Network Working Group
INTERNET-DRAFT
Expires: February 2001

Hesham Soliman, Ericsson
Claude Castellucia, INRIA
Karim El-Malki, Ericsson
Ludovic Bellier, INRIA
September, 2000

Hierarchical MIPv6 mobility management

<draft-soliman-mobileip-hmipv6-01.txt>

Status of this memo

Abstract

This draft introduces some extensions for MIPv6 and neighbour discovery to allow for the introduction of a hierarchical MIPv6 mobility management model. The proposed hierarchical mobility management for MIPv6 will reduce the amount of signalling to CNs and the HA and may also improve the performance of MIPv6 in terms of handoff speed. Moreover, HMIPv6 is well-suited to implement access control and handoffs between different access technologies.

TABLE OF CONTENTS

1. Introduction

This draft introduces the concept of a Hierarchical Mobile IPv6 network, utilizing a new node called the Mobility Anchor Point (MAP).

In Mobile IPv6 there are no Foreign Agents, but there is still the need to provide a central point to assist with MIP handoffs. Similarly to MIPv4, Mobile IPv6 can benefit from reduced mobility signalling with external networks by employing a regional hierarchical structure. For this reason a new Mobile IPv6 node, called the Mobility Anchor Point (MAP), is used and can be located at any level in a hierarchical Mobile IPv6 network including the Access Router (AR). Unlike FAs in IPv4, a MAP is not required on each subnet. Two different options are proposed in this memo for the use of a MAP. A MN may use the MAP as an alternate-care-of address (COA) or form a Regional COA (RCOA) on the MAP's subnet while roaming within a hierarchical (MAP) domain, where such a domain involves all access routers advertising that MAP. The two options are described in detail in chapters 4.1 and 4.2.

The MAP will limit the amount of Mobile IPv6 signalling outside the domain and will support Fast Handoffs to help Mobile Nodes in achieving seamless mobility. Other advantages of the introduction of the MAP functionality are covered in chapter 3.

This draft assumes the generic case of scaleable multi-level Hierarchical Mobile IP (HMIP) networks and is therefore applicable to HMIP networks in general. Hierarchical MIPv6 (HMIPv6)can assist with speeding up MIP Handoffs, hence offering advantages which are especially important for the support of real-time services.

3. Hierarchical Mobility Management using MIPv6

The aim of introducing the hierarchical mobility management model in MIPv6 is to enhance the network performance while minimising the impact on MIPv6 or other IPv6 protocols. This is achieved by using the MIPv6 protocol combined with layer 2 features to manage both IP micro and macro mobility, leading to rationalisation and less complex implementations in the MN and other network nodes. This hierarchical MIPv6 scheme introduces a new function, the Mobility Anchor Point (MAP), and minor extensions to the MN and the Home Agent operations. The CN operation will not be affected.

The introduction of the MAP concept minimises the latency due to handoffs between access routers. Furthermore, the addition of bicasting to a MAP allows for Fast Handoffs [5] which will minimise the packet losses due to handoffs and consequently improve the throughput of best effort services and performance of real time data services over the radio interface. Just like MIPv6, this solution is independent of the underlying access technology, allowing Fast

Handoffs within, or between, different types of access networks. Furthermore, a smooth architectural migration can be achieved from Hierarchical MIPv4 networks, since a dual operation of IPv4 and IPv6 Hierarchies will be possible making use of the similarity in architecture.

The introduction of the MAP concept will further diminish signalling generated by MIPv6 over the radio interface. This is due to the fact that a MN only needs to perform one regional update (MAP) when changing its layer 3 access point within the MAP domain.The advantage can be easily seen when compared to other scenarios (no MAP) where at least two BUs (Binding Updates) will be sent (to one CN and HA). A MAP may also interact with the AAA protocol to perform key distribution during handoffs and eliminate the need for re-authentication as explained in ch 10.

4. Overview of the MIPv6 Hierarchical Mobility Management

In order to introduce hierarchical mobility management in MIPv6, the protocol is extended with a new function. The proposed new functionality is the Mobility Anchor Point (MAP). It simply provides an optional mobility management function that can be located at any level in the hierarchy starting from the access router upwards.

