OverDRiVE

IST-2001-35125 (OverDRiVE)

D07

Concept of Mobile Router and Dynamic IVAN Management

Contractual Date of Delivery to the CEC:	31/03/2003
Actual Date of Delivery to the CEC	31/03/2003
Author(s):	Miklós Aurél Rónai (Editor, ETH), Christoph Barz (UBN), Matthias Frank (UBN), Christian Maihöfer (DC), Alexandru Petrescu (CRM), Markus Pilz (UBN), Octavian Pop (ETH), Ágoston Szabó (ETH), Jens Tölle (UBN), Ralf Tönjes (EED), Michel Wolf (DC)
Participant(s):	Ericsson, DaimlerChrysler, Motorola, University of Bonn
Project Title:	Concept of Mobile Router and Dynamic IVAN Management
Workpackage contributing to the Document:	WP3
Estimated Person Month:	35
Security Type: (Int/Res/IST/FP5/Pub)[1]	Pub
Document Number[2]:	IST-2001-35125/OverDRiVE/WP3/D07
Nature of the Document[3]:	(R)eport
Version (Status of the Document: D1/R1/D2/R2/F)[4]:	V1.1 (F)
Total number of pages:	93

[1] *Int* *Internal circulation within project (and Commission project Officer if requested)*
Res *Restricted circulation list (specify in footnote) and Commission PO only*
IST *Circulation within IST Programme participants*
FP5 *Circulation within Framework Programme participants*
Pub *Public document*

[2] Format: IST-2001-35125/OverDRiVE/<source>/<Deliverable Number: Dxx | Running Number for other: Rxx>:
Example: IST-2001-35125/OverDRiVE /WP1/D01 (Document comes from the WP1)

[3] (R)eport, (P)rototype, (D)emonstrator, (S)pecification, (T)ool, (O)ther

[4] V0.x=Draft, V1.x=Final. (D1=First Draft, R1=Technically Revised, D2=Final Draft, R2=Final Revised, F=Final)

Abstract: This deliverable describes the OverDRiVE concepts to connect an Ipv6 based network inside a vehicle to the Internet. These concepts comprise the Mobile Router and dynamic IVAN management. Taking the OverDRiVE requirements and scenarios into account, existing solutions for IP-based mobility management are evaluated. Based on this evaluation, Mobile Ipv6 is enhanced to support mobility of an entire network. As an optimized mobility management inside large IVANs is favoured, also interactions of micro-mobility approaches with Mobile Ipv6 are evaluated. The concept for dynamic IVAN management covers in detail the OverDRiVE trust model, network access control in mobile environments with respect to an IVAN and its interaction with an AAA infrastructure. Additionally, traffic management concepts are laid out to provide means for shaping the traffic for Mobile Router's wireless links. In particular, the Mobile Router will support multi-access. Finally, the interaction between mobility management and IVAN management is shown.

Keyword List: mobility management, mobile network, mobile router, tunnelling, mobile multimedia, multi-homing, multi-access, access control, traffic shaping

Revision History

Revision	Date	Issued by	Description
V0.0 (D)	2002/11/01	M. Petrescu M. Pilz	Started Document – proposed TOC
V0.1 (D)	2002/12/18	WP3 (Guildford)	Detailed TOC
V0.2 (D)	2003/01/08	M. A. Rónai	Authors added
V0.3 (D)	2003/02/24	M. A. Rónai	Compiling the partner's input
V0.4 (D)	2003/02/25	M. Wolf	Text added to chapter 2.
V0.5 (D)	2003/03/03	M. A. Rónai	Text added to chapter 2, executive summary added, acronyms added, some references added, CRM input added
V0.6 (D)	2003/03/04	M. A. Rónai	Reorganized BCMP and HMIP in ETH's section, moved BCMP to tunnel approaches in DC's section, Multi-homing added, History of HMIP extended, Keio proposal added, more UBN contribution added, removing unneeded acronyms
V0.7 (D)	2003/03/06	M. A. Rónai	New abstract added, ETH contribution to chapter 4
V0.8 (D)	2003/03/10	M. A. Rónai	Compiling partner's input
V0.9 (D)	2003/03/12	M. A. Rónai	Compiling partner's input, repairing the references
V0.10 (D)	2003/03/14	C. Barz	Refining access control
V0.11 (D)	2003/03/16	M. A .Rónai	Finalizing the document
V0.12 (D)	2003/03/18	M. A .Rónai	Some minor changes, ready for technical review
V0.13 (R1)	2003/03/19	M. A .Rónai	Technically reviewed doc, adding the suggestions of the reviewer
V0.14 (R1)	2003/03/22	M. A .Rónai	Changes mainly by A. Petrescu, removing not named and not referenced figures, ready for political review
V0.15 (R1)	2003/03/22	M. Pilz, C. Barz	Some minor changes and corrections
V1.0 (R2)	2003/03/31	M. A .Rónai	Politically reviewed doc, closing the document
V1.1 (F)	2003/03/31	M. A .Rónai	Some very last corrections

Concept of Mobile Router and Dynamic IVAN Management - Table of Contents

Acronyms

AAA	Authentication, Authorisation, Accounting
AAAF	Foreign AAA server
AAAH	Home AAA server
AAAL	Local AAA server
ACS	Access System
ANP	ANchor Point
AR	Access Router
BAck	Binding Acknowledgement
BAN	Body Area Network
BCMP	BRAIN Candidate Mobility Protocol
BG	Border gateway
BGP	Border Gateway Protocol
BR	Border Router
BRAIN	Broadband Radio Access for IP based Networks
BReq	Binding Request
CAN	Controller Area Network
CBQ	Class Based Queuing
CN	Correspondent Node
CoA	Care-of-Address
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DRR	Deficit Round Robin
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DRiVE	Dynamic Radio for IP-Services in Vehicular Environments
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
DVB	Digital Video Broadcast
DVB-T	Terrestrial Digital Video Broadcasting
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
FMIP	Fast Mobile IP
GPRS	General Packet Radio Service
GSR	Global State Routing
GW	Gateway
HA	Home Agent
HAWAII	Handoff-Aware Wireless Access Internet Infrastructure
HBR	Host Based Routing
HMIP	Hierarchical Mobile IP
HMIPv6	Hierarchical Mobile IP version 6
HO	Handover
HoA	Home Address
HSR	Hierarchical State Routing
ICEBERG	Internet Core Beyond the Third Generation
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force

IP	Internet Protocol
IPSEC	Internet Security Protocol
IPv4	IP version 4
IPv6	IP version 6
ISP	Internet Service Provider
IST	Information Society Technologies
IVAN	Intra Vehicular Area Network
LAN	Local Area Network
LCoA	Local Care-of-Address
LFN	Local Fixed Node
LMN	Local Mobile Node
MANET	Mobile Ad hoc NETworks
MAP	Mobility Anchor Point
MER-TORA	Mobile Enhance Routed – Temporally Ordered Routing Algorithm
MH	Mobile Host
MHTP	Multi Homing Translation Protocol
MIND	Mobile IP-based Network Development
MIP	Mobile IP
MIPv6	Mobile IP version 6
MLD	Multicast Listener Discovery
MMP	Multicast for Mobility Protocol
MN	Mobile Node
MONET	MObile NETwork
MOST	Media Oriented System Transport
MR	Mobile Router
MRHA	Mobile Router – Home Agent bidirectional tunnel
MRTP	Mobile Router Tunnelling Protocol
MS	Mobile Station
MSN	Multi Access Support Node
MT	Mobile Terminal
MTU	Maximum Transfer Unit
MU	Mobile User
MURP	MIND User Registration Protocol
NAT	Native Address Translation
ND	Neighbour Discovery
NEMO	NEtwork MObility (working group)
ORC	Optimized Route Cache Management Protocol for Network Mobility
OSPF	Open Shortest Path First
OverDRiVE	Spectrum Efficient Uni- and Multicast Services over Dynamic Multi-Radio Networks in Vehicular Environments
PAN	Personal Area Network
PANA	Protocol for carrying Authentication for Network Access
PDA	Personal Digital Assistant
PIM-{SM|DM}	Protocol Independent Multicast – {Sparse Mode | Dense Mode}
PPP	Point-to-Point Protocol
PSBU	Prefix Scoped Binding Updates
QoS	Quality of Service
RA	Router Advertisement
RCoA	Regional Care-of-Address
RFC	Request For Comments
RIP	Routing Information Protocol

RIPng	Routing Information Protocol next generation
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
THEMA	Transparent Hierarchical Mobility Agents
TLA	Top Level Aggregation
TORA	Temporally Ordered Routing Algorithm
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UR	User Registry
USB	Universal Serial Bus
UTRAN	UMTS Terrestrial Radio Access Network
VMN	Visiting Mobile Node
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

Executive Summary

The OverDRiVE project aims at UMTS enhancements and co-ordination of existing radio networks into a hybrid network to ensure spectrum efficient provision of mobile multimedia services. An IPv6 based architecture enables interworking of cellular and broadcast networks in a common frequency range with dynamic spectrum allocation (DSA). The project objective is to enable and demonstrate the delivery of spectrum efficient multi- and unicast services to vehicles. OverDRiVE issues are:

- Improve spectrum efficiency by system coexistence in one frequency band and DSA.
- Enable mobile multicast by UMTS enhancements and multi-radio multicast group management.
- Develop a mobile router, that supports roaming into the intra-vehicular area network [IVAN].

This report focuses on the latter point, investigating the idea of mobile hosts and mobile networks in vehicular environments. This research takes into account scenarios like smaller networks in passenger cars up to mobile networks in public transport vehicles (e.g. buses and trains) that comprise of a dynamic number of nodes. In these scenarios vehicles are seen as moving IPv6 networks which can use several access technologies to provide Internet connectivity. OverDRiVE denotes these networks as IVANs (Intra Vehicular Area Networks). The objective of OverDRiVE within this vast research area is to concentrate on two topics: Mobility management and IVAN management. Mobility management includes special issues like nesting of mobile networks, multi-radio access and mobility within large vehicles. Moreover, IVAN management tasks are regarded with respect to the authentication, authorization and accounting framework (AAA). Here, access control and the task of traffic management are considered.

Concerning the concept of a Mobile Router (MR) current approaches are investigated in detail for OverDRiVE's envisioned scenarios, reaching form basic constellations up to scenarios that include nested mobility, multi-access and micro mobility. The proposed concept for mobility management is based on bi-directional tunnelling between the Mobile Router and its Home Agent (MR-HA). This concept extends the well-known Mobile IPv6 host mobility approach to handle the network mobility. A detailed scenario analysis shows that the approach gives a solution for all required OverDRiVE scenarios. Furthermore, this concept leaves also room for enhancements, namely route optimization, multi-access and micro-mobility inside the IVAN.

The elaboration of a security threat analysis and a description of OverDRiVE's trust model are used as basis for a concept of Dynamic IVAN Management. Subsequently, a concept for network access control that utilizes an AAA infrastructure is laid out. This permits the roaming of nodes into an IVAN. This concept focuses on optimized signalling procedures to allow seamless handovers while preserving authentication and authorization functionalities. The utilization of comparable low bandwidth wireless links to connect whole networks to the Internet requires a traffic management concept to avoid overstressing the wireless link. The introduced traffic management concept can be used by the Mobile Router to protect the MR-HA tunnel by means of traffic shaping.

Finally, the integration of OverDRiVE concepts is shown by explaining the mechanisms of both mobility management and IVAN management. Here, co-operation is described by means of examples.

1 Introduction

Vehicular communication is expected to grow rapidly in the next years. While sitting and having idle time people want to use mobile multimedia services. Passenger cars and especially larger vehicles like buses or trains may have several users who could naturally form a local area network within the vehicle, an intra-vehicular area network (IVAN). The IVAN makes the case of a mobile network, which raises interesting new technical challenges. A mobile network may itself be a hybrid network, allowing its residing nodes to use various access interfaces. A mobile network should also appear as part of the backbone network infrastructure, supporting mobile nodes moving (topologically) into and out of the network. The mobile network is connected through the mobile router to the outside world (see Figure 1).

The mobile router should provide transparency of its (topological) mobility to its residing nodes; that is, its residing nodes should not perceive that the mobile router changes its point of attachment to the backbone network infrastructure. A mobile network may itself be one leaf IP-subnet or a tree of IP-subnets (nested mobility), with a mobile router serving to maintain its network connectivity with the backbone network infrastructure. The mobile router may support access to different types of access systems, hence enlarging its scope of mobility. In this case, the mobile router will need to support handover between different access systems. Moreover, authentication, authorization and accounting (AAA) need to be performed by the mobile terminals in the moving vehicles with regard to the used AAA mechanisms in the infrastructure.

OverDRiVE has defined a set of mobility scenarios that are used as a basis for the design of a mobility and security solution for moving networks. The core scenarios are the following:

- The IVAN moves and connects to several access systems
- Mobile Hosts (MH) move into or out of an IVAN
- MHs move inside an IVAN

The user might bring another moving network inside a mobile network by having a personal or body area network deployed (PAN/BAN). In large vehicles users are free to move around and connect to whatever access router (AR) provided to utilize seamless Internet connectivity. The architecture inside a large vehicle might not be flat but rather deploy a network of interworking entities to allow for certain optimizations regarding the mobility management protocols.

Looking in detail, three specific application scenarios are described:

- Nested Mobility: One MR is topologically below another MR
- Multi-Access: A MR might maintain more than one Internet connection to allow for optimizations and flow based routing approaches
- Mobility inside the mobile network.

In this document approaches and solutions are described in detail for the basic scenarios as well as for nested mobility, multi-access and micro mobility inside the IVAN. A bi-directional tunnel (MR-HA) approach extending the conventional Mobile IPv6 is used for handling the moving network mobility. A detailed scenario analysis shows that the approach gives a solution for all required scenarios but leaves also room for further enhancements, namely route optimization, multi-access support and mobility inside IVANs. Especially the mobility inside IVANs is addressed by investigating the interaction of the MR-HA tunnel with micro-mobility approaches (HMIP, BCMP, RIP/OSPF) inside the IVAN.

The dynamic IVAN management part focuses on the OverDRiVE trust model and derives a threat analysis for moving networks. In a further investigation it provides a concept for AAA management architecture with special focus on access control for mobile networks. A traffic management is introduced to provide means for protecting the MR-HA tunnel.

Finally, the overall integrated concept is shown by explaining the mechanisms of both mobility management and IVAN management by means of examples.

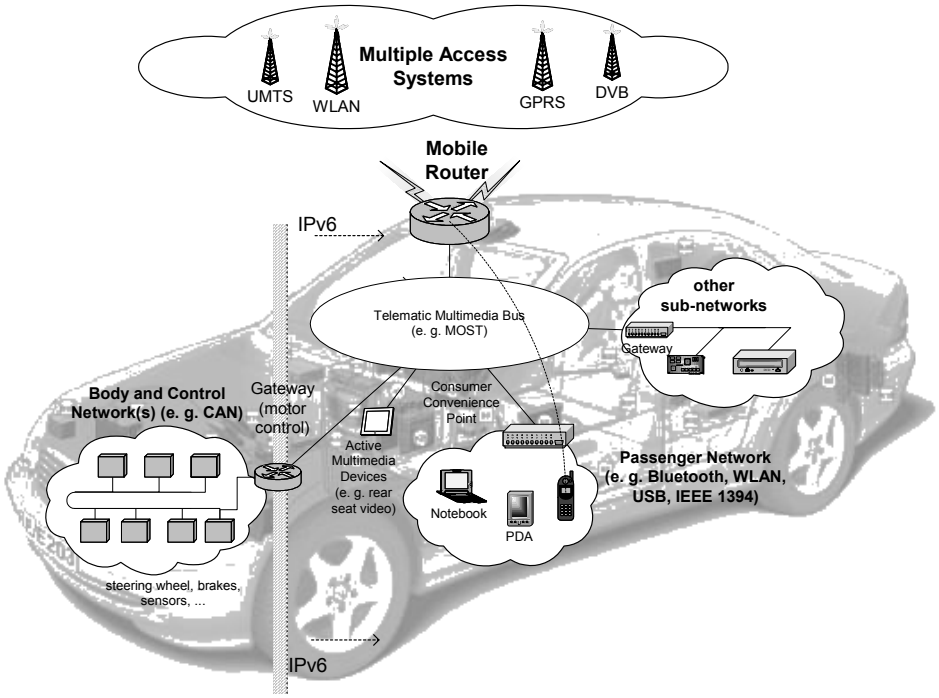


Figure 1: In-vehicle communication architecture

2 Concept of Mobile Router

2.1 Introduction

In this section we describe the requirements and the development of a design for a mobile router that serves as a connection point for a mobile network. The OverDRiVE requirements for network mobility support are presented first, in a list of generic aspects such as IPv6 architecture, transparency between network layer and transport layer, transparency of mobility management, reachability at a permanent home address and so on. We subsequently identify the Mobile IPv6 class of protocols as a solid basis to satisfy the requirements. These protocols are presented in detail and include: Mobile IPv6 (MIPv6) for hosts, Hierarchical Mobile IPv6 (HMIPv6), Brain Candidate Mobility Management Protocol (BCMP) and Dynamic Host Configuration Protocol (DHCP). The important identified alternatives are: mobility with directory services, routing protocol approaches such as Host Based Routing (HBR) and Mobile Ad hoc Network (MANET) solutions. However, these alternatives are presented as clearly not satisfying the requirements.

Having steered through this wide set of mobility candidates to support network mobility, we identify the following Mobile IPv6 extensions for network mobility support: Prefix-Scoped Binding Updates (PSBU), Hierarchical Mobile IPv6, Mobile Router Tunnelling Protocol (MRTP) and Optimized Route Cache Management (ORC) protocol. We describe in detail these four published protocols, and perform a deep analysis of their capability of dealing with key issues such as: support for local fixed nodes (LFN), for visiting mobile nodes (VMN), for secure/non-secure route optimization and for nested mobility. A table synthesizing this analysis is presented.

Next, we concentrate on developing a novel concept for network mobility support proper to OverDRiVE. This is presented as a "base" proposal, which is in fact a Mobile IPv6 bi-directional approach between MR and HA. This basic proposal is presented as supporting a wide range of mobility scenarios: simple network mobility, visiting mobile nodes. On top of this "basic" proposal we add enhancements such as multi-homing, multicast, security and mobility of nodes inside the mobile network. This is being further refined as mobility support inside the mobile network with Mobile IPv6, with Hierarchical Mobile IPv6, with BCMP and with RIPng and/or OSPF.

Route optimization aspects are not treated by the current OverDRiVE proposal and constitute further research to be performed within the OverDRiVE project.

2.2 Requirements for OverDRiVE

OverDRiVE has described in Deliverable 03 (D03) [1] the requirements and scenarios regarding mobility and functionality that are the basis for the future work in the project. This section summarizes the results of D03 with respect to the mobility management and AAA concepts described in that deliverable.

General requirement for the concepts are as follows:

- **Utilize IPv6 protocol mechanisms:** IPv6 mechanisms are solely used; necessary connectivity over IPv4 clouds e.g. due to demonstrations constrains should not be prevented by the concepts.
- **Reuse existing protocols:** If possible the use of existing protocols and concepts should be favoured to avoid duplicate work.

- **Scalability:** The solution should be scalable to a decent number of mobile nodes. As IVANs are restricted to the boundaries of a vehicle, the number of mobile nodes to be supported is limited.
- **Efficient use of radio resources:** The solution should also prevent the unnecessary use of scarce radio resources due to improper signalling overhead.
- **No changes to the outside world:** The solution should not impose any OverDRiVE specific requirements to any network entity outside the IVAN and OverDRiVE backbone domain. Especially, the solution must not require changes in access systems. However, it can be expected, that network entities outside the OverDRiVE domain are conforming to current Mobile IPv6 IETF specifications.
- **End-to-end semantics:** The solution should regard the Internet end-to-end principle. It should be prevented to deploy functionality into internal network elements, which could be handled in mobile hosts with similar efficiency. An exception to this rule would be due to insufficient mobile node capabilities (e.g. in terms of processing power, or battery consumption).

From the functional point of view the following two main requirements must be fulfilled in all mobility scenarios:

- **Session continuity** while changing the point of attachment to the Internet.
- The handover between different access systems must be transparent to existing IPv6 applications.
- **Reachability** of the mobile nodes regardless of the current point of attachment.
- It implies that a well-known (home) address exists which can be used to reach a mobile node.

In D03 several mobility scenarios were investigated. The main scenarios are shortly described:

- Moving of an Intra-Vehicular Area Network (IVAN): The IVAN moves homogeneously (network entities stay together) using a mobile router to provide the Internet connectivity for nodes within the IVAN.
- Moving into an IVAN with a mobile device: The mobile host moves into an IVAN and changes for instance its UMTS connection to a WLAN or Bluetooth connection inside the IVAN (and vice versa).
- Moving within an IVAN: in a larger IVAN (e.g. in a train). To accomplish efficient and optimized signalling and transmission topological hierarchies or micro mobility approaches might be used, involving more than one fixed (with respect to IVAN) or mobile router. Mobile nodes can move around inside the IVAN connecting to the appropriate "access router" inside the IVAN.

Nested IVANs (see Figure 2) constitute a special case where one or more IVANs are topologically aggregated below a top-level IVAN (e.g. Personal Area Network (PAN) enters a vehicle, a car is inside a ferry, etc.). The connection between the IVANs uses the same mechanisms as for connecting the top-level IVAN to the Internet. Another special case is the multi-homing / multi-access scenario in which the mobile router has multi-link capabilities accessing simultaneously more than one access network at a time, for reliable and application-adapted communication (transmission rate, cost, coverage, seamless handover, etc.)

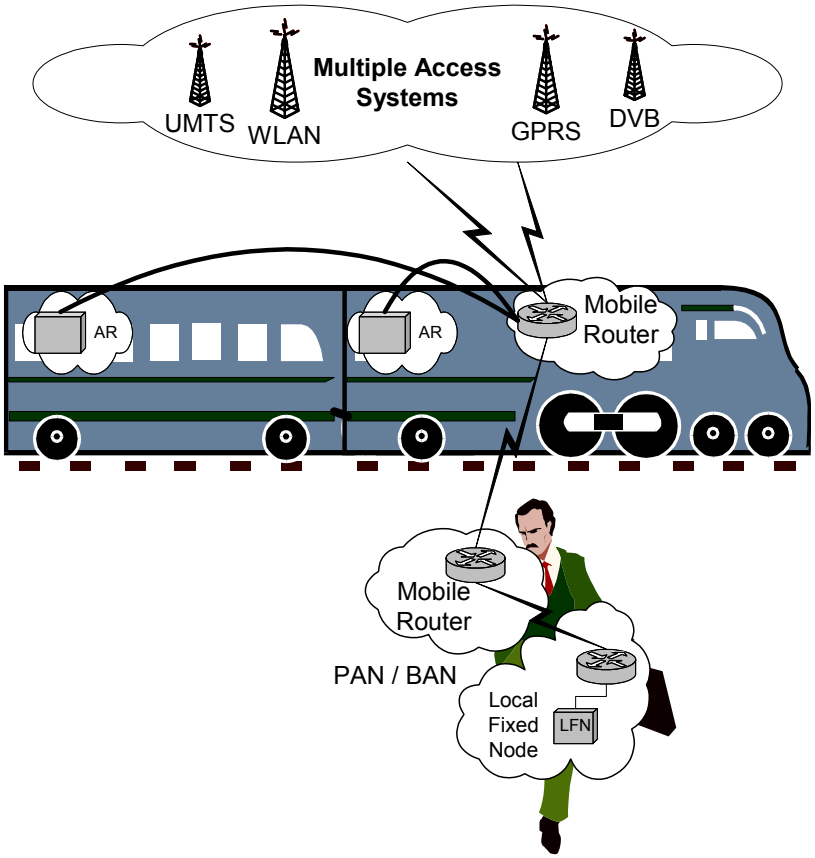


Figure 2: Nested IVANs and intra IVAN mobility

2.3 Analysis of Existing Mobility Management Solutions

2.3.1 Host Mobility Approaches

This section provides a brief overview of host mobility approaches that are potential candidates for further evolution towards supporting network mobility as described in the previous requirement section.

Existing proposals that accommodate moving hosts with a TCP/IP stack provide solutions at various layers of the stack and make different assumptions on the availability of certain types of services in Internet. Basically the following different types of approaches can be distinguished:

- Mobility with overlay tunnels and/or source routing: Mobile IP, HMIP, Fast Mobile IP (FMIP), BCMP, DHCP style allocated addresses and other optimizations
- Directory services: Session Initiation Protocol (SIP), Mobile People Architecture, Internet Core Beyond the Third Generation (ICEBERG)
- Routing protocol approaches: Cellular IP, HAWAII, Multicast Protocol approaches, MANET like approaches

2.3.1.1 Overlay Tunnel Approaches

The most mature mobility approach using IP overlay tunnels and source routing mechanisms is Mobile IP (MIP). Starting with Mobile IPv4 the protocol has been evolved naturally into IPv6 and is now an integral part of the new IPv6 protocol suite. The basic MIP proposal was subject to further proposed enhancements, which are shortly described in the sections following the Mobile IPv6 section.

Mobile IPv6

Mobile IPv6 [2] is well known for supporting host mobility by using IPv6 mechanisms like tunnelling and/or source routing. Mobile IPv6 fulfils the OverDRiVE requirements described in section 2.2, and has other advantages with respect to other mobility approaches:

- Continuous connection: Mobile IPv6 provides for transparency to applications by keeping existing connections up even when the assigned address change as a result of physical mobility.
- Ubiquitous reachability at a permanent home address: the home address is permanently registered in the Domain Name Service (DNS) directory and neither the name nor the address of an entity will change as a result of mobility.
- Clear delimitation within the TCP/IP stack: Mobile IPv6 introduces modifications to a TCP/IP stack but only at the network conceptual layer (layer 3). As a matter of fact it uses existing mechanisms of IPv6 protocols (e.g. tunnels, neighbour discovery, source routing) while keeping actual additions to the lowest possible level (the various types of caches can be merged with existing IPv6 structures). As a consequence to this, transport layer protocols are not modified and, even more importantly, applications are not modified when a computer implements Mobile IPv6.
- Easy deployment: in order to deploy Mobile IPv6 it is required to install new protocol entities: Home Agents (HA) within the domains that administrate moving hosts. These domains are leaf networks with respect to the larger Internet. Mobile IPv6 does not require any modifications to existing routing infrastructure nor to DNS.

In standard Mobile IPv6, a mobile node needs to send Binding Updates (BU) to its Home Agent and all its correspondent nodes every time it changes its point of attachment, independent of the scope of the movements. This is due to the fact that Mobile IPv6 handles macro mobility and micro mobility identically.

In the following an overview of the mobility management procedures in Mobile IPv6 is provided.

Initial Registration (Figure 3):

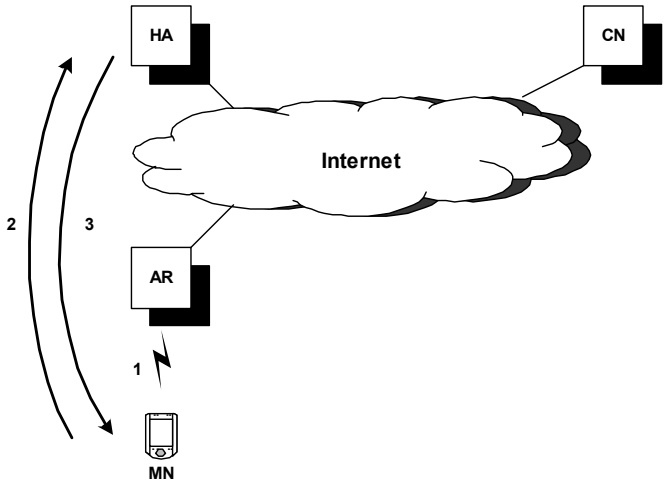


Figure 3: Registration

1. MN detects that it is no more connected to its home link from the Router Advertisement received from the *access router* (AR).
2. MN sends Binding Update to the home agent to register its current care-of address.
3. HA accepts the Binding Update and returns a Binding Acknowledgement (BAck).

Mobility (Figure 4):

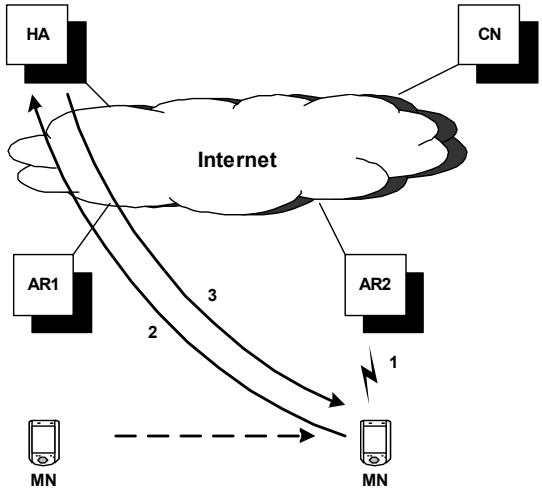


Figure 4: Mobility update

1. MN detects that it has moved to a new link from the Router Advertisement (RA) received from AR2.
2. MN sends Binding Update to the home agent to register its current care-of address.
3. HA accepts the Binding Update and returns a Binding Acknowledgement.

Route Optimization (Figure 5):

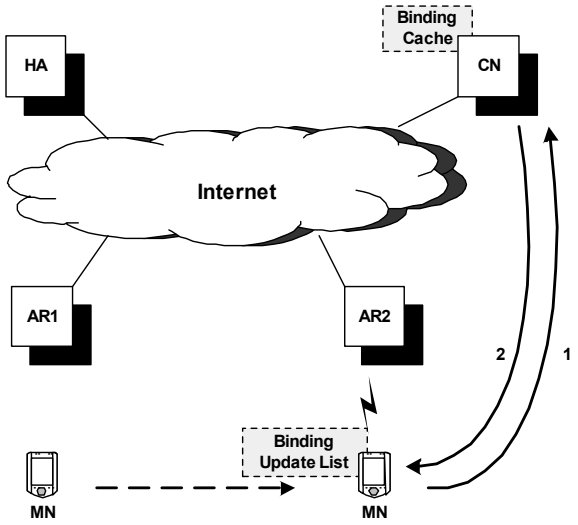


Figure 5: Route optimization

1. MN can also send Binding Update to its *correspondent node* (CN) to enable route optimization.
2. CN accepts the Binding Update and returns a Binding Acknowledgement.

Mobile IP Optimizations

This section briefly describes some optimizations developed for MIP. Various researches have been performed to improve the performance of the initial/base Mobile IP proposal. That resulted in few proposals to reduce handoff latencies and signalling overhead. Examples for that research are Hierarchical Mobile IP [3], introducing hierarchies into the signalling path. More general mobility agents are introduced by Transparent Hierarchical Mobility Agents (THEMA) [4]. A further generalized approach is called regional registration Mobile IP Regional Registration [5]. The following section will shortly explain the basics of Hierarchical Mobile IPv6 (HMIPv6).

