packet loss bellow 0.1% for for a best performance.

The behaviour of the underrated test cases exhibits packet loss ratios around 28% and one way delay in the acceptable bounds of G.114 (bellow 150ms).

The performance of the multiple voice flows relies, mainly on the configured bandwidth for the aggregated service flows. For instance, with 180 simultaneous clients in a 1Mbyte aggregated service flow there is 46% of packet loss. Nonetheless, with 25 and 50 simultaneous clients, there is, practically, no packet loss (0.1%).

The multiple voice flows tests support 75 simultaneous clients with a good conversation quality in terms of delay and packet loss metrics.

6.3.3 Video Tests

This section details the video evaluation using the Evalvid framework tools (Kao et al., 2006).

The video evaluation is performed using a single client (located in the MS side) which receives video traffic generated from the Access Service Network (ASN) side. The evaluation process is based on video files that have different characteristics, as follows:

- **Foreman video**. A video with a duration of 30s and 900 frames.
- **Highway video**. A video with a duration of 66s and 2000 frames.

Both videos can be obtained from the Evalvid site[5] and for each one, different tests have been performed, as depicted in Table 6.7.

[5] Evalvid Site: *http://www.tkn.tu-berlin.de/research/evalvid/

Delay (ms)	**Bandwidth** (Mbytes)	**Scheduler**
na	2	BE
2	2	rtPS
100	2	rtPS
150	2	rtPS
na	1	BE
2	1	rtPS
100	1	rtPS
150	1	rtPS

Table 6.7: Video tests for each video file

The minimum reserved bandwidth in all rtPS test cases is 500Kbytes. Both videos have a bit rate of 1Mbytes/s[6], therefore 2Mbytes of bandwidth represent the overrated cases while 1Mbytes of bandwidth represents the underrated cases.

The video evaluation process and the Evalvid tools characteristics are described in Appendix I.

Video Tests Results

This subsection presents the evaluation results measured by Evalvid tools for the Foreman and Highway videos.

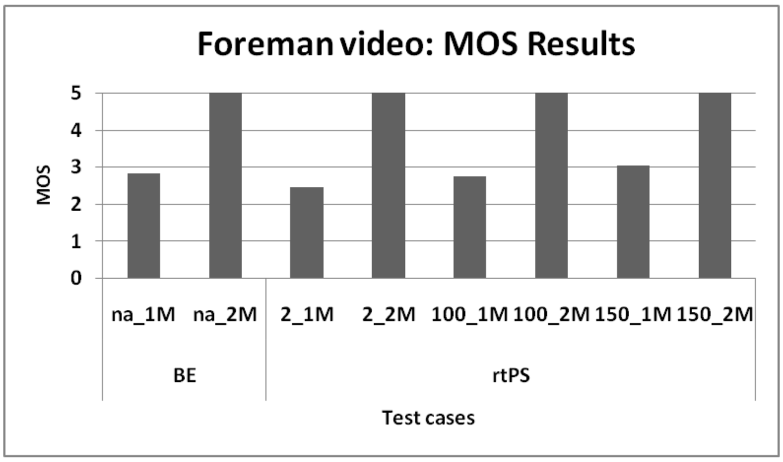


Figure 6.12: MOS of the Foreman video

[6] Considering the value measured by Evalvid tools.

Figure 6.12 presents the MOS results for the Foreman video. All the overrated test cases have the maximum classification in the 5-point scale of MOS. In the underrated test cases the video quality classification depends on the scheduling service and configured delay. For instance, the rtPS test cases configured with a maximum delay of 2 and 100ms have a lower classification when compared to the test cases configured with the BE scheduling service. Such fact is due to the high packet loss in the 2 and 100ms test cases caused by the rigorous admission criteria (low delay bounds).

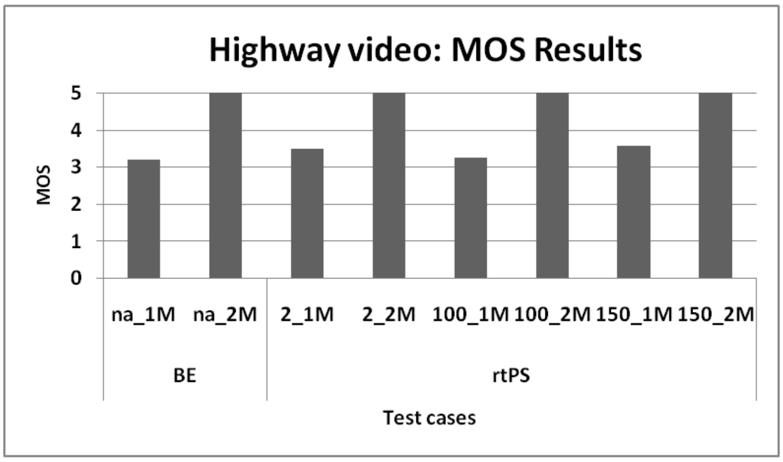


Figure 6.13: MOS of the Highway video

Figure 6.13 depicts the MOS results for the Highway video. The quality of the Highway video in the underrated test cases depends on the scheduling service and on the maximum delay configured for the service flows. Since in all the overrated test cases the video has the maximum classification in the MOS scale. The Highway video is longer than the Foreman video. This justifies the better performance obtained with the rtPS scheduling service.

Table 6.8(a) exhibits the packet loss ratio of the Foreman video. Packet loss reflects the MOS classification, since within the 2Mbytes test cases there is no packet loss, while in the 1Mbytes test cases the packet loss depends on the scheduling service. The test cases configured with the BE scheduling service have a lower packet loss ratio when compared to the test cases of rtPS configured with a delay of 2ms and 100ms.

Table 6.8(b) shows the packet loss of the Highway video. With Highway video, the rtPS scheduling service has a lower average for packet loss when com-

Table 6.8: Packet Loss Ratio

(a) Foreman Video

Test Case	Packet Loss
BE_na_1Mbytes	**5.37%**
BE_na_2Mbytes	**0.00%**
rtPS_2_1Mbytes	**6.57%**
rtPS_2_2Mbytes	**0.00%**
rtPS_100_1Mbytes	**6.23%**
rtPS_100_2Mbytes	**0.00%**
rtPS_150_1Mbytes	**4.87%**
rtPS_100_2Mbytes	**0.00%**
Average value	**2.88%**

(b) Highway Video

Test Case	Packet Loss
BE_na_1Mbytes	**7.23%**
BE_na_2Mbytes	**0.00%**
rtPS_2_1Mbytes	**5.47%**
rtPS_2_2Mbytes	**0.00%**
rtPS_100_1Mbytes	**5.47%**
rtPS_100_2Mbytes	**0.00%**
rtPS_150_1Mbytes	**5.27%**
rtPS_100_2Mbytes	**0.00%**
Average value	**2.93%**

pared to the packet loss ratio of the BE scheduling service.

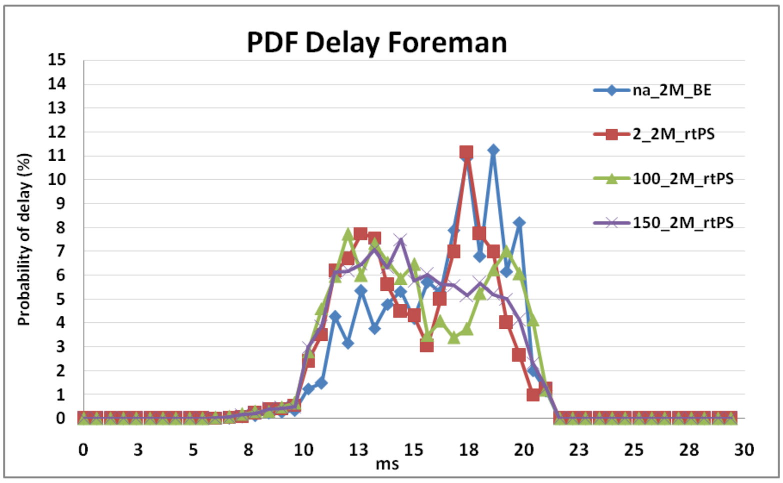


Figure 6.14: PDF delay of Foreman video (2Mbytes)

Delay is based on a Probability Distribution Function (PDF), which determines the probability of a given delay. Figure 6.14 depicts the PDF delay for the Foreman video in the overrated test cases. The tests with the BE scheduling service have an higher probability for higher values of delay. For instance, the BE test cases have more probability of having a delay of 20ms than the rtPS test cases.

For the different configured delays of the rtPS test cases, the 150ms configured delay has the lowest probability of high delay when compared to the other test cases (2ms and 100ms).

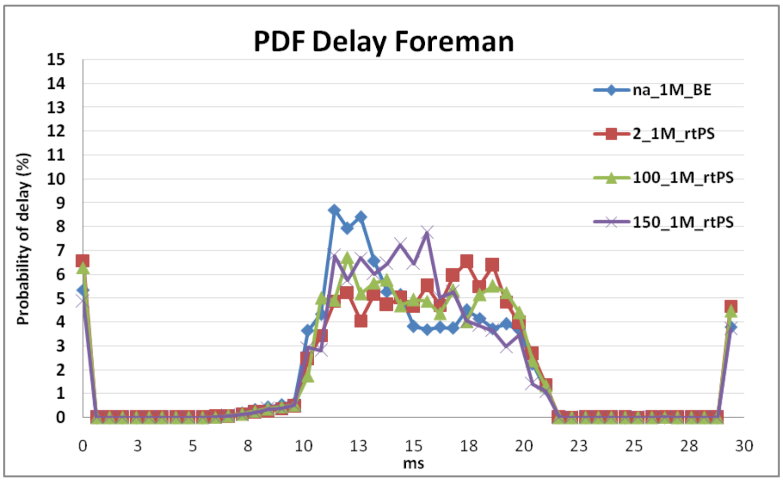


Figure 6.15: PDF delay of Foreman video (1Mbytes)

Figure 6.15 exhibits the delay determined by the PDF for the Foreman video in the underrated test cases. Evalvid tools for lost packets sets a delay of 0ms, therefore the high probability values for 0ms represent packet loss. The probability values around 30ms of delay demonstrate high variation of delay in the underrated test cases.

In the underrated test cases, the BE scheduling service has the higher probability values for lower delays when compared to the test cases configured with rtPS scheduling service. Only the rtPS test cases have an admission criteria, this fact justifies the probability of low delays with the tests cases configured with the BE scheduling service.

Figure 6.16 depicts the PDF delay for the Highway video in the overrated test cases. The behaviour of the different scheduling services is very similar with the Foreman video. The rtPS test cases configured with a delay of 2ms have probability for lower delays. For instance, this is the only test case to have a probability of 5ms of delay.

Figure 6.17 depicts the PDF delay of the Highway video in the underrated test cases. This Graphic depicts packet loss (probability for 0ms of delay) and a variation of delay (probability for delay higher than 30ms).

