

MIPSHOP Working Group
Internet-Draft
Expires: January 18, 2006

W. Haddad
S. Krishnan
Ericsson Research
H. Soliman
Flarion
G. Daley
Monash University CTIE
H. Tschofenig
Siemens AG
July 17, 2005

Optimizing Micromobility Management for Active and Dormant Mobile Nodes
[draft-haddad-mipshop-omm-01](#)

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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/lid-abstracts.txt>.

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

This Internet-Draft will expire on January 18, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

Micromobility protocols address mobile nodes (MN) movements within a particular IP network domain. This document introduces a new

Internet-Draft

OMM

July 2005

protocol "Optimized Micromobility Management" (OMM), to manage Micromobility for active and dormant mobile nodes. The suggested solution is based on the Hierarchical Mobile IPv6 (HMIPv6) proposal and aims to increase the mobility performance by reducing the handover latency and the packet loss.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	4
3.	Glossary	5
4.	Overview of HMIPv6	8
5.	Problem, Motivation and Requirements	9
6.	Overview of the OMM Protocol	11
7.	OMM Protocol Description	14
8.	Mobility for Dormant Mode Mobile Nodes	17
9.	OMM New Bits, Options and Messages Structure	19
9.1	The Address Check Information Option (ACIO)	19
9.2	The Optimized Micro-Mobility Information Option (OMMIO) .	19
9.3	Paging Zone Identifier Option (PZIO)	20
9.4	The VMAP (V) Bit	20
9.5	Modified Router Solicitation message format	21
9.6	Modified Binding Acknowledgement message format	22
9.7	The Routing Path Update (RPU) Message	22
9.8	The Location Update (LU) Message	23
9.9	The Location Acknowledgement (LA) Message	23
10.	Security Considerations	24
11.	Normative References	25
12.	Informative References	26
13.	References	26
	Authors' Addresses	27
	Intellectual Property and Copyright Statements	28

Internet-Draft

OMM

July 2005

1. Introduction

Managing Micromobility has been addressed in many different ways. Among existing proposals (e.g., [[HMIPv6](#)], [[CIP](#)], [[HAWAII](#)], etc), only the HMIPv6 proposal has been adopted by the IETF.

This document introduces a new protocol, i.e., OMM, to manage Micromobility for active and dormant mobile nodes. The suggested solution is entirely based on the Hierarchical Mobile IPv6 (HMIPv6) proposal and aims to increase the mobility performance by reducing the handover latency and packet loss. For these purposes, the OMM protocol uses Virtual Mobility Anchor Points (VMAPs) and splits the handover event into two successive phases triggered by the network and the mobile node (MN). For dormant MNs, OMM uses the VMAP nodes as Paging Agents (PA) and allows to page multiple MNs concurrently, in order to optimize the bandwidth usage and minimize the call setup delay.

2. 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 [[RFC2119](#)].

[3.](#) Glossary

Term	Definition
Mobility Anchor Point (MAP)	A Mobility Anchor Point is a router located in a network visited by the mobile node. One or more MAPs can exist within a visited domain.
Virtual MAP (VMAP)	A virtual MAP is a router located inside the IP network domain (i.e., a MAP is also a VMAP), which implements a set of features, which includes a subset of the MAP features. A VMAP node stores the MN's Regional Care-of Address (RCoA) and current Local Care-of Address (LCoA) for a limited period of time (e.g., the binding lifetime), computes the new MN's LCoA and encapsulates when needed data packets sent by the CN to the MN's current location. At any particular time during an ongoing

	session(s), the mobile node should have AT MOST one VMAP encapsulating data packets and forwarding them to its new current location. As mentioned earlier, each VMAP carries the PA functionalities and defines its own Paging Zone (PZ).
Access Router (AR)	The mobile node's default router. The AR aggregates the outbound traffic of mobile nodes. An AR can also be a MAP/VMAP.
Regional Care-of Address (RCoA)	An RCoA is an IPv6 address obtained by the mobile node from the visited network. An RCoA is an address on the MAP's subnet. It is auto-configured by the MN when receiving the MAP option.
On Link Care-of Address (LCoA)	The LCoA is the on-link CoA configured on a mobile node's interface based on the prefix is advertised by its default router.

Tree Architecture	An IP network domain has a tree architecture when any router located inside the domain (i.e., except the ARs and the root gateway(s)) has only one uplink and one or more downlink(s). Such topology has no mesh links.
Mesh Architecture	A mesh network topology is defined as a pure tree topology with additional mesh links. This means that in a mesh topology, at least one router located inside the domain has one or more mesh link(s) in addition to its uplink and downlink(s) channels.

