Internet Draft
Document: draft-petrescu-nemo-mrha-02.txt
Expires: September 2003

A. Petrescu, ed.
M. Catalina-Gallego
C. Janneteau
H.-Y. Lach
A. Olivereau
Motorola

March 2003

# Issues in Designing Mobile IPv6 Network Mobility with the MR-HA Bidirectional Tunnel (MRHA)

<draft-petrescu-nemo-mrha-02.txt>

## Status of this Nemo



## Abstract

This document describes several issues relevant to the design of a network mobility support solution that relies on the bi-directional tunnel between Mobile Router and Home Agent, with Mobile IP. Examples of issues are: conflicting Mobile IP and RIPng/OSPF requirements on link-local addresses, HA/BR co-location, and "cross-over" tunnels.

Table of Contents

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].





## 1. Introduction

This document describes several issues relevant to the design of a network mobility support solution that relies on the bi-directional tunnel between Mobile Router and Home Agent, with Mobile IP. Examples of issues are: conflicting Mobile IP and RIPng/OSPF requirements on link-local addresses, HA/BR co-location and "cross-over" tunnels.

The Mobile Router is using Binding Updates, Binding Acknowledgments, Binding Requests and Binding Errors with the Home Agent to maintain the MRHA bidirectional tunnel.

The document is organized as follows: the next section presents a short perspective on three preliminary proposals for a NEMO "Basic" type of solution; the following section lists the issues that appear in this type of protocols. Two additional sections, or appendices, give more detail of issues by way of motivations, examples and other related issues.

## 2. Definitions

Complete NEMO terminology can be found in [9].

MH: a mobile host, which is a mobile node (MN) as defined by Mobile IPv6, except all router parts. In Mobile IPv6 terminology, MN

can be either a host or a router. An MH can only be a host.

MR_HoA: mobile router's Home Address, or the home address of the mobile (egress) interface of the mobile router.

MNP: mobile network prefix, or the prefix of the link of the mobile network that will move away. Note that in the most general case a single MR may route multiple prefixes, in which case there would be multiples MNPs per one mobile network.

FN: fixed node on the home link. It doesn't stand for fixed network.

## 3. NEMO "Basic" preliminary descriptions

An exhaustive description of the proposals to support mobile networks or mobile routers with Mobile IP bi-directional tunnel can hardly fit in the usual space reserved for an Internet Draft, which is traditionally a short document. We retain three main descriptions: Cisco Mobile IPv4 for Mobile Routers [4], MRTP [13] and the "Basic" approach [22].

MRTP is a method of enabling mobile routers by using dynamic tunnel registrations between the AR's point of attachment and its HA. This tunnel allows the HA to tunnel all traffic for the mobile network prefix to the MR, and also lets the MR forward all mobile network traffic back to the home network, where it is topologically correct, and can avoid ingress routing in the visited network.





MRTP does not suffer from the authorization problem of how to show that the MR owns the routing authority for the Mobile Network.

The approach relies on the bidirectional tunnel between MR and HA. The solution proposed is valid for Mobile IPv6 as for Mobile IPv4. The MR and HA behaviours still represent a sensitive departure from the Mobile IPv6 protocol in that MR informs its HA directly about the tunnel interface and dynamically triggers additions of routing table entries in the HA's routing table for the MR's tunnel. In addition, the most recent version of the draft proposes usage of the PSBUs in order to inform the HA about the prefix of the mobile network (thus a combination with the PSBU approach). Moreover, the considerations about dynamic routing in this draft refer only to how dynamic routing would work with a MR, but not about the necessity of running a routing protocol between HA and MR.

In the Mobile IPv4 case, the network mobility support with the MRHA tunnel has been reported at least by various teams at Cisco [4] and NASA [14].

The Basic protocol proposed in [22] takes a different tack at assigning the home addresses: it assigns it to the MR's ingress interface, instead of the egress interface. In addition, it proposes a two step approach for the search algorithm in the HA's binding cache: the first step is a search based on a key that is a full /128 address, while the second step is a search based on longest-prefix match. A new aspect is that this proposals relies also on a (yet to be developped) prefix delegation scheme where the HA assigns the mobile network prefix to MR, in a dynamic manner.

For a more detailed analysis on the first two approaches (MRTP and Cisco Mobile Routers) see sections A.4.2 and A.4.3.

## 4. Issues

The following is a list of issues that we believe might be relevant when designing a Basic type of solution by the NEMO WG. Some of the issues are exemplified in the Appendices.

### 4.1 Implementation-independent specification terms

The specification of the basic network mobility support should be expressed with implementation-independent terms. In other words, clear distinction should be made between the specification of the protocol and a description of a possible implementation of this protocol. Especially, since it is to be based on Mobile IP(v6), the basic NEMO support specification should not make any assumption on how Mobile IP(v6) is implemented but instead re-use (and possibly extend) data structures from the Mobile IP(v6) specification (e.g. Binding Cache), and eventually introduce new ones if needed. Below are two examples of how attention should be payed in the specification of the protocol.





The bi-directional approach requires MR's HA to configure a "forwarding information" for the mobile network prefix towards the mobile router. Since the Mobile IP(v6) specification introduces a dedicated structure, so-called Binding Cache, to store

mobility-related "forwading information" on the HA, the specification of basic NEMO support should re-use/extend the Binding Cache to include the new mobility-related "forwarding information" for a mobile network. Even though a Binding Cache may be implemented as an extension of a routing table, the specification should relate to the Binding Cache and not the routing table. For instance, the specification should relate to the "forwading information" to be configured on MR's HA for the mobile network prefix in terms of a prefix entry in the Binding Cache instead of an entry in the routing table of MR's HA. Especially, Mobile IP(v6) specification does not specify any routing table for a HA.

Similarly, the specification should not assume that a tunnel, e.g. the MRHA bi-directionnal tunnel, is visible as a virtual network interface on the MR or HA. This is an implementation-related consideration that may not be true for all IP(v6)/MobileIP(v6) stacks.

Such considerations will allow to clearly draw the line between the specification and a description of a possible implementation, and as a result ease any future implementation of the basic NEMO support as an extention of an existing Mobile IPv6 implementation.

### 4.2 Allow for deployment flexibility

The basic NEMO support specification should not assume MR's HA to be co-located with the Border Router (BR) of MR's home network. The HA should be allowed to be a one-interface machine, separated from BR, that does only NEMO HA functionalities (as a Mobile IP(v6) HA can be). This way, HA can be deployed in a home domain without the need to upgrade deployed BRs offering an easy deployment path.

### 4.3 Dynamic routing protocol and the HA

Considering the case of a HA deployed as a one-interface machine not co-located with BR, the basic NEMO support specification should not mandate the HA to run a routing protocol, even in situation when MR runs a routing protocol. On the other hand, such HA should allow MR and BR to continue running the dynamic routing protocol as if MR was at home. Suffices it for the HA to: (1) join the corresponding multicast address, intercept all packets addressed to the link-local address of MR and encapsulate towards current MR CoA and (2) relay, or forward, towards BR all dynamic routing message exchanges coming from MR.

### 4.4 Link-local addresses

According to section 10.4.2 of Mobile IPv6 spec [12] the HA will not allow re-direction of traffic of a Home Address towards a CoA, when that Home Address is link-local. Two relevant paragraphs:

> "However, packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node."
>
> "Multicast packets addressed to a multicast address with link-local scope [], to which the mobile node is subscribed, MUST NOT be tunneled to the mobile node;"

which exposes, of course, the very nature of link-local addresses: they are local, not going anywhere.

On another hand, OSPF for IPv6 [5] requires that:

> "On all OSPF interfaces except virtual links, OSPF packets are sent using the interface's associated link-local unicast address as source."

Moreover, RIPng [16] requires that: (1) next hop addresses in routing tables managed by RIPng be link-local and (2) a large part of RIPng messages be originated and adressed to link-local addresses:

> "An address specified as a next hop must be a link-local address."

or

> "Response Messages: [...] the source of the datagram must be a link-local address."

or

> "Generating Response messages: [...] The IPv6 source address must be a link-local address of the possible addresses of the sending router's interface, except when replying to a unicast Request Message from a port other than the RIPng port."

Overall, keeping in mind that Mobile IPv6 is not dealing with link-local home addresses and that routing protocols and forwarding process make substantial use of link-local addresses, the issue is clearly how to make the routing protocols work together with Mobile IPv6. Basic NEMO support specification should enable redirection of traffic destined to MR's link-local addresses.

## 4.5 Mobile Router as a Mobile Host

There are several scenarios that involve an MR that needs to act as a MH too, that is, send normal BUs and use existing Mobile IPv6. Applications running on the MR should take advantage of MR's session continuity and universal reachability at its home address. For more example issues see section B.

## 4.6 Neighbour Discovery for MR's egress interface

Neighbour Discover on the MR's egress interface is particularly delicate in that Neighbour Discovery should act differently when MR





is at home and when MR is in a foreign network. A simple example is that when MR is at home, it has little reason to listen to RAs. However, when MR is in a foreign network, receiving RAs is very important in order to have a good working of Mobile IPv6. For more example issues see section B.

## 4.7 Separation of routing and mobility for MR

The necessity of the distinction between mobility vs. routing exchanges holds true irrespective to whether dynamic or static routing is used. If static routing is used, then BR has routes towards the mobile network through the MR, and MR has routes towards the Internet through the BR. If dynamic routing is used, then the MR and BR dynamically exchange routing information that is manually configured in the routing configuration files of MR and of BR, as well as routing information that is delivered by other routers external to the home network (be it beyond the BR or beyond the MR). The entities concerned with routing in the home network are only BR and MR. This behaviour should continue when network mobility is introduced, presumably by deploying an HA (but not touching the BR). MR and HA should exchange only the information related to mobility but not the information related to routing.

## 4.8 Prefix-based routing and host-based routing exceptions

Prefix-based hierarchical routing (where the mobile network link has a prefix that is a subset of the home-network link) is the preferred type of routing for IPv6. Practically though, it is possible for the BR to have a routing table entry containing the prefix of the mobile network, as well as a host-based entry that points to a certain LFN also in the mobile network. Those two entries might or might not have the same common sub-prefix. With a MR at home, being a normal router, BR will know how to forward to

all hosts behind the MR as well as only to the specific LFN of the host-based route. This behaviour should be maintained when the MR is no longer at home and when it has a bidirectional tunnel MRHA.

## 4.9 IPv4 Issues

The mechanisms and issues described in this draft for IPv6 mobile networks can be applied for IPv4 network mobility as well. RFC 3344 [21] provides important intuititve support for IPv4 network mobility through the 'R' bit in Registration Requests/Replies. Some solutions have already been successfully tested in [4] and [14]. The support provided in RFC 3344 [21] as well as those solutions keep the HA co-located with the BR. In a general case in which the BR and HA are kept on separate machines (scenarios 9 to 16 in section A.2.3) the same issues as in IPv6 apply to the IPv4 case.