Overall, the test cases configured, the ones configured with a delay of 100ms have the lowest probability for higher delays and the higher probability for lower

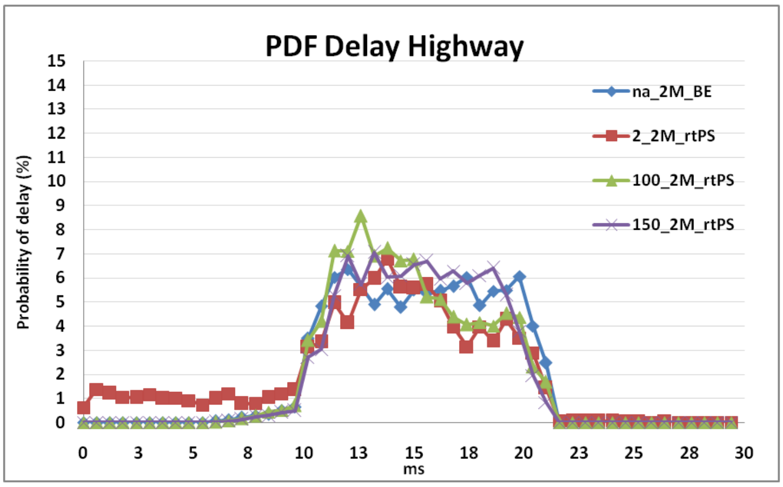


Figure 6.16: PDF delay of Highway video (2Mbytes)

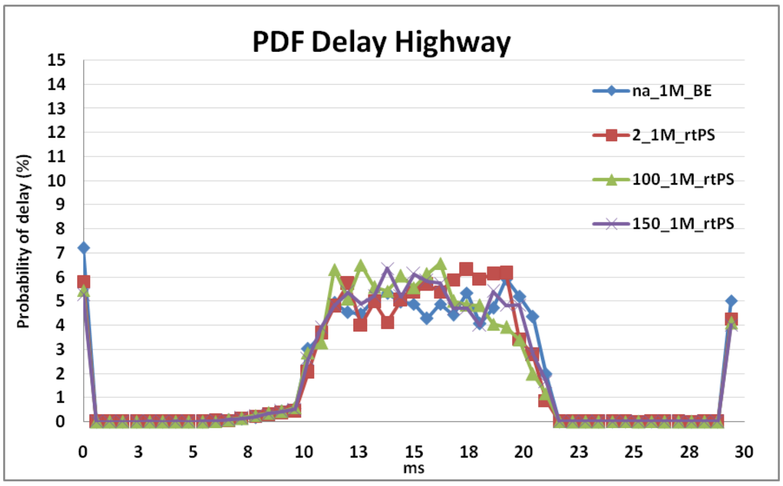


Figure 6.17: PDF delay of the Highway video (1Mbytes)

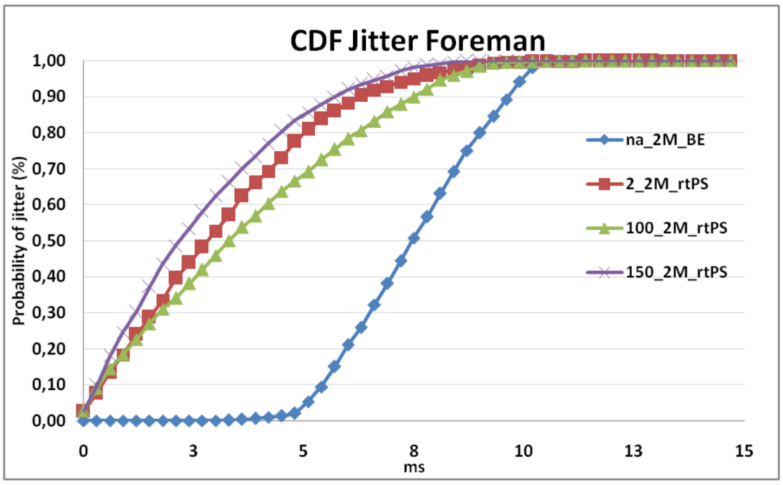


Figure 6.18: CDF jitter of the Foreman video (2Mbytes)

delays, proving therefore, the best performance.

Jitter graphics are based on the Cumulative Distribution Function (CDF) which determines the cumulative probability for jitter.

Figure 6.18 shows the CDF jitter of the Foreman video for the overrated test cases. In the overrated test cases, jitter varies between 0ms and 10ms. The test cases configured with a delay of 150ms have the highest probability of having lower jitter values. In the other hand, the tests with the BE scheduling service have higher values of jitter for the same probability. The BE scheduling service introduces a variation in jitter since there is no admission criteria with the tests configured with this scheduling service.

Figure 6.19 presents the CDF jitter of the Foreman video for the underrated test cases. In these test cases, jitter varies in an interval between 0 and 15ms, which is higher when compared to the overrated test cases.

Figure 6.20 illustrates the CDF jitter of the Highway video for the overrated test cases. The interval of variation of jitter is between 0 and 10ms, as in the Foreman video. The tests performed with the rtPS scheduling service have the highest probability for lower jitter values. The performance of the Highway video tests performed with the rtPS scheduling services are very similar when compared to the Foreman video tests. The longer durations of video establishes such behaviour for rtPS test cases. The BE scheduling service also introduces a variation of jitter, as in the Foreman video.

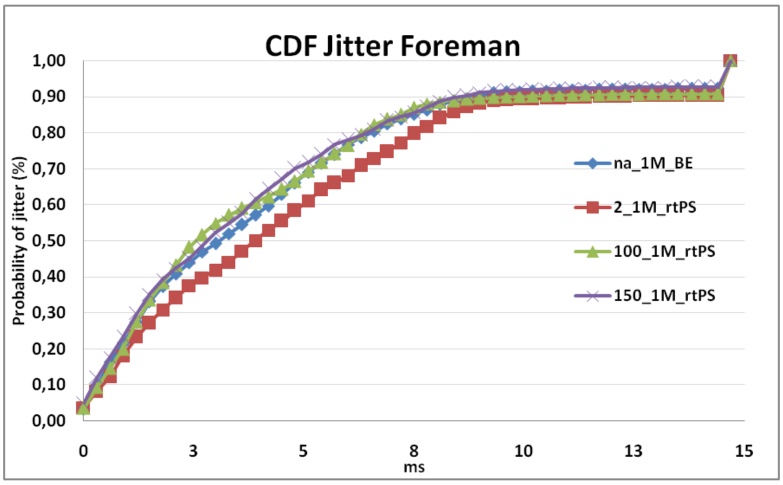


Figure 6.19: CDF jitter of the Foreman video (1Mbytes)

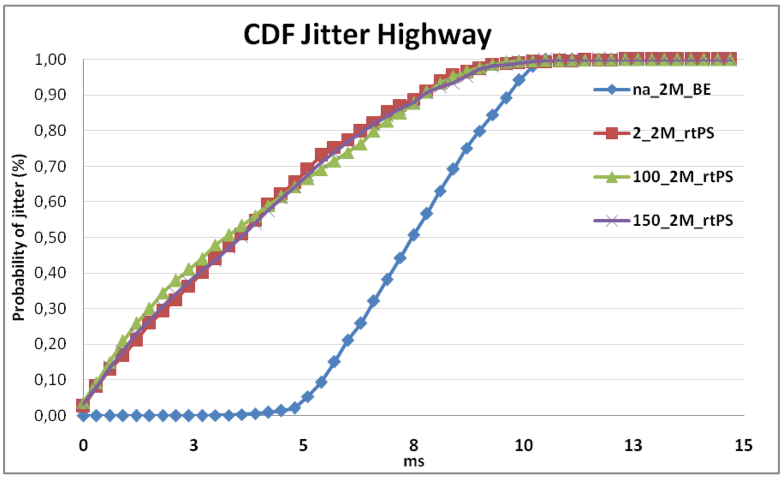


Figure 6.20: CDF jitter of the Highway video (2Mbytes)

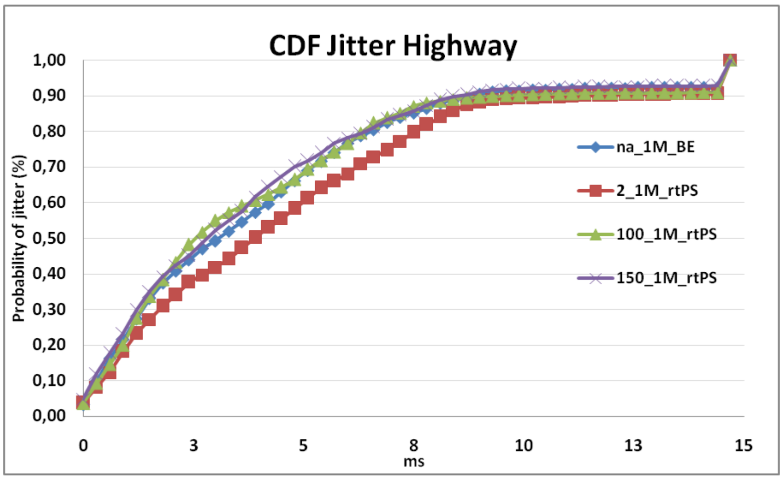


Figure 6.21: CDF jitter of the Highway video (1Mbytes)

Figure 6.21 demonstrates the jitter determined by the CDF for the Highway video in the underrated test cases. In such cases, jitter varies between 0 and 15ms.

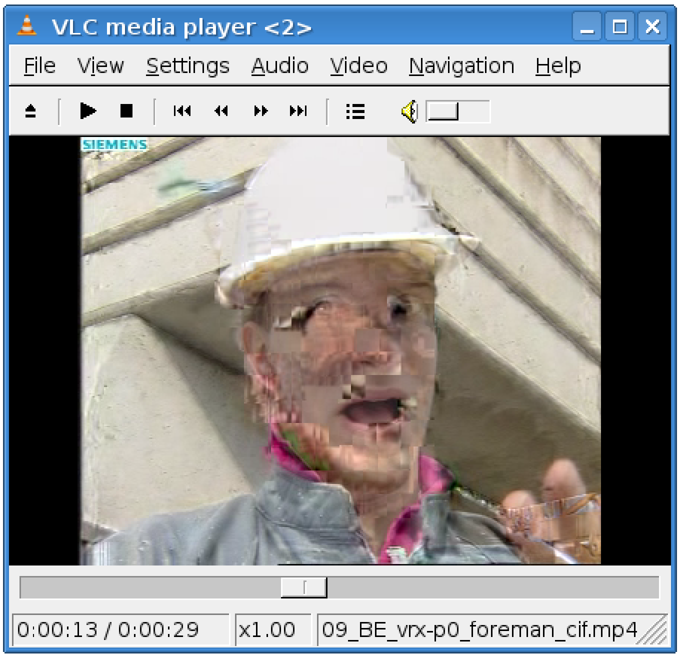
Video Tests Assessment

This subsection summarizes the video performance analysis, presented in the previous subsections.

Video files transmitted in service flows with different QoS configurations have different behaviours according to the bandwidth configured for the service flows. With the overrated (2Mbytes) test cases, video is received with an excellent quality. Nevertheless, in the underrated cases, the video quality is lower and presents annoying features as Figure 6.22 and Figure 6.23 demonstrate for the Foreman and the Highway videos, respectively.