Hierarchical Mobile IPv6

In Mobile IPv6, a mobile node sends Binding Updates to its home agent and all its correspondent nodes every time it changes its point of attachment. As a consequence, the same level of signalling and processing load is introduced on the Internet independently of the user's mobility pattern. These additional loads can be quite significant as the number of mobile nodes increases in the Internet. The other drawback is when the access point is located far away from the home agent; the signalling delay for the registration may be long enough to cause service disruption and significant packet loss. This limitation is the result of lack of hierarchy in the mobility management of Mobile IPv6.

HMIPv6 has been developed by Ericsson and INRIA and is specified in an Internet-Draft [3]. For a bit more history, several direct precursors to HMIPv6 are [45], [46], [47] (earliest HMIP reference is 1998; seminal work in the HMIP space was also guided by Sun Labs and Nokia). A new Mobile IPv6 node, called mobility anchor point (MAP), is introduced, which can be located at any level in a hierarchical network of routers. In HMIPv6, two different types of care-of addresses are distinguished: Beside the topologically correct care-of address, called "local care-of

address" (LCoA) in this context, a mobile node also obtains an address from a MAP referred to as the "regional care-of address" (RCoA). The RCoA is an address on the MAP's subnet. If there is more than one hierarchy level, a mobile node may even have several RCoAs.

A mobile node uses its (highest-level) regional care-of address for the bindings in its home agent and correspondent nodes. Then, the MAP receives all packets on behalf of the mobile node it is serving and encapsulates and forwards them directly to the MN's current local address. If the Mobile Node (MN) changes its LCoA within a local MAP domain, it only needs to register the new address with the MAP. In contrast, the RcoA registered with Correspondent Nodes (CNs) and the HA does not change, and MN's mobility within a MAP domain is transparent to CNs and the HA.

In HMIPv6, a new MAP option in the router advertisements informs MNs about the presence of a MAP (MAP discovery). Thus, the access router advertising MAP information to the attached mobile nodes defines MAP's domain boundaries. A preference value and a distance field are introduced to enable a mobile node to select among different MAPs. Furthermore, HMIPv6 adds a new flag (M flag) to the BU message.

This hierarchical approach has at least two advantages. First, it improves the handoff performance, since local handoffs are performed locally. This increases the handoff speed and minimizes the loss of packets that may occur during handoffs. Second, it significantly reduces the signalling load on the network since the signalling messages corresponding to local movement do not traverse the whole network, but stay confined to the site or at least the local domain.

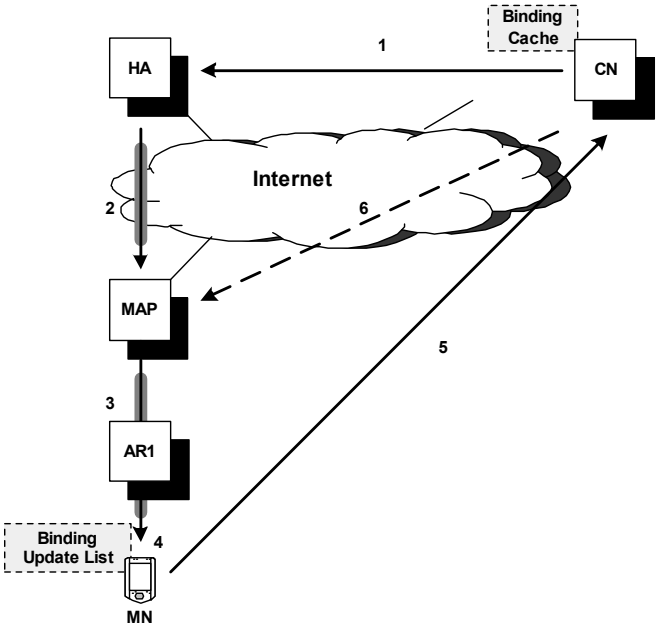


Figure 6: Hierarchical Mobile IP

1. Packets from correspondent nodes, which do not have Binding Cache for mobile node's current care-of address, are sent through mobile node's home agent.
2. These packets are intercepted by the home agent and tunnelled to the MAP.
3. The MAP receives the packets on behalf of the mobile node, encapsulates and forwards them to mobile node's current care-of address.
4. Mobile node decapsulates the packets and processes them accordingly.
5. Packets originating from the mobile node are sent directly to the correspondent node.

6. Packets from correspondent nodes with Binding Cache are sent directly to the MAP without having to go through the home agent.

In the IST project DRiVE [6] HMIPv6 was utilized and extended to provide mobility management solution for moving host additionally allowing for host controlled flow routing between different access systems. A new system entity called Multi-access support node (MSN) is responsible for several regional access systems, traffic control (which data stream uses which access system) and acts a local anchor point for mobility.

BRAIN Candidate Mobility Protocol

Similar to HMIPv6, BCMP [27] uses anchor points (ANP), but there is only one CoA, which is a permanent address while the MN does not change its ANP. Therefore the role of handover here is to inform the ANP about the MN's current AR. Thus, ANPs will encapsulate and forward packets received on behalf of MN to the MN's current AR, and after decapsulation AR will send them, through the air interface, to the MN. Another part of the BCMP handover is the buffering of the packets in old AR and tunnelling them to the new AR in order to minimize the packet loss.

Besides this regular handover, BCMP supports also a prepared handover mechanism in that a MN, which already knows the identity of the new AR, can initiate the handoff in advance.

A BCMP based network has the following entities:

- Gateway (GW) routers are legacy IP routers, without any BCMP specific extensions, with connection to external networks.
- User Registries (UR) are signalling servers that handle login and logout and maintain information about logged-in users. They do not forward data packets.
- Anchor Points (ANP) are routers that allocate IP addresses for mobile nodes.

Access Routers (AR) are routers at the edge of the network, equipped with wireless access points.

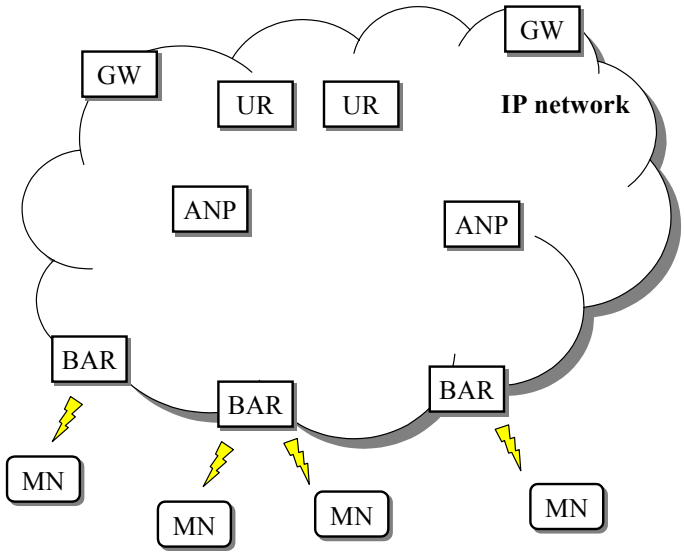


Figure 7: BRAIN Candidate Mobility Protocol

DHCP with Home Address Option

DHCP is a simple client-server based protocol for providing IP configuration data for hosts allowing them to use a given Internet access connection without configuring any parameter. Using DHCP together with Mobile IP and the introduction a home address option [7] allows for requesting simultaneously a (mobile) home address and a new home agent address via DHCP. By tightly integrating both protocols (DHCP and Mobile IP) an optimized procedure for assigning addresses could be achieved.

2.3.1.2 Directory Services

Using directory services for mobility management purposes are characterized by the fact that mobility issues are handled by higher layers in the protocol stack using a strict application specific end-to-end paradigm. This is done for example by introducing a personal layer Mobile People Architecture [8] service agents ICEBERG [10] or extended session servers SIP Mobility [11]. Neither of them supports seamless TCP sessions while changing the point of attachment for the mobile node but rather uses some kind of remote updating of the server information indicating that the receiver has a new IP address. Additionally proposals were made to use dynamic DNS services to provide mobility to IP based hosts.

2.3.1.3 Routing Approaches

Another way of supporting host mobility is to use routing mechanisms in the access network and at the access router to update the routing paths as fast as possible to allow for seamless handover between different access routers. Basically 3 different approaches can be distinguished:

- Host based forwarding
  - Examples: Cellular IP [12] , HAWAII [13]
- Multicast protocol approaches
  - Examples: Multicast for Mobility Protocol (MMP) [14], Multicast Mobility [15], Deadalus [16]
- MANET like approaches
  - Examples: all MANET protocols [18], Mobile Enhance Routed – Temporally Ordered Routing Algorithm (MER-TORA) [19]

Host based forwarding

These approaches are characterized by the fact that a specific access network is defined in which all-IP routing and access technologies are applied (HAWAII domain, Cellular IP). By using these approaches certain means the efficiency and functionality compared to Mobile IP in an all-IP access improve network. The network is connected to the Internet by means of border routers hiding the mobility inside the access network/mobility domain. These approaches are also commonly referred to micro-mobility approaches.

HAWAII uses host based routing entries and paging caches, which are updated by means of path setup messages towards the domain root router.

Cellular IP uses separate routing and paging caches for each host. The routing update is done via route update toward the gateway router. Focus is on the clear separation between macro mobility (Mobile IP) and micro mobility (Cellular IP).

The inter-domain mobility in HAWAII and Cellular IP is handled using Mobile IP and both proposals distinguish between idle and active hosts

Multicast protocol approaches

Multicast supports location-independent addressing and routing in all kind of IP multicast enabled networks. By using standard multicast administrative messages "join to" and "prune" mobile nodes can receive IP based independent from their location. Using a temporary unique multicast address the mobile joins a multicast group by sending administrative messages to the multicast router. Once the mobile moves and changes the multicast router the same unique multicast address is used to "re-join" the multicast group. Several sub-approaches like usage of standard multicast mechanisms [15], Mobile IP including multicast [20] or even multipoint-to-multipoint architectures were developed.

MANET like approaches

The IETF MANET (Mobile Ad-hoc Networks) group defines protocols used for spontaneous, ad hoc communication without any supporting infrastructure. The focus is on routing protocol support for (very) mobile nodes forming ad hoc communication groups like coming together to a meeting with laptops or moving vehicles on a road building interconnected moving networks of vehicles. The developed routing protocols can be mainly divided into two classes: table-driven and on-demand driven. The table-driven approach uses periodic status messages to update the current situation in each node. That has the advantage of fast packet routing since all information is up-to-date in the node to accomplish routing. A disadvantage is the high management load due to update messages. Examples are Destination Sequenced Distance Vector (DSDV), Global State Routing (GSR), Hierarchical State Routing (HSR), and others. On-demand protocols are using a lazy approach updating only on-demand the routing entries, which in turn yields longer propagation time at least for the first packet. When a source wants to send to a destination it invokes a discovery mechanism to find the destination. Examples for these approaches are Cluster based routing protocol, On-demand distance vector routing, Dynamic Source Routing (DSR), and others.

MER-TORA (Mobile Enhance Routed – Temporally Ordered Routing Algorithm) provides an edge mobility approach in which prefix based and host based routing is combined. It uses domain internally the TORA protocol, which was originally designed for MANET networks combined with temporary tunnels for predicted handovers.

2.3.1.4 Conclusion

Comparing the approaches with the requirements and mobility scenarios the overlay tunnel approaches are the best-suited approaches for further evolution to support moving network mobility. The main advantages compared to the other approaches with respect to OverDRiVE requirements and scenarios are:

- Basically no changes in existing access networks are necessary
- Usage of existing well-known protocols (e.g. Mobile IPv6)
- Application transparent usage of approaches
- Potential support for all OverDRiVE mobility scenarios

With respect to intra-IVAN mobility certain micro-mobility approaches seems to be viable to further optimize the handover performance and decrease routing and signalling overhead.

2.3.2 Network Mobility Approaches

In the following chapters existing approaches for supporting network mobility based on Mobile IP are discussed. A more detailed discussion can be found in [21].

2.3.2.1 Prefix Scope Binding Updates

MOTOROLA Labs Paris and INRIA have proposed the utilization of Prefix Scope Binding Updates [22]. Basically, a Prefix Scope Binding Update is an enhanced Mobile IPv6 Binding Update associating a care-of address with a prefix instead of a single address. It is assumed that all nodes in a MONET share a common prefix, and MR's ingress interface is configured with this MONET prefix. As in MIPv6, MR's egress interface is configured with the home prefix (when the MR is at home). The modified Mobile IPv6 Binding Update has a new sub-option, containing the MONET prefix field. The binding cache management in MR's home agent as well as in the correspondent nodes is changed slightly compared to MIPv6, in particular the searching for entries, so that the address comparison considers prefixes.

If the destination address of an IP packet in the correspondent node matches this prefix, it is sent to the care-of address including a routing header similar to MIPv6. The home agent intercepts all packets sent to the MONET prefix by means of proxy neighbourhood advertisements and forwards them to the MR. As a consequence, by registering one care-of address for an entire IP sub-network, all packets to nodes in the MONET are forwarded to the care-of address of the MR. The MR obtains a new CoA on each subsequent link using either stateless or stateful address configuration.

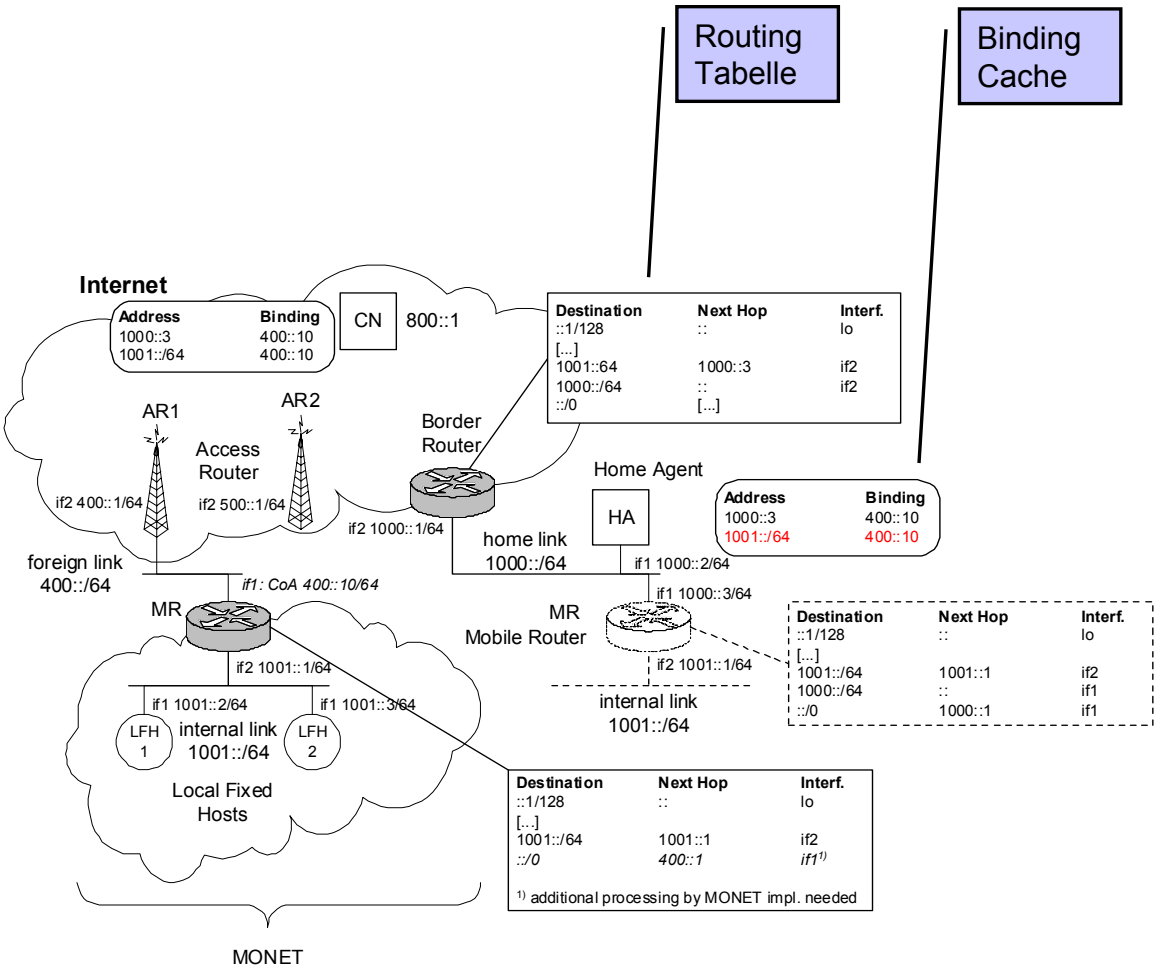


Figure 8: Prefix Scoped Binding Updates

In the Prefix Scope Binding Update solution, the MR is a modified MIPv6 mobile node. As already mentioned changes in MR's home agent and in correspondent nodes are required. The latter point is quite important, because routing optimization is only available if the correspondent node explicitly supports Prefix Scope Binding Updates. If so, this approach could reduce the so-called "Binding Update storm" problem of MIPv6: If a mobile node, or a MONET, communicates with a large number of correspondent nodes, during the handoff process a large number of Binding Updates has to be sent. With Prefix Scope Binding Updates, only one Binding Update has to be sent to every correspondent node. Hence, signalling is reduced considerably when several nodes in a MONET communicate with the same correspondent node. In contrast, no improvement can be achieved if the correspondent nodes are "scattered", i.e. the communication of the nodes in the MONET is not very correlated.

The main problem with this solution, however, is security: An authentication of the MR is possible, based on its home address, as in MIPv6. But a MR needs to be authorized to register a binding between the MONET prefix and its care-of address, because malicious attackers could claim the ownership of arbitrary prefixes. For correspondent nodes, which do not "know" the MR, this authorization is an unsolved question. One possible solution could consist of a modification of the "return routability"-mechanism used by MIPv6 to certify that the MR actually owns and serves the MONET Prefix. However, it is not possible to check return routability for every possible address behind the claimed prefix. [22] proposes to limit the check to a number of

carefully selected addresses, but of course, this does not provide absolute security. Another possibility could be authorization by some kind of a certificate, but certificates are not used in Mobile IP so far. Because of the lack of security, the existing specification of Prefix Scope Binding Updates cannot be deployed in Internet, in particular not the routing optimization function.

Analysis

The Prefix Scope Binding Update approach is explicitly designed for a limited scenario:

- The MONET is not multi-homed, i.e. it attaches to the Internet through only one MR, and the MR has only one egress interface.
- Only local fixed nodes in the MONET are considered. The Internet-Draft does not address problems related to "mobile" nodes.
- Nesting of MONETs is prohibited.

These restrictions result in a very simple MONET, consisting only of one mobile router, and having only one direct connection to Internet. It is commonly agreed that there are application fields for such a MONET, but a more general approach would be very desirable. In principle, the approach could be extended to multi-homed networks, and support for visiting mobile nodes could be added, but for this further research is necessary.

2.3.2.2 HMIP

The main focus of Hierarchical Mobile IPv6 (HMIPv6) are not mobile networks, but a hierarchical mobility management model for MIPv6, which reduces the amount of signalling to correspondent nodes and the Home Agent (HA) and may improve handoff speed (see chapter 2.3.1.1)

Dependent on the assignment of regional care-of addresses, HMIPv6 distinguishes two different modes:

- In "basic mode", the RCoA is formed in a stateless manner (auto-configuration) by combining the MAP's subnet prefix received in the MAP option with the MN's interface identifier. The basic mode is quite simple: The MAP merely is a kind of home agent that binds MN's RCoA to the LCoA, intercepts all packets and tunnels them to the corresponding LCoA.
- In "extended mode", the MN is configured with a regional care-of address that is assigned to one of MAP's interfaces (i.e. no duplicate address detection is necessary). Unlike in basic mode, the mobile node uses its home address in the MAP binding. Packets from the home agent are tunnelled to the mobility anchor point and decapsulated there. Based on the home address the MAP routes the packet and encapsulates it again. For routing optimized packets from correspondent nodes, the MAP has to check the routing header for the home address. As in extended mode routing in a MAP is based on the (global) home address of a mobile node, a slight change of the home agent is needed: When the HA tunnels packets with a site-local scope home address, it has to include a routing header in the outer packet with MN's home address as final destination. This is necessary because the MAP does not know home addresses for which it received no binding update, like e.g. site-local home addresses. The extended mode of operation can support both mobile nodes and mobile networks.

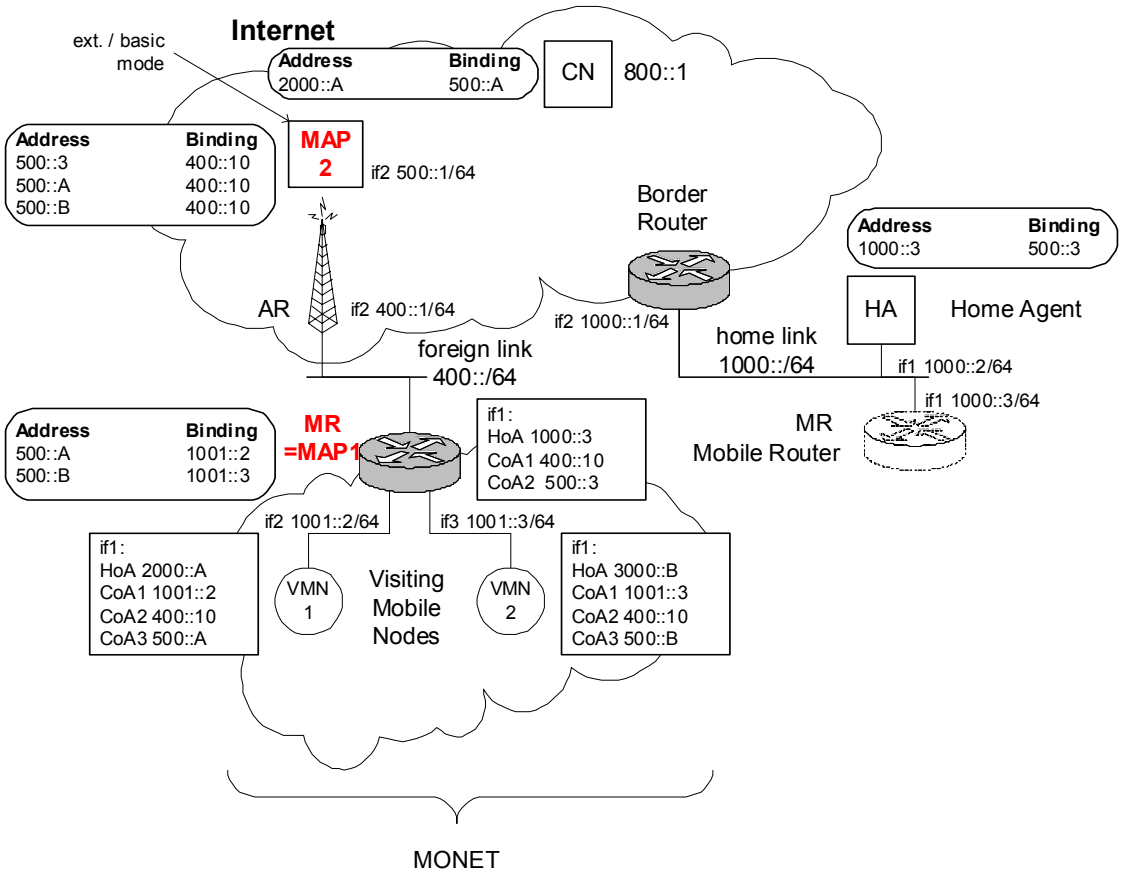


Figure 9: Mobile networks with HMIPv6

Figure 9 illustrates how mobile networks could be realized with Hierarchical Mobile IPv6. For this, a hierarchy of mobility anchor points is needed, at least consisting of the mobile router (first MAP) and a higher-level MAP (second MAP). The mobile router must be configured in HMIPv6 extended mode, while the higher-level MAP may use either basic or extended mode. Because of the hierarchy, nodes in the MONET have three care-of addresses: A local care-of address (called "CoA1" in Figure 3) and two regional care-of addresses ("CoA2" and "CoA3"). Nodes in the MONET learn the presence of the different MAPs by MAP announcements and are individually responsible for keeping the binding caches up to date. As a consequence, in an HMIPv6-based network mobility solution, all nodes in a MONET are aware of the mobility of the MR.

Analysis

Hierarchical Mobile IPv6 introduces some extensions to MIPv6 and neighbour discovery and requires minor extensions to the mobile nodes and the home agent (only in extended mode). In theory, the correspondent nodes are not affected. The mobile anchor point essentially acts as a local home agent, limiting the signalling outside a local domain and supporting fast handovers as well as certain network scenarios. The more hierarchical a network topology, the larger are the benefits from HMIPv6.

As already outlined, the Internet-Draft proposing HMIPv6 (version 6) mentions mobile networks, but the support for MONETs does not seem to be the main design goal of HMIPv6, and important questions are still left to be answered. In general, this solution only works for "mobile" nodes being aware of mobility, and every node has to handle its own mobility. "Fixed" nodes are not supported. With HMIPv6, in principle even very complex topologies are possible, including

nested MONETs, if a hierarchy of several (mobile) MAPs is used. But this is more a theoretical option, since many detail questions are not solved in this draft. The approach might not scale well to a large number of hierarchies.

The most important problem of this draft is security. In the described solution the MAP entity offers additional possibilities for malicious attacks, and this version of HMIPv6 draft does not provide any security mechanism to protect Binding Updates. In some configurations the source addresses of packets are topologically not correct, and it is not clear how HMIPv6 can deal with ingress filtering, in particular by access routers. Version 6 of HMIPv6 draft is quite old, and so it is based on outdated Internet-Drafts. This version is not adapted to recent changes in MIPv6 related to security (for example the return routability test).

Currently version 7 of the HMIPv6 draft [8] is available that improves lots of the aforementioned security problems (return routability tests, etc.), but this version does not explicitly mention mobile networks.

2.3.2.3 Mobile Router Tunnelling Protocol

The third Internet-Draft on mobile networks [23] is an interesting one. It describes how to support MONETs with Mobile IP, not even restricted to MIPv6, without any mandatory modifications to Mobile IP or routing protocol signalling. The MONET support is just realized by a bi-directional tunnel between the mobile router and its home agent. Both the mobile router and the home agent use unmodified Mobile IPv6, except that there are minor implications to the packet forwarding implementations.

Dependent on the question whether the mobile router is allowed to run a dynamic routing protocol on its home link (“fully enabled” mobile router) or not (”consumer” mobile router), two different modes are distinguished. In the former case, the MR behaves like a normal fixed router in Internet, and redirects traffic towards its home agent by means of a dynamic routing protocol. The dynamic routing protocol updates the routing state between home agent, mobile router, and gateways to Internet, so that next hop entries now point to the home agent. In the latter scenario, MR's home agent injects static routes for a restricted set of links behind the MR, when the MR is not at home, using MR's home address as the next hop. These static routes are pre-configured. In both cases, MR's home agent captures packets forwarded to the mobile router, and does a route and binding lookup. If the packet is designed for the MONET, i.e. if the next hop is MR's home address, then the packet is tunnelled to the care-of address of the MR. For the reverse direction, mobile router's default route points towards the tunnel to its home agent, so that all packets from the MONET are reverse tunnelled to the home agent.

The mobile router and its home agent must know that a tunnel is to be established, and that packets for the mobile networks must be routed through that tunnel. For this, some signalling in the tunnel is necessary. According to [23] this signalling can be either implicit (meaning that no changes to the Mobile IP messages are used) or explicit. For explicit signalling, an optional “mobile network option” is defined in order to specify prefix mappings, which may be included in Binding Updates and Binding Acknowledgments. This option is not mandatory because the information from the routing protocol should include the prefixes served by the mobile router, i.e. the home agent gets to know them anyway.

Analysis

With respect to the home link, the scenario shown in Figure 8 adapts pretty well to this solution. The only difference would be that a dynamic routing protocol "fully enabled" mode) would change the next hop entry in the gateway router from 1000::3 (home address of the MR) to 1000::2 (address of the home agent). As the already mentioned network prefix option includes also prefix information, this approach is very similar to Prefix Scope Binding Updates. But, of course, there are also differences: First, this approach does not support any routing optimization to and from the MONET, i.e. all traffic passes the home agent of the mobile router. Therefore, no binding updates are sent to correspondent nodes. Second, this approach supports "mobile" nodes, which can attach to the MONET by means of Mobile IP and can get a care-of address of the link inside of the MONET. And finally, nested MONETs are possible, because a mobile router can inject several prefixes on the home link. This at least holds for "fully-enabled" mobile routers, which can support arbitrary links behind them, both stub- and transit networks. For "consumer" mobile routers, the prefixes are statically configured, i.e. only such MONETs can be nested that use these preconfigured prefixes. However, nested mobile networks result in various, reciprocal tunnels from the mobile routers to the corresponding home agents, i.e. a very inefficient routing.

The multi-homing issue is not considered in [23]. But as dynamic routing protocols cannot only be used on the home link, but also inside the MONET, multi-homing would be possible if there was an appropriate dynamic routing protocol. As routing optimization is not used, security in this approach is less critical than in other ones. Of course, the messages exchanged between a mobile router and its home agent must be secured when the mobile router is not on its home link, which can be fulfilled by a static security association between the mobile router and its home agent, like in all other cases. Furthermore, neither Mobile IP nor routing protocols must be changed, and therefore no additional security problems occur. In this approach, a considerable part of the problem is shifted from Mobile IP to the used routing protocol: It is up to the routing protocol to decide whether a route may be injected in the home link, and up to existing Authentication, Authorization and Accounting (AAA) mechanisms to decide whether a mobile node may attach to a MONET.

Thus, the main problem with this concept is that Mobile IP is only used to establish the tunnel between the mobile router and its home agent. In reality, mobility is handled by the chosen routing protocol, on the home link, and to some extends also internally in the MONET. This may be a quite challenging issue when fast topology changes happen. The approach is able to support movement to the same extent as the chosen routing protocol can do so. In other words, if the routing protocol converges slowly, frequent handoffs cannot be handled. But, all in all, this approach is certainly simpler to implement than the other ones presented in this chapter.

2.3.2.4 Optimized Route Cache Management Protocol for Network Mobility (ORC)

At the time of writing, a relatively new protocol is being proposed in [48] and further enhanced in [49]. This recent publication shows that the domain is a potentially very fruitful area of research. It is clear that more analytical assessment and implementation experience is needed before this protocol can be fully described; but we give here a very brief overview for completeness reasons.