Random Architecture	A random network topology is used to indicate a mesh topology with additional uplinks. This means that in a random topology, at least one router located inside the domain has more than one uplink(s), in addition to its downlink(s) and mesh link(s) channels.
Local Binding Update (LBU) Message	The Mobile Node sends a Local Binding Update (LBU) message to the MAP in order to establish a binding between the RCoA and the LCoA.
Routing Path Update (RPU) Message	A Routing Path Update Message is sent by the new MN's New Access Router to the MN's Previous LCoA (pLCoA). The RPU message is used to trigger a Network Handover, which is totally transparent to the MN.
Network Handover (NH)	A Network Handover can be defined in the context of the OMM protocol, as the process triggered by the network, of re-routing data packets flow(s) sent to a particular mobile node to its new location before the MN sends an LBU message to the MAP. The NH process aims to minimize the handover latency as well as the packet loss.
Dormant Mode	A state in which the mobile node restricts its ability to receive normal IP traffic by reducing monitoring of radio channels. This allows the mobile node to save power and reduces signaling load on the network.

Paging	As a consequence of a mobile-bound packet destined for a mobile currently in dormant mode, signaling by the network through radio access points directed to locating the mobile and alerting it to establish a last hop connection.
Paging Zone	A Paging Zone is the set of Access Points

	(APs) attached to one particular VMAP. Note that this definition applies only when the particular VMAP is an access router, which is the case in most random architecture. A mobile node in dormant mode may be required to signal to the network when it crosses a paging zone boundary, in order that the network network can maintain a rough idea of where the mobile is located.
Location Update (LU) Message	A Location Update Message is sent by the Paging Agent to the MAP to update it with the current Paging Zone of a particular MN while being in a dormant state.
Location Acknowledgment (LA) Message	A Location Acknowledgment Message is sent by the MAP to one particular VMAP to acknowledge the receipt of a Location Update Message sent earlier by the same VMAP.
Paging Message (PM)	A Paging Message is broadcasted by the VMAP to all mobile nodes located within its Paging Zone. The PM message carries among others, an 128-bits parameters representing the set of all targeted mobile nodes, and a set of hash functions, which allow all mobile nodes within the PZ to check if they belong to the set of the targeted nodes.

Table 1: Glossary

For more details about terms defined above, please refer to [[HMIPv6](#)], [[TOMOP](#)] and [[Paging](#)].

The two main goals behind designing the [\[HMIPv6\]](#) protocol are to reduce both the heavy amount of signaling messages generated by the MIPv6 protocol and the handover latency. A third goal is to enable the MN to hide its movements and current location from the CN and the HA.

HMIPv6 consists on deploying one or more special nodes called Mobility Anchor Point, i.e., MAP, within the IP network domain. A MAP can be defined as a local home agent, which intercepts all packets addressed to registered mobile nodes and tunnels them to the MN.

When a MN enters to an HMIPv6 domain, it starts by selecting, then registering itself with the appropriate MAP. This is done by processing special information sent by the MN's AR in the Router Advertisement (RtAdv) message. These information allow the MN to auto-configure a regional care-of address (RCoA), which will be used by the MAP to capture packets sent from outside the domain to the MN's care-of address (i.e., RCoA), and a link care-of address (LCoA), which will be used by the MAP to locate the MN inside the MAP domain.

It should be noted at this stage that HMIPv6 recommends that the MN selects the furthest MAP to avoid frequent MAP changes, which in turn implies going through the time consuming MAP registration procedure during the handover.

Each time the MN moves to a new AR, it has to configure a new LCoA and registers it with the MAP. This is done by sending a Local Binding Update (LBU) message to the MAP. The LBU message allows the MAP to bind the new LCoA to the MN's RCoA.

5. Problem, Motivation and Requirements

HMIPv6 protocol succeeds in eliminating redundant signaling messages in MIPv6, i.e., the HoTI/HoT and CoTI/CoT messages, while keeping only critical mobility messages, i.e., local binding update (LBU) and binding acknowledgement (BA) messages, exchanged between the MN and the MAP.