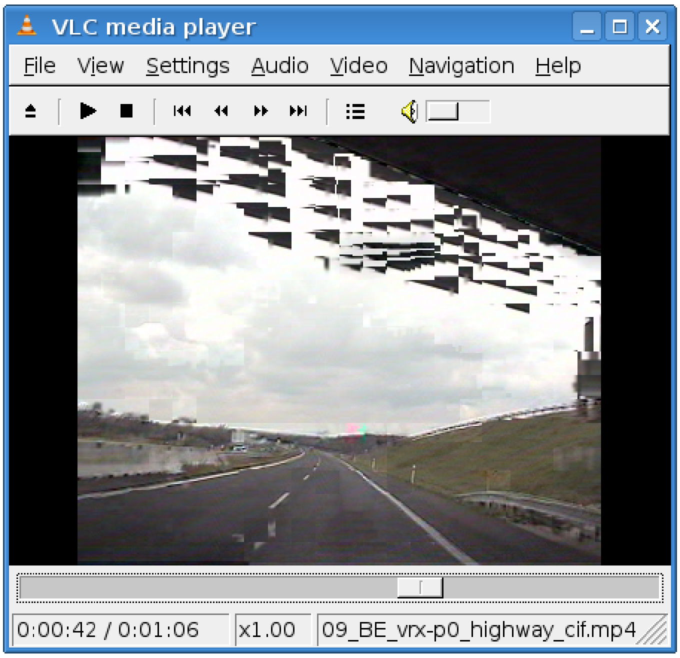
In the Foreman case, the missing frames do not allow to render its face correctly, there is somehow a superposition of frames.

In the Highway case, the rendering, after living a dark scenario (under the bridge) does not adequate to the rapid changes (entering in a lighter scenario), and the image is not rendered adequately (it has some squares).



0:00:13 / 0:00:29 x1.00 09_BE_vrx-p0_foreman_cif.mp4

Figure 6.22: Foreman video with 1Mbytes



0:00:42 / 0:01:06 x1.00 09_BE_vrx-p0_highway_cif.mp4

Figure 6.23: Highway video with 1Mbytes

The differences between the BE and the rtPS mechanisms are not so promising as originally expected. Nevertheless, rtPS achieves the best performance, in terms of delay, jitter and packet loss, when the appropriated delay is correctly configured. For instance, the video test cases configured with a delay of 150ms tend to present a best performance over the other test cases.

6.4 Conclusion

The WEIRD signalling protocols enable the dynamic configuration of service flows with a low overhead. For instance, the performance of GIST in the wireless segments is not so discrepant from the wired segments.

The support of WiMAX for demanding applications, such as voice and video, is adequated. For instance, the performance of the voice application with 75 simultaneous clients in an aggregated service flow of 1Mbyte presents a delay inside the bounds recommended in G.114.

7
Conclusion and next steps

This thesis addresses Quality of Service and mobility support in WiMAX networks. The work performed was carried out in the context of the IST FP6 WiMAX Extension to Isolated Research Network Areas (WEIRD) project.

This chapter is organized as follows: Section 7.1 summarizes the contents of the Thesis and Section 7.2 presents the next steps of the candidate.

7.1 Synthesis of the Thesis

This section summarizes the contents of the Thesis and summarizes the conclusions of the different chapters.

Chapter 2 and Chapter 3 described the Last Mile Wireless Broadband Access and the Media Independent Handover Standards, respectively. The WiMAX technology, based on the IEEE 802.16 standards family was also introduced, with particular emphasis on the support of Quality of Service in IEEE 802.16 standards and incorporated in WiMAX. This important feature of the technology under study is critical for the support of applications with different requirements, which are nuclear both to the WEIRD project and to the nowadays use of the Internet. Furthermore, the need to enable seamless handovers between different technologies triggered the analysis of the Media Independent Handover standard.

Chapter 4 enclosed the description of the WEIRD project. The chapter depicted an overview of the WEIRD architecture to support Quality of Service and mobility. The WEIRD architecture is based on the NSIS framework protocols to enable QoS signalling and on the Mobile IP protocol to allow mobility for different applications.

Chapter 5 and Chapter 6 presented the evaluation of the WiMAX technology performed through simulation and in a real testbed, respectively. The results obtained have demonstrated that WiMAX is able to follow the requirements of the ITU recommendations for voice and video applications under different scenarios. Additionally, the evaluation of the MIH standard, showed its potential to enable seamless handovers. The NSIS framework protocols used for signalling in WEIRD and which performance has been assessed, have the potential to contribute to the Quality of Service support in WiMAX networks.

In parallel with the work presented in this Thesis, the candidate has contributed to the WEIRD by being involved in the definition of the WEIRD architecture, the implementation of modules related to NSIS, the preparation of demonstrations and of first year audit, as well as the dissemination of the project results.

7.2 Next Steps

The WEIRD project has not reached the end of its life cycle. Meanwhile one of the next steps is the contribution to the implementation of the WEIRD mobility architecture. The implementation of MIH transport protocol and the integration with mobile IP protocols will be addressed.

A detailed and concrete proposal for QoS mapping in IEEE 802.16 networks is up to coming. This generic algorithm for QoS mapping aims to describe the mapping from generic QoS models into the IEEE 802.16 QoS model. For instance, to enable the mapping from the different DiffServ classes to the IEEE 802.16 classes of service. This proposal is to be proposed as IETF work in the 16ng Working Group.

Bibliography

3GPP (2007). 3GPP. http://www.3gpp.org/. Last visit: 12 November 2007.

3GPP2 (2007). 3GPP2. http://www.3gpp2.org/. Last visit: 12 November 2007.

Almes, G., Kalidindi, S., & Zekauskas, M. J. (1999a). A One-way Delay Metric for IPPM. RFC2679.

Almes, G., Kalidindi, S., & Zekauskas, M. J. (1999b). Round-trip for Delay Metric for IPPM. RFC2681.

Anastasov, J. (2007). Self-to-Self patch. http://www.ssi.bg/j̃a/#loop. Last visit: 12 November 2007.

Andrews, J., Ghosh, A., & Muhamed, R. (2007). *Fundamentals of WiMAX Understanding Broadband Wireless Networking*. Prentice Hall. ISBN 0-13-222552-2.

Ash, G., Bader, A., Kappler, C., & Oran, D. R. (2007). QoS NSLP QSPEC Template. draft-ietf-nsis-qspec-16.

Braden, B., Zhang, L., Berson, S., Herzog, S., & Jamin, S. (1997). Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification. RFC2205.

Calhoun, P. R., Loughney, J., Arkko, J., Guttman, E., & Zorn, G. (2003). Diameter Base Protocol. RFC3588.

Case, J. D., Fedor, M., Schoffstall, M. L., & Davin, J. R. (1990). Simple Network Management Protocol (SNMP). RFC1157.

Case, J. D., Harrington, D., Presuhn, R., & Wijnen, B. (2002). Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). RFC3412.

Case, J. D., McCloghrie, K., Rose, M. T., & Waldbusser, S. (1993). Introduction to version 2 of the Internet-standard Network Management Framework. RFC1441.

Chia-Yu, Y., Ke, C.-H., Shieh, C.-K., & Chilamkurti, N. (2006). MyEvalvid-NT - A Simulation Tool-set for Video Transmission and Quality Evaluation. In *TENCON 2006. 2006 IEEE Region 10 Conference*, (pp. 1–4).

Cho, D.-H., Song, J.-H., Kim, M.-S., & Han, K. J. (2005). Performance Analysis of the IEEE 802.16 Wireless Metropolitan Area Network. In *DFMA*, (pp. 130–137).

Cicconetti, C., Lenzini, L., Mingozzi, E., & Eklund, C. (2006). Quality of Service Support in IEEE 802.16 Networks. In *IEEE Network*, volume 20, (pp. 50–55).

Communications, R. (2006a). RedMAX AN-100U Base Station (Single Sector) User Manual.

Communications, R. (2006b). RedMAX SU-O (Subscriber Unit - Outdoors) User Manual.

Consurtium, W. (2006a). Deliverable D2.1 - System Scenarios, Business Models and System Requirements. http://www.ist-weird.eu (Intranet). version 1.0.

Consurtium, W. (2006b). Deliverable D5.1 - Test-bed and test environment plan. http://www.ist-weird.eu (Intranet). version 1.1.

Cordeiro, L., Curado, M., Monteiro, E., Bernardo, V., Palma, D., Racaru, F., Diaz, M., & Chassot, C. (2007). GIST Extension for Hybrid On-path Off-path Signaling (HyPath). draft-cordeiro-nsis-hypath-04.

DARPA (1981). Internet Protocol Darpa Internet Program. RFC791.

Deering, S. E. & Hinden, R. M. (1998). Internet Protocol, Version 6 (IPv6) Specification. RFC2460.

Demichelis, C. & Chimento, P. (2002). IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). RFC3393.

Dommety, G. & Leung, K. (2001). Mobile IP Vendor/Organization-Specific Extensions. RFC3115.

Droms, R. (1997). Dynamic Host Configuration Protocol. RFC2131.

Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. E., & Carney, M. (2003). Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC3315.

Eklund, C., Marks, R. B., Ponnuswamy, S., Stanwood, K. L., & Waes, N. J. V. (2006). *WirelessMAN: Inside the IEEE 802.16 Standard for Wireless Metropolitan Area Networks*. IEEE Press.

ETSI (2003). Universal Mobile Telecommunications System (UMTS); Spacial channel model for Multiple Input Multiple Output (MIMO) simulations (3GPP TR 25.996 version 6.1.0 Release 6) . http://www.3gpp.org/ftp/Specs/html-info/25996.htm.

ETSI (2006a). Broadband Radio Access Networks (BRAN); HiperMAN; Data Link Control (DLC) layer . V1.3.2.

ETSI (2006b). Broadband Radio Access Networks (BRAN); HiperMAN; Physical (PHY) layer. V1.3.2.

Farinacci, D., Li, T., Hanks, S., Meyer, D., & Traina, P. (2000). Generic Routing Encapsulation (GRE). RFC2784.

Forum, W. (2006). The Relation between WiBro and Mobile WiMAX.

Forum, W. (2007). WiMAX Forum Network Architecture. Release 1.0.0.

Fu, X., Schulzrinne, H., Tschofening, H., Dickmann, C., & Hogrefe, D. (2006). Overhead and Performance Study of the General Internet Signaling Transport (GIST) Protocol. In *IEEE Infocom, Infocom 2006*. IEEE.

GÉANT (2007). GÉANT. http://www.geant.net/. Last visit: 12 November 2007.

Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., & Patil, B. (2007). Proxy Mobile IPv6. draft-ietf-netlmm-proxymip6-01.

Gupta, V. G. (2006). IEEE P802.21 Tutorial IEEE 802.21 Media Independent Handover. http://www.ieee802.org/21/Tutorials/802%2021-IEEE-Tutorial.ppt. Last visit: 12 November 2007.

Hancock, R., Karagiannis, G., Loughney, J., & den Bosch, S. V. (2005). Next Steps in Signaling (NSIS): Framework. RFC4080.

Handley, M., Jacobson, V., & Perkins, C. (2006). SDP: Session Description Protocol. RFC4566.

