



---

## Solution for session continuity between heterogeneous networks including FWA access capability in a single operator scenario

---

Zere Ghebretensaé (editor), Wei Zhao (editor), Victor Souza  
Torshamnsgatan 23, SE 164 80, Stockholm, Sweden  
{zere.ghebretensae, wei.c.zhao, victor.souza}@ericsson.com

Dávid Jocha, János Farkas Ericsson, Hungary , {[david.jocha](mailto:david.jocha@ericsson.com), [janos.farkas](mailto:janos.farkas@ericsson.com)}@ericsson.com

Csaba Lukovszki, István Moldován, Yvette Kulik, Gábor Kovács  
Budapest University of Technology and Economics, H-1117 Budapest, Magyar tudósok körútja 2, Hungary {lukovszki, moldovan, kulik, [kovacsq](mailto:kovacsq@tmit.bme.hu)}@tmit.bme.hu

Iñigo Pinilla, Enrique Areizaga Sanchez FUNDACIÓN ROBOTIKER, Parque Teconologico, Ed 202, E-48170 ZAMUDIO – Bizkaia Spain {ipinilla, [enrique](mailto:enrique@robotiker.es)}@robotiker.es

Leonardo Ferracci [leonardo.ferracci@telecomitalia.it](mailto:leonardo.ferracci@telecomitalia.it) Telecom Italia

Identifier:	Deliverable DC1.7
Class:	Report
Version:	Public
Version Date:	21/12/2007
Distribution:	Public
Responsible Partner:	EAB, ROB, BUTE, TI
Filename:	DC1.7_Solution for Session Continuity in a single operator Scenario v1

## DOCUMENT INFORMATION

<i>Project ref. No.</i>	IST-6thFP-026442
<i>Project acronym</i>	MUSE
<i>Project full title</i>	Multi-Service Access Everywhere
<i>Security (distribution level)</i>	Public
<i>Contractual delivery date</i>	31th Dec 2007
<i>Actual delivery date</i>	21th Dec 2007
<i>Deliverable number</i>	DC1.7p
<i>Deliverable name</i>	DC1.7_Solution for Session Continuity between heterogeneous networks including FWA capable access in a single operator Scenario, public version
<i>Type</i>	Report
<i>Status &amp; version</i>	1
<i>Number of pages</i>	78
<i>WP / TF contributing</i>	WPC1
<i>WP / TF responsible</i>	EABS
<i>Main contributors</i>	EABS, ROB, BUTE, EABH, TI
<i>Editor(s)</i>	Zere Ghebretensaé, Wei Zhao
<i>EU Project Officer</i>	Pertti Jauhiainen
<i>Keywords</i>	Heterogeneous access networks, layer2 mobility, layer3 mobility, MIP, session continuity
<i>Abstract (for dissemination)</i>	This deliverable starts by presenting a reference network architecture for inter-working between, Ethernet based, SPC access network and a fixed wireless access network. It then describes two use cases, used to identify different user "mobility types", and solutions for supporting session continuity. A session at the application layer invariably puts a number of requirements to the underlying layers. Therefore the requirements on the application, transport, network and link layers are analyzed and some results from experimental tests

---

	<p>on the impact of different link layer interfaces and applications running on different Operation Systems (OS) are presented. The policy framework specified in previous deliverables is revised and policy control workflow has been illustrated based on different mobility mechanisms. The Authentication and Authorization (AA) scheme that is being used in the SPC platform to support nomadism is also revisited and some innovative methods for minimizing the overall Handover (HO) delay, by binding the AA procedure with the layer 2 connections provisioning, are presented. The document also presents a summary of the specification and deployment of a MIP based implementation to support session continuity.</p>
--	---

## DOCUMENT HISTORY

Version	Date	Comments and actions	Status
1	21.12.2007	Public version of DC1.7	final

## TABLE OF CONTENTS

DOCUMENT INFORMATION .....	2
DOCUMENT HISTORY .....	4
TABLE OF CONTENTS.....	4
LIST OF FIGURES AND TABLES .....	6
ABBREVIATIONS.....	6
REFERENCES .....	9
EXECUTIVE SUMMARY.....	11
<b>1 WHAT IS NEW .....</b>	<b>13</b>
<b>2 INTRODUCTION .....</b>	<b>14</b>
<b>3 NETWORK ARCHITECTURE.....</b>	<b>17</b>
3.1 SPC Platform Overview .....	18
3.1.1 Network Model.....	18
3.1.2 Access Edge Node .....	19
3.1.3 Resource Manager .....	20
3.1.4 Access Node.....	21
3.1.5 Service Manager.....	21
3.1.6 Service Bindings.....	22
3.1.7 Authentication and Authorization in the SPC platform .....	23
3.2 Mobile WiMAX Network Overview .....	25
3.2.1 WiMAX Connections and Service Flows .....	27
3.2.2 Authentication and Authorization.....	29
<b>4 USE CASES .....</b>	<b>31</b>
4.1 Session continuity use-cases .....	31
4.1.1 Use case 1: WLAN hopping session continuity.....	31
4.1.2 Use case 2: Heterogeneous network session continuity.....	32
4.2 Use case analysis.....	33
<b>5 SESSION CONTINUITY .....</b>	<b>36</b>
5.1 Transport and applications layers related issues to Session continuity .....	37
5.1.1 Transport and Application layers Restoration time Consideration .....	38
5.2 Network layer related issues for Session continuity .....	39
5.3 Link layer related issues to Session continuity .....	39
5.3.1 MAC learning issues.....	40
5.4 Lab Experiment Results .....	41
5.4.1 Layer 2 handover scenarios .....	41
5.4.2 Handover timeout related lab test analysis .....	42
5.4.3 Traffic Behavior in a multi-homed Computer.....	44
5.5 Conclusion .....	45

---

<b>6</b>	<b>SOLUTIONS FOR SESSION CONTINUITY IN THE SPC AND WIMAX NETWORKS</b>	<b>47</b>
6.1	Layer 2 Mobility	47
6.1.1	WLAN-WLAN	47
6.1.2	Mobility between Fixed and WLAN networks	50
6.2	Layer 3 mobility	51
6.2.1	Layer 3 mobility with MIP	52
6.2.2	Proxy MIP for SPC	53
6.3	Conclusion	53
<b>7</b>	<b>POLICY CONTROL AND QOS</b>	<b>54</b>
7.1	Policy Control Framework for session continuity support	54
7.1.1	Policy control work flow	55
7.1.2	Network-based session continuity policies	56
7.1.3	End-User-based session continuity policies	58
7.1.4	A Use Case Analysis	59
7.1.5	Conclusion	60
7.2	QoS Provisioning	60
7.2.1	QoS mechanisms in different access networks	60
7.2.2	Conclusion	63
<b>8</b>	<b>AUTHENTICATION AND AUTHORIZATION</b>	<b>65</b>
8.1	Authentication and mobility management	65
8.1.1	Service binding information within authentication messages	66
8.1.2	Key management for Handovers	67
8.2	L2 Micro-mobility and Authentication	69
8.2.1	802.1x pre-authentication	69
8.2.2	Pre-authentication and Service Binding	71
8.3	L3 Mobility and Authentication	71
8.3.1	Media independent Pre-Authentication (MPA)	72
8.4	Conclusion	74
<b>9</b>	<b>MIP IMPLEMENTATION</b>	<b>74</b>
9.1	MIP for Windows	74
9.2	MIP for Linux	75
9.3	MIPv6 over IPv4	75
9.4	Dual Stack MIPv6	76
9.5	MIP Deployment	77
<b>10</b>	<b>CONCLUDING REMARKS</b>	<b>78</b>

## LIST OF FIGURES AND TABLES

Figure 3-1 Reference Network architecture .....	17
Figure 4-1 Use-cases: WLAN hopping.....	31
Figure 4-2 Use-cases: Attachment point type change .....	32
Figure 4-3 Mobility scenarios .....	33
Figure 5-1 - Network layer approaches for session continuity .....	39
Figure 5-2 Service binding update .....	40
Figure 6-1 Mobility within the same SSID .....	48
Figure 6-2 Mobility between different SSID WLANs.....	49
Figure 6-3 Mobility between fixed and WLAN .....	50
Figure 6-4 - Mobile IPv6 architecture .....	52
Figure 7-1 Policy control architecture in terms of DC1.7 network reference model .....	54
Figure 7-2 UMTS QoS Architecture .....	62
Figure 8-1. Service binding update due to authentication.....	65
Figure 8-2. Authentication Messages containing service binding information.....	67
Figure 8-3. EAP Re-authentication message exchange .....	68
Figure 8-4. 802.1X pre-authentication principle .....	69
Figure 8-5. Pre-authentication principle for extended APs due to the separation proposed by CAPWAP.....	70
Table 4-1: Attachment point change possibilities .....	35
Table 5-1: Comparison of different applications regarding timeout.....	43
Table 5-2: Combinations of wired and wireless technologies and the chosen default gateway adapter .....	45
Table 7-1 Use Case Analysis for Policy Control.....	60
Table 8-1. Service binding information mapping into authentication messages .....	66

## ABBREVIATIONS

AA	Authentication and Authorization
AEN	Access Edge Node
AN	Access Node
AP	Access Point
ARP	Address Resolution Protocol
ASN	Access Service Network
ASN-GW	ASN-Gateway
ASP	Access Service Provider
BE	Best Effort
BS	Base Station
CAPWAP	Control And Provisioning of Wireless Access Points
CARD	Candidate Access Router Discovery
CBS	Committed Burst Size
CID	Connection Identifier
CIR	Committed Information Rate
CN	Correspondent Node
CoA	Care-of Address

---

CP	Connectivity Provider
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSN	Connectivity Services Network
CTN	Candidate Target Network
CTP	Context Transfer Protocol
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DS	Directory Service
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
EBS	Excess Burst Size
EDCF	Enhanced DCF
EIS	Excess Information Rate
EMSK	Extended Master Session Key
EN	Edge Node
FA	Foreign Agent
FHR	Frequent Handover Region
HA	Home Agent
HCF	Hybrid Coordination Function
HLR	Home Location Register
HO	HandOver
HoA	Home Address
HOKEY	Handover Keying
HSS	Home Subscriber Server
ID-P	Identity Provider
IEFT	Internet Engineering Task Force
IPTV	Internet Protocol Television
IRTF	Internet Research Task Force
LAN	Local Area Network
LMA	Local Mobility Agent
MAC	Medium Access Control
MAG	Mobile Access Gateway
MIP	Mobile IP
MIPv4	Mobile IP version 4
MIPv6	Mobile IP version 6
MMP	Mobility Management Protocol
MN	Mobile Node
MobOpts	Mobility Optimization
MS	Mobile Station
MPA	Media-independent Pre-Authentication
NAI	Network Access Identifier
NAP	Network Access Provider
NAS	Network Access Server
NFC	Near Field Communication
NPM	Network Policy Manager
nrtPS	Non-real-time Polling Service
NSP	Network Service Provider

---

OS	Operating System
OSS	Operation Support System
PANA	Protocol for carrying Authentication for Network Access
PCF	Point Coordination Function
PEP	Policy Enforcement Point
PKM	Privacy and Key Management
PHT	Proactive Handover Tunnel
PMIP	Proxy MIP
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RGW	Residential Gateway
RRA	Radio Resource Agent
RRC	Radio Resource Controller
rRK	Re-authentication Root Key
RRM	Radio Resource Management
RM	Resource Manager
rtPS	Real-time Polling Service
SA	Security Association
SCN	Service Class Name
SFID	Service Flow Identifier
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLS	Service Level Specification
SM	Service Manager
SSID	Service Set Identifier
TC	Traffic Categories
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VoD	Video on Demand
VoIP	Voice over IP
VLAN	Virtual Local Area Network
VNO	Virtual Network Operator
VPN	Virtual Private Network
WG	Working Group
WiFi	Wireless Fidelity
WiMax	Worldwide interoperability for Microwave Access
WLAN	Wireless Local Area Network
UGS	Unsolicited Grant Service
UPM	User Policy Manager

## REFERENCES

- [1] Technical Annex MUSE Phase II
- [2] DC1.5 "Network Solution to Support Nomadism in a fixed access network and dual packager roaming in a multi operator scenario", MUSE Phase II, deliverable, June 2007.
- [3] DC1.6 "Solution to Support Nomadism and roaming in between fixed and wireless networks in a multi operator scenario", MUSE Phase II, deliverable, June 2007.
- [4] DTF1.8 "FMC in Fixed Access Architecture", MUSE Phase II, deliverable, June 2007.
- [5] [http://www.airspan.com/pdfs/WP\\_Mobile\\_WiMAX\\_Security.pdf](http://www.airspan.com/pdfs/WP_Mobile_WiMAX_Security.pdf)
- [6] Tanenbaum, A. S., "Computer Networks", Fourth Edition, Prentice Hall, ISBN 0-13-066102-3.
- [7] <http://www.microsoft.com/technet/community/columns/cableguy/cg0405.msp>
- [8] P. Arvidsson and M. Widell, "Design of a session layer based system for endpoint mobility". Master's thesis, KTH, 2006.
- [9] Y. Ismailov, J. Holler, S. Herborn, A. Seneviratne, "Internet Mobility: An Approach to Mobile End-System Design", International Conference on Mobile Communications and Learning Technologies, ISBN 0-7695-2552-0, IEEE Computer Society, Los Alamitos, CA, USA, 2006.
- [10] Microsoft: "Performance Enhancements in the Next Generation TCP/IP Stack", <http://www.microsoft.com/technet/community/columns/cableguy/cg1105.msp>, 2005
- [11] Microsoft: "Windows TCP/IP Registry Entries", <http://support.microsoft.com/kb/158474>, 2007
- [12] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang and V. Paxson: "Stream Control Transmission Protocol", Request for Comments: 2960, 2000
- [13] L. Ong and J. Yoakum: "An Introduction to the Stream Control Transmission Protocol (SCTP)", Request for Comments: 3286, 2002
- [14] Perkins, Ed. C., IP Mobility Support for IPv4, RFC 3344, August 2002.
- [15] S. Gundevelli, K. Leung, V. Devarapalli, K. Chowhury and B. Patil: "Proxy Mobile IPv6", Internet Draft 2007
- [16] MUSE D T1.8 – "FMC Support in Fixed Access Architecture", MUSE Phase II, deliverable, June 2007
- [17] Stefan Mangold, et al, "IEEE 802.11e Wireless LAN for Quality of Service"
- [18] T. Clancy et al, "EAP Re-authentication Extensions", draft-ietf-hokey-erx-02, work in progress, July 2007
- [19] "IEEE Std 802.11i™-2004 (Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003))"
- [20] S. Pack and Y. Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public WirelessLAN," IEEE Networks 2002, August
- [21] S. Pack and Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model," IFIP TC6 Personal Wireless Communications 2002 , October 2002.
- [22] M. Liebsch et al, "Candidate Access Router Discovery" RFC 4066, July 2005

- [23] A.Dutta, et al "A Framework of Media-Independent Pre-Authentication (MPA) for Inter-domain Handover Optimization", draft-ohba-mobopts-mpa-framework-05, work in progress, July 2007
- [24] A.Dutta, et al "Media-Independent Pre-Authentication (MPA) Implementation Results", draft-ohba-mobopts-mpa-implementation-04, work in progress, July 2007.
- [25] Microsoft FAQ pages, <http://www.microsoft.com/technet/network/ipv6/ipv6faq.msp>, last accessed on 21st of August 2007.
- [26] USAGI project home page, <http://www.linux-ipv6.org/>, last accessed on 21<sup>st</sup> of August 2007.
- [27] "Connection of IPv6 Domains via IPv4 Clouds", RFC3056, Internet Draft.
- [28] "IPv4 over 6to4 and 6to4 mobility", draft-engelstad-ngtrans-6to4-v4v6-mobility-00.txt, Internet Draft.
- [29] "Dual Stack MIPv6 (DSMIPv6)", <http://www.ietf.org/internet-drafts/draft-ietf-mip6-nemo-v4traversal-04.txt>, IETF Draft.

## EXECUTIVE SUMMARY

In MUSE phase II, the objective of Work Package C1 (WPC1) of Sub-Project C (SPC) was to develop solutions for fixed mobile convergence on a fixed access network platform in line with the overall FMC access architecture defined by Task Force 1.8 (TF1.8). WPC1 accomplished this in three subsequent deliverables. In the first deliverable, DC1.5, a network architecture solution for supporting nomadic users in a dual packager multi provider scenario, using Ethernet, xDSL or Fibre first mile technology was presented. This was achieved by enhancing the Resource Management, Policy Control and Authentication and Authorization (AA) mechanism of the SPC network architecture. Next, in deliverable DC1.6, the solution of DC1.5 was enhanced to support nomadic users using wireless access technologies, such as public WLAN access points or “hotspots”, privately owned public WLAN access points and fixed WiMAX access networks. In this last deliverable, DC1.7, we address the issue of session continuity, for intra SPC network mobility and for mobility between the SPC and the WiMAX networks.

For this purpose, the document presents a heterogeneous reference network architecture consisting of fixed SPC access network and mobile WiMAX networks run by a single operator. Support of session continuity requires that the Handover (HO) delay of sessions be minimized in order to avoid sessions being timed out as users move between different attachment points. As the HO delay is closely related to the delays of connection provisioning and user Authentication and Authorization (AA) delays in the new attachment point, a brief description of the layer 2 connectivity provisioning and the AA solutions of the SPC platform and mobile WiMAX is also presented.

The document also presents two use cases to help elaborate the different types of user mobility. From the user cases, a number of atomic “mobility types” were identified and solution for supporting session continuity for these “mobility types” are presented.

Whenever a session is started by the application layer, it invariably puts a number of requirements that needs to be met by the underlying layers. The impact of the session continuity requirement for the application, transport, network and the link layers is analyzed in detail. To complement the analysis, some simple experimental tests were conducted, where we looked at the impact of different link layer interfaces and applications, running on different Operation Systems, to session continuity.

The policy framework specified in previous deliverables is also revised to reflect network scenarios described in this deliverable. Policy control workflow has been illustrated based on different mobility mechanisms, a policy set example is presented for session continuity support. A use case analysis is also made to illustrate better how policies are involved in supporting session continuity. QoS mechanisms and methods of different access networks including Ethernet LAN, WLAN, WiMAX, etc, are summarized and a QoS requirement for session continuity support is listed based on that.

The Authentication and Authorization (AA) scheme that is being used in the SPC platform to support nomadism is also revisited and some innovative methods for minimizing the overall HO delay, by binding the AA procedure with the layer 2 connections provisioning, is presented. In addition, the document also identifies new solutions for pre-authentication and session key management which are currently under development in different IETF WGs and explains to what extent these solutions could be applied in the platform.

Finally, we present a summary of the specification and deployment of a MIP based implementation to support session continuity. Dual Stack MIPv6 is selected because the DSMIPv6 package could perform the initial tests previously described in a standard IPv4 network.

The session continuity solution designed by WPC1 will be evaluated in a lab trial in WPC4.

## 1 WHAT IS NEW

This deliverable, which is a continuation of DC1.5 and DC1.6, presents network solution for supporting session continuity in heterogeneous networks. For this objective it presents an adaptation of the use cases, discussed in DC1.6 and TF1.8, to incorporate session continuity between the different types of networks. From the use cases, a number of atomic “mobility types” were identified and solutions for supporting session continuity for these “mobility types” are presented.

Innovative work in this deliverable includes:

- The impact of the session continuity requirement for the application, transport layer, network and the link layer is analyzed in detail. The analysis is complemented by a number of experimental tests where we looked at the impact of different link layer interfaces and applications, running on different Operation Systems, to session continuity.
- The integration of a WiMAX Access Service Network into the MUSE SPC platform is explored. This integration would bring a faster deployment of WiMAX in the access together with a faster handover between fixed and mobile networks including session continuity.
- An example of a policy set for session continuity support is presented both from network and end users' perspective. Its application is illustrated by a use case analysis and an activity pattern based policy control for mobility management is proposed.
- An innovative solution for binding the authentication and authorization procedure with the service binding creation or update is presented. The procedure and the parameters that are introduced in the authentication messages are described so that the service bindings can be created or updated.
- New solutions for pre-authentication and session key management are identified, which are currently under development in different IETF WGs and explains to what extent these solutions could be applied in the platform.

Session continuity can be addressed and supported from different layers, e.g., from IP in combination with application layer. Investigation done in this report is not meant to be exhaustive or complete and is limited only to the IP layer. Please refer to the session continuity section of [4] for a more exhaustive and generic state-of-the-art information.

## 2 INTRODUCTION

Broadband access is now a reality in many parts of the world and the launching of triple play services, i.e., video, telephony and high speed Internet access services is undergoing in many countries. Triple play services will bring many benefits to the end users. E.g., not only will end users be able to enjoy their high quality movies at any time of the day, but also replace their expensive, fixed telephony, subscription with cheaper VoIP telephony service. In fact in most of the major cities, the competitive market between telecom, cable TV and green field operators has already led to restructuring of the triple play business models forcing the operators to package bundles of their triple-play services with discounts and promotions which has led to significant price declines.

However, despite the clear improvement compared to today's single service offering, the subscription of the triple play services is still tied to a particular service attachment point; usually the end user's residence. This means users can only access these services from their residence. The next step is, therefore, to un-tie the subscription from the residence of the user and increase the level of service availability, by introducing a feature called nomadism. Nomadism is a form of discrete mobility and once the triple play services are enhanced with nomadic features, end users will be able to access these services not only from the comfort zone of their homes, but also when they are away from home, e.g., when visiting friends' houses, hotels and other public places such as public "hotspots" and Internet cafes. Nomadic users are also expected to benefit from increased deployment of "privately owned public WLAN access points", which are becoming increasingly popular as the residential users migrate to WLAN based customer premises networks (CPNs). In this case private WLAN network owners, who are willing to share their WLAN resources with public users, enter into business agreement with service providers and provide access to the customers' of the service providers. To this end, the private WLAN is partitioned into separate logical networks to support private local users and public visitors. The potential of this business model lies in the sheer number of privately owned public WLAN access points, which can be used to extend the Points of Presence (POPs) of the service providers, resulting in huge investment cost savings, while increasing the service availability for nomadic users.

