

**Mobile Networks Support in Mobile IPv6
(Prefix Scope Binding Updates)**

[draft-ernst-mobileip-v6-network-03.txt](#)

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This draft addresses the problems of routing datagrams to nodes located behind the mobile router (MR) that connects a mobile network (MONET) to the Internet, in IPv6. Mobile IPv6 [[MIPv6](#)], the solution to support host mobility, is unable to support an entire network that changes its point of attachment. We show, by means of an experiment, that the Home Agent fails in redirecting packets to nodes behind the MR, and that direct routing can not be performed either. It is thus provided Mobile IPv6 extensions to support simple cases of MONETs. A Prefix Scope Binding Update is an enhanced Mobile IPv6 Binding Update which associates a careof-address (CoA) with a prefix instead of a single address.

Table of Contents

Status of This Memo

Abstract

1. Introduction

2. Terminology and Assumptions

2.1. Terminology

2.3. Assumptions

3. Why can't Mobile IPv6 support MONETs ?

3.1. Review of Mobile IP and MONETs

3.2. Experimentation

3.2.1. Test Bed

3.2.1. Registration with the Home Agent

3.2.2. First experiment: Communication between CN and MR

3.2.3. Second experiment: Communication between CN and LFN1

3.3. Conclusion

4. Mobile IPv6 Extensions to Support MONETs

4.1. Packet format of the Binding Update

4.1.1. New Binding Update Option format

4.1.2. MONET Prefix Sub-Option

4.2. Cache Management

4.2.1. Binding Cache Entries

4.2.2. Searching the Binding Cache Entries

4.3. Extended Mobile IPv6 protocol Operation

4.3.1. Correspondent Node Operation

4.3.2. Home Agent Operation

4.3.3. MR Operation

5. Security Issues

5.1. Authentication

5.2. Authorization

5.3. Prefix Ownership

6. Changes since last draft

Acknowledgments

References

Author's Addresses

1. Introduction

The purpose of traditional mobility support is to provide continuous Internet connectivity to mobile hosts (host mobility support). In contrast, network mobility support is concerned with situations where an entire network (composed by one or more subnets) dynamically changes its point of attachment to the Internet and thus its reachability in the topology. We shall refer to such a network as a mobile network (MONET). Cases of MONETs include networks attached to people (PANs) and networks of sensors deployed in aircrafts, ships, trains, busses, cars, etc. Potential scenarios are exhibited in [\[TERMINOLOGY\]](#) and [\[SCOPE\]](#).

Mobile IPv4 [\[MIPv4\]](#) and Mobile IPv6 [\[MIPv6\]](#) are solutions for host mobility support in IPv4 and IPv6 [\[IPv6\]](#) respectively. Although it is claimed that Mobile IPv4 could support MONETs equally as single mobile nodes ([\[MIPv4\] section 4.5](#), [\[Perkins98\] section 5.12](#), [\[Solomon98\] section 11.2](#)), we argue that this is not true for Mobile IPv6. Indeed, we have carefully studied Mobile IPv6's ability for supporting MONETs, and we came to the conclusion that some modifications are needed to support them. As we show, the Home Agent (HA) fails in redirecting packets intended to nodes behind the mobile router (MR) which connects the MONET to the Internet. As a result from this, communication cannot be established between nodes behind the MR and nodes in the Internet.

Some implementations that do not strictly follows [\[MIPv6\]](#) may interpret it in a way that would allow the HA to redirect packets to nodes behind the MR, but we advocate that is surely leading to misinterpretation and pitfalls. Thus, we advocate that MONETs should be taken into account explicitly. We also advocate that nodes behind the MR MUST NOT take part in the MONET's mobility management as a result of the MR changing its point of attachment.

We therefore propose to extend Mobile IPv6 with "Prefix Scope Binding Updates" as a means to provide continuous Internet connectivity for both the MR and nodes behind it, in a simple, easy, optimal and transparent way. It is assumed that all nodes in the MONET share a common prefix (MONET Prefix) and that the careof-address (CoA) belongs to the MR. A Prefix Scope Binding Update is an enhanced Binding Update that associates a CoA to a prefix instead of a single address. A node receiving such a Prefix Scope Binding Update is able to route any packet that shows this prefix in the destination field via the MR's CoA, therefore insuring permanent Internet connectivity and direct routing to all nodes in the MONET.

In order to keep things simple, this draft does not address specific issues related with nested mobility, and multi-homing. We only

consider LFNs (Local Fixed Nodes) behind the MR.

This document assumes the reader is familiar with the terminology defined in [TERMINOLOGY] and [MIPv6], while reading [SCOPE, REQUI-1, REQUI-2, REQUI-3] is recommended. More information may be found on the MONET web page and mailing list [WEB-MONET]. The material presented in this document is mostly taken from [Ernst01].