IEEE (1990). IEEE 802-1990 Standards for Local and Metropolitan Area, Overview and Architecture.

IEEE (2004). IEEE 802.16-2004 Standard for Local and Metropolitan Area Networks Part 16: Air Interface to fixed and Mobile Broadband Wireless Access Systems.

IEEE (2005a). IEEE 802.16-2005 Standard for Local and Metropolitan Area Networks Part 16: Air Interface to fixed and Mobile Broadband Wireless Access Systems. IEEE.

IEEE (2005b). IEEE 802.16f-2005 Standard for Local and Metropolitan Area Networks Part 16: Air Interface to fixed and Mobile Broadband Wireless Access Systems Amendment 1: Management Information Base.

IEEE (2006). IEEE P802.21/D01.00 Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services.

IEEE (2007a). The IEEE 802.16 working group on broadband wireless access standards. http://wirelessman.org/. Last visit: 12 November 2007.

IEEE (2007b). IEEE 802.16g/d9 Draft IEEE standard for Local and Metropolitan Area Networks Part 16: Air Interface to fixed and Mobile Broadband Wireless Access Systems Amendment 3: Management Plane Procedures and Services.

IEEE (2007c). IEEE 802.16i/d3 IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface to fixed and Mobile Broadband Wireless Access Systems Draft Amendment: Management Information Base Extensions.

IEEE (2007d). IEEE P802.21/D07.00 Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services.

IEEE (2007e). IEEE-SA Standards Board Project Authorization Request (PAR) Form (2002). http://www.ieee802.org/21/802_21_PAR.doc. Last visit: 12 November 2007.

IEEE (2007f). The IEEE 802.21 Working Group. http://www.ieee802.org/21/. Last visit: 12 November 2007.

Intel (2003). Overcoming Barriers to High-Quality Voice over IP Deployments.

ITU (2002). Series Y: Global Information Infrastructure and Internet Protocol Aspects, Internet protocol aspects - Quality of service and network performance, Internet protocol data communication service - IP packet transfer and availability performance parameters . ITU-T Recommendation Y.1540.

ITU-T (1972). ITU-T Recommendation G.711, General Aspects of Digital Transmission Systems, Terminal Equipments, Pulse Code Modulation (PCM) of Voice Frequencies.

ITU-T (1988). ITU-T Recommendation G.722, General Aspects of Digital Transmission Systems, Terminal Equipments, 7kHz Audio - Coding within 64 KBIT/S.

ITU-T (1993). ITU-T Recommendation H.261, Line Transmission of Non-Telephone signals, Video Codec for audiovisual services at p x 64 kbits .

ITU-T (2003). ITU-T Recommendation G.114, One-Way transmission time.

ITU-T (2005a). ITU-T Recommendation G.107, The E-model, a computational model for use in transmission planning.

ITU-T (2005b). ITU-T Recommendation G.726, Series G: Transmission systems and media digital systems and networks, Digital terminal equipments - Coding of analogue signals by methods other than PCM, 40, 32, 24, 16 kbit/s Adaptative Differential Pulse Code Modulation (ADPCM), .

ITU-T (2005c). ITU-T Recommendation H.263, Series H: Audiovisual and multimedia Systems, Infrastructure of audiovisual services - Coding of moving video, Video coding for low bit rate communication .

ITU-T (2006). ITU-T Recommendation Y.1541, Series Y: Global Information Infrastructure, Internet Protocols aspects and next-generation neworks - Internet protocol aspects - Quality of service and network performance - Network performance objectives for IP-based services .

Jang, H., Jee, J., Han, Y.-H., Park, S. D., & Cha, J. (2007). Mobile IPv6 Fast Handovers over IEEE 802.16e Networks. draft-ietf-mipshop-fh80216e-02.

Johnson, D. B., Perkins, C. E., & Arkko, J. (2004). Mobility Support in IPv6. RFC3775.

JTC1/SC29/WG11, I. (2002). MPEG-4 description V.21. http://www.chiariglione.org/mpeg/standards/mpeg-4/mpeg-4.htm.

KAIST (2007). IEEE 802.16 Simulation. http://cnlab.kaist.ac.kr/802.16/ieee802.16.html. Last visit: 20 August 2007.

Kao, K.-L., Ke, C.-H., & Shieh, C.-K. (2006). An Advanced Simulation Tool-set for Video Transmission Performance Evaluation. WNS2.

Klaue, J., Rathke, B., & Wolisz, A. (2003). EvalVid - A Framework for Video Transmission and Quality Evaluation. In *13th International Conference on Modelling Techniques and Tools for Computer Performance Evaluation, Urbana, Illinois, USA*.

Koodli, R. (2005). Fast Handovers for Mobile IPv6. RFC4068.

Koodli, R. & Perkins, C. (2007). Mobile IPv4 Fast Handovers. draft-ietf-mip4-fmipv4-07.

Leung, K. K., Mukherjee, S., & Rittenhouse, G. E. (2005). Mobility Support for IEEE 802.16d Wireless Networks. In *Wireless Communications and Networking Conference, 2005.WCNC 2005*. IEEE.

Liu, F., Zeng, Z., Tao, J., Li, Q., & Lin, Z. (2005). Achieving QoS for IEEE 802.16 in Mesh Mode. In *8th International Conference on Computer Science and Informatics*, volume 5, (pp. 3102–3106).

Manner, J., Karagiannis, G., & McDonald, A. (2007). NSLP for Quality-of-Service Signaling. draft-ietf-nsis-qos-nslp-14.

Manner, J., Stiemerling, M., & Tschofenig, H. (2007). Authorization for NSIS Signaling Layer Protocols. draft-manner-nsis-nslp-auth-03.

Melia, T., Hepworth, E., Sreemanthula, S., Ohba, Y., Gupta, V., Korhonen, J., Aguiar, R. L., & Xia, S. (2007). Mobility Services Transport: Problem Statement. draft-ietf-mipshop-mis-ps-02.

Montenegro, G. (2001). Reverse Tunneling for Mobile IP, revised. RFC3024.

Narten, T., Nordmark, E., & Simpson, W. A. (1998). Neighbour Discovery for IP Version 6 (IPv6). RFC2461.

NDSL (2007). WiMAX for ns-2. http://ndsl.csie.cgu.edu.tw/wimax_ns2.php. Last visit: 12 November 2007.

NS-2 (2007). The Network Simulator - ns-2. http://www.isi.edu/nsnam/ns/. Last visit: 12 November 2007.

Perkins, C. (2002). IP Mobility Support for IPv4. RFC3344.

Postel, J. (1981). Assigned Numbers. RFC790.

Postel, J. & Harrenstien, K. (1983). Time Protocol. RFC868.

Rahman, A., Olvera-Hernandez, U., Zuniga, J. C., Watfa, M., & Kim, H.-W. (2007). Transport of Media Independent Handover Messages Over IP. draft-rahman-mipshop-mih-transport-02.

Rigney, C., Rubens, A. C., Simpson, W. A., & Willens, S. (2000). Remote Authentication Dial In User Service (RADIUS). RFC2865.

Rosen, E. C., Viswanathan, A., & Callon, R. (2001). Multiprotocol Label Switching Architecture. RFC3031.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., & Schooler, E. (2002). SIP: Session Initiation Protocol. RFC3261.

Rouil, R. (2007). NS-2 NIST add-on IEEE 802.16 model (MAC + PHY) . http://www.antd.nist.gov/seamlessandsecure/toolsuite.html.

Rouil, R. & Goilme, N. (2006). Adaptative Channel Scanning for IEEE 802.16e. National Institute of Standards and Technology.

Schulzrinne, H. & Hancock, R. (2007). GIST: General Internet Signalling Transport. draft-ietf-nsis-ntlp-13.

Simpson, W. A. (1994). The Point-to-Point Protocol (PPP). RFC1661.

Soliman, H., Castelluccia, C., Malki, K. E., & Bellier, L. (2005). Hierarchical Mobile IPv6 Mobility Management (HMIPv6). RFC4140.

Stanic, M. P. (2007). tc - traffic control Linux QoS control tool. http://www.rns-nis.co.yu/ mps/linux-tc.html. Last visit: 12 November 2007.

Stefano Avallone, Donatto Emma, A. P. & Ventre, G. (2004). A practical demonstration of Network traffic Generation. In *Eighth IASTED International Conference*.

Stiemerling, M., Tschofening, H., Aoun, C., & Davies, E. (2007). NAT/Firewall NSIS Signaling Layer Protocol (NSLP). draft-ietf-nsis-nslp-natfw-14.

Thomson, S. & Narten, T. (1998). IPv6 Stateless Address Autoconfiguration. RFC2462.

University, N. (2007). D-ITG, Distributed Traffic Generator. http://www.grid.unina.it/software/ITG/. Last visit: 12 November 2007.

Wakikawa, R. & Gundavelli, S. (2007). IPv4 Support for Proxy Mobile IPv6. draft-ietf-netlmm-pmip6-ipv4-support-00.

Walker, J. Q. (2001). A Handbook for Successful VoIP Deployment: Network Testing, QoS and More.

WEIRDConsurtium (2006). Description of Work (DoW)WiMAX Extension to Isolated Research Data networks.

WEIRDConsurtium (2007). Deliverable D2.3 - System Specification. http://www.ist-weird.eu (Intranet). version 1.3.1.

WiBro (2007). Wireless Broadband overview. http://www.wibro.or.kr/down/wibro_overview_20060315.ppt. Last visit: 12 November 2007.

WiMAXForum (2001). WiMAX System Evaluation Methodology.

WiMAXForum (2005). Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e WiMAX networks.

WiMAXForum (2006a). Mobile WiMAX - Part I: A Technical Overview and Performance Evaluation .

WiMAXForum (2006b). WiMAX System Level Simulation Software Architecture.

WiMAXForum (2007a). Second Mobile WiMAX PlugFest.

WiMAXForum (2007b). WiMAX Forum Network Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Poins). Release 1.0.0.

WiMAXForum (2007c). WiMAX Forum Network Architecture (Stage 3: Detailed Protocols and Procedures). Release 1.0.0.

WiMAXForum (2007d). WiMAX Forum site. http://www.wimaxforum.org/home/. Last visit: 12 November 2007.

Appendix

Appendix A - MIH commands

This Appendix presents a list of the MIH commands.

Command Name	(L)ocal (R)emote	**Description**
MIH Get Link Parameters	L,R	Get the status of a link.
MIH Configure Link	L,R	Configure a link and control its behaviour.
MIH Scan	L,R	Scan a list of PoAs for a specific link type.
MIH Net HO Candidate Query	R	For Network Initiated Handovers. Permit to send a list of suggested networks and PoAs.
MIH MN HO Candidate Query	R	For Mobile Node Initiated Handovers, to allow the collection of handover related information and possible candidate networks.
MIH N2N HO Query Resources	R	Command issued by the serving MIHF to the target MIHF entity to allow for resource query, context transfer, and handover preparation.
MIH Net HO Commit	R	For Network Initiated Handovers to commit the handover, informing the selected network and the respective associated PoA.
MIH MN HO Commit	R	Used by MN to notify the network that a candidate has been committed for handover.
MIH N2N HO Commit	R	Employed by the serving network to inform the target network that a mobile node is about to move towards that network.
MIH MN HO Complete	R	Commands issued by the MIHF of the MN to the MIH Function of the target network to inform of the handover process completion.
MIH N2N HO Complete	R	Commands issued by the MIHF of the MN to the MIH Function of the target network to inform of the handover process completion.