However, HMIPv6 partially succeeds in reducing the handover latency since the LBU message sent from the MN to the MAP will most likely have to travel on a relatively long path within the domain before reaching the MAP (being supposedly static), in order to trigger a re-routing of the data packets flow to the MN's new LCoA (nLCoA). Such delay may result in packet loss, which becomes more alarming if the MN is moving at a high speed within the MAP domain while running time sensitive applications.

This is mainly due to the fact that HMIPv6 recommends avoiding changing the MAP as much as possible. Consequently, HMIPv6 suggests choosing the furthest MAP in the hierarchical domain, which is in most cases the domain gateway node(s).

In addition, HMIPv6 practically converts any network topology (i.e., mesh or random) to a tree topology, which if deployed alone, lacks both robustness and load balancing features.

Based on that, HMIPv6 does not take any advantage from a mesh or random topology since all signaling messages are sent on the shortest uplink path to the root of the tree topology, i.e., the furthest MAP gateway.

But it should be noted that HMIPv6 provides the lowest handover latency among other micromobility proposals (e.g., HAWAII and CIP) for the first handover only, i.e., when the MN enters into an HMIPv6 domain. But when the MN starts moving within the MAP domain then the handover performance start decreasing when compared to the two other proposals ([\[TOMOP\]](#), [\[MIPS\]](#)).

Note that, although the mobility performance may increase in both CIP and HAWAII proposals, the CIP protocol continuously involves every node on the path between the gateway and the MN, and requires being implemented in the base station. On the other hand, the HAWAII proposal relies on sub-optimal routing path(s), which in turn can lead to an unoptimized load balancing in the access network.

Internet-Draft

OMM

July 2005

Based on the above, the requirements for a new optimized micro-mobility protocol, which offer the main advantages of each of the above protocol, are:

- a. The load of signaling messages required during the handoff procedure should be minimized as much as possible.
- b. In order to minimize or eliminate the handoff latency and packet loss, the load of signaling messages should be concentrated only near the involved MN's new AR.
- c. As it is the case in HMIPv6, the handoff procedure should result at the end in a new optimal path between the MAP and the new MN's location.
- d. Any new node in the MAP domain which may be involved in the handoff procedure should be maintained in soft-state so that invalid bindings/keys are deleted automatically.
- e. All signaling Messages exchanged between routers and between routers and the MAP are authenticated.

The above requirements led to the design of a simple proposal, which is totally built on top of HMIPv6 and increases the performance of IP handovers, which occur within an HMIPv6 domain. In addition, the OMM protocol takes full advantage from a mesh/random topology.

6. Overview of the OMM Protocol

The OMM protocol aims to bring key advantages provided by some existing micromobility proposals, like CIP, HAWAII and HMIPv6, while minimizing/eliminating their different drawbacks. The OMM protocol fulfills requirements a), b) and c) by adding at most one message between the MN's nAR and one special node (i.e., VMAP) located nearby. Moreover, the OMM protocol allows the MN to skip the DAD or, in the worst case, to perform it in parallel with exchanging data.

In short, the OMM protocol splits the IP handover into two successive events. The first one is a network handover (NH) and is triggered by the infrastructure itself (i.e., the MN's new AR). Note that the NH greatly benefits from a random network topology, i.e., it relies on sub-optimal routing of data packets (as in HAWAII) sent to the MN, in exchange for a shorter latency and minimum packets loss.

The main goals behind triggering first a network handover are to reduce the latency and packet loss as much as possible. In other words, the NH aims to eliminate the latency variable from the second event, which is the handover triggered by the MN itself according to HMIPv6 protocol.

For these purposes, the OMM protocol requires implementing a limited set of the MAP features on routers located between the MAP and the ARs, i.e., in order to convert them to VMAPs. Each time the MAP gets an LBU message from the MN, it sends a BA message, which is used also to store the MN's RCoA in the VMAP(s) located near the MN and on the path between the MAP and the MN. Note that these signaling data are stored in VMAP(s) in a soft state and must be removed immediately after the expiration of the Binding Update Lifetime set by the MN in the LBU message.

Each time, the network infrastructure triggers a NH, the VMAP simulates the MAP role for a limited period of time, i.e., until the second event is completed, thus significantly reducing the latency and packets loss.