Additionally, in Mobile IPv4 there is a distinction between the MN and FA functionality, and it is possible to have the FA separated from the MN, whereas in IPv6 MN and FA are always co-located. This gets us to the following additional cases:





- When the MR is in a visited network it can send BU's using a co-located care-of address or a Foreing Agent care-of address if an FA is available. In the latter case, two reverse tunneling modes are possible: direct delivery style and encapsulated delivery style [17].

- The MR may be itself a FA for Leaf Mobile Nodes (LMNs), or the mobile network may contain a FA for LMNs.

## 4.10 "Cross-over" tunnels

A rough definition: two MR-HA tunnels are "crossing over" each other when the path between one tunnel's endpoints includes only one of the other tunnel's endpoints.

Support of nested mobile networks is possible only when the path from MR2 to MR1's HA does not go through MR1 (path considered when both mobile routers are at home and no tunnels are in place).

An example of the dynamics of two MR-HA crossing tunnels is given in section B.6.

## 5. Security Considerations

A detailed threat analysis is to be performed for a NEMO "Basic" type of solution. But that's what the Charter says anyways.

One issue is related to when the MR runs a dynamic routing protocol. In that case, MR is able to inform the routers in the home domain about new routes (or "inject" routes in the home domain). Considering that MR might be a small device, not locked in a highly secured room, not a tamper-proof device, potentially being stolen, then it is clear that the ability to introduce routes in the home domain, and worse, propagating upper to backbones, is inducing serious risks.

### 5.1 A tool: HA ingress filtering

Home Agents supporting mobile networks are normally able to perform ingress filtering, so that only topologically correct packets leave the HA. See section B.7 on how HA could do ingress filtering.

## Acknowledgements

Authors of this document acknowledge the following WG members and non-members for their remarks, improvements to this draft and fruitful discussions:

Tim Leinumeller for many insightful remarks and implementation aspects.

Mattias Petterson.

Vijay Devarapalli.



---



TJ Kniveton.

Pekka P□□kk÷nen.

Mooi Choo Chuah.

Erik Nordmark.

## References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement

Levels", BCP 14, RFC 2119, March 1997

[2] Arkko, Jari, Devarapalli, Vijay, and Dupont, Francis, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", draft-ietf-mobileip-mipv6-ha-ipsec-03.txt, IETF Internet Draft, February 2003. (Work in Progress).

[3] Baker, F. and Atkinson, R., "RIP-2 MD5 Authentication", RFC 2082, January 1997.

[4] Cisco authors, "Cisco Mobile Networks", whitepaper browsed March 3rd, 2003 at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.pdf

[5] Coltun, R., Ferguson, D. and Moy, J., "OSPF for IPv6", RFC 2740, December 1999.

[6] Conta, A. and Deering, S.,"Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[7] Crawford, M., "Router Renumbering for IPv6", RFC 2894, August 2000.

[8] Ernst, Thierry, Olivereau, Alexis, Bellier, Ludovic, Castelluccia, Claude and Lach, Hong-Yon, "Mobile Networks Support in Mobile IPv6", draft-ernst-mobileip-v6-network-03.txt, IETF Internet Draft, March 2002. (Work in Progress).

[9] Ernst, Thierry and Lach, Hong-Yon, "Network Mobility Support Terminology", draft-ernst-nemo-terminology-01.txt, IETF Internet Draft, November 2002. (Work in Progress).

[10] Harkins, D., Mankin, A., Narten, T., Nikander, P., Nordmark, E., Patil, B. and Roberts, P., "Threat Models introduced by Mobile IPv6 and Requirements for Security", draft-ietf-mobileip-mipv6-scrty-reqts-02.txt, IETF Internet Draft, November 2001. (Work in Progress).

[11] Hedrick, C., "Routing Information Protocol", RFC 1058, June 1998.

[12] Johnson, David B., Perkins, Charles E. and Arkko, Jari, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-20.txt, IETF Internet Draft, January 2003. (Work in Progress).

[13] Kniveton, Timothy J., Malinen, Jari T. and Devarapalli, Vijay, "Mobile Router Tunneling Protocol", draft-kniveton-mobrtr-03.txt, IETF Internet Draft, November 2003. (Work in Progress).

[14] Leung, K. and Shell, D. and Ivancic, W. D. and Stewart, D. H. and Bell, T. L. and Kachmar, B. A., "Application of Mobile-IP to Space and Aeronautical Networks", IEEE Proceedngs of the Aerospace Conference, 2001.

[15] Malkin, G., "RIP Version 2, Carrying Additional Information", RFC 1723, November 1994.

[16] Malkin, G., "RIPng for IPv6", RFC 2080, January 1997.

[17] Montenegro, G., ed., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[18] Moy, J., "OSPF Version 2", RFC 2328, April 1998.

[19] Narten, T., Nordmark, E. and Simpson, W., "Neighbour Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[20] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[21] Perkins, C., ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.

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

Changes

October 2002: revision 00 submitted.

November 2002: revision 01:

- -added discussion on multicast addresses with link-local scope.
- -added Chairs' addresses.
- -modified the abstract to better express the fact that /128s are probably sufficient.
- -added section on v4 issues, and Mobile IPv4 issues.
- -added an empty IPR section.

March 2003: revision 02:

- -major overhaul from revision 01: shorter, focused on main issues, integrated some ml discussions, moved large "Motivation" parts to appendices.
- -added MH definition and used MH instead of MN when MR acts as an

MH.
-added more detailed acknowledgements.
-added "cross-over" tunnels discussion.
-added HA ingress filtering.





## Appendix A: Motivation for Full Addresses in Binding Updates

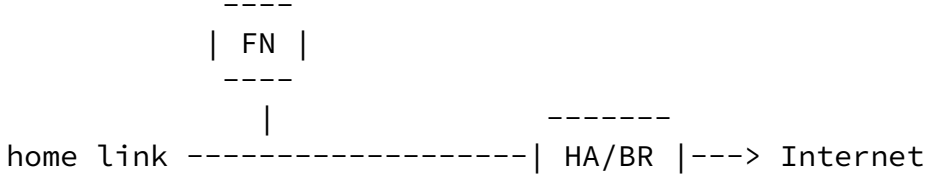
An initial remark is that traffic coming from outside the home link, or from other hosts on the home link, and directed to hosts in the mobile network (or behind the mobile router) only need to go through the L2 address of the mobile router (corresponding to its L3 address). With Proxy ND [19], it is the HA that pretends to own MR's L3 address by advertising new associations of the MR's L3 address to the its own L2 address, thus intercepting MR's home traffic and forwarding it to the current CoA of the MR.

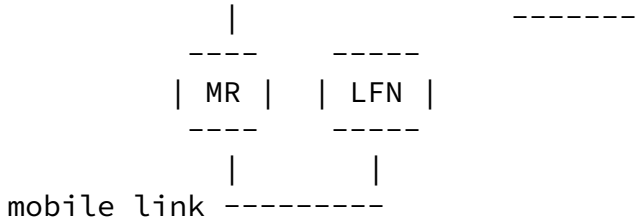
With this in mind, it can be stated that when the MR is in a foreign network, traffic coming from hosts in the mobile network and towards anywhere to the Internet, is first forwarded by the MR through the reverse tunnel MRHA to the HA. Then HA decapsulates and forwards to the address specified in the inner packet.

### A.1 Description of a Home Network

When designing a NEMO solution with the MRHA tunnel, the first steps are to carefully consider the actual behaviour of the home network when the mobile network is at home, employing normal routing. Then this behaviour should be maintained as much as possible when the MR is not at home (e.g. MR should be able to send redirects through the MRHA tunnel); reciprocically, the normal behaviour of an FR at home should change when that FR is an MR and is at home (e.g. when MR at home, the MRHA tunnel should be torn down). When the MR is in a foreign network, its presence at home is simulated by the HA (as in Mobile IPv6 for hosts).

Let us consider a simple case of a home network that supports movement of one of its links. The home network is made up of a home link and a mobile network link, separated by the Mobile Router. The home network is connected to the Internet via the Border Router, as presented in the figure:

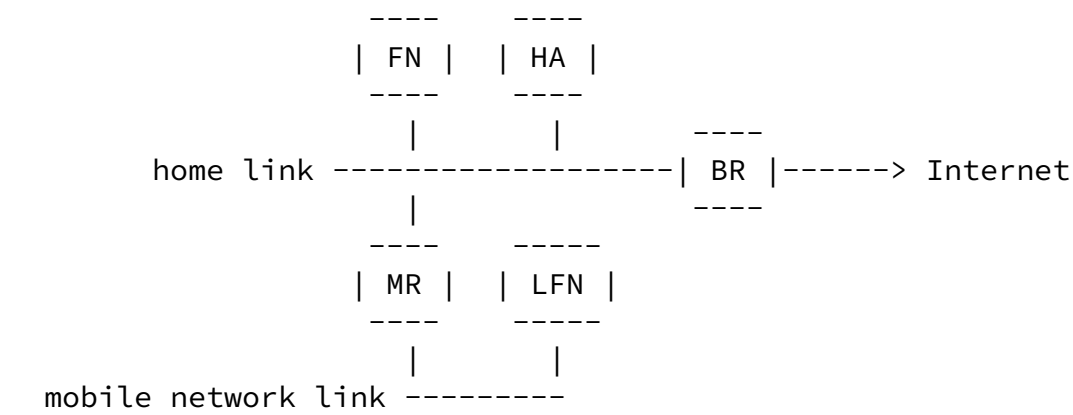





Current specification for Mobile IPv6 implies that the HA can be either co-located with the BR, or it can act as a separate one-interface machine (this is advantageous for deploying Mobile IPv6 without changing BRs). For mobile networks, the latter mode can be pictured like this:








It is assumed that routes outside the home link are managed by BR and MR, either in a static manner (operator fills in routing tables) or dynamic manner (application software partially manages routing tables). Remark that even when the dynamic style is used, it is still true that operator fills initial routing configuration files, where she/he puts the image of the network as being what the operator believes it to be. The dynamic behaviour of routing protocols intervenes when certain links come down or up due to failures, the operator view is no longer true, and the routers manage to find alternative paths. Also, the dynamic behaviour helps obtaining shortest paths over large networks, relying on several local operator's views of smaller sized networks. Addition of mobility should not change this.

If static routing is used instead of dynamic routing, then static routes are added manually both on MR and on the BR. When considering adding *static* routes in a *dynamic* manner for

prefixes shorter than /128 by Mobile IP, authors of this document realize (in truth, hopefully) that Mobile IP starts using semantics that are traditionally belonging to routing protocols.