2. Terminology and Assumptions

2.1. Terminology

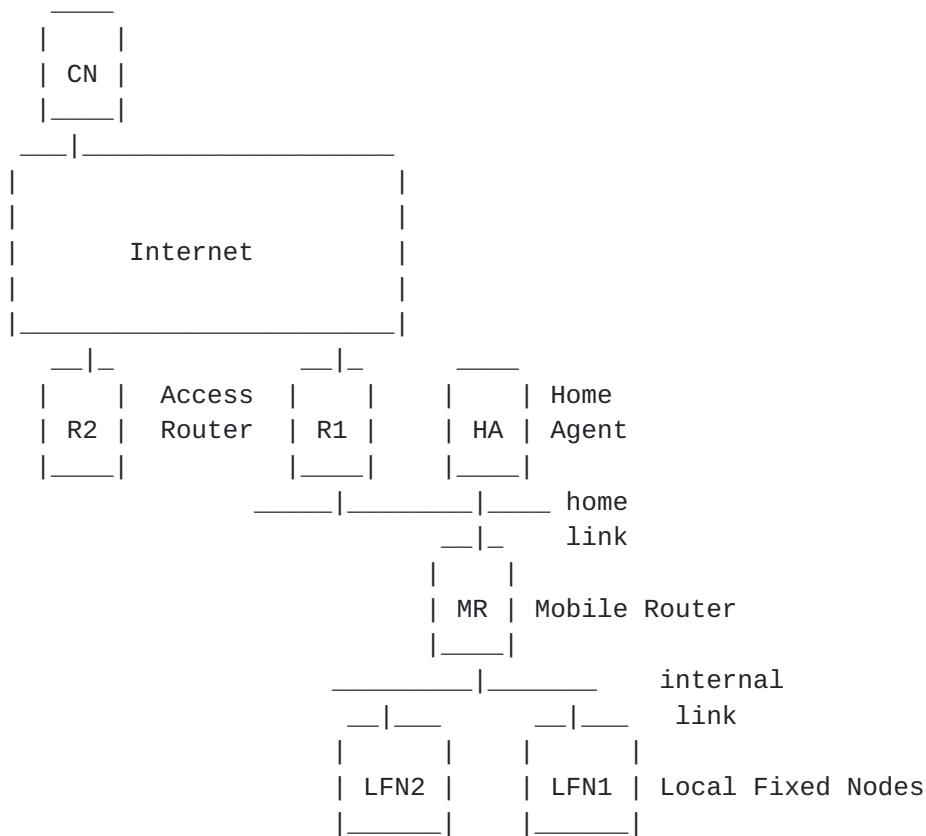


Figure 1: MONET attached to its home link

The following terms are as defined in [MIPv6]:

- o Home Agent (HA)
- o home address
- o careof-address (CoA)
- o Mobile Node (MN)

- o home link
- o foreign link

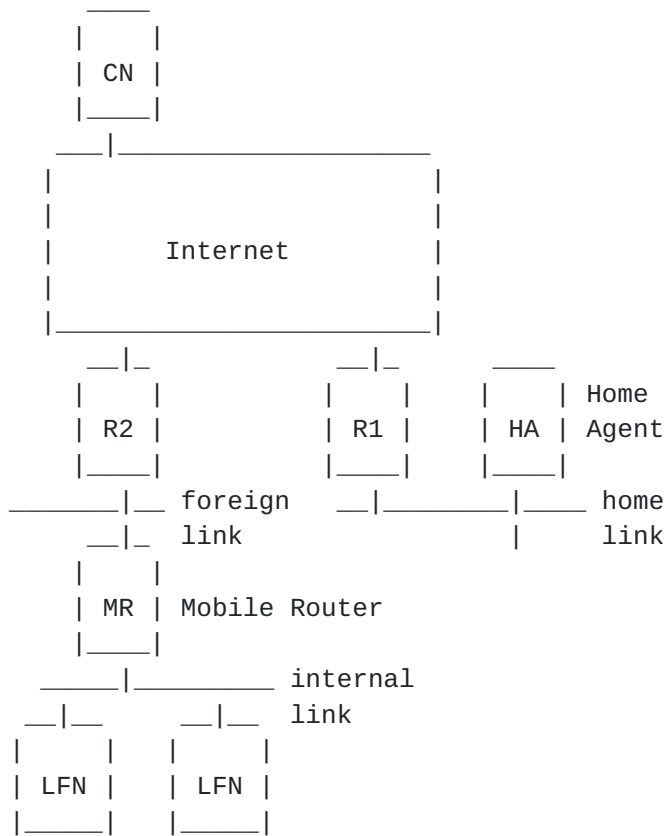


Figure 2: MONET attached to a foreign link

The following terms peculiar to MONETs are defined in [[TERMINOLOGY](#)]:

- o MONET (mobile network)
- o MR (mobile router)
- o Node behind MR
- o LFN (Local Fixed Node)
- o LMN (Local Mobile Node)
- o VMN (Visiting Mobile Node)
- o Mobile Network Prefix
- o ingress interface

- o egress interface

Figure 1 illustrates a MONET attached to its home link. In figure 2, the MONET moves and MR attaches to a foreign link. Figure 3 illustrates a larger MONET.