The MAP may be used by a MN as an alternate-COA [1] while roaming within a certain MAP domain. Alternatively, the MN MAY choose to use a Regional Care of Address (RCOA) on the MAP's subnet as its own COA while roaming within a MAP's domain. In the latter case, a MAP acts essentially as a local Home Agent (HA) for the MN. A MAP domain's boundaries are defined by the Access Routers (ARs) advertising the MAP information to the attached Mobile Nodes. The control of a MAP's mode of operation (as an alternate-CoA or a local HA) is left to the network administrator's discretion.

When the MAP is used as an alternate COA, the MAP will receive all packets on behalf of the MN and will encapsulate and forward them directly to the MN's current address. If the MN changes its current address within a regional MAP domain, it needs to register the new address with the MAP. This makes the MN's mobility transparent to the CNs it is communicating with. The MAP can also be used to execute a Fast Handoff between ARs as explained in [5].

The detailed extensions to MIPv6 and operations of the different nodes will be explained later in this document.

Although the proposed method is independent of the network topology, it is best suited to a hierarchical network or one with multi-access technologies. It should be noted that the MAP concept is simply an extension to the MIPv6 protocol. Hence a MAP-aware MN with an implementation of MIPv6 MAY choose to use the MAP or simply use the standard MIPv6 implementation as it sees fit. Furthermore, a MN can at any time stop using the MAP. This provides great flexibility, both from a MN or a network operations point of view.

The network architecture shown below illustrates an example of the use of the MAP in a foreign domain.

```
            _______
           |  HA   |
           |_______|        _______
               \           |  CN   |
                \          |_______|
                 \___          |
                     \         |
                      \    ____|
                      _\___|_
                     |       |
                     |  MAP  |
                     |_______|
                       /  \
                      /    \
                     /      \
                    /        \
               ____/____      \_________
              |         |     |         |
              | AR1/MAP |     | AR2/MAP |
              |_________|     |_________|
                    |              |
                    |              |
                  __\/____         \/
                 |        |
                 |   MN   |
                 |________|
                     __________________\
                            Movement   /
```

Figure 1: Hierarchical MIPv6 domain

In Figure 1, the MAP can help in providing seamless mobility for the MN as it moves from Access Router 1 (AR1) to Access Router 2 (AR2), while communicating with the CN. It is possible to use multi-level hierarchies of routers and implement MAP functionality in AR1 and AR2 if needed. It should be noted that AR1 and AR2 could be two points of attachment in the same RAN (Radio Access Network) or in different RANs.

Upon arrival in a foreign domain, the MN will discover the global address of the MAP. This address is stored in the Access Routers and communicated to the MN via Router Advertisements. The discovery phase will also inform the MN of the distance of the MAP from the MN.

For example, the MAP could also be implemented in AR1 and AR2, in which case the MN can choose the first hop MAP, second hop MAP, or both.

A Router advertisement extension is proposed later in this document for MAP discovery. Other service discovery methods may also be used for the same purpose. If a router advertisement is used for MAP discovery, as described in this document, all ARs belonging to the MAP domain MUST advertise the MAP's IP address. The same concept should be used if other methods of MAP discovery are introduced. The MAP option in the router advertisement should inform the MN about the chosen mode of operation for the MAP.

The process of MAP discovery continues as the MN moves from one subnet to the next. As the MN roams within a MAP's domain, the same information announcing the MAP should be received. If a change in the advertised MAP's address is received, the MN should act on the change by sending the necessary Binding Updates to its HA and CNs.

If the MN is not MAP-aware then the discovery phase will fail resulting in the MN using the MIPv6 [1] protocol for its mobility management. On the other hand, if the MN is MAP-aware it MAY choose to use the MAP implementation. If so, the MN will first need to register with a MAP by sending it a BU containing its Home Address and current address. In the case where the MN uses the MAP as an alternate-COA, the Home address used in the BU is the MNs Home Address on its home subnet. On the other hand, if the MN is using a RCOA, the Home address used in the BU is the RCOA. The MAP MUST store this information in its Binding Cache to be able to forward packets to their final destination when received from the different CNs or HAs.

The MN will always need to know the original sender of any received packets. Since all packets will be tunnelled by the MAP, the MN is not always able to determine whether the packets were originally tunnelled from the Home Agent or received directly from a CN. This knowledge is needed by the MN to decide whether a BU needs to be sent to a CN in order to initiate route optimisation. For this purpose a check needs to be performed on the internal packet's routing header to find out whether the packet was tunnelled by the HA or originated from a CN using route optimisation instead. If a routing header exists in the internal packet, containng its alternate-COA (MAP address or RCOA) and the MN's Home Address as the final destination, then route optimisation was used. Otherwise, triangular routing through the HA was used.