From the end users' perspective, access to their services from some discrete points through nomadism should be viewed only as a short term solution. In the long term, end users will not accept session interruption every time they want to move to new location. Instead, end users will expect to access their services even when they are on the move. In other words, the network should support session continuity. Unlike nomadism, session continuity places very stringent requirements on the network in terms of handover delay when an ongoing session needs to be transferred from one attachment point to another. Support of session continuity is further complicated by the fact that sessions may need to be transferred not only between attachment points within the same type of network but also between different types of access networks, which may have different support of QoS, etc. For the service providers, the increased level of service availability due to support of session continuity will help generate higher revenues and reduce churn.

The objective of Work Package C1 (WPC1) of Sub Project C (SPC) as stated in the technical annex [1] is: "...to develop a solution for nomadism and session continuity that will be added to the triple play enabled platform developed in phase I...". This deliverable, DC1.7, is the last in a sequel of three WPC1 deliverables. In the first deliverable, DC1.5 [2], we provided a network solution that supports nomadic users, in a dual packager multi provider scenario, using Ethernet, xDSL or Fibre first mile technology. This was achieved by enhancing the Resource Management, Policy Control and Authentication and Authorization (AA) mechanism of the SPC architecture. Next, in deliverable DC1.6 [3], we continued the work and extended the solution to include nomadic users connecting from public WLAN access points or "hotspots", privately owned public WLAN access points and fixed WiMAX based access networks. In this last deliverable, DC1.7, we address the issue of session continuity in heterogeneous networks run by a single operator. The work is based on the general FMC architecture jointly defined by all MUSE partners in TF1.8 [4].

The outline of this document is as follows. It starts with an executive summary, which highlights the main content of the document, followed by "what is new" and a short introduction.

Chapter-3 details the reference architecture which helps us to put the discussions of session continuity in the right context. Support of session continuity, requires that the Handover (HO) delay of session be minimized, to avoid sessions being timed out as users move between different attachment points. As the HO delay is related to the delays of connection provisioning and user Authentication and Authorization (AA) in the new attachment point a, brief description of the layer 2 connectivity provisioning and the AA solutions of the SPC platform and mobile WiMAX is also presented in this chapter.

Chapter-4 describes a couple of use cases that help us elaborate the different types of user mobility. From the user cases, a number of atomic "mobility types" were identified.

In Chapter-5 we address the impact of session continuity for the application, transport network and link layers. To complement the analysis, some simple experimental tests were conducted, where we looked at the impact of different link layer interfaces and applications, running on different Operation Systems (OS), to session continuity.

In Chapter-6 we present the solutions for supporting session continuity to the different "mobility types" identified in chapter-4.

In Chapter-7 the policy framework specified in previous deliverables is revised to reflect network scenarios described in this deliverable. Policy control workflow has been illustrated based on different mobility mechanisms, and example policy set is presented for session continuity support. QoS mechanisms and methods of different access networks including Ethernet LAN, WLAN, WiMAX, etc, are summarized and QoS requirement for session continuity support is listed based on that.

In Chapter-8, the Authentication and Authorization (AA) scheme that is being used in the SPC platform to support nomadism is also revisited and some innovative methods for minimizing the overall HO delay, by binding the AA procedure with the layer 2 connections provisioning, is presented. In addition the document also identifies new solutions for pre-authentication and session key management which are currently under development in different IETF WGs and explains to what extent these solutions could be applied in the platform.

Chapter-9 presents a summary of the specification and implementation of MIP based deployment that can support session continuity.

### 3 NETWORK ARCHITECTURE

The network architecture considered in this deliverable consists of a heterogeneous network which includes fixed and mobile access networks. It is in line with the overall FMC access architecture defined in DTF1.8 [4]. As the scope of this work is limited to session continuity in a single operator domain, there is no need for roaming agreement in order to support mobility within or between the different networks. Session continuity in case of roaming was not considered because it is an additional level of complexity. Note that also today's GSM networks generally do not support session continuity when crossing provider domains. However, all the technical details that are required to maintain and transfer an ongoing session must be worked out. To begin with the user devices must have multiple types of interface cards to be able to communicate with the different types of networks. Before a user is allowed to connect to the fixed or the Mobile access networks she has to be authenticated and authorized to connect and access her subscribed services.

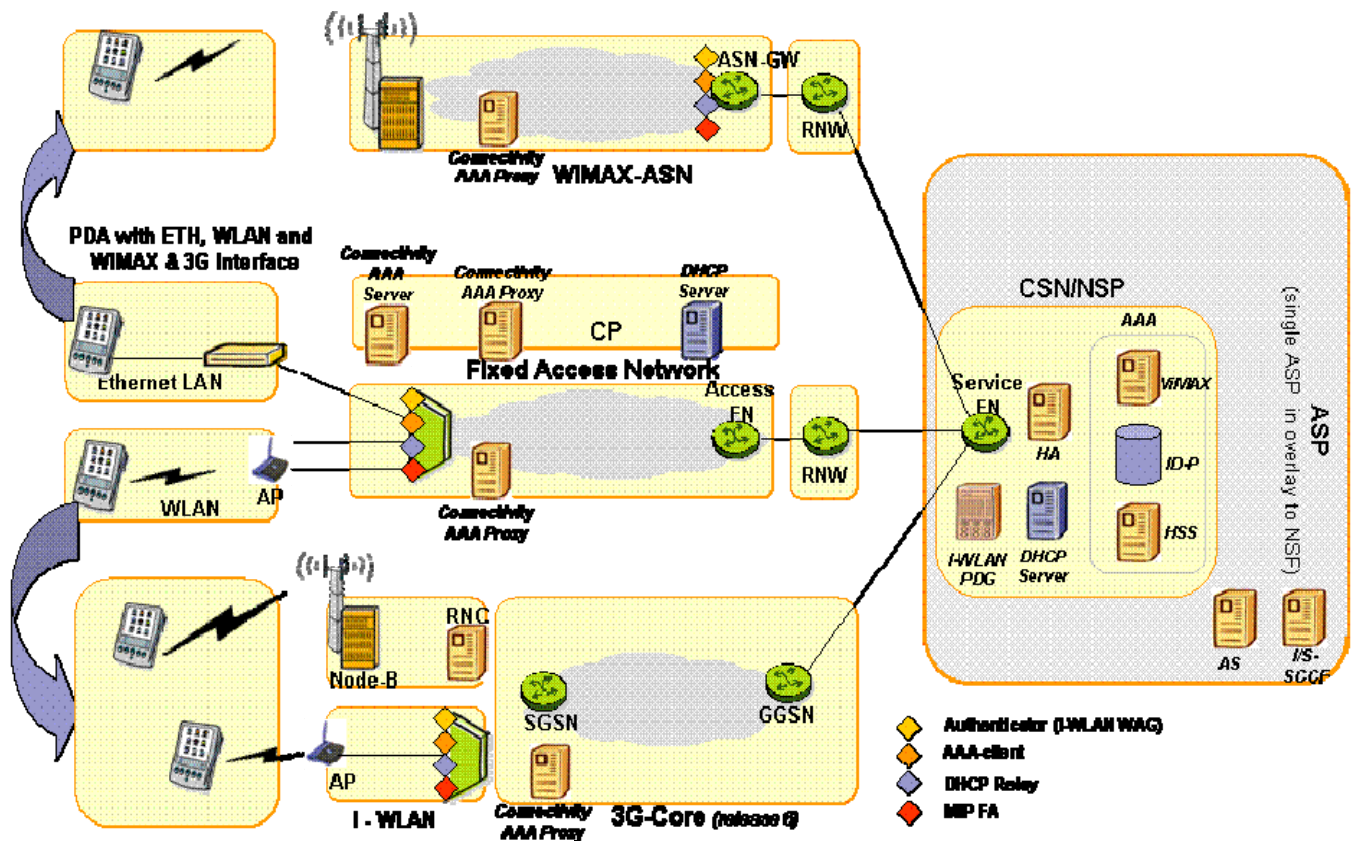


Figure 3-1 Reference Network architecture

As a result of the authorization process, a layer-2 connection is provisioned between the user device and the Edge Node (EN) in the access network. And when the user moves to a - different attachment point new layer-2 connectivity has to be re-provisioned after the user has been re-authenticated and authorized. Therefore the provisioning, authentication and authorization architecture must be designed to support the required horizontal and vertical

HandOver (HO) processes under the prescribed HO delay. In this deliverable, as the user mobility is constrained within the same provider domain, the HO delay can be minimized by using pre-authentication, described in Chapter-8, or by transferring user and session related information, such as session keys, user policy, QoS, etc to the new attachment point.

The reference architecture used in this deliverable is depicted in [Figure 3.1](#). It shows a fixed network, which in this case is the MUSE SPC type of access network, and a mobile network, which could either be a mobile WiMAX or 3GPP network. In this model, end users will be able to access their services from different networks, and are not tied to a fixed only or mobile only type of subscription as is the case in today's subscription offers. In DC1.7 we have provided a solution for the inter-working and integration of the SPC access solution and WiMAX network.

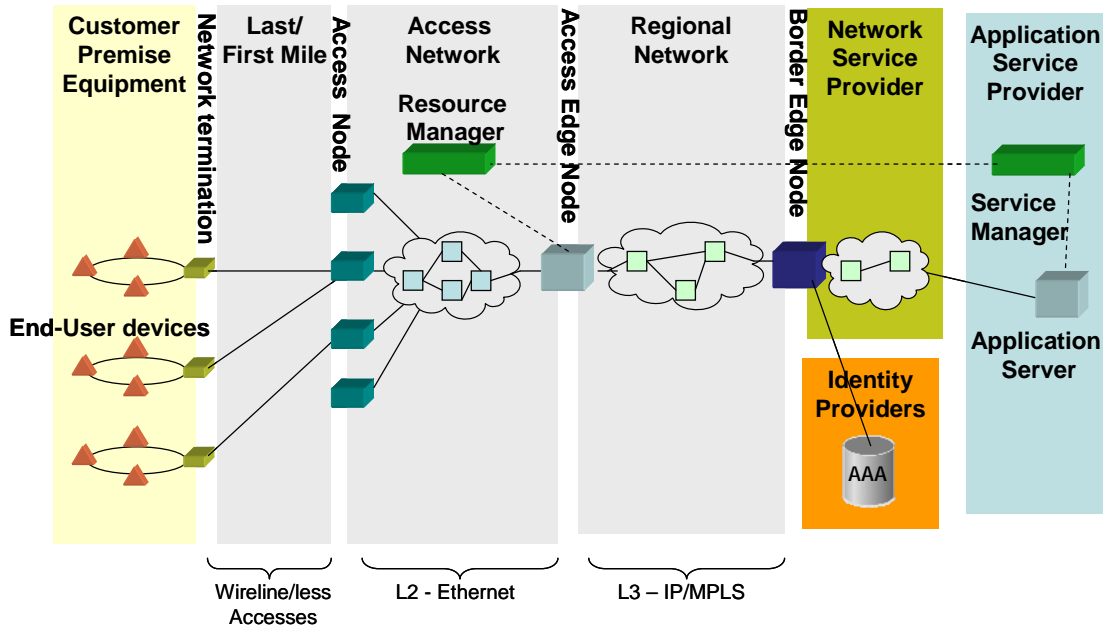
WiMAX was selected for the implementation of a session continuity solution instead of 3GPP, because the interworking with 3GPP is far more complex. TF1.8 has defined the interworking architecture, but only at a later stage of MUSE and hence too late for a detailed study in WPC1. Session continuity between a fixed access network and 3GPP is a topic that deserves more attention in future research during FP7.

### 3.1 SPC Platform Overview

The SPC platform is aimed at providing a multi-access, multi edge, multi service platform for public broadband access. The network architecture is Ethernet based, although different technologies are supported for end user access, e.g., FTTx and xDSL.

#### 3.1.1 Network Model

The network reference model of the architecture creates basically three different regions that can be possibly managed by distinct business entities. The first region is the last mile network, where a wired or wireless technology can be employed. The second one is the access network, where all the traffic coming from the customers' premises is aggregated. The third one is the regional network, the first layer-3 network in the system. The model is depicted in Figure 3-2. The key concepts of the architecture is the support for equal access, which means that subscribers have the ability to select the network service provider or the application service provider independently of the access type or access domain to which they are connected. This allows network and application service provider to broaden their offers to new areas, reaching subscribers independently of the access domain they are connected to.



**Figure 3-2 Network Reference Model**

The services delivered through the platform can have guaranteed QoS in needed cases. This is done through the negotiation of connection parameters with the Resource Manager, performed at service subscription and/or execution time. In case the resources are not available for a given customer and traffic class, he may be offered other options spanning from access with reduced quality to denial of access to the service depending on the domain policies and traffic load of the network. For example, if the traffic is best effort it can be accommodated with no bandwidth guarantees, despite of the current usage of the link. In this respect the resource manager performs functionalities of admission control of new subscriptions. Traffic separation is performed via the use of different VLANs. In order to simplify the authentication of end-user in nomadic scenarios in an access domain and across access domains boundaries a framework was developed. This framework is strongly founded in the Identity Provider (IDP) functionalities. Service subscriptions, along with identity, are stored there for future use when the end-user is not located at his home network.

### 3.1.2 Access Edge Node

The Access Edge Node (AEN) is a core component of the architecture, performing the mapping between the layer-2 access network and the layer-3 regional network. Policies that are to be enforced by the Resource Manager (RM) can be pushed down to the Access Edge Node which acts as a Policy Enforcement Point (PEP). Functionalities such as traffic shaping and monitoring can also be performed in this point of the network.

The AEN is also responsible for enabling the equal access concept. This is possible due to the creation of service bindings, which can be created by any service provider requesting

resources in the network. The role of the AEN is to manage and control the service bindings by forwarding the L2 frames from the customer premises equipments to a specific service provider using the L3 aggregation network. In this sense, the AEN can be seen as a bridge between the L2 and L3 environments.

Several other functionalities are embedded in the AEN for its strategic position, i.e., the termination of the end-users' layer-2 connection. For example, the access service provider can, on behalf of the Network Service provider (NSP), assign IP addresses to the end-users. This functionality is then carried by the AEN - a DHCP server (and proxy) is present there. Other functionalities performed by the AEN include HTTP-proxy, multicast group management and authentication.

It is very important to emphasize that different Network Service Providers can have virtually their own router installed in the AEN. This is the concept of a Virtual Network Operator (VNO). The VNO can be configured to filter traffic, for example.

### 3.1.3 Resource Manager

The Resource Manager is the element of the architecture in charge of controlling resources in the first mile and in the access network. It comprises facilities for admission control, resource reservation, monitoring, configuration and policy-based control. The logical organization of the RM is shown in Figure 3-3.

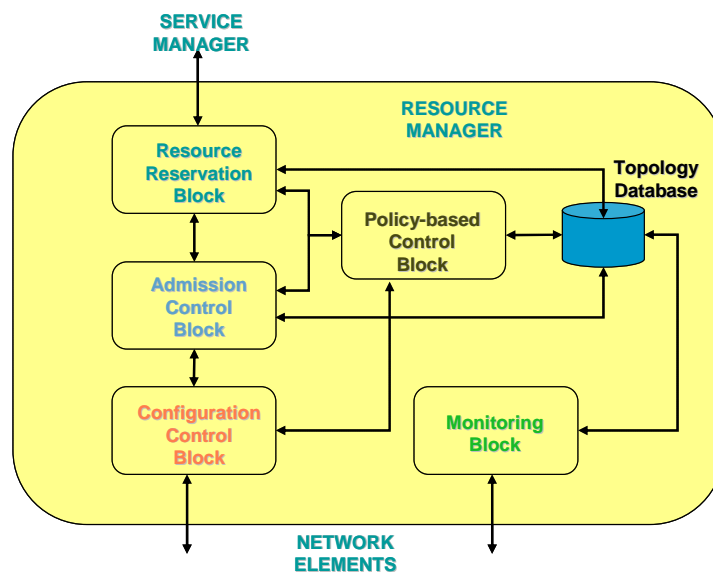


Figure 3-3 Resource Manager Block Diagram

Essentially, the Resource Manager (RM) receives requests for resources from the Service Manager residing in the service provider's domain. By evaluating the current state of resource usage and application of domain specific policies, the RM is capable of deciding upon each request. In order to take decision the RM possesses an internal database that corresponds to the full topology of the access network, including the access nodes, L2 aggregation network and access edge nodes. Moreover, it keeps track of the used resources in this topology map in a static approach to resource management.

Alternatively, the RM can poll the network elements to retrieve the actual available resources, in a more dynamic fashion. This model is used in the monitoring of first mile copper lines by contacting the Loop Qualification & Monitoring (LQ&M) software which in turn monitors DSL lines. After a decision has been taken, the configuration of network elements takes place. This happens by pushing down policies and access control lists into the network elements, for example.

### 3.1.4 Access Node

The Access Node is the element where individual physical connections to the user domain are attached and maintained. It provides a bridge between the Ethernet switching domain of the access network and the end-user's network domain. Therefore, the Access Node acts as a gateway between the physical technology used by the user devices to connect to the Access Node on the first mile (Wi-Fi, xDSL, fiber, WiMAX) and the Ethernet technology used by the aggregation network. It is the first point in the access network where traffic coming from multiple user ports is aggregated towards the access edge node. The Access Node has the role to forward and regulate traffic to/from the user ports and to/from the Access Edge Node through the layer-2 Ethernet aggregation network. It also has the responsibility to perform traffic marking (802.1P field) on the upstream of service bindings based on defined policy rules, and to perform traffic policing on the upstream of service bindings against defined policy rules.

### 3.1.5 Service Manager

The Service Manager (SM) is the component of the platform that resides in the Service Provider domain and is responsible for interacting with the system. Basically, the Service Manager has the role of receiving requests for service access from an application server and translating them into network parameters characterized in a Service Level Specification (SLS). The SM then sends the service definition (e.g., multicast group, resources required) and the authorization for that user to the Resource Manager. The Resource Manager checks whether enough resources are available to deliver the service in the specified period. If enough resources are available and the user is known to the access domain, the Resource Manager allows the service by sending the request to the Access Edge Node; otherwise the Resource Manager rejects the request and sends a negative response to the Service Manager.

The mapping between the end-user's request and the SLS sent to the Resource Manager needs to be configured in the Service Manager. This file must specify precisely the network resources that are required for optimal service delivering. For example, traffic priority and shaping parameters can be specified.

### 3.1.6 Service Bindings

A service binding is a network association that enforces the necessary transport relationship between a user network domain and a service provider domain to enable a user device to reach and access the services of a particular provider. Furthermore, the service binding guarantees the service delivery with the right integrity and QoS between a specific user and a specific provider. Service bindings are implemented by the use of Virtual LANs, providing a separate broadcast domain in the Ethernet-based access network. The VLAN separation ensures that the traffic between different users is kept independent, and users are not able to view or use resources in another user's network.

The creation and maintenance of a service binding is closely tied to the authentication of a user. A service binding can only be created after *authentication* and *authorization* processes take place. These processes are performed periodically. The authorization triggers the creation of a service binding for services that the client had previously subscribed to. Subscription to a new service triggers the creation of service binding too.

A service binding identifies a service subscription and a set of resources allocated by a combination of a VLAN in the user domain and a service agent in the access edge node. The set of parameters that uniquely identifies a service binding is:

- Service ID (e.g., 300)
- User VLAN (e.g., VLAN3)
- Username
  - *user@accessnet.com* when using port authentication
  - International Mobile Subscriber Identity when using SIM authentication
- Access domain (e.g., accessnet.com)
- Access node and port
  - Fixed info when using port authentication
  - Dynamic info when using SIM authentication
- User MAC address

The SIM card *authentication* is accomplished by a classical multi round trip exchange. Once the access node detects the presence of a user node, it initiates authentication by asking for the identity of the user. The access network will then perform identity verification with the identity provider.

The service subscriptions are maintained in the service provider and in the directory service. Once the identity is verified the access domain fetches the list of previously subscribed services from the directory service. At this point the access network asks each service provider to perform the *authorization*. Service providers will use the identity to verify the correctness of the user data and (possibly) translate the identity to an identity in a local scheme (e.g., userid). During the *authorization* process the service provider re-establishes the subscribed services by setting up or activating the needed service bindings in the access domain.

When it comes to mobility two types of service binding can be identified. Service bindings for SIM authenticated devices are always mobile while service bindings for port authenticated devices are fixed.

When it comes to the duration, service bindings can be created for a long-term use or a short-term use. Long-term service bindings are used for services featuring long subscription duration, for example VoIP, Internet and IPTV. The service bindings are *created* when the client subscribes to the service for the first time and then activated every time the user wants to access these services. After the user has finished using the service (e.g., made the VoIP call, surfed the Internet or watched the TV programs) the service binding is *de-activated* but not *terminated*.

Short-term service bindings are connection identifiers used for occasional, temporary subscriptions, for example video on demand. The service binding is then *created* and *activated* dynamically for the duration of the service. After the user is finished with the service (e.g., finished watching the video on demand movie) the service binding is *de-activated* and *terminated*.

### 3.1.7 Authentication and Authorization in the SPC platform

The Identity Provider (IDP) in the SPC solution is a special type of Service Provider who provides the service of authenticating user identities. Its role in the network is to provide the NSPs and the ASPs with a proof of the user's identity. IDPs do not need to have a specific SLA with the Access Domains. By introducing the IDP role in the network, the user is freed from being bound to any NSP and/or ASP but rather to a neutral entity. Therefore, changing the subscription status to any service provider (NSP or ASP) will not force an end-user to obtain a new identity.

#### 3.1.7.1 Authentication Method

EAP-SIM is assumed to be the basic mechanism used to obtain the authentication information from the user. EAP-SIM is flexible and it allows mutual authentication. Users can also authenticate themselves by the virtue of being physically attached to a physical port (port based authentication) but these users cannot utilize the nomadism related features of their services. Each user utilizes a SIM card to store his/her identity (the IMSI) and the shared secrets with the AAA server. This information (identity and shared secrets) needs to be known by the IDP-AAA server, which will verify the user identification and store public/private information required by the card and the IDP to perform mutual authentication. The basic piece of information shared between the IDP and the User is a set of one or more keys embedded in the SIM card and known to the IDP (shared secret). Because the card is not associated to (owned by) a Service Provider, the user can very easily change Service Provider (or NSP) and keep the same SIM card.