The protocol is another instance of network mobility protocol that uses the bidirectional tunnel between MR and HA as a starting point. It has some characteristics from the previous proposals, in that, for instance, it uses prefix-scoped binding updates. It introduces novel characteristics with respect to three aspects: (1) the home address of the mobile router is assigned to the ingress interface of the Mobile Routers (and not the egress interface), (2) there is a two-step approach in the search algorithm for the binding cache and (3) it invokes "prefix delegation" concepts for the assignment of the mobile network prefix.

In addition to these relatively minor aspects, the ORC protocol introduces one major architectural component, the ORC router. This router can be deployed relatively close to CN, eventually as the next-hop router. If such architectural modifications are introduced, some very important advantages can be obtained: perform route optimization without modification to CN. The ORC proposal mentions routing exchanges between MR and ORC routers that can be placed close to CN or even better, anywhere in the Internet.

2.3.3 Conclusion

We have provided a set of 4 representative proposals in the previous sections: prefix-scoped binding updates, hierarchical Mobile IPv6, mobile router tunnelling protocol and optimized route cache management protocol for network mobility. We have identified a set of key issues that are addressed or not addressed by each of those proposals. In this section we compare the features of the 4 protocols in a meaningful manner, according to these key issues. The results are presented in the table below.

The basic proposal of prefix-scoped binding updates encompasses the scope of Local Fixed Nodes, offers route optimization between the mobile network nodes and any CN in the Internet and potentially offers route optimization inside a nested aggregation of mobile networks (even if this is not clearly described in the published Prefix Scoped Binding Update (PSBU) drafts). The main drawbacks of basic PSBU's are related to security: redirecting a CoA to an attacker MN was already acknowledged as a very serious security risk in the mobile hosts case; in the case of mobile routers this becomes a means to redirect prefixes, i.e. the entire set of addresses of hosts belonging to that prefix. This is further worsened by the fact that current solutions for avoiding redirection of CoAs are relying on return routability tests, a method that can hardly be extended to prefixes (one can not "ping" a remote prefix).

The HMIPv6 approach offers support for Visiting Mobile Nodes, route optimization and nested mobile networks. Unfortunately the protocol has some security weaknesses that have not been addressed fully until the time of writing. Another drawback is the lack of support of multiple MR's and multiply interfaced MRs (multi-homing).

The Mobile Router Tunnelling Protocol is probably the most complete description relying on the bidirectional tunnel between MR and HA. It supports Local Fixed Nodes, Visiting Mobile Nodes and nested mobility. It also supports running a dynamic routing protocol between MR and HA, which opens new opportunities to grow the mobile network size to very large topologies. However, the protocol is not supporting (at the time of writing) any form of route optimization. And, as HMIPv6, it does not yet support multi-homing. Another drawback that has been identified with Mobile Router Tunnelling Protocol (MRTP) is that it lacks support of frequent changes of topology.

The ORC protocol is probably the most advanced published description of support of network mobility (at the time of writing), since it has integrated support for all the key issues: nesting, RO, secure RO, multi-homing. However, its strong reliance on deploying of arbitrary ORC routers at any place in the Internet raises serious questions with respect to the deployment capability of this type of protocol.

Approach	Addressed issues	Unsolved issues
Prefix Scope Binding Updates	Local fixed nodes Routing optimization	Authorization of binding updates Visiting mobile nodes Multiple MRs and multi-homing Nesting
HMIPv6	Visiting mobile nodes Routing optimization Nesting	Local fixed nodes Security, ingress filtering Multiple MRs and multi-homing
Mobile Router Tunnelling Protocol	Local fixed nodes Visiting mobile nodes Nesting	Routing optimization Multiple MRs and multi-homing Frequent changes of topology
ORC	Route Optimization. Nested mobility. RO for nested mobility. Secure RO for mobile network (with risks).	The strength of the protocol relies on the ability to deploy ORC routers anywhere in the Internet.

2.4 Concept for Mobility Management

Mobility management for the mobile network relies on a protocol that is currently under study in the NEMO Working Group at the IETF. This protocol potentially comprises very simple extensions to the Mobile IPv6 protocol.

Analyzing the scenarios presented in Deliverable D03, as well as the requirements set in the OverDRiVE project for network mobility we have chosen to use a network mobility protocol that relies on the bidirectional tunnel between the mobile router and the home agent in order to offer session continuity for mobile network nodes.

This kind of approach is further supported by relevant work that is done in the IETF NEMO Working Group.

In the following sections we describe most, if not all, of the configurations supported by the MRHA bidirectional tunnel to support network mobility.

2.4.1 Mobility Management for Mobile Networks

The main problem addressed by Mobile IPv6 is that, in the current Internet design, every IPv6 address corresponds to a fixed "location" in the routing fabric, the paths towards this location being maintained by all the intermediary routers. Due to this constraint, a host that physically moves from one location to another needs a new topologically correct address valid at the new location while at the same time maintaining the ongoing applications (i.e. a video stream is not interrupted by the address change). In order to have session continuity between these changes, a MH is permanently assigned a *Home Address* that is valid in the home domain, i.e. the official administrative domain to which this MH belongs. Mobile IPv6 provides means to dynamically maintain the correspondence between the Home Address and the various Care-of Addresses (CoA) the MH acquires in foreign networks. With the help of several Mobile IPv6 messages, i.e. Binding Requests (BReq), Binding Update (BU), Binding Acknowledgements (BAck), the HA maintains a Binding Cache with pairs of the form CoA – Home Address. When the MH is not at home, the HA acts on its behalf using proxy Neighbour Discovery, intercepting all packets directed towards the Home Address and subsequently encapsulating them towards the MH's

current CoA. In this way, MH will obtain all packets that it would have received if it were at home. In a symmetric manner, MH in a foreign domain will first encapsulate all its outgoing packets towards HA that will decapsulate and resend towards the original destination. These two encapsulation mechanisms are currently referred to as *bi-directional tunnelling* and together with binding cache management constitute the essence of the Mobile IPv6 protocol. Some of the extensions worth mentioning include security mechanisms for MN-HA communication, route optimization with return routability tests and hierarchical mobility management.

The MRHA approach to mobile networks problem space is to extensively use the bidirectional tunnel between MR and HA (with mobile hosts, that tunnel is between MH and HA). The HA acts on behalf of the link-local address of MR's moving interface (when the MR is in a foreign network). As in the mobile hosts case, the MR is using BUs and BAcks with the HA to maintain the MRHA bidirectional tunnel. The modifications to Mobile IPv6 HA and MH specifications are very small, allowing co-existence with existing implementations of Mobile IPv6 for hosts. The only important modifications involve an appropriate binding cache and routing table management on the HA and MR. Other proposals to support network mobility with an MRHA-like approach involve important modifications in routing table management *and* in protocol signalling, like for example using mobile network home prefixes instead of the full /128 address of the MR. However, these alternative approaches have important security risks due to incapability of authenticating an entire prefix (instead of an address). To entirely avoid dealing with the prefix-ownership problem[5], our MRHA approach, considers only the movement of the MR's Home Address – a full /128. This is feasible as a result of the following analysis, again similar to the Mobile IPv6 for host's case: traffic coming from outside the home link takes a certain path involving several L3 addresses. Of those, only mobile router's address is affected by mobility; even if it is part of Border Router BR's routing table (and BR does not run Mobile IPv6), BR actually uses the L2 address corresponding of that L3 address, by discovering it with Neighbour Discovery (ND) protocols. With Proxy ND, it is the HA that advertises its own L2 address as MR's L3 address, thus intercepting MR's home traffic. In this way, suffices it for HA to have a Binding Cache entry of the form MR_CoA-MR_HoA (as compared to MR_CoA-prefix). It is assumed that HA also maintains a routing table entry towards the mobile network's prefix through MR's Home Address (or a host-routing entry towards the Local Fixed Node LFN) [6]. Reversely, traffic coming from the mobile network (when the MR is in a foreign network) and towards anywhere to the Internet, is first forwarded by the MR through the reverse tunnel MRHA to the HA. Then HA decapsulates and forwards to the original destination. Remark that the absence of protocol modifications to Mobile IPv6 messages between MH and HA brings in the advantage of obtaining an MR implementation by having minimal modifications of an existing MH implementation (only table management is modified, but not the format of messages); A unique MR implementation works both for MH and MR. This is an essential advantage for OverDRiVE scenarios involving a PDA user (the PDA is the MH) getting in car where a mobile network is deployed (the car's mobile network connects to Internet with an MR)[7]. A generic initial setting for mobile networks is composed of: a large Internet cloud, a Correspondent Node CN, two Access Routers AR1 and AR2 as well as the home network composed of a Border Router BR, a Home Agent HA and the mobile network comprising the Mobile Router and a Local Fixed Node LFN. For this scenario we assume an application runs continuously between CN and LFN and that changes in addresses induced by mobility do not affect that

[5] The classic address ownership can be reformulated as a prefix-ownership problem, where MR needs to demonstrate it "owns" the prefix assigned to the mobile network to which it offers Internet connectivity.

[6] There are several ways in which HA can maintain these entries (basically: manual configuration, dynamic routing protocols, ICMP Redirect).

[7] If OverDRiVE only involved MR's then this would not have been an advantage.

communication. In our particular trials, CN is continuously streaming towards the Home Address of LFN and the LFN displays that stream on a video screen, as the packet exchanges in left diagram of Figure 10 suggests.

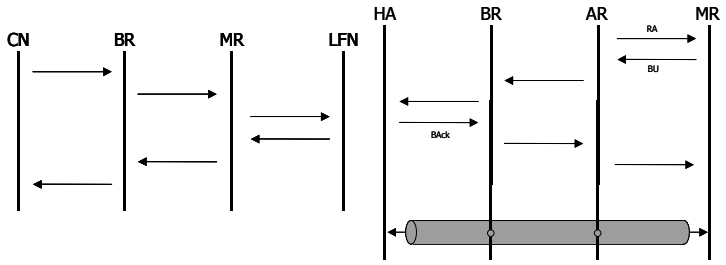


Figure 10: Initial Communication and Tunnel Setup for Simple Mobile Networks

The streaming packets and the encapsulation/decapsulation actions are illustrated in Figure 11, where bended arrows at the left of vertical bars represent decapsulations, and at the right – encapsulations. In that figure, the detailed ND messaging between BR and HA is excluded. In the other direction, when LFN needs to send a packet to CN and the mobile network is not at home, it will first send the packet to its default route, the MR. MR encapsulates back to HA which decapsulates and forwards to original destination. The diagrams b and c of Figure 12 describe the movement of the mobile network away from home towards any of the foreign networks governed by AR1 or AR2. Moving from home to AR1 triggers binding message exchanges between HA and MR in order to setup the MRHA bidirectional tunnel, as illustrated in the right diagram of Figure 10: MR receives a Router Advertisement RA, configures a new CoA and a default route. MR sends BU to HA. HA sets up its endpoint of the MRHA tunnel and replies with a Binding Acknowledgment; at this moment the MR endpoint of the MRHA tunnel is set up too. Once that tunnel is up the streaming between CN and LFN continues via the new CoA. The CN sends next application packet towards BR, BR asks for the L2 address corresponding to the L3 address of MR, HA replies pretending all packets addressed to MR, HA encapsulates and forwards this packet through the MRHA tunnel towards the current CoA. MR decapsulates the received packet and forwards to LFN.

A perfect symmetry can be noticed by drawing an imaginary horizontal axis through the centre of Figure 11: packets from CN to LFN take exactly the same path backwards, without state maintained neither on CN nor on LFN, as a consequence of bidirectional tunnelling.

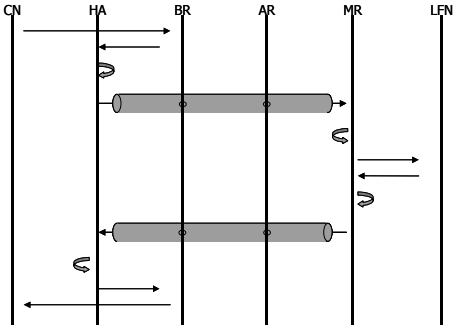


Figure 11: CN-LFN Exchanges, Simple Mobile Networks

The simplicity of this behaviour is a powerful tool in supporting mobile networks. It is very easy to realize that the simple configuration presented until here can be easily augmented with a large number of mobile networks under the same home roof (groupings of the form MR-LFN), a large number of ARs and a large number of CNs. All the involved packet exchanges are similar, if not the same, with the packet exchange in Figure 11. As presented in section 2.2, another important

OverDRiVE scenario is exhibited by a Mobile Host attaching to a mobile network (a person with a mobile device moving into an IVAN). A mobile network setup for this scenario is depicted in Figure 12. The diagram is the initial configuration with MR and MH at home. The diagrams b, c and d illustrate the movements, in that order. Top diagrams in Figure 13 present the packet exchange between different entities of the initial configuration.

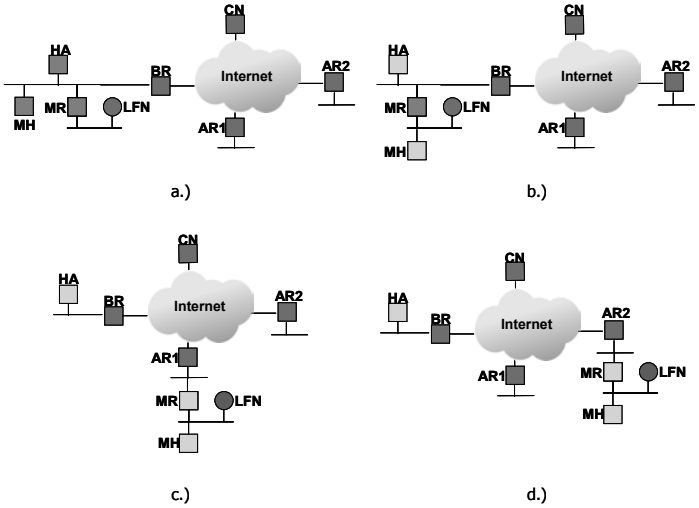


Figure 12: Mobile Host and Mobile Router, unique HA

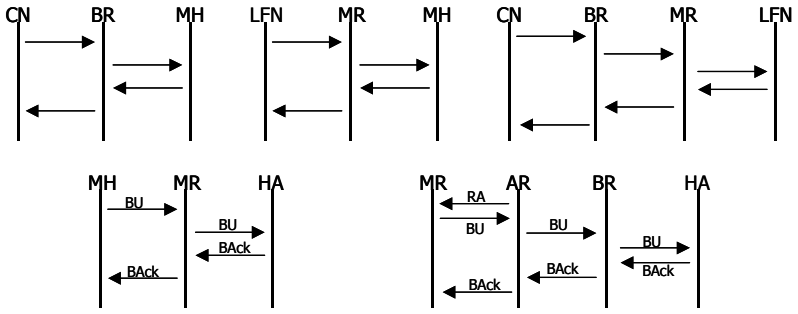


Figure 13: Initial Exchanges and Tunnel Setup, Mobile Network and Mobile Host

The packet exchanges between CN and MH corresponding to diagram c in Figure 12, and to top-left diagram in Figure 13, is depicted in Figure 15. Remark that HA performs a double encapsulation for each forwarded packet. Among the various paths, the wireless link AR1–MR is the most influenced segment by the multiple encapsulations, due to its radio characteristics. Remark also that initial communication between CN and MH involves 3 IP entities; while after movement it involves 6 entities (excluding each times the IP entities between CN and BR, and between BR and AR). The LFN–MH packet exchanges corresponding to diagram c in Figure 12, and to top-middle diagram in Figure 13 is depicted in Figure 14. Remark that even if LFN and MH are physically close to each other, many other out-of-path entities are forwarding their packets. This configuration lacks the symmetry of the simple MR case in Figure 11, the asymmetry (4 BR-HA exchanges when LFN sends to MH vs. 2 BR-HA exchanges when MH sends to LFN, see Figure 14) is due to attaching both MH and MR to a unique HA. The CN-LFN message exchanges corresponding to diagram c in Figure 12 and to top-left diagram in Figure 13 is similar to the CN-MH exchanges, except that the last decapsulation (or the first encapsulation) is performed by MR instead of MH. Note finally, it is possible to replace MH with another MR, thus obtaining a more generic nested mobile networks configuration, where message exchanges are similar.

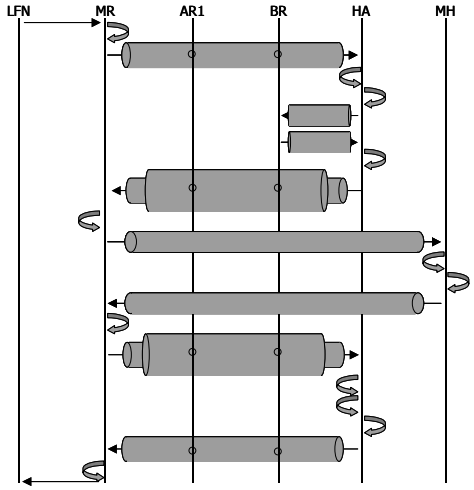


Figure 14: LFN-MH Exchanges, when MH and MR

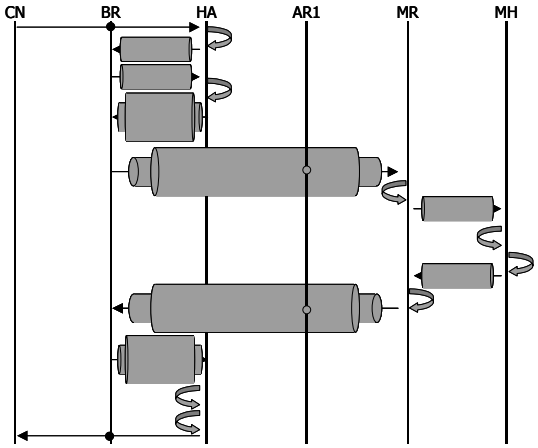


Figure 15: CN-MH Exchanges, when MR and MH

Overall, the MRHA approach to network mobility has the following characteristics:

- Little or no modification to current Mobile IPv6 protocol specification, allowing simple co-existence with Mobile IPv6 for mobile hosts. Inherits from Mobile IPv6 the session continuity and ubiquitous reachability at a permanent Home Address characteristics.
- Supports mobile hosts and networks that visit mobile networks (nested mobility).
- Naturally inherits the strong security mechanisms used by host Mobile IPv6; relies on the IPsec architecture for securing the MRHA tunnel.
- Scales up to a large number of mobile networks that roam around the edges of Internet; does not induce non-scalable routing table updates to the core network (prefix-augmented host-based routing inefficiencies are avoided).

Areas for Improvement of the MRHA Approach

At the lowest protocol level, several issues have been raised with respect to the MRHA approach. Most relate to Neighbour Discovery behaviour between HA and BR, route discovery, link-local addressing and security delegation between LFN and MR. In addition, the diagrams presented in this document show evidence of other more serious drawbacks that need to be addressed:

- *Excessive tunnelling* ("thick" tunnels): when MH attaches to the mobile network (see diagrams b and c of Figure 12) there are two MRHA encapsulating tunnels involved in the CN-MH path. Several levels of mobile networks induce excessive tunnelling that can lead to serious packet loss and worsen stack behaviour due to excessive fragmentation/reassembly. This is especially true in wireless environments.
- *Crossover tunnels* happen when the path between one tunnel's endpoints includes only one of the other tunnel's endpoints[8]. A situation leading to crossover tunnels is depicted in Figure 16, where a HA is deployed inside a mobile network. The initial configuration is in diagram a and diagrams b, c and d represent snapshots of the movement scenario. The MR2–HA2 tunnel setup procedure corresponding for the diagram d is practically impossible to perform.
- *Externally influenced intra-aggregation communication*: in the MH and MR with same HA case, depicted in diagram c of Figure 12, the LFN-MH communication (intra-aggregation) is influenced by the communication between MR and AR1 (external). If MR looses connection to AR1, then LFN looses connection to MH, a fact that, as paradoxical as it may seem, is a veritable side effect of tunnelling itself.
- *Under-optimal paths*: when comparing the length of the CN-MH communication path depicted in top-left diagram of Figure 13 to the CN-MH communication in Figure 15, it is clear that the path taken by packets is much longer than the optimal. The first diagram can be considered as an ideal to be attained, and the only optimal path that can be achieved is CN-AR-MR-MH (eliminating the BR-HA-BR additional segment). This is not the ideal path (since MH is not physically home) but represents an achievable goal, if employing Route Optimization techniques.
- *Asymmetric communication paths*: outgoing communication paths have different lengths than incoming communication paths, between the same two entities. See example in Figure 14.

[8] With *parallel* tunnels, that path includes either both or none of other tunnel's endpoints and this is the case in diagrams b, c and d of figure 5.

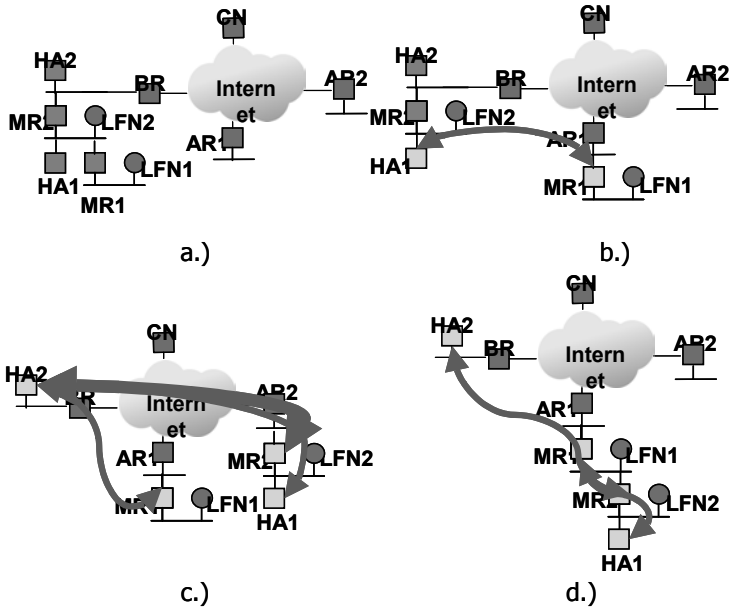


Figure 16: Crossover Tunnels

2.4.2 Analysis of Supported Non-nested Scenarios

The network mobility support with the MRHA bidirectional tunnel gives a good architectural solution for moving networks, completely relying on the un-modified Mobile IPv6 protocol. Several scenarios are fully supported by the MRHA behaviour, and this section presents an overview of these. The scenarios range from a simple mobile network to mobile networks comprising mobile hosts and to more complex aggregations of nested mobile networks.

The last scenarios will present some of the topologies that are less appropriately supported by MRHA (Border Router Home Agent (BRHA) loops) and where improvement is needed over the current MRHA behaviour as well as some extreme scenarios where the MRHA approach as specified in the previous sections encounters fundamental problems such as multi-angular routing, excessive tunnelling, crossover tunnels, externally-influenced intra-aggregation communication and multi-homing.

2.4.2.1 Basic Mobile Networks

Top picture in Figure 17 illustrates a generic preliminary setting for mobile networks. The following entities are depicted: a large Internet cloud, a Correspondent Node CN, two Access Routers AR1 and AR2 as well as the home network composed of a Border Router BR, a Home Agent HA and the mobile network comprising the Mobile Router and a Local Fixed Node.

For all the scenarios we assume an application runs continuously between various entities and that change in addresses induced by mobility does not affect that communication. In this particular scenario, CN is continuously streaming towards the Home Address of LFN and the LFN displays that stream on a video screen.

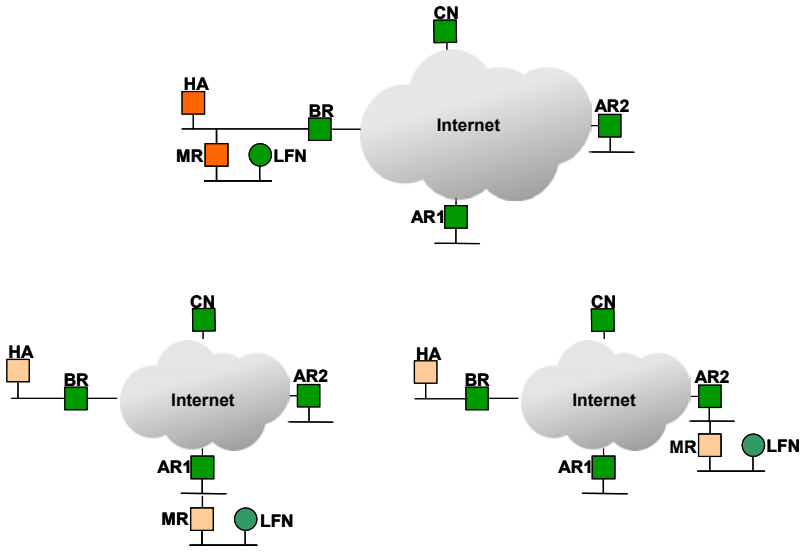


Figure 17: Basic Mobile Network Scenario

The two bottom topologies in Figure 17 describe the movement of the mobile network away from home and towards any of the foreign networks governed by AR1 or AR2. Moving from home to AR1 triggers binding message exchanges between HA and MR in order to setup the MRHA bidirectional tunnel. Once that tunnel is up with the new CoA of the MR, the streaming between CN and LFN continues where it was left when MR lost connectivity to the home network. The CN sends next UDP packet towards BR, BR asks for the L2 address corresponding to the L3 address of MR, HA replies pretending all packets addressed to MR, HA encapsulates and forwards this packet through the MRHA tunnel towards the current CoA of MR. MR decapsulates the received packet and forwards to LFN.

When MR is at home, CN starts a streaming session towards LFN. MR moves towards AR1. MR receives RA, configures a new CoA and a default route. MR sends BU to HA. HA sets the MRHA tunnel up and replies with a Binding Acknowledgment. CN sends a new packet to LFN, through BR. BR looks up LFN in its RT and finds an entry corresponding to MR. BR asks for the L2 address of MR. HA replies with its own L2 address. HA obtains the packet. HA looks up its RT and BC and encapsulates the packet towards MR's CoA. MR receives the packet, decapsulates, looks up its RT and SRT and finally forwards to LFN.

In the other direction when LFN needs to send a packet to CN and the mobile network is not at home, it will first send the packet to its default route, the MR. MR looks up its RT and SRT and decide to encapsulate towards HA. HA decapsulates, looks up its RT and BC and sends to BR. BR forwards appropriately.

The simplicity of this behaviour is a powerful tool in supporting mobile networks. It is very easy to realize that the topology presented Figure 17 can be easily augmented with a large number of mobile networks under the same home roof (groupings of the form MR-LFN), a large number of ARs and a large number of CNs. All the involved message exchanges will be similar, if not the same, with the message exchange previously presented.

2.4.2.2 Mobile Networks and Mobile Hosts

The scenario in Figure 18 illustrates a mobile network and a mobile host that are under the administration of the same Home Agent.

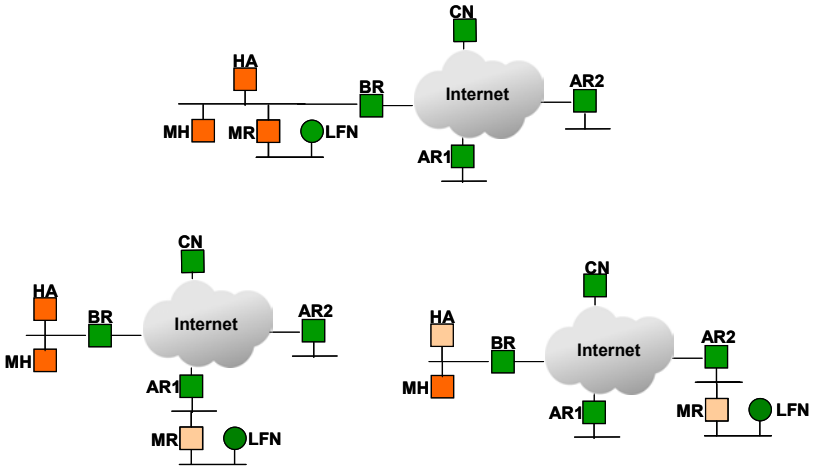


Figure 18: Mobile Network and Mobile Host at Same Home, Mobile Network Moves

The scenario in Figure 19 illustrates the same initial home configuration with one mobile network and one mobile host. The first movement involves MH attaching to the mobile network and subsequent movements involve the entire mobile network that moves together with the mobile host.

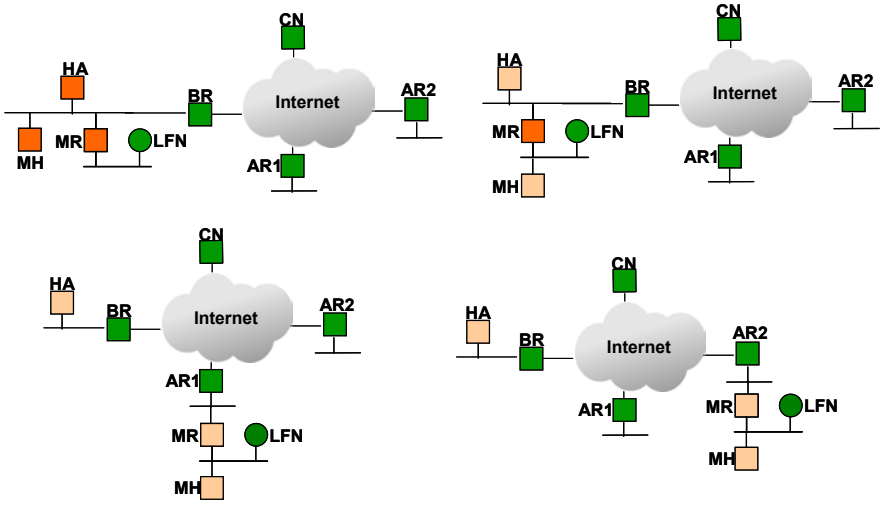


Figure 19: Mobile Network and Mobile Host at Same Home, Both Move, Homogeneous

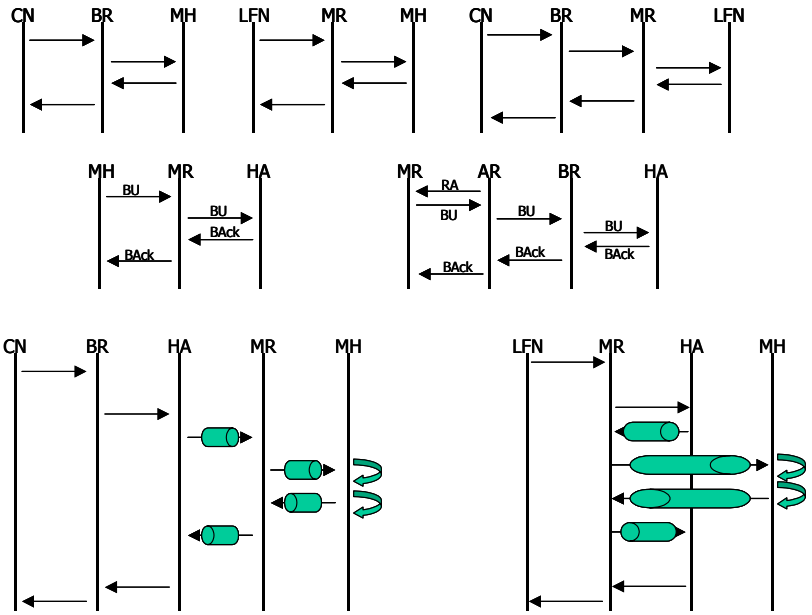


Figure 20: Initial Communication, Tunnel Setup, Subsequent Communication

Figure 21 presents a particular scenario where the first movement involves only the mobile network and subsequently MH attaches to the mobile network. This latter attachment happens when the mobile network is already in a foreign network.