To use the network bandwidth in a more efficient manner, a MN may decide to register with more than one MAP simultaneously and use each

MAP address for a specific group of CNs. For example, in Fig 1, if the CN happens to exist on the same link as the MN, it would be more efficient to use the first hop MAP (in this case assume it is AR1) for communication between them. This will avoid sending all packets via the "highest" MAP in the hierarchy and hence result in a more efficient usage of network bandwidth. The MN can use its current address as a COA as well.

4.1 Using a MAP's address as a COA

Using a MAP as an alternate-COA may be a useful tool for some mobility scenarios. In the case where a MN is also a router to which several MN's may be connected (eg. a Personal Area Network), it would not be possible for such router to obtain a new network prefix within a visited network. Hence, MNs connected to such router will end up with topologically incorrect addresses. By having the mobile router act as a MAP within the visited network, MNs connected to it may use it as an alternate-COA when registering with their HA and other CNs. Hence, maintaining the IPv6 powerful aggregation of routes witihn the backbone.

In this case the MAP option will be advertised by the AR that the MN is connected to. The MN SHOULD send a BU to the HA and CNs including the MAP's address as an alternate-COA. Hence all packets addressed to the MN will be sent through the MAP's address as specified by the MN in its BU. The MAP will (acting like a HA) tunnel the packets addressed to the MN to its current address. The details of the MAP operation will be given later in this document.

The Home Address contained in the MAP registration MUST be the same Home Address sent in the Home Agent registration. If a MN sends different BU's for different Home Addresses (in the case it has multiple Home Addresses), the same process MUST be performed for the MAP registrations. This is essential to allow a MAP to forward packets to the right COA when they are tunnelled from the HA. The MN SHOULD also have a prefix length of 128 in its BUs to the HA. This would stop the HA from being proxy for other unregistered Home addresses.

The MAP will need to know how the final destination in the packet corresponds to the registered address of a MN. This should be obvious when the packets are sent from a CN to the global Home Address of the MN or to the COA with a routing header. However, if the HA tunnels packets with addresses other than the MN's Home Address (eg. Site-local), of which the MAP would have no knowledge, the HA MUST add a routing header to the outer packet. This routing header must use one of the MN's registered Home Addresses as the final destination. This will enable the MAP to tunnel the packet to the correct destination (i.e. the MN's current address).

4.2 Using a Regional COA (RCOA) on a MAP's subnet

In this scenario, the MN would have two addresses, a RCOA on the MAP's subnet and an on-link COA (LCOA). This RCOA is formed in a stateless manner by combining the MAP's subnet prefix received in the MAP option with the MNs interface identifier.

After forming the RCOA, the MN sends a BU to the MAP. The BU will bind the RCOA (similar to a Home Address) to its LCOA. The BU MUST have both the A and D flags set. The MAP (acting as a HA) will then perform DAD for the MN's RCOA on its subnet. If successful, the MAP will return a Binding Acknowlegement (BAck) to the MN indicating a successful registration. Otherwise, the MAP MUST return a BAck with the appropriate fault code. No new error codes are needed for this operation.

The MAP will receive packets addressed to the MN's RCOA (from the HA or CNs). Packets will be tunnelled from the MAP to the MN's LCOA. The MN will decapsulate the packets and process the packet in the normal manner.

5. Neighbour Discovery extension - Dynamic MAP discovery

The process of MAP discovery can be performed in many different ways. In this document, router advertisements are used for the discovery phase by introducing a new option. The access router is required to send the MAP option in all router advertisements. This option includes the distance from the MN in terms of number of hops, the preference for this particular MAP and the MAP's global IP address. The ARs can be configured manually or automatically with this information. In the case of automatic configuration, each MAP in the network needs to be configured with a default preference, the right interfaces to send this option on and, if necessary, the IP address to be sent. The initial value of the "Distance" field MUST be set to a value of one. Upon reception of a router advertisement with the MAP option, given that a router is configured to resend this option on certain interfaces, the router MUST copy the option and resend it after incrementing the Distance field by one. If the router was also a MAP, it SHOULD send its own option in the same advertisement. In this manner information about a MAP at a certain level in a hierarchy can be dynamically passed to a MN. Furthermore, by performing the discovery phase in this way, different MAP nodes are able to change their preferences dynamically based on the local policies, node overload or other load sharing protocols being used.