Table 7.1: MIH Commands

Appendix B - IEEE 802.21 Link commands

This Appendix summarizes the Link commands specified in IEEE Std 802.21.

Command Name	**Description**
Link Capability Discovery	Query and discover the list of supported link layers events and link layer commands.
Link Event Subscribe	To perform the subscription to one or more events from a link.
Link Event Unsubscribe	To perform the unsubscription from a set of link layer events.
Link Configure Thresholds	Configure the thresholds for link parameters report event.
Link Get Parameters	Get measure parameters of the active link, such as Signal-to-Noise Ratio (SNR).
Link Action	To request actions on a link layer connection.

Table 7.2: Link Commands

Appendix C - MIH Information Elements

This Appendix presents a subset of Information Elements specified in the MIH standard.

Information Element	**Description**
TYPE IE NETWORK TYPE	Link types of the networks available in a given geographical area.
TYPE IE OPERATOR IDENTIFIER	The operator identification for the access/core network.
TYPE IE LIST OF OPERATORS	Network operator list for each type of link
TYPE IE COST	Indication of cost for a network usage.
TYPE IE NETWORK SECURITY	Security characteristics of the link layer (e.g. Authentication methods).
TYPE IE NETWORK QOS	QoS characteristics of the link layer (e.g. QoS classes and traffic type).
TYPE IE NETWORK DATA RATE	The maximum data rate supported by the link layer of the access network.
TYPE IE POA MAC ADDRESS	MAC address of PoA.
TYPE IE POA LOCATION	Geographical location of PoA. Can be geospatial location or civic location format. The Geospatial info includes Latitude, Longitude, Altitude and Map Datum. The Civic info consists of Civic Code number, civic address elements. The methods to obtain location can be by Global Positioning System (GPS) or Manual.
TYPE IE POA SUBNET INFORMATON	Subnets supported by a typical PoA.
Vendor Specific IEs	Vendor/Operator specific information.

Table 7.3: A subset of Information Elements

Appendix D - GIST Primary Message Types

This Appendix summarized the characteristics of the primary message types of GIST.

Msg type	Message purpose	Message format
Query	• Used in the discovery of the next GIST hop. • Transport a proposal for the establishment of a connection between peers.	Common-Header (with R flag setted), Message Routing Information, Session Identification, Network Layer Information, Query Cookie, and possibly NSLP Data.
Response	• Sent in response to a Query message, to acknowledge it. • Provides network information about the responding node. • Transport the response to the initial proposal for the establishment of the connection.	Common-Header (with R flag setted if association is requested), Message Routing Information, Session Identification, Query Cookie, and possibly NSLP Data.
Confirm	Acknowledges a Response message and is sent to complete the association setup.	Common-Header, Message Routing Information, Session Identification, Network Layer Information, and possibly NSLP Data.
Data	Transport NSLP data without modifying GIST state.	Common-Header, Message Routing Information, Session Identification, and NSLP Data.

Table 7.4: GIST primary message types

Appendix E - WEIRD Project Description

This Appendix provides a description of the WEIRD project.

WEIRD comprises different applications in the four testbeds. The Voice over IP (VoIP), Video Conferencing and Video Streaming applications are also considered to allow voice and video calls.

The main objectives of this project can be summarized as follows:

- Enhancements to the WiMAX tecnhology, to improve the integration of the WiMAX in two levels:

  Quality of Service Integrate WiMAX Quality of Service (QoS) mechanisms with existent IP QoS mechanisms such as Differentiated Services (DiffServ).

  Radio over Fiber Integrate WiMAX with Radio over Fiber (RoF) technology.

- Enhancements to the Internet Protocol (IP) network Control Plane, focusing on network planning and definition of guidelines for the deployment of the WEIRD architecture.

- Assessment of scenarios, including WiMAX as a backhaul solution for research in remote areas and broadband access for the project applications.

Current wireless technologies may have high deployment costs, or are not standardized which brings interoperability issues among different vendors. WiMAX plays an important role and distinguishes itself from others. WiMAX is being standardized based on the IEEE Std 802.16 family standard, by an independent organization, WiMAX Forum WiMAXForum (2007d). Different companies such as Siemens, Redline, Intel, among others, are working to avoid incompatibility issues as found in past wireless network deployments. WEIRD aims at validating the deployment of WiMAX as an access technology, overcoming actual Wireless Local Area Network (WLAN) coverage and promoting Wireless Metropolitan Area Network (WMAN) in urban and rural environments, as well as in impervious areas, such as volcanic mountains.

The research networks are connected to the GÉANT network with the WiMAX technology, as depicted in Figure 7.1. Each end network, using different technologies (e.g. Ethernet, Wi-Fi), has different applications, such as, network sensors,

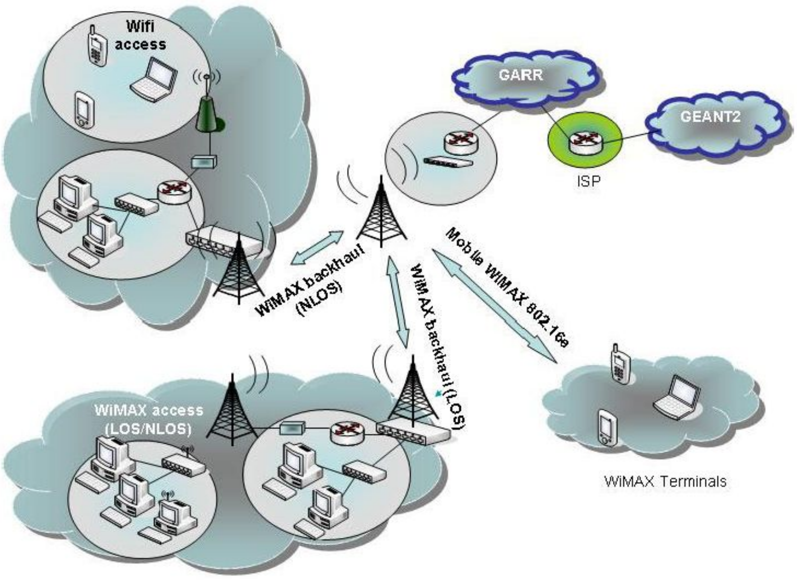


Figure 7.1: WEIRD applications scenario
Source Description of Work document WEIRDConsurtium (2006).

medical applications, multimedia applications. The need for connectivity in impervious areas associated with mobility, constitute a difficult requirement to fulfil with current wireless technologies. Wireless networks based on IEEE Std 802.11 have limited coverage, thus being used for Local Area Network (LAN). Wireless networks based on the Third Generation Partnership Project (3GPP) (3GPP, 2007) or 3GPP2 (3GPP2, 2007) recommendations, despite their proliferation, have high deployment costs when compared to WiMAX. Nowadays, wired solutions do not support the mobility as user needs and the coverage of remote areas are still an issue.

The WEIRD project is organized in different Work Packages (WP), and each one has different activities planned. The business model and system analysis (WP2000) provides the design of the WEIRD architecture, the specification of the business models and the associated scenarios. The infrastructure testbed design and implementation, WP3000, provides the integration of protocol, control mechanisms and the enhancements needed in applications to support the WEIRD system. The transport plane, carried out in the WP3000, aims to design and implement the convergence layer mechanisms with Application Programming Interface (API) and interfaces for IPv4/IPv6 networks. The API modules provide QoS management, mobility management and multi-access control. All the testbeds are integrated in the WP5000 - testbed integration. The testbed integration includes configuration of services, such as routing, Domain Name Service (DNS), video streaming, among others. But, it also includes all the installation procedures of the necessary software modules for WEIRD. The WP6000 - dissemination and exploitation is dedicated to all the actions that promote WEIRD. This standardization activity includes presentation of the WEIRD activities and results from trials and demonstration to other entities. This work package also encloses all the connections with entities like Internet Engineering Task Force (IETF)[1].

Figure 7.2 exhibits the WEIRD system. All the activities of WEIRD involve 16 partners from 6 countries. Within each Work Package different deliverables are produced, reflecting the work performed by the partners enrolled in the activities.

System Scenarios

This subsection describes the system scenarios assessed in WEIRD, the involved services and the technologies used in each one.

The system scenarios are classified in three major types, according to the WEIRD deliverable D2.1Consurtium (2006a):

Scenario A - Environmental monitoring.

Scenario B - Tele Medicine.

Scenario C - Fire Prevention.

The scenario of environmental monitoring considers volcanic and seismic regions. The monitoring equipment is installed in the field, collecting data which is sent to the observatory centers. Since the observatory centers are placed in secure areas, WiMAX can be employed to allow the communication of the equipment to the observatory centers. Wired solutions are not viable due to the long distances and the mountainous areas. The environmental applications use voice and video over IP to collect video in real-time from cameras.

The identified sub-scenarios of the Environmental monitoring are:

- **Seismic monitoring (A1) and Volcanic monitoring (A2)**. For instance, in the Vesuvius volcano there are digital seismic stations equipped with serial and Ethernet interfaces to output data. The data collected is stored locally in hard drives, and is assembled periodically to be analysed. WiMAX is the

[1] http://www.ietf.org

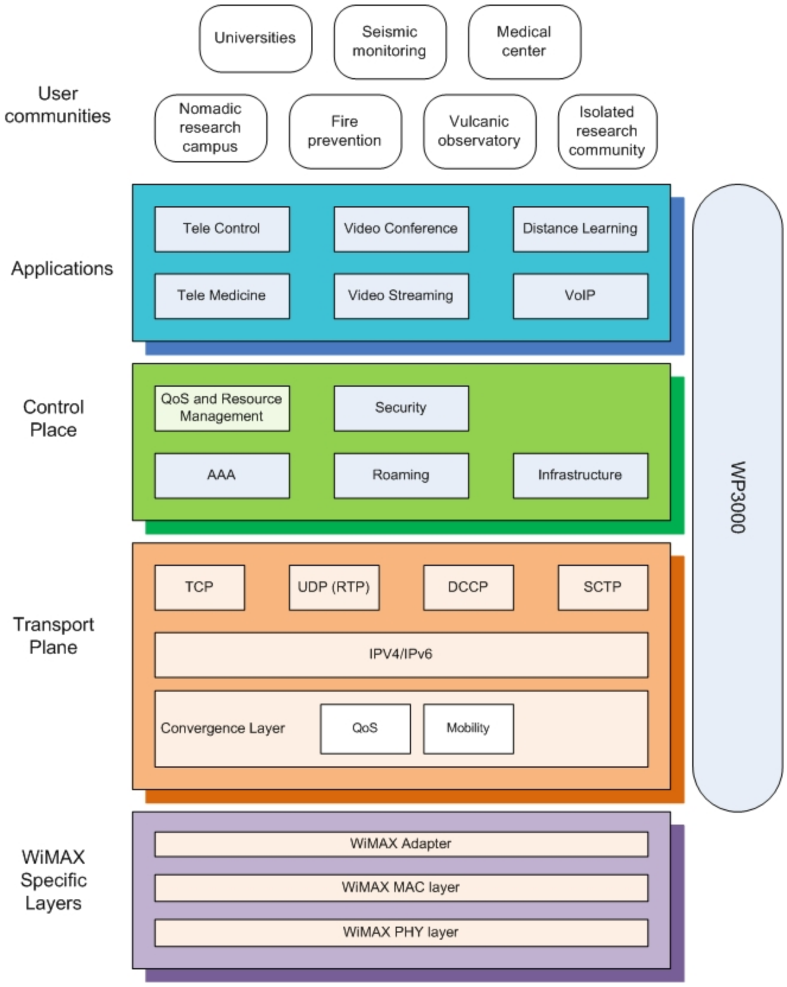


Figure 7.2: WEIRD system
Source Description of Work document WEIRDConsurtium (2006).

solution used to connect the remote stations to the acquisition center. The extensions proposed by WEIRD help to secure the access to the acquired data, so that only authorized people have access. Permanent stations can use the 802.16d technology to transmit data to a Base Station (BS), while mobile stations use 802.16e technology for data transfer. To improve the system coverage the Radio over Fiber (RoF) technology can be used. The RoF technology allows to extend the coverage, since the antennas can be placed at higher distances from the base stations. Real-time data transmission from sensors represents the main type of service. Nonetheless, voice and video over IP combined with transmission of still images, video surveillance and voice communication in real-time, are important to the environmental monitoring.