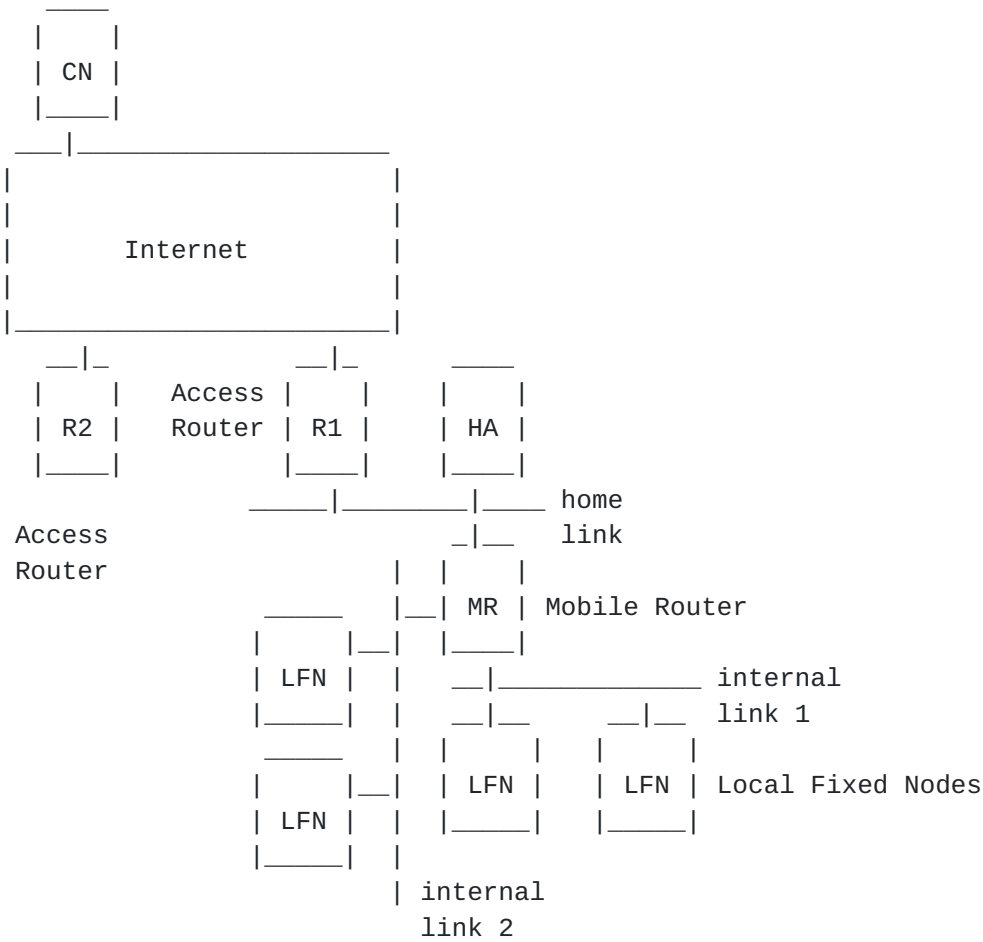


Figure 3: Larger MONET with 2 subnets

2.2. Assumptions

In order to keep things as simple as possible, we make the following assumptions and observations:

- o No Multi-homing: the MONET attaches to the Internet through only one MR, and the MR has only one egress interface.
- o MONET Prefix: network prefix common to all IP addresses in the MONET when the MR is attached to the home link. For a MONET containing only one subnet, the MONET Prefix is the prefix of this

subnet. Note that the MONET Prefix is NOT the home subnet prefix (i.e. the IP subnet prefix corresponding to the mobile router's home address, as defined in [MIPv6]). We do not either make any assumption on the number of bits common to the MONET Prefix and the home subnet prefix. The MONET Prefix may be a sub-prefix of the home subnet prefix. If, for example, the latter is a /60, the MONET Prefix must be larger than /60, and the first 60 bits of both prefixes are identical. Alternatively, they could also diverge from a smaller number of bits. For instance, an organization may decide to split the SLA field of the IPv6 address in several sub-fields (SLA1, SLA2). In this case, the MONET may be identified by a unique SLA1, and the home subnet prefix by another one. If the length of the SLA1 field is 8 bits, the length of the MONET Prefix is 60 bits and the MONET could contain up to 2^4 subnets.

- o MR's egress interface is configured with the Home Subnet Prefix
- o MR's ingress interface is configured with the MONET Prefix.
- o All LFNs in the MONET are configured with the MONET Prefix.
- o Nodes behind the MR are only LFNs (Local Fixed Nodes). We therefore do not consider specific issues related with LMNs (Local Mobile Nodes) nor VMNs (Visiting Mobile Nodes).

Although we have put these assumptions in order to restrict ourselves to the most common and easiest instances of MONETs, our solution may not necessarily be limited to these. We simply do not address the specific issues related to more complex MONETs like those comprising VMNs and LMNs. This should be investigated later. We note that Hierarchical Mobile IPv6 Extended Mode [HMIPv6] proposes to handle VMNs, but it may need additional features such as the ones proposed in this draft.

3. Why can't Mobile IPv6 support MONETs ?

In this section, we first review how the Mobile IP specifications deal with MONETs. We then show the results of an experimentation we have conducted to outline Mobile IPv6's inability to support MONETs. Then we discuss why the existing Mobile IPv6 specification is unable to support MONETs if the MR performs Mobile IPv6.

3.1. Review of Mobile IP and MONET support

Mobile IPv4 proposes to support MONETs as standard mobile nodes (see [MIPv4] [section 4.5](#), [Perkins98] [section 5.12](#), [Solomon98] [section 11.2](#)). In this situation, the mobile node is the MR connecting the

MONET to the fixed Internet. It has a permanent home address on its home link and gets a new CoA at each subsequent foreign link. As any mobile node, MR sends a Binding Update to its home agent HA to instruct it to intercept and tunnel packets via the CoA. The HA is therefore able to intercept packets intended to the home address of MR.

In order to intercept packets intended to LFNs, Mobile IPv4 suggests either of the following two solutions:

- o the HA may be configured with a permanent registration for each LFN which indicates MR's address as the LFN's CoA.
- o the MR may advertise connectivity to the entire MONET using normal IP routing protocols.

Mobile IPv6 [[MIPv6](#)] and Mobile IPv4 with Routing Optimization [[MIPv4-RO](#)] could in principle support MONETs similarly as in Mobile IPv4. However, although mentioned in [[MIPv4](#)], the current specifications [[MIPv4-RO](#)] and [[MIPv6](#)] don't mention them anymore.

3.2. Experimentation

The following sections describe an experimentation conducted to highlight shortcomings of the current Mobile IPv6 specification for supporting MONETs. It shows [[MIPv6](#)] does not allow to route a packet from the fixed Internet to a LFN behind the MR. This experimentation has been conducted on our IPv6 test bed using Francis Dupont "INRIA" IPv6 implementation under FreeBSD.

3.2.1. Test Bed

As this is illustrated on figure 5, MR has two interfaces. At home, the egress interface is attached to the home link (3ffe:306:1130:100::/64) and is configured with the home address (3ffe:306:1130:100::eui64). The ingress interface is on the internal link (3ffe:306:1130:200::/64) and is configured with the MONET Prefix. LFN1 is a fixed node on the internal link. The MR moves and attaches to a foreign link (3ffe:306:5555:7777::/64) while performing MIPv6. In a first experiment, a CN in the fixed Internet pings MR. In a second experiment, the CN pings LFN1.

3.2.2. Registration with the Home Agent

MR obtains a CoA on the foreign link and registers its primary CoA with its HA. Once the HA receives a valid Binding Update from the MR, it records in its Binding Cache the binding between MR's home address and MR's CoA. The home address is used as the key for

searching the Binding Cache [MIPv6, [section 4.6](#)]. In order to intercept packets, HA claims to be the MR. This is performed by means of a "gratuitous" Neighbor Advertisement message on behalf of the mobile node (i.e. MR), as described in [MIPv6, [section 9.5](#)].

More precisely, when it receives a home registration from MR, the HA:

- o opens a NDP proxy to intercept packets addressed to MR's home address.
- o opens a tug (a virtual interface, i.e. IPv6 in IPv6 tunnel) between MR's CoA and itself.
- o adds a host-specific route (a route to a host, not to a prefix) for MR's home address via MR's CoA through the tug.