The following figure illustrates the new MAP option.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     Type      |    Length     |  Distance     |  Pref         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     Plen      |R|M|             Reserved                      |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         Valid Lifetime                        |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                                                               |
      +                                                               +
      |                                                               |
      +           Prefix / Global IP Address for MAP                  +
      |                                                               |
      +                                                               +
      |                                                               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The alignment requirements for this option is 8n.

Fields:

Type — Message type. To be assigned.

Length — 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value 0 is invalid. Nodes MUST silently discard an ND packet that contains an option with length zero.

Distance — An 8 bit unsigned integer showing the distance from the receiver of the advertisement. It MUST be set to one in the initial Advertisement, if dynamic MAP discovery is used.

Pref — The preference of this MAP. An 8 bit unsigned integer. A value of 255 means lowest preference.

Plen — The prefix length in this option. A prefix length value of 128 indicates that the MAP option contians the MAP's IP address.

R — Indicates that the MN MUST form a RCOA

M — Indicates that the MN MUST use the MAP's Own IP address as an alternate-COA

Global Address — One of the MAP's global addresses.

To ensure a secure communication between routers, router advertisements containing the MAP option SHOULD be authenticated by AH. In the case where this authentication is not possible, a network operator may prefer to manually configure all the ARs to send the MAP option.