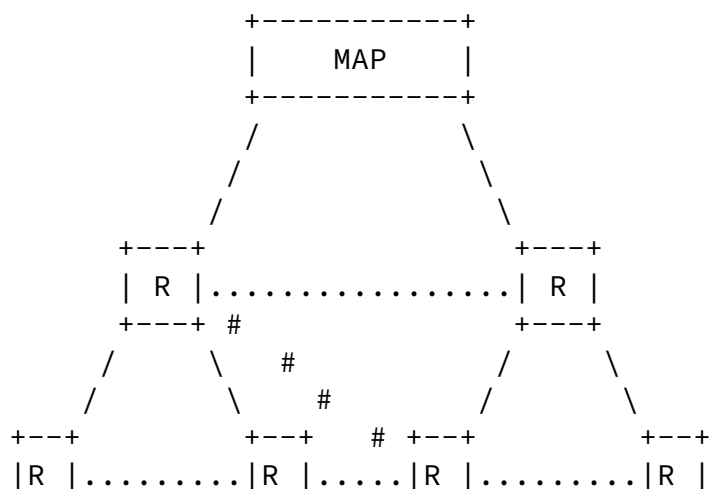
It becomes clear from the above that, in order to get the best performance from the NH, the selected VMAP must be located as close as possible to the MN's new AR (or within the nAR itself depending on the network topology).

In the OMM protocol, the second event, i.e., handover triggered by the MN, aims only to re-direct data packets flow sent to the MN to a more optimal path. Such step is needed, especially that the first event, i.e., NH, may use a sub-optimal path to pull data packets flow to the MN's new LCoA. As described in HMIPv6, the second event

updates the MAP BCE with the new MN's LCoA in order to allow the MAP to tunnel data packets to the new MN's LCoA.

Finally, it should be noted that the worst case scenario in OMM protocol is the failure of the NH, which means having only the handover triggered by the MN itself, as defined in HMIPv6. This lead us to the HMIPv6 case.

The following figure shows the VMAPs location in a full random hierarchical domain topology:



```

      +---+ #      +---+      +---+      +---+
      /   \      /   \      /   \      /   \
+---+   +---+ # +---+ +---+ +---+ +---+ +---+ +---+
|V |...|V |...|V |.|V |.|V |..|V |...|V |.|V |
+---+   +---+   +---+ +---+ +---+ +---+   +---+ +---+
***** *****  ****  ****  ****  ****  ***** *****

```

Where:

- R represents a router
- V represents a Virtual MAP (VMAP)
- ... represents a mesh link, i.e., mesh topology
- ### represents a random link, i.e., random topology
- * represents an AP

Note that having a full mesh topology only at the lowest level of the hierarchical domain topology requires converting only the ARs to

VMAPs in order to obtain maximum performance.

[7.](#) OMM Protocol Description

As mentioned earlier, OMM protocol consists on implementing a limited set of MAP features (and one new feature) in routers located between the MAP and the ARs. A router with the added set of MAP features is called a virtual MAP (VMAP). A VMAP enabled router **MUST** provide the two following features:

- o Store the MN's IPv6 addresses (i.e., RCoA and LCoA) in its Virtual Binding Cache Entry (VBCE). This is performed upon receiving a BA message carrying a binding hop-by-hop message.

- o Check the ownership of the old MN's old LCoA (oLCoA), computes the new MN's LCoA (nLCoA) and tunnel data packets sent to the MN's nLCoA. This is performed upon receiving a Routing Path Update (RPU) message.

The techniques proposed in this document work at their best when the following conditions are met:

- o The MAP domain has a random network topology.
- o Messages exchanged between routers (i.e., VMAPs and ARs), located within the same MAP domain are authenticated.
- o All routers located in the same MAP domain can be converted to VMAPs. This assumption applies also for the ARs. Note that this is not a required condition. If there are no VMAPs on the path between the nAR and the pLCoA the situation boils down to the base HMIPv6 case.

However, it should be noted that adding links between ARs and converting some or all of them to VMAPs can bring additional performance to the OMM protocol and help avoiding updating all exiting VMAPs located between the MAP and the MN each time the MN switches to a new AR.

HMIPv6 protocol requires the ARs to add the MAP functions data to their RtAdv messages sent to the MN. These information allow the MN to select the furthest MAP, auto-configure an RCoA and an LCoA and send them to the MAP in an LBU message. The two addresses enable the MAP to create the binding and to intercept data packets sent to the MN's RCoA and tunnel them to the MN's current location.

When the MN enters for the first time to an HMIPv6 domain, it MUST follow the HMIPv6 protocol. The first new step introduced by the OMM protocol consists on alerting the MN of the support for the OMM protocol. This is done by setting the Optimization (O) bit (defined

in 8.10) in the RtAdv message sent by the AR.