This scenario exposes the opportunity of application of tunnel compression with Deering-Zill tunnels. In the bottom-right configuration, packets sent by MH to CN will be encapsulated twice: once by MH itself and once by MR. Both destination addresses of the encapsulating headers have the same destination address, the HA.

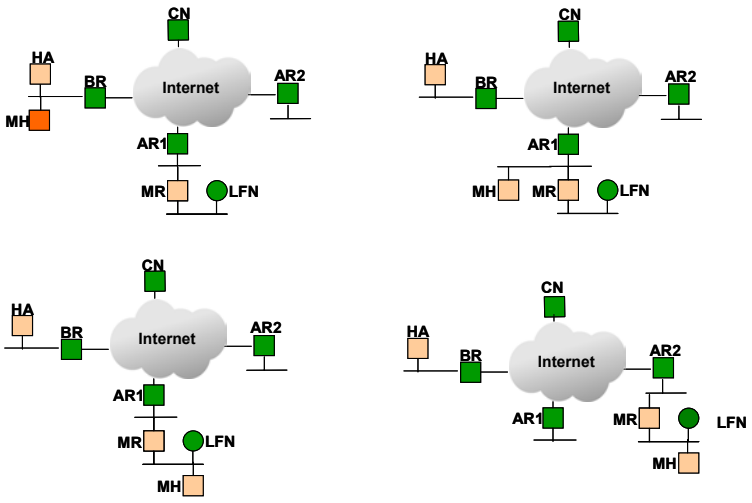


Figure 21: Mobile Network and Mobile Host at Same Home, Both Move, Initially Separated

The scenario in Figure 22 describes the case when MH and MR have different home links. The movement depicts MH attaching under the mobile network when the mobile network is still at home.

This scenario, as all other scenarios with several HAs, exposes the problem of *excessive tunnels*. When both MRs are away from home, communication between LFN and MH is encapsulated twice: once through each HA. The number of tunnels corresponds to the number of HAs in the picture.

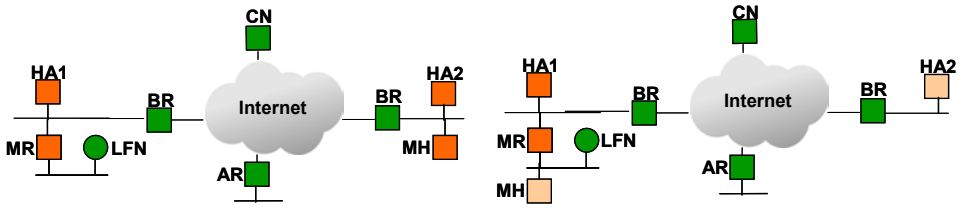


Figure 22: Mobile Network and Mobile Host with Different Homes, MH Visits

In Figure 23, the initial configuration of home domains is the same, but the first movement involves the mobile network attaching to a visited domain, then MH attaches to the mobile network and the final movement simultaneously positions MH in MR's home and vice-versa.

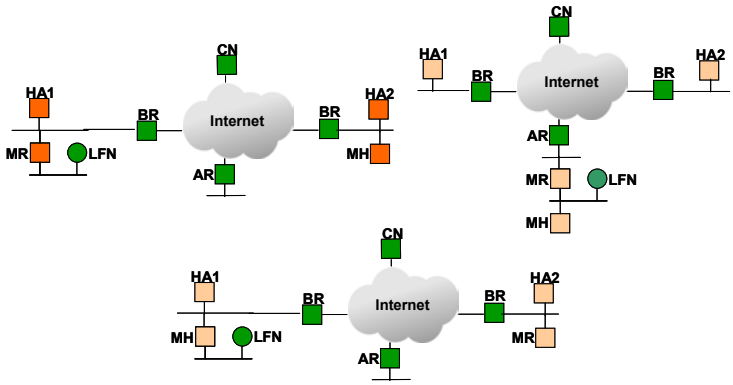


Figure 23: Mobile Network and Mobile Host, Different Homes, MH Swaps MR

In Figure 24 both MH and MR have the same home link, but have different assigned HAs. MH sends BUs to HA1 and MR to HA2. In this case there is no BR-HA loop.

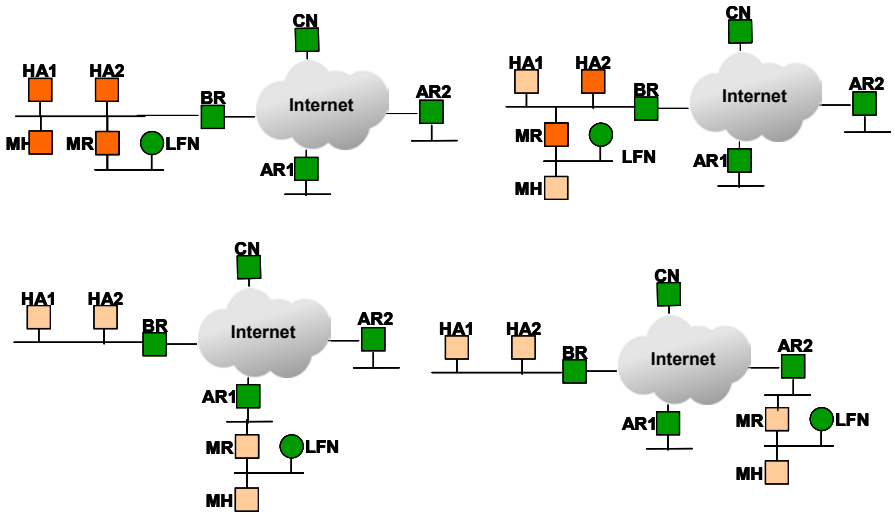


Figure 24: MR, MH, 2 HAs in Same Home Network

2.4.2.3 "Mobile" Home Agent

Figure 25 presents a Home Agent permanently attached to a mobile network.

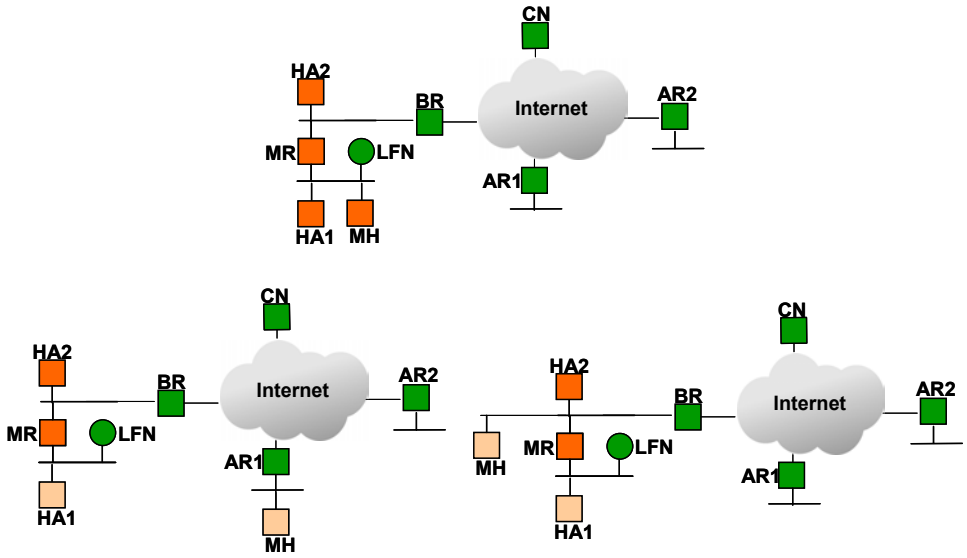


Figure 25: HA inside Mobile Network, Mobile Host Moves

In Figure 26, the HA moves homogeneously with the mobile network, thus it becomes "mobile". However, the HA is not experiencing mobility in the true sense, because it doesn't send BUs and doesn't change its address when the mobile network moves.

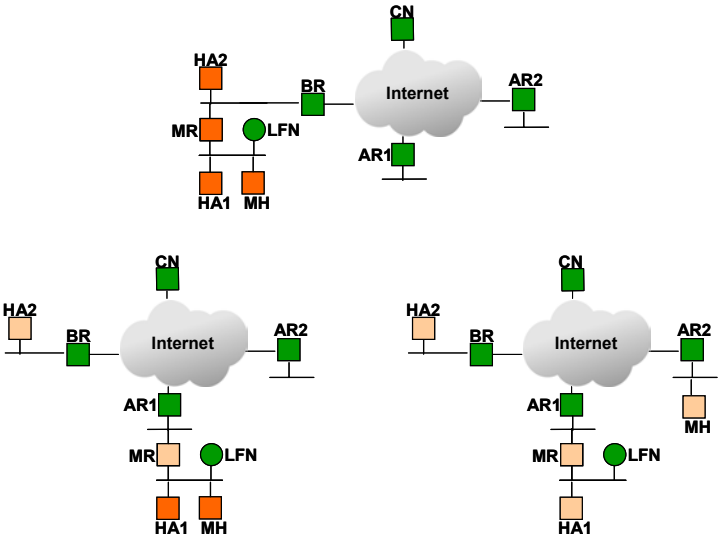


Figure 26: "Mobile" HA, MR and MH Move

2.4.3 Analysis of Supported Nested Scenarios

Figure 27 presents the simplest case for nested mobile networks. The two mobile networks are assigned to the same Home Agent and have the same home link. The figure depicts the initial movement of MR1 towards AR1 and then the movement of MR2 "nested" under MR1. This configuration helps describing the problem of *externally influenced intra-aggregation communication*. Consider that LFN1 and LFN2 communicate datagrams. When MR1 is disconnected from AR1, LFN1 and LFN2 will loose communication even if they are physically linked by MR2. This is due to lack of reachability of HA. Normally, all communication between LFN1 and LFN2 in this nested configuration will be tunnelled through HA.

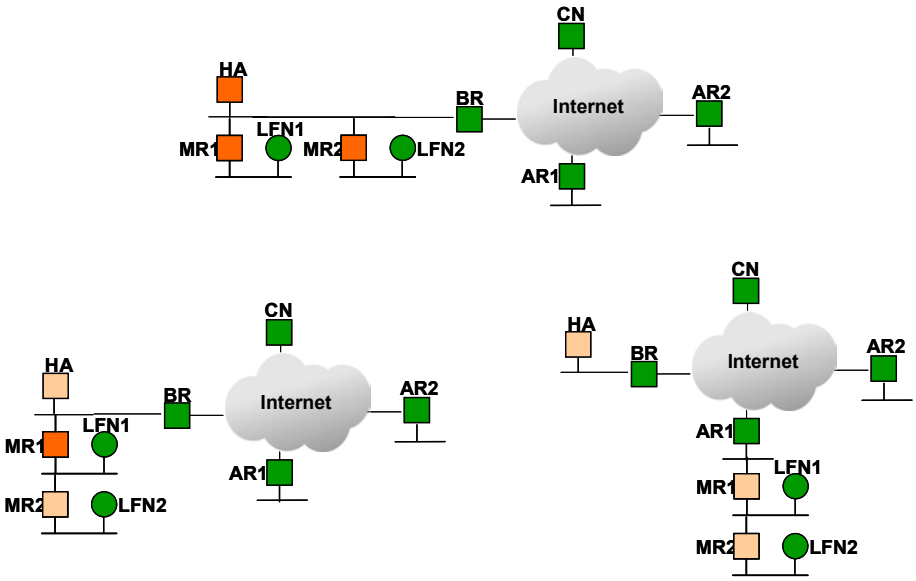


Figure 27: Nested Mobile Networks with Same Home

Figure 28 depicts a case where each MR is assigned a different HA, but has the same home network. As in the MH-MR case, the assignment of one HA for each mobile entity implies the absence of the BR-HA loop. Of course, it is not possible to plan for a home network where each mobile entity is assigned one HA, the number of mobile entities can be rather large.

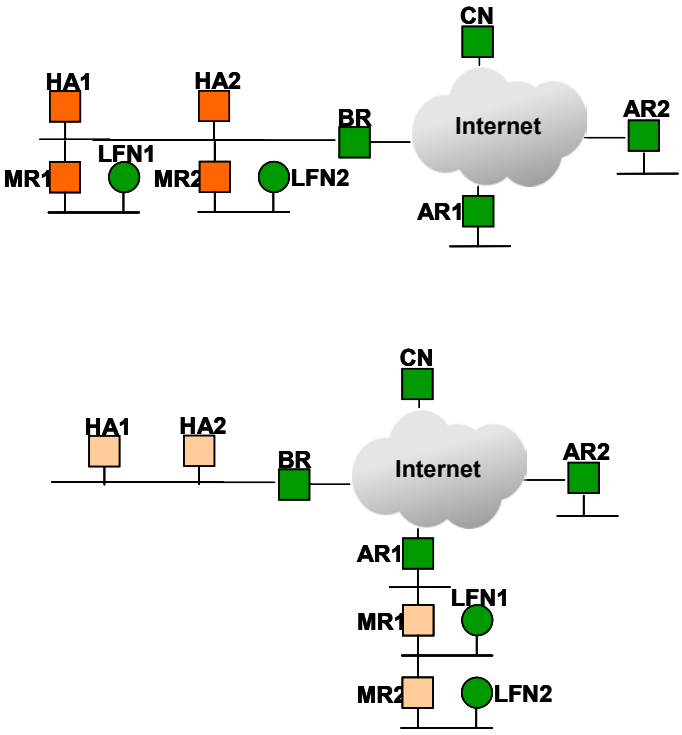


Figure 28: Nested Mobility without the BRHA Loop

Figure 29 presents the most generic case for nested mobility. Each MR belongs to a different network. MR's attach in a "nested" manner as presented. This configuration can support any number of different MRs of different homes that nest in a "serial" manner into an aggregation of nested mobile networks. Its important drawback is excessive tunnelling, where each packet is tunnelled a number of times that corresponds to the number of different HAs.

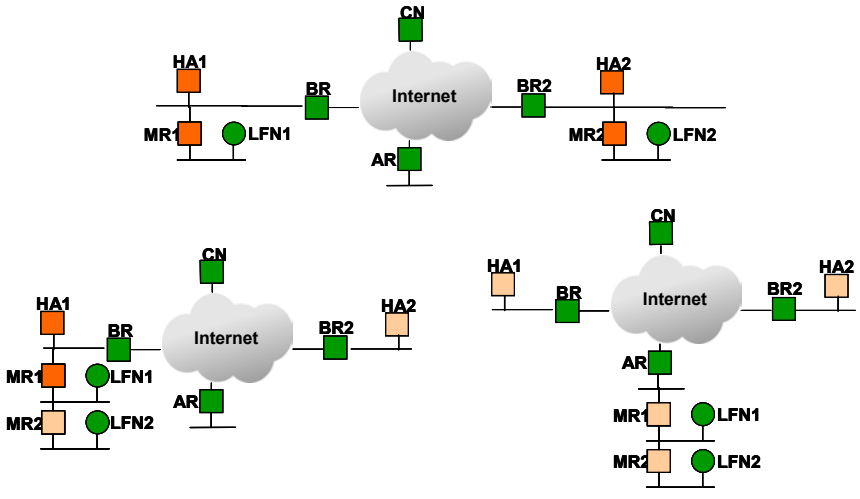


Figure 29: Nested Mobility with Different Homes

Figure 31 presents another nesting case, where the initial configuration involves a "mobile" HA. First, MR2 attaches under AR1. The MR1 leaves home and attaches under AR2.

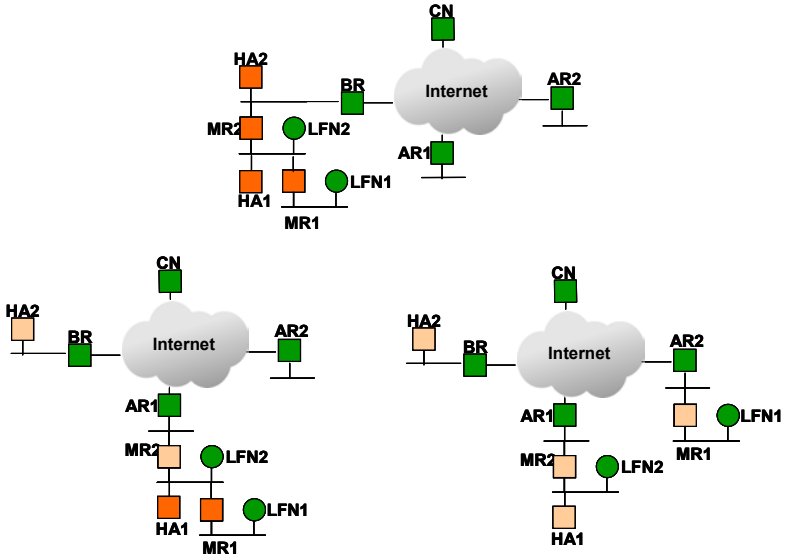


Figure 30: Nested Mobile Networks with Initial "Nesting"

Figure 31 is a particular case of nesting for "mobile" HA. The first movement involves MR1 leaving home and attaching under AR2. Then MR1 attaches under AR1. Finally MR2 attaches under MR1. This final movement is impossible with the MRHA approach as described previously. When MR2 tries to attach under MR1 it will generate a BU towards HA2. This BU will be encapsulated by MR1 towards HA1. However, HA1 is unreachable at that moment, since it is behind MR2 and HA2 does not have the binding yet. The MR1-HA1 and MR2-HA2 are "crossing over" one another.

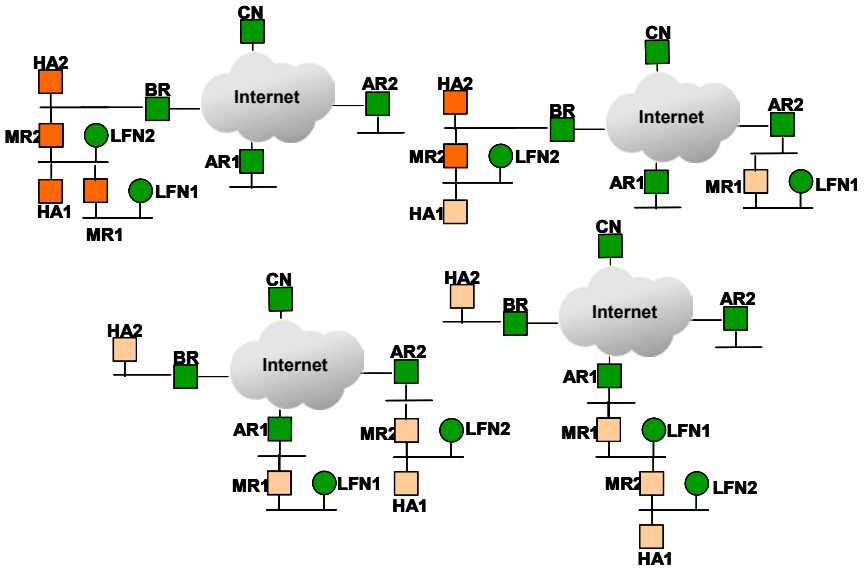


Figure 31: Nested Mobile Networks with "Crossover" Tunnels

2.4.4 Multi-homing and Multi-access

2.4.4.1 Multi-homing

In general, it is assumed that IPv6 will support *multi-homing* and this is mentioned in several documents, for instance in [29]. But in all cases details on this are missing. Recently, the IETF *Multi6* workgroup [30] has started to analyze this issue. In this context, a

"multi-homed site is a site that has more than one connection to the public Internet with those connections through either the same or different ISPs."

Another, more formal definition can be found in [31], consisting of three steps:

- A *site* is an entity autonomously operating a network using IP and, in particular, determining the addressing plan and routing policy for that network.
- A *transit provider* operates a site, which directly provides connectivity to the Internet to one or more external sites. The connectivity provided extends beyond the transit provider's own site. A transit provider's site is directly connected to the sites for which it provides transit.
- A *multi-homed* site is one with more than one transit provider.

As already mentioned, the application of this notion of *multi-homing* to mobile networks is problematic, because a mobile network not necessarily has to be a site. There is a quite good survey available, presenting possible approaches related to multi-homing at network- and transport level [32]. The two most important solutions are the following ones:

- A site only receives one network prefix from one ISP. Redundancy, load sharing and session continuity are achieved by a tight coordination between the different ISPs.
- A site has several prefixes, one from every ISP. Secondary links, i.e. tunnels, are established between the site exit routers and ISP's border routers, which are used in case of a link failure of a primary link. This requires almost no coordination between the different ISPs, but does not provide load sharing. [33] is such an example.

There are some more ideas presented in [32], but none of them is mature enough to be deployed. Furthermore, there is a proposal for a transition solution based on native address translation (NAT) called Multi Homing Translation Protocol (MHTP) [34]. The main idea behind MHTP is that multi-homed traffic is transformed into single homed traffic at a router close to the source and transformed back into multi-homed traffic at the last router before the destination. MHTP is not a routing protocol but relies on Border Gateway Protocol 4+ (BGP4) for decisions regarding the selection of the optimal path. Each Top Level Aggregation (TLA) is required to have a translation router, called MHTP rendezvous point, connected to the rendezvous-points of other TLAs. All in all, MHTP is designed for very static multi-ISP scenarios and does not address a dynamic multi-radio environment.

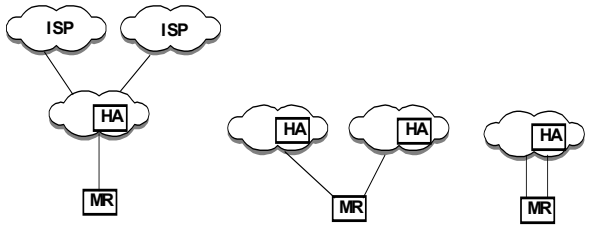
A common property of all these multi-homing concepts is that they assume rather static scenarios. It is not simple to apply them to dynamic changes of the network topology, which certainly will occur when mobile networks are considered. In other words: If a mobile network is connected to Internet by different ISPs at the same time, probably new mechanisms are needed to handle this situation.

2.4.4.2 Multi-access

Multi-access is the capability to connect a terminal to several network attachment points of different technologies simultaneously for obtaining access to the same application services. In addition each access system may provide further different application services. There can be simultaneous connections to different access systems, or connections to only one access system at a time. In a multi-access scenario the mobile network nodes can have multiple IP interfaces: they are multi-homed.

The following sections distinguish between multi-homing and multi-access topics on the one hand dealing with the egress interface of the MR and on the other hand with the ingress interface of the MR.

2.4.4.3 MR egress interface issues



a) b) c)

Figure 32: Multi-homing multi-access scenarios

HA Site multi-homing: In this case the focus is on the network side. Figure 32a) shows a multi-homed network. However, if the home network of a moving network is multi-homed, this is invisible to the MR, since all traffic to and from the MR is tunnelled between the HA and MR. Hence site multi-homing is here not considered further.

MR multi-homing: In this case the moving network is multi-homed. One or several mobile routers could provide multi-homing. In the following only one MR is assumed. Figure 32b) shows a multi-homed moving network, where the MR is connected to different home networks. In this case the MR can select the appropriate home network. However the MR-HA bi-directional tunnelling "hides" the access system. If the home network supports different access systems, the MR could not select the best access system.

MR multi-access: Figure 32c) shows a multi-homed moving network, where the MR is connected to one home network, but over different access systems. The MR acquires a CoA at the different access systems. The MR sets up a bi-directional MR-HA tunnel over each access system. To select the most suitable path, the MR must be provided with enough information for making the policy decision on the interfaces to be used. An example could be to use always the link with the highest bandwidth or lowest delay. Moreover, the selection might be guided by application specific criteria.

Usually, to divert traffic from different services to different interfaces the moving network must use different CoAs when initiating connections. When the moving network changes its point of attachment the MR-HA bi-directional tunnel is updated according to the new CoA. In a multi-access scenario the mobile router might hand over active transport connections from one interface to another by using global mobility management, i.e. Mobile IP to update the CoA at the HA.

Unfortunately, the new address binding diverts all traffic to the new access system. A solution which is depicted in Figure 33 would be to collocate with the HA a flow router that differentiates the traffic on a per flow basis [35].

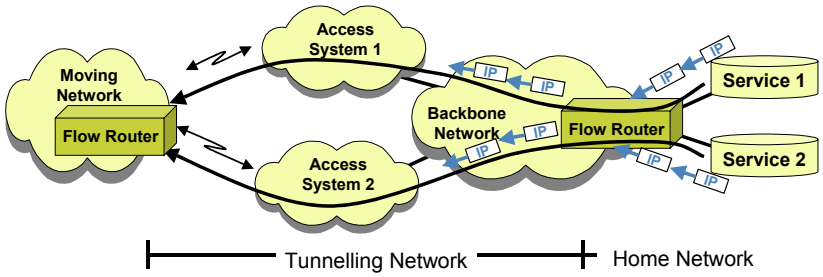


Figure 33: Flow routing for multi-access mobile networks

Optionally a flow can be identified based on the source/destination address, source/destination port number, transport protocol number quintuple, or based on the IPv6 flow label combined with the source address of the CN.

In a multi-access scenario the HA maintains a binding cache consisting of Home Address – CoAs mappings. In this case of multiple CoA the HA investigates the flow to forward to the corresponding binding. Technically, the flow router employs Hierarchical Mobile IPv6 (HMIPv6) with extensions to allow more elaborate traffic distribution [36]. The mobile router controls the flow routing and informs the flow router in the home network about the flow distribution over the access systems.

In a moving network the Local Fixed Nodes (LFNs) and MHs are not directly aware of the multi-homing, because all traffic is routed to the MR. However, the LFNs and MHs will have application specific demands. Therefore they must register these demands at the MR. Please note that this requires an interworking between the application layer and the network layer. An approach to distribute the traffic over the appropriate access systems is to collocate a flow router with the MR. The MR distributes the available access system resources according to the demands. The MR implements an optimization procedure to map the flows on the access systems. Vice versa the MR notifies the LFN if the access system capabilities change due to movements. Figure 34 shows the registration procedure.

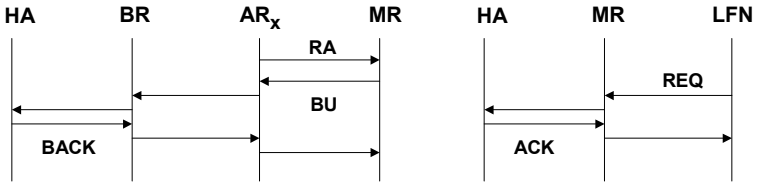


Figure 34: Tunnel set-up and flow routing set-up

The LFN will send the packets to the MR. The MR intercepts the packets and tunnels them over the appropriate interface depending on the flow.

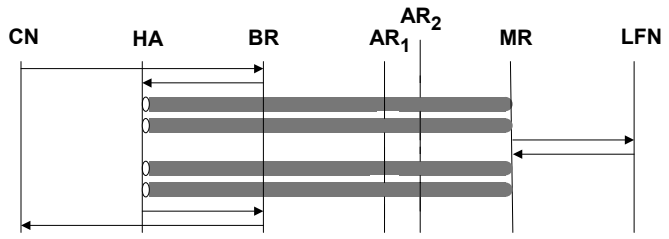


Figure 35: Communication with flow routing

A more detailed analysis of the traffic management implications and mechanisms can be found in section 3.5.3.

2.4.4.4 MR ingress interface issues

1. Single MR

Figure 36 shows a multi-homed moving network, where a single multi-access MR has one ingress interface to the mobile network and multiple egress interfaces, one to each access network. In this case, as it was described above, if a mobile network node has application specific demands a mechanism is needed which informs the MR about these demands and the mobile network nodes about the access networks' capabilities.

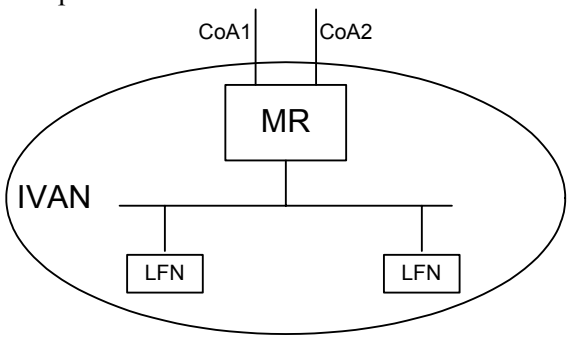


Figure 36: Multi-homed moving network with one mobile router

2. Multiple MRs, IVAN is a single subnet

Figure 37 shows a mobile network, where the MRs, LFNs and MNs share the same LAN. In this case, if mobile network nodes have application specific demands they can choose a MR by configuring their default router appropriately. Thus, there is no need for a special mechanism, as in the single MR case. However, there is still need for a mechanism to inform mobile network nodes about access networks' performance.

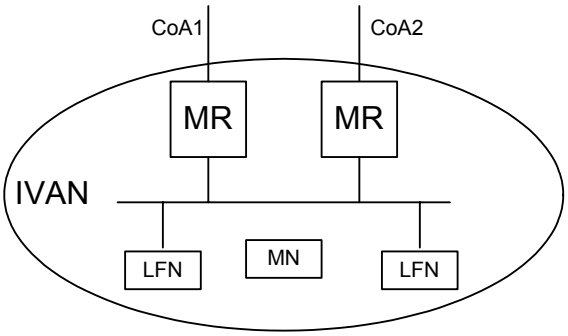


Figure 37: Multi-homed moving network with multiple mobile routers, one IP subnet

Moreover, mobile routers has to detect the presence of other mobile router in the mobile network [81], for instance to handle cases when a mobile router's egress interface is down. This can be achieved by manual configuration but for greater flexibility it is desirable for mobile routers to be able to discover alternate routes automatically. A mobile router can do so by listening for Router Advertisement message on its ingress interfaces. When a mobile router receives a Router Advertisement message with a non-zero Router Lifetime field from one of its ingress interfaces, it knows that another mobile router, which can provide an alternate route to the global Internet, is present in the mobile network.

Note, that in case of single mobile router with multiple egress interfaces the solution is trivial, since the mobile router should be able to "realize" it has multiple routes to the global Internet [81].

