Abstract:
This is the first Deliverable of workpackage WP1 of the Moby Dick project. It describes the Moby Dick overall architecture as defined after an overall project duration of ten months up to the date of preparation.

Keyword list: UMTS, W-CDMA, Mobile IP, QoS, Mobility, AAA, Charging
... For every art aims at this, that the thing which has been made should be adapted to the work for which it has been made; ...

Marcus Aurelius Antoninus, "Meditations",
Book VI, Chapter 16.
# Table of Contents

EXECUTIVE SUMMARY .............................................................................................................. 7

ABBREVIATIONS ......................................................................................................................... 8

1 INTRODUCTION .......................................................................................................................... 10

2 MOTIVATION .............................................................................................................................. 11

3 OVERALL MOBY DICK OPERATION ...................................................................................... 13
   3.1 Stationary use ......................................................................................................................... 13
      3.1.1 Authentication ................................................................................................................. 13
      3.1.2 Profile ............................................................................................................................. 13
   3.2 Mobile use .............................................................................................................................. 14
      3.2.1 Handover .......................................................................................................................... 14
      3.2.2 Paging .............................................................................................................................. 14

4 MOBY DICK REQUIREMENTS AND CONSTRAINTS ............................................................. 14
   4.1 User Service Requirements .................................................................................................. 15
      4.1.1 Premium Service ............................................................................................................. 15
      4.1.2 Regular Signature Service .............................................................................................. 15
      4.1.3 Pre-Paid Service .............................................................................................................. 15
   4.2 Network evolution constraints ............................................................................................ 16
   4.3 Technology specific requirements ....................................................................................... 16
      4.3.1 W-CDMA specifics ........................................................................................................ 16

5 MOBY DICK ARCHITECTURE .............................................................................................. 19
   5.1 Conceptual view .................................................................................................................... 19
   5.2 Mobile Terminal Software Architecture ............................................................................. 20
      5.2.1 Functional elements ........................................................................................................ 21
      5.2.1.1 Enhanced TCP/IP stack ............................................................................................. 21
      5.2.1.2 Networking Control Panel (NCP) ................................................................................ 22
      5.2.1.3 Mobile-Terminal Networking Manager (MTNM) ......................................................... 22
      5.2.1.4 Radio Modem Support for WCDMA (ASWCDMA) ...................................................... 22
      5.2.1.5 Radio Convergence Function for WCDMA (RCFWCDMA) ........................................... 22
      5.2.1.6 Radio Channel Manager (RCM) .................................................................................. 22
      5.2.2 Interface definitions ........................................................................................................ 23
   5.3 Radio Gateway Software Architecture ............................................................................... 23
      5.3.1 Functional elements ........................................................................................................ 24
      5.3.1.1 Interworking Function (IWF) ..................................................................................... 24
   5.4 Access Router Architecture ................................................................................................. 24
   5.5 Physical view on the Moby Dick Architecture .................................................................... 24
   5.6 Physical Components .......................................................................................................... 25
5.7 Correspondent Node, e.g. web server
5.7.1 Home Agent
5.7.2 Paging Agent
5.7.3 Paging Agent local
5.7.4 Radio Gateway
5.7.5 Access Router
5.7.6 Wireless LAN Access Router
5.7.7 AAAC Server
5.7.8 QoS broker
5.7.9 Core Network Router

6 SPECIAL INTERFACE ISSUES

6.1 Integrated Session Setup procedure
6.1.1 Assumptions
6.1.2 Requirements
6.1.3 MAQ Scenario
   6.1.3.1 Pros of MAQ
   6.1.3.2 Cons of MAQ
6.1.4 MQA Scenario
   6.1.4.1 Pros of MQA
   6.1.4.2 Cons of MQA
   6.1.4.3 Accounting
   6.1.5 Summary of session setup scenarios

6.2 Registration Scenario
6.2.1 CoA Acquisition
6.2.2 Problem statements
6.2.3 Proposed solution
6.2.4 Discussion & Open Issues

6.3 Handover scenario

7 SUMMARY AND OUTLOOK

8 REFERENCES

9 APPENDIX A: FIRST VERSION OF D0201

10 APPENDIX B: FIRST VERSION OF D0301

11 APPENDIX C: FIRST VERSION OF D0401

12 APPENDIX D: TERMINOLOGY

12.1 Network Components
   12.1.1 Access Network (AN)
   12.1.2 Access Routers (AR)
   12.1.3 Mobile Node (MN)
   12.1.4 Mobile Host (MH)
   12.1.5 Access Link (AL)
   12.1.6 Access Point (AP)
   12.1.7 Access Gateway (AG)
   12.1.8 Access Network (AN)
<table>
<thead>
<tr>
<th>Section</th>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1.9</td>
<td>Serving Access Router (SAR)</td>
<td>42</td>
</tr>
<tr>
<td>12.1.10</td>
<td>Old Access Router (OAR)</td>
<td>43</td>
</tr>
<tr>
<td>12.1.11</td>
<td>New Access Router (NAR)</td>
<td>43</td>
</tr>
<tr>
<td>12.1.12</td>
<td>Candidate Access Router (CAR)</td>
<td>43</td>
</tr>
<tr>
<td>12.2</td>
<td>Network Protocol Terminology</td>
<td>43</td>
</tr>
<tr>
<td>12.2.1</td>
<td>Care-of Address (CoA)</td>
<td>43</td>
</tr>
<tr>
<td>12.2.2</td>
<td>Correspondent Node (CN)</td>
<td>43</td>
</tr>
<tr>
<td>12.2.3</td>
<td>AAAH</td>
<td>43</td>
</tr>
<tr>
<td>12.2.4</td>
<td>AAAF</td>
<td>43</td>
</tr>
<tr>
<td>12.2.5</td>
<td>Foreign Network</td>
<td>43</td>
</tr>
<tr>
<td>12.2.6</td>
<td>Home Address (HA)</td>
<td>43</td>
</tr>
<tr>
<td>12.2.7</td>
<td>Home Network (HN)</td>
<td>43</td>
</tr>
<tr>
<td>12.2.8</td>
<td>IP Diversity</td>
<td>43</td>
</tr>
<tr>
<td>12.2.9</td>
<td>Link-layer address</td>
<td>43</td>
</tr>
<tr>
<td>12.2.10</td>
<td>Visited network</td>
<td>43</td>
</tr>
<tr>
<td>12.2.11</td>
<td>Administrative Domain</td>
<td>43</td>
</tr>
<tr>
<td>12.2.12</td>
<td>Attendant</td>
<td>43</td>
</tr>
<tr>
<td>12.2.13</td>
<td>Foreign domain</td>
<td>44</td>
</tr>
<tr>
<td>12.2.14</td>
<td>Home domain</td>
<td>44</td>
</tr>
<tr>
<td>12.3</td>
<td>Mobility Management Terminology</td>
<td>44</td>
</tr>
<tr>
<td>12.3.1</td>
<td>Paging</td>
<td>44</td>
</tr>
<tr>
<td>12.3.2</td>
<td>Paging Area</td>
<td>44</td>
</tr>
<tr>
<td>12.3.3</td>
<td>User mobility</td>
<td>44</td>
</tr>
<tr>
<td>12.3.4</td>
<td>Personal mobility</td>
<td>44</td>
</tr>
<tr>
<td>12.3.5</td>
<td>Handover (also known as handoff)</td>
<td>44</td>
</tr>
<tr>
<td>12.3.6</td>
<td>Context-aware Handover</td>
<td>44</td>
</tr>
<tr>
<td>12.3.7</td>
<td>Network Assisted Handover</td>
<td>44</td>
</tr>
<tr>
<td>12.3.8</td>
<td>Roaming</td>
<td>44</td>
</tr>
<tr>
<td>12.4</td>
<td>Security</td>
<td>44</td>
</tr>
<tr>
<td>12.4.1</td>
<td>Authentication</td>
<td>45</td>
</tr>
<tr>
<td>12.4.2</td>
<td>Authorization</td>
<td>45</td>
</tr>
<tr>
<td>12.4.3</td>
<td>Credential(s)</td>
<td>45</td>
</tr>
<tr>
<td>12.4.4</td>
<td>Data confidentiality</td>
<td>45</td>
</tr>
<tr>
<td>12.4.5</td>
<td>Data integrity</td>
<td>45</td>
</tr>
<tr>
<td>12.4.6</td>
<td>Data security</td>
<td>45</td>
</tr>
<tr>
<td>12.4.7</td>
<td>Digital signature</td>
<td>45</td>
</tr>
<tr>
<td>12.4.8</td>
<td>Encryption</td>
<td>45</td>
</tr>
<tr>
<td>12.4.9</td>
<td>Identification</td>
<td>45</td>
</tr>
<tr>
<td>12.4.10</td>
<td>Masquerade attack</td>
<td>45</td>
</tr>
<tr>
<td>12.4.11</td>
<td>Non-repudiation service</td>
<td>45</td>
</tr>
<tr>
<td>12.4.12</td>
<td>Replay attack</td>
<td>45</td>
</tr>
<tr>
<td>12.4.13</td>
<td>Repudiation</td>
<td>45</td>
</tr>
<tr>
<td>12.4.14</td>
<td>Security association</td>
<td>46</td>
</tr>
<tr>
<td>12.4.15</td>
<td>Security audit</td>
<td>46</td>
</tr>
<tr>
<td>12.4.16</td>
<td>Security audit trail</td>
<td>46</td>
</tr>
<tr>
<td>12.4.17</td>
<td>Security policy</td>
<td>46</td>
</tr>
<tr>
<td>12.5</td>
<td>QoS Terminology</td>
<td>46</td>
</tr>
<tr>
<td>12.5.1</td>
<td>Best-Effort Traffic</td>
<td>46</td>
</tr>
<tr>
<td>12.5.2</td>
<td>Premium Traffic</td>
<td>46</td>
</tr>
<tr>
<td>12.5.3</td>
<td>Signalling Burst</td>
<td>46</td>
</tr>
<tr>
<td>12.5.4</td>
<td>Signalling Load</td>
<td>46</td>
</tr>
<tr>
<td>12.5.5</td>
<td>Signalling Path</td>
<td>46</td>
</tr>
<tr>
<td>12.5.6</td>
<td>Best-Effort Traffic Delay</td>
<td>46</td>
</tr>
<tr>
<td>12.5.7</td>
<td>Multicast Resource Reservation Session</td>
<td>46</td>
</tr>
<tr>
<td>12.5.8</td>
<td>Premium Traffic Delay</td>
<td>46</td>
</tr>
<tr>
<td>12.5.9</td>
<td>Reservation Capable Router</td>
<td>46</td>
</tr>
<tr>
<td>12.5.10</td>
<td>Reservation Initiator</td>
<td>46</td>
</tr>
</tbody>
</table>
13 APPENDIX E: BACKGROUND INFORMATION ........................................... 48

13.1 W-CDMA .............................................................................. 48
   13.1.1 UMTS Existing Architecture ........................................ 48
   13.1.2 Access Stratum Protocol Layers .................................. 49
   13.1.3 Mobile Node (MN) modes: ........................................... 53

13.2 Ethernet ............................................................................ 54

13.3 Wireless LAN ..................................................................... 54

14 APPENDIX F: RELATED WORK ................................................... 57

14.1 Related Projects ................................................................. 57
   14.1.1 WINE GLASS .............................................................. 57
   14.1.1.1 Radio Gateways ....................................................... 57
   14.1.1.2 Mobility Management ............................................. 57
   14.1.1.3 Quality of Service .................................................. 58
   14.1.1.4 Authentication, Authorisation and Accounting .......... 58

14.2 Standardisation Bodies ....................................................... 59
   14.2.1 MWIF Overview .......................................................... 59
   14.2.2 3GPP2 ........................................................................ 60
   14.2.3 IETF and IRTF approaches .......................................... 62
      14.2.3.1 Seamobyobjectives and historic review ................. 62
      14.2.3.2 Hierarchical Mobile IP ......................................... 63
      14.2.3.3 IETF AAA ............................................................ 64
      14.2.3.4 IRTF AAAArch ................................................... 65

15 APPENDIX G: W-CDMA INTERFACE ........................................ 67
Executive Summary

In recent years, two parallel developments could be observed in telecommunications. First, the tremendous success of the Internet and second, the success of the mobile telephones. UMTS is the technology which will integrate both developments. However, it is not clearly visible in the existing architecture which of the two network philosophies, connection oriented 2 G based architecture or packet-oriented Internet compatible technology, will dominate. Currently researchers and marketing people from both Network provider and equipment vendor tend towards a long term All-IP based solution. Both technologies have their advantages and disadvantages and, since we have never seen a revolution in the network infrastructure, the transition process from a connection-oriented world to a packet-oriented world will be smooth and backward compatibility is a very important issue.

Within the Moby Dick project, we took the opportunity to go straight forward towards an All-IP based solution without taking care of such backward compatibility issues to the connection-oriented “Telephone World”, however, to the currently deployed Internet. Based on this assumption, a wireless IP world replacing any connection-oriented elements of the network, the IST project Moby Dick develops and implements an architecture which substitutes all the network elements and mechanisms historically based on the GSM based network architecture and combines these with available IP based mechanisms and network elements to come to a scalable network architecture which would be a possible candidate for the 3.5 G and beyond based wireless access network infrastructure. At the end of this project the consortium should be able to give an answer to the question if the Internet Protocol is able to replace the existing connection-oriented infrastructure. The Moby Dick goal is to answer this question quantitatively and qualitatively. Where required, Moby Dick modifies and changes existing protocols but does not target the development of fundamental new protocols.
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAAF(domain)</td>
<td>Foreign AAA server</td>
</tr>
<tr>
<td>AAA.h</td>
<td>Home AAA server</td>
</tr>
<tr>
<td>AAA.f</td>
<td>Foreign AAA server</td>
</tr>
<tr>
<td>AG</td>
<td>Access Gateway</td>
</tr>
<tr>
<td>AR</td>
<td>Access Router</td>
</tr>
<tr>
<td>ARQ</td>
<td>Automatic Repeat Request</td>
</tr>
<tr>
<td>AS</td>
<td>Access Stratum</td>
</tr>
<tr>
<td>ASM</td>
<td>Application Specific Module</td>
</tr>
<tr>
<td>BCCCH</td>
<td>Broadcast Control Channel</td>
</tr>
<tr>
<td>BU</td>
<td>Binding Update</td>
</tr>
<tr>
<td>CCCH</td>
<td>Common Control Channel</td>
</tr>
<tr>
<td>CN</td>
<td>Corresponding Node</td>
</tr>
<tr>
<td>CTCH</td>
<td>Common Traffic Channel</td>
</tr>
<tr>
<td>CoA</td>
<td>Care-of Address</td>
</tr>
<tr>
<td>DC</td>
<td>Data Channel</td>
</tr>
<tr>
<td>DCCH</td>
<td>Dedicated Control Channel</td>
</tr>
<tr>
<td>DCF</td>
<td>Distributed Co-ordination Function</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>DTCH</td>
<td>Dedicated Traffic Channel</td>
</tr>
<tr>
<td>FDD</td>
<td>Frequency Duplex Division</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>GC</td>
<td>General Control</td>
</tr>
<tr>
<td>GGSN</td>
<td>Gateway GPRS Support Node</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GTP</td>
<td>GPRS Tunnelling Protocol</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>HMIP</td>
<td>Hierarchical Mobile IP</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IRTF</td>
<td>Internet Research Task Force</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber ID</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LLA</td>
<td>Local Link Acquisition</td>
</tr>
<tr>
<td>LDAP</td>
<td>Light-weight Directory Access Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MAQ</td>
<td>Sequence: Mobile Node, AAA Framework, QoS Framework</td>
</tr>
<tr>
<td>MAP</td>
<td>Mobility Anchor Point</td>
</tr>
<tr>
<td>MIP</td>
<td>Mobile IP</td>
</tr>
<tr>
<td>MT</td>
<td>Mobile Terminal</td>
</tr>
<tr>
<td>MN</td>
<td>Mobile Node</td>
</tr>
<tr>
<td>MQA</td>
<td>Sequence: Mobile Node, QoS Framework, AAA Framework</td>
</tr>
<tr>
<td>MRF</td>
<td>Media Resource Function</td>
</tr>
<tr>
<td>NAI</td>
<td>Network Access Identifier</td>
</tr>
<tr>
<td>NAS</td>
<td>Non Access Stratum</td>
</tr>
<tr>
<td>NAR</td>
<td>New Access Router</td>
</tr>
<tr>
<td>OAR</td>
<td>Old Access Router</td>
</tr>
<tr>
<td>ODMA</td>
<td>On Demand Multiple Access</td>
</tr>
<tr>
<td>ODBC</td>
<td>Open Data Base Connectivity</td>
</tr>
<tr>
<td>ODTCCH</td>
<td>ODMA Dedicated Traffic Channel</td>
</tr>
<tr>
<td>OCCCH</td>
<td>ODMA Common Control Channel</td>
</tr>
<tr>
<td>ODCCH</td>
<td>ODMA Dedicated Control Channel</td>
</tr>
<tr>
<td>PA</td>
<td>Paging Agent</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>PCCH</td>
<td>Paging Control Channel</td>
</tr>
<tr>
<td>PCF</td>
<td>Point Coordination Function</td>
</tr>
<tr>
<td>PDCP</td>
<td>Packet Data Convergence Protocol</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>QoSB(domain)</td>
<td>Quality of Server Broker including a policy server</td>
</tr>
<tr>
<td>RBE</td>
<td>Rules Based Engine</td>
</tr>
<tr>
<td>RLC</td>
<td>Radio Link Control</td>
</tr>
<tr>
<td>RNS(domain)</td>
<td>Radio Network Server</td>
</tr>
<tr>
<td>RR(subnet)</td>
<td>Radio Router for a specific sub network</td>
</tr>
<tr>
<td>RRC</td>
<td>Radio Resource Control</td>
</tr>
<tr>
<td>SAP</td>
<td>Service Access Point</td>
</tr>
<tr>
<td>SHCCH</td>
<td>Shared Channel Control Channel</td>
</tr>
<tr>
<td>SCM</td>
<td>Session Control Manager</td>
</tr>
<tr>
<td>SGSN</td>
<td>Serving GPRS Support Node</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLS</td>
<td>Service Level Specification</td>
</tr>
<tr>
<td>TDD</td>
<td>Time Division Duplex</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>URP</td>
<td>User Registration Protocol</td>
</tr>
<tr>
<td>W-CDMA</td>
<td>Wideband Code Division Multiple Access</td>
</tr>
</tbody>
</table>
1 Introduction