### A.2 Scenarios

For the sake of completetess, we first describe a simple "manual" scenario for mobile networks based on the MRHA tunnel, that exposes relative simplicity, that uses static routing and doesn't use Mobile IP.

Then, adding the Mobile IP behaviour, we present detailed scenarios of communication between an FN on the home link and an LFN on the mobile network link and a CN on the Internet, when the mobile network is at home and away from home in a visited network, and when the HA is co-located with the BR and separated from the BR. All in all, 16 simple scenarios are presented.

The scenarios where HA is co-located with BR (1 up to 8) expose that there is no need for MR to communicate prefixes to its HA via BUs. In a normal routing function, when the MR is at home, it exchanges routing information with the BR (co-located with the HA) and thus those prefixes are communicated by e.g. RIP or OSPF. When the MR is not at home, this behaviour continues, but through the MRHA tunnel.





The scenarios where HA and BR are separated (9 up to 16) expose that HA needs an entry in its routing table in order to be capable of forwarding packets to the MR (when it is not at home).

An additional scenario is then presented where MR at home is using ICMP Redirect, a functionality that might be needed even when the MR is not at home.

#### A.2.1 Manual Mobile Networks

Authors of this draft have experimented with "manual" mobile networks in IPv4, where the addition of routes and tunnels on the MR and on the BR are done manually, by operators talking on the phone.

A home network was used that contains about 10 routers and about 12 subnets. That home network is connected to the Internet with a BR.

All routers have static routes among them.

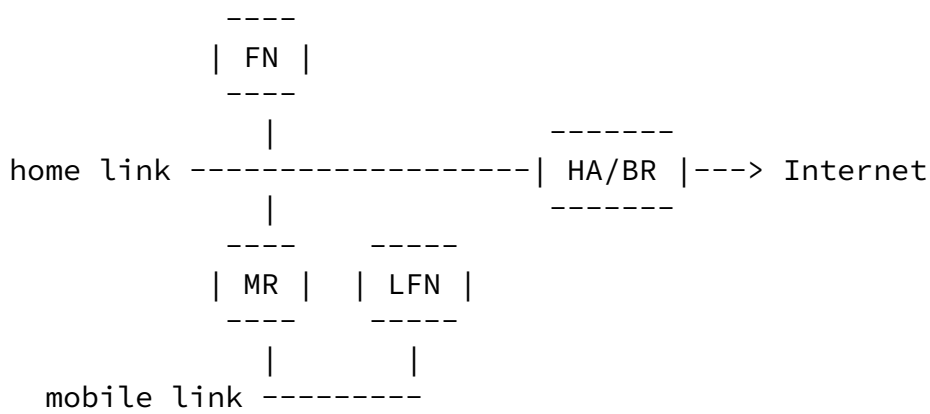
Then, one slice of that home network (the mobile network) containing one "MR", one normal router and 6 subnets, was disconnected from home, and moved across the Atlantic. Once the "MR" was connected on the other side, it was manually configured with a new IPv4 address, mask and default route. Then a tunnel interface and a route were manually set up on the MR, a tunnel interface and a route were manually set up on the BR. All other routes on all other routers where not touched. Mobile IP software was not used.

The entire network (the home and the mobile network) looked, and acted, as if the mobile slice were at home. During this, several applications were tested between hosts in the mobile network, hosts in the home network and hosts on the Internet (incidentally, one of the applications was relying on Mobile IPv4 for hosts, but in no relation with the mobile network moving).

Again, this "manual" mobile networks scenario was not using any dynamic routing protocol, and the tunnel was not supporting any form of broadcast of multicast.

### A.2.2 Scenarios with Co-located HA and BR

1. FN sends packet to LFN, mobile network home, HA/BR colocated





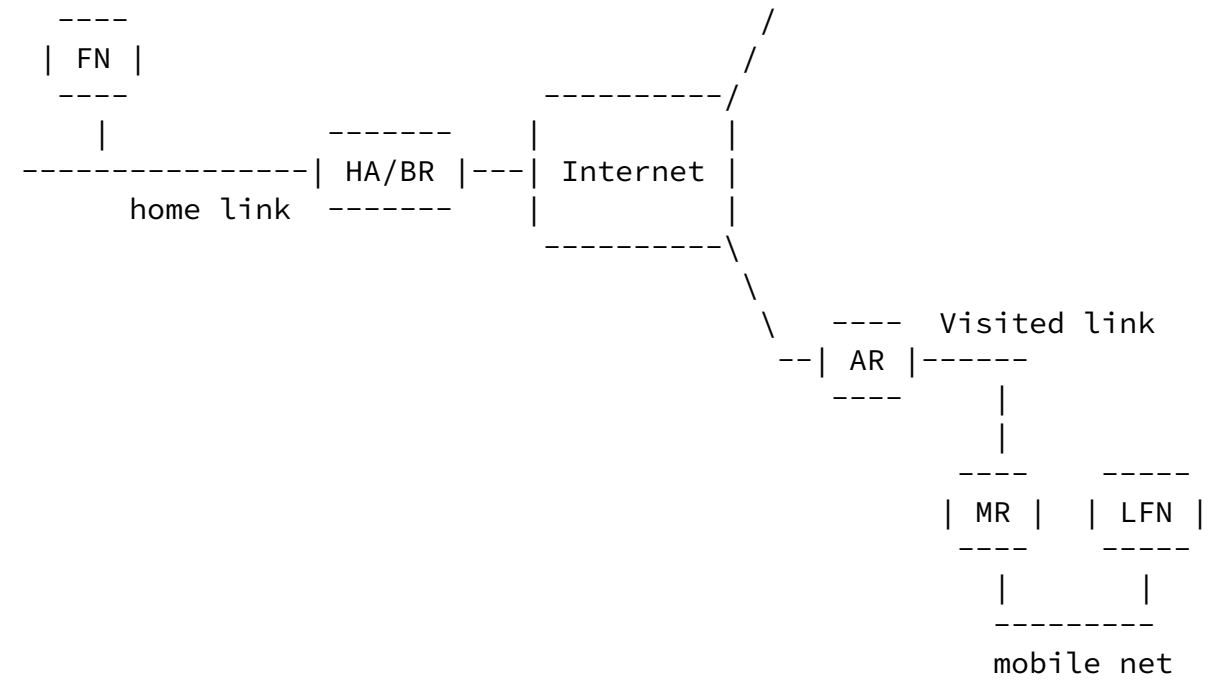



-FN scans its routing table for LFN's address, and finds default route towards BR.
-FN sends NS for L2 address of BR.
-BR replies NA.
-FN sends packet to BR.
-HA scans its BC to find out whether MR is at home; BR scans its routing table for LFN's address, and finds route through MR;

-BR sends NS for MR.
-MR replies NA with its L2 address.
-BR forwards packet to MR and sends ICMP Redirect to FN such that subsequent packets from FN to LFN go straight through MR and not through BR.
-MR forwards packet to FN.

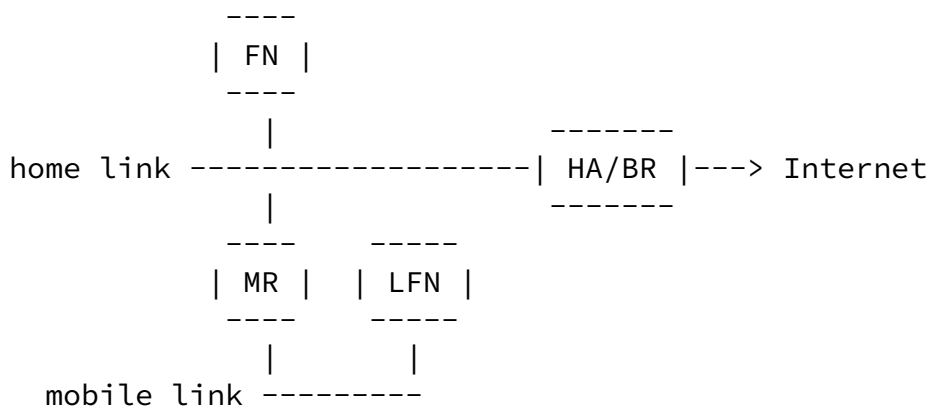
The sensitive issue exposed here is the way in which initially the packet travels from FN to BR to MR, the dynamic addition of an entry in the routing table of the FN (even if FN doesn't run a routing protocol) and that subsequent packets will not go through BR, but from FN to MR to LFN.

2. FN sends packet to LFN, mobile network visits, HA/BR colocated



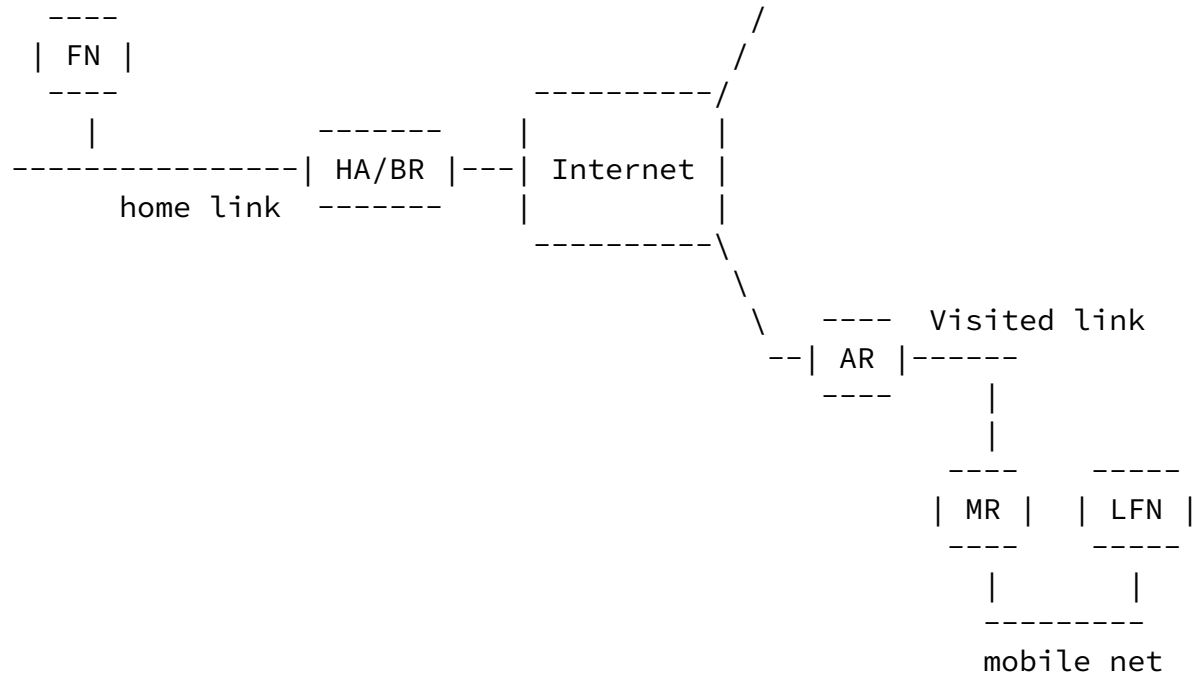

-FN scans its routing table for LFN's address, and finds default route towards BR.
-FN sends NS for L2 address of BR.
-BR replies NA.
-FN sends packet to BR.
-BR scans its routing table for LFN's address, and finds route through MR;
-BR (being an HA) scans its BC and its routing table and finds it needs to encapsulate this packet towards MR's CoA.
-BR encapsulates through the MRHA tunnel to MR's CoA.
-MR decapsulates and forwards to LFN.