3. Multiple MRs, mobile network with several subnets.

Figure 38 shows the case where an IVAN posses multiple MRs and several IP subnets. In terms of access network selection, this case is similar to single MR case, while in terms of MRs presence discovering it is similar to multiple MR and one subnet in IVAN case.

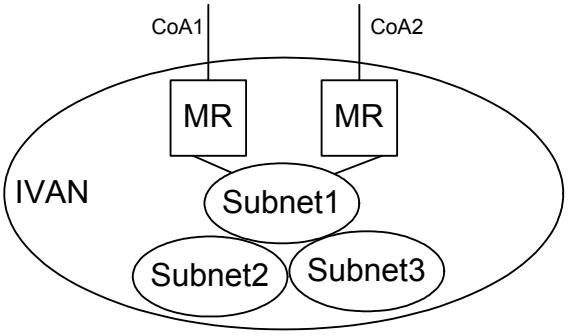


Figure 38: Multi-homed moving network with multiple mobile routers, several IP subnets

2.4.5 Multicasting

Delivery of multicast sessions to nodes within a mobile network is of paramount importance to the OverDRiVE demonstrator. The multicast mobility support is a task treated within the Work Package 2; for more detail on that support, please see the WP2 deliverables. We will contend to describe here only one particular approach, that is to enhance the Mobile IPv6 multicast "home subscription" method, that is designed for hosts running Mobile IPv6.

It is assumed that, in addition to performing mobility functions on behalf of the local fixed nodes, a mobile router will also perform all the multicast subscription protocols for the nodes within the mobile network, without interacting with the multicast routing protocols in the visited network. With the "home subscription" method, the mobile router will interact with the HA in order to cleanly maintain the mobile nodes' multicast subscription. In short, the nodes in the mobile network use MLD (Multicast Listener Discovery) protocol to inform MR about their subscriptions to the multicast sessions. The mobile router will run a multicast-enabled dynamic routing protocol with the HA, through the bidirectional tunnel MR-HA. Multicast sessions will be delivered to the nodes in the mobile network through this tunnel. Contrary to the "remote subscription" methods, the MR will not perform multicast routing interactions with the visited domain.

For a complete description of the home subscription method for multicast for Mobile IPv6 for hosts, see the OverDRiVE Work Package 2 deliverables [87].

2.4.6 Security Aspects

The sections that describe Access Control in the Dynamic IVAN management are describing in detail most security aspects in a mobile network environment. Here we mention only some aspects related to threats that might exist in the basic type of solution describe above. It is possible that a dynamic routing protocol is run between MR and HA in order to maintain connectivity between entities in the mobile network and entities in the home domain. Traditionally, dynamic routing protocols are run on boxes that benefit from the ultimate access control mechanism: access is physically reduced to skilled personnel in highly secure computer rooms. In the OverDRiVE context however, a mobile router is placed in a car and for some scenarios even in a shirt pocket of an IP networking-unaware person. In such a scenario, the threats can come from malicious users benefiting from physical access to a router exchanging routing information vital to the well working of the entire Internet. Unless tamper-proof devices are used, a potential attacker gains an opportunity to inject unofficial routes in the home domain (which in the worst case is trusted by the core Internet and thus attacker induces fake routes in the worldwide backbones). A proper security relationship must be developed between the home network and the mobile network deployed in a car or owned in a shirt-pocket. This security relationship should be refined such that owners of mobile networks are not able to fool the home domain about the routes towards each other. For example, if user A is granted rights to own mobile network B by the home domain, then user C granted rights to net D must not be able to re-route traffic of net B towards D.

2.4.7 Mobility Management for Mobile Nodes in Mobile Networks

In the bus and the car scenario if there is only one available radio technology (i.e. 802.11 WLAN) for the communication with the mobile router, there is no need for local mobility management, because inside this kind of vehicles the users do not move from one place to another, and even if they move their terminals can use the same intra-vehicular access router (AR) to stay connected with the mobile router. In larger vehicles (i.e. train, ship), where multiple AR could be used, there is a need for an IP layer mobility management scheme. The scopes of this section are to examine several mobility management solutions regarding intra-IVAN MN mobility, focusing on address assignment and handover management, and the cooperation of these solutions with MRHA.

2.4.7.1 Mobile IPv6 (MIPv6)

Mobile IPv6 is a classical solution based on IP tunnelling and source routing. A short introduction to Mobile IPv6 can be found in section 2.3.1.1. When a MN changes its access router inside

IVAN, it needs to obtain a new Care-of-Address (CoA) and needs to update at least its HA. Since this HA is outside the IVAN, the BU has to be sent through the MRHA tunnel and thus the handoff delay could be very large and several BUs should be sent through the scarce radio link (Figure 39).

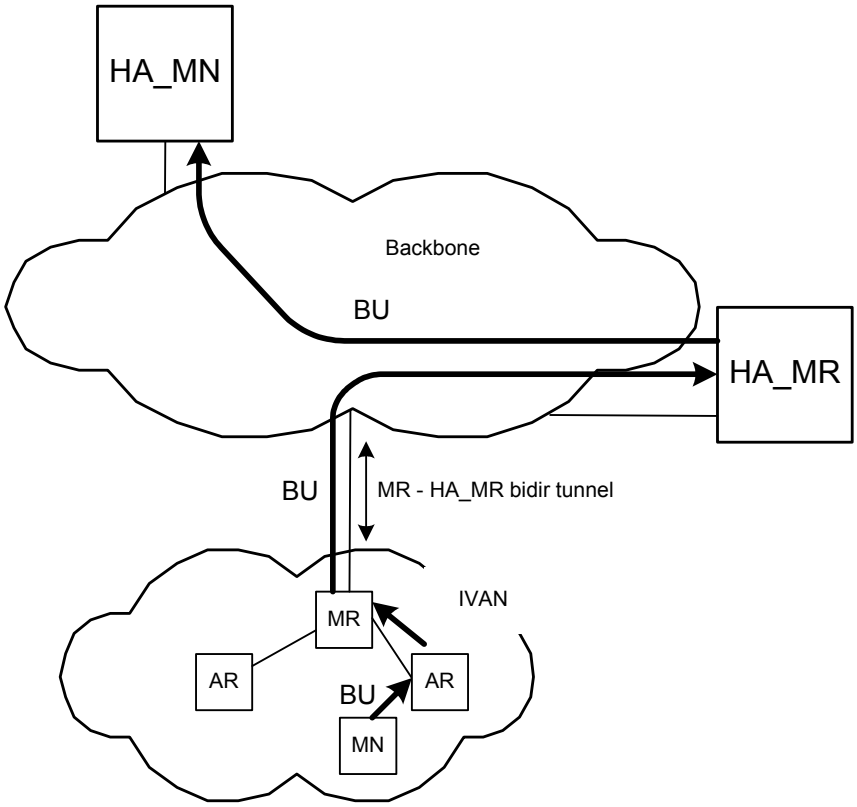


Figure 39: Handover inside IVAN with MIPv6

In order to overcome this drawback, there is a need for such local mobility management schemes, which hides these intra-IVAN movements from the outside of IVAN.

2.4.7.2 HMIPv6

Hierarchical Mobile IPv6 mobility management protocol (HMIPv6) is an extension to Mobile IPv6 and IPv6 Neighbour Discovery to support local mobility handling. It reduces the amount of signalling between the Mobile Node, its Correspondent Nodes and its Home Agent, and the handoff latency by placing a new Mobile IPv6 node in the network hierarchy, called Mobile Anchor Point (MAP) which limits the amount of Mobile IPv6 signalling outside the local MAP domain. Minor extensions to the mobile node operation are also needed, while the correspondent node and Home Agent operation will not be affected. A more detailed description about this solution can be found in section 2.3.1.1.

HMIPv6 and IVAN

Figure 40 shows the HMIPv6 architecture that can be used for L3 mobility inside the IVAN, in the case when the MRHA tunnel is used for network mobility management. One MAP is used, thus inter-domain handover is not needed.

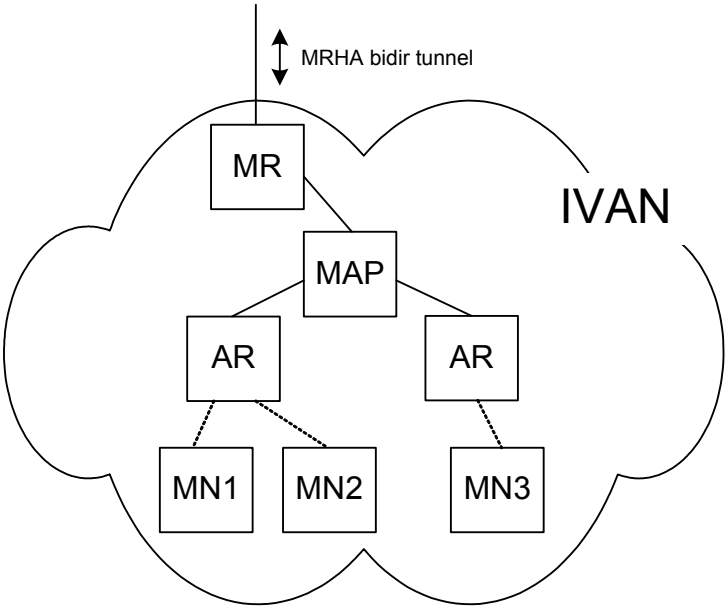


Figure 40: IVAN with HMIPv6

Login into the IVAN

When a mobile node moves into an IVAN, it needs to configure two CoAs: an RCoA and an on-link CoA (LCoA). These addresses are formed in a stateless manner. After forming the RCoA based on the prefix received in the RA's MAP option, the mobile node sends a local BU to the MAP. This BU specifies the MN-s RCoA in the Home Address Option. The LCoA is used as the source address of the BU. This BU will bind the mobile node's RCoA (similar to a Home Address) to its LCoA. The MAP (acting as a HA) will then perform Duplicate Address Detection (DAD) for the mobile node's RCoA on its link and return a Binding Acknowledgement to the MN. After registering with the MAP, the mobile node register its new RCoA with its HA through the MRHA tunnel by sending a BU that specifies the binding (RCoA, Home Address) as in Mobile IPv6. The home address option is set to the Home Address, the care-of address (RCoA) can be found in the source address field or the alternate-CoA option. The MN may also send a similar BU (i.e. that specifies the binding between the Home Address and the RCoA) to its current correspondent nodes.

Handover inside the IVAN

When the mobile node moves inside IVAN, it should only register its new LCoA with the MAP, sending a BU to it. In this case, the RCoA stays unchanged and BUs are not sent to its HA and CNs.

2.4.7.3 BCMP mobility approach

BCMP (BRAIN Candidate Mobility Management Protocol) [27] serves an alternative solution for the management of MN mobility inside the IVAN. A detailed description can be found in section 2.3.1.1. BCMP uses the MIND User Registration Protocol (MURP) to register the mobile nodes in the network (see [27]).

BCMP and IVAN

Figure 41 shows the BCMP based architecture in IVAN. The Mobile Router (MR) acts as GW of the IVAN and has no BCMP capabilities. One ANP is used, thus inter-domain handover is not needed in this case.

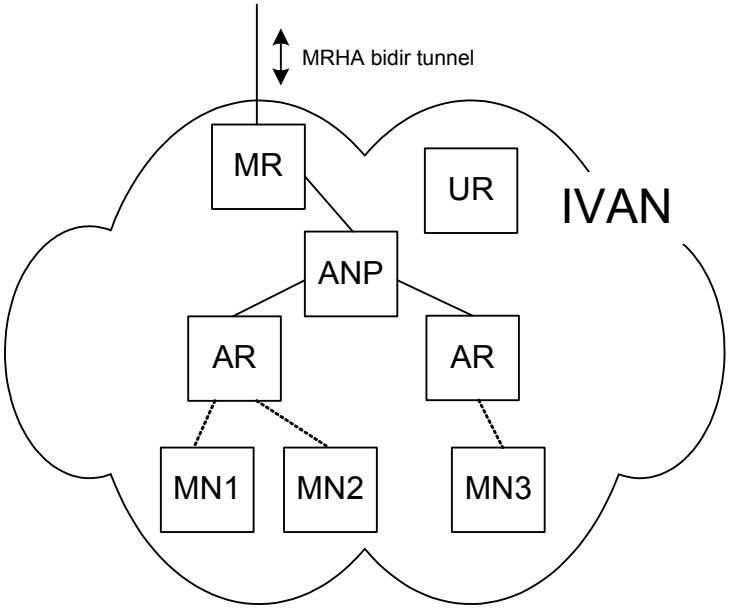


Figure 41: BCMP based architecture in IVAN

Address assignment

When the MN enters IVAN, it first logs in to an AR. Hence, it has to request a new CoA. According to the BCMP method, the address distribution inside IVAN is the task of the ANP. The ANP thus starts an AAA procedure to identify and authenticate the MN and then allocates a new CoA. The MN informs its HA about this new address by sending a BU message via the MRHA bi-directional tunnel. This step has to be done only once, when the MN first enters IVAN. It is not needed to change CoA even when the MN moves from an AR to another one. This implies that while in the IVAN, the MN has a permanent CoA. Thus, exact registration of current positions of MNs inside the IVAN is desired. Hence, the ANP maintains a table of CoAs currently in use by MNs together with the addresses of ARs so that the ANP can decide which way to send a packet destined to a MN's CoA. Thus, when e.g. a packet arrives from the MRHA tunnel, it is forwarded to the ANP. The ANP looks up its table and checks the CoA -> AR associations. Then the ANP encapsulates the packet and tunnels it towards the chosen AR. When a handover occurs between ARs it is the ARs' task to inform the ANP to change its entry in the table.

In BCMP, a new CoA must be obtained if the MN changes ANP. In our case this does not occur since one single ANP can handle a whole IVAN's needs.

Handover inside the IVAN

In BCMP there are two ways to perform the handover when a MN changes Access Routers – a regular and a prepared way. Since the handoff procedure only involves entities below the level of the MR, the same steps described hereunder can be applied for the case of MNs changing ARs in an IVAN.

If the handover is not planned, e.g. the MN lost connection with the old AR (oAR), the MN first sends a check-in message to the new AR (nAR). Since the nAR cannot authenticate this message, it sends a query to the oAR. If the oAR recognizes the MN identified in the query message, it replies to the nAR with the MN's parameters and context. Knowing the context of MN, nAR is able to acknowledge MN's handoff. During this authentication process packets may arrive to the oAR, which is unable to transmit them to the MN simply because the connection between them does not exist. Thus, these packets are stored in the oAR's buffer. If the handoff happens without errors, the nAR indicates to build a temporary tunnel between oAR and nAR in order to transmit the buffered packets to their recipient, MN. In addition, the nAR sends a redirect message to the ANP, causing the ANP to change its CoA -> oAR entry to CoA -> nAR.

If there is a situation that the MN is within two ARs reach, but the MN would like to handoff from the current one to another one, a prepared handoff can be performed. In this scenario the current AR will be referred as old AR (oAR) and the new candidate AR as new AR (nAR). First the MN sends a handoff preparation signal to the oAR, causing the oAR to send the MN's attributes and context to the nAR. Upon receipt, the nAR replies to the oAR. This triggers an acknowledgement message from the oAR to the MN and a request for building a temporary tunnel between the oAR and the nAR. From this time on, packets destined to the MN via oAR will not be posted to MN but to nAR through the temporary tunnel. At the time MN checks in at nAR it delivers packets stored in its buffer to MN, builds the tunnel between oAR and nAR down and sends redirection message to the ANP, causing the ANP to change its CoA -> oAR entry to CoA -> nAR.

Summarizing the features of the technology and the examinations mentioned above, we can conclude that the following problems can be solved with BCMP:

- the handoff can be processed quickly and full context of the MN can be transferred to the new AR
- there is no need for gaining new CoA at every time the MH changes AR. Thus, BU storm can be avoided and hence signalling overhead can be minimized.

As drawback we can mention, that since BCMP is working with tunnels, multicast and route optimization is not supported in a BCMP network.

2.4.7.4 RIPng/OSPF based local mobility approach

Another possibility of hiding the movements inside IVAN is to use a common routing protocol (RIPng/OSPF) in order to propagate the necessary information when a MN changes its AR. It means that MN does not change its CoA as moving between AR's inside IVAN, and when handover occurs informs the new AR about its CoA. The AR receiving this signal inserts a host route into its routing table. This information is then propagated throughout the IVAN by the traditional mechanism provided by the routing protocol involved. Similarly, the old AR must be notified by the MN about its departure. In response to that the old AR has to remove that entry from its routing information base and flood to other routers that the MN is no longer reachable through it.

Possible Advantages

- There is no need for a special mobility management entity in IVAN
- Routing is highly optimized between MR and MN's (if it makes sense in that special IVAN topology)

Possible Disadvantages

- AR and MN software must be modified with AR-MN signaling protocol.
- Each router has to maintain O(#MN) routing table entries.
- Convergence speed
    - OSPF: after flooding, each router in the IVAN has to perform an SPF calculation, but with an efficient shortest path tree updating algorithms and with that special topology changes (MNs are just leaves of the tree) this could be made very fast.
    - RIP: convergence may be lengthy because of the slow propagation of information (counting to infinity problem).

2.4.8 Conclusion of the mobility management inside mobile networks

As seen above, the mobility management of MNs inside of the IVAN cannot be efficiently solved by the classical solution offered by the Mobile IPv6 method. With MNs simply changing ARs, a lot of updating actions are triggered involving many entities outside the IVAN as well, and this implies ineffective usage of scarce resources such as the radio link of devices. With the growing number of entities involved the route of binding update messages lengthens, the procedure of a handoff slows down, signalling overhead grows and thus, communication becomes less effective. These drawbacks can be more or less moderated by choosing a proper micro-mobility protocol for handling intra-IVAN movement of MNs. The selected protocol should hide the fact of MN's movement from the world outside of IVAN so that BU messages are not needed to be sent every time the MN changes ARs. If the chosen protocol fulfils the need of handling MN movement exclusively inside the IVAN, it also gives solution for the problems entrained when the entities outside the IVAN are involved.

3 Concept of Dynamic IVAN Management

3.1 Introduction

One essential part of the OverDRiVE concepts for moving mobile networks is management tasks for the IVAN. Here, the IVAN is viewed as a dynamic network with respect to number, types and preferences of nodes that are forming the IVAN.

Within the OverDRiVE project Dynamic IVAN management spans a lot of important tasks to be carried out. But to concentrate on aspects that are in particular important to mobile networks and reflect the dynamic nature of the IVAN, two important aspects are identified.

One important issue in mobile environments is security and prevention of threats. While wired networks are often installed inside a building and operated by a well known administration, nodes inside the IVAN do not always know each other and therefore no per se trust relationships exist. After inspecting security threats and describing a trust model for OverDRiVE, a concept of network access control is presented to reflect the need for trust inside the IVAN.

A further topic that is handled within dynamic IVAN management is the observation and management of traffic that encompasses the MRHA tunnel. With respect to the multiple access systems that the IVAN can use to attach to the Internet, the path between a MR of the IVAN and its HA changes according to the available wireless technology. The tunnel is faced with changing characteristics of the network path by means of bandwidth, delay and jitter. In this situation dynamic IVAN management provides a scalable concept for traffic management.

3.2 Scope of AAA in OverDRiVE

The concepts of dynamic IVAN management make use of AAA as a fundamental service. As AAA does not only cover mobile networks but also many issues within the fixed Internet world, the scope to apply and extend AAA ideas is bound to the two main concepts of dynamic IVAN management:

- Network Access Control and
- Traffic Management.

Network Access Control utilizes the AAA backbone (Diameter, [55]) and provides a basic infrastructure for controlling and limiting access from the service provider point of view. Likewise the clients and their home networks can determine which kinds of services are provided and which policies are used. Generally, AAA provides a basis to prevent security flaws, which are described in section 3.3.2.

Within the concept of Traffic Management the AAA backbone is mainly used to allow signalling of current link characteristics between the IVAN and its home network to manage the traffic that is conveyed via an MRHA tunnel. This task is a basic preparatory work to prioritize traffic and to take into account the impact of vertical handovers. OverDRiVE does not seek for a QoS scheme like IntServ or DiffServ for the IVAN and nodes within, but to mirror the need of favouring vital information exchanges, e.g. vehicle maintenance tasks, instead of leaving the available bandwidth to stubborn data flows.

3.3 Entities, Security Threats and a Trust Model for OverDRiVE

Before the conceptual work is laid out, a close look is taken at the entities, which are involved in dynamic IVAN management. From this point a description of security threats is given. These threats are mainly concerned with the security issues at the network layer that could arise on the last hop.

Most of these security threats exist because of the lack of trust in the mobile environment. Therefore a trust model by means of trust relationships is described for the IVAN and corresponding entities. Here, the background of an existent AAA backbone and roaming agreements is used to establish trust relationships.

3.3.1 Entities

In this section a short overview is sketched about the entities that are involved in network access control. While the nodes that participate in the network and host mobility tasks are already presented in chapter 2, additional AAA nodes for dynamic IVAN management are introduced. The following AAA entities (see Figure 42) of different domains are referenced throughout this chapter:

- The home AAA server of the IVAN that includes the MR, LMN and LFN, ($AAA_{(MR..)}$)
- the home AAA server of ARs and ($AAA_{(AR2-3)}$)
- the home AAA server of the VMN ($AAA_{(VMN)}$).

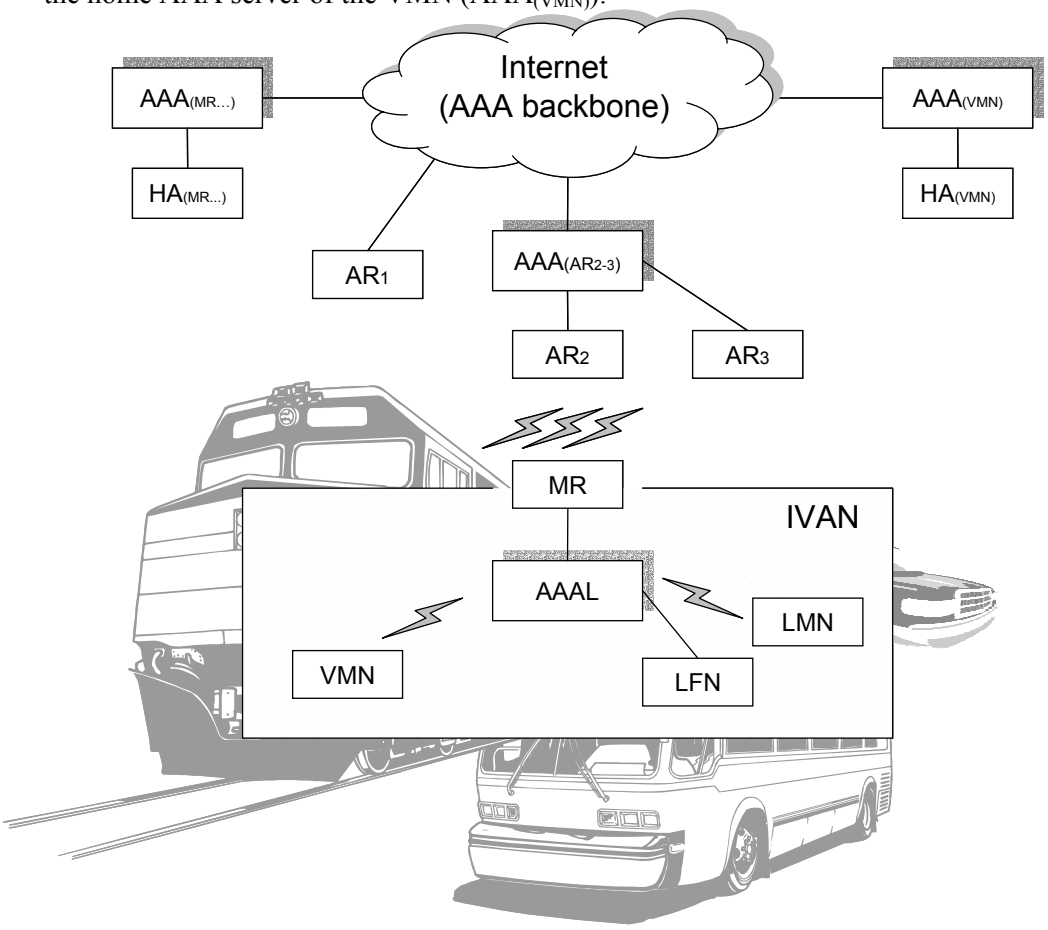


Figure 42: Network Entities

Additionally, a local AAA server (AAAL) inside the IVAN is introduced to allow performance enhancements that are further described in section 3.4.2.
It is assumed that all AAA servers in the fixed Internet can contact each other to perform AAA specific tasks, e.g. roaming agreements for mobile nodes can be checked to test whether it is allowed for a node to attach to a foreign domain.

3.3.2 Security Threats

Before taking a look at the concept of network access control this section describes security threats that are present in public access scenarios. In this section an overview on threats is given from a network layer perspective.

With respect to the IVAN, different link layer technologies are available to access the Internet. The MR connects the IVAN to the Internet via

- Cellular network technologies (e.g. UMTS, GPRS),
- Broadcast technologies (e.g. DVB-T) and
- Wireless LAN (e.g. 802.11b, 802.11a).

Furthermore inside the IVAN different technologies are envisioned like:

- Fixed vehicular network technologies (Controller Area Networks (CAN), Media Oriented System Transport (MOST)),
- LANs (e.g. Ethernet),
- Wireless LAN (e.g. 802.11b, 802.11a),
- Personal Area Networks (e.g. Bluetooth) and
- Peripheral Connections (e.g. USB, Firewire).

The listed technologies provide different types of communication channels, i.e. point-to-point links and shared medium access can be provided. Moreover only threats that arise on shared medium access technologies are discussed. This suffices, as a point-to-point link can be seen as a special case of a shared medium link where only one communication peer is present. Thus, the common scenario is a public access network where access is given via

- a shared medium between the MR and AR and
- a shared medium between the nodes in the IVAN.

The variety of protocols leads to a number of different threats, however they can be filed as follows:

Denial-of-Service: (DoS) The attacker attempts to prevent legitimate users of a service from using this service by e.g. "flooding" a network or disrupting a service to a specific system or person.

Eavesdropping: The attacker taps to the transmission media and reads the contents of data in transmissions.

Man-in-middle: The attacker intercepts messages, possibly substitutes information and retransmits them so that the two original parties still appear to be communicating with each other directly.

Replay attack: The attacker captures or intercepts a user's authentication tokens and directly uses these authentication tokens (e.g. session ID in URL, cookie, etc.) to

access service restricted to a certain user's account omitting user authentication.

Service Theft: Using the service of someone else, e.g. by capturing EAPOL-Logoff (Extensible Authentication Protocol Over LAN) and using borrowed credentials (unauthorized usage of addresses).

As most threats at the network layer are based on common procedures like:

- eavesdropping or sending data packets,
- creating or modifying data packets,
- acting with a sniffed link layer or network layer address and
- learning information about a communication peers,

particular threats may fall into multiple categories. There is not always a clear border between different attack types. For example a Man-in-the-Middle attack can be used to start a DoS attack by dropping some or all packets of the affected node

3.3.2.1 Threats at the physical and link layer

As OverDRiVE aims at the development and extension of IPv6 based protocols, it is out of the project's scope to define security enhancements that exclusively affect the physical or link layer (e.g. enhancements of 802.11 security mechanisms). Additionally, the encryption of application data is out of the scope of the OverDRiVE project, as this tasks can be is performed above the network layer. Although OverDRiVE's concepts do not present countermeasures against particular physical layer, link layer or cryptography related threats some of these are presented as they can arise in the context of public wireless networks.

Frequency Jamming: Within the wireless context it is possible to jam the frequency of the used wireless technology almost every time.

Hijacking: The modification of link layer specific management frames, e.g. in IEEE 802.11 networks, is an additional threat that arises from below the network layer. While acting as a legitimate access point, an attacker can start a DoS and try to continually disconnect devices from an access point.

Cryptanalysis: Today's cryptographic methods are based on the principle that it is very unlikely to gather the secret that communication peers use. Within the wireless context a number of researchers exposed flaws in the Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11 standard. As a result intruders have increasingly begun to develop techniques of exploiting these weaknesses.

Means to avoid these threat scenarios can be provided by integrating active monitoring for potential intrusions or extensions of the specific link layer protocol, e.g. IEEE 802.11i. These issues are out of OverDRiVE's scope as they cannot be tackled with network layer specific approaches.

3.3.2.2 Threats at the network layer

This section describes a set of threats that are present in public multi access scenarios. They are not only important to OverDRiVE's mobile network architecture as they can also appear in

similar environments. The main objective of this section is to identify security flaws that must be taken into account for further AAA concepts.

As security is becoming a key aspect in many standardization groups and protocol design teams, this section also takes into account the progress that has been made in different IETF working groups [61][62].

The subsections take a look on security aspects from two viewpoints. Firstly, security threats from the client's perspective are described. Afterwards a discussion about security threats for the serving side is given.

Client-side security threats

A critical task for a mobile node is the attachment to a new network. After discovering a peer entity that provides access to the Internet via a router, a node has to configure its IP address. The peer entity that provides link layer access and the first hop router are not always known in a mobile environment, i.e. neither a Security Association [76] nor a shared secret is established. At this point, mechanisms like [77] and [78] cannot be used as the node has not yet configured its network layer address and therefore it is not possible to use transport protocols.

If the node that attached to the new network is not able to authenticate the unknown network entities, at least two threats can arise in this scenario: False router advertisements and the frustration of auto-configuration for IPv6.