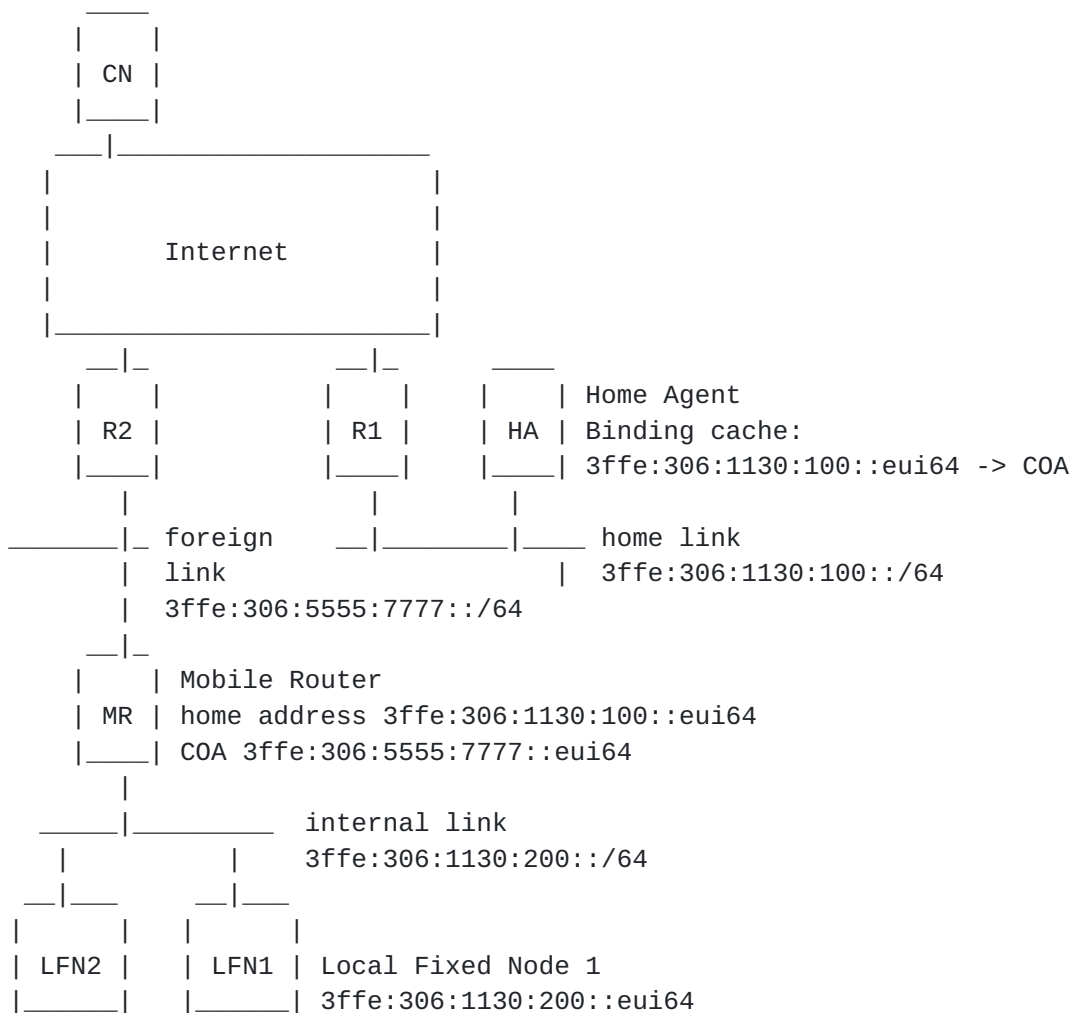


Figure 5: Packets sent from CN to LFN1 are dropped by Home Agent

3.2.3. First experiment: Communication between CN and MR

CN pings MR's home address (3ffe:306:1130:100::eui64). When the packet gets to the home network via R1, R1 sends NDP messages to discover the MAC address corresponding to the destination address (i.e. MR's home address). HA answers with its address on behalf of MR. The packet gets routed to the HA. In the standard IPv6 input function of the HA, the packet is routed through the tunnel, i.e. tunneled to MR's CoA. The packet therefore gets re-routed to the current location of the MR where it is de-tunneled and correctly received.

3.2.4. Second experiment: Communication between CN and LFN1

CN pings LFN1's IP address (3ffe:306:1130:200::eui64). When the packet gets to the home network, R1 checks its routing table to reach LFN1. R1 has a route to the MONET; MR's home address is the next hop toward LFN1. R1 sends NDP messages to discover MR's MAC address. HA answers with its address on behalf of the MR. The packet is transmitted on the home link and intercepted by HA. However, HA does not have a route to the MONET Prefix. The ping packet is thus sent to the default route, i.e. R1, which forwards it again to the HA. THE PING PACKET ENTERS A ROUTING LOOP UNTIL THE TTL EXPIRES.

3.3. Conclusion

We see that obtaining a CoA and requesting the HA to redirect incoming packets intended for MR doesn't require modifications in [\[MIPv6\]](#) as this could be done independently for a host or for a router. As a result, packets intended to MR are correctly intercepted by the HA and tunneled to MR.

However, although HA is able to intercept datagrams intended to LFNs, it is unable to encapsulate them to MR's CoA because it does not have a route to the MONET Prefix. The MR's registration only tells the HA to record a host-specific route in its routing table. A network route for the MONET Prefix (prefix of the MR's ingress interface) via MR's CoA is missing.

Since the HA is unable to redirect packets intended to LFNs and CNs don't have an entry in their Binding Cache to route packets directly to LFNs, no communication at all is possible between CNs and LFNs. We conclude that the Mobile IPv6 specification needs:

- o explicit clarification in order for the HA to redirect all packets intended to the MONET, but extensions are more likely needed.

o extension in order to transmit packets from the CN to LFNs by the most optimal route.