3. LFN sends packet to FN, mobile network home, HA/BR colocated




-LFN scans its routing table for FN's address, and finds default route towards MR.
-LFN sends NS for L2 address of MR.
-MR replies NA.
-LFN sends packet to MR.
-MR scans its routing table for LFN's address, and finds route 'on-link';
-MR sends NS for FN.
-FN replies NA with its L2 address.
-MR forwards packet to FN.

4. LFN sends packet to FN, mobile network visits, HA/BR colocated




-LFN scans its routing table for FN's address, and finds default route towards MR.
-LFN sends NS for L2 address of MR.
-MR replies NA.
-LFN sends packet to MR.

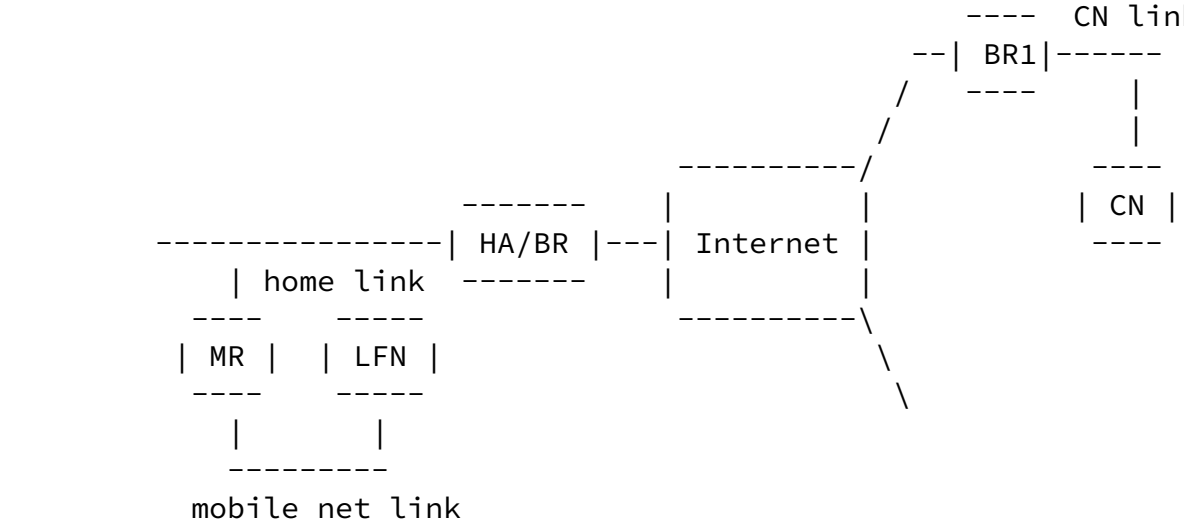
-MR encapsulates this packet through the MRHA tunnel and sends to HA.
-HA receives this packet and decapsulates.
-HA scans its routing table for FN's address, and finds route 'on-link';
-HA sends NS for FN.
-FN replies NA with its L2 address.





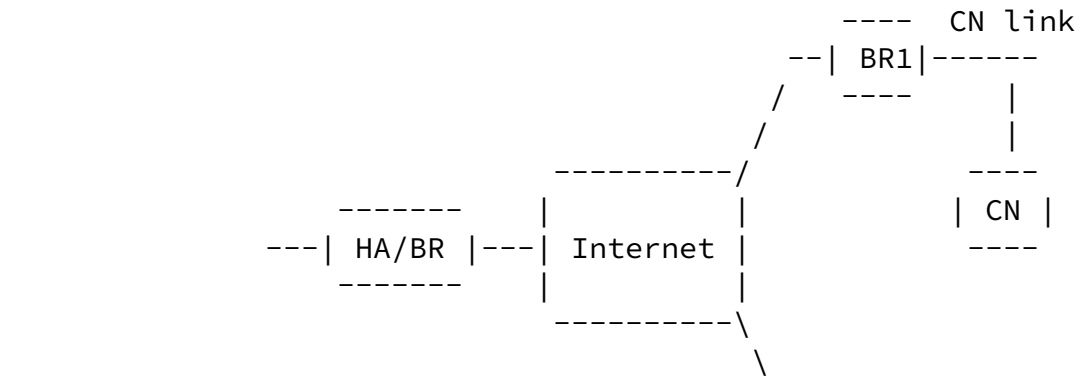
-HA forwards packet to FN (on behalf of the MR).

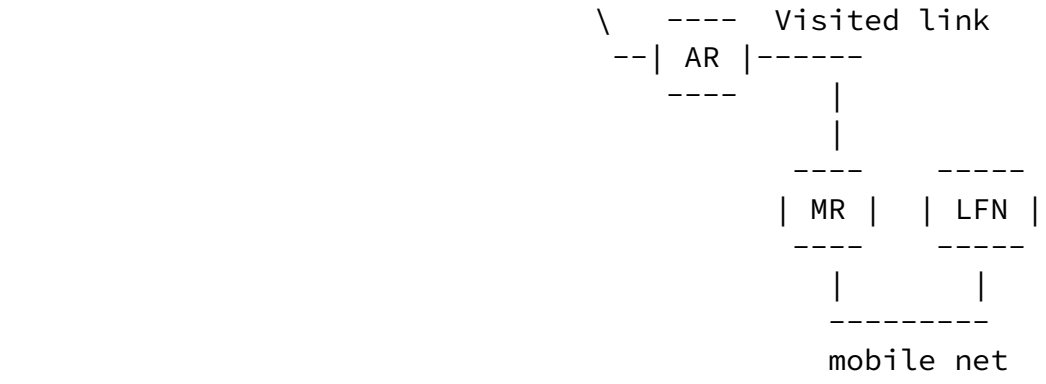
5. CN sends packet to LFN, mobile network home, HA/BR co-located




-BR receives packet from CN towards LFN.
-HA scans its BC to see whether MR is at home; BR scans its routing table and finds dest through MR.
-BR sends NS for L2 address of MR and MR replies NA.
-BR forwards packet to MR.
-MR forwards packet to LFN.

6. CN sends packet to LFN, mobile network visits, HA/BR colocated






-BR receives packet from CN towards LFN.
-BR scans its routing table and finds dest through MR.
-BR scans its routing table and its BC and realizes it needs to send this through the MRHA tunnel.
-BR sends the packet through the MRHA tunnel to MR.
-MR decapsulates and forwards to LFN.

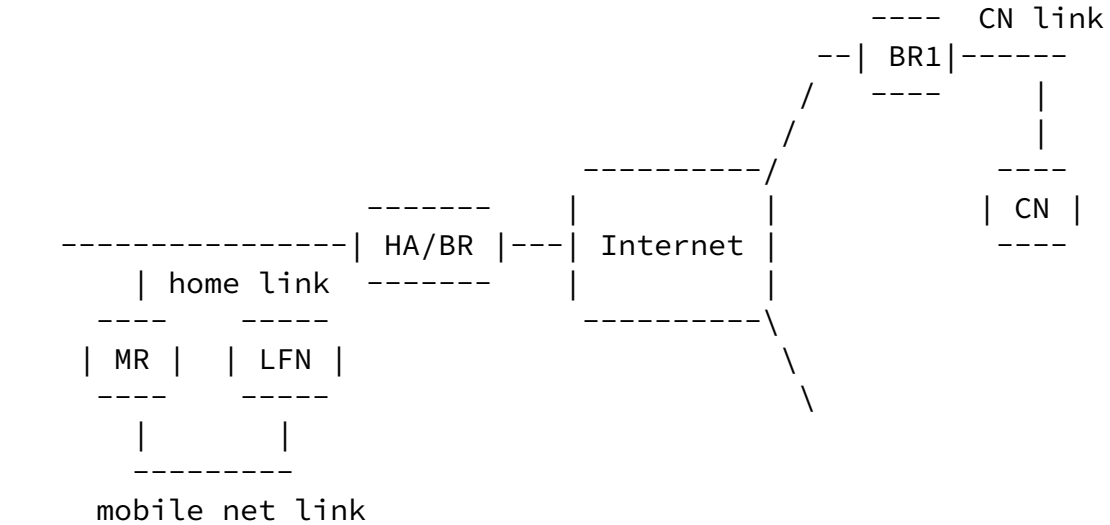
(this is sometimes referred to as triangular routing, since the





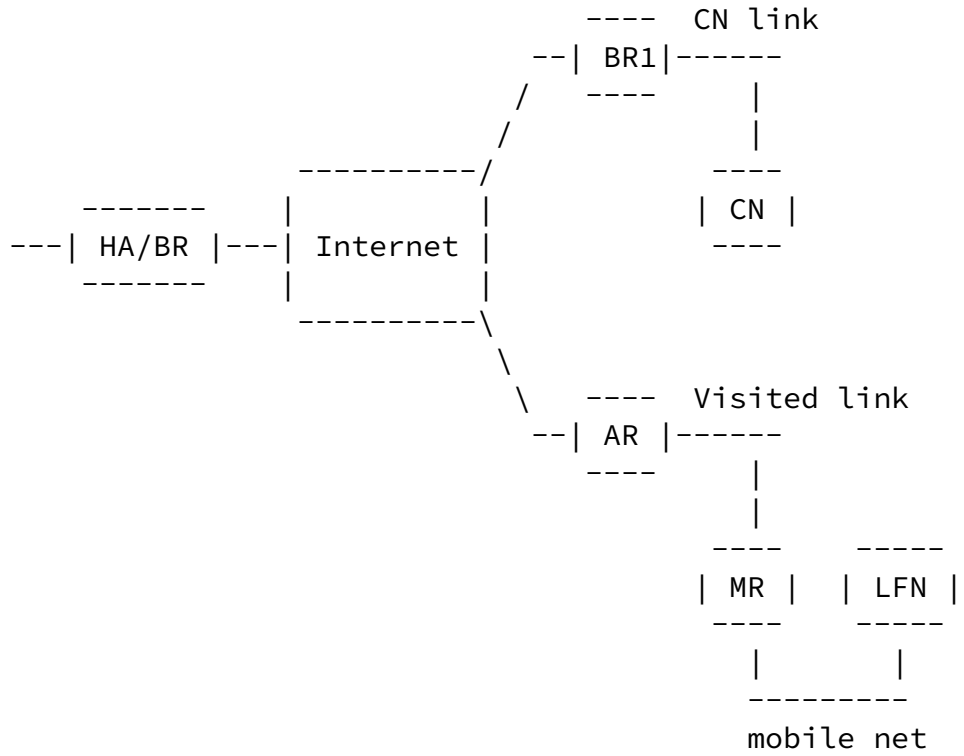
packet from CN to LFN travels artificially through BR)

7. LFN sends packet to CN, mobile network home, HA/BR colocated




-MR receives packet from LFN towards CN.
-MR scans its routing table to and finds dest through BR.
-BR forwards packet to Internet towards CN.
-BR1 forwards packet to CN.