This deliverable describes the first version of the architecture of the Moby Dick network infrastructure. The goal is to provide QoS-enabled and AAA supported mobility on a heterogeneous network infrastructure. So Moby Dick merges mechanisms of three different research areas namely QoS, AAA, and Mobility management. This document should be regarded as baseline document throughout the whole duration of the project. Moby Dick targets a generic architecture supporting all kind of layer 2 access technology, however, the architectural considerations are restricted to Ethernet, Wireless LAN, and W-CDMA technologies. Since the integration process of QoS, Mobility, and AAA issues to provide a M-commerce capable all-IP based wireless Internet infrastructure is quite complex it is quite supposable that the first trial of the architecture specification does not require further iteration processes towards an open, stable, and scalable platform for “3.5 G and beyond” based access networks.

The big challenge within the architecture is to find an ideal mixture of QoS, Mobility, and AAA elements, mechanisms and functions which approach as far as possible to the optimised Moby Dick architecture. The definition of the Moby Dick architecture can be regarded as an optimisation problem since each of the three major research areas has already solutions for various problems, however, it is clear that first, the combination of these individual mechanisms can not be combined from a technical point of view boundlessly and second, mechanisms and elements of one research area may have a negative impact on the mechanisms and elements of the other research area. For this reason, the Moby Dick architecture will be a best practice compromise between mechanisms, requirements, and solutions from the above mentioned three research areas.

The structure of the document is as follows:

Chapter 2 starts with an overall motivation for the project Moby Dick. Here the authors would like to summarise again the motivation for the overall project.

Since Moby Dick is targeting a “3.5 G and beyond” wireless network infrastructure assumptions and requirements based on selected usage scenarios are required to have a realistic input to the architecture definition. Chapter 3 describes from a non-technicians user point of view a general summary of the general Moby Dick overall operations scenario and gives a brief description of business model related issues.

Chapter 4 points out requirements extracted from the operational scenario described in chapter 3. These requirements are high level requirements which will be transferred into lower layer requirements within the different workpackages.

Chapter 5 describes how these requirements are mapped first into a functional architecture which will then in a second section be mapped down to the first version of the Moby Dick overall architecture.

Chapter 6 summarises some technical details which are important to the whole project.

In chapter 7, a conclusion is given.

The overall structure of the project has the following nature: WP1 does define the overall Moby Dick architecture. WP2, WP3, and WP4 are the so-called implementation workpackages. Here QoS issues (WP2), Mobility related issues (WP3) and AAAC related issues (WP4) will be specified based on the overall architecture on a more detailed level. The current status of these implementation workpackages can be found in Annex A, Annex B, and Annex C respectively.
2 Motivation

The personal communication networks that are operating nowadays, and also those that are planned for deployment in the near future, are based on the architectures of Public Switched Telephone Networks (PSTN), Integrated Services Digital Networks (ISDN), 2G and 3G mobile. These network architectures are quite different, which makes their interworking quite complex. One thing that makes them similar, however, is that they are based on connection-oriented service principle. Voice services are still predominant there.

Computer networks have always been used in quite different application areas. Because of different networking technologies, their deployment also poses interoperability problems. These networks have always been packet-switched.

The advances in packet-data communications have initiated the departure from traditional circuit switching paradigm in personal communications in favour of packet-switching. This process, known as convergence, is quite advanced now in fixed (terrestrial) networks.

The situation in mobile communications networks, however, is different. The wireless environment poses a set of complex technical challenges that have to be addressed to enable packet-switched services. Among the most important are: mobility management, location management, user identification, communications re-routing, control of the radio communications channel, and many others.

Nevertheless, the recent advances in packet data communications have created an outstanding opportunity for development of fully integrated wireless/wired environments. The ability of IP protocol suite to support aggregation of different types of traffic designates this protocol as a prospective candidate for provisioning of end-to-end services that are much independent of the underlying media, diversification of services, differentiation of quality of service, as well as simplification of network management.

The importance of IP communications has already been recognised in UMTS where IP-based services are supported by means of tunnelling.

Many telecom operators question the concept of bringing packet switching into the existing UMTS environments. It is believed that, anyway, this is an intermediate step towards pure IP-based solutions. There also exists a strong belief that many of the required networking components are already in place, and only improvements are necessary. But there is also much uncertainty about the scope and depth of the necessary changes [45].

An issue that is central to the Moby Dick Project is that the behaviours of the information-driven society create an unprecedented raise of expectations with respect to the infrastructure. The ability to create services that respond to the demand becomes a major issue that will determine the success of the solutions that will stem from the Moby Dick network architecture. The evolving behaviours affect usage scenarios that, in turn, call for deployment of new business models. The need to change the way of thinking of Internet in terms of business relations will become even more urgent as the mobile personal communications will become a pre-dominant form of activity in the Internet.

Taking this point of view, the challenge of Moby Dick is to develop a mobile, all-IP QoS-enabled and audited network architecture.

The unresolved architectural issues that are of special focus in Moby Dick fit into several categories:

?? The mobility model

These problems are related to the management of data flow, which has to be sustained during handover between two cells. This should be true for handovers within the same networking technology (horizontal handover), as well as handovers between distinct technologies (vertical handovers).

While Mobile IPv6 as generic mobility management is intended to provide macro-mobility (inter-domain handoffs), the mobility support in Moby Dick has to be enhanced to handle micro-mobility (intra-domain handoffs). Micro-mobility is of central importance here, since most of the handovers are expected to take place within an administrative domain. Standard Mobile IPv6 itself is incapable to ensure service disruption times short enough to meet the requirements of real-time traffic. Some enhancements need to be introduced, evaluated in simulation, and validated in the field-trials [42].

?? Subscriber management

The key focus of subscriber management is to develop a uniform subscriber management infrastructure that includes authentication, authorisation, accounting, and charging (AAAC). This strategy must fit into the base mobility model, and at the same time has to consider different business models and charging schemes that might be involved. The need for tight relation with QoS
component of the infrastructure, as well as some performance considerations increase the complexity of it [44].

?? Resource management problems

The management problems are concerned with the resource usage both in the access part of the network and in the IP core network. Efficient resource management is required to assure appropriate QoS levels for QoS-sensitive end-to-end IP-based services. The definition of the services, resource apportioning across the classes as well as definition of the interface to the charging component is part of it [43].

?? The physical layer problems

These relate to the fundamental connection capabilities of the underlying networking technologies, and the need for separation of those control functions that are physical-media dependent, and those that can be pushed to IP layer.

When considered separately, each of the above-listed issues presents a scientific and technological challenge. When taken together, they set the framework for research on prospective and future-proof architecture for mobile communications.
3 Overall Moby Dick Operation

Within this chapter, a basic Moby Dick operational scenario is described.

At first, each user is from a contractual point of view somehow assigned to his home domain. Within Moby Dick, this home domain could be from a technical point of view an Ethernet according to 802.3 standard, a wireless LAN (802.11), or a Moby Dick specific WCDMA TDD cell. Furthermore, each domain consists of at least one IP subnet. Each IP subnet corresponds to one lower layer network access cell. As already mentioned, this can be either an 802.11, 802.3 or W-CDMA based network. In turn, every mobility management related operation (handover) is a joint layer 2 and layer 3 supported operation.

As already mentioned, a user has a contract with the provider of the home network (home domain). This provider maintains an AAA entity (AAA.h) which is responsible for validating and verifying any credentials pertinent to the user. This kind of authority can be either located at the user premises or at any other location within the domain of the home network provider. Contract details of the contract between user and provider are agreed based on a Service Level Agreement (SLA) which is transformed into a User Profile which is stored on the AAA.h entity. Content of this profile is next to others, roaming permissions and QoS parameters. A Mobile User is allowed to connect itself using any mobile device in any location to the network. The provider of the foreign network (foreign means here that the use has no direct contract with the network the user wants to use) provides the user with network resources/service according to the SLA reflected in the profile of the home domain. Here it might be the case that no roaming agreement exists between the provider of the home domain and the provider of the foreign domain (of course this is part of the profile) and in this case no service is delivered to the mobile user.

A user is allowed to move around and the required hand-over procedures enable the user to maintain any existing connection while moving is based on the agreed SLA with the provider of the home network. Furthermore, within Moby Dick, different business models are considered (e.g. pre-paid or post-paid charging) and the resource distribution/service consummation is somehow documented for Auditing and appropriate charging issues.

Details of the QoS concept are provided in the section D0201 of the Annex, details of the Mobility Management scenario are provided in section D0301 of the Annex and all the AAA specific issues are provided in section D0401 of the Annex.

In the following, based on the above described high level scenarios, some more technology-specific considerations are summarised.

Within a framework that integrates mobility, AAA, and QoS in heterogeneous networks, a wide range of ways in which the user perceives the “network” is possible. Obviously, some assumptions need to be made about how the Moby Dick network will be used as an aid to make design decisions. From a wide range of possible scenarios, we need to concentrate on a few to optimise the effort and therefore the cost of the network and the associated functions.

The following sections identify some typical, more detailed usage scenarios. Some of these are proposed for implementation in the Moby Dick project. This needs to be done separately for two situations, i.e.:

i) When stationary without changing the point of attachment to the network and
ii) when changing the point of attachment via handover.

3.1 Stationary use

3.1.1 Authentication

It is assumed that the user will be required to supply credentials for authentication. More detailed authentication procedures will be defined within the framework of WP4. Following this, the network will need to manage the maintenance of the authorisation for the use of the network without intervention of the user – since user mobility will be supported, some basic user involvement is required. Further, in the case of emergency calls and some set of free services, the user will not be required to authenticate himself or herself.

3.1.2 Profile

Similar to the existing 2G architecture, the operator maintains a user profile identifying the user. The detailed structure of the profile depends on the business case. The profile reflects a contract between the user and the service provider.
3.2 Mobile use

There is a number of assumptions that could be made for a mobile user:

1. The mobile user moves mainly within the same domain and technology during a session. The access point may be changed frequently. Before moving to a new domain or technology, the old session is usually closed and a new one started. Handover between technologies and domains are therefore very infrequent.

2. The mobile user moves mainly within the same domain, but the access point and the technology may be changed frequently. Before moving to a new domain, the old session is usually closed and a new one started. Handover between domains are therefore very infrequent.

3. The mobile user moves mainly within the same technology, but the access point and the domain may be changed frequently. Before moving to a new technology, the old session is usually closed and a new one started. Handover between technologies are therefore very infrequent.

4. The mobile user moves in an environment where the access point, the domain, or the technology may be changed frequently. Handovers of all types occur quite frequently.

For the Moby Dick project, we cater for assumption for all 4 assumptions. Knowing well that integrating AAA, Mobility and QoS signalling require additional time which may not be available for supporting seamless handover without any degradation of the service quality during handover, Moby Dick tries to go for a compromised solution considering requirements from all 3 directions (AAAC, Mobility, and QoS).

3.2.1 Handover

It should be noted that seamless mobility cannot be provided without paying some price with respect to QoS and AAA. While loss of data may not be noticeable, even the best handover will provide some additional albeit small delay, which must be reflected in the QoS models.

Taking these as the underlying assumptions, we arrive at the following requirements:

- The implementation in the Moby Dick project will ensure seamless intra-domain handover, i.e. handover with minimum delay and loss of data. However, some deterioration of perceived QoS due to the small delay may need to be accepted. This maximum loss of quality during handover should be quantified and guaranteed.
- Inter-domain handover may not be seamless because of additional AAAC specific effort. Such a handover may result in a short interruption of the session with possible loss of data. This is acceptable because it is assumed that this will be very infrequent and noticeable for the user, e.g. because he or she is crossing the border to another country.

Handover is likely to be a time where the offered QoS and cost may change. This will have to be handled automatically by the range of values given in the profile.

3.2.2 Paging

In the case of paging, some additional delay is inevitable as the paging agent exchanges messages with the mobile host. The following is assumed:

- Paging is only invoked in the beginning of a session (from the correspondent node).
- Paging is only invoked by signalling messages (from the correspondent node). This implies that under no circumstances date packets will invoke paging and that this case is not considered.
- QoS requirements involving loss of data can be met, QoS requirements on delay may not.

4 Moby Dick Requirements and Constraints

Having the generic scenario described in chapter 3 in mind, within this chapter requirements for the architecture are presented. The requirements comprise user acceptance considerations as well as technology-specific issues and can be split into several parts which are presented in the next sections of this chapter. Two major types of requirements were placed on the development of the Moby Dick architecture. The first type of requirements were centred on the end-user service, what should be provided to the user – and these included the requirements from the points of view of both the user itself and from the service provider. The second type of requirements were concerned with the network: the network should be developed based on existing IETF mechanisms (added with “sensible” evolutions) in order to be able to seamlessly interoperate with the overall Internet.
4.1 User Service Requirements

The basic requirement from the user point-of-view was that the Moby Dick network should support voice and data services, across three different technologies (Ethernet, wireless LAN – 802.11 -, W-CDMA), with quality of service provision comparable to future UMTS networks.

From the service provider’s point of view, the requirements were substantially more complex. Service providers required this network:

1. to be as controllable as a UMTS network, which had major impact on the usual approach to IP network services.
2. the network had to be fully audited, individually per customer, with (near) live charging. Thus each user may have an individual profile, i.e. a description of the different network services he may access in the network, depending on the specific service level agreement he has. The increase effort in AAAC required is very significant, when compared with traditional IP networks; however, is at the same level of current mobile telecommunication networks.

