

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 28, 2008

D. Damic
D. Premec
B. Patil
M. Sahasrabudhe
Nokia Siemens Networks
S. Krishnan
Ericsson
February 25, 2008

Proxy Mobile IPv6 indication and discovery
draft-damic-netlmm-pmip6-ind-discover-03.txt

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/1id-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 August 28, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

Proxy Mobile IPv6 is a network-based mobility protocol that enables mobility management for an IP host as it moves across different points of attachment within the mobility domain. An IP host whose mobility is being managed by the network is unaware of the access

Internet-Draft [draft-damic-netlmm-pmip6-ind-discover](#)

February 2008

networks capability to do mobility management on its behalf using Proxy Mobile IPv6. This draft proposes mechanisms by which the host is informed of Proxy Mobile IPv6 support, as well as how to actively discover such capability in the network that host attaches to. The ability of the host to discover or be aware of Proxy Mobile IPv6 support in the access network enables better decision making in terms of the network selection and attach procedure as well as the choice of mobility management.

Table of Contents

1.	Introduction and Scope	3
2.	Terminology	4
3.	Problem Statement	4
4.	Proposed Solutions	5
4.1.	PMIP6 indication in the Router Advertisement	5
4.2.	Alternate Prefix Information Option	6
4.3.	Router Solicitation Client-based Mobility Flag	9
4.4.	DHCPv6 extensions	10
4.4.1.	Home Network Identifier Option	10
4.4.2.	Home Network Information Option	12
4.4.3.	Note on DHCPv4	13
5.	Security Considerations	13
6.	IANA Considerations	13
7.	Acknowledgements	13
8.	References	14
8.1.	Normative References	14
8.2.	Informative References	14
	Authors' Addresses	15
	Intellectual Property and Copyright Statements	17

1. Introduction and Scope

Proxy Mobile IPv6 [[I-D.ietf-netlmm-proxymip6](#)] is a network-based mobility management protocol which does not require any signaling from the mobile node to enable IP mobility as the node moves and changes its point of attachment. PMIP6 is based on Mobile IPv6 [[RFC3775](#)] principles albeit the fact that the host is not involved in the mobility management. A Mobile IPv6 capable host may choose not to have the network perform mobility management on its behalf, via Proxy Mobile IPv6, in some scenarios.

PMIP6 protocol as specified in [[I-D.ietf-netlmm-proxymip6](#)] is applicable within the scope of a single PMIP6 domain. However deployment scenarios may include a broader scope than a single domain.

Scenarios where mobility is managed by the network are usually referred to as running in Proxy MIP (PMIP) mode. Analogously, when mobile nodes manage mobility themselves we are talking about host-based mobility. There are several scenarios in which host-based Mobile IP and Proxy MIP support co-exist in the same network. Two cases are described below, and a more exhaustive interactions analysis can be found in [[I-D.giaretta-netlmm-mip-interactions](#)]:

- o Simultaneous support for different mobility modes:
The operator may need to support mobility services for hosts which may not include MIP client functionality, as well as those implementing Mobile IP within the same PMIP6 domain. Discovery of the capabilities of the host and the network enables appropriate services to be triggered for all types of hosts.
- o Session continuation accros different domains:
Mobile node roaming in/out of the PMIP6 domain aims to continue the ongoing session either retaining or substituting the assigned mobility mode. For example, MN running a MIP6 session in the network moves to a PMIP6-enabled domain. Depending on the privileges and policies, the session may either continue by using

host-based mobility, or the network would take over the mobility management and begin handling the MN in the PMIP6 mode.

Existing IPv6 mechanisms, such as Neighbor Discovery protocol (NDP) or DHCPv6, are currently insufficient for the purpose of mobility mode detection or capability negotiation. This document proposes means by which the network can advertise PMIP6 capability and service being provided in the network, and provide specific configuration parameters to mobile nodes. The proposal also provides a method by which the MN can proactively participate in mobility mode selection by sending the explicit mode indication.

[2.](#) Terminology

The keywords "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](#)].

PMIP6 prefix

Prefix assigned to the MN while residing within the PMIP6 domain. The prefix is topologically anchored at the LMA, thus providing IP session continuity all throughout that LMA domain. Depending on the mobility scope, this prefix can be assigned by the LMA or some other mechanism.