8. LFN sends packet to CN, mobile network visits, HA/BR colocated




-MR receives packet from LFN towards CN.
-MR scans its tables and finds it needs to send it through the MRHA tunnel.
-BR receives this packet, decapsulates and forwards to Internet.
-BR1 forwards this packet to CN.

(this is sometimes referred to as triangular routing, since the packet from LFN to CN travels artificially through BR)

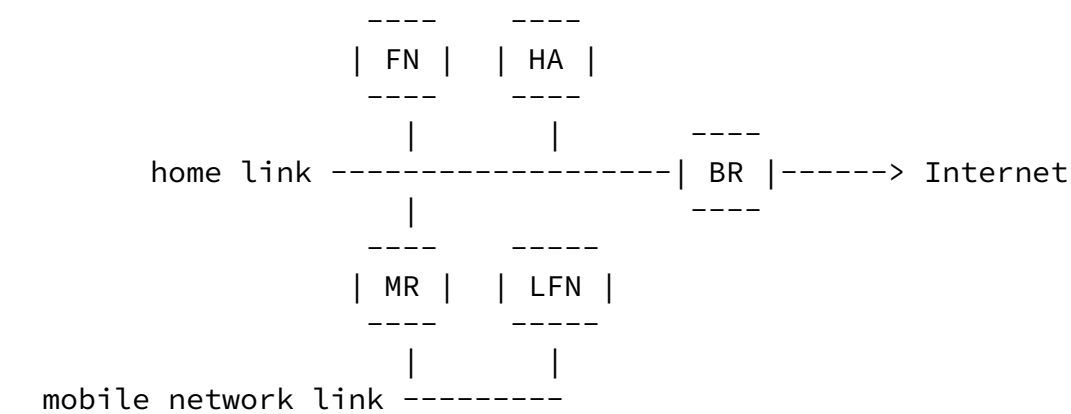


---



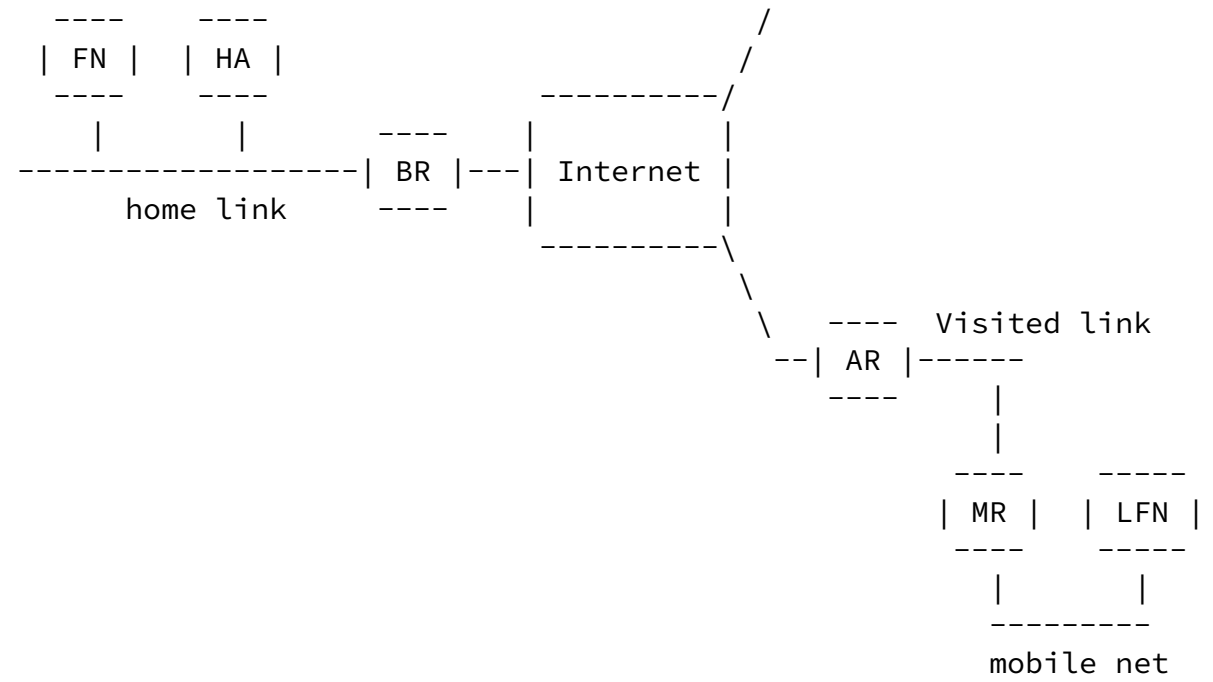
A.2.3 Scenarios with HA and BR Separated

9. FN sends packet to LFN, mobile network home, HA separated BR



-FN scans its routing table for LFN's address, and finds default
route towards BR.
-FN sends NS for L2 address of BR.
-BR replies NA.
-FN sends packet to BR.
-BR scans its routing table for LFN's address, and finds route
through MR;
-BR sends NS for MR.
-MR replies NA with its L2 address.
-BR forwards packet to MR and sends ICMP Redirect to FN such that
subsequent packets from FN to LFN go straight through MR and not
through BR.
-MR forwards packet to FN.

10. FN sends packet to LFN, mobile network visits, HA separated BR




-FN scans its routing table for LFN's address, and finds default



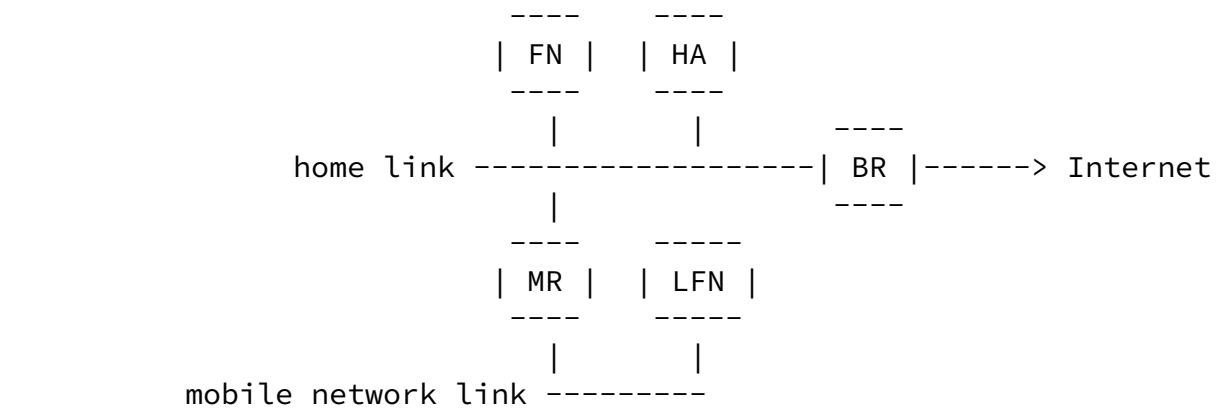


route towards BR.
-FN sends NS for L2 address of BR.
-BR replies NA.
-FN sends packet to BR.

-BR scans its routing table for LFN's address, and finds route
 through MR;
-BR sends NS for MR.
-HA replies NA with its L2 address (on behalf of MR).
-BR forwards packet to HA and sends ICMP Redirect to FN such that
 subsequent packets from FN to LFN go straight through MR and not
 through BR.  BR also sends ICMP Redirect to HA, such that HA knows
 a route through MR.  The logic of this last ICMP Redirect is
 described in section 6.1.
-HA scans its routing table for LFN's address, and finds through MR;
-HA scans binding cache and finds 'through MRHA tunnel';
-HA encapsulates and sends packet to MR.
-MR decapsulates and forwards to LFN.

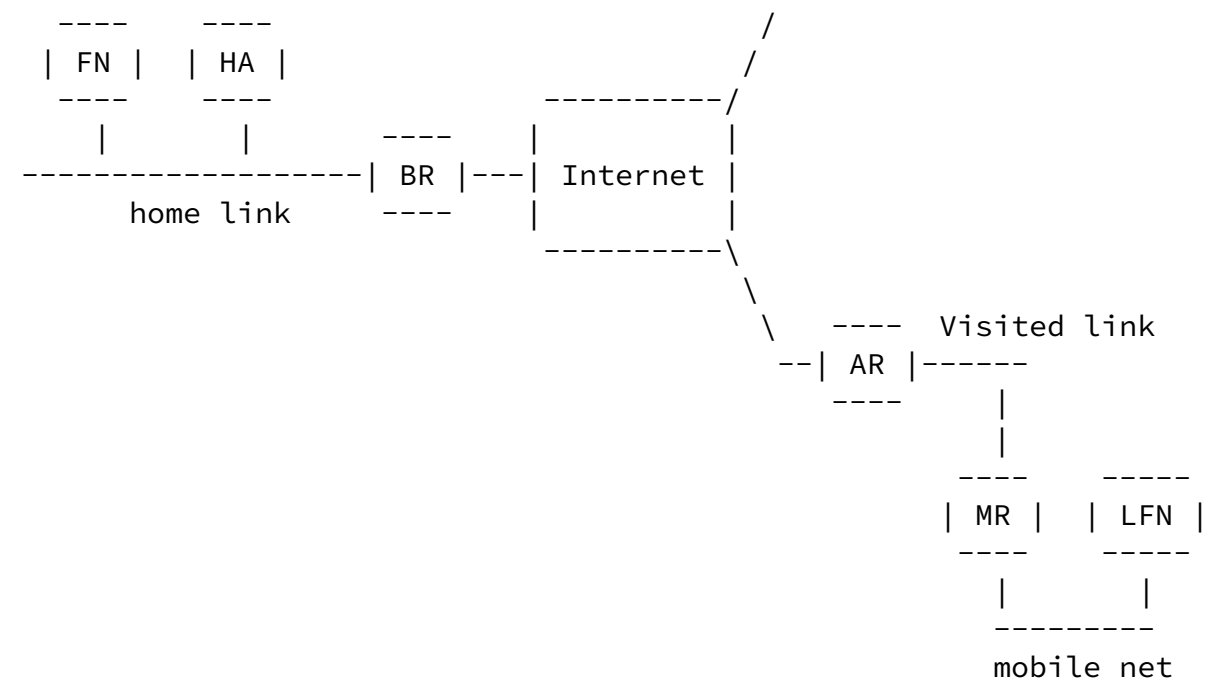
The problem in the above case is how to inform the HA about the
route towards MR.  When MR at home, and HA being a host, normally
HA doesn't have a route towards MR.