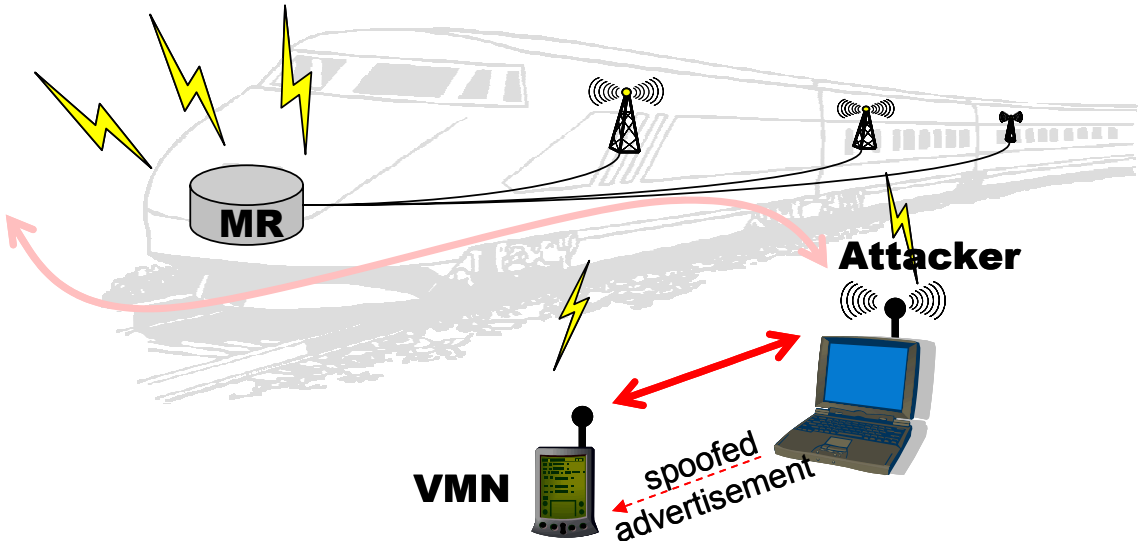


Figure 43: False Router Advertisement

Discovering the default gateway

In Figure 43 a scenario is depicted where the attacking node sends a false router advertisement to a VMN. After detecting different possible link layer access points the VMN decides to associate with the attacking node, i.e. none of the access points of the IVAN are used. The VMN tries to attach to the attacker, who is able to mimic an access point. Consequently, the VMN is subject to different threats:

- The attacking node acts as a proxy/bridge and advertises the same prefix and address configuration style as the IVAN.
- The attacking node advertises its own different prefix and advises auto-configuration.

- The attacking node advertises its own different prefix and runs a DHCP-service.

In all cases the attacking node can wiretap and control the packet flow of the VMN. This opens up DoS as well as eavesdropping threats to the VMN. Here, a DoS attack can either be the sending of unusable advertisements to prevent the VMN from attaching to a network, or it can as well be a directed preparation of more sophisticated threats.

If the attacking node acts as a proxy or bridge and advertises the same prefix as the IVAN, it is also possible for the attacking node to send packets on behalf of the VMN. This opens the chance for threats like service theft and remote DoS attacks. This scenario presumes that the link layer is not encrypted; otherwise the attacking node might be unable to inject wrong packets.

If the Attacker node sends out its own prefix, it can act as a MR inside the IVAN and route all traffic through its own home network. This is possible due to the use of

- IPv6 Stateless Address Auto-Configuration [82] via Router Advertisements or
- the Dynamic Host Configuration protocol [83].

Even if the IVAN supports a protected link layer protocol by means of authentication or encryption, this scenario can take place as the attacking node opens up its own MRHA tunnel that is not visible to the IVAN. The Attacker node acts as a router between the VMN and other nodes. Thus, the attacking node is able to wiretap particular messages, e.g. registration messages like dynamic DNS [79] or Binding Updates [84] to utilize route optimization. A Binding Update to a correspondent node (CN) involves the Return Routeability Procedure [84], which is used to agree upon a shared secret between the VMN and the CN. As the Attacker node can intercept these messages, it is able to start an attack on behalf of the VMN – the current mobile IPv6 draft [84] does not oblige a mobile node to encrypt Return Routeability messages towards it's HA, but it advises to do so (section 6.1.3 in [84]).

The inherent challenge to overcome the problem of false router advertisements is to identify the router. The main means to avoid the attachment to a node that sends out false router advertisements is that the network layer must be aware of the peer's identity. Thus, the node is able to verify the identity of the node that sends router advertisements.

Communication with local nodes

Additional threats can arise at the network layer while using the Neighbour Discovery protocol [80] without authentication information. Neighbour Discovery (ND) is used for a couple of tasks that must be carried about, examples are:

- determine link-layer addresses of peers,
- perform duplicate address detection,
- advertise additional network prefixes and
- redirecting traffic to a preferable on-link router.

The threats based on the use of ND are not only present in mobile environments but also in fixed and wired networks. In the following these concerns are depicted.

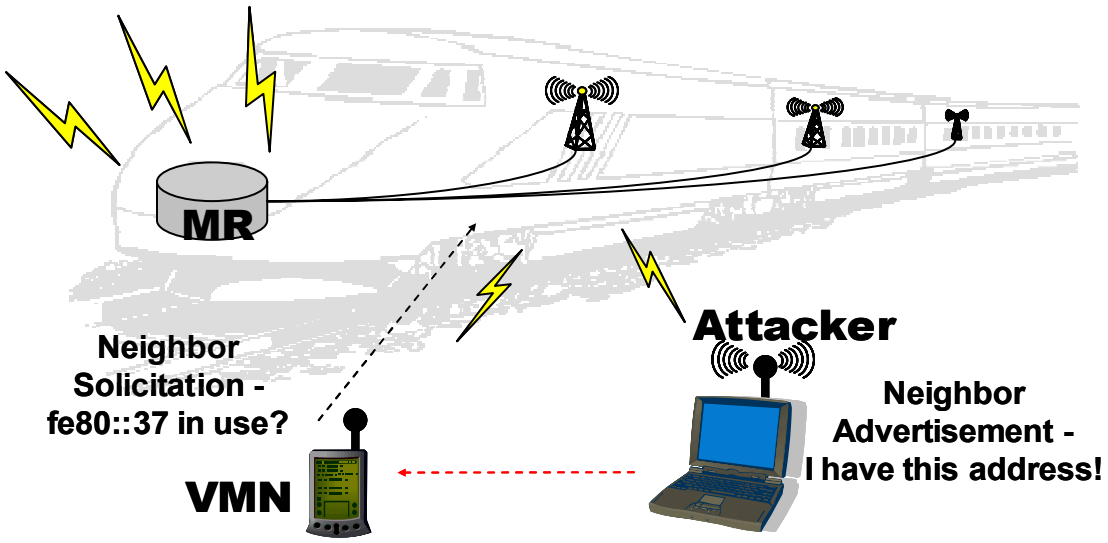


Figure 44: Frustrating Stateless Auto-Configuration

When a VMN attaches to the IVAN and has detected the available on-link prefixes, it has to configure its IPv6 addresses. As mentioned in the prior section, this can be performed in a stateless or stateful (e.g. DHCP) manner. The stateless version utilizes the co-operation of all nodes that are at the same link in contrast to the DHCP-link mechanism that is based on a server that assigns addresses to nodes as discussed in the prior section. In case of a stateless address auto-configuration the node that prepares its IPv6 addresses uses Neighbor Solicitation packet asks via a multicast packet if a chosen address is already in use. If an attacking node gathers this packet and replies with a Neighbor Advertisement that claims the use of the address (see Figure 44), the affected node must restart the address configuration procedure. While the attacking blocks each configuration trial, the node is not able to configure an IP address and is therefore exposed to a DoS attack.

Even when a node has attached to the network, multiple messages that involve the ND protocol are vulnerable to security threats, e.g.

- **Neighbor Solicitation Message** sent by a node to determine the link-layer address of a neighbour, or to verify that a neighbour is still reachable can be forged.
- **Neighbor Advertisement Message** responses to a Neighbour Solicitation message to announce a link-layer address change can be faked.
- **ICMP Redirects Message** can be spoofed.
- **Path MTU messages** can be spoofed.

A solution to overcome the problem of spoofed messages sent by neighbour nodes is protection by message authenticating. Although, IPsec could do this in conjunction with AH as a matter of principle, it is not clear how to solve the problem this way (see section 3.4.1).

Server-side security threats

The services provided by an IVAN are also due to security threats. In the following, one example is sketched that describes a class of threats – good entities go bad. A second scenario describes the need for traffic observation if the MRHA tunnel is absent. Additionally, the consequences of missing authentication are presented.

Routing involved threats

A trustworthy node like the MR of an IVAN can be infected, e.g. Trojans or viruses. In order to counter implied threats means must be provided to revoke authorization via online available blacklists.
The threat that a once good router goes bad can also have a large-scale effect regarding the MRHA tunnel (see section 2.4). It is possible that a dynamic routing protocol runs between MR and HA in order to maintain connectivity between entities in the mobile network and entities in the home domain. Traditionally, dynamic routing protocols run on boxes that benefit from the other access control mechanism, e.g. access is physically restricted to skilled persons in secured computer rooms. In the OverDRiVE context however, a mobile router is placed in a car and for some scenarios even in a shirt pocket of an IP networking-unaware person. In such a scenario, additional threats can come from malicious users benefiting from physical access to a router by exchanging routing information vital to the entire home domain of the IVAN, as sketched in Figure 45. Unless tamper-proof devices are used, a potential attacker gains the opportunity to inject unofficial routes in the home domain (which in the worst case is trusted by the core Internet and thus the attacker induces fake routes in the worldwide backbones). A proper framework of authorization must be established between the home network and the mobile network deployed in a car or owned in a shirt-pocket. This framework should assure that owners of mobile networks are not able to fool the home domain about the routes towards each other.

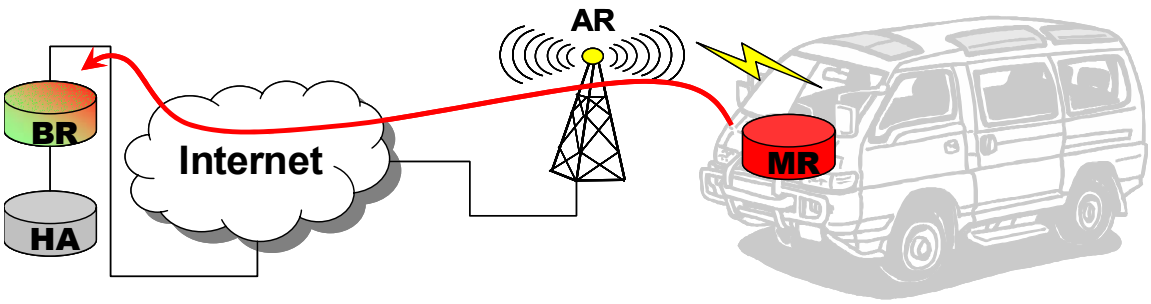


Figure 45: A good router goes bad

Misuse of Resources

One important issue for the operator of a network is the observance of economic principals. If an operator wants to provide services for mobile users two distinct approaches can be taken:

- royalty free usage or
- charging on the basis of roaming agreements.

If a particular service is provided that follows the second approach, the identity of the person to charge is very important. Furthermore the operator aims at an appropriate distribution of available services to each node that is participating in the network. These objectives can only be fulfilled by authenticating nodes or a corresponding person that uses a service. Furthermore, the operator has to check that resources are used in accordance with other conditions. For example, if a node is granted access to the IVAN and the uplink to the Internet cannot be used by all nodes because of a small bandwidth, congestion should be avoided by restricting access to services or allowing only a particular bandwidth to be used for a node.

Lack of Security Policy

A security threat that is beyond the scope of technical aspects is the lack of a security policy and rules that must be complied with. The statement of conditions that must be fulfilled for both, the network operator and the user can be used to clarify and prevent certain threats that are mentioned within prior sections.

This task should not only include overall principles how nodes and their users must behave while attached to a domain, but also identify the mechanisms and procedures used to prevent security threats. Furthermore, the explicit naming of applicable protocols helps to identify missing pieces of an overall security concept.

3.3.3 Trust Model for OverDRiVE

Before going into details on the protocols that can be used to secure communication inside the IVAN and extensions that must be designed, a close look at the different entities and their relation by means of trust are presented. This gives an overview how security threats can be prevented not only by means of a generic protocol but also by utilizing the inherent trust relationships present inside an IVAN. Here, mutual authentication is needed: Firstly, the network operator must be sure to whom services are delivered. Secondly, users must also be sure of the network they are communicating with in order to avoid being fooled, e.g. by rogue access points starting man-in-the-middle attacks. The first step is to derive the trust relationships that are needed to identify a trustworthy peer and to establish a secure communication. Two trust relationships are possible beside the initial non-existent relationship.

Static trust relationship: Two nodes have a static trust relationship if they are able to verify each other's claimed identity, i.e. they can authenticate each other without additionally involved entities. For example: both nodes have a commonly shared secret to authenticate data. This does not imply that no signalling is involved to agree on keys for subsequent data exchange, e.g. both can identify the communication peer without further signalling but need to agree on a cipher suite and keys to perform a secure data exchange. If not specifically mentioned, it is assumed that nodes from the same administrative domain have a static trust relationship.

Dynamic trust relationship: This kind of trust relationships is built via a system of static trust relationships. Nodes that want to establish a dynamic trust relationship may need to utilize static trust relationships to prove the claimed identity of a peer. Therefore, the decision whether or not an unknown peer is trustworthy may entail signalling. If not specifically mentioned, it is assumed that nodes from the different administrative domains have no static trust relationship and therefore need to establish a dynamic trust relationship.

Beside the differences stated, it is assumed that dynamic trust relationships exist only for a short time and may be re-established depending on the security policy that is used. E.g. a dynamic trust relationship between the IVAN and a visiting node lasts only until the latter leaves the mobile network.

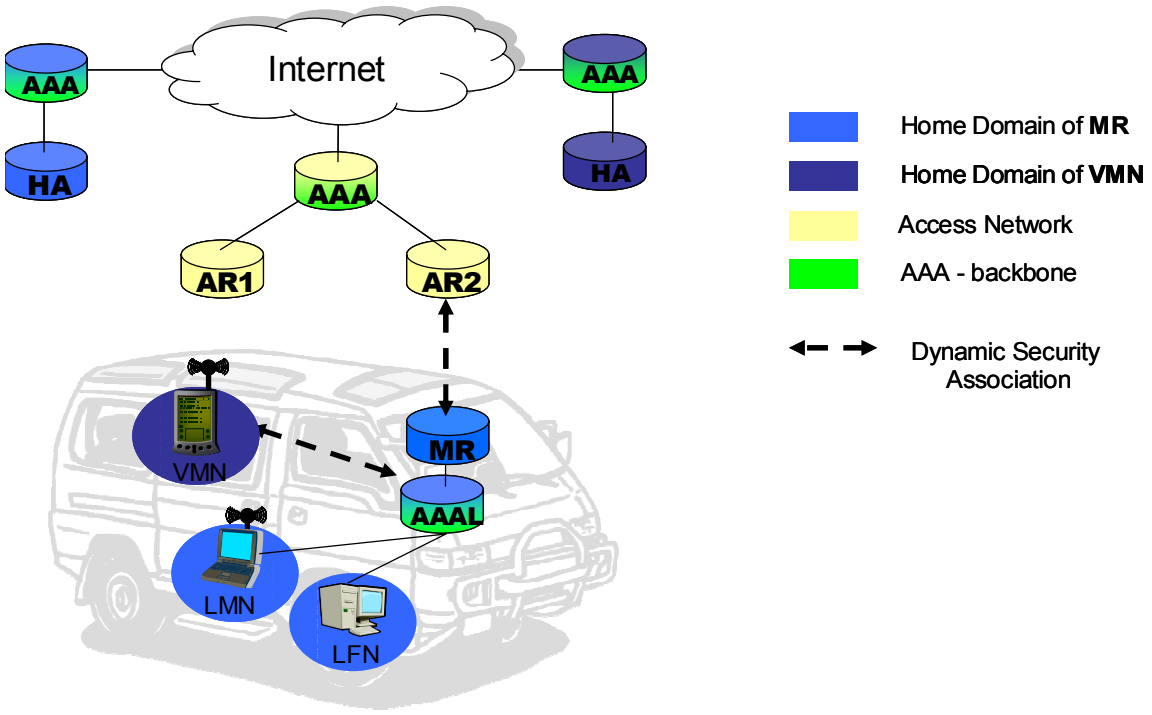


Figure 46: Trust relationships

The OverDRiVE trust model is depicted in Figure 46. The specific trust relationships are described in the following. First, it is straightforward to assume that the client has a security association with the home domain and therefore with the contained AAA server, since that is roughly what it means for the client to belong to the home domain. Figure 46 introduces three home domains and their corresponding nodes:

- Home domain of the MR includes:
  - AAA home server,
  - HA of the MR,
  - local AAA server (AAAL) inside the IVAN,
  - LMNs and LFNs.
- Home domain of the Access Network includes:
  - AAA home server,
  - first hop router of the MR when attached to the Internet (ARs)
- Home domain of a visiting Node:
  - AAA home server,
  - VMNs.
  - HA of VMNs

Nodes that belong to the same domain can share a static trust relationship, i.e. they know each other and belong to an administrative domain. Therefore the initiation of a security association, e.g. needed by IPsec, can be configured in a static or dynamic way.

However, requiring such bilateral security relationships is not scalable if all nodes that might communicate together must have statically configured trust relationships; the AAA framework must provide mechanisms to build dynamic trust relationships. The build-up of a dynamic trust relationship is based on an AAA backbone that is connected via the Internet. Therefore, the setup of a dynamic trust relationship for a VMN is based on the static trust between the AAA home domains involved.

3.4 Network Access Control

The need for Network Access Control can be seen from two sides in OverDRiVE's envisioned vehicular environments: On the one hand a client wants to connect to a trustworthy network and on the other hand a network wants to take up only trustworthy clients. Especially in public transport vehicles, which allow mobile users to attach to the mobile network, means are needed to secure the network by starting with mutual authentication. This paves the way to grant access rights to individual users and enable accounting for services, e.g. information or multimedia services that are accessible in the IVAN. Thus, mobility of hosts and users within the OverDRiVE architecture leads to the crucial question if a node can trust its communication peers.

The concept of network access control for OverDRiVE mobile networks provides one basic step towards secure network access. While security threats for specific network protocols may be prevented by introducing authentication and encryption of messages, the question whether a node is allowed to attach to the network or not, must also be answered. Within OverDRiVE the procedure of negotiate access rights is handled by network access control.

The generic access control question can be expressed in the following way: Is user *U* allowed to perform action *A* on resource *R*? If this question is positively answered, the user must of course be certain that the performed action fulfils the expected needs. In the context of OverDRiVE's IVAN this question can be transformed to a network specific decision:

- Is the IVAN allowed to connect to an AR?
- Is a mobile node allowed to roam into the IVAN?

These questions must be answered before providing services to the user. The general idea of the service provider side, i.e. AR or IVAN, is to identify a node and restrict the use of resources that affect AR's and IVAN's operability. On the other hand, the service user, i.e. the IVAN or a mobile node, can decide whether it wants to accept the service offered by a provider. Examples of more concrete concerns that arise for a network access provider or network service user are listed in Table 1.

Network Access Providers	Network Service Users
provide access to • trustworthy users	use access from • trustworthy providers
secure access to • restricted areas and services • particular operations	secure access to • personal data
suspend access • due to network changes	suspend access • to indicate dormant mode

• due to exploitation of resources • if security violations are indicated	• to indicate security concerns
reject access • when a node leaves the network • when a node is unreachable • if a node violates security policies	drop access • when security is compromised • when access is no longer needed

Table 1: Different views on network access

Here again, the most important issue is to establish a secure communication between the peers that are trying to answer the above-mentioned question. If the IVAN must decide whether an unknown host is allowed to attach to the network, the new host's identity must be obtained and verified. Further on, it is assumed that either the network node can be identified or the combination of the user and the node provides means for unambiguous identification.

The concept of network access control is seen in the context of the Authentication, Authorization, and Accounting (AAA) framework. Therefore, entities that provide basic services for the transport of user and network information, as well as points for the retrieval of information and decision points for authentication and authorization issues exist. Queries contain at least identification information that is compared to a policy repository to accomplish decisions. Furthermore the decision point might not be co-located with the enforcement point, e.g. the question of whether granting access or not, is decided somewhere in the Internet and not in the IVAN.

The task of defining a framework for network access control information is not further regarded within the OverDRiVE project. Here, mainly binary decisions are taken into consideration, e.g. whether a node is allowed to attach to the network at a given point in time. The motivation behind this approach is to take a look at the implied signalling that is introduced by network access control in mobile environments. This opens ways to refine access control concepts with respect to mobile environments, where changing the point of attachment introduces a delay that must be kept as small as possible to hide the complex task of authentication, authorization and accounting. Nevertheless, OverDRiVE's approach does permit extensions for network access control, which specify what a user or node is allowed to do or more exactly: Which resources can be accessed and what operations can be performed on a host or user basis. It is envisioned that network access control and corresponding policies handle multiple categories or types of information, such as financial, personnel or classified information. With the benefit of network access control a foundation is laid out to allow further negotiations about resource usage.

In the following section, network access control is regarded from two points of view: Firstly, network access control between mobile routers (MRs) and Access Routers (ARs) that connect the IVAN to the Internet and, secondly, network access control within the IVAN.

3.4.1 Basic Protocols for Network Access Control

The construction of a dynamic trust relationship via an AAA infrastructure can be performed in conjunction with the Diameter base protocol [55]. However, the Diameter base protocol needs to be extended to be used for authentication and authorization tasks. It is mainly a protocol that provides an AAA backbone. Thus, additional protocols must be included to establish the concept of network access control in OverDRiVE mobile networks. Taking the roaming of a VMN into

the IVAN as an example and assuming that only a simple binary decision is performed by network access control, at least the following tasks must be performed:

1. VMN and the IVAN must mutually authenticate each other on the last hop.
2. The IVAN must decide if the VMN is allowed to attach to the IVAN
3. With the IVAN's permission network access is granted to the VMN and the mobility management can take place.

To further identify which layers and protocols are involved to perform network access control the basic protocols and their co-operation are sketched. As we want to control the access at the network layer, the latter and layers beneath are candidates for the establishment of a secure communication.

For IEEE 802.11 networks the 802.1x authentication protocol can be used to authenticate nodes (respectively ports [60]) at the link-layer. The 802.1x protocol uses the Extensible Authentication Protocol (EAP, [59]) to accomplish authentication. EAP is a generic solution that provides different authentication methods for peers. Although EAP is originated from PPP, it can also be used in LAN environments (EAPOL, [60]). For link layer protocols that do not provide the ability of using EAP for authentication, solutions from the IETF PANA working group [61] may fill this gap, as one of their current goals is to provide a solution to exchange EAP information at network layer. To accomplish the task of mutual authentication via the Diameter based AAA backbone, EAP authentication methods like EAP-TLS [63] and the EAP-Diameter interface [64] are identified as candidates for OverDRiVE.

Further on, the node that acts as authentication peer for a VMN and MR is called AAA client. An AAA client introduces an abstraction from the particular authentication method on the last hop. This client is the first entity that a node contacts to perform the task of network access control, even before an IP address is assigned.

3.4.1.1 Network Access Control by Proxy Chaining

Figure 47 gives an overview of the proxy chaining principle in the context of EAP-TLS and Diameter. Here, the AAA client negotiates the authentication method via EAP and exchanges the certificates to allow mutual authentication. The AAA client is thereby only a pass-through between the AAA server in the foreign domain (AAAF) and the VMN.

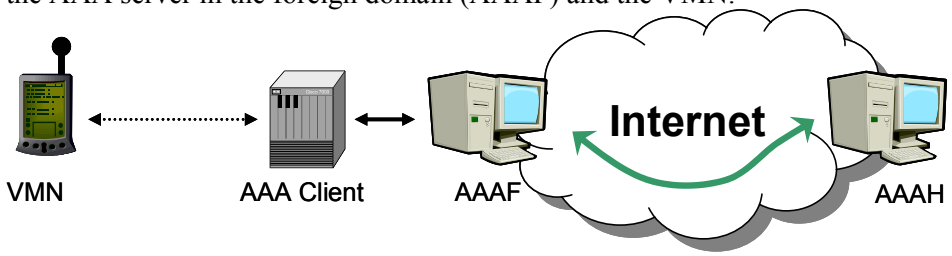


Figure 47: AAA signalling between VMN and AAA home server

The decision whether or not the network access control is conducted successfully involves not only the AAAF server. The latter has to perform additional queries that involve other AAA servers. In Figure 47 the case is presented that the AAA server of the VMN (AAAH) has a direct roaming agreement with the AAAF server. Therefore, the AAA servers can agree on the policy that must be applied for the VMN. It is to mention that the roaming decision can also involve additional servers that reside between AAAF and AAAH.

This particular type of information exchange between the foreign and home domain is called Proxy Chaining and described in [65]. This approach is based on RADIUS [54], which has a security related deficiency as RADIUS provides only hop-by-hop security. Diameter tries to tackle this deficiency by introducing the concept of end-to-end security; therefore the main principle of proxy chaining can be applied again without the mentioned security considerations.

However, the signalling may still involve multiple AAA servers from different domains to accomplish the network access control, i.e. nodes may not attach to the new domain until a decision is made by all participating entities.

3.4.1.2 Network Access Control by Certificate based Roaming

A second approach that is defined in [66] and also bases on RADIUS addresses two issues of the Proxy Chaining idea:

- Security issues of proxy chaining and
- improved scalability.

The main idea of certificate based roaming is to include information that is needed to carry out authorization within a certificate. Therefore the authentication and authorization can be performed at the AAAF server. Authentication can be decided by the AAAF server when a roaming association is known with the VMN that wants to attach to the foreign domain, e.g. VMN and AAAF have the same trusted root authority. If the authorization information is included in the certificate that was needed to authenticate the new peer, the AAAF node is able to derive the policy that must be applied to the VMN.

This approach provides means to speed up the network access control decision. However, all information must be included in a certificate. This approach opens the question how to deal with revoked certificates that are no longer valid due to changes. If revocation lists must also be checked prior to granting access, the implied signalling is similar to the proxy-chaining approach in the last section.

3.4.1.3 Mobility Management support by AAA

The main principle of proxy chaining is the negotiation of a policy for a node that is visiting a foreign domain. This message exchange already needs a full round trip to the home AAA server of the visiting node; therefore it is beneficial to include the mobility management. This saves a additional round trip time after answering the question whether or not a node is allowed to attach to the network. This co-operation between Mobile IP and AAA is already described in [56] and [57]. As a benefit, when the AAA signalling arrives back at the foreign domain, the mobility management is also partially concluded.

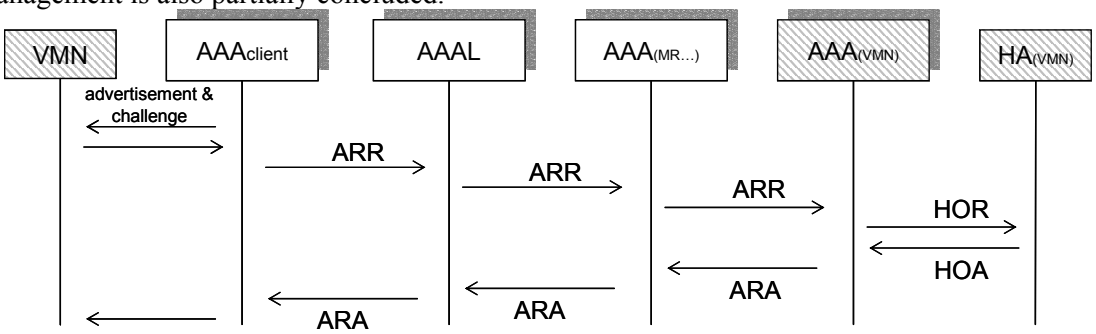


Figure 48: Mobility Management for a VMN

Figure 48 depicts the message exchange that describes a possible co-operation between network access control and mobility management (cf. [57]). Following abbreviations are used:

- ARR - Authentication-authorization-Registration-Request
- ARA - Authentication-authorization-Registration-Answer
- HOR - Home-Agent-MIPv6-Request
- HOA - Home-Agent-MIPv6-Answer

If authentication or authorization decisions must be answered in conjunction with VMN's home domain, the VMN's HA can also be involved. In case of a positive answer the VMN is granted access and the mobility management has almost finished, as the HA of the VMN already updated binding cache information. Figure 49 shows the same signalling principle for the MR.

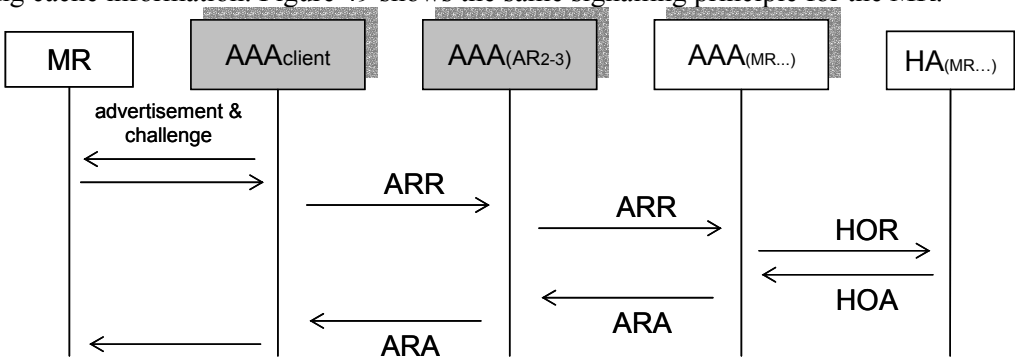


Figure 49: Mobility Management for the MR

3.4.2 Performance Enhancements to AAA signalling

When the proxy chaining approach (see section 3.4.1.1) is used, the minimum delay caused by the network access control signalling via AAA entities is at least one round trip time of the VMN or MR and the corresponding home AAA server. Round trip time does not only include routing delay but also the processing of authentication data and negotiations between multiple AAA servers that participate in the network access control decision. While this impact can be marginal for best effort services (like web surfing) and real-time multimedia applications like VoIP or video conferencing can be severely disrupted. In mobile environments it is therefore desirable to support the continuity of sessions

1. while changing the point of attachment inside an administrative domain (intra-domain handover) and
2. if administrative domains are crossed (inter-domain handover).

Thus the speeding up of network access control is desired. An approach to reduce security implied signalling for intra-IVAN nodes as well as for the Mobile Router is addresses in the following.

3.4.2.1 Mobile Routers

Performance enhancements regarding network access control signalling for the MR are discussed on the basis of handover situations. In this context different types of handovers are regarded in the following subsections. Note that until the network access decision between the MR and AR has been completed, traffic may not be routed via this connection. If the traffic conveyed by the MR cannot be easily mapped to the remaining active interfaces, this will introduce a delay for all nodes in the IVAN. Especially multimedia applications, which are seen as future IP based services, will be affected because of their sensitivity to delay. The next paragraph introduces

ideas how network access control decisions could be accelerated during a mobile network's handover.

Attaching to the same domain

If the MR attaches to a new AR both must mutually authenticate. Suppose the new AR belongs to the same domain as the last AR, i.e. MR and the new AR have already learned credentials from their domains. In this case the authentication procedure should not need a full round trip as the negotiations between the AAA server of the MR and the AAA of both ARs have already been performed. Consequently, network access control is negotiated between the IVAN and the AAA server of ARs' domain and the mobility management should be delegated to Mobile IP or handled transparently to the MR and its home domain.