#### 3.1.7.2 Initial Connection (no services provisioned)

When the user first connects to the Access network, the Access Network will perform identity verification with the IDP and if successful, return a successful authentication to the user. At this point the user is directed to a self provisioning portal where he/she can pick the desired service providers and services. After the user picks the desired services the user identity is associated with the selected services.

### 3.1.7.3 Normal usage (services provisioned)

When the user first connects to the Access network, the Access Network will perform identity verification with the IDP. Once the identity is verified, the Access Network asks the associated Service Provider to perform the authentication (using the public identity). The Service Provider will use the identity to verify the correctness of the user and (possibly) translate the identity to an identity in a local scheme (e.g. userid). The Service Provider will then be able to provide the service to the user (e.g. setup service bindings, QOS, accounting, deliver services, etc.)

### 3.1.7.4 Authentication message sequence

The Authentication is accomplished by a classical multi round trip exchange. Once the Access Point detects the presence of a user node, it initiates authentication by asking for the identity of the user. Based on the identity of the user the RADIUS Access Request is created and sent to the IDP AAA Server based on the realm. This is usually the RADIUS server part of the RADIUS proxy present on the AEN. The AES RADIUS proxy forwards this to the IDP AAA server(s) and forwards the RADIUS Access Challenge back into the Access Network. The Access Challenge is converted into a EAP message at the Access Node and sent to the client using 802.1X. The client responds with another EAP message over 802.1X which is carried to the AAA server over RADIUS. It is possible that multiple such round trips can happen before the client is fully authenticated. At the end the AAA server sends either an Access Accept or an Access Reject to complete the authentication. If an Access Accept is received, the AN sends an EAP Success to the user and allows access to the system. If an Access Reject is received the AN denies access to the system. Please note that the CAAF is not bound to using RADIUS as the AAA protocol and can easily be modified to use other AAA protocols like DIAMETER, if required. After performing the authentication sequence as detailed in this section the AES performs the authorization sequence for the subscribed services as detailed in the next section.

Once authentication is completed the Access Edge Node queries the Directory Service to obtain the list of services to which the user is subscribed to. The interface between the AEN and the DS is based on Web Services. This process is performed once and only once after every successful full authentication as described in the previous section.

### 3.1.7.5 Service Identification

The DS returns the Get-Service-Response message with the list of subscribed services for the specified identity. A subscription defines the Service Provider providing the service, the service identifier, and the VLAN to which the service is mapped on the User Device. Using this subscription information, the AEN determines the Service Provider providing the service.

### 3.1.7.6 Service Authorization

After determining the Service Provider the AEN determines the address of the AAA server of the provider using configuration information. The AES then sends a RADIUS Access Request to the Service Provider AAA containing the User-Name attribute (obtained from authentication) and the Service-Type (obtained from the service subscription information). After the AAA verifies the correctness of the username and the service information it initiates

the verification and reservation of the necessary network resources through the Resource Manager via the Service Manager residing in its own administrative domain.

#### 3.1.7.7 Resource Request

The Service Manager receives the Set-Service-Request and determines the Resource Manager in charge of the Access Network based on the fully qualified domain name received in the Set-Service-Request. Once resolved, it generates a Reserve-Resource-Request message to the Resource Manager. The Resource Manager validates this request and if the validation process is successful, it performs resource and admission control on the requested service level specification. If adequate resources are available to grant the request, it then sends the Set-Policy-Request message the AEN to activate the service bindings with a specific set of policies.

#### 3.1.7.8 Resource Allocation

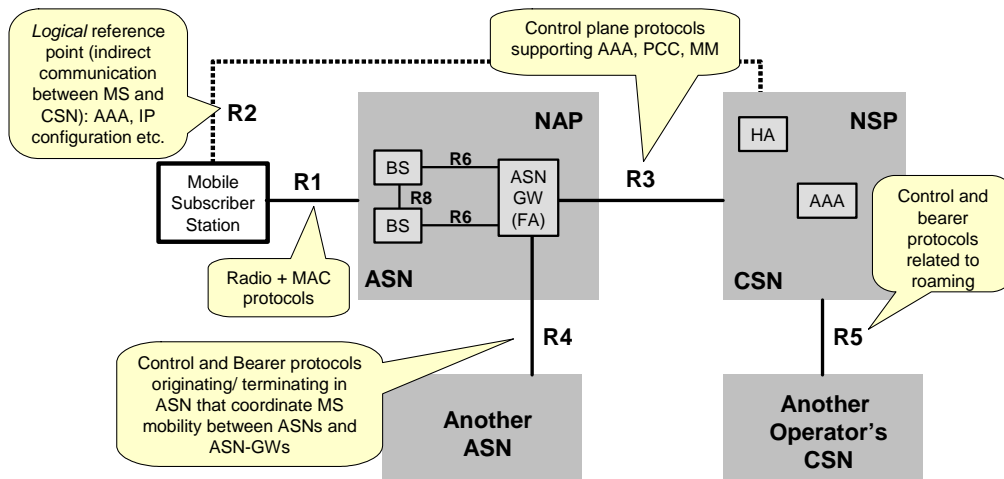
Once the AEN performs the actual resource reservation it responds to the Resource Manager with a Set-Policy-Response. The Resource Manager marks these resources as used and then responds to the Service Manager with a Reserve-Resource-Response. The Service Manager responds to the AAA to let it know whether the service activation process was successful. If it was successful the AAA responds with a Radius-Access-Accept message to the AEN. Otherwise it sends a Radius-Access-Reject.

#### 3.1.7.9 Service Duration

The service may be authorized either infinitely, until the user logs off, or for a specific time period. If limited time authorization is used, the specific time period is communicated to the AEN using a Session-Timeout attribute. When the user no longer wishes to use the subscribed services he/she can commence the de-authentication / de-authorization procedure by sending a EAPoL Logoff message to the AN. This initiates a sequence of events in the AEN and the SP domains which frees up all the resources allocated for the subscribed services and clears up the authentication state. This procedure is also initiated by the AN without any user intervention if the service was authorized only for a limited duration.

## 3.2 Mobile WiMAX Network Overview

In order to support end-to-end mobility, the WiMAX forum has defined an end-to-end Network Reference Model (NRM), consisting of the Access Service Networks (ASN) run by a Network Access Provider and Connectivity Service Networks (CSN) run by a Network Service Provider (NSP). As shown in Figure 3-4, the standard specifies the interfaces between the different network functional nodes and different networks. Within the ASN there are two key elements dealing with the mobility of the Mobile Subscriber Stations (MS), these are the Base Station (BS) and the ASN Gateway (ASN-GW). The BS is responsible for managing the radio resource over the air interface while the ASN-GW is responsible for control and aggregation of the traffic from one or more WiMAX base stations and managing handover between them, including authentication, service flows and key distribution between base stations.



**Figure 3- 4 WiMAX Network Reference Model**

The R6 interface between the BS and the ASN GW specifies an IP network or alternatively a pure layer 2 network, which means that it should be possible to manage all the connections between the different BSs associated with that particular ASN GW at link layer. Furthermore, the specification of the R4 interface, for communication between ASN-GWs in different ASNs will enable multi-provider WiMAX networks in line with the MUSE Access Network Architecture. The R3 Interface specifies the communication between the ASN and the CSN which is at the core of the network providing control and management functions such as AAA, HA and DHCP

Within the WiMAX specifications, different types of ASN Profiles have been specified as a tool to manage diversity in ASN node usage and implementation. The main 3 ASN profiles are:

- Profile A:
  - Centralized ASN Model with BS and ASN GW in separate platforms through R6 interface
  - Split RRM: RRA in BS and RRC in ASN-GW
  - Open interfaces for Profile A: R1, R6, R4, and R3
- Profile B:
  - Distributed ASN solution with the BS and ASN GW functionalities implemented in a single platform
  - Open interfaces Profile B: R4 and R3
- Profile C:
  - Similar to Profile A, except for RRM being non-split and located in BS.

Out of the three, Profile C, shown in Figure 3-5 fits best into the MUSE SPC network architecture due to the physical separation between the BS and the ASN-GW. Since the complete Radio Resource Management is in the Base Stations, the user connections are terminated in a similar way as the DSLAMs terminate the xDSL lines. The separation of the radio functionality and network management facilitates inter-vendor interoperability as it allows network operators to select a different vendor for each function and so avoid conflicts and duplications.

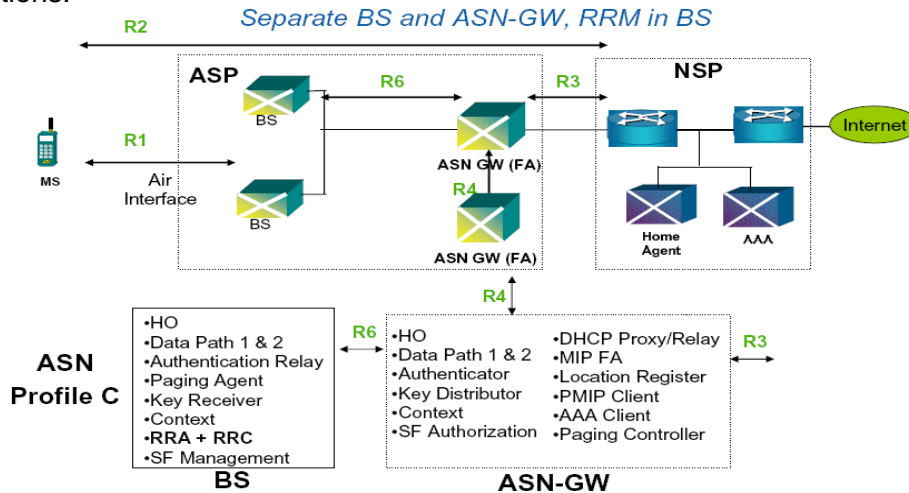


Figure 3-5 Access Service Network Profile “C”

In Figure 3-6 the R6 interface, between the BSs and the ASN-GW, is shown as pure layer 2 network. Furthermore, due to the Ethernet Convergence Sub-layer (Ethernet-CS), it is possible to have Ethernet connectivity between the Mobile Station and the ASN-Gateway.

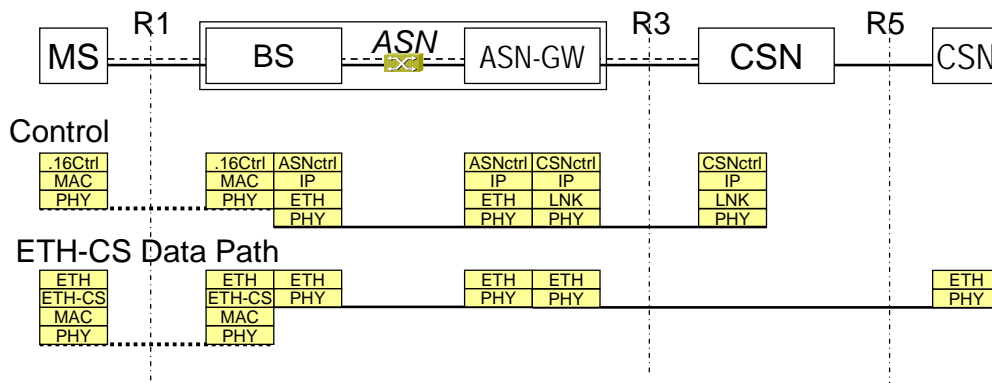


Figure 3-6 Protocol Stack for Ethernet-CS over 802.16e

### 3.2.1 WiMAX Connections and Service Flows

One of the key features of WiMAX is its connection oriented link layer connectivity between the BS and the Mobile Subscriber Station. Before any service related data can be communicated, the BS and MS first establish a unidirectional logical link between the peer MACs called a connection. The outbound MAC then associates packets traversing the MAC

interface into a service flow to be delivered over the connection. The QoS parameters associated with the service flow define the transmission ordering and scheduling on the air interface as shown in Figure 3.7. The service flow parameters can be dynamically managed through MAC messages to accommodate the dynamic service demand. The service flow based QoS mechanism applies to both Downlink (DL) and Uplink (UL) to provide improved QoS in both directions. Mobile WiMAX supports a wide range of data services whose detail can be found in chapter 8.

For every connection there is an identifier called Connection Identifier (CID) and for every CID there is a Service Flow Identifier (SFID) that determines the QoS parameters of that connection.

- Connection identifier (CID) – is a 16-bit value that identifies a transport connection or an UL/DL pair of associated management connections (i.e., belonging to the same Subscriber Station (SS)) to equivalent peers in the MAC of the Base Station (BS) and SS. The CID address space is common (i.e., shared) between UL and DL and can be specified how it is partitioned among the different types of connections. It maps to a Service Flow Identifier (SFID), which defines the QoS parameters of the service flow associated with that connection.
- Service Flow ID - is an SFID is assigned to each existing service flow. The relationship between SFID and transport CID, when present, is unique

The connections provided by WiMAX are transparent to the Ethernet, and they can also carry the 802.1Q VLAN tag.

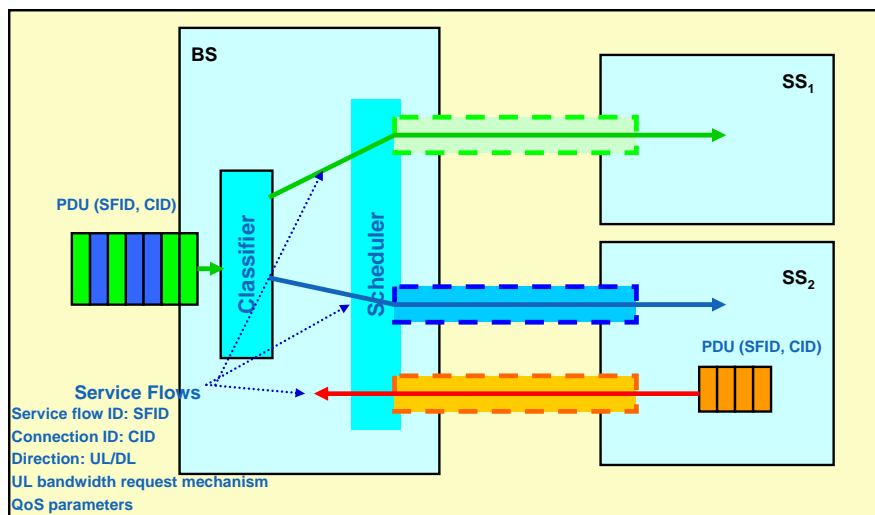


Figure 3-7 WiMAX QoS mechanism

The Service Flow Management (SFM) and Service Flow Authorization (SFA) are the logical functional entities, closely associated with QoS, located in the ASN that act as policy enforcement and policy decision points. For ASN Profile C, the SFM function is located in the BS and the SFA function is located at the ASN GW. The Service Flow Manager (SFM) located in the BS is responsible for the creation, admission, activation, modification, and deletion of IEEE 802.16e-2005 service flows. It consists of an Admission Control (AC) function, data path function and the associated local resource information. AC decides whether a new service flow can be admitted to the system. Service Flow Authorization (SFA) is located at the ASN GW and is responsible for evaluating any service request against the subscriber's QoS profile. If the SFA already has the user QoS profile then it evaluates the incoming service requests against the user's profile. If the SFA does not have the user profile then it sends the service request to the Policy Function (PF) for decision making. The Policy Functions (PFs) and its associated database reside in the CSN of both the home and the visited network.

### 3.2.2 Authentication and Authorization

In WiMAX 802.16e Authentication is achieved using a public key interchange protocol which ensures not only authentication but also the establishment of encryption keys [5]. In public key interchange schemes each participant must have a private key and a public key. The Public key is known widely whereas the private key is kept secret. WiMAX 802.16e-2005 standard defines a Privacy Key Management (PKM) protocol which allows for three types of authentication:

- RSA based authentication - X.509 digital certificates together with RSA encryption
- EAP based authentication (optional)
- RSA based authentication followed by EAP authentication

PKM authentication protocol establishes a shared secret key called Authorization Key (AK) between the MS and the BS. Once a shared AK is established between the BS and the MS, Key Encryption Key (KEK) is derived from it. The KEK is then used to encrypt subsequent PKM exchanges of Traffic Encryption Key (TEK).

In the RSA based authentication, a BS authenticates the MS by virtue of its unique X.509 digital certificate which has been issued by the MS manufacturer. The X.509 certificate contains the MS's Public Key (PK) and its MAC address. When requesting an AK, the MS sends its digital certificate to the BS which validates the certificate and then uses the verified PK to encrypt an AK which is then sent back to the MS. All MSs that use RSA authentication have factory installed private/public key pairs (or an algorithm to generate the keys dynamically) together with factory installed X.509 certificates.

In the case of EAP based authentication the MS is authenticated either through a unique operator issued credential, such as a SIM or through an X.509 certificate as described above. The choice of authentication method depends on the operator's choice of type of EAP as follows:

- EAP-AKA (Authentication and Key Agreement) for SIM based authentication,
- EAP-TLS for X.509 based authentication

- EAP-TTLS for MS-CHAPv2 (Microsoft-Challenge Handshake Authentication Protocol)

The BS associates the MS's authenticated identity to a paying subscriber and hence to the services the subscriber is authorized to access. Thus, through the exchange of AK, the BS determines the authenticated identity of the MS and the services it is authorized to access.

#### 3.2.2.1 Security Association

A Security Association (SA) is defined as the set of security information shared between a BS and one or more of the MSs connected to that BS in order to support secure communications across the WiMAX access network. Three types of SA have been defined, primary, static and dynamic. Each MS establishes a primary SA during the MS initialization phase. Static SAs are provided within the BS. Dynamic SAs are created and destroyed in real time in response to the creation and termination of service flows. Each MS can have several service flows on the go and can therefore have several dynamic SAs. The BS makes sure that the assigned SAs are compatible with the service types the MS is authorized to access.

#### 3.2.2.2 Authorization

Following authentication, MS requests authorization from the BS. This is a request for an AK as well as for an SA identity (SAID). The Authorization Request includes MS's X.509 certificate, encryption algorithms and cryptographic ID. In response, the BS carries out the necessary validation (by interacting with an AAA server in the network) and sends back an Authorization reply which contains the AK encrypted with the MS's public key, a lifetime key and an SAID. After the initial authorization, the AAA via the BS periodically reauthorizes the MS.

#### 3.2.2.3 Traffic Encryption

As we have seen above, the authentication and authorization process results in the assignment of an Authorization Key, which is 160 bits long. The Key Encryption Key is derived directly from the AK and is 128 bits long. The KEK is not used for encrypting traffic data; for this we require the Traffic Encryption Key (TEK) which is generated as a random number in the BS using the KEK encryption algorithm where KEK is used as the encryption key. TEK is then used for encrypting the data traffic.

## 4 USE CASES

In SPC deliverable DC1.6 [3] we described a couple of use cases used to extract a number of architectural requirements for a network that supports nomadism. In this section the use cases are revisited and adapted to highlight different types of mobility and the resulting issues related to session continuity that need to be addressed.

### 4.1 Session continuity use-cases

This section presents two use cases that have been defined to describe session continuity.

#### 4.1.1 Use case 1: WLAN hopping session continuity

Bob works for a company that has customers all over the world. Bob can do most of his work at home, but sometimes he prefers to be at the company office for face-to-face meetings with colleagues or customers. This afternoon he and a colleague had an appointment with a customer to discuss a new project.

After the meeting Bob returns home. While walking through the park towards his home, he starts a VoIP phone call, and makes a long conversation on his WiFi enabled multimedia device. He achieves this by connecting to an available WiFi network, as some of the houses nearby provide public access. He has a premium subscription so his call is transmitted in a traffic class having high priority. As the radio signal becomes weak, his equipment automatically connects to another access point providing public access. During the transition, the phone call is not disconnected neither suffers any significant quality degradation. Along his walk Bob hops from one public available wireless access point to another as illustrated in Figure 4-1.

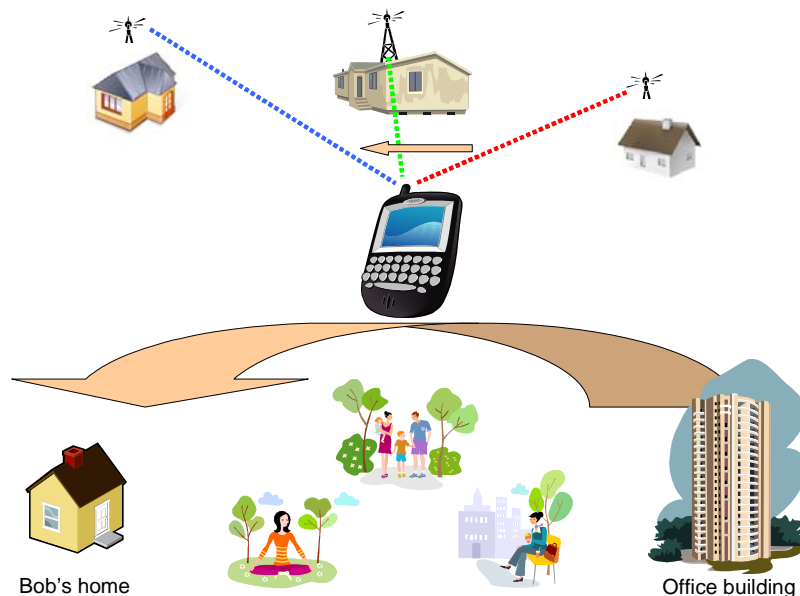


Figure 4-1 Use-cases: WLAN hopping

#### 4.1.2 Use case 2: Heterogeneous network session continuity

Eva is a medical doctor specialized in elderly care. She works in a hospital, and is responsible for a number of elderly people living in different parts of the city (or even in different cities) affiliated to the hospital. Being a mother of two kids, she can usually work from home, from her patients' houses or any other place where she can get secured Internet connectivity. Due to the need to work from different places, the hospital has subscribed to a video telephony and a secured remote access (VPN) service to help her work from remote places. Eva, as well as her patients, have high speed Internet subscription at their homes, which is paid by the hospital to facilitate her work and improve the health care of her patients. She has a best effort VPN subscription carried in the available spare bandwidth but always providing connectivity.