Since we address a mobility architecture, there are several mobility concepts to be supported. These concepts are terminal mobility, user mobility, and service mobility. Within Moby Dick, a user must not be bound to certain devices (user mobility), however during and after a session the system must be able to identify which user is using or has used which devices, so user mobility will be supported, however, service mobility concepts are out of the scope of this project.

In Moby Dick it is assumed that the Telecommunication Operators will offer a huge variety of network services. The associated management costs would be very high, both in terms of resources and time. Thus some “target” types of network services to be provided in this network were identified (this following list of target types does NOT mean that exactly this types will be implemented, but for scalability reasons we believe that the total amount of services is very limited):

- Premium Service – the user subscribes a service that allows him to get whatever the network is able to offer until a maximum limit is reached;
- Regular Signature Service – the user subscribes a service with very specific service parameters (bit-rate, delay, jitter, packet loss, availability);
- Pre-Paid Service – the user is allowed to use a certain amount of network resources, until a pre-paid budget is exhausted.

The Moby Dick network must be able to support the specific details of each of these types of services. Each of these services will have some constraints associated with, and some of these have to be managed in real-time. The now following service description does not claim to be a complete list of services supported by the Moby Dick architecture. There services represent characteristic sub-set of variations of services which could be deployed on top of such an architecture. However, examples of various sectors of the old economy it was shown, that offering too much different services result in increasing management cost and for this reason service bundles are formed which give the user the possibility to select between several service packets. We often see in industry so-called “professional” service, an “advanced user” services and a “standard” service. Within this classes the lower layer services could be separated as follows:

4.1.1 Premium Service

A user with a premium service requires his service parameters to be satisfied at all times, inclusive during and after handovers, i.e. when changing cells, technological boundaries, or provider domains. This may be critical, especially if we think that the user, during his movement, may try to do a handover to a cell that does not have sufficient resources to comply with its QoS contract. Some “intelligent” handover decision mechanisms have to be used. For instance, degrading other non-premium connections by a small amount may be sufficient to comply with this user contract. Also, the best-effort traffic must be used in an elastic way to achieve these goals. The AAAC functions, especially the Accounting and Charging are comparably simple in this kind of profile.

4.1.2 Regular Signature Service

This type of service is the most flexible, as the specific details of the service will depend on the user profile. Typically, the contract will allow some kind of degradation in the QoS parameters, providing the network operator with some flexibility from the management point of view. However, this type of service may require complex AAAC procedures such as ….

4.1.3 Pre-Paid Service

The pre-paid service is a service where the user pays in advance for certain resources. Thus, user activity must be monitored continuously to prevent excess usage without payment, that is, to prevent the user to spend more than he paid for. This type of service is the most demanding in terms of AAAC functions.
4.2 Network evolution constraints

The network architecture had several constraints originated by foreseen developments in IP technology, and by the need to retain overall internetworking with the Internet. The network using throughout IPv6 will be based on an IPv6 core network and three different technologies access networks, namely, W-CDMA (UMTS), Wireless LAN (802.11), and Ethernet (802.3). Standard IP methods (with some enhancements) for handling QoS and mobility have to be developed. Mobile terminals may travel from one access network to another, within this infrastructure, using any kind of services, with assured QoS, regardless of the access network it uses.

Targeting the goal to support both, user and terminal mobility, each user is virtually linked to a user specific profile. This profile is located from a functional point of view in the home network of the mobile user, or at a position which is closely linked to the home area e.g. via an AAAH entity.

This function basically replaces the HLR register of the 3GPP architecture AND extends this with additional user specific QoS related information.

4.3 Technology specific requirements

The network technology considered is an all IP-based network and the IP version 6, IPv6, is to be used. The underlying access technologies should be implemented as transparent as possible to the QoS-, Mobility- and AAAC entities. Moby Dick addresses an interaction between QoS-, Mobility-, and AAAC entities. This kind of interaction should be as independent as possible from link layer technologies and for reasons of efficiency, this interaction should be reduced to a minimum to avoid complexity. Users must be able to enable and disable security features regarding data integrity and confidentiality.

Within Moby Dick, the following global assumptions and requirements are considered:

?? The system carries IP traffic only.
?? One W-CDMA cell equals one IP subnet.
?? Mobility Management is based on Mobile IPv6 – enhanced where required.
?? The Access Gateway has two IPv6 addresses, one towards the core network, the other on the wireless interface.
?? Support Mobile IP services based on MIP:
   ?? Maintaining the same routable IP address of a mobile node or mobile network.
?? Support seamless hand-over between
   - different access cells based on the same technology in one administrative domain
   - different access cells based on the same technology in different administrative domains
?? Provide robust authentication, authorisation accounting auditing, and charging services (AAAC)
?? Network access must be based on successful authentication and authorisation

4.3.1 W-CDMA specifics

The Moby Dick architecture is based on a EURECOM platform [52]. This platform, currently under development, has for the W-CDMA-specific part of Moby Dick some constraints. For this reason relevant Moby Dick-specific issues will be reported within this section.

The W-CDMA specific issues in greater detail are:

?? The QoS attributes of DiffServ are mapped to the UMTS QoS architecture [13].
?? The Radio Access Bearer service introduced in the UMTS architecture between the UE and the SGSN is no longer present (see 0 for more details on this architecture). This implies a need to replace the PDP Context Activation procedure. A UE uses this procedure in order to establish a virtual connection with its GGSN and to express its QoS requirements for the connection. It may also ask for a dynamic address allocation in case of IPv6 stateless address auto-configuration. The PDP Context Activation procedure is illustrated in Figure 1.
For each PDP context a different QoS profile may be requested. If a QoS requirement is beyond the capabilities of the UMTS network, the network negotiates the QoS profile as close as possible to the requested QoS profile. The UE either accepts the negotiated QoS profile, or deactivates the PDP context. If the PDP Context Activation Procedure fails or if the SGSN returns an Activate PDP Context Reject message, then the UE may attempt another activation up to a maximum number of attempts.

The replacement is part of the RRC/ Middleware entities described below.

?? The W-CDMA architecture is simplified as shown in the figures below.

Figure 1: PDP Context Activation Procedure for UMTS

Figure 1: User Plane
The Radio Gateway is not only a typical “Node B” (Base Station with Physical Layer only) as defined in UMTS, but also handles the following entities:

- The physical layer + MAC layer
- An access to data traffic via the RLC and PDCP layers which is responsible to convey data over “Radio Bearers”
- A control function (RRC) which provides an interface to connect the mobile nodes, setup, and release radio bearers for signalling and data.

The Radio Gateway can be seen as a Node B + a subset of the RNC.
5  Moby Dick Architecture

5.1  Conceptual view

Figure 3 presents the Moby Dick architecture from a conceptual point of view. In general, a network consists of several domains. A domain within this context is an administrative domain which means that such a domain typically belongs to another network operator and these network operators maintain roaming agreements with each other.

The IP backbone is QoS aware, in details the nodes – respectively egress, ingress, and interior routers - will support Differentiated Services (DS).

Two foreign domains with different access network technologies are given in this example:

- Domain A: has only two W-CDMA access sub-networks.
- Domain C has a mixed set-up with Ethernet, W-CDMA, and wireless LAN (802.11) as access technologies.

The Correspondent Node (CN) is connected via an unknown QoS supporting access technology to the backbone and is located in the administrative Domain D.

The Home Agent (HA), “home” QoS Broker (QoS.h), and the Home AAAC server (AAAC.h) are placed currently in the same home domain – Domain B. However, this is not a must. Both, the HA and the QoS.h have to be placed in the same domain but the AAAC.h can be located somewhere else in a different domain. In this case, some additional AAA communication has to take place.
The Paging Agent (PA) will be somewhere, connected as well through a QoS aware network technology to the backbone.

For Moby Dick access networks the following components are necessary:

- **QoSB**: QoS Broker for management of the QoS “requests” via profiles.
- **AAAC.f**: Foreign AAAC server for handling Authentication, Authorisation, Accounting, and Charging issues.
- **(Radio) Access Routers**: They are policy points in the access network. Each air interface W-CDMA or wireless LAN (802.11) – will cover one IP sub-network. The Radio Access Router (RAR) will have at least one radio interface and one fixed line interface to the domain network. Access Router (AR) will have only interfaces to fixed lines and to each access interface a sub-network will be assigned.
- **Routers (R)**: They are normal ingress (for incoming flows), egress (for leaving flows), and interior (inside a DS domain) DS routers.

Optional for the access domains will be a local Paging Agent (PAI). A local PA offers direct communication, if needed. This leads to less signalling through the backbone.

**Please note:** Since we will have a QoS end-to-end architecture, the following components have to be Differentiated Services capable:

- **CN or the router next to this node**: The CN is the source of the flow.
- **All routers**: Since they have to forward the packets of QoS flows.
- **HA**: In case, the CN does not know the location of the MT, the packets will be sent to the HA which has then to forward the traffic to the “new” location of the MT.
- **PA**: If the MT is in idle state, the HA will forward the first few packets to the PA by using tunnelling. This tunnels have to be DS aware and will be probably implemented by mapping the respective DS codepoint from the tunnelled IP packet into the codepoint of the tunnelling IP packet.

**Connectivity to the QoS aware IP backbone:** The different domains are connected via at least one DS egress/ingress router to the backbone. The same is valid for the inter-connection of the access networks to the domain’s “backbone”. These “sub-network” access routers can be fully mashed. However, they should have full IPsec, DS, and mobility support. These are the first and important policy points for incoming traffic (from the MT towards the backbone).

**Need to support IPsec:** Apart from the interior routers and components, which will communicate only within a domain, all components should be IPsec-aware. A Correspondent Node (CN) is within the project network node located in any domain communicating with a Mobile Node (MN). A CN, of course, can also be a MN. The QoS aware backbone is an IP backbone network operated by one or more operators.

### 5.2 Mobile Terminal Software Architecture

The software architectures for the mobile terminal (MT) is illustrated in Figure 4

Essential characteristics are:

- **The Extended Socket Interface** provides extension to the conventional Socket interface to support QoS-aware applications and invocation of IP signalling.
- **The Networking Management Interface** provides a means for setting of user networking preferences and obtaining networking status.
- **The Radio Management Interface** provides a means for obtaining radio information.
- Providing the extended socket interface, the enhanced TCP/IP stack will incorporate the necessary protocol extensions and enhancements to support the mobility, QoS, and AAA functions required by Moby Dick.
- **The Networking Control Panel (NCP)** provides a user interface to allow a user to manage his networking activities.
The Mobile-Terminal Networking Manager (MTNM) does not implement any protocol; it complements the enhanced TCP/IP protocol stack to provide additional assistance in managing the mobile terminal’s handover process. The MTNM does not implement a protocol.

A radio network device driver for the mobile terminal comprises 3 components: the Radio Channel Manager, a specific Radio Convergence Function and a specific Radio Modem Support.

The Radio Service Interface is a connection-oriented abstraction of the radio interface for QoS-enabled wireless technologies.

A Radio Modem Support (RMS) is concerned with the support of the peripheral interface to the radio modem. In Moby Dick, the W-CDMA stack refers to a modified Access Stratum of the 3GPP UTRAN access. It is labelled $\text{AS}_{\text{WCDMA}}$.

A Radio Convergence Function (RCF) supports the Radio Service Interface and implements the necessary convergence mechanism to map between the Radio Service Interface and the native radio interface (via the RMS) of a specific wireless technology.

The Radio Channel Manager (RCM) supports the conventional network device interface to the TCP/IP stack and the Radio Management Interface to facilitate handover operations. It manages the establishment and release of abstract radio channels, and separates IP traffic into them according to the different QoS requirements.

### 5.2.1 Functional elements

#### 5.2.1.1 Enhanced TCP/IP stack

The enhanced TCP/IP stack will be based on the LIVSIX release of IPv6 and MIPv6 implementation.
It will
?? Incorporate the necessary extensions and enhancements to support the mobility, QoS, and AAA functions required by Moby Dick
?? Support the standard Socket interface
?? Support the Extended Socket Interface
   ?? Extended version of certain standard primitives to carry QoS
   ?? New primitives for indication of change in QoS
   ?? New primitives to allow invocation from outside the protocol stack of certain IP signalling, such as Router Solicitation, User Registration, etc

5.2.1.2 Networking Control Panel (NCP)
The NCP manages the user’s networking activities.
It will
?? Provide a user interface to
   ?? Obtain user’s preferences in network selection
   ?? Allow the user to invoke a manual handover between access networks
   ?? Provide feedback and information about the networking environment, such as the status of 802.11b and WCDMA
?? Make use of the Networking Management Interface to
   ?? Set user network selection preference
   ?? Set configuration of handover strategy: manual, automatic, both
   ?? Invoke a manual handover between access networks
   ?? Obtain feedback and information about the networking environment, such as the status of 802.11b and WCDMA

5.2.1.3 Mobile-Terminal Networking Manager (MTNM)
The MTNM manages the mobile terminal’s handover process.
It will
?? Support the Networking Management Interface to
   ?? Get user preferences in network selection from the NCP
   ?? Obtain configuration of handover strategy: manual, automatic, both
   ?? Execute the manual handover initiated via the NCP
?? Support automatic handover decision-making based on user preferences and intra-administrative-domain handover rules
?? Dynamically reconfiguring and administering the enhanced TCP/IP stack and the network device drivers in the co-ordination of handover process, such as switching on and off network interfaces, initiating relevant mobility, QoS, and AAA signalling, etc.
?? Use the Radio Management Interface to
   ?? Monitor the availability of the access networks and radio quality condition by obtaining information from the RCM
?? Use the standard network device interface to
   ?? Switch on and off network interfaces during handover
?? Use the Extended Socket Interface to
   ?? Initiate relevant Mobility, QoS and AAA signalling during hand-over
?? Use the standard Socket Interface to
   ?? Get intra-administrative-domain handover rules

5.2.1.4 Radio Modem Support for WCDMA (ASWCDMA)
The ASWCDMA layers provide the ASWCDMA interface to upper layers (e.g. RCFWCDMA).

5.2.1.5 Radio Convergence Function for WCDMA (RCFWCDMA)
The RCF maps between the RSI and the native WCDMA radio interface.
It will
?? Support the Radio Service Interface to
   ?? Map the abstract radio channels onto the real radio channels and vice versa
   ?? Provide information about the availability and quality of WCDMA access
?? Access the WCDMA radio modem via the ASWCDMA

5.2.1.6 Radio Channel Manager (RCM)
The RCM serves to provide an abstraction of the radio interface.
It will
?? Support the standard network device interface
?? Support the Radio Management Interface to
   ?? Provide information about the availability and quality of the radio
?? Use the Radio Service Interface to
   ?? Initialise control channels
   ?? Establish and release abstract data channels
   ?? Separate IP traffic according to different QoS requirements and RSI’s QoS definition associated
   with the abstract data channels

5.2.2 Interface definitions
The following interfaces are defined:
?? Extended Socket Interface (ESI)
?? Networking Management Interface (NMI)
?? Radio Management Interface (RMI)
?? Radio Service Interface (RSI)
?? Access Stratum W-CDMA Interface (ASWCDMA): The W-CDMA Access Technology (Access
   Stratum) layers provide an API to interface with upper layers such as the RCM (usually called Non
   Access Stratum). This interface is pictured in Appendix F.

These different interfaces will meet requirements of the functional elements previously described.

5.3 Radio Gateway Software Architecture
The software architectures for the mobile terminal (MT) is illustrated in Figure 5

![Figure 5: Radio Gateway Software Architecture](image)

Essentially, the Interworking Function (IWF) manages the relay of IP traffic between the radio and the IP
domains, performing the necessary QoS mapping.
5.3.1 Functional elements

5.3.1.1 Interworking Function (IWF)

The IWF will
- Use the Radio Management Interface to
  - Monitor the availability of the access networks and radio quality condition by obtaining information from the RCM
- Perform the necessary QoS mapping between the radio and the IP domains
- Use the standard Socket interface and the Extended Socket Interface to
  - Relay IP traffic between the radio and the IP domains

5.4 Access Router Architecture

Figure 6 depicts a functional overview of the access router.