11. LFN sends packet to FN, mobile network home, HA separated BR



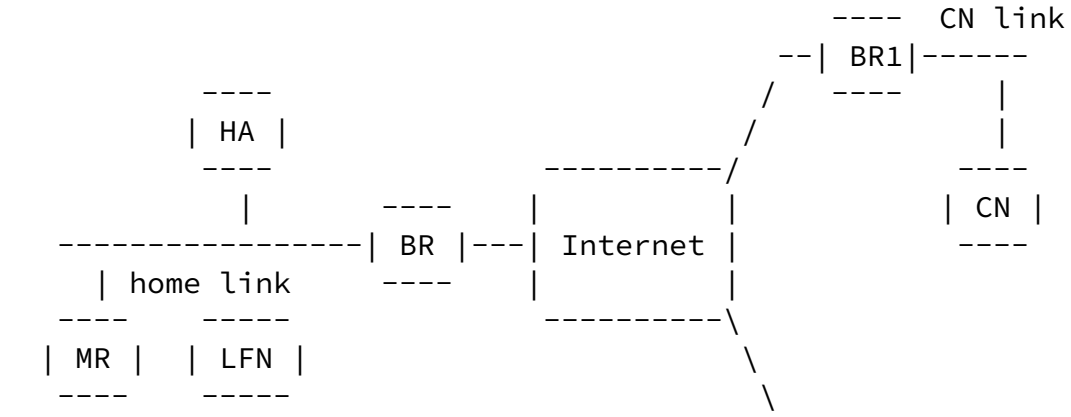

-LFN scans its routing table for FN's address, and finds default
 route towards MR.
-LFN sends NS for L2 address of MR.
-MR replies NA.
-LFN sends packet to MR.
-MR scans its routing table for LFN's address, and finds route
 'on-link';
-MR sends NS for FN.
-FN replies NA with its L2 address.
-MR forwards packet to FN.

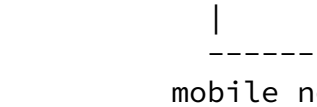
12. LFN sends packet to FN, mobile network visits, HA separated BR




-LFN scans its routing table for FN's address, and finds default route towards MR.
-LFN sends NS for L2 address of MR. MR replies NA.
-LFN sends packet to MR.
-MR encapsulates this packet through the MRHA tunnel and sends to HA.
-HA receives this packet and decapsulates.
-HA scans its routing table for FN's address, and finds route 'on-link';
-HA sends NS for FN.  FN replies NA with its L2 address.
-HA forwards packet to FN (on behalf of the MR).

13. CN sends packet to LFN, mobile network home, HA separated BR





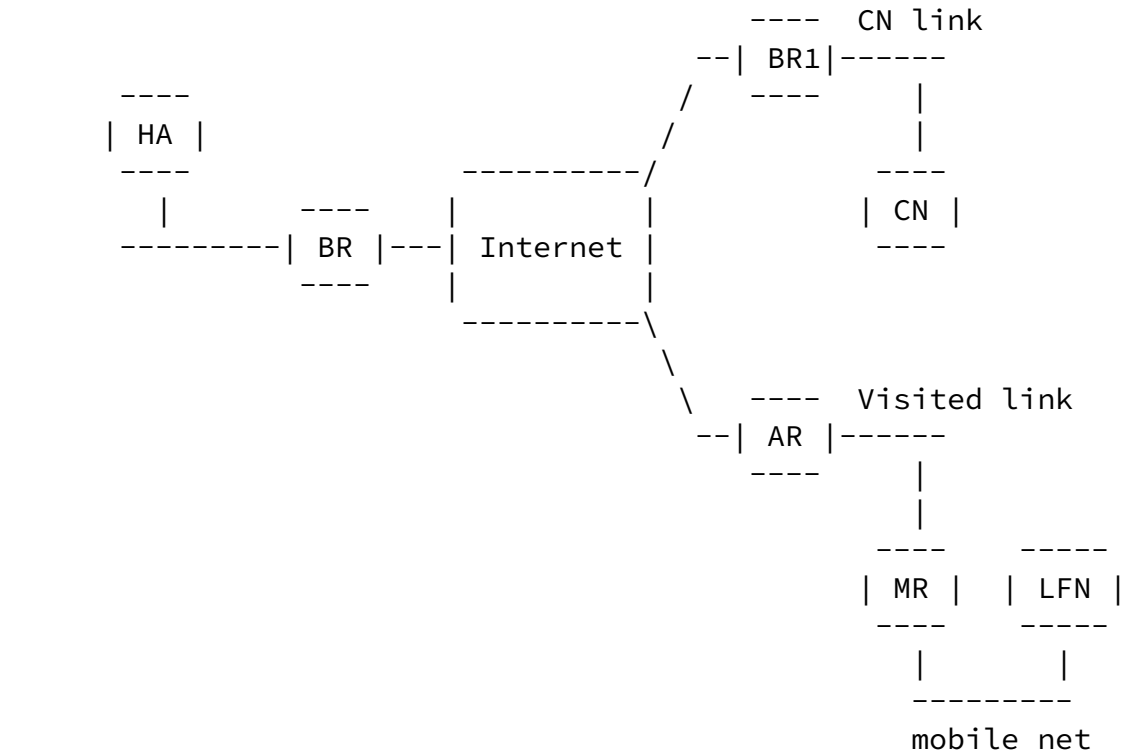
mobile net link

-BR receives packet from CN towards LFN.
-BR scans its routing table to and finds dest through MR.
-BR sends NS for L2 address of MR.
-MR replies NA.
-BR forwards packet to MR.
-MR forwards packet to LFN.





14. CN sends packet to LFN, mobile network visits, HA separated BR

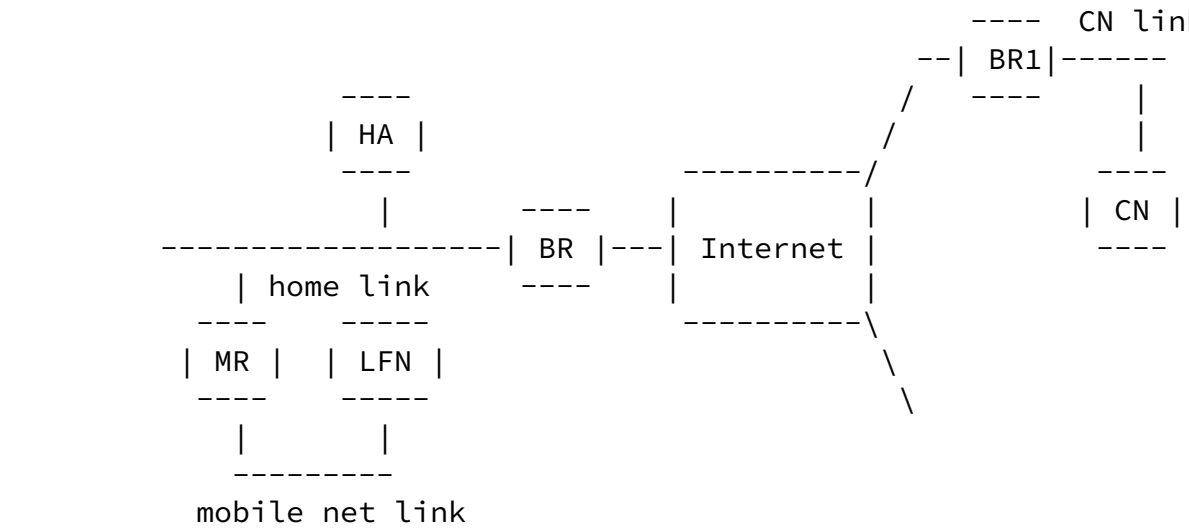


-BR receives packet from CN towards LFN.
-BR scans its routing table to and finds dest through MR.
-BR sends NS for L2 address of MR. HA replies NA on behalf of MR.
-BR sends Redirect to HA informing it about a route towards MR.
-Simultaneously with previous packet, BR forwards packet to HA.
-HA scans its routing table and finds an entry to MR (added as a result to ICMP redirect), it also has a BC entry for MR, so it sends the packet through the MRHA tunnel.

The problem in the above case is how to inform the HA about the route towards MR. When MR at home, and HA being a host, normally

HA doesn't have a route towards MR.

15. LFN sends packet to CN, mobile network home, HA separated BR



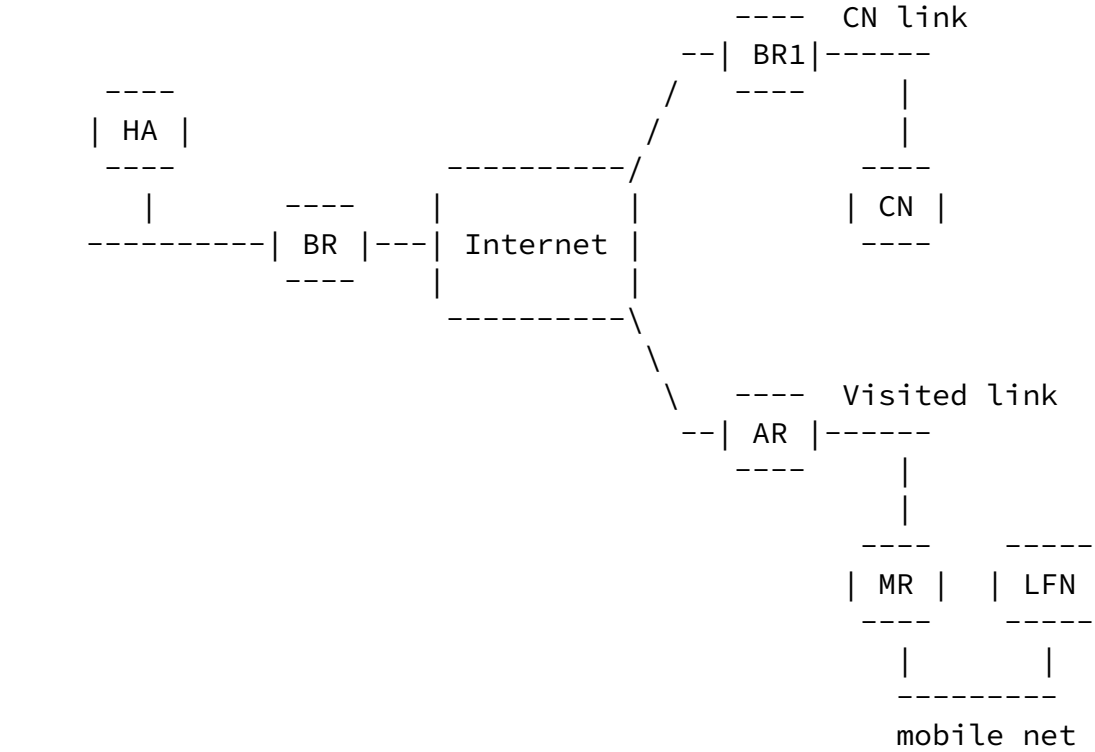

-MR receives packet from LFN towards CN.
-MR scans its routing table and finds dest through BR.
-BR sends packet to CN



---



16. LFN sends packet to CN, mobile network visits, HA separated BR




-MR receives packet from LFN towards CN.