Some other Mobile IPv6 implementations do indeed interpret the behavior of the HA in face of a MR registration. In such implementations, the HA may have a network route for the MONET Prefix via MR's CoA. We advocate that such an implementation does not strictly follow [MIPv6] and may probably not comply with it. Leaving too much room for interpretation surely leads to misinterpretation and pitfalls, not to say security holes. Thus, MONETs should be taken into account explicitly, and separately from [MIPv6].

4. Mobile IPv6 extensions to support MONETs

4.0. Overview

According to the observations made in [section 3.2.4](#), we propose to extend Mobile IPv6 with "Prefix Scope Binding Updates". Instead of establishing a one-to-one relationship between a home address and a CoA, the binding establishes a many-to-one relationship between the set of nodes that share the same MONET Prefix and a CoA.

Prefix Scope Binding Updates are Binding Updates that associate a CoA with the MONET Prefix instead of the full 128-bits IPv6 home address. The MONET Prefix is carried in a new Sub-Option and requires a new flag in the Mobile IPv6 Binding Update Option.

MR sends Prefix Scope Binding Updates to its HA and all the CNs communicating with the MR itself or any LFNs behind it. The Prefix Scope Binding Update instructs its recipients to use the MONET Prefix as a netmask in the Binding Cache. The procedure for searching the Binding Cache is slightly modified for this purpose. As a result, the MR's CoA is returned for all destination addresses corresponding to the MONET Prefix.

As we can see, a sole Prefix Scope Binding Update message allows registration of an entire MONET, independently of the number of LFNs, and transparently to them. Our solution therefore preserve routing aggregation. In addition, direct routing between a CN and the MONET is also made possible by means of a single registration. This is particularly useful for a CN communicating with several LFNs from the same MONET.

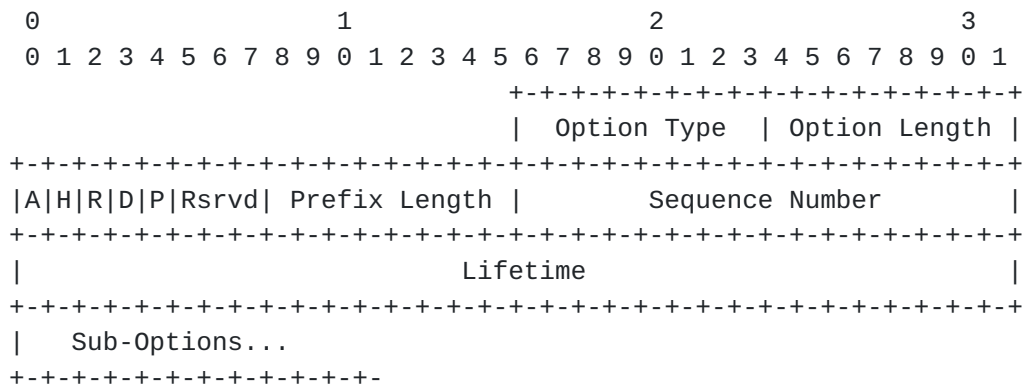
4.1. Packet Format of the Binding Update

We propose to extend the Mobile IPv6 Binding Update Option with an extra flag "Prefix Scope Registration" (P) taken from the "Reserved" field. In addition, the "MONET Prefix Sub-Option" is a new sub-

option that contains the MONET Prefix.

4.1.1. New Binding Update Option Format

The Binding Update option is encoded in type-length-value (TLV) format as follows:



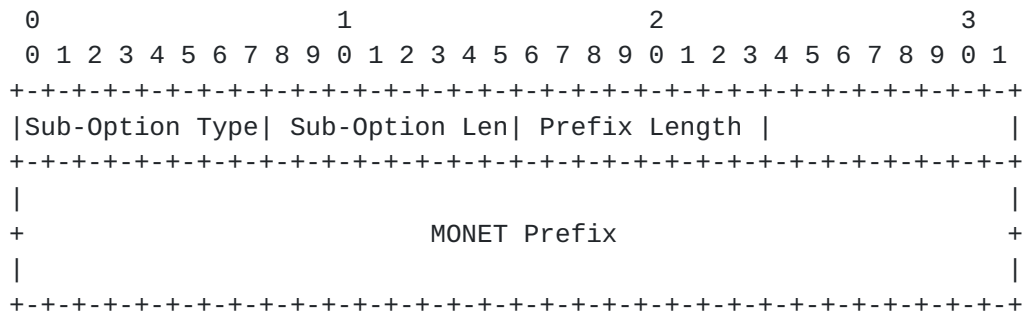
Prefix Scope Registration (P)

When set, it indicates that the sending mobile node attempts to register a CoA for an entire network. It also requests the receiving node to process the MONET Prefix Sub-Option and to re-route packets with a destination address that corresponds to the MONET Prefix.

Rsrvd

This field is reduced from a 4-bit field to a 3-bit field to account for the addition of the "Prefix Scope Registration" bit. The remaining 3 bits are unused and MUST be initialized to zero by the sender and MUST be ignored by the receiver.

4.1.2. MONET Prefix Sub-Option



The MONET Prefix is filled by the sending mobile node to request the receiving node to record a Prefix Scope entry in the Binding

Cache (see [section 4.2](#)).

The Prefix Length field is set to the (nonzero) length of the MONET Prefix.

The MONET Prefix field is set to the prefix of the MONET.

4.2. Cache Management

4.2.1. Binding Cache Entries

Binding Cache entries are as defined in [[MIPv6](#)] with minor changes:

- is added a "Prefix Scope Registration" (P) flag indicating whether this Binding Cache entry corresponds to a 128-bits address or a prefix. If set, the "home address" field is filled with a MONET Prefix instead of a full 128-bits address.

- the value of the "Prefix Length" field received in the Binding Update that created or last modified this Binding Cache entry is modified. This field is only valid if the "Prefix Scope Registration" flag or the "Home Registration" flag is set on this Binding Cache entry. If the "Prefix Scope Registration" flag is set, the "Prefix Length" corresponds to the length of the MONET Prefix, otherwise the meaning is as defined in [[MIPv6](#)].

4.2.2. Searching the Binding Cache Entries

The Binding Cache is searched for an entry corresponding to the destination address of the packet. The destination address is compared against the home address field of entries recorded in the Binding Cache.