- **Monitoring volcanic unrest and eruptions at Hekla volcano (A3) and Monitoring seismic activity in remote volcanic/geothermal area (A4)**. The monitoring is held by fixed Global Positioning System (GPS) stations, permanent seismic station, portable seismic sensors, gas-monitoring, video cameras and tilt recording tools. The seismic and GPS stations detect seismic activity and deformations of the surface caused by the ascending magma. The cameras, with a low frame-rate video, cover all sides of the mountain, revealing the location of the eruptive site. The tilt recording tools monitor geothermal activities. The collected data is transferred to a processing center. The real-time data is displayed on maps. WiMAX is used to allow the connection to the processing center. The coverage areas overlap each other, in order to implement redundancy. Mobile WiMAX allows VoIP communications from the technicians in the field to the processing center.
- **Mobile Monitoring (A5)**. Users, carrying multiple interface terminals, can have access to the data collected in the processing centers. WiMAX, can be used as an access technology, when the user terminal is equipped with a IEEE Std 802.16 interface. The connection to the processing center network is through an IP network. Different services can be associated with these users, such as VoIP and video conference.

E-health, the tele medicine scenario, can benefit from WiMAX to improve the quality of life, by overcoming the current limitations. Nowadays, patients must travel to far-away hospitals to be followed-up, there is not the concept of “remote follow-up”. Data for simple diagnosis is collected at fixed places or on moving medium (e.g. ambulances). The elderly people are only monitored when present at fixed places, like home. There is no remote assistance to assist patients that need reminders about medications, therapies and basic health instructions. The tele medicine application assists a doctor on the field, allowing the doctor to send images and data, and collect a second opinion using video streaming.

The identified sub-scenarios of the tele medicine scenario are:

- **Specialized skill at the house of the patient (B1)**. A doctor is on the field with a medical device connected to a notebook and sends data using a WiMAX channel to the centre. The doctor can collect images and upload them to a server in the centre to be analysed by specialists. Video conference and voice conference can be used to collect the result of the analysis performed by the expert, or to have a second opinion. WiMAX is the support of the communications on the field.

- **Medical Information exchange while travelling (B2)**. Mobile medium, such as ambulances, can be equipped with mobile WiMAX stations to allow transfer of images and video conference with the hospital. While travelling to the hospital, a surgery can be prepared, faster diagnosis can be performed with the medical devices in the ambulance.

As it is today, the main method to detect fires relies in local people living at the hazardous zones. The alert is communicated using a cell phone to the command center of the fire brigades. Nevertheless, isolated and mountain regions and deserted areas, have a poor fire detection. The installation of sensors, video and infrared cameras depends on the communication technology to transfer the data. Current wireless technologies, such as Global System for Mobile communications (GSM)/General Packet Radio Service (GPRS) have an high deployment cost, or have some limitations regarding the image quality.

The fire prevention scenario can be decomposed in the following sub-scenarios:

- **FireStation (C1)**. This scenario transmits still images and text description from the Forest Fire Simulation System (FireStation) to a mobile unit in the field, such as a Laptop. WiMAX allows the real-time data collection and transmission, voice and video communications with the central command station, transmission of high quality still images and continuous video monitoring.

- **Fixed and Mobile Video Surveillance (C2)**. Fixed video cameras transmit video and meteorological parameters. These cameras can be controlled via a web page, the same that provides access to the data collected by the camera. A human operator analyses the video to detect a fire. A mobile unit can be used to monitor the fire. This unit has video cameras and allows the transmission of text data (GPS position and meteorological parameters) as well as video data. The support for voice communications is an added value since all the communications rely on the cell phones.

- **Wireless Sensor Networks in Fire Scenario (C3)**. Sensors can be installed in forests. These sensors can measure temperature, humidity, wind direction and velocity. The information collected by these sensors can improve fire prevention and the fire combat. Sensors transmit data to a sink node, which connects to an IP network through WiMAX.

All the services, aforementioned in the different scenarios, rely on WiMAX for an improved and more secure performance.

WEIRD Testbeds

This subsection provides details about the WEIRD testbeds, which have different applications installed.

The deliverable D5.1 Consurtium (2006b) describes the activities performed in each testbed. The deployment of WiMAX is performed in different phases: The first considers the WiMAX 802.16d equipment; The second is based on the mobile WiMAX (802.16e) equipment.

Each testbed is associated to a specific scenario, thus avoiding the difficulties inherent to the deployment of scenarios in all the testbeds. Table 7.5 exhibits the association between the testbeds and the scenarios.

Testbed	**Scenario**
WIND-Ivrea (Italy)	Tele medicine
VTT-Oulu (Finland)	Seismic and Volcanic monitoring
PTIN-UoC (Portugal)	Fire prevention
ORANGE-UPB (Romania)	General applications

Table 7.5: Testbed Scenarios

Each testbed deploys the services associated with its related scenario, nonetheless general applications such as real-time VoIP, real-time data collection and transmission and generic data applications can be deployed, as well.

WIND-Ivrea testbed

The Ivrea testbed is planned for different areas, urban, suburban, rural and for different conditions such as Line of Sight (LOS) and Non Line of Sight (NLOS). It includes IEEE Std 802.16d and IEEE Std 802.16e BSs, as well as mobile and fixed Customer Premises Equipment (CPE). RoF is also employed to extend the system coverage. This testbed is based on the Alcatel 7387 product for WiMAX.

VTT-Oulu testbed

This testbed includes IEEE Std 802.16d BS and IEEE Std 802.16e BSs, as well as fixed and mobile CPEs. The testbed is planned for urban, rural environments where volcanic mountains impose NLOS conditions and long range coverage. The video streaming application is used to test mobility in this testbed.

ORO-UPB testbed

This testbed aims to interconnect two islands, the Orange island and the UPB island. The testbed is also deployed for LOS and NLOS conditions. Diverse applications, such as VoIP and video conferencing are deployed to test different services, supported by WiMAX.

PTIN-UoC testbed

This testbed, deployed between the Lousã Mountain and the University of Coimbra is depicted in Figure 7.3.

The testbed is based on the Redline equipment, more specifically the AN-100U series. The advanced fire prevention scenarios impose support for mobility and NLOS conditions. The UoC is the main interface between the testbed and the GÉANT network. A point-to-point link assures the connection of the testbed to the UoC premises. The FireStation application scenario is implemented in Lousã and allows the transmission of images and text information to mobile units in the field (served by a WiMAX connection). The fixed and mobile video surveillance

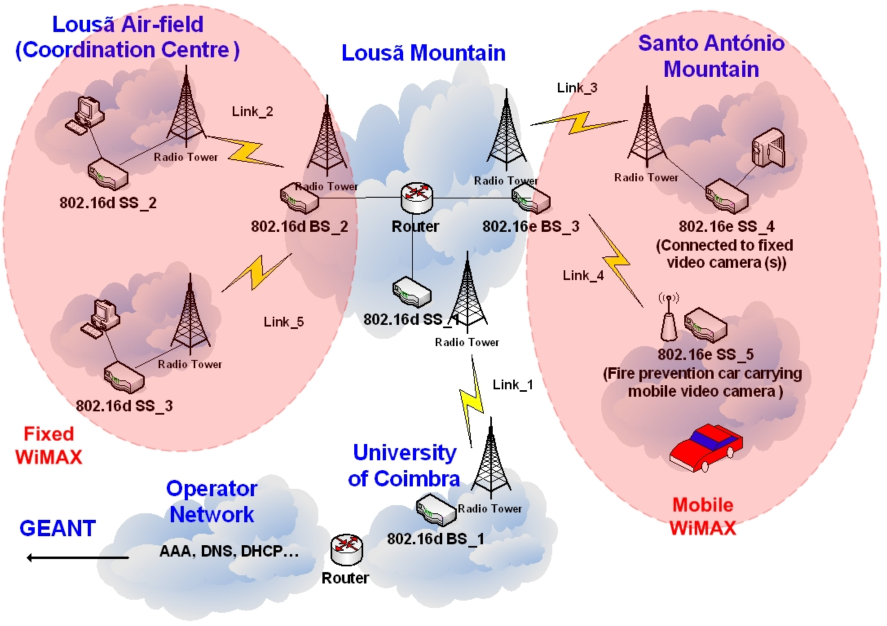


Figure 7.3: UoC Testbed
Source deliverable D5.1 Consurtium (2006b).

scenario is implemented in the Santo António mountain and allows the transmission of images, from fixed and mobile cameras, to the Coordination Centre.

The above described testbeds are connected through the GÉANT network in order to support research data exchange.

Appendix F - WEIRD Architecture

This Appendix describes the WEIRD architecture.

WEIRD architecture can be decomposed as follows:

- **Application and Service Macro-Layer**. That includes the architectural layers and functions performing management, control and also operations of data at higher layers.
- **Transport Macro-Layer**. That includes the architectural layers and functions performing management, control for resources and traffic and operations on data in order to transport the data traffic.
- **Management Plane**. Which includes management functions medium and long term related with service management at the Application and Service Macro-layer and traffic management at the Transport Macro-layer.
- **Control Plane**. This plane includes all the layers performing short term control actions. For instance, signalling for the applications and routing and traffic engineering for transport layers.
- **Transport/Data Plane**. To transfer the user application data.

The WEIRD scope includes the Subscriber Station (SS), the Access Service Network (ASN) constituted by the BS and the Access Service Network Gateway (ASN-GW) and some segments of the Connectivity Service Network (CSN). The modules included in the CSN aim at supporting the End-to-End (E2E) signalling chain and the mobility scenarios.