-MR encapsulates this packet through the MRHA tunnel.
-HA receives this packet, decapsulates and sends to CN.

### A.3 MR Redirects to BR

Also, consider the scenario where the FN has a default route towards the MR instead of the BR, and sending packets to a CN on the Internet. This might very well happen when the MR is at home and sending RAs, in addition to the RAs sent by the BR. FN might configure a default route through the MR instead of the BR. If MR is at home, MR will redirect the FN towards the BR. So, even if this looks like a wrong configuration on the FN (its default route should point to BR and not MR), packets will still travel correctly when MR is at home. This should be maintained when the MR is not at home. There are two possibilities: either the HA (replacing the MR) redirects the FN towards the BR, or it is the MR itself that sends the respective ICMP redirect message to the FN (through the MRHA tunnel). The first case supposes that HA maintains a routing table, which contains routes towards the mobile network. This is less desirable if the HA is not co-located with BR, and where we prefer not to have routing interactions with the HA. The latter case is more plausible, keeping the default routing behaviour to the MR.

### A.4 Informing the HA about the Route to MR

In certain scenarios presented previously, with the HA dissociated from the BR and the MR in the visited network, there is a need for the HA to maintain in its routing table an entry towards the MR. A scenario where packets from CN towards LFN are looping between BR and HA has been described in detail in section 3.2.4 of [8]. Several solutions exist to avoid this looping, described below.





#### A.4.1 ICMP Redirect from BR to HA

One alternative for avoiding the loop problem is by using ICMP Redirects [19] sent by BR to HA in order to communicate to HA the route it misses towards the MR. ICMP Redirects are deployed and used in existing networks. The classic behaviour of ICMP Redirects is presented in scenario 1. Scenarios 10 and 14 with MR-not-at-home and BR dissociated from HA, present the fact that classic ICMP Redirects are not triggered normally and thus modifications are needed.

In addition to the normal behaviour with ICMP Redirects, described in [19], it could be modified according to the following. The decision by BR to send ICMP Redirect towards HA can be taken in at least three ways:

- allow a number of iterations of a packet looping between HA and BR and after this fixed number decide to send the Redirect to HA such as the looping stops. This modifies the normal behaviour of BR.

- another possibility is for BR to react at the moment it receives the proxy NA from HA (on behalf of the MR), compare to the current entry it has in the Neighbour Cache for MR, and then decide that, because MR has moved away, send Redirect to HA to inform HA about the route to MR. This is the route (or set of routes) normally maintained by the BR with the MR, doesn't contain any form of the new position (CoA) of the MR. This route, or set of routes (in which case a set of Redirects are sent), is copied from BR's routing table. All routes that have destination the MR's home address need to be communicated to HA with ICMP Redirects. This modifies the normal behaviour of BR.

- yet another possibility is to consider modifications on HA (from vanilla Mobile IPv6), but don't touch BR, such that HA generates a new packet, thus obtaining a classic ICMP Redirect from BR.

  When the HA receives a packet that is not for itself, it encapsulates it with an IP-in-IP tunnel, having the src address its own address and the destination address copied from the dst address of the original packet. Then try to route this packet and find the default route towards BR. Then BR sends a normal ICMP Redirect informing HA there is a better route for this packet towards MR. Thus HA acquires the MR route dynamically. The packet will be passed on by BR to HA again, and further details are needed here. Remark that this is equivalent to one iteration of the loop (a particular case of the fixed iterations loop mentioned previously).

### A.4.2 Static Route Method

This is proposed by [4] and [13], where a route is statically introduced in the HA upon receiption of a Binding Update from MR. This route for MR's prefix may point towards MR's home address (next hop), towards a specific tunnel to MR's home address(output

interface), or towards a specific tunnel to MR's care-of address (output interface).

The first approach proposed in [4] suggests to configure a new static tunnel on the MR's HA towards MR_HoA. This static tunnel, that we call here MR_HoA_tunnel, is to be used as output interface of a new static entry added in the routing table of HA for MR's prefix: MR prefix -> MR_HoA_tunnel. Upon reception of a data packet from CN addressed to a LFN, MR's HA will consult its routing table and find a match for that packet for this static route since LFN address matches MR's prefix. As a results it will encapsulate the packet with an additional header that will have MR's HA as source address and MR_HoA as destination address. In order to forward this packet, now addressed to MR's Home Address, the MR will first consult its binding cache and discover MR's Care-of address. It will thus send the packet through the MRHA tunnel towards MR's current location. It is worth mentionning that this approach introduces a double encapsulation of an incoming packet to be forwarded to the MR: the first is due to the MR_HoA_tunnel, the second to the MRHA tunnel.

The second approach proposed in [13] suggests a similar method but avoids the overhead introduced by the two tunnels. It consists in configuring a static route in MR's HA routing table for MR's prefix towards MR's Home Address: MR prefix -> MR_HoA. Upon reception of a data packet from CN addressed to a LFN, MR's HA will consult its routing table and, again, find a match for that packet for this static route since LFN address matches MR's prefix. This indicates the MR's HA that the packet should be routed towards MR_HoA. From its binding cache it discovers MR's CoA and as a consequence forwards the incoming packet from the CN directly through the MRHA tunnel. This approach reduces the overhead of the MR_HoA_tunnel but requires a suitable coordination of the routing table and binding cache on the HA.

A third possible approach is similar to the previous one but directly uses the MR's care-of address as the tunnel termination point instead of MR's home address. As such the new static entry added in the routing table of HA for MR's prefix is then MR prefix -> MRHA_tunnel.

Analyzed from the perspective where HA is separated from BR, and where MR doesn't normally maintain routes with HA, then this addition might seem superfluous. Consider a situation where MR and BR maintain routing information and where that manual route is added on HA. When the MR is not at home, consider that administrator decides to add a new fixed subnet at home, with its own router neighbouring with BR on the home link. Consider the new subnet's prefix being a longer prefix derived from the prefix assigned to the MR's subnet. This is perfectly feasible by changing configurations on the MR and BR. That can work perfectly

even if MR is not at home. But if HA doesn't participate in this exchange (which is the case if HA separated from BR) then the manual route added previously in the HA is no longer valid. Thus, a potential issue.





Using PSBUs as proposed in [8] and [13] has many side-effects not clearly considered. When the mobile network is assigned several prefixes instead of one, then it is not clear whether several BUs are being sent or only one with several prefixes inside. Remark that in the vanilla Mobile IPv6 case, only one CoA can be sent with a BU (the alternative CoA is only an alternative not a substitute).

### A.4.3 Dynamic Route Method

It is possible for the HA, being either separated or co-located with the BR, to run a specific routing protocol, participating in the routing interactions between BR and all other neighbouring routers on the home link. Thus, the HA always has the necessary route it needs to join the MR's network.

If the HA is a one-interface machine, and separated from the BR, it seems that it maintains information that is not always necessary to its well working as a HA. For example, it will maintain routes to all neighbouring routers, be it fixed or mobile. The routes to the fixed neighbouring routers are not necessary for its working as a host, since it suffices to only have a default route towards a BR, that will normally dynamically Redirect it towards the other fixed routers. Moreover, if HA runs a dynamic routing protocol, its route updates will never be taken into account by other routers, since they will always be one hop further than the routes already known by them. Thus it might be possible to have the HA as a silent routing, only receiving route updates from the neighbouring routers, but never sending route updates, since it does not have a network behind it (it is a "host") whose reachability it needs to advertise.

RIP [11] supports having a silent host that only listens to update messages, but does not advertise new routes. With OSPF [18] the "listening only" requirement is complicated by the fact that the HA would needs to participate in OSPF's HELLO protocol.

The advantage of using this solution is that it does not require additional changes to Mobile IPv6, and PSBUs are not needed. The disadvantage is that if the MR does not run a routing protocol then we still need some way of telling the HA the routes to the MNPs.

## Appendix B: Examples and Other Issues

### B.1 Example of issue for Mobile Router as Mobile Host

If the MR is at home and it has an address configured on the moving interface other than a link-local address, then the MR can act as an MH too, and send normal Mobile IPv6 BUs, binding that Home Address to a newly configured CoA; thus allowing the MR to be an MH for itself only, ignoring the LFNs. If the MR at home doesn't have other addresses than link-local on the mobile interface then the MR can not send normal Mobile IPv6 BUs and can not be an MH. It can however be an MR for the hosts on the mobile network.

### B.2 Multicast Subscriptions of the MR





When the MR is at home, it normally joins certain multicast groups related to routing (e.g. all-routers multicast group with site scope). This is assumed by dynamic routing protocols, or by renumbering mechanisms. When the MR is no longer at home, its multicast subscription should continue as if it were at home. This can be achieved by "home subscription" techniques considered in relation with Mobile IPv6.

### B.3 Examples of issues for Neighbour Discovery for MR

When MR is at home and sends RA towards the home link, it should not advertise itself as being capable of being a default router (Router Lifetime should be 0).

When the MR is visiting, it should not respond to RSs sent on the visited link and it should not send RAs on the visited link.

When the MR is at home, it doesn't normally use any information received from RAs sent by a neighbouring router, i.e. the BR. It has a link-local address and if it has a larger scope address configured on an interface, then that is normally done manually. Actually, routers are usually prohibited from using information received in RAs more than for logging and synchronization purposes. When the MR is in a foreign network, it needs a way to configure a Care-of Address. In the hosts case this is done by stateless or stateful autoconf. In the MR case, the stateful is possible, while the stateless is normally prohibited. A good way for address autococnfiguration for the MR should be identified, be it DHCP, or modified RAs, or modified router's behaviour to accept RAs.