![Access Router Software Architecture](image)

Figure 6: Access Router Software Architecture

The access router is a IPv6 compliant standard machine with routing capabilities and additional functional module blocks.

- The AAA attendant acts as AAA client and is responsible for communication between AAAC server on behalf of the MN. This includes all security specific functionalities like key handling and network access procedures.
- The DiffServ Module has the tasks marking, and scheduling of the data packets forwarded towards the MN.
- The Policy Enforcement Point PEP is responsible for policing issues. The policy information of provided by the AAAC framework (profile).
- Mobility management related issues are handled by the Mobility manager. This comprises context transfer, handover and paging issues.
- An Accounting module provides data for Auditing and charging issues.

5.5 Physical view on the Moby Dick Architecture

In the following, a sub-set of a physical view and the choice of the operation system of a Moby Dick infrastructure are shown.

**Please note:** AAAC server and QoS Brokers are not mentioned here because of not overloading the picture. Both types will run on Linux. The operating system of the CN is open but it will be most likely Linux.
5.6 Physical Components

As a preparation for implementation, the following types of physical elements were identified based on the logical and conceptual Moby Dick architecture:

i) Mobile Terminal
ii) Correspondent Node, e.g. web server
iii) Home Agent
iv) Paging Agent
v) Paging Agent local
vi) Radio Gateway
vii) Access Router
viii) Wireless LAN Access Gateway
ix) AAAC Server
x) QoS broker
xi) Router

At least one component instance of each of the above 11 types will be implemented if not commercially available (e.g. a standard router is commercially available), but there will be several instances of some, e.g. 1, 7. Initially, a set of functions has been identified for each of the physical element types, and these
will be one or more software modules of the implemented system. The following sub-sections contain the
initial list of functions that are associated with each physical element type. They represent the maximum
list of functions, and some physical element instances may not need all of them. Each function includes
handling the associated message flows.
Note: The AAA client is a function within other physical elements.

5.6.1 **Mobile Terminal**
- Handover
- Paging
- MIPv6 incl. Alternative CoA support
- Awareness of Context Transfer
- Network Access procedure including Authentication and Authorisation
- DiffServ-Aware
- Authentication and Authorisation
- Charging advice and approve charging
- IP-Sec support
- W-CDMA support
- Wireless LAN support
- Ethernet support

5.7 **Correspondent Node, e.g. web server**
- MIPv6 support (binding cache)
- DiffServ-Aware
- IP-Sec support
- Support for applications

5.7.1 **Home Agent**
- MIPv6
- DiffServ-Aware
- Key handling
- IP-Sec support

5.7.2 **Paging Agent**
- Paging
- DiffServ-Aware
- Key handling
- IP-Sec support

5.7.3 **Paging Agent local**
- Paging
- DiffServ-Aware
- Key handling
- IP-Sec support

5.7.4 **Radio Gateway**
- W-CDMA Support
- Radio Access procedure (control)
- Packet forwarding support
- QoS Mapping
- Communication protocol AR-RG or direct support with respect to QoS and AAAC features
- Paging awareness and mapping
5.7.5 Access Router
- Context Transfer
- DiffServ Support
- Network Access procedure
- Policy enforcement
- Handover incl. Bi-Casting
- AAAC Client including key handling
- Metering of resource usage
- IP-Sec support
- Paging awareness
- Communication protocol AR-RG with QoS and AAA features if necessary

5.7.6 Wireless LAN Access Router
- Wireless LAN support incl. radio access procedure
- Context Transfer
- DiffServ Support
- QoS Mapping
- Network Access procedure
- Policy enforcement
- Handover incl. Bi-Casting
- AAAC Client including key handling
- Metering of resource usage
- IP-Sec support
- Paging awareness and mapping

5.7.7 AAAC Server
- Authentication
- Authorization
- Accounting
- Charging
- IP-Sec support
- Interaction with metering, QoS broker, HA and AAAC Client
- Auditing
- Profile handling
- Key handling
- Binding update
- Database for policy management (DT)

5.7.8 QoS broker
- Interface with the AAA entity
- Inter QoS manager interface
- Mobility management interface
- Network management interface (traffic statistics and router configurations)
- Managing QoS of the network

5.7.9 Core Network Router
- DiffServ Support
6 Special interface issues

Within Moby Dick, there are three basic scenarios which are relevant to QoS, Mobility, and AAA issues. These scenarios are QoS session setup, registration, and handover procedure. Within the implementation workpackages (WPs for QoS, WP3 for Mobility and WP4 for AAA+AC), relevant sections of these scenarios will be described in greater detail. However, each of their workpackage will focus on the workpackage-specific issues and will go into greater detail.

Within the next three chapters, these three procedures will be described from a more abstract point of view with the goal to propose an initial message flow concept which tries to combine requirements from all the three directions. An optimal combination and an effective interaction between mobility, QoS, and AAA taking care of the requirements of all three directions is almost unreachable. The following example will explain this more detailed:

The basic interest of the QoS workpackage is to provide a high level QoS – also during handover, which is in the ideal case based on a signalling protocol which is able to guarantee a mobile user a desired QoS. In case of mobile scenarios this kind of QoS signalling requires some time and introduces some overhead. This overhead in terms of additional time may lead to the fact that in case of a hand-over procedure from one network to another, the desired QoS can not be maintained in a seamless way. Additionally, within Moby Dick authorised access of authenticated users is foreseen. This requires additional resources with respect to time and would result in an even worse mobility management and QoS provisioning capability during handover.

So it is clear that the Moby Dick solution will be a compromise between requirements from the three poles.

6.1 Integrated Session Setup procedure

QoS Session Setup is the setup of a QoS Session for a terminal/application. A detailed definition of a QoS session can be found in D0201 section of Annex B in this document. In the D0401 section of this document (Annex C), the terminology “session” is explicated in more generic view not only restricted to network layer parameters.

6.1.1 Assumptions

The following assumptions are considered:

- Whether the user gets QoS session depends on Authentication and Authorisation (AA) and the currently available resources in the network
- In general, if both are independent and it does not matter whether AA is done before checking resources or after (MAQ or MQA both possible solutions)
- Network state changes much more frequently then user profile
- MN already has full BE network access
- User profile QoS parameters are already present at AAAC.f if they were distributed in registration phase
- Metering/accounting is done at AR (in a second step it may be necessary to also get information from QoS entity)

6.1.2 Requirements

Based on the above mentioned assumptions the following requirements are generated:

- If authorisation depends on network resources AA MUST be done after resource checking (MQA)
- Existing QoS and AAA protocols should be taken into account for solution
- MN MUST get final response
- An AAA request is not a service request so it SHOULD NOT be overloaded by service specific parameters which are of no use for AAA infrastructure
- MN CAN contact AAAC directly because MN is already registered and may be told the AAAC.f address in registration phase, but we then still need an AAA client on the MN and have to live with the AAA protocol on that (wireless interface) and the AAA client on access router which does accounting must then be informed by AAAC.f server after approving MN to start accounting session

6.1.3 MAQ Scenario

The MAQ scenario means that the QoS entity is involved before the AAA entity in the session setup process. From a logical sequence point of view, there are considered two different abstract procedures of the message flow. The MAQ scenario first involved the authentication process and after a positive authentication, QoS entities will be contacted. Figure 8 shows the detailed message flow.
This solution has several advantages and disadvantages which will be summarised in the following sections.

6.1.3.1 Pros of MAQ
- QoS protocol does not have to deal with AA parameters

6.1.3.2 Cons of MAQ
- May overload AAA with QoS service specific things
- Unclean interface to AAA (session stop is also signalled via AAAC?)
- In case we allow negotiation we have either a triangular communication path or everything is tunnelled via AAA which overloads AAA and takes longer
- MN needs to speak to two different entities and probably even with 2 protocols
- Does not take into account existing protocols like RSVP (signalling between MN and QoS)
- Authorisation can not be done on the basis of available resources, Authorisation could also specify whether negotiation is possible
- Negotiation result can only be a “less than authorised for” otherwise a second authorisation is needed
- This scenario does not work without AAAC architecture

6.1.4 MQA Scenario
In contrary to the MAQ scenario, the MQA scenario first involved the QoS entity and after a QoS negotiation phase, the authentication process is started. The next figure shows the detailed message flow.

6.1.4.1 Pros of MQA
- Clean interface to AAA (only needed parameters & messages)
- Existing protocols like RSVP can be used for MN QoS communication
- No triangular communication in case of negotiation
- Supports authorisation based on current network status
- MN does not need to speak 2 protocols (especially it does not need to speak AAA protocol)
- Since network state changes much more frequently this sequence could be optimised to MQ only until timeout of the QoS Registration Session in the AAAC server
- This scenario does not presume AAAC architecture (AAA function in QoS can be dummy)

6.1.4.2 Cons of MQA
- Must tunnel AA parameters via QoS signalling protocol
- Longer blocking of resources in case AA is done after negotiation (but compared to e2e path reservation the AA transaction will be very fast because intra-domain)

MN | AR | QoS | AAAC.f
---|---|---|---
QoS Sess Req. (QoS/AA parm,…) | negotiation | QoS Sess Res | Lock resources
| | | | Auth Req (user ID, Credentials…)
| | | | Auth Res (QoS parm)
| | | | Accounting Conf
| | | | Accounting

Figure 9: MQA Message Flow

6.1.4.3 Accounting
Accounting Configuration is dotted because this message may not be needed. The meter on the AR can simply generate information for all flows it sees. However, the AAAC.f in this case has more work to do because it must map the data to certain sessions. Furthermore, the AAAC.f must then take care of the accounting session stop but that requires information from QoS (MQA) or MN (MAQ) at the end of the session.

6.1.5 Summary of session setup scenarios
As just mentioned, within this section problems currently discussed on the mailing list of the Moby Dick project are summarised. The above described scenarios do not claim to be the only possible solutions how to integrate QoS, Mobility, and AAA issues within Moby Dick to come to an optimised session setup scenario, but summarise the discussion currently taking place on the mailing list. The goal of this chapter was to work out the principle differences between the two possible scenarios and the positive and negative impacts coming up with the possible solutions. Within D0201, more detailed QoS session setup scenarios are presented, however, this restricts the current focus to QoS issues only. At a later stage, results of this discussion will be introduced into the integrated scenario.

6.2 Registration Scenario
Registration is the procedure of changing the point of attachment (including switch on the MN). User and terminal are identified in the network. It is the process of MN getting L3 connectivity and becoming reachable throughout the network according to the standard Mobile IP methods defined by [7]. Attachment is the point of time, a MN is able to start a session setup (“receiving and sending”). The Mobile Node informs the HA (BU) during “mobile IP” period. The registration process start after the local link acquirement (LLA).

Figure 10 shows the whole registration process consisting of three sub-sections, the care off address acquirement phase, the AAA phase and the final mobile IP procedure.
6.2.1 CoA Acquisition

Within Moby Dick the Authentication and Authorisation process starts after the CoS acquirement procedure defined in [7]. From a security point of view, it is certainly better to assign CoA after authentication & authorisation but that would require using/implementing L2 signalling between MN and AR and modify the existing process defined in mobile IP [7]. So for ease of implementation we assume that CoA has been done before. More detailed information about the CoA acquirement procedure can be found in the D301 section which is part of Annex B of this document.

6.2.2 Problem statements

The MN MUST NOT directly speak to AAAC.f server because that introduces a couple of problems:

- Authentication/authorisation before CoA acquisition would become very difficult.
- MN would need to speak AAA protocol (AAAC protocol i.e. RADIUS, DIAMETER was never designed for use between MN and AAAC server). For further information of RADIUM and DIAMETER please have a look to Annex C.
- MN would need to dynamically discover AAAC.f server
- AR would need to be able to identify AAAC signalling and let those messages pass through (actually this would require more or less complex ingress filtering and introduces potential security risks because packets from a non trusted MN are allowed to enter to provider network).

There MUST be a communication between AAAC.h and HA to:

- Allow session key distribution via AAA.
- Potentially allow BU piggybacking as optimisation.
- Allow DHAAD via AAA.
- Handle MIP originated de-registration.

QoS entity SHOULD NOT be involved in the registration process:

- QoS is not necessarily needed, the MN could well be happy with best effort
- Do not integrate Mobility & QoS that way but in the way that each of some can be used without the other (QoS setup is done in the QoS session setup scenario).
- If QoS is application based it does not make sense to setup QoS at registration time.

6.2.3 Proposed solution

The now proposed solution it the currently discussed solution for registration. It assumes that there exists two long term trust relationships which have been previously setup. One is between the foreign and home AAAC server (This may be an indirect one via a number of brokers). The second is between MN and AAAC home server which is established at the time the contract is made. Furthermore it is assumed that all entities in one administrative domain have a trust relationship.

The MN contacts the Access Router (AR) with a User Registration Protocol (URP) of some kind. ICMPv6 [33] could be used as proposed in [47]. MN has to provide AR with an identifier and the necessary credentials which are needed to proof MN identity (authentication). The NAI [46] can be used for identifying a user. The AR is the AAAC client and sends an authentication & authorisation request to his local AAAC server. The request is routed to the home AAAC server according to the NAI (domain
part). The AAAC home server performs authentication & authorisation. If successful the home server generates a session key and distributes it to the HA in his domain as well as to the MN in the authentication and authorisation response which is sent back to the issuing AR. For the interface between AAAC home server and HA a form of extended BU can be used. The response also contains all information of the user profile which are necessary to have in the foreign/current domain of the MN. The AR sends a URP response to the MN containing the session key. The distribution of the session key is secured via the previously established trust relationships. Accounting information is generated by a meter and the AAAC client located at access router. This information is passed to foreign AAAC server. In case the home domain does the charging, the accounting information must be forwarded to the home domain. In case the foreign domain does the charging, records are sent to the home domain.

We think that it is possible to piggyback BU on this registration request and thus to save one complete roundtrip. However, in a first step the BU can be made separately (after authorisation has been approved and the AAAC.h HA message exchange does not include BU) as specified by MIPv6.

Charging advice and Charging approvement are currently out of scope of this scenario.

The above case is the case in which registration is successfully completed. However, in reality at least the following failures could occur:
- Invalid NAI (could not find home AAAC)
- Either AAAC.f, intermediate AAAC proxy or AAAC.h failure
- Authentication of the request failed (e.g. improper credentials)
- Authorisation failed
- HA failure (e.g. no HA)
- Transport layer and below failures

A Registration is cancelled by de-registration. The de-registration could be potentially originated at all entities:
- MN originated
  o URP de-registration
- AR originated
  o L2 shutdown detect (if AR is able to detect this)
- AAAC Server originated
  o AAAC session timeout (MN did not re-authenticate, re-authorise)
  o AAAC.h forced de-registration (e.g. prepaid out of money)
- HA originated
  o Registration timeout

6.2.4 Discussion & Open Issues
- No objection raised against registration proposal
- De-registration as proposed is bad because HA needs to speak AAA protocol, however, a viable alternative solution has not yet been identified.

6.3 Handover scenario

The following slide presents an initial handover process. This handover procedure must be integrated with QoS and AAA issues.

Handover is similar to the registration procedure. The fundamental difference is the fact that a session is ongoing. This means before the handover process a session has started and at point of time the handover is initiated the session has not yet stopped. A more detailed hand-over scenario is shown in Appendix B. This scenario is for inter-domain handover since no additional Authentication is described.

A MN receives a Beacon signal from a neighbour access cell (1) and sends a router solicitation message to the OAR, (Old Access Router) (2). This is the router currently responsible for the session. After this a negotiation phase (2) – (5) between MN, OAR and NAR takes place and finally the handover is executed. After this for a short duration of time the OAR bicast the packets towards the MN via both, the old wireless connection as well as via the NAR (8). After predefined period of time the bicast is stopped (9) and a neighbour advertisement is sent to the NAR (10). The process terminates with the BU (11, 12). With this mechanism the disconnection time during handover will be minimised. More detailed handover description will be performed within D0301 (Annex B).