Eva is visiting a patient who has some serious medical problems. Using her multimedia enabled laptop, via the patient's home LAN she connects to the medical VPN. This way she can access the patients EMR and analyze the test results to make the necessary diagnostic. When preparing to leave Eva disconnects the notebook from the LAN to leave to another patient. As there are data transactions still going on the notebook connects to a WLAN providing public access thus remaining connected to the medical VPN. The connection to the database is not lost during the attachment point change. During her way to the next patient, the WLAN signal becomes weak. As there is no suitable WLAN network available, before losing the WLAN connection, the laptop connects to the WiMAX network and continues the data transactions as depicted in Figure 4-2. During this change the data transfer session is continued without a major disturbance.

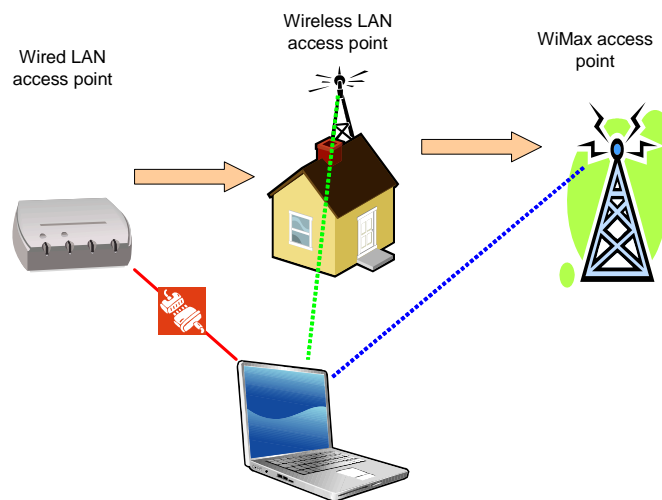


Figure 4-2 Use-cases: Attachment point type change

## 4.2 Use case analysis

As can be seen by the use cases studied in the previous section, there are several mobility types that need to be considered. In order to get a clear understanding of the issues related to session continuity, let us decompose the use cases into simple “mobility types”. Ordered by their complexity, all the different “mobility types” are shown in Figure 4-3 in order to illustrate the different problems that need to be overcome in each situation. Mobility types 1 to 3 in Figure 4-3 deal with the same access technology, namely Wi-Fi terminal connectivity in the SPC access network, while scenarios 4 and 5 deal with Ethernet and WiMAX respectively.

In the first use case, Bob is making a VoIP call using the available Wi-Fi access point while he is walking. If we have a closer look to what it means, we realize that several types of handovers can be identified as Bob walks towards home. In the case of mobility type-1 in Figure 4-3, Bob’s terminal changes connection between two APs connected to the same AN. This type of change implies that a service binding already exists for Bob at the serving AN but the same service binding can not be used in the new attachment point, since the parameters of this service binding that relate to the AN port would be incorrect at the visited AN.

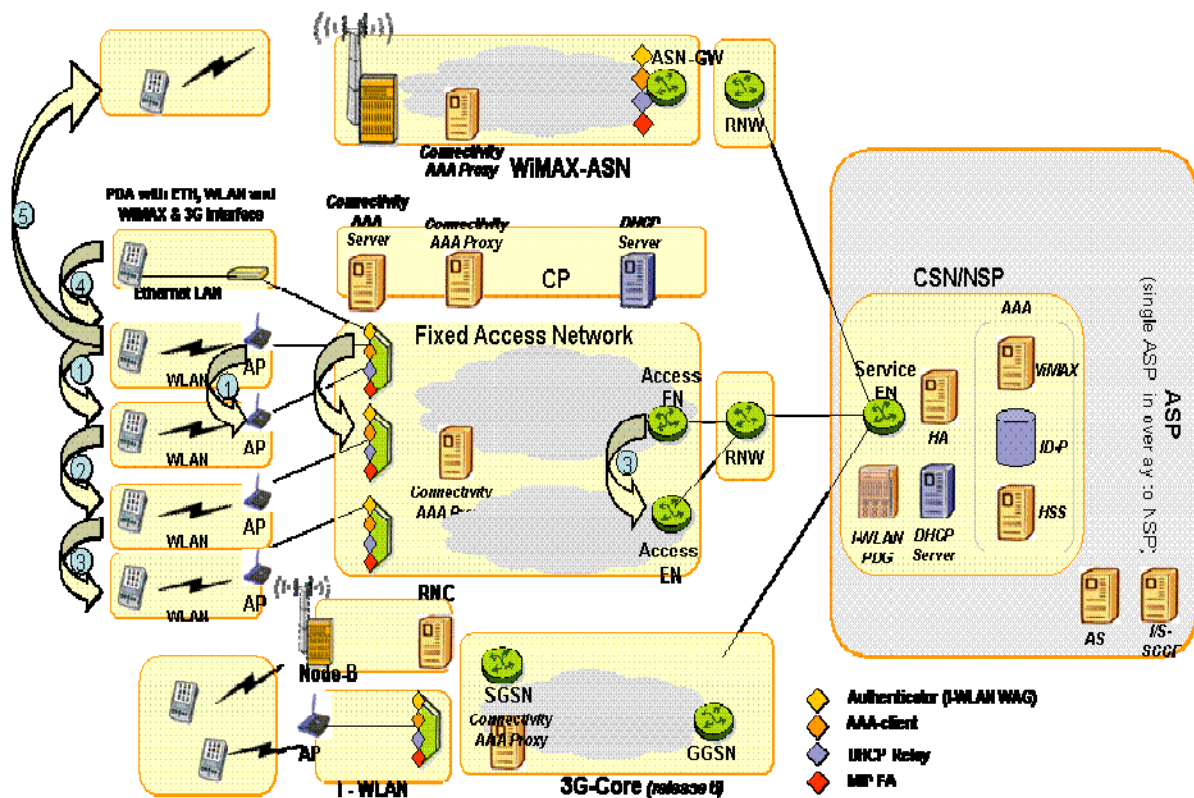


Figure 4-3 Mobility scenarios

In mobility type 2, Bob’s terminal is changing its point of attachment between two APs connected to different ANs but under the same EN range (both AN connected to the same EN). This implies that the service binding connection is completely new for the new AN. However this information is already known for the EN which will not need to create a new record for Bob but only an update of his point of attachment.

Mobility type 3 imposes a stronger impact for the network adaptation. In this case Bob’s terminal moves between AN connected to different ENs. This means that the service binding is completely new for both the AN and the EN and needs to be updated accordingly.

These three “mobility types” described above could be seen as L2 mobility scenarios. The reason for this is the L2 orientation of the SPC platform together with the single operator scope of this work. The L2 orientation means that connections between the end user and the edge of the access network are managed at L2. Accordingly an appropriate adaptation of the L2 parameters will enable the continuation of the end user session as long as the IP parameters are not changed.

However, these are not the only “mobility types” to be considered if we analyze the second use case, where Eva changes her point of attachment between her Ethernet network and external WLAN network when she is at a patient’s house. Mobility type 4 in Figure 4-3 depicts this case. In this case the L2 mobility management is not enough. Using a different type of interface would mean, most likely, a new IP address assignment. For this reason, higher layer mobility management, such as MIP, is needed to guarantee the continuation of the session in Eva’s terminal.

A similar approach is true for the “mobility-type” 5 in Figure 4-3. In this situation Eva changes her point of attachment between a WLAN AP and a WiMAX BS. As before, the new technology will impose a change of the IP address and accordingly L3 mechanisms need to be considered. However, this is not the only adaptation that the network needs. Since WiMAX has its own access network specification, a proper alignment between WiMAX architecture and the SPC platform is needed in terms of service binding configuration and mobility management coordination

From	To	Use-Case	Description	Technology specific	SB reloc	Solution
LAN	LAN		Unplug cable and plug in to an other port of the home hub or switch		no	No SPC platform interaction
			Unplug cable and plug in to the neighbor’s switch		port	Section 6.
			Unplug cable and plug in to the neighbor’s switch, which belongs to an other AN.		AN	
			Similar as previous. Not realistic.		EN	
WLAN	WLAN	1	More access points of the same WLAN are present, for example a WiFi network at an airport. All APs are configured with the	No SSID change	no	No SPC platform interaction

From	To	Use-Case	Description	Technology specific	SB reloc	Solution
			same SSID, therefore the client can move seamlessly within their range. This solution already exists today.			
			WLAN change can be managed by the OS. A TCP session can survive for a few seconds.	SSID change	no	
			See the use-case. There are technical differences, based on SSID change or SB relocation	No SSID change	port	Section 6.
				SSID change	port	
				No SSID change	AN	
				SSID change	AN	
				No SSID change	EN	
				SSID change	EN	
LAN		2	See the use-case and previous comment about the differences.		no port AN EN	
WLAN	LAN	~2	This is the inverse direction of the use-case. From a technical point of view, there is no new requirement.		no port AN EN	
WiMax	WiMax		Simple WiMax session continuity		AN EN	Solved in WiMax
LAN			Similar to #15-16, except the access technology		AN EN	
WiMax	LAN		Inverse direction of #23-24		AN EN	
WLAN	WiMax	2	This is a change between different wireless access types.		AN EN	Section 6
WiMax	WLAN	~2	Inverse direction of #27-28.		AN EN	

**Table 4-1: Attachment point change possibilities**

A summary of the different mobility types is shown in Table 4-1. It should be noted that even for the simple types of mobility, such as mobility types 1 and 2, maintaining the session requires much more complex issues than simply re-creating the service binding at the new location. When moving to a new AN, support of session continuity requires the tasks of authentication and authorization, admission control and resource management.

## 5 SESSION CONTINUITY

Session continuity is a very broad term subject to different interpretations depending on the context, in which it is being addressed. Therefore, it is prudent to have a look what a “session” is, before diving at the details of session continuity and address the issues involved in supporting session continuity. According to [6] “sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash)”. Summarizing: a session stores the *state* of an application in order to allow recovering in case of any disruption.

Secondly, the continuity of a session does not implicate the movement of a terminal. From the above definition a *user* can be the object of movement. In other words, a session can be bound to a terminal but also to a client of the system. In the former case part of the state can be stored in the end-user’s terminal. In the later the system state information has to be stored in the network.

Finally a break in the service accessibility is permitted. Although this might at first glance simplify the design of a solution it brings new issues to be considered. The most relevant one is the non-deterministic timeout of applications when a session is interrupted. Another aspect is the poor end-user experience as real-time and interactive services can be intolerant to any connectivity outages.

In the context of the MUSE, Task Force-8 (TF1.8) and Sub Project C (SPC) have jointly adapted the definition of ETSI/TISPAN, which reads as follows:

"The ability of a user or terminal to change the network access point while maintaining the ongoing session. This may include a session break and resume, or a certain degree of service interruption or loss of data while changing to the new access point."

From the above definition it is clear that session continuity can be seen as a further enhancement of nomadism. In essence both mechanisms aim at providing the end user with the ability to move in the network. In both cases the end-user expects to find the services it had previously subscribed to. The most outstanding difference between session continuity and nomadism is related to the accessibility to the service. In the nomadic scenario the end-user closes the application and restarts it from the beginning again. A new subscription process does not need to be executed, as the previous subscription must be enough. However in the session continuity scenario the end-user is allowed to keep its applications running. An interruption in the service accessibility can happen but the session in itself must be maintained. Obviously, the initial subscription is also enough. A good example to illustrate the difference is a Video on Demand (VoD) service. In the nomadic scenario the end-user stops the ongoing video session and closes the media player. When she reconnects from another point of attachment in the network, she has to be re-authenticated and if successful, the network resources needed to access the service will be reserved and her device will be configured with an IP address. At this point she can open the service portal and restart watching the movie from the beginning again. In the session continuity scenario the end-user

does not need to stop the video being watched. Re-authentication is performed automatically, resources are allocated and an IP address is obtained. The end-user continues to watch the movie with possibly a momentarily freeze in the image or a few glitches due to packet losses as the only trace of the handover.

One should bear in mind that the handover time includes the time for creating a new connection (regardless of layer-2 or layer-3 solution is used) plus the time to create a new service binding. Therefore, the time to restore a service binding is constrained by the maximum time needed to keep the session of that particular service alive.

In the following section we will discuss the implication of session continuity for different layers in the network. But as it turns out, analysis of the different layers regarding to their impact on session continuity by itself does not provide a complete picture of what happens in real life situations. Therefore, in order to get hands on understanding for the requirements, two types of simple lab experiments have been conducted. In the first experiment we look at the impact of different link layer interfaces to session continuity and examine whether the assumption that layer 2 mobility causes session disconnection is true or not. In the second experiment we test the impact on session continuity for applications running on different Operating Systems. Related to the lab tests, we provide a summary of the network traffic behavior from [7] when a computer is connected to both a wired and wireless networks.

## 5.1 Transport and applications layers related issues to Session continuity

The basic problem related to session continuity in IP/TCP(UDP) networking resides in the transport layer. The session layer binds the communication end-points (sockets) to IP addresses in the network layer. When a node then moves to another sub-network it can either keep its previously configured, but now topologically incorrect IP address and thus remain unreachable, since the routing in the network is not based on full host routes, or it can get a new, topologically correct IP address and lose its transport layer-session, since the new IP address can not be bound to the session. Because of the way the transport layers were designed and implemented in IP/TCP(UDP) networking, no rebinding of IP addresses is permitted. Taking the above description into consideration two architectural potential solutions can be identified:

- Change the transport layer to accommodate IP address changes;
- Change the network layer to allow a node to keep its IP address.

In the first option a mechanism to rebind sockets to a new IP address must be designed. It is been proved that this is feasible [8] [9]. In this work the cooperation of the session and transport layers results in a neat solution. The concept of mobility is extended to include mobility of devices, applications and any other objects. A mobile object is an abstract entity that moves the notion of naming from devices to objects. Mobile object names are formed by the name of the object and a domain, e.g., object@domain.com. In order to be useful a mobile object needs to provide a service to its users. To reach a service a user must prefix a mobile object name with the name of the service he/she is willing to access. Therefore the access is performed by solving a name, for example service.object@domain.com.

The mobile objects are assigned globally unique names which are mapped to their current positions on the network as in any other architecture that provides mobility. Before disconnecting from a network the mobile object sends a suspend message to all objects that have open sessions with it. When the mobile object is attached to the network again, the Session Name Server is informed of the new network address. At this point a resume message is sent to all objects that had open sessions with the mobile object. The sessions can then continue where they were interrupted.

In the second option, a different address is handed out to the physical network card at each new attachment point; for this to work, the configuration of the new IP address must be transparent to the application layer, as described in section 5.2.

### 5.1.1 Transport and Application layers Restoration time Consideration

The time to restore a connection is a very important aspect when session continuity is to be provided. The session continuity concept states that a break in the service accessibility is permitted. Although this might at first glance seem to simplify the design of a solution it brings new issues to be considered. The most relevant one is the non-deterministic timeout of applications when a session is interrupted. Some applications simply cannot cope with any network outages while others are tolerant to a large extent. Another aspect is the poor end-user experience, since real-time and interactive services can be intolerant to network outages.

Timeouts are also used in the transport layer in the end-user devices, more specifically by the protocols that guarantee the delivery of packet (e.g., TCP). If the transport layer cannot receive the expected packets during a certain period of time it resets the connection and the session is lost. Therefore the handover time of the underlying layer must not exceed the transport layer timeout. If the handover time is higher than the transport layer timeout the application must be paused before the handover. In order to express numerically the timeout values and verify the connectivity in case of handover we have conducted a series of measurements on PCs with Windows and Linux based operating systems. The results are presented in section 5.4.4. For reliable transport transmission such as TCP there are still issues related to retransmission that need to be solved.

Generally speaking the handover time at the lower layers must be less than any timeout in the higher layers if the session must be continued. If by any means the session can be paused then the handover can exceed the timeout values. For example, [8][9] proposes changes in the TCP layer to allow pausing of ongoing TCP sessions. In this way the transport layer will not timeout. The same rule is valid also for application layer protocols. If the application protocol cannot be paused the handover time must be smaller than the application layer protocol timeout.

## 5.2 Network layer related issues for Session continuity

It is an accepted wisdom that IP addresses are currently used for two functionalities: a locator functionality, as the IP address is used to route packets in the network, and an identity functionality, as the IP address is also used to identify one machine and one specific network interface. This dual functionality of IP addresses is one of the aspects that make mobility of nodes a difficult task. This is what the network solution tries to solve. Essentially, a virtual network layer interface can be created over the physical one, and although different addresses are handed out to the physical network card this should remain transparent to the applications. A tunnel is created between the mobile node and an anchor point in the home network. By informing the home network of the current physical location end-to-end connectivity can be restored.

As shown in Figure 5-1, the network layer approaches break these two functionalities into two different entities. Therefore, one extra layer is created. Generally speaking, this layer can be called an identity layer – it is used to identify a unique machine in the world. In this way mobility is eased in the sense that to find a given node the identity should be used. This is analogous to the real world scenario, where you locate people based on their identities, the names. Obviously, the identity information must be coupled to a locator. The coupling of both data is dynamic in nature, i.e., must be updated in the event of mobility. When a node moves its identity remains the same, but the locator changes, this means that in order to keep track of identity-locator associations a network node is needed.

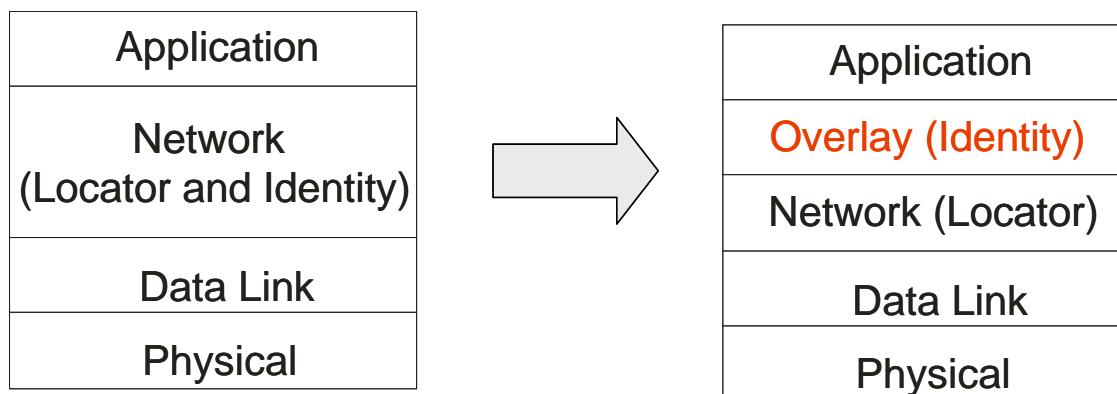


Figure 5-1 - Network layer approaches for session continuity

## 5.3 Link layer related issues to Session continuity

Changing the attachment point of the client in the network always assumes several steps of reconfiguration. The first step is to establish the layer 2 connectivity at the new location, then restore the IP connectivity. These steps are supported by the current operating systems, however the session continuity is not ensured. Thus, in order to maintain session continuity, we have to establish MAC layer connectivity and then handle the layer 3 session continuity. If the MAC layer connectivity can be restored without affecting the layer 3, i.e., the mobility is hidden from the IP layer, then we have a layer 2 mobility. In general restoring layer 2 connectivity involves the following steps:

- Authentication
- Service binding update
- MAC learning issues

After authentication, service binding update is required. This procedure is triggered by the authentication and updates the service binding to the new location as shown in Figure 5-2.

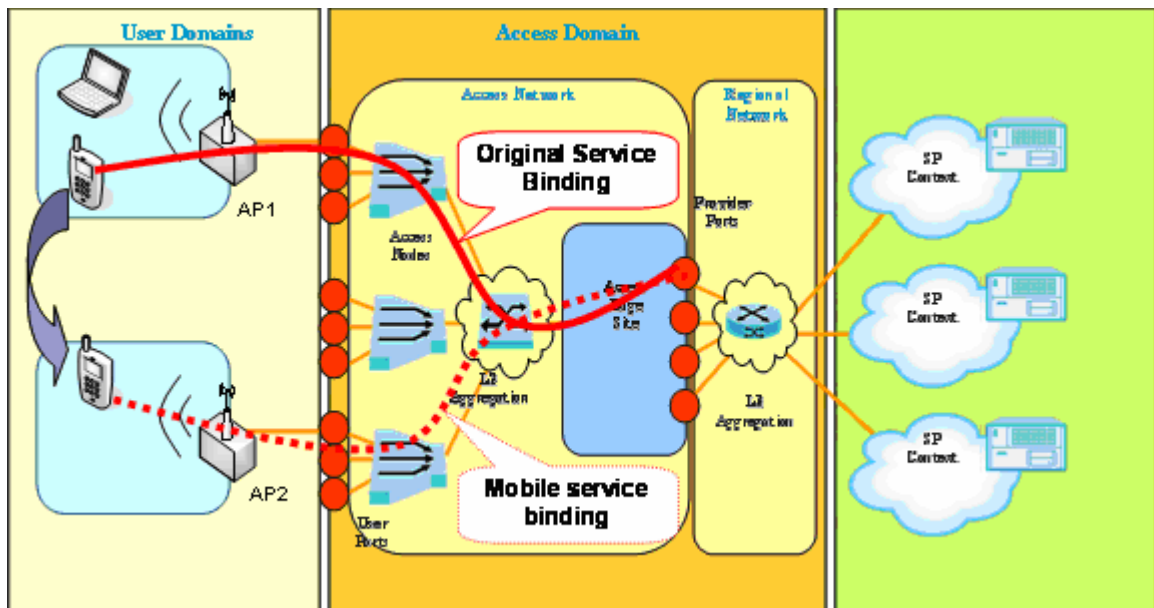


Figure 5-2 Service binding update

### 5.3.1 MAC learning issues

In the case when the handover is between different types of interfaces, e.g. Fixed-WLAN, or WiMAX-WLAN, the MAC address of the client may change. Although after the movement and when the layer 2 connectivity is re-created, e.g., using layer 3 mobility management, the IP devices the client was communicating with may still use the MAC address of the previous interface for communication. They will continue using that address until the ARP cache information times out. This requires the Edge Site to delete the ARP entry with the old MAC from its ARP table after handover.