Assume the MR is at home and a non-link-local (site- or global) home address is configured on the interface connecting to the home link (supposedly the same interface that will change CoAs when visiting). The MR-at-home will do periodic NAs for this home address; this behaviour should stop when MR is visiting. This modified behaviour is already taken into consideration by Mobile IPv6 MN. In the particular MR case, most ND operations of MR are delegated to the HA, and such most entries of Neighbour Cache, Destination Cache that are related to the home link will disappear. New entries that are relevant in the foreign network will populate those tables. When coming back home, all ND entries should be replaced back with the entries related to the home network.

Another specific case in point is the default route. As already presented with the router behaviour with respect to RAs, a default route is not normally configured by MR from a received RA. When the MR is in a foreign network, it should have a default route that points to its BR (but through the MRHA tunnel) and another non-tunnelled default route towards the current AR. Moreover, all MR's routing table entries that pointed to BR when the MR was at home, should still continue to point to BR (through the MRHA tunnel). The same is true for all routing table entries of the BR.

## B.4 Router Renumbering





Router Renumbering for IPv6 [7] is a technique where routers of a home network are instructed to change the prefixes they advertise. In the context here, it should be possible for the MR to be re-numbered when it is at home as well as when it is visiting.

The renumbering mechanisms provided by Mobile IPv6 (mobile prefix solicitations and advertisements) are not relevant for changing the prefixes advertised by the MR towards the mobile network; but these mechanisms should still be used for MR when MR is acting as an MH. In order for router renumbering to work for MR when acting as MR, the MR should at least be able to maintain its multicast subscription to all-routers group valid at home.

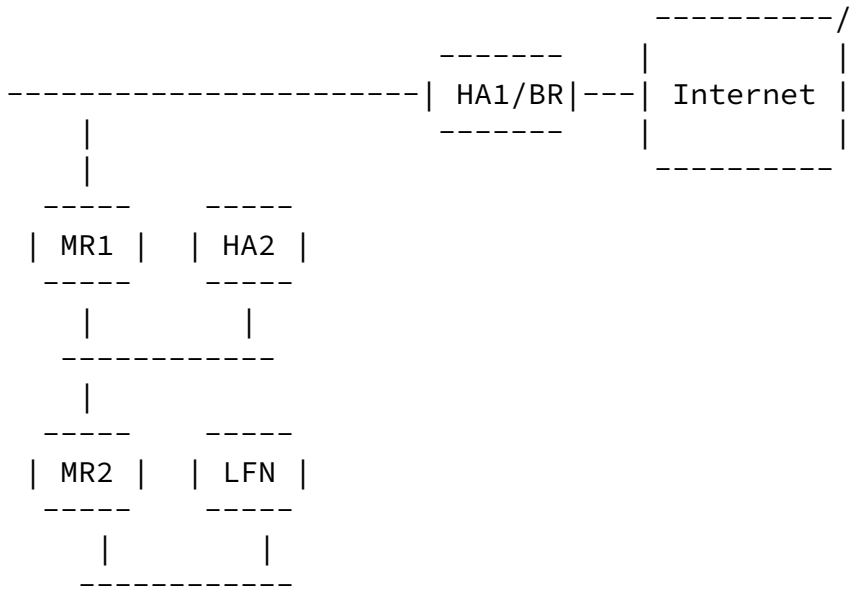
## B.5 Example of disconnected operation issue

An example of an important inconvenient of using exclusively vanilla Mobile IPv6 with MRHA is when nesting: consider two mobile networks, each MR having its own HA in different domains. The

first MR attaches to an AR and the second MR attaches under the first mobile network. In this case, two LFNs situated one on the first net and the second on the second net are capable to communicate with each other, but communication goes through both first MR's HA and through second's. In practice this exposes a paradox where if first MR loses connection to AR, then even if the two nets stay attached, the two LFNs can not communicate.

## B.6 Example for the "cross-over" tunnels issue

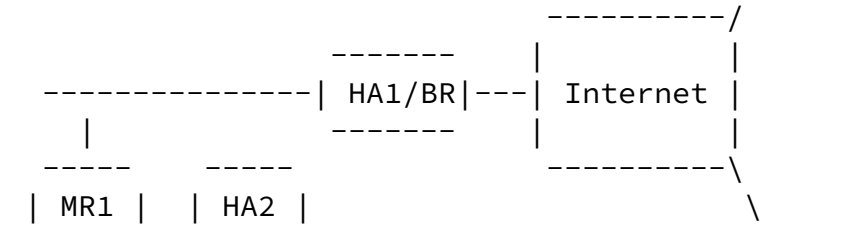
Consider the following example, where both MRs are at home and where MR1's mobile network contains HA2. MR1 belongs to HA1 and MR2 belongs to HA2.



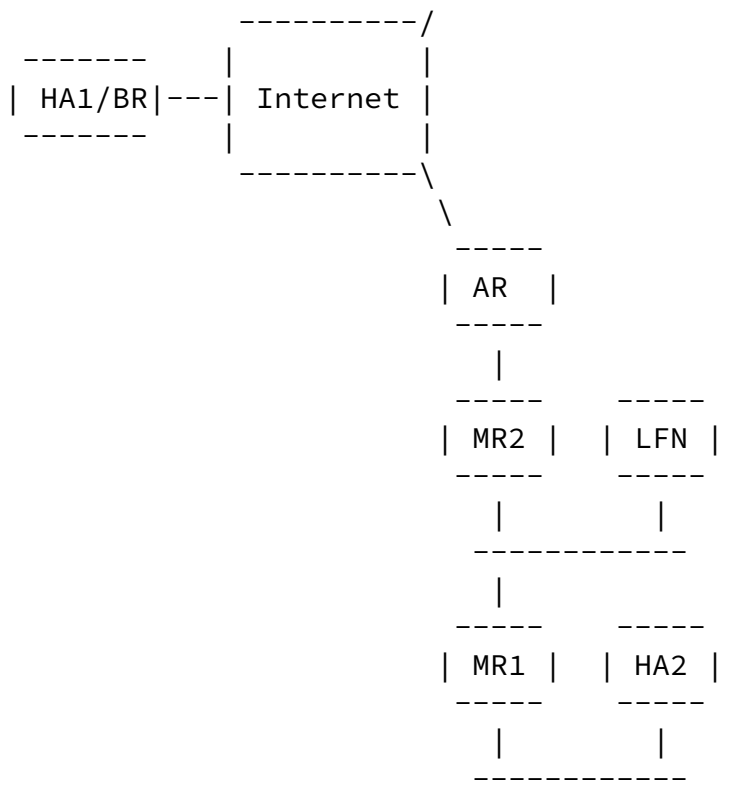

In the next step, consider that the MR2's mobile network goes visit AR, like in the figure below:







The tunnel setup procedure of this movement is between MR2 and HA2. This tunnel can be easily setup; consider now the next movement:



After this movement, MR1 tries to setup its bidirectional tunnel with HA1, by sending a BU to HA1. This BU is encapsulated by MR2 towards HA2. However, HA2 is no longer at home (having moved together with MR1); thus the tunnel between MR1 and HA1 can not be set up, because if it were set up, it would have "crossed over" the tunnel between MR2 and HA2. If one were to draw the two tunnels in the above picture, a tunnel would be between MR2 and HA2 and the other between MR1 and HA1. The path MR1-HA1 includes only the MR2 endpoint of the tunnel MR2-HA2.

## B.7 Example of use of HA ingress filtering

HA should verify that packets it receives from the MRHA tunnel have a source address that matches what's in HA's routing table. HA

should have a route for the mobile prefix pointing into the MRHA tunnel, and the LFN should have use a source address derived from that prefix when sending its packets. Other packets will be dropped.

## Appendix C: A Digression

Two types of approaches have been distinguished in designing a network mobility support with Mobile IPv6 and the bidirectional tunnel.

### Clean-slate Mobile IP-centric approach

In this approach, it is assumed that a home network is in fact a new 1-link network. This home network connects to the Internet with one or more BRs. The BRs have HA functionality with Mobile IP for hosts. There are no other routers or hosts in the home network than the BRs and the MRs. MRs are seldom at home. MRs and BRs would presumably have little need to run a dynamic routing protocol. Most, if not all, routing information exhanges happen with Mobile IP BUs.

Nodes in the mobile networks communicate with CNs. Those CNs are anywhere in the Internet, but not in the home network (there's no node in the home network than BRs and/or other MRs).

### Evolutionary approach

In this type of approach, it is assumed that a home network is already deployed. The home network has several routers that run dynamic routing protocols (non-Mobile IP) to maintain connectivity between various endpoints. The home network is connected to the Internet with one or more BRs.

From this, it is possible to "mobilize" some slices (or chunks of this network), maintaining session continuity and reachability at a permanent home address for fixed nodes of that slice. Consider that the slice that needs to be physically disconnected from the home network uses a router (called "MR") that connects the slice to the home network. A minimal deployment effort could be the following: (1) modify software on MR and (2) place a new box with new software on the link where MR was connecting the slice to the home network (this entity called "HA"). MR and the slice move away and HA stays in place.

## Intellectual Property Rights Considerations

Consult Motorola on IPR (authors believe no IPR here, but depends

who asks; the complete and authoritative answers can be found from IPD or Public Relations of Motorola, corelated with IPD of ECRL).





Chairs' Addresses

Thierry Ernst,
French National Institute for Research in Computer Science and Control
Visiting Researcher at WIDE Project
Jun Murai lab. Faculty of Environmental Information,
Keio University.
5322 Endo, Fujisawa-shi, Kanagawa 252-8520, Japan.
Phone : +81-466-49-1100
Fax : +81-466-49-1395
E-mail: ernst@sfc.wide.ad.jp
Web: http://www.sfc.wide.ad.jp/~ernst/

Timothy J. Kniveton
Communication Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1 650 625-2025
EMail: timothy.kniveton@nokia.com
Fax: +1 650 625-2502

Authors' Addresses

Alexandru Petrescu
Motorola Labs
Espace Technologique de St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69354827
Alexandru.Petrescu@motorola.com

Miguel Catalina-Gallego
Motorola Labs
Espace Technologique de St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69352541
Miguel.Catalina@motorola.com

Christophe Janneteau
Motorola Labs
Espace Technologique de St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69352548
Christophe.Janneteau@motorola.com

Hong-Yon Lach
Motorola Labs
Espace Technologique de St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69352536
Hong-Yon.Lach@motorola.com

Alexis Olivereau
Motorola Labs
Espace Technologique de St Aubin
Gif-sur-Yvette 91193
France
Phone:  +33 1 69352516
Alexis@motorola.com

Internet Society.