6. MIPV6 extensions - Sending Binding Updates

This section outlines the extensions proposed to the BU option used by the MN in MIPv6. A new flag is added: the M flag that indicates MAP registration. When a MN registers with the MAP, the M flag MUST be set to distinguish this registration from a Home Registration or a BU being sent to a CN.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                    |  Option Type  | Option Length |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |A|H|R|D|M| Res | Prefix Length |        Sequence Number        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                            Lifetime                           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Sub-Options...
    +-+-+-+-+-+-+-+-+-+-+-+-+-
```

Description of extensions to the BU option:

M   If set indicates a MAP registration.

Res   3 bit reserved field

7. MN OPERATION

This section is concerned with the extensions to the MN's operation in a foreign network due to the introduction of the MAP. Unless otherwise specified, the normal MN operation in [1] applies.

7.1 MAP discovery

When a MAP-aware MN receives a router advertisement, it should search for the MAP option. One or more options may be found for different IP addresses or subnet prefixes.

A MN SHOULD register with the MAP having the lowest preference value. A MAP with a preference value of 255 SHOULD not be used in the MAP registration. A MN MAY however choose to register with one MAP rather than another depending on the value received in the Distance field, as long as the preference value is below 255.

A MN SHOULD store the received option(s) and choose at least one MAP to register with. Storing the options is essential as they will be compared to other options received later for the purpose of the move detection algorithm.

If no MAP options are found in the router advertisement, the MN MUST use the MIPv6 protocol as specified in [1]. If the MN receives a duplicated MAP option (having the same IP address or prefix) with different preference values or Distance values, the MAP IP address SHOULD not be used as an Alternate-COA in any BU's sent by the MN.

Finally if the M flag is set in the MAP option, the MN MUST register with the MAP and inform its HA.

A MN MAY choose to register with more than one MAP simultaneously or use both MAP address and its own address as COAs simultaneously with different CNs.

7.2 Registration with the MAP - Sending Binding Updates

After MAP discovery has taken place, a MN can register with one or more MAPs. The MN performs this regional registration by sending a BU to the MAP with the appropriate flags set. The contents of the BU will depend on the MAP's mode of operation.
When registering with a MAP, the A flag SHOULD be set and the M flag MUST be set in the BU. The H flag MUST not be set when registering with a MAP. A MN SHOULD wait for a BAck (Binding Acknowledgement) from the MAP before using the MAP address or a RCOA from the MAP's subnet as an alternate COA in its BUs.

After successfully performing registration with a MAP, a MN can start sending BUs, with it's Alternate-COA,to CNs and its HA. The MAP's IP address or RCOA MUST be included in the Alternate-COA sub-option.

If the MN uses a MAP's address as an alternate-COA, then for each home address registration sent to the HA with a MAP's address as the COA, a BU MUST be sent to the same MAP using the same home address.

The MN SHOULD send a separate home registration BU for each home address, with the prefix length value set to 128. This stops the HA from forming home addresses for that MN on each link that the HA is connected to, thus ensuring consistency in the Binding Caches of both the MAP and HA for the MN.

7.3 Receiving packets in a foreign network

When in a foreign network, a MN needs to know which path a packet has taken from the CN to the MN. That is, whether triangular routing was used via the HA or route optimisation was used. When using HMIPv6, all packets received from a CN will be tunnelled by the MAP to the MN.

When using the MAP's address as a COA, packets tunnelled by the HA to the MAP will be decapsulated and then encapsulated again with the MAP's address as the source address.

Therefore a check on whether the packet was tunnelled by the HA will not be sufficient to decide whether route optimisation is required.

Hence, a generic check for the existence of a routing header in the encapsulated packet (i.e. with CN as source address), where the MN's home address is the final address, will be sufficient to determine whether the path was route optimised or not.
If the routing header does not exist, the MN SHOULD send a BU with the appropriate information to initiate route optimisation.
It should be noted that such check is generic and would work for all the various use cases of MIPv6 including the different MAP modes of operation in this memo.

8. MAP Operation

8.1 MAP Discovery

As mentioned previously, the MAP discovery is done via router advertisements having the new MAP option added. A MAP will be configured to send its option or relay other MAPs' options on certain interfaces. The choice of interfaces is done by the network operator and depends on the network architecture. A default preference value should be assigned to each MAP. It should be noted that a MAP can change its preference value at any time due to various reasons (e.g. node overload or load sharing). A preference value of 255 means that the MAP SHOULD not be chosen by a MN. This value could be reached in cases of node overload or node failures.

The MAP option is propagated down the hierarchy. Each router along the path to the access router will increment the Distance field. If a router that is also a MAP receives advertisements from other MAPs, it SHOULD add its own MAP option and propagate both options to the next level in the hierarchy.

8.2 Receiving and forwarding Packets for a MN

The MAP operation is in many ways similar to the HA operation described in [1] with some modifications. Upon reception of a BU from a MN with the M flag set, and provided it is allowed to accept this message (i.e. no local policy restrictions) the MAP MUST process the BU and if successful, add the information to its Binding Cache.

The MAP will need to determine how it should act based on the information given in the BU. Two different modes of operation are described below.

8.2.1 Using a MAP's address as a COA

In this scenario, the BU from the MN will contain its LCOA as a source address and its Home address. A MAP MUST first check if the MN is authorised to use the MAP in this mode. If so, the MAP SHOULD process the BU in the normal manner.