Local (on-link) prefix

Topologically correct IPv6 prefix available for address autoconfiguration within the local domain, for example valid within a scope of a single AR/MAG.

[3.](#) Problem Statement

A host which attaches to a network which is a part of a PMIP6 domain may use stateless address autoconfiguration (SLAAC) or DHCPv6 to configure its addresses. The type of prefix advertised to the host or configuration parameters returned to it may vary depending on variables such as policy, host preference, host capability etc.

In case PMIP6 is used as a mechanism for managing mobility or for emulating the home link to the MN, the network obtains the home

prefix for the MN and provides the same to the MN. Prefix is assigned to the MN for the entire session, and must be consistently advertised throughout the entire PMIP6 domain. For MIP6 capable nodes it is sufficient to supply any globally routable local prefix/address that the MN will use to configure the care-of address (CoA) on its interface.

At the point when network allocates the address/prefix for the given mobile, or the Access Router begins advertising the specific IPv6 prefix information the network is unaware of the capability of the MN which is attempting to attach to the AR:

NDP and DHCP messages as defined today cannot serve as specific PMIP6 mobility triggers. Furthermore, the profile associated with a user in AAA is not sufficient for deciding about the mobility protocol for that MN as the device and terminal capabilities may change. For example: Profile or policy parameters associated with a subscriber authorizing PMIP6 service cannot be used in triggering network mobility since the capability of the host or preference cannot be determined.

The AR or MAG in the access network should anticipate different types of IPv6 mobility services and terminals, and make sure the correct service is assigned to the mobile node. The network should take into account mobility preference of the mobile, in case such information is provided beforehand, in the router solicitation (RS) or a DHCP request.

Explicit mechanisms and protocol extensions are needed to:

- o enable the access network to advertise the PMIP6 support to the MN
- o provide the MN with more reliable parameters allowing it to choose the mobility protocol based on its capabilities or other criteria
- o allow MNs to indicate their mobility mode preferences

4. Proposed Solutions

This document proposes extensions to the NDP and DHCPv6 protocols that may serve as triggers for PMIP6 mobility selection. The proposed extensions include: a new indication flag in the RA, new prefix information option for the Router Advertisement, flag extension to the Router Solicitation messages, as well as modifications for the related DHCPv6 MIP6 bootstrap extensions.

4.1. PMIP6 indication in the Router Advertisement

As per [\[RFC5075\]](#) the AR should use the Flags Expansion option to further extend the flags field of the Router Advertisement message. This memo proposes the AR SHOULD use this RA expansion option to explicitly indicate mobility management capabilities of the access network. By setting the "N" flag in the Flags Expansion option, AR advertises its capability for network-based mobility management (i.e., PMIP6 support).

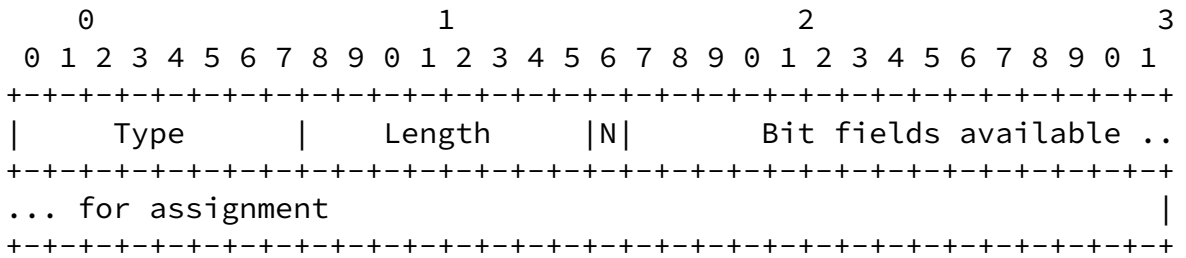


Figure 1. RA Flags Expansion option with the PMIP6 indication

Type

Type - 8-bit identifier of the option type

To be assigned by IANA, as indicated in [[RFC5075](#)]

Length

Length = 1; The length MUST be checked when processing the option in order to allow for future expansion of this option if the need arises.