Layer 2 mobility may require an additional step, handling the DHCP request after the MAC connectivity is established. The client may think that it is connected to a different subnet and requires new IP address. The DHCP request must be intercepted and the old IP address must be re-assigned.

## 5.4 Lab Experiment Results

In the following we will present the results of some simple experimental tests conducted to get a hands on experience on some of the issues that constraints for session continuity. In the first test, the survivability of a session when switching between fixed and WLAN access within the same layer 2 network is studied. In the second lab tests we examine dual-homing i.e., a single IP address per fixed and WLAN interfaces scenario in the context of session continuity. Related to the second tests, we provide a summary of network traffic behaviour from [7] for a multi-homed computer connected to wired and wireless networks.

The observations of the experiments are summarized below

### 5.4.1 Layer 2 handover scenarios

The purpose of this experiment is to prove that a break in the layer 2 connection does not result in an application layer disconnection and to identify the impact on session continuity. This experiment was conducted on a laptop with an Ethernet interface and a WLAN card with Windows XP and Linux operating systems (latter with kernel version 2.6.22). The test set up included two bridging wireless APs.

#### 5.4.1.1 Fixed interface connectivity scenario

In this experiment, the client is connected to an FTP server and starts a download. While downloading, the Ethernet cable is plugged out from the switch and connected to another port. This causes the network connection to be broken for a few seconds, but the same IP address is leased from the DHCP server.

The conclusion of these tests is that the short break of the link layer connection does not imply the session break, if all transport and application layer timing requirements are met. In the current scenario the FTP connection continues both on Windows and Linux machines. Hence layer 2 mobility is possible

#### 5.4.1.2 Fixed to WLAN layer 2 handover scenario

This experiment investigates dual-homing, i.e., a single IP address per fixed and WLAN interfaces scenario. The session is handed over from the fixed network interface to the wireless interface, when both interfaces are configured to the same static IP address. Since one IP address can be assigned to only one interface in an IP network, the two interfaces can not be up and running at the same time, so the fixed interface is up and wireless interface is down at the beginning. Then, the Ethernet cable is plugged out, and in the meantime the WLAN interface is enabled. The client connects to the WLAN, while using the same IP address configured manually. The same test was conducted in the reverse order too, i.e., disconnect from the AP and plug in the Ethernet cable. Now the same IP was used but on the Ethernet interface.

The outcome of this experiment was that the FTP connection did NOT disconnect. The conclusion is that both the Windows XP and the Linux stacks CAN handle Layer 2 mobility for FTP without any additional software if the same IP address is configured to both interfaces (they can not be up at the same time).

#### 5.4.1.3 WLAN to WLAN L2 handover scenario

The purpose of the test is to verify if L2 handover is possible within WLANs with different SSID. This means that the two wireless access points may be operated by different business actors (users, operators), but they are on the same subnet and share the same IP address pool. On the client machine the same static IP address is configured for the wireless interfaces.

The test results showed that no problem arises during the handover to a wireless AP with a different SSID. However, in some tests the session gets disconnected, because the switching from one AP to the other took too long and higher layers can not tolerate the outage. Setting the preferred network list in the client helps much. Connecting to the most preferred SSID speeds up the reconnection and hence reduces the outage to about 1 second.

The conclusion is that both on Windows XP and Linux when switching to an AP with different SSID and keeping the same IP address, the connection does not get broken, however slow handover may cause disconnection because of higher layer timing requirements.

#### 5.4.1.4 Observations

If the MAC address of the computer has changed during a session such as in 5.4.1.2, the default gateway between the computer and the communicating peer may still have the old MAC address associated in the ARP table with the IP address, and tries to forward the packet to the old interface. The entries are updated after around 2 minutes of idle state depending on the operating system. Hence the ARP table must be updated as soon as the handover takes place.

### 5.4.2 Handover timeout related lab test analysis

A fundamental question is if transport connections can be maintained after a handover and having been reassigned the same IP address. Experiments were made between machines with different operating systems (Windows, Linux) and running different types of applications, and machines on different geographical sites.

The observations of the experiments are summarized below:

- In case of connections with a Windows machine at one end, for any types of applications the transport connection survives for around 7 seconds, if the network interface of the Windows machine went down. That is, the socket is released after around 7 seconds and if the interface is not brought back up (including DHCP) in that time, the connection is released by the Windows operating system. The same result was observed independently from the distance between the two machines (though it must be noted that the connection between the two machines was excellent so the RTT was very low) and from the application used (FTP data transfer, network file system data transfer, FTP control traffic, VoIP, Skype, IRC).
- Windows does not release UDP sockets after 7 seconds.

- Between machines with Linux operating system the TCP connection survives even if the interface of one of the machines is down for 1 minute.
- If the Windows machine at one end of the connection stays connected, and the interface of a remote Linux machine is brought down, the connection stays alive even after 1 minute.
- Microsoft has implemented TCP fast reconnect for Windows Vista and future products to DAD and DHCP in parallel [10].
- TCP Keep Alive messages are sent after the connection is in idle state for 2 hours on Windows [11].

The table below summarizes the experiments made. It gives for each application whether it was able to resume the connection after some (10-60) seconds of outage, it gives the cause of disconnection and some additional comments..

		Disconnected?	Cause	Comment
Applications	Web browsing (Opera)	Yes on Windows No on Linux	Windows released the TCP socket after ~7 seconds.	
	IRC (Skype chat)	No	UDP	
	FTP (console ftp)	Yes on Windows No on Linux	Windows released the TCP socket after ~7 seconds.	
	Network file system (samba)	Yes on Windows No on Linux	Windows released the TCP socket after ~7 seconds.	
	P2P (utorrent)	Yes on Windows No on Linux	Windows released the TCP socket after ~7 seconds.	
	Video (VLC player) over HTTP/TCP	No	RTP/UDP	No buffering, some seconds fall out
	Helix Player Video)	Yes on Linux	A pop-up window is exhibited as soon as the buffer empties out. The session cannot be continued after the window pops up.	A buffer correctly sized in the application could allow session continuity.
	Voice (Skype)	Yes on Windows No on Linux	Windows released the TCP socket after ~7 seconds.	
	VoIP (sjphone) and IP phone	No	UDP, SIP	Some seconds fall out

**Table 5-1: Comparison of different applications regarding timeout**

A solution to handover and multi homing related problems in the transport layer could be SCTP (Stream Control Transmission Protocol) defined in RFC 2960 [12] and 3286 [13].

### 5.4.3 Traffic Behavior in a multi-homed Computer

The following is a summary of the network traffic behavior from [7] for a multi-homed computer, connected to both a wired and wireless network running Windows XP or Windows Server 2003:

- For traffic initiated by other computers that are neighbours of the multi-homed computer, the traffic flows over the network adapter attached to the common subnet. For example, if a neighbouring computer on the Ethernet-based subnet of the multi-homed computer initiates traffic, the traffic flows over the Ethernet network adapter.
- For traffic initiated by other remote computers (located beyond the locally attached subnets), the traffic flows over the network adapter corresponding to the destination IP address chosen by the initiating computer. For example, a multi-homed Windows XP-based computer will register the IP addresses for both wired and wireless network adapters in the Domain Name System (DNS) using DNS dynamic update. When another computer queries for the name of the multi-homed computer, it will get both of the multi-homed computer's IP addresses in random order. The DNS client resolver in Windows XP chooses the first IP address in the list returned by the DNS server.
- For traffic initiated by the multi-homed computer for neighbouring destinations, the traffic flows over the network adapter attached to the common subnet. For example, if a neighbouring computer is on the Ethernet-based subnet of the multi-homed computer, the traffic flows over the Ethernet network adapter.
- For traffic initiated by the multi-homed computer for remote destinations, the traffic flows over the network adapter associated with the currently chosen default route in the IP routing table, unless there are additional routes to the remote destination.
- Assuming that the multi-homed computer is running mostly client applications and accessing servers on remote subnets, most of the traffic of the multi-homed computer is in the last category (traffic initiated by the multi-homed computer for remote destinations)
- TCP/IP for Windows determines the current default route from the following criteria:
  - Select the default route that has the lowest metric.

- If there are multiple default routes with the lowest metric, choose the default route corresponding to the network adapter that is highest in the binding order.

By default, TCP/IP for Windows determines the metric for the default route by using the Automatic Metric feature, which assigns the metric to routes associated with the configuration of an adapter based on its link speed. (For more information, see An explanation of the Automatic Metric feature for Internet Protocol routes).

Table 4-2 lists the combination of wired and wireless technologies, their associated automatic metrics, and the resulting chosen default gateway adapter for a multi-homed computer running Windows XP with SP2.

Wired technology	Automatic metric	Wireless technology	Automatic metric	Chosen default gateway adapter
10BaseT	30	802.11b	30	Uses binding order
10BaseT	30	802.11a or 802.11g	25	802.11a or 802.11g (wireless)
100BaseT	20	802.11b	30	100BaseT (wired)
100BaseT	20	802.11a or 802.11g	25	100BaseT (wired)

**Table 5-2: Combinations of wired and wireless technologies and the chosen default gateway adapter**

To override the automatically calculated metric for the default route of a manually configured IP address configuration, specify the default route metric from the advanced properties of the Internet Protocol (TCP/IP) component. For more information, see Default Gateway Behaviour for Windows TCP/IP. To override the automatically calculated metric for the default route for DHCP client computers, you can use the Default Router Metric Base Microsoft vendor-specific DHCP option. To change the automatically calculated metric for the default route for all the Windows XP and Windows Server 2003-based DHCP client computers on a specific subnet, add the Default Router Metric Base option as a scope option to the DHCP scope corresponding to the subnet.

## 5.5 Conclusion

As exposed in this chapter, session continuity can be provided in different layers of the stack. The utilization of different solutions depends on different parameters in the single operator scenario. The first one is management of IP addresses pool. If the networks pre-handover and after handover draw IP addresses from the same pool a layer-2 solution can be applied. Otherwise only a layer-3 solution can implement the handover.

Furthermore the use of distinct mobility mechanisms can be defined by policies. These could be user or network policies. The first one can be used when the end-user is willing to interfere and decide which kind of solution should be used in his device. In the second one, more likely to happen, the access network provider can decide the solution to be used on a case basis. The access network provider can choose the solution that presents better performance, i.e., where the handover is faster or simpler. The policies could also be used to favour the lowest kind of mobility in the stack also aiming at having a fastest handover time.

## 6 SOLUTIONS FOR SESSION CONTINUITY IN THE SPC AND WIMAX NETWORKS

As described above Chapter-3, the SPC platform is an Ethernet based layer-2 access network. Typically, the layer 2 Access Nodes (ANs) are connected through layer-2 aggregation network to the Access Edge nodes (AENs). Similarly the WiMAX Access Service Network (ASN) profile C also provides layer 2 connectivity to the Access Service Network Gateway (ASN-GW). The AENs and ASN-GWs perform similar functionalities, when connecting to the NSP network. The different access networks host authenticator for authentication of end-users and AAA clients for translating the EAPoL messages to RADIUS/DIAMETER messages. They also host DHCP relay agents to relay DHCP request and Mobile IP Foreign Agents (FA).

### 6.1 Layer 2 Mobility

The layer-2 solution for session continuity is based on the fact that the same IP address is handed out to a given user after she has moved to another port in the access node or to another access node. Currently when a device disconnects from one port in the access node the IP address is put back right away in the pool of available address and thus could be assigned to another device. So, in order to make the layer-2 solution feasible the system should reserve the IP address for the device for a period of time after the disconnection in case the device reconnects to the same access domain during that period.

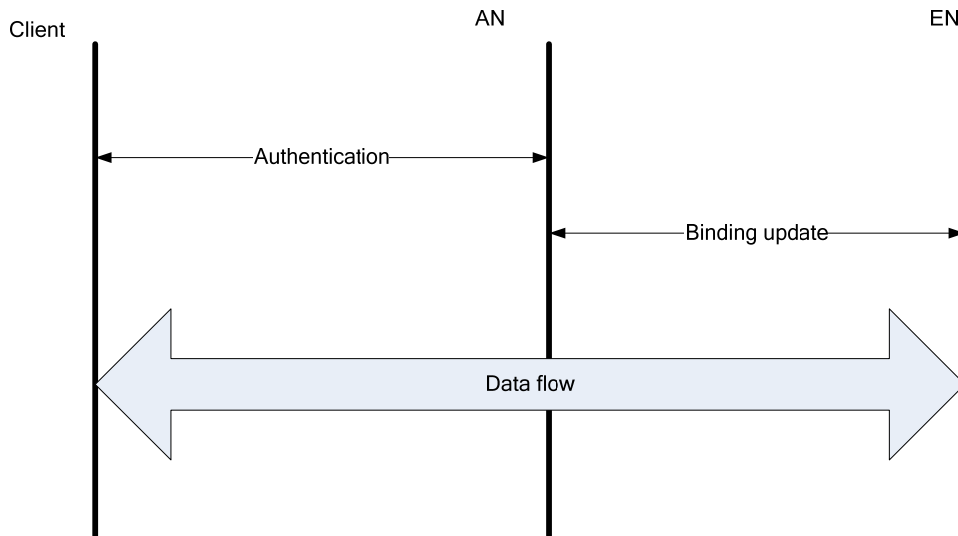
In the following we describe the steps for the support of layer 2 mobility for the different “mobility types” identified from the use cases in section 4.2.

#### 6.1.1 WLAN-WLAN

One of the most common mobility use cases is the movement of the user while changing the attachment point in the network. There are two sub-cases: changing to an AP with the same SSID and different SSID. The first use case describes this scenario.

##### 6.1.1.1 Same SSID

An example of this scenario is when the mobile client moves in the coverage area of a WiFi network at an airport. All APs are configured with the same SSID, therefore the client can move seamlessly within their range. An extended scenario is when the provider has a greater network with more APs downtown.



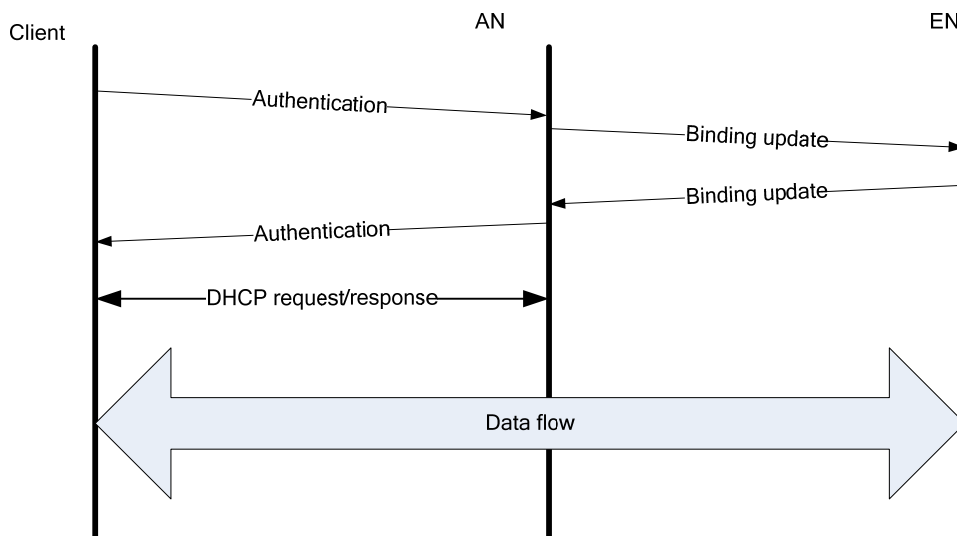
**Figure 6-1 Mobility within the same SSID**

The steps of the handover are presented in Figure 6-1. The handover is initiated by the client software. Since the new AP has the same SSID, the client software can perform the handover in a timely manner, i.e. before the connection becomes very weak. A further advantage is that the association with the new AP does not imply reconfiguration of the WLAN interface, the user is not even notified about the handover. (the interface does not go down/up).

The handover starts with an authentication. The AN authenticates the client and automatically initiates the binding update. After the binding update is completed, the communication can be resumed. The IP connectivity is not affected, since the IP address remains the same. Mobility is hidden from the IP layer.

#### 6.1.1.2 Different SSID

Public hot-spots owned by different end-users may have different SSIDs, although the use case is similar to the previous one. In these cases, the handover is more complex, involving reconfiguration of the WLAN interface (Figure 6.2).



**Figure 6-2 Mobility between different SSID WLANs**

The handover is initiated by the client when the signal strength from the previous AP goes below a critical level. Then, the client software searches for other APs and selects one based on signal strength and preference level configured in the client.

After the client associates to the new AP, the authentication phase starts. After the client is authenticated, two actions are triggered simultaneously:

- authentication triggers the service binding update
- the authenticated user starts the DHCP request since the client considers that it is connected to a different network

The DHCP request must be intercepted by the AN, and the same IP address must be renewed to maintain session continuity. The DHCP message exchange must be handled by the AN, since the binding update may still not be finished at this time.

#### 6.1.1.3 Movement within the same AN or between ANs

For both previous cases the changing of the attachment point to the provider network may involve a single AN (changing the AN port only) or may involve two ANs (change from an AN to a different AN). The handover mechanism for these sub-cases does not differ, however moving to a different AN involves resource management – resources must be reserved in the aggregation network to provision the new AP.

The resource management in this case is performed with the new binding setup. Policies define the resource management decisions that may result in the following results:

- Resources available, binding setup successful
- Resources unavailable, service downgrade required
- Resources unavailable, binding rejected

Policies are defined in Chapter-8.

### 6.1.2 Mobility between Fixed and WLAN networks

This mobility scenario is one of the most common use cases: the user plugs out the Ethernet cable and connects to the WLAN network or vice-versa. When both the Ethernet and WLAN interfaces connect to the same Ethernet domain, Layer 2 mobility can be assumed.

The IP address of the client will not change, however its MAC address will change. Therefore an update is needed at the default gateway in order to update the ARP cache (Figure 6.3).

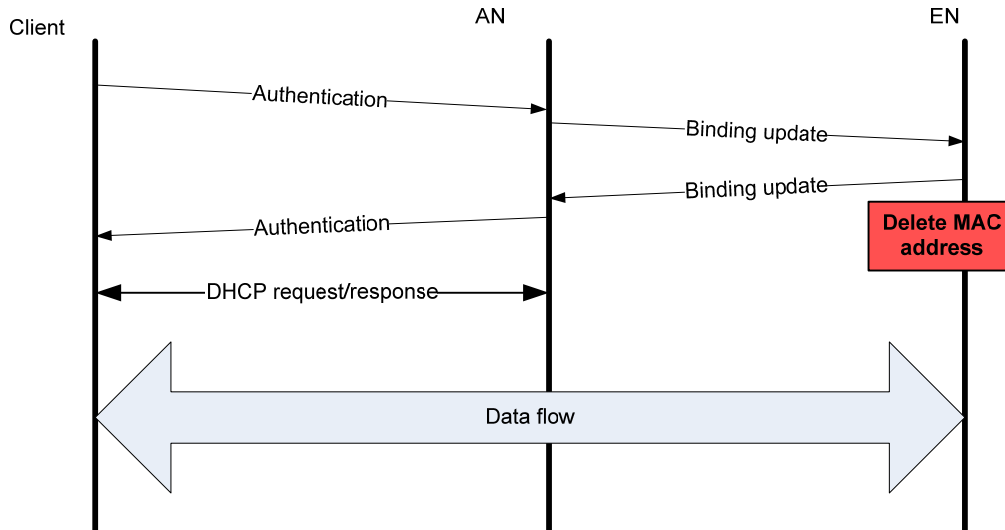


Figure 6-3 Mobility between fixed and WLAN

The handover is initiated by the client when the Ethernet cable is either plugged in or out. We suppose that the WLAN interface is also up by default. This is a case when a laptop is used, for example. There are two sub-cases: first, when fixed connection is up while WLAN interface is enabled and second when WLAN connection is used while fixed link is plugged on.

#### 6.1.2.1 Case 1: Fixed to WLAN

While fixed connection is up and running, when the WLAN interface is enabled the operating system will try to connect to an available wireless network. The most preferred WLAN network will be selected. First, the WLAN interface will associate to the access point then the authentication starts. After authentication, the client software will ask for IP address using DHCP. If the authentication or association fails, the client software will continue to search for other wireless networks, and if the IP assignment by DHCP fails, the client will stop trying. The session continuity requires that after handover the IP address should be maintained. Thus, after authentication the EN will have information about the active service binding to the client through the fixed interface, and should allow to connect and to respond to DHCP requests. However, the same IP address cannot be assigned to two interfaces at the same time.

We must enable the client to connect to the wireless network, to ensure that connection will be available when fixed connection becomes unavailable. Thus, based on service policy we can either assign a valid IP address to allow the client to use the WLAN interface too for communication or a special IP address can be assigned just to ensure that the WLAN connection remains available. When the fixed connection becomes unavailable, the DHCP server will force the client to renew its IP address, assigning the address of the fixed interface. However, at the IP level in the default gateway the MAC address of the fixed interface is still cached in the ARP table. In order to ensure IP level connectivity, the ARP table entry at the EN should be deleted after switching to the WLAN interface.

The network must be able to detect the break of the fixed connection. This may be a difficult task, since the RGW to which the client is connected to will not notify about any change. There are several possible solutions:

- Periodic keep alive
- When fixed connection becomes unavailable, client automatically will switch to the other interface. The access node can detect the traffic at this interface.

#### 6.1.2.2 Case 2: WLAN to Fixed

In this case the WLAN interface is used for communication while the cable is plugged in the fixed interface. If the network policy is that the fixed connection has priority over the wireless connection, the fixed interface should be used when available.