The WEIRD architecture was developed taking into consideration the needs for the applications existing in the project scenarios. The applications are firstly classified in two main types:

- **WEIRD-aware applications**. That are able to use the services offered by WEIRD directly.
- **Legacy applications**. Applications that can not be changed but that will use the WEIRD services via an intermediate agent - WEIRD Agent.

Another important classification of the applications considers the signalling protocol supported, mainly Session Initiation Protocol (SIP):

- **SIP-aware applications**. That support SIP. Such applications rely on the SIP protocol defined on the RFC 3261 (Rosenberg et al., 2002).
- **non-SIP applications**. That are not compliant with SIP. Such applications must be assisted by other means, such as the Next Steps in Signalling (NSIS) framework.

Security in the WEIRD architecture is distributed in three levels: At the network level, assuring that only authorized devices can use the WiMAX access channel; At the service level, only authorized users can use network resources and; At the application level, only authorized customers can activate applications. The Authentication, Authorization and Accounting (AAA) server and the SIP-Proxy, deployed in the CSN network, play an important role in the WEIRD security.

The resource provisioning in the WEIRD architecture can be performed in different zones, at individual or aggregated levels: In the SS-BS zone at per individual service flow and aggregated level and; In the zones BS-(ASN-GW), (ASN-GW)-CSN zones at aggregated level. The resource provisioning can be achieved by management actions and/or by service invocation. With the management actions, the entities negotiate the Service Level Agreement (SLA) and the Service Level Specification (SLS). The allocation of resources is done through management actions by the Resource Manager of each segment. With the service invocation the resource provisioning checks the authorization of an user and the resources requested. So, in primarily step, the user must be authenticated. After authentication, the admission control mechanisms verify the availability of resources. The quantification of resources to be admitted and provided in each segment is communicated via different levels of signalling (at the network level through NSIS and at the data link through the IEEE 802.16 mechanisms).

Figure 7.4 represents the high-level system of the WEIRD architecture. The SS/Mobile Station (MS) or CPE, the ASN and the CSN are the main entities.

The SS/MS, providing WiMAX connectivity to users, can be classified as single or multiple user. The multiple user SS may have interfaces for wired and wireless networks. As depicted in Figure 7.4, the WEIRD Agent is one software module in the SS/MS and is responsible for triggering resource provisioning for legacy applications. The basic WEIRD Agent pre-provisions resources before applications start-up, while the Enhanced WEIRD Agent performs resource reservation on-demand basis, when applications make requests.

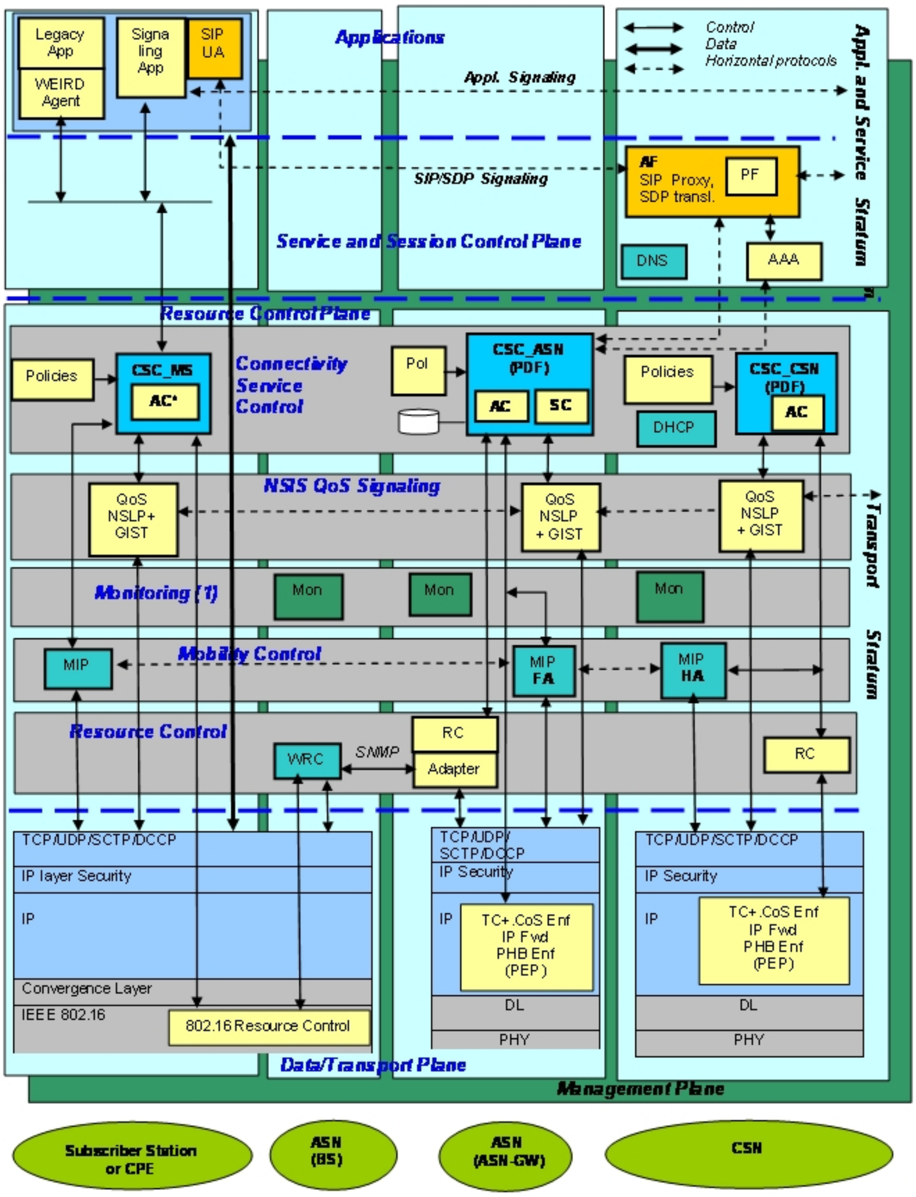


Figure 7.4: WEIRD Architecture
Source deliverable D2.3WEIRDConsurtium (2007).

The Connectivity Service Control (CSC_MS) module interacts with the WEIRD Agent and NSIS and also performs Admission Control (AC) in the SS segment in the case of a multi-user SS. The WEIRD-aware applications use the WEIRD API, an interface provided by the CSC_MS, to perform resource provisioning.

The ASN-GW is a "core entity" in the WEIRD Architecture since it manages and controls the resources in the WiMAX, BS and ASN-GW and ASN-CSN segments. This entity allows the WEIRD architecture to be vendor independent, since the Resource Controller (RC), comprised in the ASN-GW has a vendor-independent API. The ASN-GW contains interfaces to perform authentication, authorization and accounting information for QoS reservations as well for user/device access. The interface to perform AAA functions, is compliant with the Diameter protocol (Calhoun et al., 2003), which improves the Remote Authentication Dial In User Service (RADIUS) protocol (Rigney et al., 2000), widely used nowadays.

The CSC_ASN modules perform the main functions of the ASN, which include service control, admission control. The service controller processes the signalling associated to the QoS requests, triggers the AAA for applications and triggers the admission control providing the QoS parameters of the requests. The admission controller performs admission control in the wired and wireless WiMAX links. The admission controller database contains information about the network topology and information with the reserved and/or assigned resources.

The ASN-GW interfaces with NSIS, to receive and transfer QoS signalling messages necessary to perform resource reservations. The resource controller performs functions such as mapping QoS parameters to IEEE Std 802.16 Class of Service (CoS) and service flow management for WiMAX connections.

In order to allow SIP applications to perform dynamic reservations, the ASN-GW implements interfaces with the SIP proxy, to transform the SIP QoS definitions into a QoS specification (QSPEC) (Ash et al., 2007) to perform the QoS signalling. The management plane in the ASN-GW contains an interface to the resource manager, which performs resource pre-provisioning for applications.

The CSN holds the content and applications servers and other services. The SIP proxy manages application signalling and triggers resource reservation for SIP applications. The AAA server, performs the AAA functions. The networking monitoring system allows the monitorization of the ASN-GW. The WEIRD Administration Console allows to monitor the WEIRD components status. The CSC_CSN modules performs admission control in the CSN network and interfaces with the NSIS for the E2E signalling chain.

Appendix H - NIST extension

This Appendix describes the NIST extension for ns-2 and provides a comparison with other extensions for ns-2.

The ns-2 is an event simulator used to simulate network protocols such as TCP or UDP over different standard technologies (wired, wireless or satellite). Medium Access Control (MAC) and physical functionalities of IEEE Std 802.16e are implemented in an add-on package for ns-2 (Rouil, 2007). Although IEEE Std 802.16e supports different sets at physical and MAC layers, NIST add-on implements the following:

- **physical layer**
  - WirelessMAN-OFDM profile.
  - Time Division Duplexing (TDD) as the duplexing method for the Point-to-Multipoint (PMP) topology.
- **MAC layer**
  - Management messages to perform the network entry process (with no authentication).
  - IEEE Std 802.16e extensions to support scanning and handovers.
  - Fragmentation and reassembly of frames.
  - Default scheduler providing round robin uplink allocation to registered MSs according to bandwidth requested.

NIST extension is not complete, other important features of the standard are not implemented. For instance, service flows and QoS scheduling, periodic ranging and power adjustments are left outside of current implementations.

Other IEEE Std 802.16 extensions exist for ns-2. The Networks & Distributed System Laboratory (NDSL) extension (NDSL, 2007) implements service flows and QoS scheduling services. Nevertheless it is based on IEEE Std 802.16d and the documentation is rather complete.

The Computer Network Laboratory of the Korea Advanced Institute of Science and Technology (KAIST) (KAIST, 2007) has implemented an extension for the IEEE 802.16 simulation supporting the Best Effort scheduling service and a round robin scheduling among service flows. But there is no support for mobility and the documentation also lacks.

The WiMAX Forum is also developing a WiMAX system level simulation software (WiMAXForum, 2006b) addressing fixed and mobile WiMAX releases. The mobile WiMAX release supports IEEE Std 802.16e features (power saving mechanisms) as well as mobile IP mechanisms. But this release is not available to non WIMAX Forum members.

Appendix I - Applications Categorization

This Appendix describes the characteristics of the Voice and Video applications.

The WiMAX Forum in the system evaluation methodology (WiMAXForum, 2001) specifies different WiMAX traffic models, characterizing traffic in terms of bandwidth, latency and jitter. Table 7.6 depicts the characteristics of WiMAX application classes.

Class	**Application**	**Bandwidth**	**Latency**	**Jitter**
1	Multiplayer Interactive Gaming	Low (50 kbps)	Low (< 25 ms)	-
2	VoIP & Video Conference	Low (32-64 kbps)	Low (< 160 ms)	Low (< 50 ms)
3	Streaming Media	Low to High (50 kbps to 2 Mbps)	-	Low (< 100 ms)
4	Web Browsing & Instant Messaging	Moderate (10 kbps to 2 Mbps)	-	-
5	Media Content Downloads	High (> 2 Mbps)	-	-

Table 7.6: WiMAX application classes

To evaluate mobility performance and Quality of Service support in WiMAX classes 1 and 2 are chosen, since these application classes are the most demanding in terms of delay and jitter. Other authors, such as Rouil & Goilme (2006) and Leung et al. (2005) consider these kind of applications to evaluate QoS and mobility performance.