Bits

Router Advertisement bit 8 - the "N" flag

(To be assigned by IANA.) This bit is set by the AR to indicate

the access network supports network-based mobility management, i.e., PMIP6. Other bits are available for further assignment.

4.2. Alternate Prefix Information Option

The AR is allowed to include multiple IPv6 prefixes in the single RA message where each prefix is contained in an own Prefix Information Option [RFC4861]. In case the access network supports PMIP6, the AR MAY chose to simultaneoulsy advertise local on-link IPv6 prefixes, as well as the individual PMIP6 prefix for that MN. For this specific case, the two different types of prefixes SHOULD be cleary differentiated.

The Alternate Prefix Information Option shall provide host with additional prefix information for the purpose of stateless IPv6 address autoconfiguration. In case the network supports multiple mobility service types, the AR may provide alternative option to the mobile node leaving the choice of the mobility service to the terminal.

In order to make use of the service indication and selection, the MN has to be enhanced for processing of the new Alternate Prefix Information option. Mobile nodes that are capable of processing the Alternate Prefix Information option should use the obtained information according to internal configuration and policy to decide whether to configure PMIP6 MN-HoA or MIP6 CoA on its network interface. Node incapable of understanding the Alternate Prefix option SHALL ignore it.

The format of the option supports regular operation and backwards compatibility for all legacy terminals by allowing flexibility in prefix assignment. Depending on the network policy and capabilities, the AR can advertise on-link prefixes, or the PMIP6 prefix as default

information within the Prefix Information Option. By specifying the Prefix Type, the alternative prefix information can then be provided in the new option.

[illegible]

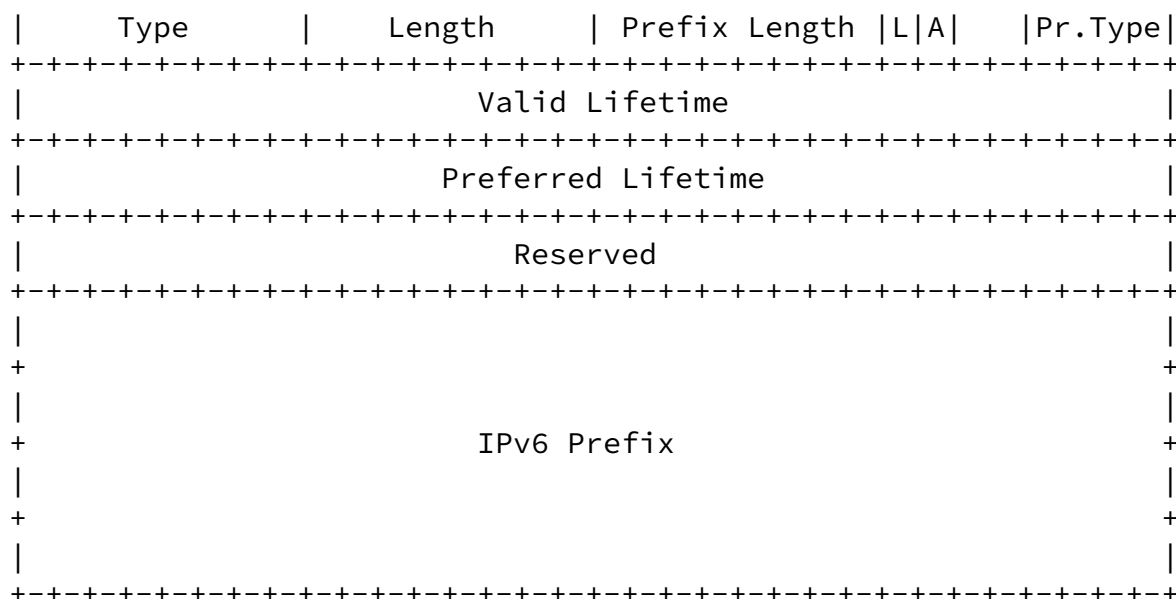


Figure 2. Alternate Prefix Information Option

Fields:

Type

8-bit identifier for the Alternate Prefix Information option (to be assigned by IANA).

Length 4

Prefix Length

8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

L

1-bit on-link flag. Use of the flag as defined in [RFC4861]: When set, indicates this prefix can be used for on-link determination, when not set the advertisement makes no statement about on-link or off-link properties of the prefix. .