When the fixed network connection becomes available, the client will ask for IP address by DHCP. After authentication, the following steps will be done:

- The service binding to the fixed interface must be set up
- On the wireless connection the DHCP should revoke the IP address and issue a different one (either valid or a special)
- The same IP address must be leased on the fixed connection
- The ARP cache entry for the IP address must be cleared

The wireless connection should not be interrupted, since we must anticipate the interrupt of the fixed connection, and then we have to return to the wireless connection.

## 6.2 Layer 3 mobility

Regardless of the kind of solution used to provide session continuity network address handling has to happen. If a network solution such as Mobile IP is used the Mobile Node (MN) is always expected to be addressable at its Home Address, even if it is not currently located in its home network. The MN also possesses a physical underlying network interface which has a locally assigned IP address, called Care-of Address (CoA). When the node is roaming the Care-of Address is assigned by the visited network. However the new address is not visible to applications that only see the virtual interface and home address.

### 6.2.1 Layer 3 mobility with MIP

The main network layer mobility management candidate for providing session continuity is Mobile IP [14]. Two kinds of Mobile IP exist; MIPv4 is the original version for IPv4 networks, while MIPv6 is a recent development for IPv6 networks. Both protocols work in a similar manner but MIPv6 has no Foreign Agent. A common assumption to both protocols is that the mobile node is always expected to be addressable at its Home Address (HoA), even if it is not currently located in its home network. A virtual interface is created in the mobile node and the home address is assigned to this interface. The status of the new virtual network interface is always *up*.

In MIP terms the host which the mobile device is exchanging messages with is called Correspondent Node (CN), while the client terminal is called a Mobile Node (MN). The Correspondent Node can be a server or another end-user device. The mobile node also possesses a physical underlying network interface which has a locally assigned IP address, called Care-of Address (CoA). When the node moves this network address changes, however the change is not visible to applications that only see the virtual interface and home address.

In MIPv6 the Corresponding Node sends traffic to the mobile node IPv6 Home Address (HoA) via the MIPv6 Home Agent (HA), which reroutes the traffic to the mobile IPv6 care-of address. When the MN changes the Care-of Address (CoA) the MIPv6 protocol updates the HA with the new CoA. The service can then continue. Figure 6-4 illustrates the scenario where MIPv6 is deployed on the Internet.

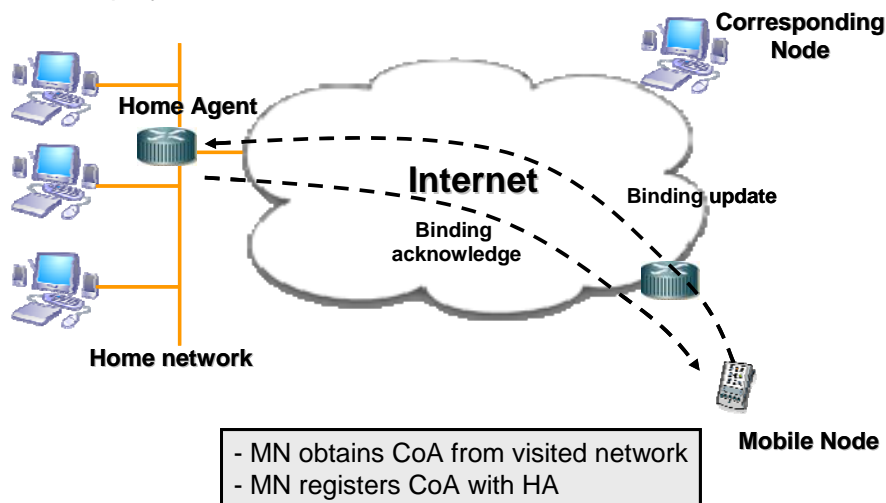


Figure 6-4 - Mobile IPv6 architecture

More on the MIP implementation related issues is detailed in Chapter-9

## 6.2.2 Proxy MIP for SPC

Proxy MIP is a network based IP mobility solution where the host does not take part in the mobility signaling, route update is done by signaling between access routers. Recently the MIPv6 based version, PMIPv6 is being under study in IETF [15], and IPv4 is going to be supported for dual stack hosts.

An important advantage of the proxy MIP solution is that it does not require the client TCP/IP stack to be modified, i.e. no operator software (MIP) is installed on the client's machine, the standard stack operates on the mobile node.

In the PMIPv6 solution the IPv6 prefix follows the mobile node and always sees the same network prefix. The home network of the mobile node has an LMA (Local Mobility Agent) function, and each visited network access router implements a MAG (Mobile Access Gateway), which can be mapped to the SPC platform's Edge Node Complex.

When a handover takes place the general procedure is the following:

- the access is authenticated
- right after the MAG function retrieves the mobile node's profile from the home network (containing the home address and prefix),
- an IPv6 tunnel is established to the LMA, which is used to forward all traffic from and to the mobile node
- the MAG sends a Proxy Binding Update to the LMA, which is acknowledged by a Proxy Binding Ack message
- Router Advertisement are uni-cast to the user with the home network prefix. And the user acts as an ordinary IPv6 when using the stateless auto-configuration.

As the L3 address of the node does not change in PMIP, this procedure is in line with the layer 2 solution described in [Chapter-6](#), which considers the same IP address to be reassigned after each handover.

To integrate PMIP into the SPC platform the MAG and LMA functions should be added to the Edge Node Complex.

## 6.3 Conclusion

The SPC platform is based on L2 technologies that make possible layer 2 mobility while supporting layer 3 mobility too. In this chapter solutions are presented for different mobility types taking into consideration the advantages of the SPC platform. The given solutions include layer 2 handovers between WLAN and fixed technologies, and also provide guidelines for layer 3 mobility. Layer 2 mobility suites well the SPC platform, and for mobility within a single operator it is the most convenient solution. For mobility within the coverage of the same NSP, a Layer 2 mobility suite well within the SPC platform, and is the most convenient solution as it will optimize the HandOver times while keeping the same IP address. For layer 3 mobility, a network-based mobility solution (Proxy MIP) is presented besides the classical Mobile IP based solution. The main advantages of the Layer 2 mobility and the Proxy MIP solutions are that they do not require client support, i.e. no client software modification is required to support mobility.

## 7 POLICY CONTROL AND QOS

### 7.1 Policy Control Framework for session continuity support

The policy control architecture as defined in DTF1.8 [4] was adapted toward the network reference model for this deliverable and shown in Figure 7-1

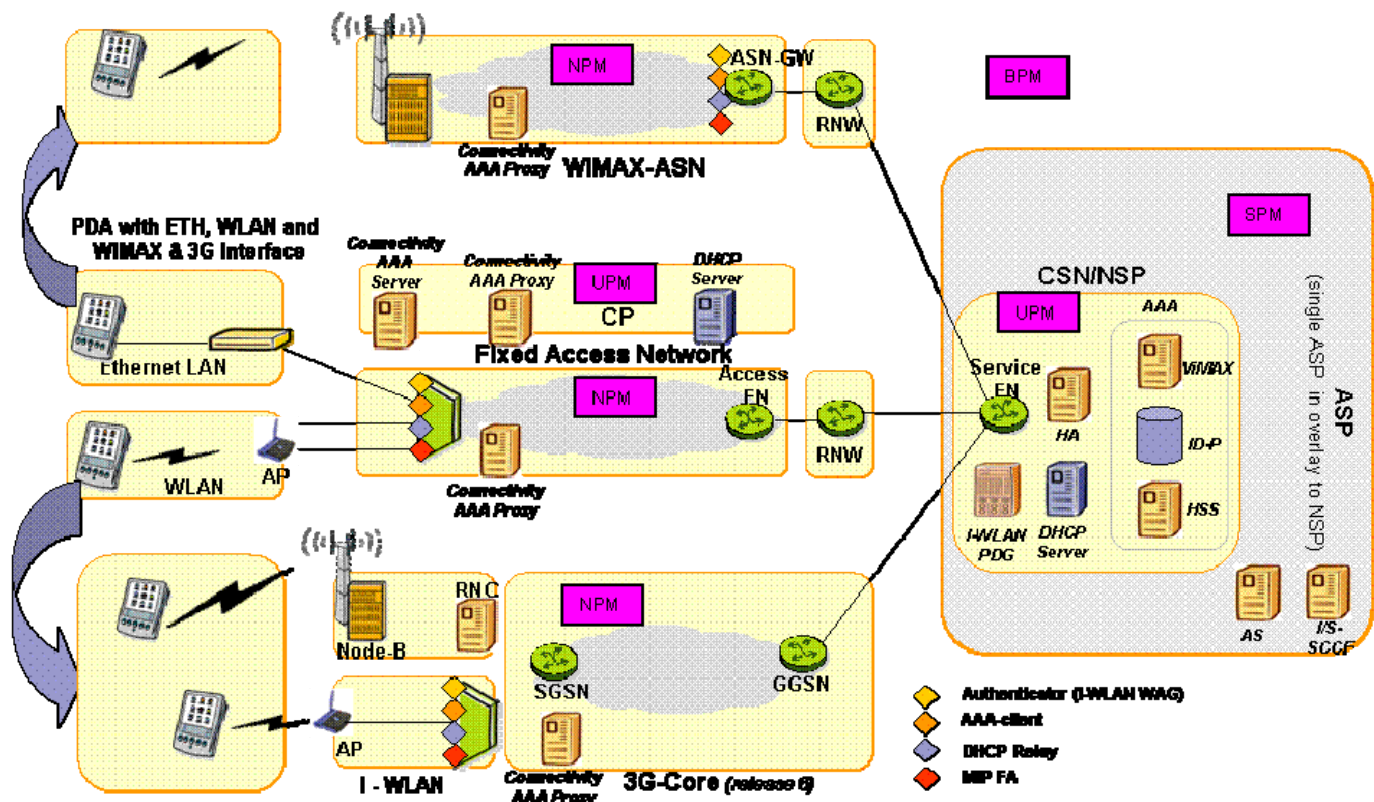


Figure 7-1 Policy control architecture in terms of DC1.7 network reference model

Note our work focuses on the policy control functionalities within the operator's network. Policy control inside home network or in the residential gateway is for further study.

### 7.1.1 Policy control work flow

It is assumed in the network reference model that session continuity for moving customer equipments and applications is maintained within the same Connectivity Provider, Network Service Provider, Application service Provider and Packager domain, i.e., CP-h, NSP-h, ASP and Packager-h in Figure 7-1, policy instances for a given user in UPM, SPM and BPM should be identical or rather there should be just one single instance per user subscribed service in these policy managers. Thus the policy manager localization and policy transfer described in DC1.5 for roaming users can be skipped, i.e. there will be no inter-domain policy interaction in the scenarios. This implies the delay introduced by policy control can be reduced, which is necessary to maintain session continuity. However, since the user can well hop between different access types, NPM can be different.

Session continuity needs to be implemented based on “quick enough” handover. To achieve this, a feasible mobility mechanism is required. The common mobility mechanisms used today are mainly SIP based mobility and MIP based mobility. Study has shown that either mechanism is able to provide handover time fast enough to sustain session continuity without network assistance [16]. Based on the abovementioned result, [16] has proposed signaling optimization for SIP based application and a mobility controller for MIP based applications in order to achieve acceptable handover delay. This network assisted mobility implies mobility policies should be used.

User Policy Manager, or UPM, is the best candidate to handle mobility related policies. UPM has information about user Ids and services a user has subscribed to. To handle session continuity, the following information can be added to user policies for a given service a user subscribes to:

- Session Continuity Support: Y/N
- Mobility mechanism: SIP/MIP/Layer 2

Given these parameters for a given application, UPM can decide what policies to use to instruct mobility controller or other mechanisms to take effect.

Another mobility mechanism investigated by this deliverable is layer 2 mobility, in the case when a user is moving within the same administrative domain, i.e., no IP address change is needed when moving, layer 2 mobility can be used. As described in Chapter-6, layer 2 mobility provides lower delay, thus a better support for session continuity.

When a user movement is detected, e.g., un-plug of an Ethernet cable, moving to the coverage of another WLAN AP, etc, the UPM will make the following decision for this user:

1. What are the currently subscribed services on the device?
2. Among all these applications, which one(s) needs session continuity support?
3. Will the session continuity be supported by layer 2 or layer 3 or higher layers mobility management?
4. For layer 3 and higher layers mobility support is MIP enough, or application layer mobility management such as SIP is needed?

Based on the answer to these four questions, the corresponding policies will be enforced in the network, for instance to invoking mobility controller or setting up new service binding, etc, and the handover will start to take effect. It is clear that if the UPM has to take decision following the abovementioned four steps each time a user movement occurs, it will result in a long delay. Therefore an optimization process can be introduced. For instance, since the user movement usually have some patterns, such as leaving home for work at work days at 8 in the morning, coming back home through a certain street at 6 in the afternoon, go from the living room to the laundry room 10 in the morning on Saturdays, etc, a pattern based optimization process can be applied.

### 7.1.2 Network-based session continuity policies

Network based policies for session continuity support can be further categorized by different mobility provisioning mechanism, i.e., layer 2, MIP or SIP mobility.

Some policy examples will be presented in this chapter to illustrate how policies in a system can look like. This is however a non-exhaustive list and may be different from what a network operator chooses to install in his/her network.

Layer 2 mobility based policies examples should include the following aspects:

Condition 1: session continuity support needed

Condition 2: moving within the same administrative domain

Condition 3: keeping the same IP address

Action 1: choose network at new location.

Condition 1-1: pre-choose new network based on pattern

Action 1-1: read pattern and choose network before moving occurs.

Condition 1-2: choose new network based on signal strength

Action 1-2: detect signal strength and choose network.

Condition 1-3: choose new network based on resource availability

Action 1-3: query resource manager before choosing network

Action 2: network selection

Condition 2-1: Action 1 has found a proper network

Action 2-1: instruct the user to use this network

Action 3: Re-Authentication/Authorization

Condition 3-1: pre-authentication/authorization is needed

Action 3-1: perform pre-authentication/authorization

Condition 3-2: 802.1x AAA is preferred

Action 3-2: perform 802.1x AAA

Condition 3-3: SIM based AAA preferred

Action 3-3: perform SIM based AAA

Condition 3-4: PANA AAA preferred

Action 3-4: perform PANA AAA

Condition 3-5: No AAA needed

Action 3-5: no action

Action 4: AAA handling

Condition 4-1: AAA passed or no AAA needed

Action 4-1: grant access to the new network  
Condition 4-2: AAA failed  
Action 4-2: deny access

Action 5: Set up new service bindings

Condition 5-1: pre-defined service binding exists for this service  
Action 5-1: use pre-defined service binding.  
Condition 5-2: can borrow other service bindings temporarily  
Action 5-2: change parameters of an existing service binding for use  
Condition 5-3: new service binding can be set up  
Action 5-3: set up a new service binding  
Condition 5-4: no service binding can be set up  
Action 5-4: use default best effort connection or reject the service

Similarly, MIP based policies examples can look like these:

Condition 1: session continuity support needed  
Condition 2: MIP is used for mobility

Action 1: choose network at new location.

Condition 1-1: mobility controller is available  
Action 1-1: invoke mobility controller for network selection  
Condition 1-2: mobility controller is not available  
Action 1-2: invoke normal MIP process

Action 2,3 and 4 are similar to actions for layer 2 policies.

For SIP based policies:

Condition 1: session continuity support needed  
Condition 2: SIP is used for mobility

Action 1: choose network at new location.

Condition 1-1: pre-choose new network based on pattern  
Action 1-1: read pattern and choose network before moving occurs.  
Condition 1-2: choose new network based on signal strength  
Action 1-2: detect signal strength and choose network.  
Condition 1-3: choose new network based on resource availability  
Action 1-3: query resource manager before choosing network

Action 2: network selection

Condition 2-1: Action 1 has found a proper network  
Action 2-1: instruct the user to use this network

Action 3: SIP mobility session set up

Condition 3-1: SIP signaling optimization is available  
Action 3-1: invoke optimization process  
Condition 3-2: SIP signaling optimization is not available  
Action 3-2: invoke normal SIP signaling process

Actions for AAA are similar to that for layer 2 policies.

### 7.1.3 End-User-based session continuity policies

Responsibilities of end-user based policies to support session continuity include:

- User movement pattern management
- User movement prediction
- New location report
- Movement prediction evaluation/modification
- User network connection preparation

One typical example of an end-user based policy set can be:

For user movement pattern management:

Condition 1: work day

Condition 1-1: 8am - 8.30am

Action 1-1: put location to the kitchen

Condition 1-2: 8.30am - 9.00am

Action 1-2: put location to be on the way to work

Condition 1-3: 9.00am – 11.30am

Action 1-3: put location to office

Condition 1-4: 11.30am -12.30pm

Action 1-4: put location to restaurant

Condition 1-5: 12.30pm-3.00pm

Action 1-5: Put location to office

Condition 1-6: 3.00pm-5.30pm

Action 1-6: Put location to meeting room

Condition 1-7: 5.30pm-6.00pm

Action 1-7: put location to be on the way back home

Condition 1-8: 6.00pm – 7.30pm

Action 1-8: put location to be in the kitchen

Condition 1-9: 7.30pm – 9.30pm

Action 1-9: put location to be in the living room

Condition 1-10: after 9.30pm

Action: put location to be in the bedroom

Condition 2: Saturday

Condition 2-1: 8am - 8.30am

Action 2-1: put location to the kitchen

Condition 2-2: 8.30am – 12.30pm

Action 2-2: put location to be in downtown

Condition 2-3: 12.30pm – 4.30pm

Action 2-3: put location to stadium

Condition 2-4: 4.30pm – 6.30pm

Action 2-4: put location to downtown cinema

Condition 2-5: 6.30pm – 8.30pm

Action 2-5: Put location to downtown restaurant

Condition 2-6: after 8.30pm

Action 2-6: put location to home

Condition 3: Sunday

Condition 3-1: 8am - 8.30am

Action 3-1: put location to the kitchen  
 Condition 3-2: 8.30am -10.30am  
 Action 3-2: put location to laundry room  
 Condition 3-3: 10.30am – 4.30pm  
 Action 3-3: Put location to home  
 Condition 3-4: 4.30pm – 8.00pm  
 Action 3-4: Put location to parent’s home  
 Condition 3-5: after 8.00pm  
 Action: Put location to home

For user network connection preparation:

Condition 1: location is downtown  
 Action 1: prepare to switch to 3G network  
 Condition 2: location is on the way to work  
 Action 2: prepare to switch to neighbor’s WLAN network  
 Condition 3: location is in the laundry room:  
 Action 3: prepare to switch to apartment’s public WiFi network  
 Condition 4: location is parent’s network  
 Action 4: prepare to switch to parent’s WLAN network

Other responsibilities can have similar policy set, and it is up to the network operator to work out the exact policy set based on its own network status and customers.

### 7.1.4 A Use Case Analysis

For use case 2, where Eva gets connected to her work through heterogeneous networks, the policy framework can work as following (Table 7.1):

Activities	Policy Involvement
Eva is visiting one of her patients	End User policy: Conditions: Workday, 9.00-10.00, Actions: put end user location to this patient’s home
She gets connected through the patient’s LAN to medical VPN	Normal AAA and Security Policies applied as for nor-roaming case.
Eva is leaving for another patient’s house, and her notebook is disconnected from the LAN but connected to a WLAN for the data transactions to be remained connected. During her way, the WLAN signal is becoming weak, so the notebook gets connected to a WiMAX network and continues the date transactions.	End User Policy: Workday, 10, put end user location to on the way to another patient Mobility Policy: Conditions: a. Session continuity support is needed b. New Location is in the same network Administrative Domain c. Keep the same IP address for Eva’s Laptop d. Choose network based on

	<p>signal strength</p> <p>Actions:</p> <ol style="list-style-type: none"> <li>1. Detect signal strength and choose a network (in this case WLAN)</li> </ol> <p>Detect signal strength change and connect to other networks when needed (in this case WiMAX)</p>
--	---

**Table 7-1 Use Case Analysis for Policy Control**

### 7.1.5 Conclusion

It can be concluded that no extra functional blocks to policy control framework defined previously in this project are needed for session continuity support. However, more sophisticated policies need to be defined and enforced to fulfill the high requirement in terms of delay for mobility management, which is a key to guarantee successful session continuity. One possible approach to improve the “hit rate” of network selection for example can be based on patterns, and more innovative or clever approaches can be expected in this area.

## 7.2 QoS Provisioning

### 7.2.1 QoS mechanisms in different access networks

#### 7.2.1.1 QoS in Ethernet LAN

Ethernet in itself is a best-effort network, which does not have any built-in QoS support. To provide QoS in an Ethernet network, a number of operations is needed, such as traffic marking, admission control, etc. Traffic marking in Ethernet is done through the Class of Service (CoS) field in the VLAN tag, which is a 3-bit tag that provides 8 different possibilities for traffic differentiation. Traffic marking is usually done at the network edges, in the DC1.7 reference model, the residential gateway with the home Ethernet LAN (if there is any), the access node and the Access Node (AN) should all be able to perform traffic marking, however, the AN and Access Edge Node (AEN) should be equipped with re-marking functionality to gain a better control of traffic from end users.

At the network edge, admission control or traffic conditioning is also needed to make sure that traffic going into the network is in line with some pre-defined or desired network conditions. Admission control can be based on statically configured policies, or it can also be based on measurements, where end user equipments use measurements on payload traffic to predict the bandwidth availability of the network. In Ethernet LAN, both of these two methods are applicable. QoS in Ethernet is provided based on different classes defined by CoS field in the VLAN tag, with each class associated with a specific bandwidth profile addressing the feature of this class. Metro Ethernet Forum has defined four parameters to specify a bandwidth profile, namely Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIS), and Excess Burst Size (EBS). These parameters give a description of what the network can provide to each class. QoS in Ethernet LAN can be provisioned with over-provisioning, or it can be provisioned through differentiated treatment of traffic marked with different CoS together with effective admission control and policing. In DC1.7 reference model, given the relatively mass bandwidth Ethernet can provide, it would be good to use over-provisioning at the home network Ethernet LAN. In the aggregated part of the access network where bandwidth could cause a resource problem, a

DiffServ type of QoS mechanism can be applied based on CoS markings in the VLAN tag.