Current discussion points for this scenario are how to stop the bicast process. Proposed solutions are to add a message or to do it automatically via timer.

Figure 12: Initial handover scenario
7 Summary and Outlook

This Deliverable should be regarded as a baseline document for the whole Moby Dick project, with the assumption that the presented architecture is not the final one and will be extended until the life-time of workpackage WP1 will end. It summarises the work during the first ten months of the project and includes a description of generic operational scenario requirements. These requirements are on a generic level, since more detailed requirement descriptions will be provided by the three implementation workpackages. First drafts of these deliverables are given in Annex A, Annex B, and Annex C.

The Moby Dick Architecture has two goals which are orthogonal: First, the Internet Protocol is regarded as convergence layer for mobility management, AAAC, and QoS issues. This requires a lower layer technology independent solution. On the other hand, Moby Dick will manage resources of the scarce wireless access technology efficiently, namely W-CDMA. This goal cannot be reached without any inter-layer signalling mechanisms which immediately brings some technology-specific issues into the architecture, and will be solved in the framework of Moby Dick.

The first step of the project phase is due. This phase covered mainly theoretical and specification work. The next phase has already started and is reflected in the mentioned annexes. This phase covers the transfer of the specification and the theoretical work towards implementations. These implementations will go for a best practice compromise to share the results with the European society to strengthen Europe’s position in the wireless area.
8 References

Remark on Internet Drafts, Request for Comments (RFC) documents and Web-sites.

The following statements are included in Request For Comments 2026 - "The Internet Standard Process -- Revision 3" (S. Bradner, Harvard University, October 1996) and briefly describe the treatment of Internet Drafts and Internet RFCs:

?? Internet Drafts: "An Internet-Draft that is published as an RFC, or that has remained unchanged in the Internet-Drafts directory for more than six months without being recommended by the Internet Engineering Steering Group (IESG) for publication as an RFC, is simply removed from the Internet-Drafts directory. At any time, an Internet-Draft may be replaced by a more recent version of the same specification, restarting the six-month timeout period."

?? Internet RFC: "It is important to remember that not all RFCs are standard track documents, and that not all standard track documents reach the level of Internet Standard. In the same way, not all RFCs which describe current practices have been given the review and approval to become Best Current Practices (BCPs)."

In addition, RFC can have the attribute "informational", so they are only for information and might not become the standard track.

Web-sites have a life-time. They might change or will disappear. Web-servers might be shut down or their IP name (server name) will not be up-to-date anymore.


[18] www.ietf.org


[34] 3G TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2 (Release 1999)"

[35] 3G TS 29.060: "GPRS Tunnelling protocol (GTP) across the Gn and Gp Interface".


B. Aboba, M. Beadles: The Network Access Identifier; RFC 2486, January 1999


Mobile Wireless Internet Forum, Architecture Requirements, Technical Report MTR-002, Release 0.6


Mobile Wireless Internet Forum, Network Reference Architecture, Technical Report MTR-004, Draft 0.7


Mobile Wireless Internet Forum, Open RAN Architecture in 3rd Generation Mobile Systems, Technical Report MTR-007, Release V.0.3.0 (March 2001)


3GPP, 1999, 3GPP TR 23.922, ‘Architecture for an All IP network’, V 1.0.0


Jonsson L., 3GPP2 Requirements for 0-byte ROHC IP/UDP/RTP Header Compression, Internet Draft, March 2001, work in progress

http://www.ietf.org/html.charters/seamoby-charter.html


[71] Srinivas et al.: Mapping of Basic and Digest Authentication to DIAMETER AAA Messages, Internet Draft, draft-srinivas-aaa-basic-digest-00.txt, July 2001
9 Appendix A: First Version of D0201 (Status: not public - internal)
10 Appendix B: First Version of D0301 (Status: not public - internal)
11 Appendix C: First Version of D0401
12 Appendix D: Terminology

This chapter presents a terminology to be used for documents and discussions within the Moby Dick project. Some other fora or projects are currently working over common terminology. In order to avoid Moby Dick re-inventing the wheel, this document is indeed a simple collection of what has been produced so far in those or other areas. The terminology summarised in this section explains the wording used in the base document. Further terminology can be found in Annex A, Annex B and Annex C.

12.1 Network Components

12.1.1 Access Network (AN)

The fundamental new concept to be introduced is that of the Access Network (AN) which supports enhanced mobility. It is a working assumption that to support routing and QoS for mobile devices, we need specialised routing functions (i.e. not OSPF or other standard IGP's) which are used to maintain forwarding information for these devices as they move physically, and these functions are implemented in IP routers with this additional capability.

12.1.2 Access Routers (AR)

A Router residing on the edge of an Access Network and connected to one or more access points. An Access Router offers IP connectivity to MHs. The Access Router may include intelligence beyond a simple forwarding service offered by ordinary IP routers.

We can distinguish three types of these: Access Routers (AR) which handle the last hop to the mobile; Access Gateways (AG) which form the boundary on the fixed network side and shield the fixed network from the specialised routing protocols; and (optionally) internal Access Network Routers which may also be needed in some cases to support the protocols. The Access Network consists of the equipment needed to support this specialised routing, i.e. A/AG/AR.

12.1.3 Mobile Node (MN)

An IP node capable of changing its point of attachment to the network. The Mobile Node may have routing functionality.

12.1.4 Mobile Host (MH)

An IP node capable of changing its point of attachment to the network. The Mobile Host only refers to an end-host without routing support.

12.1.5 Access Link (AL)

A facility or medium over which a Mobile Host and an Access Point can communicate at the link layer, i.e., the layer immediately below IP.

12.1.6 Access Point (AP)

An Access Point is a layer 2 device which is connected to an Access Router and offers the wireless link connection to the Mobile Host. Access Points are sometimes called 'base stations' or 'access point transceivers'. An Access Point may be a separate entity or co-located with an Access Router.

12.1.7 Access Gateway (AG)

An Access Gateway that separates an Access Network from other IP-networks. This separation is only visible on lower layers than on IP layer. In The Moby Dick case the Access Gateway separates between the between the air/W-CDMA at one side and a fixed/wired medium at the other side. An Access Router and an Access Gateway may be the same physical node. The Access Gateway looks to the fixed network like a standard IP router.

12.1.8 Access Network (AN)

An IP network which includes one or more Access Network Routers. The terms Access Network and (administrative) domain are often used interchangeably (e.g., "intra-AN" is "intra-domain") since often an Access Network has its own administration.

12.1.9 Serving Access Router (SAR)

The Access Router currently offering the connectivity to the Mobile Host. This is usually the point of departure for the Mobile Host as it makes its way towards a new Access Router (then Serving Access Router takes the role of the Old Access Router). There may be several Serving Access Routers serving the Mobile Host at the same time.
12.1.10 Old Access Router (OAR)
An Access Router that offered connectivity to the Mobile Host prior to a handover. This is the Serving Access Router that will cease or has ceased to offer connectivity to the Mobile Host.

12.1.11 New Access Router (NAR)
The Access Router that offers connectivity to the Mobile Host after a handover.

12.1.12 Candidate Access Router (CAR)
An Access Router to which the Mobile Host may move next. A handover scheme may support several Candidate Access Routers.

12.2 Network Protocol Terminology

12.2.1 Care-of Address (CoA)
The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. The protocol can use two different types of care-of address: a "foreign agent care-of address" is an address of a foreign agent with which the mobile node is registered, and a "co-located care-of address" is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

12.2.2 Correspondent Node (CN)
A peer with which a mobile node (MN) is communicating. A correspondent node may be either mobile or stationary.

12.2.3 AAAH
Home AAA Server. This AAA server is located in the home network administration area and takes over the AAA specific functions of the home network AAA server. Further explanation can be found in Appendix C.

12.2.4 AAAF
Foreign AAA Server. This Server takes of the AAA specific functions in the visiting network.

12.2.5 Foreign Network
Any network other than the mobile node's Home Network.

12.2.6 Home Address (HA)
An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

12.2.7 Home Network (HN)
A network, possibly virtual, having a network prefix matching that of a mobile node's home address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node's Home Address to the mobile node's Home Network.

12.2.8 IP Diversity
IP diversity means the splitting and combining of packets at the IP level.

12.2.9 Link-layer address
The address used to identify an endpoint of some communication over a physical link. Typically, the Link-Layer address is an interface's Media Access Control (MAC) address.

12.2.10 Visited network
A network other than a mobile node's Home Network, to which the mobile node is currently connected.

12.2.11 Administrative Domain
An intranet, or a collection of networks, computers, and databases under a common administration. Computer entities operating in a common administration may be assumed to share administratively created security associations.

12.2.12 Attendant
A node designed to provide the service interface between a client and the local domain.
For instance, a broker may obtain and provide authorisations, or assurances that credentials are valid.

### 12.2.13 Foreign domain
An administrative domain, visited by a Mobile IP client, and containing the AAA infrastructure needed to carry out the necessary operations enabling Mobile IP registrations. From the point of view of the foreign agent, the foreign domain is the local domain.

### 12.2.14 Home domain
An administrative domain containing the AAA infrastructure of immediate interest to a Mobile IP client when it is away from home.

### 12.3 Mobility Management Terminology
In this section some terminology is defined. More mobility related terminology can be found in Appendix B.

#### 12.3.1 Paging
Paging is a procedure initiated by the Access Network to move an Idle MH into the Active State. As a result of paging, the MH establishes a SAR and the IP routes are set up.

#### 12.3.2 Paging Area
A Paging Area is a part of the Access Network, typically containing a number of ARs/APs, which corresponds to some geographical area. The AN keeps and updates a list of all the Idle MHs present in the area. If the MH is within the radio coverage of the area it will be able to receive paging messages sent within that Paging Area.

#### 12.3.3 User mobility
User Mobility refers to the ability of a user to access services from different physical hosts. This usually means, the user has an account on these different hosts or that a host does not restrict users from using the host to access services.

#### 12.3.4 Personal mobility
Personal mobility complements user mobility with the ability to track the user's location and provide the users current location to allow sessions to be initiated by and towards the user by anyone on any other network. Personal mobility is also concerned with enabling associated security, billing and service subscription authorisation made between administrative domains.

#### 12.3.5 Handover (also known as handoff)
Handover is the process involved when an active MH (in the Active State) changes its point of attachment to the network, or when such a change is attempted. The access network may provide particular capabilities to minimise the interruption to sessions in progress.

#### 12.3.6 Context-aware Handover
A handover that is governed by a certain specific requirement to be fulfilled while handing the connection between two ARs.

#### 12.3.7 Network Assisted Handover
A handover where the AN collects information that can be used in a handover decision.

#### 12.3.8 Roaming
Roaming refers to a particular aspect of user mobility. Roaming is an operator-based term involving formal agreements between operators that allows a mobile to get connectivity from a foreign network. Roaming includes, for example, the functionality by which users can communicate their identity to the local AN so that inter-AN agreements can be activated and service and applications in the MH's home network can be made available to the user locally.

### 12.4 Security
In this section some terminology is defined. More security related terminology can be found in Appendix C.
12.4.1 Authentication
The act of verifying a claimed identity, in the form of a pre-existing label from a mutually known name space, as the originator of a message (message authentication) or as the end-point of a channel (entity authentication) [54].

12.4.2 Authorization
An "authorisation" is a right or a permission that is granted to a system entity to access a system resource. An "authorisation process" is a procedure for granting such rights. To "authorise" means to grant such a right or permission [41].

12.4.3 Credential(s)
Data that is transferred or presented to establish either a claimed identity or the authorisations of a system entity [41].

12.4.4 Data confidentiality
The property that information is not made available or disclosed to unauthorised individuals, entities, or processes (i.e., to any unauthorised system entity) [41].

12.4.5 Data integrity
The property that data has not been changed, destroyed, or lost in an unauthorised or accidental manner. Deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values [41].

12.4.6 Data security
The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorised. Both data confidentiality service and data integrity service are needed to achieve data security [41].

12.4.7 Digital signature
A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity [41].

12.4.8 Encryption
Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state [41].

12.4.9 Identification
An act or process that presents an identifier to a system so that the system can recognise a system entity and distinguish it from other entities [41].

12.4.10 Masquerade attack
A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity [41].

12.4.11 Non-repudiation service
A security service that provide protection against false denial of involvement in a communication [41].

12.4.12 Replay attack
An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack [41].

12.4.13 Repudiation
Denial by a system entity that was involved in an association (especially an association that transfers information) of having participated in the relationship [41].
12.4.14 Security association
A relationship established between two or more entities to enable them to protect data they exchange. The relationship is used to negotiate characteristics of protection mechanisms, but does not include the mechanisms themselves [41].

12.4.15 Security audit
An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures [41].

12.4.16 Security audit trail
A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results [41].

12.4.17 Security policy
A set of rules and practices that specify or regulate how a system or organisation provides security services to protect sensitive and critical system resources [41].

12.5 QoS Terminology
In this section some terminology is defined. More terminology related to QoS can be found in Appendix A.

12.5.1 Best-Effort Traffic
Best-effort traffic is a traffic type that has no reservation entry in the router.

12.5.2 Premium Traffic
Premium traffic is a traffic type that the router distinguishes from best-effort traffic and forwards its packets according to a QoS agreement.

12.5.3 Signalling Burst
The signalling burst denotes a certain number of signalling messages that arrive to the input port(s) of the router without interruption, causing persistent load on the signalling message handler.

12.5.4 Signalling Load
Signalling load is the load that manifests itself as the time required to process the incoming signalling messages.

12.5.5 Signalling Path
A signalling path is a sequence of network nodes and links along which signalling messages travel from one signalling end-point to the other.

12.5.6 Best-Effort Traffic Delay
Best-effort traffic delay is the forwarding time of a packet that does not belong to any premium traffic flow passing through a resource reservation capable router.

12.5.7 Multicast Resource Reservation Session
A multicast resource reservation session (or, in short, multicast reservation) denotes that certain QoS treatment is applied to the packets of every traffic flow related to a multicast group.

12.5.8 Premium Traffic Delay
Premium traffic delay is the forwarding time of a packet that belongs to a premium traffic flow passing through a resource reservation capable router.

12.5.9 Reservation Capable Router
By definition, a router is reservation capable if it understands a resource reservation protocol that signals the set-up or tear-down of resource reservation sessions or changes in an existing reservation session.

12.5.10 Reservation Initiator
The reservation initiator is the signalling end-point that initiates the resource reservation session setup.
12.5.11 Resource Reservation Session
The reservation initiator is the signaling end-point that initiates the resource reservation session setup.

12.5.12 Signalling End Point
A signalling end-point is a network node capable of initiating and terminating resource reservation sessions.

12.5.13 Signalling Load
Signaling load is the load that manifests itself as the time required to process the incoming signalling messages.

12.5.14 Session Load
Session load is the load that manifests itself as the excess processing power required to keep track of many reservation session

12.5.15 Signalling Path
A signalling path is a sequence of network nodes and links along which signalling messages travel from one signalling end-point to the other.

12.5.16 Policy Decision Point
A logical entity that makes policy decisions for itself or for other network elements that request such decisions

12.5.17 Policy Enforcement Point
A logical entity that enforces policy decisions.

12.5.18 Policy Information Base
Collections of related Provisioning Classes (PRCs) defined as a module.

12.5.19 Service Level Agreement
The documented result of a negotiation between a customer/consumer and a provider of a service, that specifies the levels of availability, serviceability, performance, operation or other attributes of the service [5].

12.5.20 Service Level Specification
Specifies handling of customer's traffic by a network provider. It is negotiated between a customer and the provider, and (for DiffServ) defines a set of parameters (such as specific Code Points and the Per-Hop-Behaviour, profile characteristics and treatment of the traffic for those Code Points) and their values. An SLS is a combination of an SLA (a negotiated agreement) and its SLOs (the individual metrics and operational data to enforce).
13 Appendix E: Background Information

13.1 W-CDMA

13.1.1 UMTS Existing Architecture

The general UMTS architecture, as currently specified, is presented in Figure 13. The architecture is split into 3 domains: user equipment domain, access network domain and the core network domain [12]. User equipment is the equipment used by the user to access UMTS services. User equipment has a radio interface to the infrastructure domain. The infrastructure domain consists of the physical nodes that perform the various functions required to terminate the radio interface and to support the telecommunication services requirements of the users.