1-bit autonomous address-configuration flag. When set indicates that this prefix can be used for stateless address configuration as specified in [[RFC4862](#)].

Prefix Type

4-bit unsigned field. The field indicates the type of the prefix provided in the payload. Allowed values:

- 0 On-link IPv6 prefix bound to the first hop AR
- 1 PMIPv6 prefix anchored at the associated LMA

Valid Lifetime

32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity. The Valid Lifetime is also used by [[RFC4862](#)].

Preferred Lifetime

32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. A value of all one bits (0xffffffff) represents infinity. See [[RFC4862](#)].

Reserved

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

IPv6 Prefix

An IPv6 address or a prefix of an IPv6 address. The length of the prefix is given by the Prefix Length field, and the purpose of the prefix is defined by the Prefix Type field. A router SHOULD NOT send a prefix option for the link-local prefix and a host SHOULD ignore such a prefix option.

Description:

The Alternate Prefix Information option provides host with an additional prefix information for stateless address autoconfiguration. Respective of the prefix already provided in the regular Prefix, this option may contain either the topologically

correct on-link prefix (type set to 0), or the PMIPv6 prefix (type 1) for the purpose of establishing network-based mobility management. The option appears in Router Advertisement packets only and MUST be silently ignored for other messages.

[4.3.](#) Router Solicitation Client-based Mobility Flag

If a mobile node that chooses or prefers to do its own mobility signaling enters a PMIPv6 network it cannot do so since the PMIP domain makes the MN believe that it is in fact in its home network. This section describes a mechanism by which a mobile node in a PMIPv6 network can signal to the PMIPv6 network whether it would like to make use of the Proxy Mobility service or not. This document modifies the format of the Router Solicitation Message specified in [\[RFC4861\]](#) to include a new client-based mobility flag. As a result of this the router solicitation message format will look like the following figure:

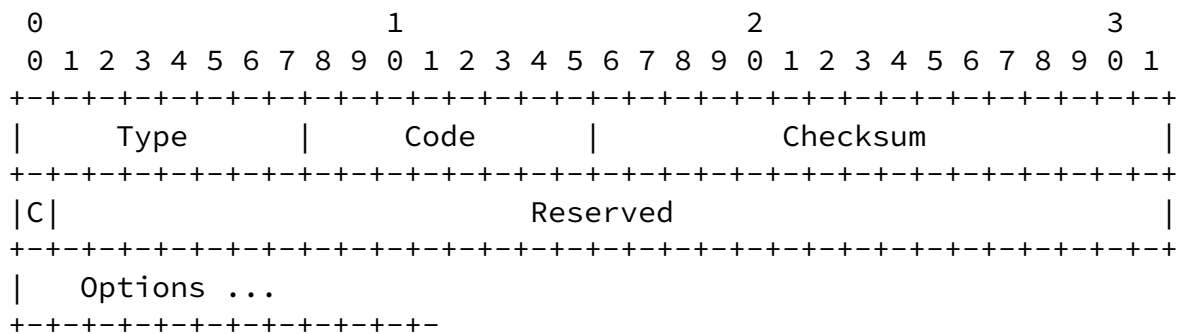


Figure 3. Client-based mobility flag in the Router Solicitation

ICMP Fields:

Type 133

Code 0

Checksum

The ICMP checksum. See [\[RFC4443\]](#)

C

If this bit is set, it means that the sending MN would like to perform its own signaling.

Internet-Draft [draft-damic-netlmm-pmip6-ind-discover](#) February 2008

Reserved

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

A mobile node that utilises this mechanism and wants to perform its own signaling, MUST set the C bit to one. The MAG that receives it SHOULD respond with a Router Advertisement containing a topologically correct prefix for the link (i.e., Not the emulated PMIPv6 prefix). MNs which are not aware of this specification will not set the C bit and hence the MAG would provide them with proxy mobility service. MAGs not aware of this bit when a client sets the C bit to 1 will ignore it as specified in [[RFC4861](#)]. Hence there are no backward compatibility issues

[4.4.](#) DHCPv6 extensions

This section describes how a mobile node can use DHCP [[RFC3315](#)] to detect that it is located in the PMIP domain and to inform the AR of its preference to use PMIPv6 or host-based MIPv6 as a mobility management protocol.