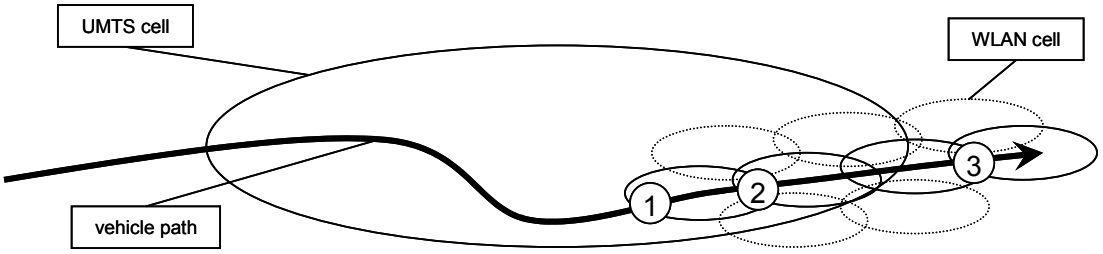


Figure 50: Handover scenario for the MR

Attaching to a new domain

Before performance enhancements for the MR are presented, IVAN handover situations are described in more detail.

The first scenario is a MR connected to the Internet via an UMTS-like link and moves into a WLAN hotspot. This is sketched in Figure 50 at point 1. The WLAN cell is superposed by the already established UMTS-like radio link. Sufficient time might be available to mutually authenticate the MR with the AR of the detected WLAN. The work of network access control can therefore be performed. If network access control is accomplished successfully, the MR can decide how to use the resources in this multi access scenario (see section 2.4.4.2) in an optimal way. As the existent sessions processed by the MR are sharing the bandwidth of the UMTS access system and this connection does not break away, session disruptions can be avoided.

At point 2 in Figure 50 a new situation arises for the MR. The IVAN is connected to the Internet via multiple radio access technologies. The traffic load between the Internet and the IVAN exceeds each of both links, therefore the MR routes data packets via both interfaces. In this multi access scenario the MR has only a limited timeframe to manage a handover. Network access control and mobility management should be processed within the handover's restricted time frame. Thus, network access control signalling and the MRHA tunnel must be established in time, otherwise packets must be sent via the alternative interface, queued or dropped. Hence, established sessions from nodes inside the IVAN are affected.

The last scenario contains multiple WLAN hotspots that are available for Internet access. This is pictured at point 3 in Figure 50. The MR does not have the ability of a "fallback" link that has a superposing coverage area as at points 1 and 2. The time to decide to change the point of attachment is again limited.

Looking at the network access control decision as gathering information from a repository of administrative information, the main idea for enhancements is to prepare and distribute necessary information in advance. This can be seen as caching network access control information at IVAN's AAAL server and AAA servers of probable next domains. For this purpose the IVAN needs to inform neighbouring domains before the handover is made. This can be accomplished via geographical or at least adjacency information gathered from AAA servers in currently visited domains.

Based on the information obtained, the IVAN also has a possibility to decide which handover should be performed, if alternatives are given. Though the MR has not physically detected the next ARs, the information about next points of attachment should be sent to the IVAN's AAA home server. This allows the distribution of necessary information to AAA servers, which will shortly be visited. As a result, network access control that is negotiated between multiple entities of different domains is prepared in advance to allow a more seamless handover.

3.4.2.2 Nodes in a Mobile Network

There are different types of nodes that reside in the IVAN (see section 3.3.3) regarding the need for caching network access control information. LFNs and LMNs administratively belong to the same domain as the IVAN. For these entities the integration of an AAAL server in the IVAN (see Figure 46) is used to bypass the communication with the home AAA server over the air interfaces of the MR.

When a VMN attaches to the IVAN for the first time, network access information must be gathered before network access can be granted. This involves the home domain of the visitor and the home domain of the IVAN. Once the VMN is inside the mobile network and all network access control related information can be cached at the local AAA server; the VMN's movement can be handled in the same way as for LMNs with the support of the AAAL node.

Hence, placing a local AAA server (AAAL) inside the IVAN introduces an entity that allows caching of network access control information from AAA entities of the same or foreign domains.

3.4.3 Caching Network Access Control Information

The approach of proxy chaining (see section 3.4.1.1) to perform network access control involves all AAA entities that are on the path between the attaching node and the home AAA server. When this approach is integrated into a mobile environment performance issues arise as stated in section 3.4.2. This is also visualised in Figure 51. Here, the node has to initiate the network access control task by contacting an AAA client in the foreign network (arrow 1). In order to check the credentials and gather network access control information for that node the AAA server of the foreign domain (AAAF) has to contact the AAA server of the node's home domain (AAAH) and ask for the policy that can be applied for the visiting node (arrows 2, 3). Consequently the AAA client passes back the result (arrow 4).

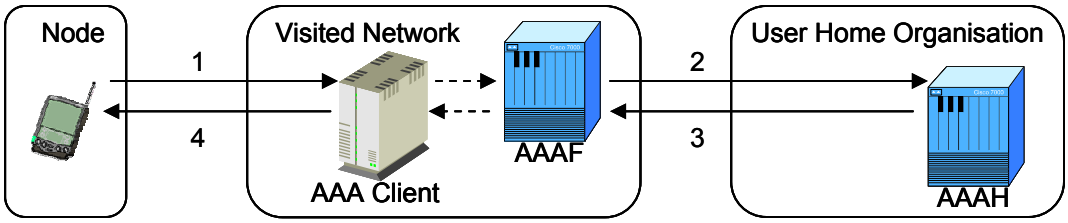


Figure 51: Normal AAA signalling

A promising alternative that avoids the tedious signalling to the home agent is certificate based roaming (see section 3.4.1.2). All information the foreign AAA server needs to know is included in a certificate that the attaching node offers to the server. But it is not clear whether all pre-conditions can be fulfilled if this approach is used for network access control. The following questions arise:

- Can all information be included in a certificate?
- Can a node easily update its certificate due to administrative changes?
- Is the certificate kept safe as every attachment to a new domain does not involve a query to the home domain?

With respect to Figure 51 the information whether the node can attach to the visited network is only carried out between the node itself and the visited network.

Within OverDRiVE an alternative approach is used to perform network access control. The approach is based on the observations made in section 3.4.2. If the information needed for network access control is distributed to the AAA server of the foreign domain, the decision can be performed without the need for a full round trip time to the home AAA server. However, the data that is forwarded to the foreign AAA server contains only temporary valid data that become invalid after a defined period of time. Thus, the main idea is to temporarily cache network access control data at a foreign AAA server. Figure 52 shows the basic idea of the enhanced OverDRiVE AAA signalling. Here, the policy is still retrieved from the home domain. To allow the foreign domain to act as policy decision point on behalf of the home domain, a policy of the node in question is cached at the foreign AAA server. In this way the AAAF has the power to derive the needed information for network access control on its own.

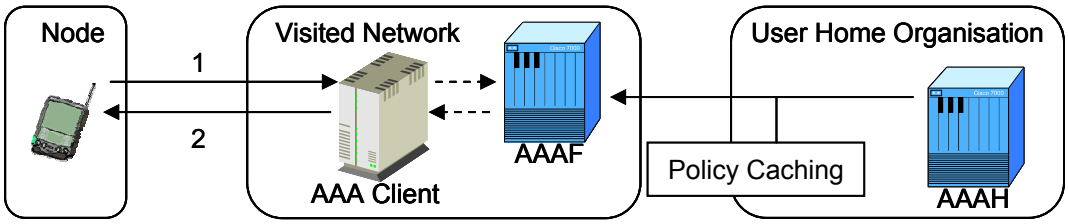


Figure 52: Enhanced AAA signalling

If no policy is available for the node, signalling similar to Figure 51 is needed. But, if all necessary information is already available, an abridged signalling (Figure 52, arrows 1, 2) can be performed.

3.4.3.1 Requirements

In order to allow a description of the message exchange, the following requirements have to be fulfilled:

- If an AAA server is able to perform caching of network access control information, it should distribute information about this capability to neighbouring AAA servers (see below) and mobile nodes in the network.
- If an AAA server is able to cache network access control data and acts as foreign AAA server to mobile nodes, at least the AAA home server of the attaching node must agree on distributing the correspondent data.
- If an AAA server is able to cache network access control and a node is aware of these capabilities, the node should be integrated in the agreement process about forwarding network access control information.
- If the validity period of cached information about network access control ends, this information must be discarded.
- If the validity period of cached information about network access control can be revised, the issuing AAA server and the AAA server destined for reception must agree on methods to assure data consistency, e.g. the issuing server can refresh or outdate information.
- If the foreign AAA server is able to perform network access control without involving the AAA servers of other domains (including the node's home domain of the attaching node), mobility management information may not be forwarded to the home domain (see section 3.4.3.2).

The benefit of caching network access control information at foreign domains relies on two basic ideas. Firstly, when a node attaches frequently to the same foreign domain, the information can be kept in the cache and updated, if necessary. Secondly, network access control information is distributed in advance, thus the time to handover to a new point of attachment is decreased.

As information about the mobility profile of a node and therefore of its user may be protected, the node and the node's home domain should be able to restrict the caching of information.

3.4.3.2 Co-operated Mobility Management

The co-operation between mobility management and AAA (section 3.4.1.3) requires the forwarding of binding update information to the home domain of the visiting node. As this task can also be managed by a mobile node that wants to attach to a foreign network, the mobility management may be

- handled by the foreign domain, i.e. mobility is handled transparently for the mobile node and its home domain,
- handled by the mobile node without AAA signalling or
- handled by AAA signalling.

While the first alternative is transparent to the mobility management of the mobile node and its home domain, an interface is needed between AAA entities and micro mobility management within the foreign domain. The second and third alternative is already specified by MIPv6 and [57]. If the mobility management is started by AAA signalling and the network access control decision can be performed at the foreign domain due to cached information, the foreign domain

may decide whether the mobility management is performed by forwarding AAA information to the home domain or left to the mobile node.
Furthermore, information about adjacent networks is forwarded to the mobile node before it can physically detect them. An additional decision process can be conducted by the mobile node, e.g. trustworthy and suitable networks that are advertised by the current network's AAA server can be propagated.

3.4.3.3 Message Exchange for Network Access Control

The concept of Network Access Control for OverDRiVE introduces new messages that must be exchanged between the entities. In the following, an overview of the needed messages types is given.

Caching Advertisement and Solicitation

The introduction of caching for network access control needs messages to advertise and solicit this capability. These messages need to be exchanged between AAA servers that want to exchange profile information to allow caching. Additionally, a mobile node can participate in the decision whether caching is allowed or not. But, a mobile node is not allowed to send caching advertisements, as it must not distribute network access control information about itself.

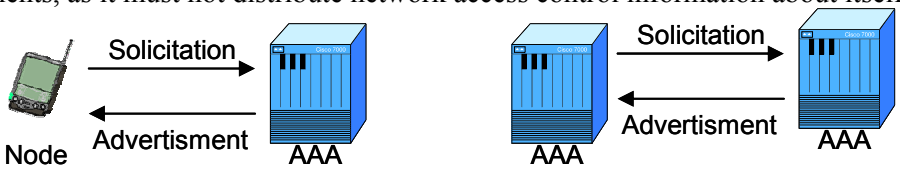


Figure 53: Advertisement and Solicitation

Figure 53 gives a conceptual overview of the caching advertisement and solicitation messages.

Capability Negotiation and Information Transfer

Before the actual information transfer is processed, two AAA entities must negotiate about a common format and interpretation of the transferred information. This includes for example a common information format that is used for the derivation of a network access control policy. In Figure 54 the conceptual message exchange is depicted.

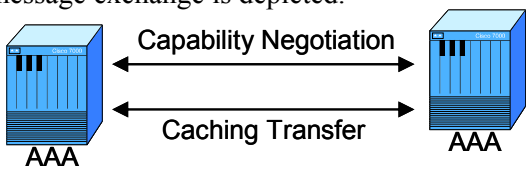


Figure 54: Negotiation and Transfer

Adjacency Advertisement, Solicitation and Notification

In order to allow the exchange of network access control information before a mobile node attaches to a new domain, i.e. abridged signalling as described in section 3.4.2 can take place, Adjacency messages should be exchanged between the network currently visited, the mobile node and the home domain.

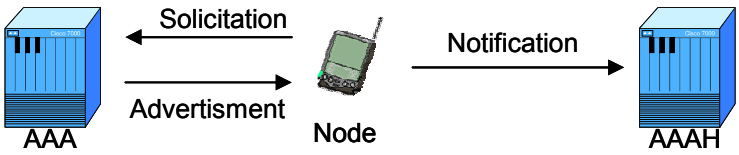


Figure 55: Proximity Messages

An AAA server inside the visited network should advertise information about nearby networks that provide wireless access to the Internet. This information can be statically or dynamically configured. When a node receives this information it can decide if this information should be sent to the home AAA server or discarded. If the AAAH receives a notification from a node it should also start a decision procedure about caching network access control information. If caching takes place, it should proceed via the former described message exchange.

3.5 Concept for Traffic Management

3.5.1 Introduction

In an IVAN all wired and wireless nodes are able to share the multi-radio network resources accessed via the MR. All traffic from within the IVAN to the Internet and vice versa has to traverse the MR-AR wireless links. These radio links are believed to be the bottleneck for connections from within the IVAN to the Internet and vice versa. Efforts have to be made not to overload these links. To achieve this, both traffic shaping and policing are an appropriate choice.

In the following the requirements identified in D03, which can be satisfied by traffic management are taken up. Building on these requirements a concept of traffic management is being introduced.

3.5.2 Requirements

D03 states requirements, which have to be coped by the OverDRiVE mobility concept. Requirements that can be addressed by traffic management are:

- Scenario 3a (Network/Traffic management/QoS) – It is feasible to allow for network management actions at the intermediate IVAN in case of nested mobility because the external connection probably is a scarce resource.
- General – The solution should not impose any OverDRiVE specific requirements to any network entity outside the IVAN and outside the OverDRiVE backbone domain. Especially the solution must not require changes in the access systems.

One of the most important scenarios for understanding the need for traffic management and service classification is the roaming of one IVAN into another IVAN. The nested IVAN itself could consist of many nodes, which produce a large amount of traffic. Nodes from within the outer IVAN have to be protected against this possibly large amount of traffic. In case of a mobile car it has to be guaranteed that important car related services like telematics services, off-board navigation, maintenance or software update have higher priority in relation to common user data.

When designing a traffic management concept for mobile networks the characteristics of a wireless link and of vertical handovers have to be taken into account. Unlike in a fixed-link scenario a wireless link can change its bandwidth and delay characteristics over time and space. This means a non-guaranteed bandwidth for the different access systems. As a consequence no absolute bandwidth guarantees can be given. Only relative assertions can be made. A vertical

handover, i.e. a handover between different access systems, generally results in an abrupt change of link characteristics. Traffic flows have to be rescaled to the new link bandwidth.

However, it is not in the scope of the OverDRiVE project to use a QoS framework like IntServ [69] or DiffServ [70]. Not only that these frameworks have not found broad acceptance in the Internet community so far, it is also not trivial to adapt these frameworks to the mobile context [85]. This would be a premise for the use in the IVAN. In addition the required infrastructure for IntServ and DiffServ is contrary to the general requirements formulated in D03. D03 demands that no OverDRiVE specific requirements should be imposed to a network entity outside the IVAN and OverDRiVE backbone domain. Both IntServ and DiffServ require specific support of the routers.

A local mechanism is preferred which allows local control of bandwidth distribution in response to local needs and makes no assumptions on entities in the Internet besides in the IVAN and the OverDRiVE backbone domain.

3.5.3 Traffic management approaches

In the OverDRiVE approach each MR maintains a bidirectional tunnel to its HA for every access system it uses to connect to the Internet. All outgoing and incoming traffic, apart from traffic using route optimization mechanisms for unicast or multicast, is forwarded via the MR-HA tunnels. If route optimization for mobility-enhanced hosts is used, traffic from within the IVAN is directly routed to the CNs and vice versa. This is achieved by the use of care-of addresses and binding caches in the CNs. This traffic will not traverse any MR-HA tunnel. Multicast traffic can either be forwarded to the IVAN by the HA or in case of remote subscription is directly routed to the IVAN without traversing the home domain of the IVAN.

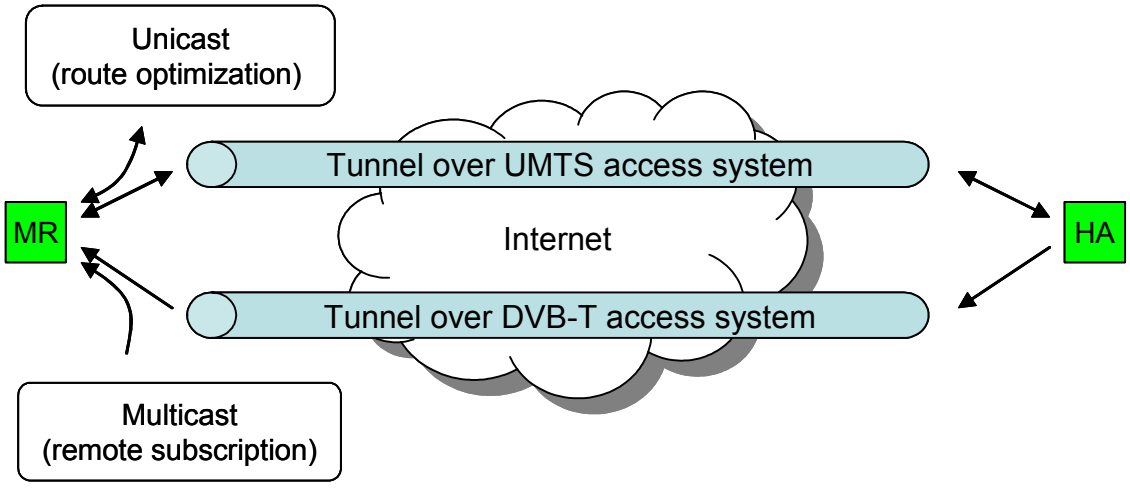


Figure 56: Traffic management approaches

Traffic management in the OverDRiVE mobile networks can be applied at different entities and levels. Outgoing traffic from the IVAN could be shaped at the MR. It has knowledge of the link capacity (at least the MR can monitor the link capacity and give an estimate if no hard QoS agreement by the wireless service provider is given). In case of incoming traffic, a traffic shaping mechanism at the AR could prevent overloading the link to the MR. Unfortunately, this would violate the D03 requirements as stated in section 3.5.2, because no changes to the outside world

are allowed. Instead of shaping at the AR the HA of the MR could do the job because a great fraction of the traffic to the IVAN will traverse the MR-HA tunnel.

In case of incoming TCP traffic discarding some of those packets could cause the TCP congestion control mechanism to reduce the amount of data sent. In case of multicast traffic the remote subscription of IVAN nodes to multicast groups could be regulated via the AAA authorization mechanism.

To realize a fully-fledged traffic management at the mobile router application layer information must be used to build up policies and a management database. This application specific information would require a special API and incorporate information regarding bandwidth, delay and priority. It would also be feasible to give the MR a vector of for instance bandwidth values at which the application would like to be informed when changes occur. That information could be used to support fast application adaptation e.g. scalable video codecs, etc. A possible solution and practical implementation experience can be found in [75].

Since this application interaction is out of scope of the OverDRiVE project and it is somehow contrary to the tunnelling approach, OverDRiVE concentrates on mechanisms that do not require any reservation specific interaction between the application and the IVAN

3.5.4 Traffic Shaping

A simple approach of traffic shaping for the IVAN is depicted in Figure 57:

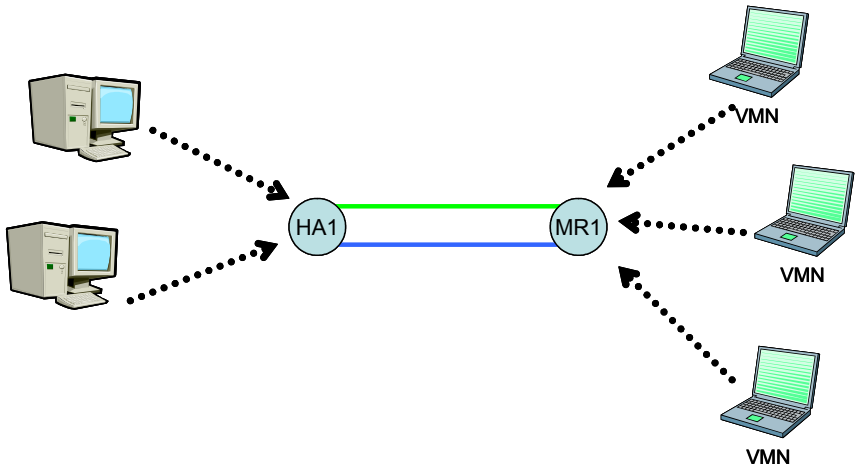


Figure 57: Simple traffic shaping approach

Several streams are merged at the MR and HA. However, the capacity of the wireless links may not be sufficient to transport all the traffic. Two basic tasks have to be performed in order to achieve traffic shaping at the MR and the HA:

- characteristics of the wireless links have to be transmitted to the HAs
- a scheduling strategy has to be chosen

The first task can be performed by sending well-defined messages from the MR to the HA. The information to be exchanged via these messages is summarized in subsection 3.5.4.2.

Additionally scheduling at the HA and the MR is needed to distribute the available bandwidth between the nodes on each side.

An approach for implementing a fair queuing strategy has been published in [74] where an efficient way of realising fair queuing by Deficit Round Robin (DRR) has been proposed. The DRR approach is a simple modification of the traditional round-robin service to avoid the scheduling unfairness with different packet lengths without having high effort for inserting packets into sorted queues. The queues of active flows are served in traditional round-robin manner, but instead of serving one packet per flow for each round a certain quantum of bytes is assigned to each queue. If a packet could not be sent due to a longer packet length, the quantum is added to a deficit counter and the packet is served in one of the next rounds when the deficit counter is larger than the packet length.

The DRR proposal is designed for implementation in a router, where the router software including DRR is exclusively using the router CPU. For an implementation in a software protocol, as it might be the case for the mobile router or its home agent in the OverDRiVE/IVAN scenario, working within the operating system on a host (and thus sharing the CPU with application processes), some modifications have to be done to avoid a "busy waiting" service with DRR when only a small quantum of few bytes is added in each round without serving a packet at all. Thus, after one complete round without sending a packet, the service is interrupted until a certain timeout (e.g. 10 ms) to increment the counters and restart the service. The use of one global timer has the advantage of avoiding individual rate timers for each queue, which require high precision for high sending rates. Also other variations of scheduling strategies may apply (as variations of fair queuing from [68], [71], or rate/burst control as from [72]). However, the DRR approach seems to be the most promising regarding simplicity and efficiency [73].

3.5.4.1 Nested Scenario

A more complex scenario arises when nested mobility is considered. An example is shown in Figure 58:

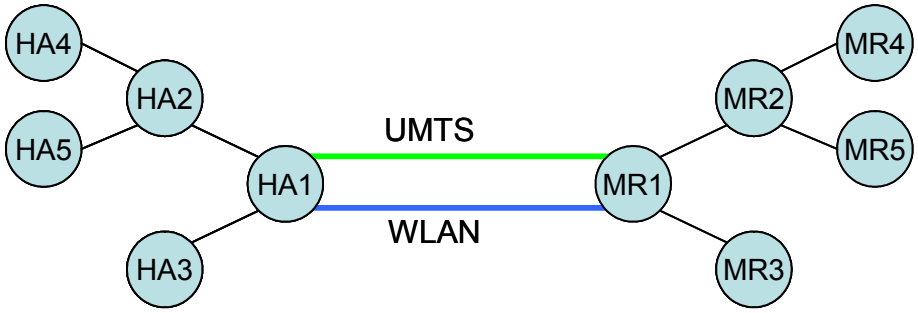


Figure 58: Traffic shaping with nested mobility

First consider the case that MR1 is connected to the Internet only via a UMTS-like link. If MR2 roams into the IVAN and connects via WLAN to MR1 the formerly described approach will fail. This is because MR2 would tell HA2 that the wireless link it uses to connect to the Internet is a WLAN connection. Because of the higher bandwidth of the WLAN connection much traffic will be discarded at HA1. This especially includes the packets of the HA2-MR2 tunnel. HA1 could not look into the HA2-MR2 tunnel and make reasonable decisions, on which packets to discard, which would privilege non tunnelled data packets entering HA1.

A solution to this problem is the propagation of the capacity of the smallest link to the nested mobile routers, which have to propagate this information to their home agents. This also applies

for mobile routers that occur deeper in the nesting hierarchy, for example for the HA4-MR4 tunnel.

However, the aggregation of different tunnels and additional traffic over a single link can lead to an overload situation at a HA/MR which can force the HA/MR to discard packets. The alternative would be to reserve bandwidth for all routers of the nesting hierarchy at all levels of the hierarchy. This would require a pursuance of traffic flows of multiple nesting hierarchies, which is hard to achieve because of the tunnelling, combined with a possible encryption.
A Class Based Queuing (CBQ) approach [67], where traffic can be hierarchically distributed and surplus bandwidth can be shared between sub-trees of the hierarchy is not feasible because an approach like this would require a packet classifier with full insight in all tunnel levels.
In a multi-access scenario the bottleneck link has to be propagated for each access system, which is again calculated via the minimum of all hierarchies for each link. For the sake of simplicity we assume that nesting mobile routers only use a single uplink towards their upper mobile router because of

- available intra IVAN Technologies (only WLAN and Bluetooth seem to be appropriate).
- exponential increase of network paths by combining different links.

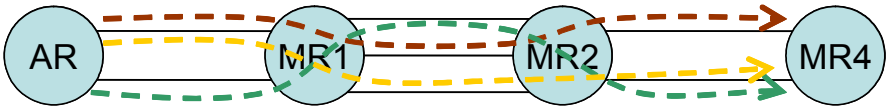


Figure 59: Example of multiple network paths combining different links

For details on multiple-access see chapter 2.4.4, which describes the adaptation of the DRiVE flow routing approach to mobile networks. In case of a vertical handover the same massages can be used as already described. An update of the information at the mobile routers and the home agents is required.

3.5.4.2 Message exchange for traffic shaping

As already indicated in the previous section, a signalling mechanism is needed in order to exchange link characteristics

- between mobile routers
- between a mobile router and its home agent

Mobile routers have to exchange both information on the up- and the downlink channel characteristics. Downlink channel characteristics need to be exchanged in order to be able to inform the pertaining home agents, which with this information are able to adapt the traffic to the IVAN to the local link characteristics as depicted in Figure 60.

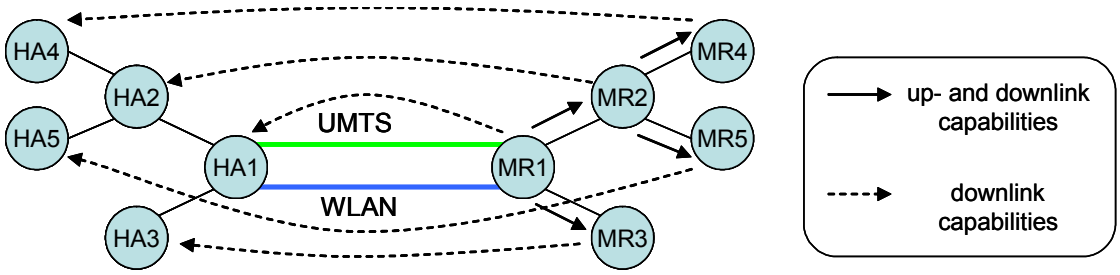


Figure 60: Message exchange with nested mobility

In case of a shared medium for uplink and downlink (e.g. Wireless LAN IEEE 802.11b), this additional information has to be propagated to the mobile routers and their home agents. Because there are no separate up- and downlink channels, means must be taken in order to balance up- and downlink traffic. It also depends on the situation if such a link is a bottleneck or not. However it is assumed that traffic will be asymmetric, i.e. there will be more downlink than uplink traffic.

4 Integrated Concept of Mobile Router and Dynamic IVAN Management

This section provides a summarized and integrated view of the 2 main topics covered in this deliverable: mobility management and dynamic IVAN management. Using different mobility scenarios the principles of interaction between both concepts is explained. A refined concept and a detailed description of the interaction is subject of deliverable D17 due to April 2004.

We presented an exhaustive analysis of mobile networks high-level behaviour using the MRHA bidirectional tunnel. Several particular configurations were described, with unique or several mobile hosts, mobile routers and nested mobility. In this section we will evidence the match of those configurations to the OverDRiVE scenarios.

4.1 Scenarios

The OverDRiVE scenarios are basically the following:

1. A vehicle is moving using its MR-HA connectivity to allow for seamless communication for all connected LFN, which reside in the IVAN. While changing the access system certain tasks for both mobility management (update the MR-HA tunnel) and network access control (AAA) must be performed.
2. The vehicle stops and a VMN enters the IVAN. To allow seamless communication the VMN must perform steps to connect with the IVAN and its AAA infrastructure and secondly updates its mobility bindings at it home agent.
3. Once the VMN is inside the vehicle it moves inside the complex IVAN and changes access routers. To perform host mobility in an efficient way, a micro-mobility approach is used, which interact with the macro-mobility and perform certain AAA tasks.

From a mobile networks standpoint, firstly, note that the first scenario involves a mobile network that includes one mobile router MR, one local fixed node LFN and one HA. This fits exactly the high-level configuration described in Figure 17 of section 2.4.2.1. Second, note that scenario 2 corresponds exactly to the configuration in Figure 18 where both the VMN and the MR belong to the same Home Agent. The third scenario corresponds to Figure 41.

4.2 Overall Entities

Figure 61 shows the location of all involved entities in location management and AAA functions. For scenario 3 a train with several access routers inside the IVAN is assumed. The following chapters describe the principles of inter-working of mobility management and AAA entities.