If the "Prefix Scope Registration" flag is set in the entry under comparison, the comparison is made on the "Prefix Length" set of initial bits. If the prefix of the destination matches the MONET Prefix recorded in the entry, the destination is located in a MONET.

If the "Prefix Scope Registration" flag is not set, the comparison is made on the 128-bits addresses. If the destination address matches the home address, the destination is a mobile node.

In both case, the CoA of the corresponding entry is returned.

4.3. Extended Mobile IPv6 Protocol Operation

The MR is a new entity similar to the MN. The MR Operation makes use of most of the MN Operation extended with the ability to set the (P) bit to 1, to fill the MONET Prefix Sub-Option, and to send Binding Updates to all CNs that communicate with any LFN in the MONET.

The CN Operation and the HA Operation are extended in order to process the MONET Prefix Sub-Option and to transmit packets to the CoA of the MR. The MONET Prefix Sub-Option is processed if the (P) bit from the Binding Update Option is set. Packets are transmitted to the MR's CoA if the destination address matches the MONET Prefix.

The following sections only describe changes according to sections 8, 9 and 10 of the [MIPv6].

4.3.1. Correspondent Node Operation

Receiving (Prefix Scope) Binding Updates

Upon receiving a Binding Update, the CN performs validity checks as described in [MIPv6] [section 8.2](#). In addition, if the "Prefix Scope Registration" (P) bit in the Binding Update Option is set, the CN received a Binding Update from a MR and the Binding Update must include a MONET Prefix Sub-Option. This option MUST be ignored if the "Prefix Scope Registration" (P) bit is not set.

If the Binding Update is valid, the CN creates a new entry in its Binding Cache as this is performed in [MIPv6]. In addition, if the (P) bit is set, the CN creates a second Binding Cache entry similar to the first one as follows:

- o the "Prefix Scope Registration" bit is taken from the corresponding field as found in the Binding Update Option,
- o the "Prefix Length" field is taken from the corresponding field as found in the MONET Prefix Sub-Option,
- o the "Home Address" field is filled with the prefix taken from the "MONET Prefix" field as found in the MONET Prefix Sub-Option.

Figure 6 shows the content of the Binding Cache.

Sending Packets

Before sending any packet, the CN examines searches the Binding Cache for an entry corresponding to the destination address (see [section 4.2.2](#) "Searching the Binding Cache"). If a CoA is

returned, a routing header is inserted as specified in [[MIPv6](#)].

4.3.2. Home Agent Operation

Primary care-of address registration

Upon receiving a Binding Update, the HA performs validity checks as described in [[MIPv6](#)] [section 9.3](#). In addition, if the "Prefix Scope Registration" (P) bit in the Binding Update Option is set, the HA received a Binding Update from a MR and the Binding Update must include a MONET Prefix Sub-Option. This option MUST be ignored if the "Prefix Scope Registration" (P) bit is not set.

If the Binding Update is valid, the HA creates a new entry in its Binding Cache as it is performed in [[MIPv6](#)]. In addition, if the (P) bit is set, the HA creates a second Binding Cache entry similar to the first one as follows:

- o the "Prefix Scope Registration" bit is taken from the corresponding field as found in the Binding Update Option,
- o the "Prefix Length" field is taken from the corresponding field as found in the MONET Prefix Sub-Option,
- o The "Home Address" field is filled with the prefix taken from the "MONET Prefix" field as found in the MONET Prefix Sub-Option.

Figure 6 shows the content of the Binding Cache.

Intercepting Packets

Datagrams sent by the CN to the IP address of the LFN are routed up to the home link of the MR where they are intercepted by the HA as specified in [[MIPv6](#)] [section 9.5](#).

Tunneling Intercepted Packets to a Mobile Node

For any packet sent to a mobile node or a LFN for which the HA is the original sender of the packet, the HA is operating as a CN and the procedures described in [section 4.3.1](#) applies.

While acting as a HA, all packets addressed to the MR or a LFN are intercepted on the home link. The HA examines its Binding Cache for an entry corresponding to the destination address (see [section 4.2.2](#) "Searching the Binding Cache"). If a CoA is returned, the packet is tunneled to this CoA as specified in

[MIPv6].

4.3.3. MR Operation

Obtaining a care-of address

Similarly to a standard MN Operation defined in [MIPv6], the MR obtains a new CoA on each subsequent foreign links using either stateless or stateful DHCPv6 address configuration.