The QoS requirements for VoIP applications and video streaming applications (subset of WiMAX class 2) are resumed in Table 7.7.

Applications	**Jitter**	**Bandwidth**	**Packet Loss Rate**	**(One-way) Latency**
Voice over IP (VoIP)	Very-low (< 30ms)	Low (21 to 320kbps)	≤ 1%	Low (< 150ms)
Video Streaming	Low (< 100 ms)	Low to High (50 kbps to 2 Mbps)	≤ 5%	Moderate (≤ 4 to 5s)

Table 7.7: QoS requirements and Recommendations

The QoS requirements of VoIP applications are determined by the implemented codecs. Different voice codecs exist, such as the ITU G.726 (ITU-T, 2005b), ITU G.722 (ITU-T, 1988), ITU G.711 (ITU-T, 1972), among others. Nevertheless, the pulse code modulation (G.711) is the most used (Intel, 2003). The G.711 voice codec, when compared to other voice codecs, is not the best performant in terms of packet loss and bandwidth conservation since G.711 does not compress data. Nonetheless G.711 provides features for bandwidth conservation like the voice activity detection which allows to avoid sending full packets with silence.

Table 7.8 summarizes voice bandwidth requirements when employing G.711 codec with a Constant Bit Rate (CBR) stream.

Parameter	**Value**
Packetization Interval	20 ms
Voice Payload	160
Packets size	200 bytes. Considering the payload 160 plus the IP header (20), the UDP header (8) and the RTP header (12).
WiMAX Frame size	206 bytes. Only considering the 6 byte generic MAC header plus the 4 byte CRC. No optional sub-headers considered. In most part of the headers considered, the CRC is not included in the NIST add-on. The size of the frame depends on the message type.

Table 7.8: Voice data characteristics

Video applications have different QoS requirements, which are determined by data representation format (e.g. MPEG-4), stream type (Variable Bit Rate (VBR) or CBR). Streaming-video applications can be more tolerant to delay and jitter effects since buffer mechanisms allow to ‘absorb’ the delay variation issues.

Voice Applications

To evaluate the quality of voice applications, Mean Opinion Score (MOS) is used as a subjective measure. The 5-point scale of MOS, allow to have an evaluation of the perceived user video and voice quality in WiMAX networks. Despite the MOS scale other mechanisms exist to evaluate call quality objectively exist (Walker, 2001):

- **PSQM (ITU P.861) / PSQM+**: Perceptual Speech Quality Measure.
- **MNB (ITU P.861)**: Measuring Normalized Blocks.

- **PESQ (ITU P.862)**: Perceptual Evaluation of Speech Quality.
- **PAMS (British Telecom)**: Perceptual Analysis Measurement System.
- **The E-model**: Which is defined in the ITU-T G.107 recommendation (ITU-T, 2005a).

The Perceptual Speech Quality Measure and Perceptual Analysis Measurement System send a reference signal through the telephony network and then compare the reference signal with the signal that is received on the other end of the network. This comparison is performed by digital processing algorithms. These models are not suited for data networks since they can not determine network characteristics such as delay, jitter, and packet loss.

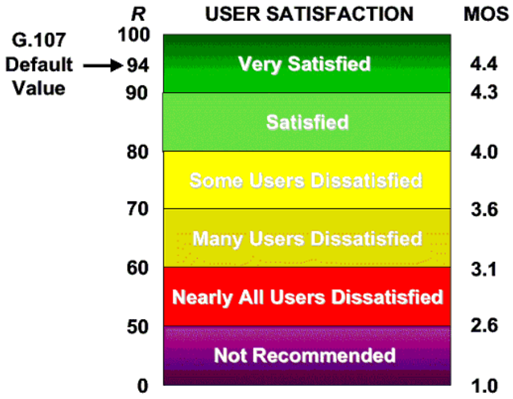


Figure 7.5: E-model and MOS mapping
Source Walker (2001).

The E-model is a cumulative non-linear quality score with a range from 0-100 (worst-best) based on a set of additive impairment factors. The Equation 7.1 demonstrates the Rating factor R of the E-model.

$$R = R_0 - I_s - I_d - I_e + A \tag{7.1}$$

R_0 corresponds to the signal-to-noise ratio or packet loss. I_s is the combination of all impairments that occur with the voice signal. I_d represents the impairment caused by delay. I_e represents the impairments caused by low bit-rate codecs. The advantage factor A is used for compensation of the impairment factors. When the R factor is obtained, it can be mapped into the MOS, as depicted in Figure 7.5.

The E-model is widely accepted and deployed for objective voice quality assessment of Voice in data networks. The E-model allows to determine if a data network is ready to carry VoIP calls.

MOS value	**Description**
5	Perceptible
4	Just perceptible but not annoying
3	Perceptible and slightly annoying
2	Annoying but not objectionable
1	Very annoying and objectionable

Table 7.9: Mean Opinion Score for Voice

Table 7.9 depicts the different values of the MOS scale for voice applications.

Video Applications

With simulation tools, such as ns-2, video quality is evaluated, using VBR/CBR traffic flows or H.263/H.264/MPEG-4 video trace files. Standard evaluation processes only include network performance data (throughput, delay, jitter, and lossrate) to determine video quality. Such metrics do not reflect the user perceived quality. The work of Kao et al. (2006) integrates Evalvid framework (Klaue et al., 2003) into ns-2, making possible the measurement of the user perceived video quality.

The user perceived video quality is measured by the Peak Signal Noise to Ratio (PSNR) parameter, which is determined by comparing each pixel in the original and distorted frame.

As with the Evalvid framework, video is described according to different characteristics, such as data representation format, resolution, framerate, compression rate and colour spaces.

The most representative picture scanning formats of the H.261 (ITU-T, 1993) and H.263 (ITU-T, 2005c) video codecs are Common Intermediate Format (CIF) and Quarter Common Intermediate Format (QCIF). With CIF the luminance sampling structure has 352 pixels per line and 288 lines per pixel. The colour difference samples are disposed such that their block boundaries coincide with luminance block boundaries as shown in Figure 7.6. For instance, with a H.261 video the CIF allows an aspect ratio of 4:3. H.263 video codec also specifies a picture clock frequency of 30000/1001 pictures per second, this means approximately 29.97 frames per second. QCIF also specifies the resolution of *176x144*, since it divides the frame height and width by two.

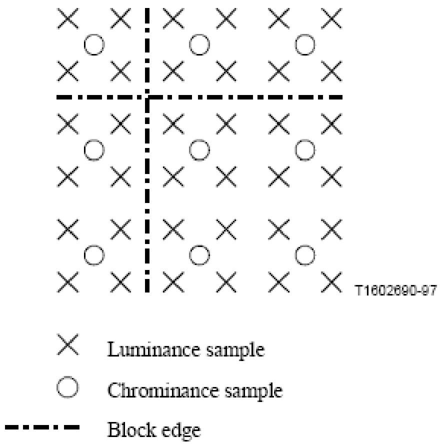


Figure 7.6: Positioning of luminance and chrominance

Video colour space is defined in the YUV format. YUV model is used in Phase Alternating Line (PAL)[2], National Television System Committee (NTSC)[3] and Sequential Color with Memory (SECAM)[4] video standards since it models the human perception of colour more closely than other colour models, such as the RGB model widely used in computer graphics hardware. The YUV model defines the colour space in terms of one lumma component (brightness) and two chrominance (colour) components. The Y channel represents the lumma, brightness or lightness and is decodable by black and white TVs. While the U and V channels represent the colour components. The U channel corresponds to the difference between blue minus lumma (B-Y). Thus the V channel corresponds to the difference between red minus lumma (R-Y).

The video must be encoded into a Moving Pictures Experts Group (MPEG) data format to be transported over UDP or TCP connections. The MPEG-4 format (JTC1/SC29/WG11, 2002), defined in the ISO/IEC 14496 standard, extends MPEG-1 standard adding new features such as support for 3-D rendering and digital rights management.

[2] Used in Europe and other countries.

[3] Used in the North United States of America.

[4] Used in France.

The resynchronization approach of MPEG-4 is based on the Group of Blocks (GOB) used by the H.261 and H.263 standards. Each GOB contains macroblocks and specifies the order in which intra-frames and inter-frames are arranged. The GOB constitutes a group or successive pictures within a MPEG-coded video stream; and each video stream consists of successive GOPs. Group of Pictures (GOP) can contain the following picture types:

- **I-picture** (Intra coded picture) reference picture, corresponds to a fixed image and is independent of other picture types. Each GOB begins with this type of picture in the Intra mode.

- **P-picture** (Predictive coded picture) contains difference information from the preceding I or P-Frame. Always coded in the Inter mode.

- **B-picture** (Bidirectionally predictive coded pictures) contains difference information from the preceding and/or following I or P-Frame. This type of frames achieve the highest compression requiring the lowest transmission bandwidth. The I-frames have the lowest compression of the three frame types but can be encoded and decoded faster.

To evaluate the video quality at the receiver side the PSNR method is used as an objective metric of performance. PSNR method allows to evaluate the distortion introduced by the network alone[5]. Table 7.10 demonstrates the relation between PSNR and MOS 5-point scale.

PSNR[dB]	**MOS value**	**Description**
> 37	5	Perceptible (Excellent)
31 - 37	4	Just perceptible but not annoying (Good)
25-31	3	Perceptible and slightly annoying (Fair)
20-25	2	Annoying but not objectionable (Poor)
< 20	1	Very annoying and objectionable (bad)

Table 7.10: Mean Opinion Score for Video

The PSNR is calculated frame by frame, what represents a disadvantage with videos with higher number of frames. Chia-Yu et al. (2006) use the decodable frame rate to avoid the PSNR overhead calculations. The decodable frame rate

[5] Ignoring the distortion caused by the encoding and decoding processes.

corresponds to the number of decodable frames over the total number of frames. Since in a GOB the I frame is decodable only if all the packets that belong to the I frame are received. The P frame is decodable only if the preceding I or P frames are decodable and all the packets that belong to the current P frame are received as well. The B frame is decodable only if the preceding and succeeding I or P frame are both decodable and all the packets that belong to the current B frame are all received.

Video Evaluation Process

The video evaluation process using the Evalvid framework consists on the different steps. First, videos in the H.264 format are converted into the YUV format (a raw format without loss). Second, a reference video file is created by converting a MPEG4 video which has been converted from the YUV video file. This reference video file allows the determination of MOS of the original video file and is used later to retrieve MOS of the transmitted videos. Third, MPEG4 video file is prepared to be transmitted over the network, *MP4Box* utility creates RTP streams that allow the transmission of the video file using RTP protocol. Fourth, video is transmitted over the network, while at the same time traces of the transmitted and received packets are collected at the sender and receiver side respectively. Fifth, a tool which compares the traces, the resultant transmission file of *mp4trace* and the original MPEG4 video file allows the construction of the transmitted video. And finally the video is encoded into YUV format to be compared with the original YUV video file to determine the Peak Signal Noise to Ratio (PSNR) and the respective MOS.