The second step starts when the MAP sends a BA message after receiving an LBU message from the MN. The MAP MUST insert in the BA

message a new hop-by-hop option called "Virtual Binding" (VB). The VB must carry the MN's two IPv6 addresses sent to the MAP in the BU, the binding lifetime and the "Address Management Key" (Kam). Note that the Kam SHOULD be derived from hashing the shared secret established between the MN and the MAP so that the MN does not need to store a new Key.

Finally, the MAP MUST authenticate the VB option with the Kam and MUST encrypt the Kam field with a shared key pre-computed between the MAP and the VMAPs.

Upon receiving a BA message carrying a VB hop-by-hop option, the VMAP starts by checking if its VBCE has an entry corresponding to the MN's LCoA. If this is the case, the VMAP should update any existing value (e.g., binding lifetime) with the new one carried in the VB option. In case there is no entry, the VMAP MUST create one, which includes all data sent in the VB.

The third step occurs when the MN switches to a new link. In such scenario, the MN starts by sending a RtSol message, which MUST contain its RCoA, its pLCoA and a proof of ownership of the two addresses.

The proof is carried in a new option (i.e., "Address Check" (AC) option defined in [Section 9.1](#)) and is presented as the result of the following:

Proof = First[64, HMAC(Kam, (RCoA | pLCoA))]

The MN's addresses and the proof of ownership are carried in two different options defined in [Section 9.1](#) and [Section 9.2](#)

The VMAP MUST delete from its VBCE all information related to one particular MN upon the expiration of the binding lifetime, unless another BA is sent by the MAP carrying a new binding lifetime (i.e., the MN has sent a new LBU message carrying the same LCoA to the MAP).

The next step in the OMM protocol consists on triggering a network handover (NH). This is done by the MN's nAR upon receiving a RtSol message, which contains the two options. In such scenario, the AR SHOULD send in parallel a Route Path Update (RPU) message to the MN's pLCoA (carried by the RtSol message) and a RtAdv message to the MN. Note that the RPU message MUST be signed by the nAR.

When a VMAP receives an RPU message, it starts by checking its VBCE for an entry which contains the couple (RCoA, pLCoA). If an entry is found, the VMAP first checks whether the proof contained in the message is valid. If so, it computes the MN's nLCoA IID and updates its VBCE with the new MN's nLCoA. The same IID MUST be computed by the MN and in the same following way:

$$\text{nLCoA(IID)} = \text{First}[64, \text{HMAC}(\text{Kam}, (\text{RCoA} \mid \text{pLCoA} \mid \text{New_Subnet_Prefix}))]$$

After updating its VBCE, the VMAP starts tunnelling data packets sent by the MAP to the MN's pLCoA to its new location (i.e., nLCoA). The VMAP MUST delete the MN's corresponding entry from its VBCE at the expiration of the routing binding lifetime (RBL) sent by the MN's nAR in the RPU message. Note that the RBL value may be predefined.

After the MN gets a new LCoA, it MUST send an LBU message to the MAP. The LBU message updates the MAP's BCE, re-route the data traffic by using a more optimized route between the MAP and the MN and update the VMAP (i.e., via the BA message) on the new path between the MN and the MAP. It should be noted that many VMAPs may be updated by one specific BA message. However, the decision to turn on/off more than one VMAP on a particular path should be taken based on the network topology around that path.

Internet-Draft

OMM

July 2005

8. Mobility for Dormant Mode Mobile Nodes

In addition to the micro-mobility optimization described for active MNs, this proposal introduces a new technique to page MNs while being in dormant mode and moving across different Paging Zones (PZ). Our approach applies the hash-based paging procedure using bloom filters [HBP] to the OMM protocol. Note that such technique can be used to page several MNs located in the same PZ concurrently, thus significantly reducing the paging bandwidth consumption and the call setup delays.

As mentioned earlier, our solutions consists on adding Paging Agent (PA) functionalities to the VMAPs. In addition, the suggested solution introduces a new Paging Zone Identifier (PZI), which allows the MN to detect when entering to a new PZ. The PZI MUST be carried in the RtAdv message.