The infrastructure domain is further split into the access network domain, which is characterised by being in direct contact with the user equipment and the core network domain. The access network domain consists of the physical entities that manage the resources of the access network and provides the user with a mechanism to access the core network domain. These entities are called Radio Network Subsystems (RNS). They are the access part of a UMTS network offering the allocation and the release of specific radio resources to establish means of connection between a UE and its corresponding Serving GPRS Support Node (SGSN).

The core network domain consists of the physical entities that provide support for the network features and telecommunication services. These entities include functionalities such as the management of user location information, control of network features and services, the transfer (switching and transmission) mechanisms for signalling and for user generated information. The Gateway GPRS Support Node (GGSN) is the node that is accessed by the external packet data networks. It contains routing information for the packet switched attached users. The GGSN is the first point of interconnection with a UMTS network. The SGSN is the node that is serving the UE. It is the part of the core network domain which is directly connected to the access network domain that provides the user’s access.

Figure 14 shows a closer view at the protocols in the user plane of the UMTS network.
The UE and RNS include L1, MAC, RLC and PDCP layers. These layers are further detailed in [10].

The RNS, SGSN and GGSN include the ATM layers plus a specific protocol, the GPRS Tunnelling Protocol for the user plane (GTP-U) [35]: This protocol tunnels user data between the RNS and the SGSN, and between the SGSN and the GGSN in the core network and is built over its own UDP/IP stack, used only for addressing purpose. GTP encapsulates all PDP User Protocol Data Units (PDU) where User IP packets are treated as transparent data. They cannot benefit from the features introduced in IPV6 such as QoS, encapsulation, …

13.1.2 Access Stratum Protocol Layers

This section provides an overview on the UMTS Radio Interface Protocol Architecture in order to prepare for discussions on the W-CDMA interface requirements to be defined within the framework of the Moby Dick project. The information is a summary of [10] and [11].

The radio interface is layered into three protocol layers and interfaces to User-Plane (U-Plane) and/or Control-Plane (C-Plane):

- **Non Access Stratum**
  - Mobility Management, Call Control
    - General Control, Notification, Dedicated Control
    - Terminates in Core Network
    - Terminates in UTRAN

- **Access Stratum**
  - Layer 3
    - C-Plane
    - U-Plane
  - Data Link
    - PDCP
    - RLC
    - MAC
  - Physical Layer
    - Local Inter-Layer Config. Control
    - Transport Channel SAP
    - Logical Channel SAP

**Figure 15: Radio Interface**

The Access Stratum offers services through the following Service Access Points (SAP) to the Non-Access Stratum:

- General Control (GC) SAPs;
- Notification (Nt) SAPs; and
Dedicated Control (DC) SAPs.

The RLC sub-layer provides ARQ (Automatic Repeat Request) functionality closely coupled with the radio transmission technique used. UTRAN retransmission functionality (RLC provision): the Core Network (CN) can request UTRAN to prevent all loss of data. In case of changed Radio Interface Iu-connection point (SRNS relocation) the loss of data relies on Duplication Avoidance mechanism.

Control services, allowing the RRC layer to control lower layers locally (i.e. not requiring peer-to-peer communication) are provided at Control SAPs (C-SAP).

A layer provides services through a set of service primitives (operations) to higher layers.

Layer 1 Services and Functions

Physical Layer offers information transfer services to MAC and higher layers.

Transport Channels: How and with what characteristic data is transferred
Logical Channels: What is transported

General classification of transport channels: (1) **Common** transport channels (2) **Dedicated** transport channels

(1) In-band identification of UE’s when particular UE’s are addressed
(2) When UE’s are identified by physical channels (code + frequency with FDD, code + time-slot + frequency with TDD)

Explanation for the following tables:

?: Up-link channel
?: Down-link channel
||: Or

**Common transport channels:**

?? Random Access Channel (RACH) ?
Contenction based up-link channel used for small amount of data. (initial access, non-real-time dedicated control and data traffic)

?? ODMA Random Access Channel (ORACH) ? (Not addressed in Moby Dick)
A contention based channel

?? Common Packet Channel (CPCH) ?
A contention based channel used for transmission of bursty data traffic. Only in FDD mode and only in up-link direction. Channel is shared by UE’s in a cell. CPCH is fast power controlled.

?? Forward Access Channel (FACH) ?
Common down-link channel without closed-loop power control. Small amount of data transport.

?? Down-link Shared Channel (DSCH) ?
Shared by several UE’s carrying dedicated control or traffic data.

?? Up-link Shared Channel (USCH) ?
Shared by several UE’s carrying dedicated control or traffic data. Only in TDD mode.

?? Broadcast Channel (BCH) ?
Down-link channel used for broadcast of system information.

?? Paging Channel (PCH) ?
Down-link channel used for broadcast respective control info into the entire cell.

**Dedicated transport channels:**

?? Dedicated Channel (DCH) ? || ?
Channel dedicated to one UE for up-link or down-link

?? Fast Up-link Signalling Channel (FAUSCH) ?
Up-link channel used to allocate dedicated channels in conjunction with FACH

**ODMA Dedicated Channels (ODCH)**

Dedicated to one UE used in relay link. (Not addressed in Moby Dick)

Each transport channel is assigned Transport Format (encoding, interleaving, bit-rate, mapping onto physical channels).

**Layer 1 Functions:**

- Macro-diversity distribution / combining and Soft-Handover execution
- Error detection on transport channels and indication to higher layers
- FEC encoding/decoding and interleaving/de-interleaving of transport channels
- Multiplexing of transport channels and de-multiplexing of coded composite transport channels
- Rate matching
- Mapping of coded composite transport channels on physical channels
- Power weighting and combining of physical channels
- Modulation and spreading / de-modulation and de-spreading of physical channels
- Frequency and time (chip, bit, slot, frame) synchronisation
- Measurements and indication to higher layers (e.g. FER, SIR, interference power, transmit power, ..)
- Closed-loop power control
- RF processing
- Support of timing advance on up-link channels (**TDD only**)
- Support of up-link synchronisation (**TDD only**)

**Layer 2 Services and Functions:**

**MAC**

- Not acknowledged data transfer between peer MAC entities without data segmentation provision (assigned to upper layers).
- On request of RRC execution of radio resource re-allocation and change of MAC parameters (change of transport format, change of transport channel type). **In TDD mode MAC can handle resource allocation autonomously.**
- Local measurement and report to RRC (traffic volume and quality indication)
- Mapping between Logical- and Transport Channels
- Selection of appropriate Transport Format for each transport channel (assigned by RRC)
- Priority Handling between data-flows of one UE
- Identification of UE’s on common transport channels (in-band identification of UE)
- Multiplexing / De-multiplexing of higher layer PDU’s
- Traffic monitoring and reporting to RRC
- Ciphering

MAC layer provides data transfer services on **logical channels**.

Two types are defined:

1. Control Channels (C-Plane info)
2. Traffic Channels (U-plane info)

ODMA (On Demand Multiple Access) channels are not considered within the framework of the Moby Dick project!

**Logical Control Channels:**

- Broadcast Control Channel (BCCCH)
  Broadcasting system info
- Paging Control Channel (PCCH)
  Transfer of paging info
- Common Control Channel (CCCH)
  Bi-directional channel for transmitting control info between network and UE’s. Used by UE’s, which have no RRC connection with the network and to access a new cell after cell reselection.
- Dedicated Control Channel (DCCH)
  Bi-directional point-to-point channel that transmits dedicated control info between a UE and the network.
- Shared Channel Control Channel (SHCCH)
**Bi-directional** channel that transmits control info for up-link and down-link shared channels between network and UE’s. TDD only.

- ODMA Common Control Channel (OCCCH) - (Not addressed in Moby Dick)
- ODMA Dedicated Control Channel (ODCCH) - (Not addressed in Moby Dick)

**Logical Traffic Channels**

- ODMA Dedicated Traffic Channel (DTCH) - Dedicated point-to-point channel, dedicated to one UE for the transfer of user information. Up- and Down-link
- ODMA Dedicated Traffic Channel (ODTCH) - Point-to-point channel for transfer of user-info between UE’s - (Not addressed in Moby Dick)
- Common Traffic Channels (CTCH) - Point-to-multipoint unidirectional channel for transfer of dedicated user info for all or a group of UE’s

**RLC**

*Services provided to the upper layer*
- Data Transfer
- Maintenance of QoS as defined by upper layers
- Notification of unrecoverable errors

*RLC functions*
- Segmentation and re-assembly
- Concatenation and Padding
- Transfer of user-data
  + Acknowledged + unacknowledged data transfer
  + Transparent data transfer (no additional protocol info)
- Error correction
- In-sequence delivery of higher layer PDU’s
- Duplicate detection (on RLC PDU level)
- Flow control
- Sequence number check (in unacknowledged data-transfer mode)
- Protocol error detection and recovery.
- Polling.
- Status transmission.
- SDU discard.
- Estimated PDU Counter (EPC) mechanism.
- Suspend/resume function.
- Stop/continue function.
- Re-establishment function.

**PDCP**

- Mapping of Network PDU’s from one network protocol to one RLC entity
- Compression / De-compression (TCP-IP header compression!)

**Layer 3 - Uu Stratum Services and Functions**

**Uu Stratum Services**

*General Control*
Provides an *information broadcast* service (NAS info)
Info is transferred on an *unacknowledged* mode link

*Notification*
Broadcast Paging info to UE’s ion a certain geographical area
Info is transferred on an *unacknowledged* mode link
This service should allow addressing of a specific UE or all UE’s in a specific geographical area
**Dedicated Control**
Establishment and release of connections (point or group connections)

**RRC functions**
- Broadcast of information provided by the non-access stratum (Core Network).
- Broadcast of information related to the access stratum.
- Establishment, re-establishment, maintenance and release of an RRC connection between the MN and UMTS Network (UTRAN).
- Establishment, reconfiguration and release of Radio Bearers.
- Assignment, reconfiguration and release of radio resources for the RRC connection.
- RRC connection mobility functions.
- Paging/notification.
- Routing of higher layer PDUs.
- Control of requested QoS.
- UE measurement reporting and control of the reporting.
- Outer loop power control.
- Control of ciphering.
- Slow DCA (TDD).
- Arbitration of radio resources on uplink DCH.
- Initial cell selection and re-selection in idle mode.
- Integrity protection.
- Initial Configuration for CBS.
- Allocation of radio resources for CBS
  - Configuration for CBS discontinuous reception
  - Timing advance control.

**13.1.3 Mobile Node (MN) modes:**
The Mobile Node can be either in

1. IDLE mode or
2. CONNECTED mode

After power on, the MN stays in IDLE mode until it requests to establish a RRC connection. In idle mode, the UE is identified by non-access stratum identities, such as IMSI (International Mobile Subscriber Number) or TMSI (temporary MSI).
The connection mode is entered when the RRC connection is established (between UE and RNC). The UE is assigned a radio network temporary identity (U-RNTI and C-RNTI) to be used as UE identity on common transport channels.
The UE leaves the connected mode and enters the idle mode when the RRC connection is released or at RRC connection failure.

**Figure 16: Mobile Node modes**
13.2 Ethernet

IEEE 802.3 (Ethernet) is a standard for wired LANs. Fast Ethernet (IEEE 802.3u) and Gigabit Ethernet (IEEE 802.3ab) are evolutions of the Ethernet standard that provide higher data transmission speeds. All of them are well-known protocols and we are not going to detail their procedures here. In the basic set-up, all the stations in an Ethernet network share the medium, and contend in an equal basis for its use. Data delivery is best effort without QoS guarantees.

IEEE 802.1p is the standard that provides LAN elements (bridges, switches) with capabilities for supporting time-critical communications in a shared media environment. (Note: this is part of the 802.1D standard, which discusses bridges behaviour, but its importance has long superseded by the 802.1p relevance to IEEE LANs).

In the simplest form, a bridge receives a frame, decides to which port to forward it, and transmits it. With 802.1p, multiple transmission queues (with different priorities) exist for each output port. An algorithm for selecting frames from the queues is suggested in 802.1p (priority queuing), but others can be implemented. The key idea behind this standard is that different frames will receive different forwarding treatment, thus providing time-critical communications with smaller network delays. These frames can be selected either by user priority or by port configuration. There are eight defined traffic priorities:

<table>
<thead>
<tr>
<th>User priority</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (default)</td>
<td>Best Effort</td>
</tr>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>Spare</td>
</tr>
<tr>
<td>3</td>
<td>Excellent Effort</td>
</tr>
<tr>
<td>4</td>
<td>Controlled Load</td>
</tr>
<tr>
<td>5</td>
<td>Video</td>
</tr>
<tr>
<td>6</td>
<td>Voice</td>
</tr>
<tr>
<td>7</td>
<td>Network Control</td>
</tr>
</tbody>
</table>

Bridges can implement less queues per port, and perform a re-mapping of these user priorities. Best effort traffic, corresponding to non-marked frames, will not be mapped to the lowest priority unless the number of output queues is smaller than four.

A final note related with Ethernet switches. Although a switch can be considered a special type of multi-port bridge, most of them act in cut-through mode, transmitting a frame before its complete reception. This implies that priority is only relevant in the context of accessing a backbone – however care must be taken in modifying any priority information due to the frame checksum field.

13.3 Wireless LAN

The IEEE 802.11 standard is the world’s first wireless LAN standard for packet data applications operating in the 2.4GHz unlicensed frequency band supporting data rates between 1 and 11 Mbps (with an extension to the physical layer, resulting in 802.11b). Two radio physical layers are possible within the standard: FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum).

There are two classes of wireless local networks:

1. Ad-hoc networks: all the stations are within mutual communication range of each other, communication is direct between stations without using other communication devices. These networks are called IBSS (Independent Basic Service Set) in the IEEE 802.11 standard.
2. Infrastructure networks: networks that use access points to allow their associated stations to communicate among themselves and to distribution systems. Using a distribution system is possible to interconnect several BSS’s to form an Extended Service Set (ESS).

The IEEE 802.11 uses a shared medium for transmission (radio channels in the 2.4 GHz band). So some MAC protocol is needed to regulate the access to the medium of the different stations in a wireless network. There are two modes to do this:

- Carrier-sense multiple access with collision avoidance (CSMA/CA): A mandatory contention-based protocol similar to IEEE 802.3 Ethernet. The 802.11 specification refers to this mode as the distributed co-ordination function (DCF).
Priority-based access: An optional contention-free access protocol usable on infrastructure network configurations containing a controller called a point co-ordinator within the access points. The 802.11 specification refers to this mode as the point co-ordination function (PCF).

As the name implies, the access mechanism for DCF is entirely distributed. This can result in two workstation transmitting simultaneously since each node is responsible for determining if it is safe to transmit. To determine if it is safe to transmit, a station must:

- First sense the medium for a required time interval to ensure that no other station is transmitting or plans to transmit.
- If not then it can proceed with transmission
- If the node senses that another node is transmitting then it will go into a back off mode.
- In back off mode the station, selects a random interval to use for its back off timer

The station decrements its back off timer only when the medium is idle. Once the station’s back off timer reaches zero, it transmits. DCF also supports the use of Request To Send (RTS) and Clear To Send (CTS.) IEEE 802.11 requires that all devices support RTS and CTS. However, their use is optional. By using an RTS/CTS/DATA/ACK sequence of transmissions, the effects of a “hidden node” can be mitigated. It should be noted that Acknowledgement (ACK) packets and CTS packets are given higher priority than DATA frames. This means that a workstation needing to send an ACK or a CTS packet once it receives a DATA or RTS packet, can do so without going through the contention phase presented above. This priority is implemented through the use of different Inter-Frame Space (IFS) intervals. For DCF, two such intervals are specified. The first is DIFS, or DCF IFS, which is the mandatory time for sensing the channel prior to data transmission. DIFS is used when transmitting DATA or an RTS packet. The second interval, Short IFS (SIFS), is the time for sensing the channel prior to sending a CTS or ACK frame. Because SIFS is much shorter than DIFS, a station receiving a packet will always be able to send an ACK or CTS before any other station can send data because it only has to wait 1 SIFS while the other stations must wait at least 1 DIFS.