#### 7.2.1.2 QoS in WLAN

The original 802.11 WLAN does not come with a strong support for QoS. In WLAN, QoS is supported by differentiating station behaviors in the following areas:

- When should a station start to transmit packet?
- When a collision occurs, how long should a station wait before it can start transmission again?
- How does each station differentiate its own traffic?

In 802.11, access to the media is based on CSMA/CA to avoid collision. Original 802.11 defines two access methods, namely Distributed Coordination Function (DCF) and Point Coordination Function (PCF).

For DCF, answers to the above-mentioned issues are:

- Every station listens to the channel to be idle for a certain period of time, and then it can start transmission independent of each other.
- When a collision occurs, a station will double its back-off time before retransmission.
- One queue for all packets within a station.

It is clear that DCF is a best-effort type of mechanism which does not have any QoS support. PCF introduces a coordinating station in the WLAN called Point Coordinator. It has the following feature:

- Every station is polled by a CP before it can start transmission, and the channel idle time can be shorter than in DCF case.
- No collision should occur if everything works as defined, because stations are polled for transmission. This reduces the long back-off time and increase the channel efficiency.
- One queue for all packets within a station.

The PCF can give certain priorities to some stations in the WLAN when polling for packet transmission, which can give favorable conditions to time-critical applications or services. However [17] has described the insufficiency of 802.11 as to provide QoS in WLAN.

Based on this observation, IEEE approved 802.11e as an enhancement to provide better QoS in WLAN. It is supposed to be backward compatible with 802.11 and introduces two new access methods: Enhanced DCF (EDCF) and Hybrid Coordination Function (HCF). In EDCF, QoS is supported by introducing Traffic Categories (TC), with each TC having different QoS parameters associated to it. Each station that implements 802.11e can maintain 8 different queues which are grouped into 4 QoS classes. Within each class, 4 parameters can be specified to provide various QoS features. Again, HCF appoints a coordinator to poll stations for transmission. So 802.11e has the following QoS feature:

- Each station is polled by a CP before transmission.
- No collision should occur.

- Eight queues for different packets that can be grouped into 4 classes based on 4 QoS parameters. Provide differentiated treatment to packets.

However, it should be noted that WLAN does not provide any guaranteed QoS, but rather a DiffServ flavored QoS.

### 7.2.1.3 QoS in 3G

In 3G, or more specifically in UMTS networks, QoS is considered end to end, i.e. from one terminal equipment to another terminal equipment. QoS is provisioned by means of bearer services which cover different part of the whole network. Bearer Services are implemented in layered structure and specify QoS characteristics at each layer. A typical Bearer Service Architecture from 3GPP in Figure 7-2 gives an overview of how bearer services can look like. Bearer Services use a mechanism similar to protocol stacks, which means upper layer Bearer Services can use the functionality provided by lower layer Bearer Services.

A bearer service includes all aspects to enable the provision of a contracted QoS. These aspects are among others the control signalling, user plane transport and QoS management functionality.

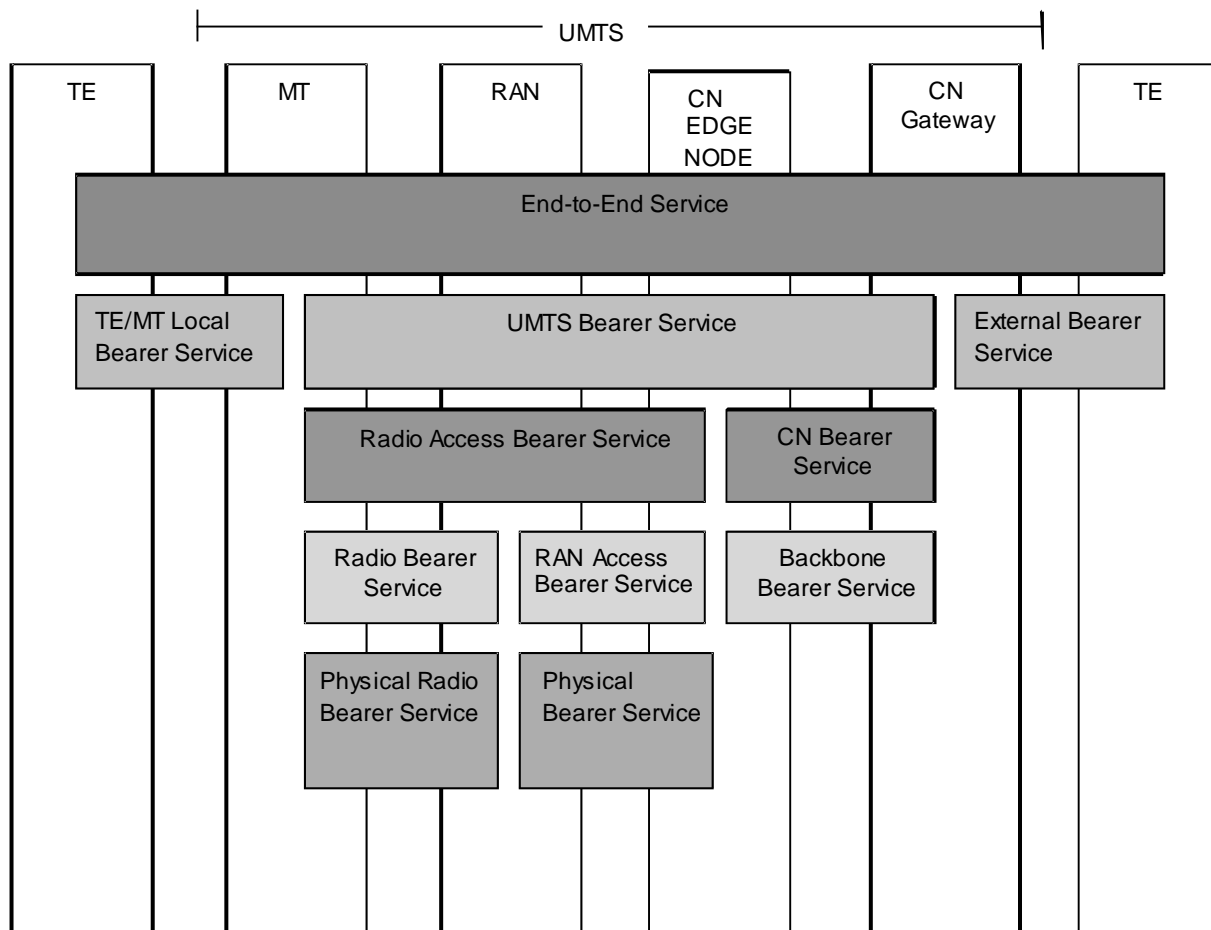


Figure 7-2 UMTS QoS Architecture

UMTS defines 4 QoS classes, namely conversational class, streaming class, interactive class and background class.

Each bearer service has a list of attributes that describes QoS features provided by this bearer service:

- Traffic class, one of the 4 classes defined in UMTS.
- Maximum bit rate
- Guaranteed bit rate
- Delivery Order
- Maximum SDU size
- SDU format information
- SDU error ratio
- Residual bit error ratio
- Delivery of erroneous SDUs
- Transfer delay
- Transfer handling priority
- Allocation/retention priority
- Source statistics descriptor
- Signalling indication

Before packets can be transferred, Bearer Services are setup through signalling, each with a specification of attributes. During the data transfer, Bearer Services remain the same, and they are torn down when a session comes to an end.

### 7.2.2 Conclusion

In order for the roaming session to be able to maintain session continuity and its QoS features, different access technologies need to have a coordinated QoS architecture from the following aspects:

#### **Bandwidth Management**

Bandwidth management can be separated into two areas: provisioning principle and admission control mechanism. Based on the diversity of QoS mechanisms introduced by different access technologies, a good recommendation can be static provisioning. This can in general give a higher resource utilization, and requires less interactions from the roaming session. When static provisioning is used, admission control can also be relatively simple at the edge of each access type.

#### **Class of Service**

It is also clear from the previous chapter that different access networks have different CoS classifications. To achieve session continuity, either these different CoS classes have to be unified, or a mapping mechanism is needed for each access pair.

**Edge Functions**

Different edge equipments from different access networks should have coordinated edge functions in terms of policing, shaping, firewalling etc. QoS parameters such as CIR, CBS, etc should be treated, understood, managed or monitored in the same way by different access edges.

**Protection Switching**

All access networks should have a restoration mechanism to maintain QoS in a single network failure case or unexpected faulty case. The failover time requirement to maintain session continuity has to be fulfilled by each access network.

**Common QoS Architecture**

A good way to support session continuity from QoS perspective is to be able to come up with the best-practice type of recommendations for each access type, and work out a common QoS architecture based on that. However, at present, higher layer QoS awareness may be needed.

## 8 AUTHENTICATION AND AUTHORIZATION

### 8.1 Authentication and mobility management

As stated in section 5.3 there is a need in the SPC platform to accommodate the service binding establishment for mobile users. Regardless of the schemes used at the client side to maintain the session, the network itself needs to adapt to the user movements, otherwise the session continuity efforts at the client becomes useless. Such process of service binding accommodation is closely related to the authentication procedure. In what follows, the authentication steps and their relationship with the service binding establishment are presented.

In a static scenario, at subscription time, a user will send her credentials to the AN when requested. By authenticating the credentials, the SPC access platform would allow this user traffic into the network. Once the user is authenticated, she can access a web portal in which Network Service Providers as well as services to be accessed are selected. However, if a certain service session is to be maintained when the user changes her point of attachment, such authentication/service selection process is not appropriate and a more dynamic authentication process is used as explained in section 3.1.7. The unavoidable authentication procedure should enable the automation of the service selection process so that the user experience is not degraded.

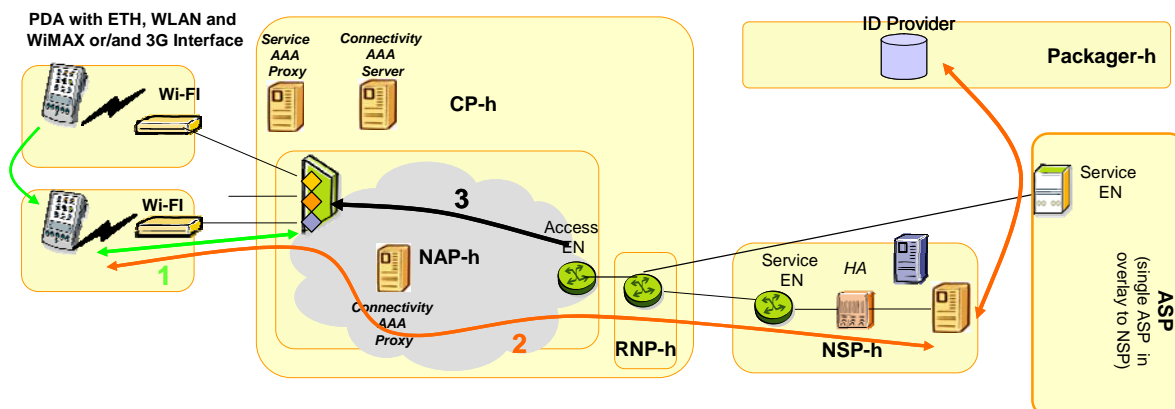


Figure 8-1. Service binding update due to authentication

Figure 8-1 depicts the case in which a user who is already accessing his service at his initial location, moves to a different point of attachment. The steps that take place are the following:

1. The MS moves, the new point of attachment requests authentication and the MS sends necessary credentials stored in its SIM card. It should be noted that the way the new point of attachment requests authentication depends on the technology used. In this example a Wi-Fi is used and accordingly, 802.1X is the access control technology that applies. Note that a CAPWAP tunnel should be included to reflect the role separation between the AP (only radio related) and the AN (authenticator) as shown in [3].

2. Based on authentication information, the EN realizes that the service binding in the serving AN already exists but some info needs to be updated. Section 8.1.1 details which type of information could be included in the authentication messages so that the service binding update can be done.
3. The EN updates the service binding in the AN by means of EAP message. As long as the user credentials are valid for the new point of attachment and the necessary information for the service binding is correct, the EN can apply the necessary changes.

### 8.1.1 Service binding information within authentication messages.

As stated before, the information contained in the authentication messages could be used for the establishment of the service bindings.

Table 8-1 summaries how this information is transported. The first column identifies the type of information that is transported. The second column details the field or attribute of the authentication messages in which the information is encapsulated. The last column specifies which entity along the authentication chain introduces the mentioned information in the specific field or attribute

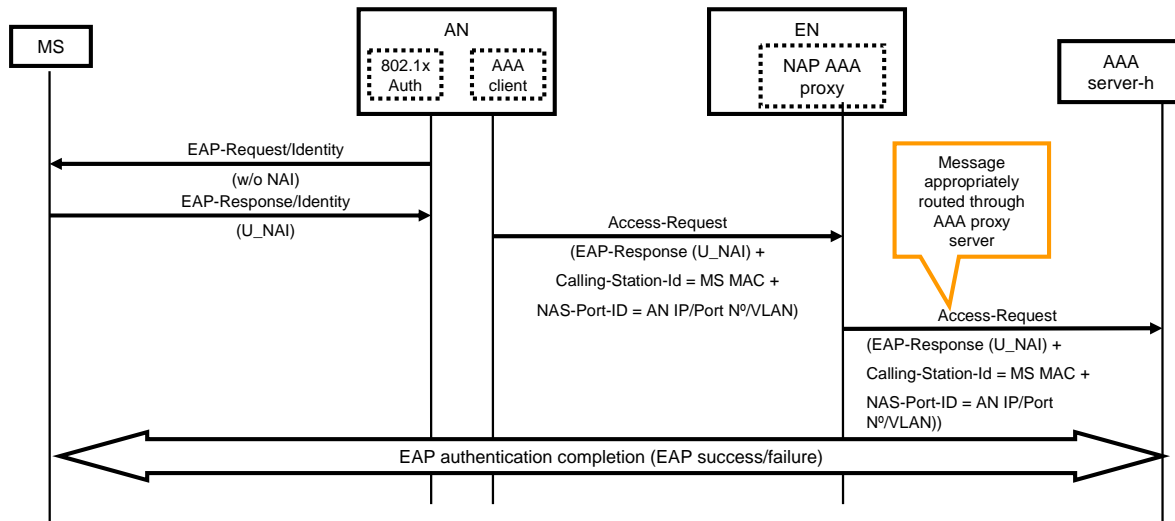
Information	Field or Attribute	Entity introducing the info
User name, domain and service description	<i>NAI (Network Access Identifier)</i> . It follows the username@realm notation. In this case the realm information could be extended to include the service description. E.g: <i>user@hsi.accessnet.com</i>	Generated by the client and introduce in EAP-Packets.
MAC address of the user terminal	<i>Calling-Station-Id RADIUS attribute</i> . This is prepared for some sort of identification of the Calling Station which in this case is the end user terminal	Introduced by the RADIUS client at the AN
AN id	<i>NAS-IP-Address RADIUS attribute</i> . As long as the AN can be identified by its IP address, this attribute could be used	Introduced by the RADIUS client at the AN
AN port definition	<i>NAS-Port-Id RADIUS attribute</i> . It is a string that allows the description of the AN port including interface type, port number, vlan etc	Introduced by the RADIUS client at the AN

Table 8-1. Service binding information mapping into authentication messages

The message flow presented in

Figure 8-2, includes all the parameters and attributes explained in

Table 8-1. It illustrates the type of information carried during the authentication process.



**Figure 8-2. Authentication Messages containing service binding information**

The first EAP-Response/Identity message, carried in an EAPOL frame in this case (the access control depicted is 802.1X) is then encapsulated into an Access Request (this is the RADIUS message). As shown, the NAI identifier is carried within the EAP Response within the Access Request. However, this is not the only information contained in the Access Request, since the AN introduces further information. As illustrated, the end user device MAC address is introduced thanks to the *Calling-Station-Id* attribute as well as the AN port description, which is included into a *NAS-Port-ID* attribute (since this attribute can also contain the NAS IP address it might be unnecessary to use an extra attribute, namely *NAS-IP-Address*, for this purpose)

### 8.1.2 Key management for Handovers

Regardless of the access technology used (Ethernet, WLAN, etc) in the SPC, the authentication process relies on the EAP framework (Ethernet and WLAN use EAPOL and WiMAX uses PKM to carry EAP messages). The current model of EAP requires the peer to engage in a full EAP exchange with the EAP server in its home domain every time the peer needs to re-affirm access to the same authenticator or moves from one authenticator to another.

In order to overcome the delay caused by this “re-authentication” scheme, there are different solutions. However, all of these solutions are either EAP lower layer specific and/or EAP method specific, while a more general solution capable of a faster re-authentication is desired. The extension of the EAP protocol to enable EAP re-authentication is an ongoing work that is being carried out by the Handover Keying (HOKEY) WG of the IETF.

The main idea of the extension of EAP for re-authentication is the definition of new EAP messages that enable EAP peers to prove their identity in a faster manner in the subsequent authentication phases once the peer had successfully authenticated at the first point of attachment. As result of the first authentication, the peer derive a Re-authentication Root Key (rRK) from the EMSK (non of them are handed out afterwards) which at the same time is used to derive new keys to proof peer key possession. The new EAP messages described in [18] make use of the derived keys to shorten the authentication process and to authenticate the peers in the new point of attachment (or to re-authenticate users in the same point of attachment). The process explained in [18] is illustrated in the following Figure 8-3:

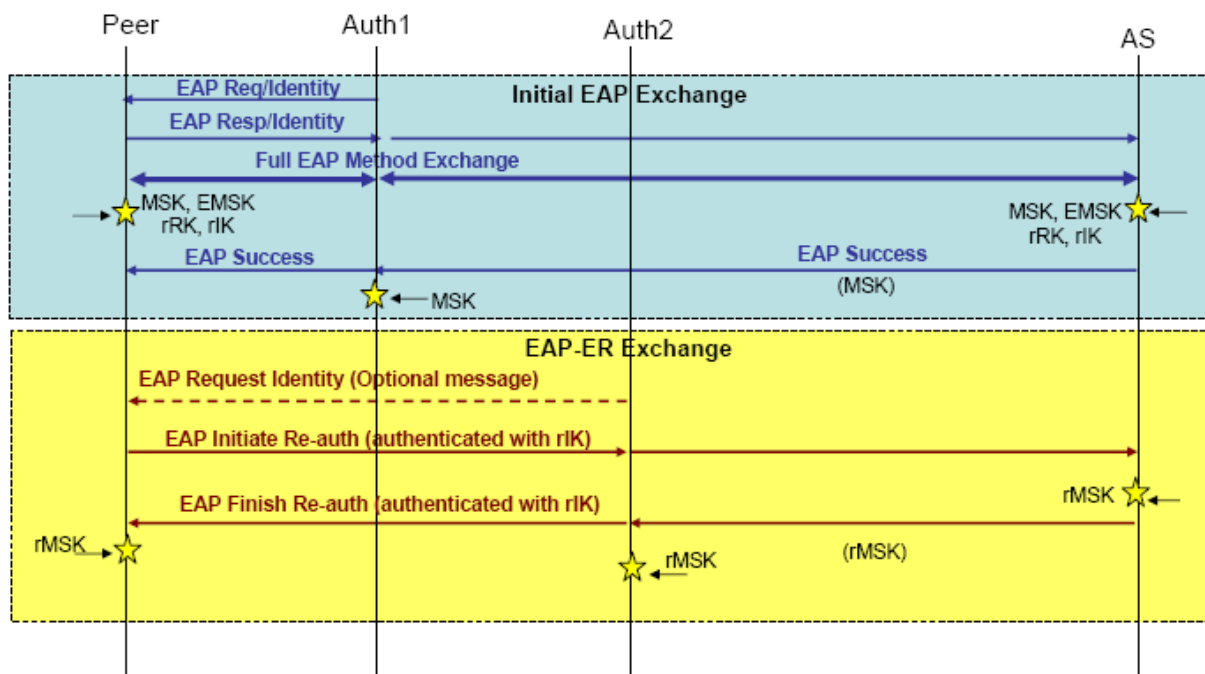


Figure 8-3. EAP Re-authentication message exchange

From the point of view of the SPC platform, the implementation of this approach is really attractive since it improves the handover time when different technologies are being used. This is due to the fact that Ethernet as well as WLAN rely on EAP as the upper layer for authentication.

## 8.2 L2 Micro-mobility and Authentication

There are certain cases in which the continuation of the session does not imply special actions for the moving end user's device. Those are the cases in which maintaining the same IP address is enough for the end user device to keep sessions alive. This is the situation for the use case 1 described in section 4.1.1. Even though the solution proposed for these cases is specific and not generic, including certain features in the SPC could help to enhance the performance for this micro-mobility. In this case micro-mobility refers to the mobility of the user in a limited domain where the same IP address could be maintained, i.e., served by the same EN or the same AN.

One of these scenarios is the case of a moving user hopping between different Wi-Fi access points. Regardless if this user is moving within the same or different SSIDs, maintaining the same IP address is enough to maintain the session. In any of these cases, service binding handling as described above would be necessary from the network perspective.

From the authentication perspective, the choice of the authentication protocols and methods will impact the handover time and the end user perception accordingly. In the case of Wi-Fi access there are several enhancements that could be used in order to improve its performance. Particularly interesting for the SPC work is the usage of 802.1X pre-authentication which is detailed and discuss in the following section.

### 8.2.1 802.1x pre-authentication

This enhancement to 802.1X authentication is presented in [19] and is aimed at speeding up the authentication process of a 802.11 MS by doing an authentication with a new point of attachment before actually moving to this point of attachment. The main principle, as depicted in

Figure 8-4, is that the serving AP is used to communicate with the target AP via the distribution system that connects both APs together. Hence, the MS will exchange all the authentication information with the target AP via the serving AP. Once the authentication is done, the MS could move to the new AP, where access would be granted for it.