When a MN in a dormant mode detects that the PZI has changed, it MUST send a RtSol message to the AR. The RtSol message MUST carry its HoA and the PZI. The latter is used to notify the AR, i.e., VMAP, that the MN is in a dormant mode. Upon receiving the RtSol message, the AR sends an LU message to the MAP to notify it about the new location of the MN. The LU message MUST contain the MN's RCoA and MUST be authenticated by the VMAP. When the MAP receives an LU message, it creates/updates the MN's corresponding BCE with the new source address, i.e., VMAP, sent in the LU message. After that the MAP MAY send back an LA message to the VMAP

When an incoming call arrives to the MN's RCoA address, the MAP starts by checking the corresponding BCE and tunnels the packet to the corresponding VMAP. The receipt of a packet carrying a VMAP address as destination address serves to notify the VMAP that the inner destination address, i.e., RCoA, carried by the packet needs to be paged. For this purpose, the VMAP will periodically, e.g., every 1 second, generate an 128-bit parameter using all RCoAs that need to be paged, i.e., to empty its queue. The computed parameter and all hash functions used to generate it are carried by the paging message sent by the VMAP to all nodes in its PZ. Upon receiving paging message, a MN SHOULD process it in the following way:

- o If the MN is in active mode, then it SHOULD discard the message.
- o If the MN is in dormant mode, then it can detect if it is being paged by checking the bits positions {H1(RCoA), H2(RCoA), ..., Hk(RCoA)} in the 128-bit parameter sent in the Pmes. Note that {H1(), H2(), ...} are the hash functions used by the PA to compute the parameter from the set of RCoAs which are waiting in the queue to be paged. If any of the bit position is 0, then the

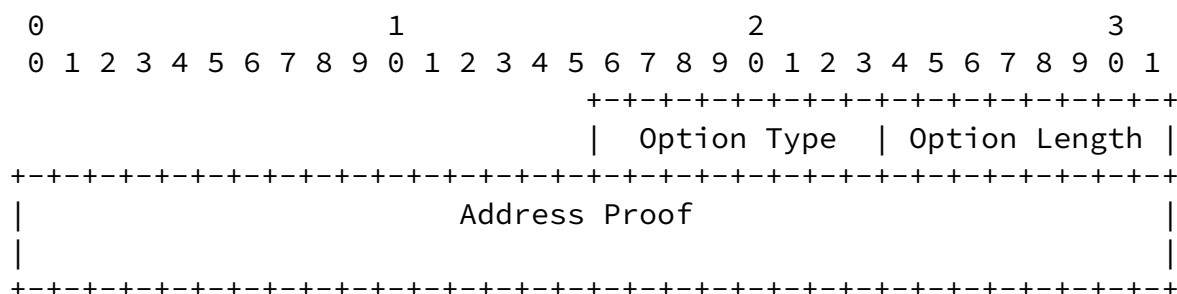
corresponding RCoA is not paged. Otherwise, the MN's RCoA is paged and MUST proceed according in the same way described above for an active MN.

9.

OMM defines new bit and options to be carried by the RtSol message. The new bit and options are the following:

9.1

This option is used to carry the address check proof created by the mobile node. This option is used to verify whether the mobile node is really the owner of the addresses carried in the OMMIO option. The format of the option is the following:



Option Type

Option Length
Length of the option.

This contains the pLCoA and the RCOA of the mobile node

[9.3](#) Paging Zone Identifier Option (PZIO)

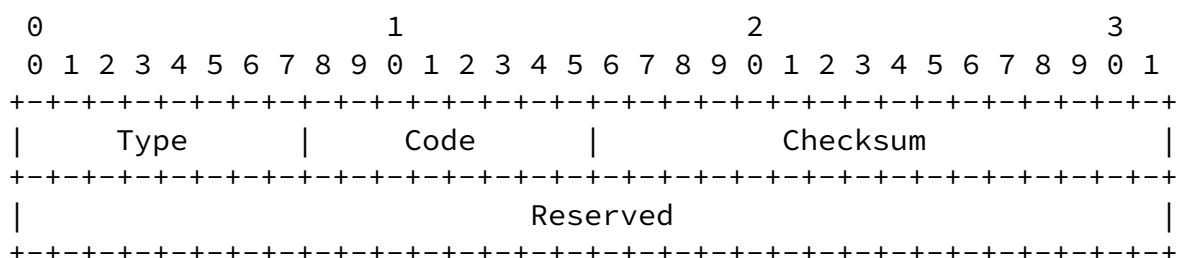
The PZI option will be specified in a future version of this document.