PCF supports both asynchronous and time-bounded services such as voice traffic, and would be used in a WLAN with an existing infrastructure (access-points). In this type of system there is a Point Co-ordinator, generally an access point, that uses a poll-response scheme and provides nearly isochronous operation. If stations have time sensitive data to transmit, they will request that the PC add them to its polling list. Periodically, the PC will gain access to the medium to begin a contention-free period (CFP) These CFPs are limited so that contention (DCF) periods are able to occur. To gain access to the medium, the PC uses DCF and then transmits a beacon to mark the beginning of the CFP and advertises the expected length. All stations mark the expected duration in their Network Allocation Vector (NAV) After the beacon, PCF IFS (PIFS) is used when transmitting so stations using DCF will not get to transmit since PIFS is shorter than DIFS. During this CFP, the PC can send data to a station (or multiple stations), a Contention-Free poll(CF-Poll), or a Contention-Free ACK (CF-ACK.) This can be done in single or multiple frames. The stations during this period can CF-ACK a data frame from the PC or send data to the PC in response to a CF-Poll. At the end of the CFP, the PC will send a Contention-Free End (CF-End) to let all station know that the CFP has ended an that the DCF contention period has begun. All these concepts are illustrated in figure below (taken from the ANSI/IEEE Std. 802.11, 1999 edition). However, it is important to realise that available products only implement the DCF mode of operation.

![Figure 17: Medium access in PCF mode](image-url)
Three classes of frames are used in the MAC layer of the IEEE 802.11 standard: management frames, control frames, and data frames. Management frames are used to establish initial communications between stations and access points. Control frames are used to assist in the delivery of data frames. We have already seen several examples: RTS, CTS, ACK, CF-End, etc. Data frames are used mainly to carry information of upper layers.

One specially interesting management frame is the beacon frame. It is used by stations to discover 802.11 networks. In an infrastructure network the access points periodically send beacon frames. In an ad-hoc network all stations periodically send beacon frames. This allows new stations to discover, synchronise and join the IEEE 802.11 network. It is possible to actively look for a IEEE 802.11 network by sending a management frame called Probe request. A beacon frame has enough information for a station to join the corresponding network, for example service set identity, supported rates, information for timing synchronisation, etc. As it is a frame, potentially other information could be included there (for example, some vendors use this frame to send proprietary extensions to the protocol).

There are also proposed mechanisms to increase efficiency of PCF [48][48], studies about supporting voice services over 802.11[49] [49], [50], introduction of service differentiation for DCF [47], and many others.
14 Appendix F: Related Work

14.1 Related Projects

14.1.1 WINE GLASS

IST-1999-10699 WINE GLASS (Wireless IP Network as a Generic Platform for Location Aware Service Support), a 2-year European 5th Framework Program project started in January 2000, researches into and develops a Beyond-3G mobile Internet architecture and testbed. The DiffServ-based WINE GLASS architecture is composed of IPv6-based administrative domains, supporting hybrid wireless access of 802.11b WLAN and emulated UTRAN (without the conventional 3G Core Network), interconnected by an IPv4 backbone.

While 3GPP release 4 and 5 rely on an overlay architecture where IP is used in the Core Network for transport only [10], [11], the WINE GLASS architecture [68] goes a step further in the use of IP within the network. In WINE GLASS, the standard GPRS-based UMTS Core Network is replaced by a pure IPv6 backbone where standard UTRAN Radio Network Controllers (RNCs) are attached to via dedicated entities called UTRAN-IP Gateways. Each UTRAN-IP Gateway is associated with one RNC (may be co-located) to form an IPv6 subnet to perform interworking between UTRAN and the IP backbone. IPv6-based technologies are used in order to provide Mobility Management, Authentication-Authorisation-Accounting (AAA) and Quality of Service (QoS) support.

14.1.1.1 Radio Gateways

As mentioned above, the WINE GLASS architecture introduces UTRAN-IP Gateways to perform interworking between UTRAN and the IP backbone. Three basic functions are supported by the UTRAN-IP Gateway:

- Interworking with the backbone and the IP standard transport functions. This includes:
  - Relay of Internet traffic (IPv6 packets) from/to the mobile attached to the RNC to/from the IPv6 backbone,
  - Mapping of end-to-end (i.e. transport level) QoS onto UTRAN QoS support.
- Support a newly defined Non-Access-Stratum (NAS) signalling for Session Control and Mobility Management that had to be introduced in WINE GLASS due to replacement of the GPRS-based Core Network by a pure IPv6 backbone. This includes:
  - Procedures to handle connections (PDP Context) over UTRAN. The UTRAN-IP Gateway is a NAS signalling termination point (instead of the standard GPRS-based Core Network).
  - Interworking with AAA.
  - Inter UTRAN-IP Gateway signalling for handover between RNCs.
- Support standard RANAP (AS) signalling since the interface between UTRAN and the IPv6 Core Network (i.e. the UTRAN-IP Gateway) is the standard 3GPP Iu-ps interface. This includes the support for SRNS relocation.

WINE GLASS proved this approach to be successful and the experience of this project is to be re-used in Moby Dick where a similar entity called Radio Gateway is to support interworking between the IPv6 backbone and the W-CDMA access network. While WINE GLASS UTRAN-IP Gateway was dedicated to the UTRAN access only, Moby Dick will research into and develop a Radio Gateway functional architecture to support any kind of QoS-enabled access technologies so that it can be used with the Moby Dick W-CDMA access as well as others (e.g. HiperLAN/2, IEEE802.11e, etc).

14.1.1.2 Mobility Management

In WINE GLASS, Mobile-IPv6 is used to handle macro-mobility (i.e. movements between access points “far” one from the other according to the network topology). This includes the following movements:

- Between two 802.11b (or Ethernet) IPv6 subnets,
- Between two RNCs in UTRAN, and
- Between a 802.11b (or Ethernet) subnet and UTRAN (i.e. one RNC): this is vertical handover.

On the other hand, the legacy access mobility management scheme is used to handle micro-mobility. This includes the following movements:

- Between two 802.11b Access Point within the same IPv6 subnet, and
- Between two Node-Bs attached to the same RNC in UTRAN. Here standard UTRAN-internal mobility management procedures (e.g. handover) are used.
WINE GLASS proved the suitability of Mobile-IPv6 to support macro-mobility and highlighted its potential weaknesses in supporting seamless handover especially in the case of applications with stringent delay requirements. Starting from this experience, Moby Dick is to investigate IPv6-based mobility protocols to provide seamless mobility in addition to mobile-IPv6. This will include refinement, evaluation and possibly implementation of some proposals under standardisation at the IETF such as Fast Mobile-IPv6 (FMIPv6), Hierarchical Mobile-IPv6 (HMIPv6) [24] or other innovative approaches.

14.1.1.3 Quality of Service

The WINE GLASS QoS architecture aims to provide Soft-guaranteed QoS to mobile users. Soft-guaranteed QoS means to design the system taking into account QoS and partially QoS negotiation mechanisms, but without an effective guarantee about the QoS levels. For that reason, in addition to its advantages compared to IntServ/RSVP with respect to scalability and operation in a mobile environment, DiffServ is used in the IP backbone to provide QoS. No Connection Admission Control is performed at the Core Network (i.e. IP backbone) level and availability of resources is guaranteed by a suitable dimensioning (i.e. over-provisioning of the capacity) in the backbone. On the other hand Connection Admission Control is performed in the UTRAN access thanks to the AAA attendant function on the UTRAN-IP Gateway. This QoS architecture is suitable as long as the bottleneck is considered to be the access (and not the core) that is the case in WINE GLASS and future IP-based wireless systems incorporating only QoS-enabled access technology with limited capacity such as UTRAN. QoS classes have been defined at the application level, at the IP level and in the UTRAN access. In WINE GLASS, packet marking is done in the Mobile Terminal by mapping the application-level QoS class into corresponding DiffServ Code Point (DSCP). QoS mapping between IP (DSCP) and UTRAN is implemented in the Mobile terminal and UTRAN-IP Gateway thanks to a static mapping table implementing “best matching” QoS classes mapping.

Moby Dick will benefit from the experience of DiffServ and QoS mapping functions provided by WINE GLASS. In addition, Moby Dick is to investigate alternative (or more advanced) QoS functionalities in order to provide a true end-to-end mobility-enabled IPv6-based wireless Internet architecture. The objective being to propose and architecture enabling mobile users to benefit from QoS irrespectively of the network they attach to (Home or Foreign) and minimising the impacts of mobility on QoS provisioning and guaranteeing.

14.1.1.4 Authentication, Authorisation and Accounting

The AAA architecture of WINE GLASS relies on the introduction of one (or more) AAA server in the IPv6 backbone of each Administrative Domain. The Diameter protocol is used to handle inter-AAA-Server communications as well as communications between an AAA-server and Attendants (i.e. AAA clients). For the UTRAN access, an Attendant is placed in each UTRAN-IP Gateway that is performing Access Control and Connection Admission Control:

?? The user provides its credential in the Attach phase (NAS signalling). Once it has been authenticated the user can request establishment of data channels (PDP contexts).

?? User QoS profile is checked on the AAA server when the mobile requests PDP context activation.

For the WLAN 802.11b access, an Attendant is placed on each Edge Router. AAA messages between MN and Attendant can be included in Stateless/Stateful address auto-configuration procedure. It is worth mentioned that, except some very immature proposals, there is currently no standard protocol (so called User Registration Protocol - URP) for AAA communication between the Mobile Terminal and the Attendant. Due to the lack of open source implementation of Diameter and URP, no real AAA protocol has been deployed within the WINE GLASS testbed. However, a very basic AAA server (to discuss with Attendant located on UTRAN-IP Gateways) has been implemented to support basic Authentication and Authorisation of Mobile Terminals attached to the UTRAN access. Accounting has not been considered within WINE GLASS.

The general AAA architecture proposed in WINE GLASS may be re-used and extended in Moby Dick. The main objective is to research into interoperability of AAA and QoS framework in a mobile environment. Other issues such as optimisation of AAA procedures in case of intra-domain mobility (AAA context transfer between Attendant, etc…) or accounting mechanisms should be worked on.

The official web page of the project is: http://domobili.cselt.it/WineGlass/
14.2 Standardisation Bodies

There are several working groups and organisations working on a network architecture merging the two network paradigms - on one hand, the POTS network and the Internet and on the other hand, the wired and wireless network where the Internet plays a dominant role. As consequence of this trend, within the IETF community some work started addressing this migration process on several levels. Mobile IPv6 [7] has been developed to support mobile nodes and is unable to support mobile networks efficiently. Here, the Mobile IPv6 ability to support mobile networks is discussed and some required extensions are proposed. But also within the IETF there exist several competing approaches which will be briefly introduced in the following sections.

A further movement towards such kind of open architecture could be observed within the Mobile Wireless Internet Forum (MWIF). MWIF is an international non-profit industry association. Its mission is to drive an open Internet architecture that enables seamless integration of mobile (wireless) telephony and IP-based services (voice, data, video, web, etc.) for the mobile wireless networks, meeting the needs of network operators and Internet service providers, and is independent of the air interface. The focus is on accelerating the deployment of open, Internet-based standards for mobile wireless networks, and its motivation is interoperability and open standards [15].

14.2.1 MWIF Overview

The MWIF Architecture Principles Technical Report [55] intends to support business goals as for significant cost reduction, accelerated time to market, variety of services with open service creation environment and to grow Internet services business. The overall intention is to develop a scalable and distributed architecture. Similarities to Moby Dick directions can be derived from architectural principles like having the Internet Protocol (IP) in the Access Networks and the Core Network for transport and control as well as to adopt Internet official protocol standards as they are discussed and specified within the framework of IETF standardisation. A minimum set and capabilities of the architecture includes services for AAA (Authentication, Authorisation & Accounting), Quality of Services, IP Mobility, Security, Session Management as well as Naming and Directory Services. In order to allow scalability within the entire architecture, logical separation of user data and control as well as services is a requirement. A decomposed Gateway architecture is considered in the MWIF architecture in order to separate bearer from signalling traffic. Furthermore, separation of Mobility management from Session management is a requirement. In the MWIF architecture, mobility management shall be hierarchical and independent of other functions within the architecture. Support of Terminal-, Personal- and Session Mobility is planned with an architecture keeping the MWIF Core Network independent of the access technology.

Figure 18 shows the MWIF layered architecture, as it is specified in [57]. The MWIF architecture is distributed to four logical layers, which is the Transport layer for Access Network and Core Network area, the Control layer, a layer for Services and one for the Applications. Referring to Figure 18, security issues are assigned to several layers (e.g. distributing database functionality from control). This is in order to ensure authorised use of network resources and services. The Application layer refers to applications and services provided by 3rd parties to end-users. Access to the other layers is considered to be supported with an Open API. The Service layer comprises for example Directory Services, Location Server, Policy Server and Authorisation relevant functional elements. Even IP DNS is assigned to this layer. The Control layer comprises again Authentication and Accounting as well as Mobility management, Resource management and Address management. The respective document [57] refers to Macro Terminal Mobility and Inter-administrative Domain Terminal Mobility as well as to handover control for Macro Terminal Mobility and Inter-administrative Domain Terminal Mobility for the Mobility management functionality assigned to the Control layer. The Resource manager assigned to this layer is responsible for controlling the Core Network bandwidth. Address management refers to control of address assignment, which is allocation and de-allocation of IP addresses within the address space of an administrative domain. The Transport layer is responsible for IP bearer and signalling transport from individual users to the Core Network. It comprises Access Network as well as Core Network elements. Figure 1 refers to an Access Gateway, which is a node separating Access Network and Core Network. It conveys bearer streams between the Access Network and the Core Network based on QoS policy and authorisation levels. Furthermore, it asserts terminal and network requested QoS to bearer and control data packets, it transports control streams between AN and IP Core Network. The Network Reference Architecture [58] describes the functional entities of the Core Network. The MWIF technical report [59] proposes IP in the RAN as a transport option. The document “considers how IP networks and protocols can be applied as a transport option for Radio Access Networks within 3rd Generation mobile systems and the benefits which might be provided. Within this work IP is only considered as a transport option over the RAN internal
interfaces and RAN interfaces to the core network, without any changes to the RAN architecture or radio control protocols. With report [59], the forum intends to influence and support input to 3GPP and 3GPP2 as well as to the IETF.

With respect to the Radio Access Network, MWIF refers to protocols and models specified within the framework of 3G standardisation. This is the consideration of Interfaces like [Iu], as well as 3GPP2 related interfaces respectively. Other systems such as IEEE802.11 wireless LAN and Bluetooth are not considered in [59] due to the different background and assignment of complexity.

For appropriate QoS within the RAN, techniques like MPLS, DiffServ and IntServ are considered within the framework of MWIF’s IP in the RAN activity, but always with respect to transport of radio packets over the IP protocol through the RAN between wireless Access Points (Node-B’s) and the respective RNC. With respect to IP security, the document [59] refers to RADIUS, which supports endpoint authentication using encrypted passwords. DIAMETER is a backward compatible extension of RADIUS that allows definition of application profiles supporting different kinds of access control and authentication. IPSEC supports secure tunnels between endpoints with and without encryption.

Same as Moby Dick intends, the MWIF architecture shall adopt existing or evolving IETF protocols in order to extend wireless support. Furthermore, the architecture shall inter-operate with other next generation fixed and mobile networks and Media Gateways (legacy or PSTN). Unlike Moby Dick, the MWIF architecture shall maintain compatibility to interfaces specified within the framework of 3GPP [Iu, Iu'] and 3GPP2 [open A and Abis]. Furthermore, the Radio Access Network (RAN) is still handled separately from the Core Network part in order to allow independent evolution. RAN & Core Network area is to be separated with an Access Gateway. Support of legacy networks and terminals is considered via appropriate Gateways.