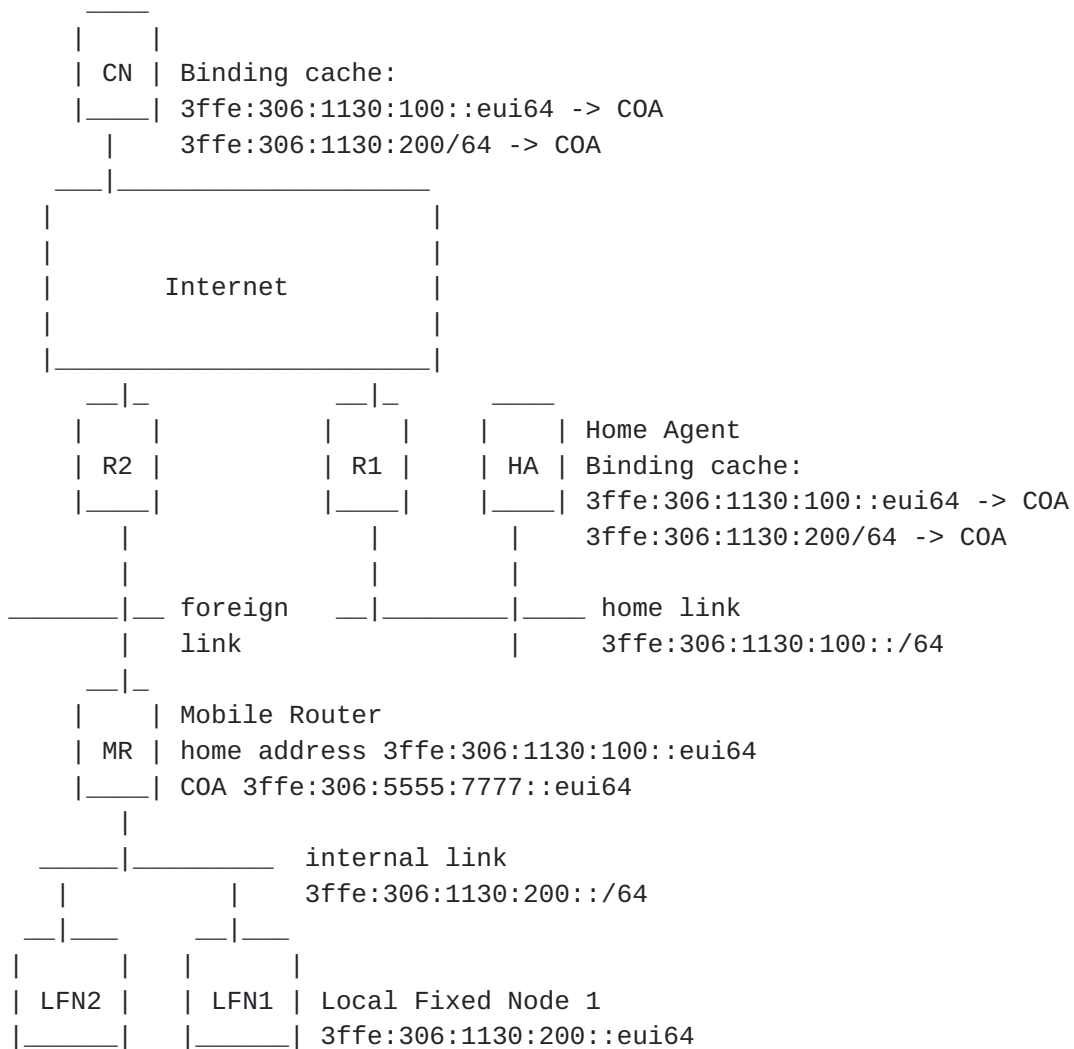


Figure 6 : MONET Prefix is recorded in the Binding Cache

Receiving encapsulated packets from the Home Agent

The MR may receive packet encapsulated to its CoA. Those packets may indeed be intended to the MR itself or to any LFN served by the MR. The reception of an encapsulated packet

tunneled from the MR's HA is an indication that the original sender may not have a Binding Cache entry for the MONET Prefix. In this case, the MR may deduce that a Prefix Scope Binding Update should be sent to the original sender of the packet.

Sending Prefix Scope Binding Updates

A MR serving as a gateway to a MONET sends Prefix Scope Binding Update datagrams to its HA, its own CNs, and CNs of the LFNs it is serving. Prefix Scope Binding Updates are sent as specified in [[MIPv6](#)] [section 10.6](#) and 10.8 and the Binding List is filled accordingly. In addition, the MR sets the "Prefix Scope Registration" bit in the Binding Update Option and inserts a MONET Sub-Option. The "Prefix Length" and the "MONET Prefix" fields are filled according to the MONET Prefix owned by the MR.

Bypassing ingress filtering

In order to bypass ingress filtering, the MR may encapsulate all outgoing packets to the destination with its CoA as the outer source address.

5. Security Issues

Prefix Scope Binding Update faces a number of security issues and is subject to modifications when a solution to secure Mobile IPv6 is found [[MIPv6-SECURITY](#)]. We are therefore monitoring ongoing discussion on the IETF mobileip mailing list.

5.1. Authentication

The registration of the MR's CoA for a MONET Prefix does not break authentication and does not differ from the standard Mobile IPv6 registration for a Mobile Node. In Mobile IPv6, the Mobile Node is authenticated by the CN based on its home address, whatever the content of the Binding Update. Similarly, nothing breaks the authentication of the sender of a Prefix Scope Binding Update. The MR operates as a standard Mobile Node and has a home address. Authentication is still based on this home address. Recipients of the prefix scope Binding Updates are not misled about the identity of the sender. The MR is clearly authenticated by its HA and CNs whatever is contained in the Binding Update.

5.2. Authorization

Discussion in the mailing list and IETF meetings have advocated a need to extend Mobile IPv6 with authorization. In the standard Mobile

IPv6, the Mobile Node is authenticated by its HA and CNs but those have no guarantee that the Mobile Node is allowed to send a Binding Update for the home address specified in the Binding Update. Indeed, the Mobile IPv6 policy is to accept whatever is being carried in the Binding Update as long as the sender is authenticated.

A MR willing to send Prefix Scope Binding Updates faces the same authorization issue. In addition, a means is required to authorize a MR to register a binding between the MONET Prefix and its CoA. In other words, we need a means to certify that the MR actually owns and serves the MONET Prefix.

5.3. Prefix Ownership

Two solutions are currently considered as suitable for ensuring address ownership for a Mobile Node: Cryptographically Generated Addresses (CGA) and Return Routability (RR) [[IETF-52](#)]. Both could be adapted for MRs, although it would require some enhancements to the protocols.

A Cryptographically Generated Address is obtained from a hash of a public key. The address is thus bound to a private key / public key pair that is used to sign the Binding Update. Extending the concept of CGA towards 'Cryptographically Generated Sub-Prefixes' does not seem to be applicable, except for specially long sub-prefixes. Indeed, the robustness of the algorithm against collisions is directly dependent on the space available to generate the (hopefully) unique identifier.

Return Routability model consists in verifying that the claimed home address is actually reachable at the given CoA. RR-based solutions would be easier to consider for ensuring prefix ownership. Whereas it cannot be envisioned to check return routability for every possible address behind the claimed prefix, it can be sufficient to check only a limited number of addresses, provided that they are properly chosen. For example, MR Home Agent address, MR Home Address, and any MNN Home Address may be enough for a CN to validate a received Prefix Scope Binding Update.