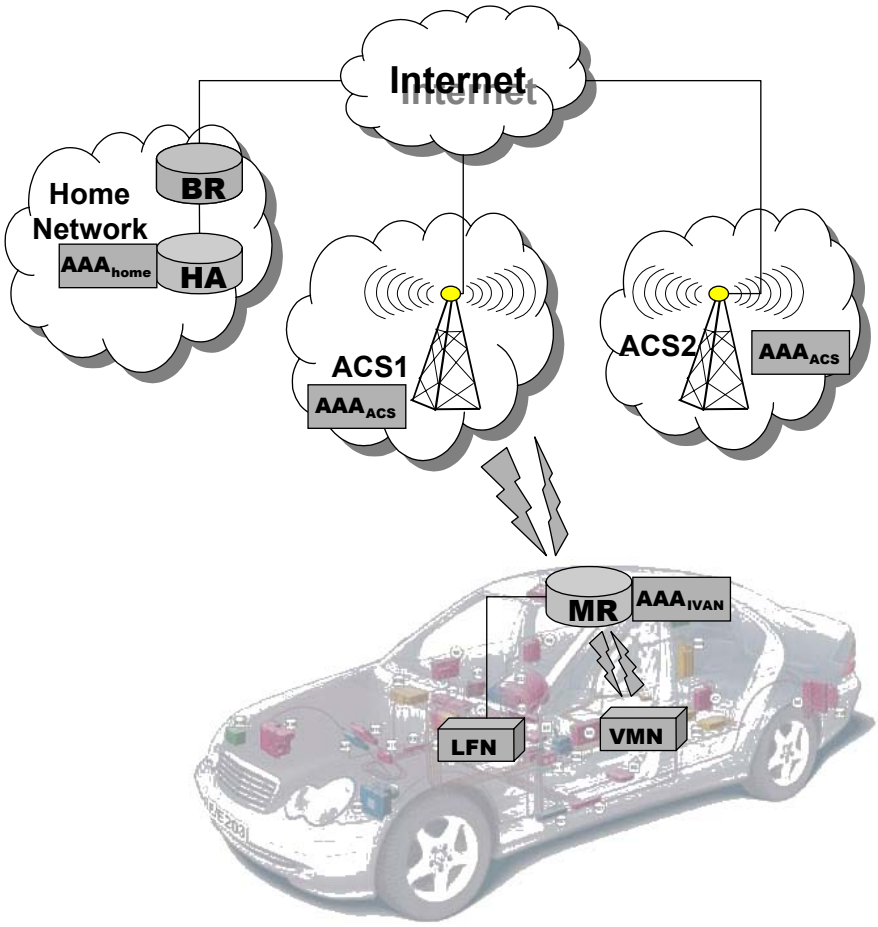


Figure 61: Overall entities

4.3 Vehicle mobility

As shown in Figure 61 the scenario is motivated by a passenger car that contains one LFN within its IVAN. Handover is performed from ACS1 to ACS2. As the access systems belong to different domains an inter-domain handover must be performed.

In this scenario the car is attached to the Internet via ACS1. The MR has already performed network access control tasks and established the MR-HA tunnel. The packet exchange between the LFN and a CN within the Internet has been handled as described in section 2.4.1 (see Figure 11). As OverDRiVE's bi-directional tunnel approach is transparent for nodes within the IVAN the LFN, which is not capable of performing mobility management tasks, can exchanges packets with a CN that resides in the fixed Internet using vanilla IPv6. The tunnel between the MR and its HA is represented by a bold dark line in Figure 62 on the left hand side.

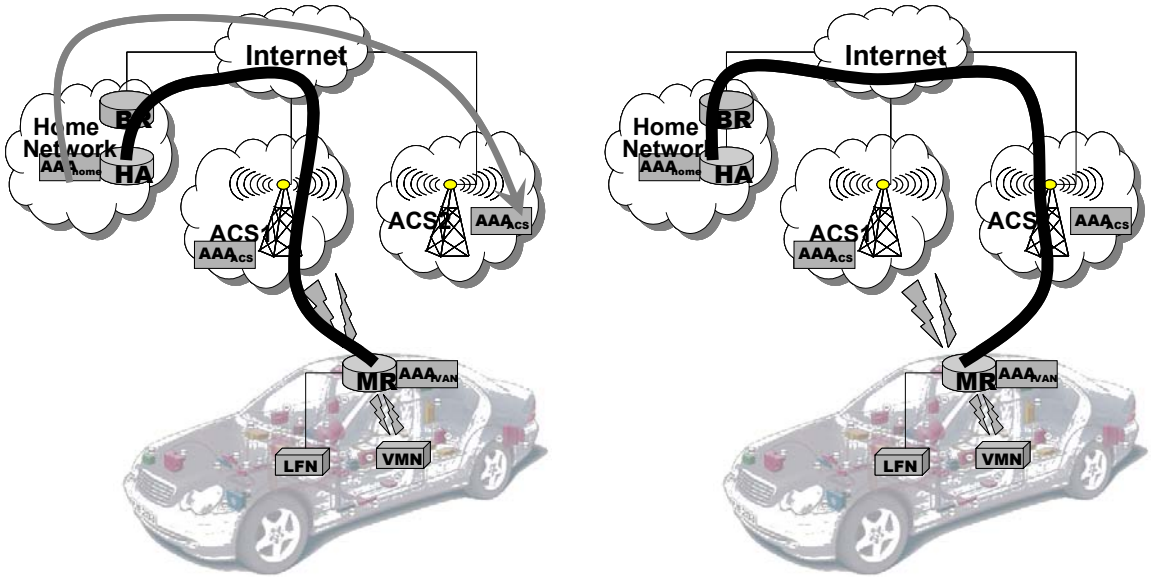


Figure 62: Tunnel set-up and information caching

While the MR is connected via ACS1, the AAA server in the domain of ACS1 informs the MR about adjacent domains. This information transfer is based on the message exchange presented in section 3.4.3, i.e. AAA entities have information about adjacent domains and advertise it to attached nodes. The MR decides to transfer the information about the adjacent domain to its AAA home server, as the MR and his home AAA server supports the concept of caching network access control information. Consequently, the home AAA server contacts the AAA server of ACS2 and sends network access information about the IVAN. This message flow is sketched on the left side in Figure 62 by the light grey arrow between the AAA home server and the AAA server of ACS2.

As soon as the car detects the availability of ACS2, network access control takes place by exchanging credentials at link layer between the ACS2 and the MR. Since the AAA server of ACS2 has cached network access control information for this IVAN, the decision to grant access is performed without involving other AAA servers. Therefore, the MR can be assigned a CoA and the mobility management can take place.

The result of the mobility management performed by the MR is depicted on the right side in Figure 62: The MR-HA tunnel is now established via ACS2. An example of the detailed signalling is shown in section 2.4.1 (see Figure 10).

The inter-domain handover has been performed. Consequently, the packet exchange continues without introducing particular tasks for LFN and CN.

4.4 A VMN roams into an IVAN

While a wireless interface of the MR is in the coverage area of the access system ACS2, the driver stops to take up a friend that is waiting at a bus stop. The driver's friend is using Internet services via an available hotspot. When she enters the car, her handheld gives information about the car's wireless technology that is available. As she wants to stay connected, she decides to roam into the IVAN.

4.4.1 Network Access Control

The driver does not allow everybody to use his car's network including access to the Internet, because he must pay for it. In this case, he explicitly granted access for his friends, including the one he has just picked up. Thus, network access control allows the roaming of the handheld into the IVAN. As the credentials of the entering handheld are transmitted to the local AAA entity in the car, no caching information could be found. Therefore, the home AAA server of the car's network must be contact to grant the access.

4.4.2 Mobility Management

The high-level vehicle mobility involves in addition to the mobility of the mobile network, mobility of a visiting mobile node into the mobile network (the user getting into the car). This corresponds to the figure below that is the same as described in section "Mobile Networks and Mobile Hosts". Remark that the access routers AR1 and AR2 are placed within the access systems ACS1 and ACS2 respectively. Remark also that the VMN and MR have a same unique Home Agent. The exact message exchange for mobility management is described in section "Mobile Networks and Mobile Hosts".

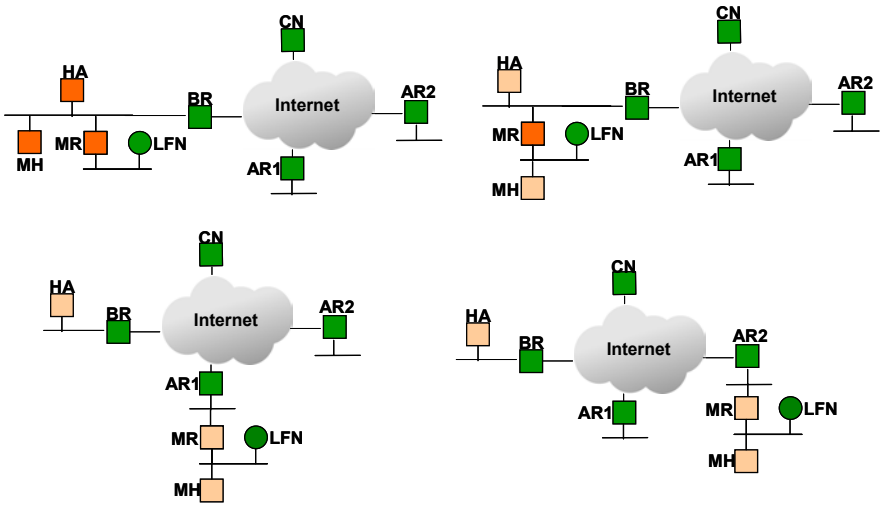


Figure 63: Mobile Networks and Mobile Hosts

Remark that in this case, the MH has the role of a VMN and that the visitor only connects inside the mobile network. For the cases where the visitor needs to connect inside the mobile network, as well as outside of the mobile network, see variations described in section "Mobile Networks and Mobile Hosts".

A Digression

A fully integrated access controlled mobility management for IVAN is relatively difficult to build without a full experience support from an eventual implementation. However, a top-down conceptual approach can help achieve a relatively high level of understanding. In this section we try to exercise this approach. Consider the following simple sequence of steps:

- a fixed host in the mobile network communicates with the content provider;
- the mobile network moves and attaches to a new ACS;
- the mobile network is authorized to the new ACS and subsequently the communication continues seamlessly between the host in the car and the content provider.

From this sequence it is clear that, in addition to the useful communication between LFH and CN, an important set of signalling messages will be used for two goals: (1) maintain mobility bindings at the Home Agent and (2) perform access control.

As exposed in the previous sections, there is potentially a wide set of ways to intertwine these two sets of messaging. Let us present here a rough outline of a possible sequence:

- MR receives a signal indicating presence of a new ACS;
- MR asks for permission from new ACS, the new ACS contacts home of MR and obtains permission for MR, subsequently MR is granted permission;
- MR initiates signalling to update mobility bindings at the HA;
- if both previous operations are successful, the communication between the content provider and the host in the car continues where it left.

Analyzing this rough sequence, it is clear that several improvements can be made. The first striking observation is that communication between ACS and home domain happens twice: one for access control and another for mobility management. A same set of messages could be used to perform both operations in a single message exchange between ACS and the home domain.

Another observation is deduced from the analysis of an eventual "no" answer from the home domain (as in a case where the home domain might not be reachable). In that case, it might be preferable for ACS to still grant a limited form of access to the IVAN, albeit the reachability at a permanent home address concept for the mobile network is clearly compromised.

A third observation relates to cases where visiting mobile nodes are connecting to the car. This scenario will involve an additional access control leg between the mobile network and the visiting mobile node. In this case, one aspect that induces clear inefficiencies is that the access control messaging between the VMN and its home domain, will be forced through the MR's home domain, even if the entities involved in making the decision are not at all related to the MR's home domain (those entities are presumably the ACS and the VMN's home domain).

A final observation is about potential optimizations when successively connecting between ACSs. It is clearly possible to for the access control message exchanges not to go all the way back to the home domain, when two ACSs are relatively close. In that case, access control information from the home domain can be shared, or "cached" by a set of ACSs that relatively close.

4.4.3 Traffic Management

At the beginning the new VMN can use all of the available bandwidth. But after a view minutes the HA of the IVAN receives a data stream for the car maintenance – the new telematics software update is distributed. Therefore the queuing mechanism at the HA prioritises the software update and drops packets destined to the VMN.

4.5 VMN mobility inside an IVAN – large vehicle scenario

The scenario in Figure 61 focuses on a large IVAN, such as a train. The vehicle is in connection with various type of access systems via the MR. The MR maintains a bi-directional tunnel between itself and its HA. Every communication between the train and the backbone is handled by means of this MRHA tunnel. This means that the handover of the MR between ACS1 and ACS2 is handled by the MRHA approach. In our scenario the mobility management inside the IVAN is handled by the BCMP (BRAIN Candidate Mobility Protocol) approach (see section 2.3.1 and 2.4.7.3). Some issues of the BCMP-MRHA combined solution were published in [86].

BCMP introduces new network elements into IVAN: the Anchor Point (ANP) and the Access Routers (AR). The functions of the network entities in IVAN are the following:

- The MR of the train behaves as a gateway router of the train and its task is to maintain the MRHA tunnel to ensure continuous Internet connection for the IVAN. The MR has no BCMP capabilities. The MR encapsulates packets coming from the IVAN and forwards them towards the HA via the MRHA tunnel. Packets arriving to the IVAN are decapsulated by the MR and forwarded to the ANP.
- The ANP's task is to maintain the pool of distributable addresses inside the IVAN and participate in the login procedures of Visiting Mobile Nodes (VMN). The ANP maintains a table of the addresses of VMNs associated with the proper ARs as next hops. Since being directly connected with the MR, the ANP receives all incoming traffic and tunnels the packets towards the VMNs via the ARs. The ANP is responsible to track the location of the VMNs inside the mobile network
- The ARs serve as wireless access points for VMNs so they can connect to the BCMP network. There could be several ARs in a large vehicle.

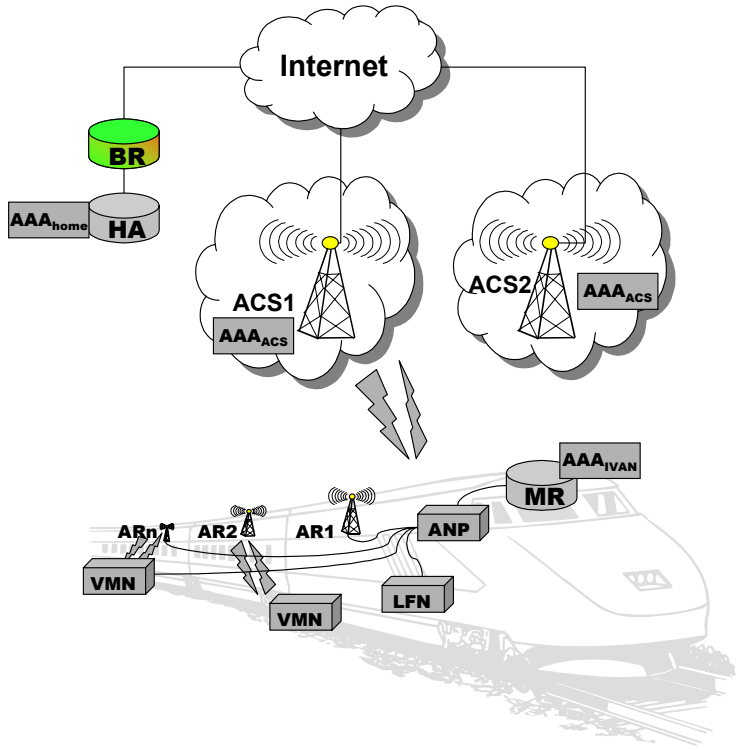


Figure 64: BCMP based architecture in IVAN

If a MN moves from a carriage of an AR to another one the MN performs a handoff between ARs. According to the BCMP concept this handoff can be performed either a prepared or an unprepared way. Regardless of the way of handoff chosen the actions during logging out from an AP and logging in to another one are seamless for entities above the level of the ANP.

Similarly to the handoff procedure, every actions related to the BCMP concept involve entities only below the ANP's level. Thus, interworking with the MRHA macro-mobility

concept is ensured since the maintenance of the MRHA tunnel and the sending of Binding Update messages upon entering the IVAN are signalling procedures that are independent of the BCMP architecture of the IVAN.

The login of a mobile user into the IVAN could be performed as described in section 4.4 or according the MIND User Registration Protocol (MURP) as described in [27].

5 Conclusion

Due to further wide spread deployment of IP based communication in the private and professional environment, devices and gadgets speaking IP become more and more common. The trend towards ubiquitous computing and seamless networking everywhere and every time requires sophisticated mobility management solutions to enable seamless and optimized communication in a heterogeneous communication infrastructure (2G/3G cellular systems, WLAN, Bluetooth, digital broadcast systems). On the other hand a successful introduction of such new services requires an efficient and inherent AAA functionality to protect the mobile networks and entities, to authenticate users and to allow for charging of services.

This deliverable describes a concept for IP based mobility management and AAA framework and functions for moving IP networks. The work is based on the requirements and scenarios that were defined in deliverable D03 [1]. Based on Mobile IPv6, OverDRiVE's bidirectional tunnel approach between the MR and its HA provides all functions to deliver seamless IP connectivity for moving networks over different access systems. It supports both simple IPv6 devices located fixed in the moving network and sophisticated Mobile IPv6 devices, which roam in and out of mobile networks. For mobility inside IVANs the interaction with micro-mobility approaches is explained. In the deliverable a whole set different configuration options is discussed and the implications for mobility management are studied. The work influenced and was influenced by the current standardization activities within the IETF NEMO group.

The described AAA framework interacts tightly with the IP mobility management protocol to provide the foundations for secure communication. The main focus of the work was laid on detailed concepts for access control and traffic management in IVANs. Optimizations for AAA signalling applied to the moving network environment ensure faster AAA operation. Traffic management functions allow to prioritise traffic and to avoid overstressing the (often) low bandwidth of wireless links by shaping traffic at MRs and their HAs.

By means of examples for certain mobility scenarios the interaction of functionality is explained and shown. Refined concepts and a detailed description of the message exchange are subject to the deliverable D17 that is due to project month 24 and will be available at the beginning of March 2004.

References

[1] OverDRiVE Deliverable 03: OverDRiVE Scenarios, Services, and Requirements; http://www.ist-OverDRiVE.org

[2] Mobility Support in IPv6; http://www.ietf.org/html.charters/mobileip-charter.html; IETF draft

[3] H. Soliman, C. Castelluccia, K. El-Maki, L. Bellier: Hierarchical MIPv6 mobility management (HMIPv6). Internet draft, work in progress, draft-ietf-mobileip-hmipv6-06.txt

[4] P. McCann. T. Hiller, J. Wang, A. Casati, C. Perkins, P. Calhoun: "Transparent Hierarchical Mobility Agents (THEMA)", Internet Draft (work in progress), draft-mccann-thema-00.txt, March '99.

[5] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP Regional Registration", Internet Draft (work in progress), draft-ietf-mobileip-reg-tunnel-02, March '00.

[6] DRiVE: http://www.ist-drive.org

[7] Charles E. Perkins and T. Jagannadh : "DHCP for Mobile Networking with TCP/IP", IEEE Symposium on Computers and Communications (ISCC'95), Alexandria, Egypt

[8] H. Soliman, C. Castelluccia, K. El-Maki, L. Bellier: Hierarchical MIPv6 mobility management (HMIPv6). Internet draft, work in progress, draft-ietf-mobileip-hmipv6-07.txt, July 2002

[9] P. Maniatis, M. Roussopoulos, E. Swierk, M. Lai, G. Appenzeller, X. Zhao, and M. Baker. "The Mobile People Architecture. ACM Mobile Computing and Communications Review (MC2R), July 1999. http://mosquitonet.stanford.edu/publications.html.

[10] H.J. Wang, B. Raman, C. Chuah, R. Biswas, R. Gummadi, B. Hohlt, X. Hong, E. Kiciman, Z. Mao, J.S. Shih, L. Subramanian, B.Y. Zhao, A.D. Joseph, and R.H. Katz. "ICEBERG: An Internet-core Network Architecture for Integrated Communications". IEEE Personal Communications, (Special Issue on IP-based Mobile Telecommunication Networks.), 2000. http://iceberg.cs.berkeley.edu/publications.html.

[11] E. Wedlund and H. Schulzrinne: "Mobility Support using SIP". In Proc. of Second ACM/IEEE International Conference on Wireless and Mobile Multimedia WoWMoM99, SeattleWashington, USA, August 1999.

[12] A. Valko.: "Cellular IP - A New Approach to Internet Host Mobility." ACM Computer Communication Review, January 1999

[13] R. Ramjee, T. LaPorta, S. Thuel, and K. Varadhan.: "IP micro-mobility support using HAWAII". INTERNET DRAFT work in progess, July 2000. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-hawaii-01.txt.

[14] A. Mihailovic, M.Shabeer, A.H. Aghvami: "Multicast for Mobility Protocol (MMP) for emerging internet networks", Proceedings of PIMRC2000, London, UK, September '00.

[15] J. Mysore and V. Bharghavan.: "A New Multicast-based Architecture for Internet Mobility", ACM MOBICOM 97, October 1997. http://www.acm.org/pubs/articles/proceedings/comm/262116/p161-mysore/p1%61-mysore.pdf.

[16] S. Seshan, H. Balakrishnan and R. H. Katz: “Handoffs in Cellular Wireless Networks: The Daedalus Implementation and Experience”, ACM/Baltzer Journal on Wireless Networks, ‘95.

[17] Thomson, Narten: Ipv6 Stateless Address Autoconfiguration, RFC 1971, RFC 2462

[18] Laura Marie Feeney: “A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks”, Technical Report, Swedish Institute of Computer Science, 1999

[19] A. O'Neill, G. Tsirtsis, and S. Corson: "Edge Mobility Architecture", Internet Draft (work in progress), draft-oneill-ema-01.txt,March ‘00.

[20] M. Stemm and R. Katz. “Vertical Handoffs in Wireless Overlay Networks.” ACM Mobile Networking (MONET), Special Issue on Mobile Networking in the Internet, Winter 1998. http://HTTP.CS.Berkeley.EDU/~stemm/publications/monet97.ps.gz.

[21] M. Wolf, M. Scharf, R. Eberhardt: “ Evaluation of Mobility Management Approaches for IPv6 based Mobile Car Networks”, KiVS 2003, February 2003, Leipzig

[22] T. Ernst, A. Olivereau, L. Bellier, C. Castelluccia, Hong-Yon Lach.: “Mobile Networks Support in Mobile IPv6 (Prefix Scope Binding Updates)”, draft-ernst-mobileip-v6-network-03.txt

[23] T. J. Kniveton, J. Malinen, V. Devarapalli, C. E. Perkins: “Mobile Router Tunneling Protocol”, draft-kniveton-mobrtr-03.txt

[24] Lasse Sundström: The Dynamic Host Configuration (DHCP)

[25] Montavont, Noel: *Handover Management for Mobile Nodes in IPv6 Networks*, IEEE Communications Magazine, Vol. 40 No. 8, August 2002

[26] Chang-Woo Lee, Seung-Jin Lee, Sung-Bum Joo, Chul-Hee Kang: Fast and Lossless Handoff Method considering Duplicate Address Detection in Ipv6-based Mobile/Wireless Networks

[27] IST-2000-28584 MIND, D2.2: MIND protocols and mechanisms specification, simulation and validation; http://www.dit.upm.es/~ist-mind/deliverables/MIND_D22_annex.pdf

[28] Kellerer et al.: (Auto) Mobile Communication in a Heterogeneous and Converged World", IEEE Personal Communication, Dec 2001.

[29] R. Hinden, M. O’Dell, and S. Deering.: “Aggregatable Global Unicast Address Format”. RFC 2374, July 1998.

[30] http://www.ietf.org/html.charters/multi6-charter.html.

[31] draft-ietf-multi6-multihoming-requirements-02.txt, Nov. 2001

[32] draft-survey-IPv6-multi-homing-00.txt, July 2001.

[33] J. Hagino and H. Snyder. IPv6 Multihoming Support at Site Exit Routers. RFC 3178, Oct. 2001.

[34] M. Py. Multi Homing Translation Protocol (MHTP). Internet-Draft, work in progress, draft-py-multi6-mhtp-01.txt, Nov. 2001.

[35] R. Tönjes, T. Lohmar, M. Vorwerk, R. Keller: „Flow Control for Multi-Access Systems"“, IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC 2002), Lisbon, 15-18. Sep.2002

[36] H. Soliman, K. El Maki, C. Castelluchia: “Per-flow movement in MIPv6”, IETF Internet Draft draft-soliman-mobileip-flow-move-02.txt (work in progress), July 2002

[37] C. Barz, M. Frank, H.-Y. Lach, A. Petrescu, M. Pilz, M. Wolf, L. Zömbik: "Network Access Control in OverDRiVE Mobile Networks", Submitted to IST Mobile & Wireless Communications Summit 2003, Aveiro, Portugal, 15-18 June 2003.

[38] Alexandru Petrescu, Michael Wolf, Markus Pilz, Hong-Yon Lach, Christophe Janneteau: "OverDRiVE Mobile Networks", Submitted to IST Mobile & Wireless Communications Summit 2003, Aveiro, Portugal, 15-18 June 2003.

[39] A. Striegel, R. Ramanujan, J. Bonney, "A Protocol Independent Internet Gateway for Ad Hoc Wireless Networks", in Proceedings of Local Computer Networks, LCN 2001.

[40] Yuan Sun, Elizabeth M. Belding-Royer, Charles E. Perkins, "Internet Connectivity for Ad Hoc Mobile Networks", International Journal of Wireless Information Networks special issue on Mobile Ad Hoc Networks, 2002.

[41] J. J. Garcia-Luna-Aceves, C. L. Fullmer, E. Madruga, D. Beyer, T. Frivold, "Wireless Internet Gateways (WINGs)", in Proceedings of MILCOM 1997,vol.3, pp. 1271– 1276.

[42] Christian Bettstetter, Jin Xi, "Wireless Internet Multihop Access: Gateway Discovery, Routing and Addressing", Proceedings of the International Conference on Third Generation Wireless and Beyond, 3GWireless 2002.

[43] Fred Baker, "OSPFv3 as a Manet Routing Protocol", Presentation to IETF, March 2002.

[44] C. Keszei, N. Georganopoulos, Z. Turanyi, A. Valko, "Evaluation of the BRAIN Candidate Mobility Management Protocol", IST Global Summit, Barcelona, September 2001

[45] C. Castellucia, "Toward a Hierarchical Mobile IPv6 Architecture", Eighth IFIP Conference on High Performance Networking, HPN '98, September 1998, Vienna.

[46] E. Gustaffson, A. Jonsson and C. Perkins, "Mobile IP Regional Tunnel Management", IETF Internet Draft, draft-ietf-mobileip-regtun-01.txt (work in progress), August 1999.

[47] J. Malinen, C. Perkins, "Mobile IPv6 Regional Registrations", IETF Internet Draft, draft-malinen-mobileip-regreg6-00.txt (work in progress), July 2000.

[48] R. Wakikawa, K. Uehara, K. Mitsuya and T. Ernst, "Basic Network Mobility Support", IETF Internet Draft, draft-wakikawa-nemo-basic-00.txt (work in progress), February 2003.

[49] R. Wakikawa, S Koshiba, K. Uehara and J. Murai, "ORC: Optimized Route Cache Management Protocol for Network Mobility", In Proceedings of the 10th IEEE International Conference on Telecommunications, ICT 2003, Papeete, Tahiti, February 2003.

[50] BRAIN: http://www.ist-brain.org

[51] MIND: http://www.ist-mind.org

[52] S. Aladdin. Host Controlled Forwarding. IST-1999-12515/DRiVE/D15.3.

[53] A. Petrescu, M. Catalina-Gallego, C. Janneteau, H.-Y. Lach, A. Olivereau, "Issues in Designing Mobile IPv6 Network Mobility Support with the MR-HA Bidirectional Tunnel (MRHA)", IETF Internet Draft, draft-petrescu-nemo-mrha-02.txt, Work in Progress, March 2003.

[54] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[55] Pat R. Calhoun, John Loughney, Erik Guttman, Glen Zorn, Jari Arkko, "Diameter Base Protocol", draft-ietf-aaa-diameter-17.txt, December 2002, work in progress

[56] Pat R. Calhoun, Tony Johansson, Charles E. Perkins, "Diameter Mobile IPv4 Application", draft-ietf-aaa-diameter-mobileip-13, October 2002, work in progress

[57] Stefano M. Faccin, Franck Le, Basavaraj Patil, Charles E. Perkins, "Diameter Mobile IPv6 Application", draft-le-aaa-diameter-mobileipv6-02.txt, September 2002, work in progress

[58] J. Kempf, E. Nordmark, "Threat Analysis for IPv6 Public Multi-Access Links", draft-kempf-ipng-netaccess-threats-02.txt, work in progress

[59] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998

[60] IEEE Standard for Local and metropolitan area networks, "Port-Based Network Access Control", IEEE Std 802.1x, 2001

[61] IETF PANA Charter, http://www.ietf.org/html.charters/pana-charter.html

[62] IETF SEND Charter, http://www.ietf.org/html.charters/send-charter.html

[63] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999

[64] T. Hiller, G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-00.txt, June 2002, work in progress

[65] B Aboba, J. Vollbrecht, "Proxy Chaining and Policy Implementation I Roaming", RFC 2607, June 1999

[66] B. Aboba, "Certificate-Based Roaming", draft-ietf-roamops-cert-02, April 1999, work in progress

[67] S. Floyd and V. Jacobson, "Link-sharing and Resource Management Models for Packet Networks", in IEEE/ACM Transactions on Networking, Vol. 3 No. 4, August 1995

[68] G. Chandranmenon, S.Suri, G. Varghese. "Leap Forward Virtual Clock: A New Fair Queuing Scheme with Guaranteed Delays and Throughput Fairness". Proceedings of IEEE INFOCOM '97, Kobe, Japan, April 1997

[69] R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: an Overview", RFC1633, June 1994

[70] S. Blake, D. Black, M. Carlson, E.Davies, Z. Wang, W.Weiss, "An Architecture for Differentiated Services", RFC2475, December 1998

[71] J. Bennett, H. Zhang. "WF2Q: Worst-case Fair Weighted Fair Queuing" Proceedings of IEEE INFOCOM '96, San Francisco, March 1996

[72] XTP-Forum. Xpress "Transport Protocol Specification", XTP Revision 4.0. XTP-Forum, March 1995

[73] M. Frank, P. Martini, "Fairness and Delay/Loss Study of an End-to-End Bandwidth Regulation Scheme", 23rd Annual Conference on Local Computer Networks, LCN `98, Boston, October 1998

[74] M. Shreedhar, G. Varghese. "Efficient Fair Queuing using Deficit Round Robin" IEEE/ACM Transactions on Networking, Vol. 4, No. 3, June 1996

[75] E. Kovacs, R. Keller, T. Lohmar, R. Kroh, and A. Held: "Adaptive Mobile Applications over Cellular Advanced Radio", PIRMC2000

[76] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998

[77] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998

[78] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol ", draft-ietf-ipsec-ikev2-05.txt, February 2003, work in progress

[79] P. Vixie, S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997

[80] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC2461, December 1998

[81] draft-ng-nemo-multihoming-issues-00.txt

[82] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998

[83] R. Droms, J. Bound, Bernie Volz, Ted Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", 2 Nov 2002, draft-ietf-dhc-dhcpv6-28.txt, work in progress

[84] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6" Internet draft, work in progress, draft-ietf-mobileip-ipv6-21.txt

[85] Braun, Castelluccia and Stattenberger, "An Analysis of the DiffServ Approach in Mobile Environments",IWQiM1999

[86] Miklós Aurél Rónai, Michael Wolf, Ralf Tönjes, Alexandru Petrescu, "Mobility Issues in OverDRiVE Mobile Networks", in proceedings of the IST Mobile Summit 2003 conference

[87] OverDRiVE homepage: http://www.ist-overdrive.org