By using DHCP, mobile node and the AR are able to exchange following information:

- o AR can let the mobile node know that the access network supports the PMIPv6 protocol
- o AR can inform the mobile node of the PMIPv6 prefix
- o mobile node can inform the AR wheather it should provide a PMIPv6 service to it or if the MN prefers to run MIPv6 by itself

Draft [[I-D.ietf-mip6-hiopt](#)] defines new DHCPv6 options used to facilitate bootstrapping of a MIPv6 based mobility service. One of the options introduced by the draft is a Home Network Identifier option (OPTION_MIP6-HNID) by which the mobile node can request information about the home network and indicate its preference for the location of the HA: in the visited network or in the target network.

[4.4.1.](#) Home Network Identifier Option

The Home Network Identifier option is extended with an additional code to allow the mobile node to explicitly request information about the availability of the PMIP service at its current point of attachment.

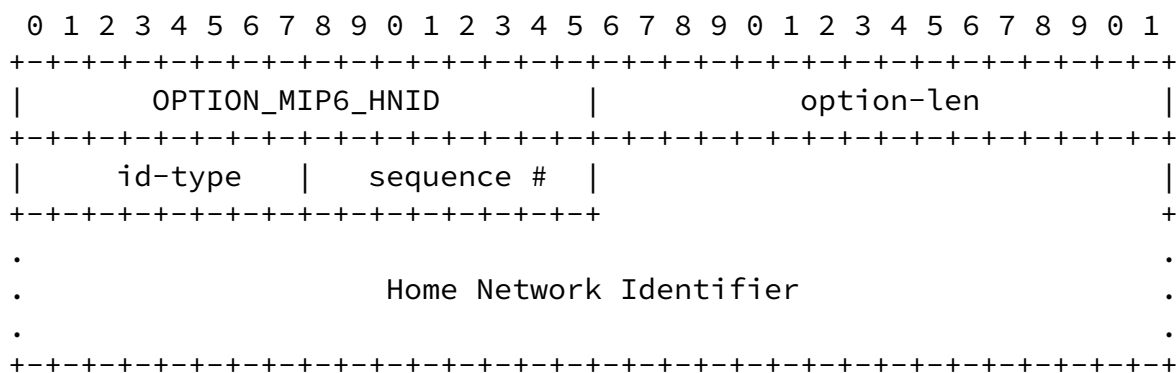


Figure 4. Home Network Identifier option format

option-code

OPTION_MIP6-HNID (TBD)

option-len

Total length of the option in octets

id-type

The type of Home Network Identifier:

- 0 Visited domain (local ASP)
- 1 The target network
- 2 No preference
- 3 PMIP domain

When the mobile node wants to learn if the access network supports PMIP6 service, it SHALL include Home Network Option setting the id-type field to 3. When the id-type is set to 3, the Home Network

Identifier field MAY be set to 0 if the mobile node wants to learn about the PMIP6 support in the local domain. Alternatively, if the mobile node wants to inquire about the support for PMIP6 service in a particular network, the mobile node MAY set the Home Network Identifier field to the network realm as FQDN.

The mobile node can learn information about a particular network type by sending separate Information Request messages with different id-types. If the mobile node wants to acquire the information about the visited network, target network and the PMIP6 domain in a single message exchange, it MAY include several Home Network Identifier options in the request message. There may be several Home Network Identifier options with the id-type 1 and/or 3 in a single message.

[4.4.2.](#) Home Network Information Option

Draft [[I-D.ietf-mip6-hiopt](#)] defines a new DHCPv6 option Home Network Information option. This option is used by the DHCP server to convey to the mobile node information about inquired network(s). The information provided could be a home subnet prefix (one or more), home agent address(es) and home agent FQDN(s). There is a separate suboption for each type of information provided (prefix, home agent address and home agent FQDN).

If the id-type field of the Home Network Identifier option indicates the network which is not supported by this access network or if the mobile node is not authorized for the requested network, the DHCP server's response SHALL include the Home Network Information option with the option-len set to zero.

If the mobile node inquired information about the PMIP domain, the relevant information about the PMIP domain will be provided in the Home Network Information option. In this case the only relevant information is prefix. Since in PMIP mode the mobile node does not interact with the home agent directly, home agent's address and FQDN SHALL not be provided to the mobile node.