9.4 The VMAP (V) Bit

The VMAP bit is a new bit used in the OMM proposal to request VMAP node(s) located between the MAP and the MN's current location to store the MN's addresses (i.e., RCoA and LCoA) and the binding lifetime in their VBCE(s). The VMAP bit **MUST** be set by the MAP in the BA message each time the MAP receives a valid LBU message from the MN. Note that the MN **MUST** ignore such bit.

9.5 Modified Router Solicitation message format

The modified Router Solicitation sent from a MN supporting this specification would look like this





IP Fields:

Source Address

The Source Address MUST be the MN's nLCoA.

Destination Address

Typically the all-routers multicast address.

Hop Limit 255

ICMP Fields:

Type 133

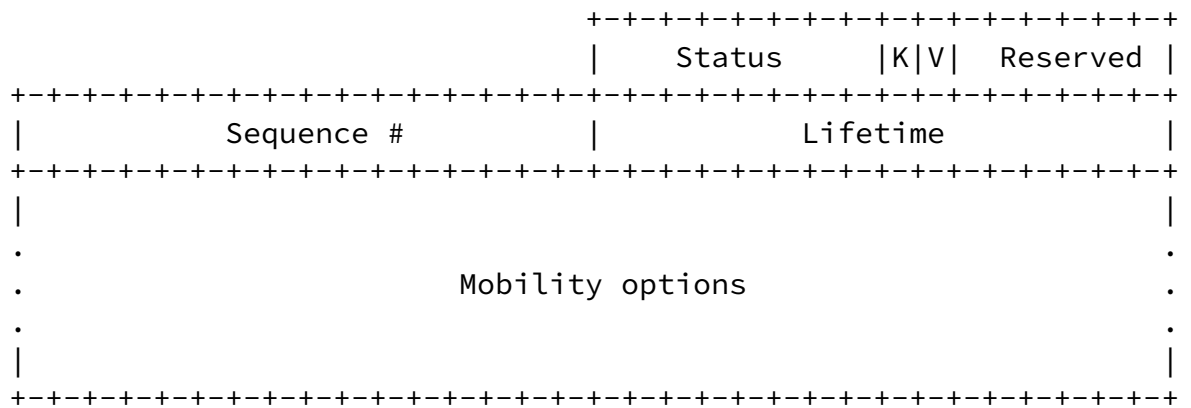
Code 0

Checksum The ICMP checksum. See [[ICMPv6](#)].

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

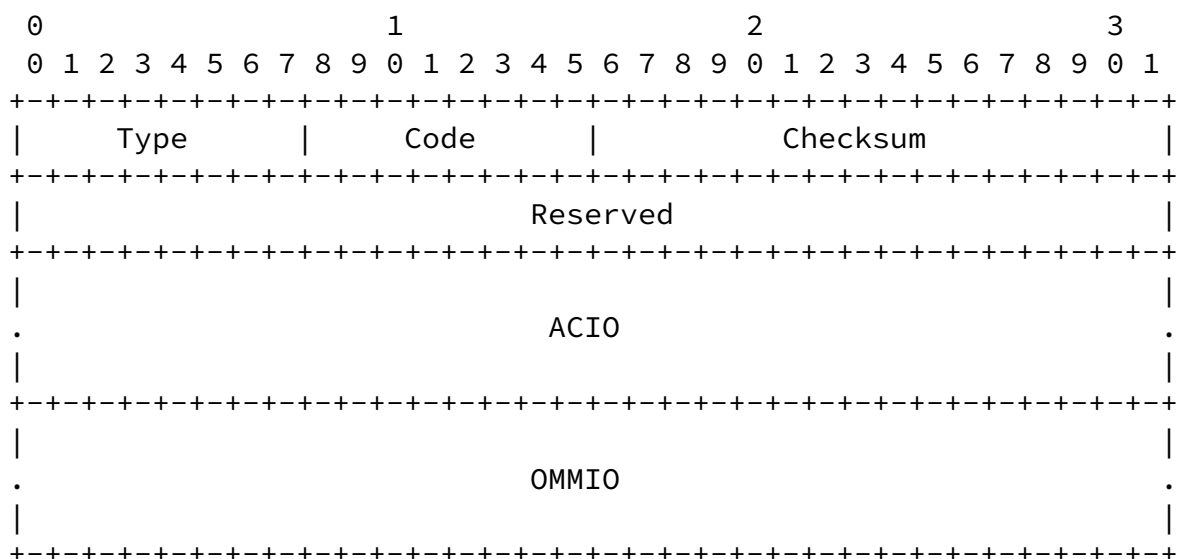
9.6 Modified Binding Acknowledgement message format

When the binding acknowledgement message sent by the MAP it contains the VMAP (v) bit as described. The modified BA looks like this.