If the A flag was set, the MAP MUST send a BAck to the MN.

All packets directed to the MN will be received by the MAP and tunnelled to the MN. Upon reception of an encapsulated packet with no routing header in the outer packet, the packet is decapsulated in the normal way. If the inside packet contains a destination address that doesn't belong to the MAP, the MAP should check its Binding Cache to see if the address belongs to any of its registered MN's. If it does, the packet MUST be tunnelled to the MN's current address. Otherwise, the packet is processed in the normal way.

If the encapsulated packet contains a routing header in the outer packet containing the MN's home address as the next destination, the MAP MUST process the routing header in the normal way, then tunnel the packet to the MN's current address.

8.2.2 Using a RCOA on the MAP's subnet

In this scenario, a MAP would have no knowledge of the MN's Home address. The MN will send a BU to the MAP with the M, A and D flags set. The aim of this BU is to inform the MAP that the MN has formed a RCOA (contained in the BU as a Home address) and request that a MAP performs DAD on its behalf. This is identical to the HA operation in [1]. If the operation was successful, the MAP MUST respond with a BAck to the MN indicating a successful operation. Otherwise a BAck is sent with the appropriate error code. No new error codes are introduced for HMIPv6.

8.3 The MAP as a Mobile Router (MR)

In the case where a Mobile Router (MR) is located in a foreign network, the MR will not be able to obtain a new network prefix for the MNs attached to it. Hence, the MR MUST act as a MAP and advertise the MAP option to the MNs attached to it. The MAP option MUST have the M flag set to ensure that the MNs register with it. This will allow the MNs to be reachable without advertising host specific routes to other routers within the network. This approach maintains IPv6 route aggregation and ensures that no additional routing table entries are required due to the MR's network mobility.

9. HA Operation

The Home Agent operations are affected in a minor way by the introduction of the MAP. The only impact due to HMIPv6 on the HA implementation is that when tunnelling packets to the MN with destination addresses other than the addresses registered by the MN in its Home Registration, the HA MUST include a routing header in the outer packet with the MN's registered home address as the final destination. This is done to enable the MAP to find the right routing entry for the MN, since it has no knowledge of a non-unicast global home address for the MN.

10. AAA Considerations for IPv6

The MAP can be utilised to perform access control on MNs and may interact with the protocol which will be defined for AAA in IPv6. The MAP can speed up a handoff by having the MN's security credentials which will allow it to verify whether a certain node is allowed access to the network. This allows greater efficiency in distributing keys only to certain nodes in the network.

One example of the interaction between a MAP and the AAA infrastructure can be seen when considering the handoff scenario. A MAP can store the MN's security credentials after the MN is allowed network access by the AAA infrastructure. During an intra-domain handoff, the MAP could pass the MN's secrity credentials to the "new" AR to avoid performing the AAA process. These credentials depend on the access enforcement policies in AAAv6 and will not be covered by this draft.

11. Acknowledgements

The authors would like to thank Conny Larsson (Ericsson) and Mattias Pettersson (Ericsson) for their valuable input to this draft.
In addition, the authors would like to thank the following members of the working group in alphabetical order: Eva Gustaffson (Ericsson), Dave Johnson (Rice University), Annika Jonsson (Ericsson), Fergal Ladley (Ericsson) and Erik Nordmark (Sun) for their comments on the draft.

12. Notice Regarding Intellectual Property Rights

Ericsson may seek patent or other intellectual property protection for some or all of the technologies disclosed in this document. If any standards arising from this disclosure are or become protected by one or more patents assigned to Ericsson, Ericsson intends to disclose those patents and license them on reasonable and non-discriminatory terms. Future revisions of this draft may contain additional information regarding specific intellectual property protection sought or received.

13. References

[1] D. Johnson and C. Perkins, "Mobility Support in IPv6",

draft-ietf-mobileip-ipv6-12.txt, February 2000.

[2] E. Gustafsson, A. Jonsson and C. Perkins, " Mobile IP Regional Tunnel Management ", draft-ietf-mobileip-reg-tunnel-02.txt (work in progress), March 2000.

[3] C. Perkins, Editor. "IP Mobility Support", RFC 2002, October 1996.

[4] K. El Malki and H. Soliman " Fast Handoffs in Mobile IPv4". (work in progress)

[5] K. El Malki and H. Soliman " Fast Handoffs in Mobile IPv6". draft-elmalki-handoffsv6-00.txt (work in progress)

14. Appendix A: Planned additions to future revisions

In addition to the existing proposal, the following sections are planned for future revisions:

- MAP discovery. Other ways for dynamic MAP discovery are being investigated. The reuse of Router renumbering has been suggested and if suited, it may be included in the next revision.

- quick discovery of MAP failures will be essential for the reliability of this mechanism. Some suggestions for handling these scenarios will be included in future revisions.

- Detailed notes for implementors will also be added.

15. Authors' Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nokia Corporation
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972-894-6709
EMail: Raj.Patil@nokia.com
Fax : +1 972-894-5349

Phil Roberts
Motorola M/S M8-540
1501 West Shure Drive
Arlington Heights, IL 60004
USA

Phone: +1 847-632-3148
EMail: QA3445@email.mot.com

Questions about this memo can also be directed to:

Hesham Soliman
Ericsson Australia
61 Rigall St., Broadmeadows

Melbourne, Victoria 3047
AUSTRALIA

Phone: +61 3 93012049
Fax: +61 3 93014280
E-mail: Hesham.Soliman@ericsson.com.au

Claude Castelluccia
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
France

email: claude.castelluccia@inria.fr
phone: +33 4 76 61 52 15
fax: +33 4 76 61 52 52

Karim El Malki
Ericsson Radio Systems AB
Access Networks Research
SE-164 80 Stockholm
SWEDEN

Phone: +46 8 7573561
Fax: +46 8 7575720
E-mail: Karim.El-Malki@era.ericsson.se

Ludovic Bellier
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
France

email: ludovic.bellier@inria.fr
phone: +33 4 76 61 52 15
fax: +33 4 76 61 52 52