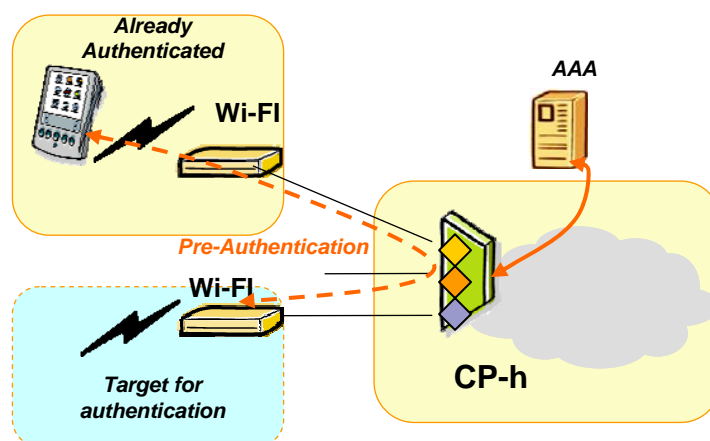
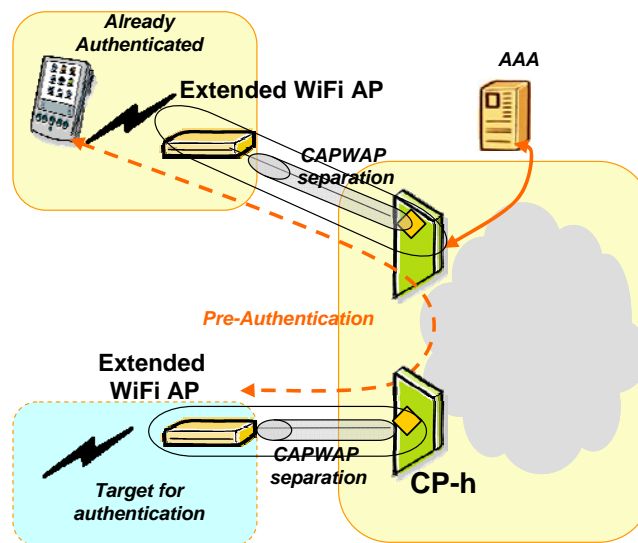


Figure 8-4. 802.1X pre-authentication principle

For this scenario to be completely inline with MUSE requirements regarding trust of RGW devices, the CAPWAP approach should be applied. As described in [18], this approach enables the separation of the radio and the management functions for the APs. In this situation the authenticator function of the AP is located at the ANs. However, this fact does not change the pre-authentication principle described above. The only difference is that the authenticator entity for each AP is located at the AN instead of being physically located at the AP itself. This is depicted in Figure 8-5. However, for the sake of simplicity, the remaining text refers only to the APs as whole (regardless if the functions are physically separated or not, the AP could still be seen one element)



**Figure 8-5. Pre-authentication principle for extended APs due to the separation proposed by CAPWAP.**

As described in [19], there are a number of issues related to 802.1X pre-authentication deployment:

- The MS starts the authentication with the target AP. There should be a mechanism through which the MS decides which is the best AP to move to. This mechanism is not defined by the 802.1X pre-authentication and could be based on basic signal strength measurements or on more sophisticated mechanism as describe in [20] and [21] where a Frequent Handover Region (FHR) is defined.
- In order to forward the 802.1X pre-authentication packets correctly to the target AP, the BSSID of the target AP is used as its MAC. This might have certain configuration constrains
- Another Ethertype is defined to differentiate between 802.1X pre-authentication frames and normal 802.1x frames. This is due to the switch traversal problem of 802.1X messages.

As stated before, the distribution system that connects the APs is used to forward the 802.1X messages between the MS and the target AP. Hence, layer 2 connectivity between APs is required because 802.1X is encapsulated directly over L2 frames. For this communication to take place in the SPC platform there are two different approaches that could be taken:

1. The first approach would be that messages between APs are forwarded via EN. This way, the forwarding principles of the SPC platform persist.
2. Another possibility would be to configure the intermediate switches in the aggregation network to permit inter AP communication. This mechanism would go against the SPC forwarding principles but would still be possible

### 8.2.2 Pre-authentication and Service Binding

Pre-authentication has been presented as a mean to speed up the handover process in a 802.11 environment, however within the SPC platform its make before-break principle, could be very beneficial for the service binding establishment.

As presented before the information carried into an authentication process could be used to take service binding establishment decisions. At the same time, the pre-authentication enables the authentication of MS with its future AP by means of its serving AP. This implies that the authentication messages containing service binding information, traverse the network before the MS actually moves. Combining these two solutions together would enable the service binding creation/update before the actual movement of the MS occurs, easing the continuation of the sessions at the client side.

One important issue regarding this approach is the next hop (or target AP) selection. Pre-authenticating to several AP would create different service bindings. This situation is undesirable from the performance and security point of view. Accordingly the appropriate mechanism for the next hop selection becomes crucial for this scenario. At the same time limiting the number of pre-authentications permitted, would reduce the scope of this problem.

### 8.3 L3 Mobility and Authentication

The cases which are not under the L2 micro-mobility scope presented in section 8.2 need special measures to achieve session continuity. The reason for this is that all these scenarios need a change in the IP address assigned to the MS. In some cases, the IP change is due to a change into the access technology used. In some other cases, the network management policy would force this new IP address acquisition (e.g, two remote places receive IP addresses from different DHCP servers with different IP pools). This situation is inline with the use case 2 (see section 4.1.2) as described by the use case analysis performed in section 4.2 about the possible mobility scenarios.

As stated in Chapter 6.2, the proposed solution for these scenarios is MIP, which enables the continuation of end user sessions when the device's IP address changes. On the other hand, the main authentication solution used in the SPC platform, when it comes to mobility and nomadism, is based on 802.1x and EAP-SIM. In principle, the combination of both solutions is straightforward; when a MS moves between networks it has to authenticate first in order to get the authenticator port opened. Once the MS is authorized in an access port the MIP signalling can take place. This is the basic solution proposed for the SPC platform regarding authentication and mobility management.

The problem of this approach is, of course the delay introduced as result of the chained message exchange (first authentication and then mobility management). Next section presents a novel initiative aimed for enhancing the handoff performance by means of pre-authentication. The implementation of this feature is not straightforward in the SPC platform but could be useful to decide future steps (it should be understood as possible future work).

When talking about L3 mobility, it is important to emphasize the statements presented in sections 8.1 and 8.1.1, regarding the L2 network adaptation. Even though the session at the end user side are maintained thanks to MIP, the access network still needs to react on end user movement and update the service binding accordingly. For this reason, the mechanisms explained before regarding the service binding information sent within the authentication messages are still valid and should be used also in L3 mobility cases.

### 8.3.1 Media independent Pre-Authentication (MPA)

Different approaches have been presented in the last years, in order to improve the handover or the handoff performance. Each of them tries to reduce the handoff time exploiting one specific feature related to the mobility process e.g. some initiatives try to reduce the time needed to decide which is the most suitable next hop, like CARD (Candidate Access Router Discovery) [22]; others, like CTP (Context Transfer Protocol) are designed to carry state that is associated with the services provided for the mobile terminal, or context, among access routers. However, most of them, like Fast Mobile IPv4/v6 are bounded to one mobility management protocol in particular and propose enhancement to these specific protocols.

Within the IP Mobility Optimizations (Mob Opts) Research Group (part of the IETF) there is a novel initiative which describes the Media-independent Pre-Authentication (MPA) [23], a new handover optimization mechanism that addresses the issues on existing mobility management protocols and mobility optimization mechanisms to support inter-domain handover. MPA is a mobile-assisted, secure handover optimization scheme that works over any link-layer and with any mobility management protocol and is best applicable to support optimization during inter-domain handover.

Even though MPA is in an early stage, it could be very beneficial for the future development of the SPC platform in the case of an inter-technology type of handover. The idea behind MPA is the same as that of 802.1x pre-authentication, but in this case is extended to work on higher layers.

The principle behind MPA operation as described in [23] is the following. A MS should be able to obtain an IP address and further configuration parameters in a secure manner, as well as to send IP packets before it actually attaches to the Candidate Target Network. For this purpose MPA defines four basic procedures. The first one is referred to as "pre-authentication", the second is referred to as "pre-configuration", and the combination of the third and fourth procedures are referred to as "secure proactive handover".

The pre-authentication should enable the creation of a security association between the MS and the CTN, named "PMA-SA". This security association is the base for running a configuration protocol in a secure manner which constitutes the pre-configuration phase. Then the PMA-SA is used to execute a tunnel management protocol to establish a PHT (Proactive Handover Tunnel) between the mobile node and an access router of the CTN. After that, the MS is able to send and receive IP packets, including signaling messages for binding update of the Mobility Management Protocol (MMP) to be used as well as data packets transmitted after completion of binding update. The final step is to delete or disable the PHT immediately before attaching to the CTN when it becomes the target network and then re-assigning the inner address of the deleted or disabled tunnel to its physical interface immediately after the mobile node is attached to the target network through the interface.

MPA does not specify the protocols to use for each of these procedures and only explains the framework for them to work correctly. Furthermore the work presented [24] exemplifies a possible implementation for MPA with its first implementation results. One of the cases presented in [24] discusses the usage of MIPv6 as the MMP. This mobility management is similar to the one proposed for the SPC work.

The main difference between the implementation proposal and the current status of the SPC platform is the authentication mechanisms. From the MPA point of view, an IP based authentication mechanism is more convenient, because it is possible to use the same IP to communicate with the authenticator but also with the correspondent peers in any other session. With this respect one of the innovations needed in the SPC platform would be to enable some sort of IP based authentication e.g. PANA (this is the method suggested in [24]). Besides that, a best candidate discovery mechanism should be enabled in the platform so that the MS is able to identify which is the best network to move to. The requirements to fulfill the pre-configuration could be easily met by the DHCP servers implemented in the platform. The other issue that would need to be addressed is the management of the tunnel for the pro-active secure handover. As proposed in [24] the most straightforward implementation would be an IPSec tunnel. This tunnel could be bootstrapped by the PANA procedure (in case PANA is used as the IP based authentication method)

## 8.4 Conclusion

The main conclusion of the described work is that the unavoidable steps of authentication and authorization could be linked to the adaptation process needed by the SPC platform to provide session continuity. The forwarding mechanisms described for this platform impose the creation, deletion and update of the service bindings which are tightly related to the user profile. The information contained in the authentication messages is inline with the one needed for the service bindings and so it can be used for the adaptation process. In the cases where the handover of the session is to be done within the same L2 domain we can conclude that there are available standards that can be used to speed up the handover and so ease the continuation of the session. With this regard the pre-authentication described in IEEE 802.11i fits perfectly within the SPC platform in case WLAN is used as the access technology.

For other cases, where the handover has to be treated in higher layer the conclusion is that the authentication is not able to provide standard mechanisms to speed up the process. However the main standard tracks of interest for SPC were identified through the course of this document.

## 9 MIP IMPLEMENTATION

As can be seen from the analysis of the use cases [in Chapter 4-2](#), session continuity can be supported as long as the user terminal maintains the same IP address in the new attachment point. This requirement is of course by far too restrictive. In a realistic scenario, user mobility should not be constrained within the same subnet and thus the layer 3 mobility management, such as MIP, should be to support all the “mobility types” identified from the use cases.

One of the tasks of WPC4, is to demonstrate the concept of session continuity, in a Lab environment, and the work for this is on going within SPC4 activity. In the following we describe a summary of the specification and implementation of MIP based deployment to support session continuity.

### 9.1 MIP for Windows

The IPv6 protocol for Windows provides correspondent node support as described in the draft titled "Mobility Support in IPv6" (now RFC 3775) [25]. The IPv6 protocol for Windows does not provide mobile node or home agent support. By default, the correspondent node functionality is disabled and binding updates are required to use the IPSec Authentication Header (AH) for authentication. The correspondent node functionality can be enabled manually.

A Mobile IPv6 Technology Preview has been developed by Microsoft Research and supports full correspondent node, mobile node, and home agent functionality for computers running various versions of Windows. However, this software is not currently available to the public. Microsoft will consider making a version of Mobile IPv6 available for use in the future if there is sufficient customer demand.

A Windows solution would be a simple option due to the fact that so far all the clients in the SPC platform are Windows based. The software used for user authentication has been

extensively tested in this environment. However, as exposed above, Windows does not have any implementation of MIPv6 MN. No other client software could be found and apparently Microsoft has no MIPv4 development either.

## 9.2 MIP for Linux

The few existing MIPv4 packages in Linux were implemented in old kernels and should be avoided. If Linux is to be used the solution must therefore be based on Mobile IP for IPv6, MIPv6.

Implementation of the IPv6 stack in the Linux kernel has been around for years. The installation of the IPv6 networking stack in a Linux machine can be simply achieved by compiling the Linux kernel with an experimental option named "Internet Protocol Version 6" in the Networking section. However, the IPv6 protocol stack of generic Linux kernel was too buggy and was not fully conformed to the IPv6 specifications. Due to lack of maintenance, some parts of the stack were out of date.

In this context, the USAGI (Universal Playground for IPv6) project [26] was launched. The USAGI Project aims to improve IPv6 environment on Linux and to spread the deployment of IPv6 in a worldwide scale. Today this project concentrates on MIPv6 development for Linux 2.6. Several improvements have been added to the kernel, libraries and applications. Many of their efforts have been merged into the mainline Linux kernel tree, 2.6 especially.

Although MIPv6 for Linux seems to be promising one obvious requirement is that the underlying network must support IPv6 traffic. The SPC platform currently supports only IPv4 traffic and therefore extra mechanisms should be used in order to utilize the MIPv6 implementation. One of the possible ways is to use tunneling techniques.

## 9.3 MIPv6 over IPv4

Since the SPC platform is IPv4-only any IPv6 traffic must be transmitted over IPv4. The 6to4 mechanism [27] allows one to send IPv6 packets over a pure IPv4 network without need for explicitly configuring tunnels. The IETF (expired) draft "IPv4 over 6to4 and 6to4 mobility" [28] adds value to the first one by outlining how a 6to4-enabled host can be provided with transparent IPv4 and IPv6 connectivity and mobility no matter if the host is located in a 6to4 network or is roaming in an IPv4-only network. The procedure allows one to use MIPv6 and 6to4 without any changes and without any new protocols. Please refer to the drafts for further details not covered in the present document.

In this solution the MN is an IPv4/IPv6 dual stack terminal, which knows the IPv4 address of a 6to4 router. The MN IPv6 CoA is generated by the MN as a 6to4 address using the current IPv4 address. When the MN moves, the IPv4 address is changed and the IPv6 CoA is regenerated as a new 6to4 address. The new IPv6 CoA triggers the MIPv6 to update the HA.

The MIPv6 HA is situated in an IPv6 part of the BlueNet service network. This part could be IPv6-only or dual stacked. In the IPv6-only case there is a need for a 6to4 border router connected to the IPv4 part of the network. In the dual-stacked case, the 6to4 router is implemented within the HA node. In this architecture the Correspondent Node must be a

MIPv6 enabled node installed in an IPv6 network. It gets the MN HoA from the HA when the MN starts the session.

Although the solution seems to be neat there is currently no known implementation of this draft. Therefore MIPv6 using 6to4 cannot be used in the SPC platform.

## 9.4 Dual Stack MIPv6

The Dual Stack MIPv6 (DSMIPv6) [29] is an extension of MIPv6 with IPv4 capabilities, with the aim of offering mobility of both IPv4 and IPv6 traffic using only one protocol. All MIP related control traffic (e.g., binding update) uses the original MIPv6 protocol with IPv4 extensions to announce also IPv4 home addresses and IPv4 care-of addresses. Both IPv4 and / or IPv6 traffic can furthermore be tunnelled over both IPv4 and / or IPv6 (all 4 possible combinations). Please refer to the draft for further details not covered in the present document.

The draft specifies a mechanism to enable one to run the dual stack MIPv6 over a pure IPv4 network. The steps for achieving session continuity follow:

- MN and HA will set up two tunnels with pre-configured end points:
  - IPv6 over IPv4 tunnel: HA IPv6 address – MN IPv6 HoA
  - IPv4 over IPv4 tunnel: HA IPv4 address – MN IPv4 HoA
- Optionally the MN can be authenticated by the network;
- MN gets an IPv4 CoA in the access network by DHCP;
- MN creates an IPv6 CoA mapped from the IPv4 CoA;
- MN sends binding update with both CoAs and HoAs to HA;
- HA updates its binding cache for the MN.

The dual stack MIPv6 was implemented by Ericsson in an internal project based on MIPL for Linux kernel 2.6.16 and the current version is 2.6.16.36. It has a modification of the source address selection so the HoA is always selected for IPv6 traffic. It has all four combinations of IPv4 and IPv6 tunnels implemented. The code consists basically of a kernel, a MIPv6 daemon (*mip6d*) and some monitoring tools.

The *mip6d* daemon runs in user space. When it detects the link state “link up” a DHCP request is triggered. After the IPv4 address is assigned, the 6to4 tunnel is reconfigured by the daemon. Then the MIPv6 binding update is performed. The whole handover process takes approximately 3 to 5 seconds.

Initial tests with the code were performed in the RedHat Enterprise 4 using a Cisco router between MN and HA. The traffic between the MN and the corresponding node was generated by ping and web surfing. In order to see what was happening at network level

Ethereal, *netstat*, *ifconfig* and the DSMIPv6 monitoring tools themselves were used. It was possible to verify the correctness of network addresses, routing tables and tunnels. It was also possible to see the traffic being forwarded between MN and HA, MN and Internet. When the underlying IPv4 address of the MN was changed one could see the session continuity happening.

Since the DSMIPv6 package could perform the initial tests previously described in a standard IPv4 network it was the chosen solution for the SPC platform network.

## 9.5 MIP Deployment

For the reasons outlined in the previous subsections the dual stack mobile IPv6 package was chosen to be used for the lab deployment in the SPC platform. Since the SPC platform is a pure IPv4 network two tunnels have to be set up with pre-configured end points. The first one is an IPv6 over IPv4 tunnel. It starts in the home agent (IPv6 virtual interface) and finishes in the mobile node (IPv6 HoA). The second one is an IPv4 over IPv4 tunnel. It starts in the home agent (IPv4 address) and ends in the mobile node (IPv4 HoA).

For the lab deployment two new machines were installed. The first one is a client laptop (the mobile node) running Enterprise RedHat 4. The DSMIPv6 package was installed on this machine. No VLANs were needed since both test scenario uses only one service at a time. The second machine is the home agent and it also runs Enterprise RedHat 4. This machine was installed in the BlueNet network with a local IPv4 address. The client is connected to the access network and also possesses a home address from BlueNet address space. This scenario is depicted in Figure 9-1.

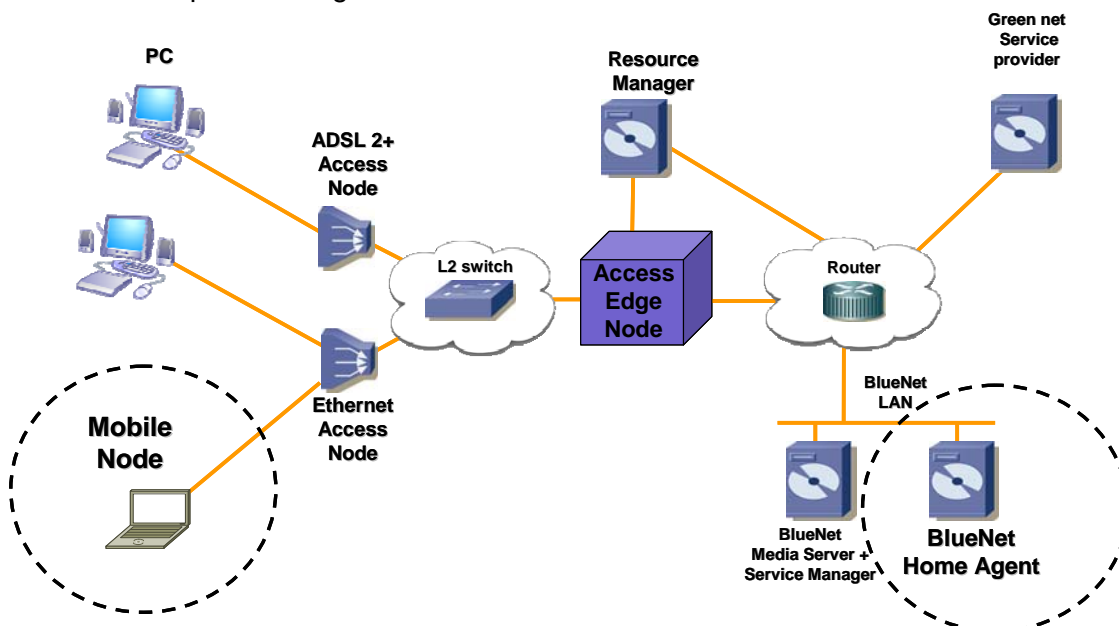


Figure 9-1 - MN and HA installed in the prototype

The results from the demo arrangement will be conducted and the results will be presented in another deliverable.

## 10 CONCLUDING REMARKS

In MUSE phase II, Work Package C1 (WPC1) of Sub-Project C (SPC) was tasked to deliver three deliverables. In the first deliverable, DC1.5, a network architecture solution for supporting nomadic users in a dual packager multi provider scenario, using Ethernet, xDSL or Fibre first mile technology was presented. This was achieved by enhancing the Resource Management, Policy Control and Authentication and Authorization (AA) mechanism of the SPC network architecture. Next, in deliverable DC1.6, the solution of DC1.5 was enhanced to support nomadic users using wireless access technologies, such as public WLAN access points or “hotspots” such as privately owned public WLAN access points. In this last deliverable, DC1.7, we address the issue of session continuity, for intra SPC network mobility.

Providing a complete solution of session continuity for different types of applications in heterogeneous networks is of course a very complex task, which can not be solved within the scope of this deliverable. Therefore, the main focus of this deliverable has been to analyze some typical “user mobility” cases and suggest layer-2 and layer-3 mobility solutions to support session continuity. Some innovative methods of binding the AA procedure with the layer 2 connections provisioning is presented. To complement the analysis, some simple experimental tests were conducted, where we looked at the impact of different link layer interfaces and applications, running on different Operation Systems, to session continuity.type layer 2 and layer 3 based session continuity. The ideas developed in this deliverable are now being used in specification and implementation of MIP based deployment to support session continuity.