9.7 The Routing Path Update (RPU) Message

The Routing Path Update message sent from a nAR supporting this specification would look like this



IP Fields:

Source Address

The Source Address MUST be one of nARs addresses.

Destination Address

The pLCoA of the MN.

ICMP Fields:

Type	<To Be Assigned By IANA>
Code	0
Checksum	The ICMP checksum. See [ICMPv6].
Reserved	This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
ACIO	The Address check information option as specified above
OMMIO	The OMM information option as specified above

[9.8](#) The Location Update (LU) Message

The location update message will be specified in a future version of this document.

[9.9](#) The Location Acknowledgement (LA) Message

The location acknowledgment message will be specified in a future version of this document.

Internet-Draft

OMM

July 2005

[10.](#) Security Considerations

The OMM protocol assumes that all signaling messages exchanged between routers (e.g., VMAPs) located within a MAP domain are authenticated.

The OMM protocol does not introduce nor amplify any new or existing attacks or threats. However, it should be noted that triggering a network handover without providing a proof of ownership of the previous LCoA mentioned in the RtSol message sent by the MN to the nAR may allow to re-direct/steal data packets sent to another node attached to the MN's previous AR.

11. Normative References

- [EAR] J. Choi, D., Shin, "Fast Router Discovery with RA Caching", [draft-jinchoi-dna-frd-00](#), July 2004.
- [ICMPv6] A. Conta, S. Deering, M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", [draft-ietf-ipngwg-icmp-v3-06](#), November 2004.
- [HMIPv6] H. Soliman, K. elMalki, C. Castelluccia, L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)", [draft-ietf-mipshop-hmipv6-04](#), December 2004.
- [MIP6] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [NDIS] T. Narten, E. Nordmark, W. Simpson, H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", [draft-ietf-ipv6-2461bis-01](#), October 2004.
- [SEND] J. Arkko, J. Kempf, B. Sommerfield, B. Zill, P. Nikander, Secure Neighbor Discovery (SEND), [draft-ietf-send-ndopt-06](#), July, 2004.
- [TERM] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[12.](#) Informative References

- [CIP] A. Valko, "Cellular IP: A New Approach to Internet Host Mobility", ACM Computer Communication Review, January 1999.
- [HAWAII] R. Ramjee, K. Varadhan, L. Salgarelli, S. Thuel, S.Y. Wang, T. La Porta, "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-Area Wireless Networks," IEEE/ACM Transactions on Networking, , Vol 10, No. 3, June, 2002.
- [HBP] P. Muta and C. Castelluccia, "Hash-Based Paging and Location Update Using Bloom Filters", ACM/Kluwer Journal on Mobile Networks and Applications, (MONET), Vol. 10, No. 2, December 2004.
- [TOMOP] L. Peters, I. Moerman, B. Dhoedt, P. Demeester, "Influence of the Topology on the Performance of Micromobility Protocols", Proceedings of WiOpt'03, March 2003, Sophia Antipolis, France.
- [MIPS] D. Saha, A. Mukherjee, I. Misra, M. Chakraborty, N. Subhash, "Mobility Support in IP: A Survey of Related Protocols", IEEE Network, Vol. 18 No. 6, November 2004.

[Paging] J. Kempf, "Dormant Mode Host Alerting ("IP Paging") Problem Statement", [RFC 3132](#), June 2001.

[13.](#) References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.

Haddad, et al.

Expires January 18, 2006

[Page 26]

Internet-Draft

OMM

July 2005

Authors' Addresses

Wassim Haddad
Ericsson Research
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 #2334
Email: Wassim.Haddad@ericsson.com

Suresh Krishnan
Ericsson Research
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Email: Suresh.Krishnan@ericsson.com

Hesham Soliman
Flarion

Email: H.Soliman@flarion.com

Greg Daley
Monash University CTIE
Centre for Telecommunications and Information Engineering
Department of Electrical and Computer Systems Engineering
Monash University, Clayton, Victoria 3800
Australia

Phone: +61 3 9905 4655
Email: Greg.Daley@eng.monash.edu.au

Hannes Tschofenig
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany

Email: Hannes.Tschofenig@siemens.com

Haddad, et al.

Expires January 18, 2006

[Page 27]

Internet-Draft

OMM

July 2005

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of

such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.