If the access network wants to force the PMIP mode for the mobile node, it MAY respond to both visited domain and target domain(s)

inquiries with a Home Network Information option containing the 0-length data.

[4.4.2.1.](#) Avoiding the premature prefix advertisement

When the netlmm domain supports the DHCP extensions specified here, the AR may want to defer advertisement of the prefix until both the mobile node and network have exchanged their capabilities and preferences for a mobility management mode. This can be achieved by setting the 'M' or 'O' flag in Router Advertisement message forcing the mobile node to use DHCP. In this way the AR can delay the prefix advertisement until the DHCP exchange is completed.

[4.4.2.2.](#) Choosing the PMIP mode

If the client decides that it would use PMIP6 service offered by the access network, it SHALL send the (additional) Information Request message containing Home Network Information sub-option with the Home Network Information field containing the PMIP network prefix.

[4.4.3.](#) Note on DHCPv4

Home Network Identifier option and Home Network Information option defined for DHCPv6 could be adopted, with some modifications, for DHCPv4. This would enable the single stack IPv4 host to become aware of the PMIP service support by the access network. Whether the approach of adopting the DHCPv6 options for DHCPv4 is feasible in this particular case is for further study.

The IPv4 host would include the Home Network Identifier option, indicating its preferences, in the DHCPDISCOVER message. DHCPOFFER message would include Home Network Information option indicating the network type(s) supported by the access network and authorized for the mobile node. The mobile node would indicate its choice in the DHCPREQUEST message by including the Home Network Information option with the id-type field set to the selected network type.

[5.](#) Security Considerations

The mechanisms described in this document use neighbor discovery messages to communicate mobility preferences and indications between the MN and the network. An on-link attacker can send spoofed router advertisements and spoofed router solicitation in order to deny mobility service to the node. The usage of SEND [[RFC3971](#)] could prevent this from happening.

[6.](#) IANA Considerations

The following Extension Types MUST be assigned by IANA:

- o PMIP6 "N" indication flag in RA flags expansion option
- o Alternate Prefix Information Option type
- o Client-based mobility flag for RS message
- o DHCPv6 Home Network Information Option (id-type 3 PMIP)

[7.](#) Acknowledgements

TBD.

[8.](#) References

[8.1.](#) Normative References

[I-D.ietf-mip6-hiopt]

Jang, H., Yegin, A., Chowdhury, K., and J. Choi, "DHCP Options for Home Information Discovery in MIPv6", [draft-ietf-mip6-hiopt-11](#) (work in progress), February 2008.

[I-D.ietf-netlmm-proxymip6]

Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6",

[draft-ietf-netlmm-proxymip6-11](#) (work in progress),
February 2008.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", [RFC 4443](#), March 2006.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.
- [RFC5075] Haberman, B. and R. Hinden, "IPv6 Router Advertisement Flags Option", [RFC 5075](#), November 2007.

[8.2.](#) Informative References

- [I-D.giaretta-netlmm-mip-interactions]
Giaretta, G., "Interactions between PMIPv6 and MIPv6: scenarios and related issues",
[draft-giaretta-netlmm-mip-interactions-02](#) (work in progress), November 2007.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.

Authors' Addresses

Damjan Damic
Nokia Siemens Networks

Heinzelova 70a
Zagreb 10000
Croatia

Phone: +385 1 6331 337
Email: damjan.damic.ext@nsn.com

Domagoj Premec
Nokia Siemens Networks
Heinzelova 70a
Zagreb 10000
Croatia

Phone: +385 1 6105 923
Email: domagoj.premec.ext@nsn.com

Basavaraj Patil
Nokia Siemens Networks
6000 Connection Drive
Irving, TX 75039
US

Phone:
Email: basavaraj.patil@nsn.com

Meghana Sahasrabudhe
Nokia Siemens Networks
313 Fairchild Drive
Mountain View, CA 94043
US

Phone:
Email: meghana.sahasrabudhe@nsn.com

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

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

Internet-Draft [draft-damic-netlmm-pmip6-ind-discover](#) February 2008

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

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.

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, THE IETF TRUST 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.

Intellectual Property

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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).