6. Changes since last draft

Changes from [draft-v2](#) to [draft-v3](#)

- Security section updated to take into account recent discussion on the mobileip mailing list about security: [section 5.2.1](#) and 5.2.2 are replaced by [section 5.3](#).
- Terminology: all the terminology used in this draft has been refined in order to comply with [[TERMINOLOGY](#)] discussed in [WEB-MONET].
- Rewording of most sections

Changes from [draft-v1](#) to [draft-v2](#)

- Abstract rewritten
- Extended section about security issues.
- Clarification between "home subnet prefix" and "MONET Prefix" in the terminology.
- [Section 3.3](#) divided into 3.3 and 3.4
- Added section "Receiving encapsulated packets from the Home Agent"
- Minor misspelling corrections

Changes from [draft-v0](#) to [draft-v1](#)

- Updated definitions of the terminology [section 2.2](#), particularly:
 - o clarified the distinction between possible kinds of nodes located in the MONET: Local Fixed Nodes (LFN) and Visiting Mobile Nodes (VMN).
 - o clarified that the MR has (at least) two interfaces, one on the home link, one on the internal link (within the MONET)
- New example showing IPV6 addresses
- Added a description of an experimentation outlining HA is unable to tunnel packets to the MONET if the final destination is not the MR itself.

- Enhanced section about security concerns

Acknowledgments

This work has originally been supported by Motorola Labs Paris and ANRT (French ``Association Nationale de la Recherche Technique'') under CIFRE convention number 97595. This CIFRE convention associates: a firm, Motorola Labs (Paris, France); a French academic laboratory (INRIA Rhône-Alpes, Grenoble) and a French university (University Joseph Fourier, Grenoble). We would like to thank Francis Dupont (ENST Bretagne) for his careful reading, valuable comments and suggestions, and also Christophe Janneteau (Motorola Labs), Alexandru Petrescu (Motorola Labs), Ryuji Wakikawa (WIDE Project, Keio University), and Koshiro Mitsuya (WIDE Project, Keio University) for all their comments. The first author would like to thank both Motorola Labs Paris and INRIA Rhône-Alpes, for being given the opportunity to bring this topic to the IETF.

References

- [Ernst01] Thierry Ernst "Network Mobility Support in IPv6", PhD Thesis, University Joseph Fourier Grenoble, France, October 2001.
- [HMIP] Hesham Soliman, Claude Castelluccia, "Hierarchical MIPv6 mobility management", <[draft-ietf-mobileip-hmipv6-03.txt](#)>, IETF, February 2001. Work in progress.
- [IETF-52] Proceedings IETF Meeting Salt Lake City, December 2001, <http://www.ietf.org/proceedings/01dec/slides/mobileip-6/>
- [IPv6] S. Deering and R. Hinden. Internet Protocol Version 6 (IPv6) Specification. [RFC 2460](#), December 1998.
- [MIPv4] C. Perkins (Editor). "IP Mobility Support", [RFC 2002](#), October 1996.
- [MIPv4-R0] C. Perkins and D. B. Johnson. "Route Optimization in Mobile IP", Sun Microsystems and Carnegie Mellon University, February 2000. Work in progress.
- [MIPv6] D. B. Johnson and C. Perkins. "Mobility Support in IPv6", April 2000. Work in progress.
- [MIPv6-SECURITY] G. Montenegro, A. Petrescu "MIPv6 Security:

- Assessment of Proposals"
<[draft-montenegro-mobileip-mipv6-seceval-00.txt](#)>,
IETF, November 2001. Work in progress.
- [Ownership] P. Nikander. An Address Ownership Problem in IPv6,
<[draft-nikander-ipng-address-ownership-00.txt](#)>,
IETF, February 2001. Work in progress.
- [Perkins98] C. Perkins, "Mobile IP, Design Principles and
Practices". Wireless Communications Series.
Addison-Wesley, 1998. ISBN 0-201-63469-4.
- [REQUI-1] Thierry Ernst, Hong-Yon Lach
"Requirements for Network Mobility Support",
<[draft-ernst-monet-requirements-00.txt](#)>,
IETF, February 2001. Work in progress.
- [REQUI-2] Lach, Boot, Janneteau, Olivereau, Petrescu
"Mobile Network Scenarios, Scope and Requirements",
<[draft-lach-monet-requirements-00.txt](#)>,
IETF, February 2002. Work in progress.
- [REQUI-3] T. J. Kniveton, J. T. Malinen, V. Devarapalli,
C. Perkins. "Mobile Router Support with Mobile IP"
<[draft-kniveton-monet-requirements.txt](#)>,
IETF, February 2002. Work in progress.
- [Solomon98] J. D. Solomon. "Mobile IP, The Internet Unplugged".
Prentice Hall Series in Computer Networking and
Distributed Systems. Prentice Hall PTR, 1998.
ISBN 0-13-856246-6.
- [TERMINOLOGY] Thierry Ernst, Hong-Yon Lach
"Terminology for Network Mobility Support",
<[draft-ernst-monet-terminology-00.txt](#)>,
IETF, February 2002. Work in progress.
- [WEB-MONET] MONET web page <http://www.nal.motlabs.com/monet>

Author's Addresses

Please direct questions about this memo to first author

Thierry Ernst,
WIDE Project and INRIA
Jun Murai lab, 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/>

Alexis Olivereau
Motorola Labs Paris,
Networking and Applications Lab (NAL)
Espace Technologique - Saint Aubin
91193 Gif-sur-Yvette Cedex, France
Phone: +33 1 69 35 25 16
Email: Alexis.Olivereau@crm.mot.com

Ludovic Bellier
INRIA - PLANETE team
ZIRST-655 avenue de l'Europe
38330 Montbonnot Saint Martin, France
Email: Ludovic.Bellier@inrialpes.fr

Claude Castelluccia
INRIA - PLANETE team
ZIRST-655 avenue de l'Europe
38330 Montbonnot Saint Martin, France
Phone: +33 4 76 61 52 15
Email: Claude.Castelluccia@inrialpes.fr

Hong-Yon Lach
Motorola Labs Paris,
Networking and Applications Lab (NAL)
Espace Technologique - Saint Aubin
91193 Gif-sur-Yvette Cedex, France
Phone: +33 1 69 35 25 36
Email: Hong-Yon.Lach@crm.mot.com