14.2.2 3GPP2

3GPP2 is a Standard Developing Organisation (SDO) that was formed between Chinese, Japanese Korean and North American national SDOs to specify IS-41 based 3rd Generation cellular system, often referred as cdma2000. Currently, 3GPP2 is working on All IP Network specifications for cdma2000 networks.
In the rest of this chapter we present an overview of the 3GPP2 All IP Reference Architecture. Please note that the work in this area is still on going. Thus things mentioned here are subject to change before the specification are completed.

As there is a lot of similitude between 3GPP and 3GPP2 All IP architecture, the simplified 3GPP All IP Reference Architecture is summarised in Figure 19. Please refer to [62] for more details.

![Figure 19: GPP All IP Reference Architecture](image)

The All IP architecture currently discussed in the 3GPP2 is illustrated in Figure 20. This is a schematic vision. Please refer to [61] for more details.

The architecture is described in 3GPP2 Network Architecture Model (NAM) document. The basis of architecture is in the evolution of the cdma2000 specifications. Like the 3GPP architecture, also 3GPP2 All IP network architecture can be split into several domains:

![Figure 20: 3GPP2 All IP Reference Architecture](image)

Access Network and Access Gateway together equals roughly to combination of RAN and GPRS of the 3GPP architecture; They provide IP bearers from Mobile Station to IPT core network. However, the
functional split is slightly different; e.g. user authentication is done in the cdma2000 Access Network, while in 3GPP those are GPRS network functionality (register and attach functionalities).

Session Control Manager (SCM) and Media Resource Function (MRF) of the 3GPP2 have very similar functionality than the CSCF and MRF of the 3GPP. Also in 3GPP the SCM has several identified roles: Interrogating SCM (I-SCM), Serving SCM (S-SCM), and Visited SCM (V-SCM). The roles of those are practically the same than respective CSCFs of the 3GPP.

While the 3GPP has incorporated all database into HSS (Home Subscriber Server), the 3GPP2 architecture has block called 'Databases'. The different databases of the 3GPP2 architecture in turn have similar functionalities than the HSS of the 3GPP.

While in 3GPP the QoS management functionalities are incorporated into RAN and GPRS network entities, in 3GPP2 architecture we can see separate QoS management functions. The subscription QoS manager (SQM) makes policy decision on QoS allowed for user session based in subscriber profile and current QoS allocation for users. On the other hand core QoS manager (CQM) makes decisions on use of the QoS resources within one core network.

The 3GPP2 All IP architecture relies on Mobile IP (MIP) infrastructure for roaming between different access gateways. Thus, MIP Home Agent and Foreign Agent are introduced in the reference architecture. Please note that MIP is used for mobility management across Access Gateways and 3GPP2 proprietary protocol is used for mobility within one Access Gateway’s area.

The Gateways of 3GPP2 resemble very much the Gateways of the 3GPP, Media Gateway Control Function, Media Gateway, and Trunk Signalling Gateway of 3GPP2 have similar functionality than MGCF, MGW, and T-SGW of 3GPP respectively. However, 3GPP2 introduces also Network Capability Gateway (NCGW), which main task is to authorise servers’ use of the network resources. In 3GPP architecture functionality of NCGW is embedded into CSF.

14.2.3 IETF and IRTF approaches

There are several proposals, currently published by Internet Drafts, which address Moby Dick relevant issues.

The following proposals target a “Open Radio Router” concept similar to Moby Dick:

14.2.3.1 Seamobyobjectives and historic review

Seamoby[66] is an IETF working group originated from the mobieip working group. This separation was done in order to concentrate specific efforts to the development of a new protocol would allow state information to be transferred between edge mobility devices. There was no clear idea on this “state information” that could be transferred; examples at the time were AAA information, security, QoS properties, Robust Header Compression information, specific routing protocols information, etc.

Seamoby was thus idealised as the “working piece” for the provision of the real-time services in mobile IP environments. Its results should allow for real-time services to work with minimal disruption across heterogeneous wireless and wired networks. Currently, Seamoby is working on key areas for real-time service provision in mobile environments: Context Transfer, Handoff Candidate Discovery, and Paging (“Dormant Mode Host Alerting”).

“Context Transfer” arises due to the fact that changes of communications path due to roaming sometimes includes a change in communications media between the mobile terminal and the network (e.g. in Moby Dick, changing from wireless to wired LANs) – and in the case of cellular networks, these changes can occur very fast. MobileIP does handle the change of attachment point, but active IP flows need to be kept, in the same “context”. The IP flow context that might be useful to transfer could include, issues as security context, policy, QoS information, header compression, and accounting/AAA information. Seamoby aims to analyse the requirements and trade-offs of such a context change, and eventually develop a protocol to transfer this information with real-time applications constraints. This is associated to the so-called “fast-handoff” notion, under development in the mobieip working group.

“Handoff Candidate Discovery” is the natural complement of this work. The mechanisms under development for handoff (in mobieip) assume that a set of candidates has already been chosen and that handoff should be initiated to all of them. However, “seamless” handoffs may be best achieved by considering multiple handoff candidates and selecting one or more of them as targets for context transfer.
Thus, Seamoby will define this work in a problem statement, and if needed, will define the requirements and the protocol for a handoff candidate discovery protocol, which could be used with any mobility management protocol.

“IP Paging” (Dormant Mode Host Alerting) is typically used in networks that support mobile devices that periodically enter dormant mode to reduce power consumption. Seamoby will develop a protocol to enable network devices to track a mobile that has moved from its last point of attachment, while in dormant mode, allowing the mobile's packets to be delivered.

There are several potential relationships between the Seamoby working group and the Moby Dick project.

First, it is important to recognise that Seamoby and mobileip are closely coupled – much work may be of interest to both groups, specially due to the already mentioned relationships between Seamoby and its “foster” group. Second, Moby Dick work clearly interacts with both groups, and, depending on the specific approach to take in the Moby Dick architecture, each one of these groups will be more or less interested in Moby Dick developments and trials.

In terms of results, current pace of development inside Seamoby may question the usage of its proposed solutions in the Moby Dick trial. However, the project aims can be closely mapped into some of the objectives of the Seamoby working group. Some of the proposals under discussion on the Paging and Context Transfer areas may have some impact on Moby Dick developments. Thus, if Moby Dick is able to proceed in its own scheduled development, it is highly possible for the project to present its own results as a contribution to the working group activities. This type of interaction would be extremely beneficial for the project, both from the technical and administrative point of view. However, it may require some added flexibility by the consortia members, in order to advocate and support the solutions implemented inside the project (and eventually, adapt some of those to the results of the interactions inside the IETF).

### 14.2.3.2 Hierarchical Mobile IP

There is the general perception that although Mobile IPv6 (MIPv6) [23] is a good protocol to face macro-mobility issues, it has certain deficiencies when dealing with micro-mobility issues. But micro-mobility is a potentially usual and important case (for example, in the Moby Dick environment): a mobile node is away from its home network and moving across different IP subnets in a visited domain. For this reason there are several proposals to complement Mobile IPv6 to improve its efficiency when dealing with micro-mobility. Examples are hierarchical Mobile IP for IPv6 (HMIPv6) [24][25] and Regional Registrations [26]. In this section we are going to describe HMIPv6. More information about HMIPv6, and the related approach Mobile IPv6 Regional Registrations, can be found in the references and also in Appendix B.

HMIPv6 proposes a hierarchical mobility management model that complements MIPv6 to deal with micro-mobility issues with the aim of minimising the latency due to handovers, and reducing the amount of mobility signalling. Hierarchical means that at least two routers are involved in managing the MN mobility (the HA as in MIPv6 and at least one more in the visited domain). We don’t do a detailed description of protocols and procedures, that can be found in the references. We want to give the basic idea of how this approach works, what are its advantages and requirements.

In MIPv6 mobility management is done by the Home Agent (HA) (no hierarchy). In HMIPv6 at least one level of hierarchy is introduced, a new function called Mobility Anchor Point (MAP) is done in a router at the visited domain. The MAP is not constrained to be in the same subnet as the Mobile Node (MN), in fact any physical location for the MAP is possible within the visited domain, although better performance is achieved by connecting the MAP to the border router of the network is serving. Thus, a MAP is not needed in each subnet, although there can be more than one MAP in a domain, allowing the use of more than one level of hierarchy in mobility management of MN’s.

A MAP provides an address or a prefix to form addresses that can be used as a global CoA by MN’s visiting the domain. The HA or CN’s (after route optimisation) use this address to send packets to the MN. The MAP will tunnel these packets to the MN within the MAP domain using a Local CoA (LCoA). The LCoA is an on-link IPv6 address in the subnet where the MN is. If the MN moves to another subnet within the MAP domain, the global CoA does not change, only the MAP must be informed of the new LCoA of the MN. Compare this with MIPv6, in the case of a handover, the HA and all the CN’s must be informed of the new MN CoA. Now we can see the advantages of HMIPv6 for micro-mobility. The handover latency is reduced because mobility is managed locally. Besides, the MAP can support Fast Handovers [27] (both proposals are compatible). Also, mobility signalling load is reduced. No mobility signalling is sent out of the MAP domain in case of an intra-domain handover, and only the MAP (perhaps more than one if the MN is using a multi level hierarchy) must be informed of the change (in MIPv6 the HA and all the CN’s must be informed). HMIPv6 architecture is shown in Figure 21.
HMIPv6 is an extension to MIPv6, a MN that is HMIPv6-aware can use the MAP or can use the standard MIPv6 implementation (ignoring the MAP and registering the LCoA in the HA). Moreover, the MN can use the LCoA with certain MN’s (for example, those in its same subnet to avoid going through the MAP) and the global CoA with the rest.

There are two MAP modes in HMIPv6. In Basic Mode, the MN forms an IPv6 address in the MAP subnet (Regional CoA or RCoA) using the MAP announced prefix. The MN uses the RCoA as the global CoA. In Extended Mode, the MN uses the MAP IPv6 address as an alternate-CoA. The decision of which mode to use is a network administration one. Each MAP can support only one mode at a time.

To use HMIPv6, a MN must discover the MAP’s serving the domain it is visiting. To do this, a new MAP option for Router Advertisement messages is proposed. This option includes the distance to the MAP in number of hops, a level of preference in using this particular MAP, the MAP global IPv6 address, and an indication about the mode of operation (basic or extended) of the MAP. If the MAP is operating in basic mode, the MAP option includes also the MAP’s subnet prefix. To propagate the MAP option from the MAP to the MN there are different possibilities. For example, the routers in the domain, including the MAP and the Access Routers (AR’s) can be manually configured to propagate the MAP option on certain interfaces. The result is that the MN receives router advertisements from its AR including a MAP option for each MAP that it is serving the subnet where the MN is. It is up to the MN to choose one or more (more than one level of hierarchy) MAP’s to use. A MAP domain is defined as the subnets where the MAP option of a particular MAP is received. The domains of different MAP’s can overlap.

After discovering the MAP, the MN must register in it. This is done using a extended Binding Update (BU) option that allows to indicate a MAP registration, differentiating it from a HA registration or a BU sent to CN’s.

Summarising the advantages of HMIPv6, it allows reducing the signalling load in intra-domain handovers (no signalling is sent outside the domain), and intra-domain handovers delay is reduced because the handovers are managed locally. Hierarchical proposals seem to be useful also in the integration of AAA infrastructure and QoS provision in MIPv6 [29][51][24], mainly due to the idea of using the MAP as a point to provide context transfer to the MN in handovers, but how this can be exactly done is not clearly defined yet. Last, a paging framework can be easier to create in a HMIP environment.

HMIPv6 also has disadvantages, it implies some modifications to the basic MIPv6, it means more complexity in the network, end-to-end delay can be longer because the intermediate processing, and potentially inter-domain handovers delay can be increased.

14.2.3.3 IETF AAA

The AAA WG developed requirements for Authentication, Authorisation and Accounting as applied to network access and Mobile IPv4 [2], [3], [4], [1]. Requirements were gathered from several groups and
the AAA WG then solicited the submission of protocols meeting the requirements, and evaluated the submissions. Currently the AAA WG focuses on the development of an IETF Standards track AAA protocol namely the DIAMETER protocol which is the successor of the RADIUS protocol. Currently there are a couple of drafts which define: The DIAMETER base protocol, network access application, Mobile IPv4 application and security. Two interesting related drafts which are currently individual submissions have been presented on the last IETF: DIAMETER Mobile IPv6 application [70] and the mapping of basic and digest authentication to DIAMETER [68].

14.2.3.4 IRTF AAAArch

A number of different Internet Services require Authentication, Authorisation, Accounting and Audit Support. The IETF AAA WG [6] defines short term requirements for a protocol that will support such services for network access and MobileIPv4 only. The AAAARCH WG will work to define a next generation AAA architecture that incorporates a set of interconnected "generic" AAA servers and an application interface that allows Application Specific Modules access to AAA functions. The architecture's focus is to support AAA services that:

- Can inter-operate across organisational boundaries,
- are extensible yet common across a wide variety of Internet services,
- enables a concept of an AAA transaction spanning many stakeholders,
- provides application independent session management mechanisms,
- contains strong security mechanisms that be tuned to local policies and
- is a scalable to the size of the global Internet.

The AAAARCH group has made a proposal on how the relevant architecture elements are arranged, combined, where they are located, and how they will interact [64] (see Figure 22). The entities encompass a generic AAA Server, an Application Specific Module (ASM), a policy and data repository (PR, DR) and the service equipment and accounting. The AAA Server evaluates policies through the use of a Rule-based Engine (RBE), whereas the ASM interacts with the service equipment.

The RBE resides inside an AAA server. The AAA server receives service requests from the Service Equipment via an ASM or from other AAA servers. A request received by the AAA server is inspected and evaluated considering the policies stored in the PR. To evaluate policy conditions, it may be necessary to consult other AAA servers or the service equipment. This is done firstly by sending requests to other AAA servers and secondly via an ASM. ASMs are needed additionally to enforce policy actions. Therefore, ASMs configure the service equipment for the provisioning of a service and the accounting process. The AAA server also performs policy actions itself. It holds session and transaction states, records accounting data, and logs events. The event log can be used for verifying the systems behaviour or for a later auditing process. The protocols used in this architecture according to

Figure 22 include (1) as a generic AAA protocol, which is assumed to be standardised in the IETF based on the work done in the research group, (2) a particular Application Programming Interface (API) or the AAA protocol or subset thereof, (3) a protocol or API for accessing the PR and DR depending on the implementation (e.g. Light-weight Directory Access Protocol (LDAP), Open Database Connectivity (ODBC), etc.), (4) a protocol between a legacy AAA client and a protocol gateway, (5) a protocol or API between an ASM and the service equipment to which it is connected and (6) an application specific interface between service provisioning and accounting functionality.
The AAAARCH group work is based on the work of the AAA WG, the Policy Framework Working Group as well as security working groups. The AAAARCH WG attempts to co-ordinate closely with the AAA WG and reports in each IETF AAA WG meeting.
15 Appendix G: W-CDMA Interface

This section introduces the interface between the Access Stratum (AS) entities and the Non-Access Stratum (NAS) entities shown in the figures of sections 5.2 and 5.3.

The W-CDMA provides a set of services to upper layers, as described in the following flows:
**RG Broadcast Service**

![Diagram](https://via.placeholder.com/150)

**Figure 24: broadcast service**

**RRC Connection Establishment**

![Diagram](https://via.placeholder.com/150)

**Figure 25: RRC connection establishment**
**Signaling Data Transfer**

![Diagram of Signaling Data Transfer]

**Radio Bearer Establishment**

![Diagram of Radio Bearer Establishment]
User Data Transfer

Radio Bearer Release

Figure 28: User Data transfer

Figure 29: Radio bearer release