MIP6 Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 23, 2008

H. Jang
A. Yegin
Samsung
K. Chowdhury
Starent Networks
J. Choi
Samsung

May 22, 2008

DHCP Options for Home Information Discovery in MIPv6
draft-ietf-mip6-hiopt-17.txt

Status of this Memo

Abstract

This draft defines a DHCP-based scheme to enable dynamic discovery of Mobile IPv6 home network information. New DHCP options are defined which allow a mobile node to request the home agent IP address, FQDN, or home network prefix and obtain it via the DHCP response.

Table of Contents

1. Introduction

Before a mobile node can engage in Mobile IPv6 signaling with a home agent, it should either know the IP address of the home agent via pre-configuration, or dynamically discover it. The Mobile IPv6 specification [RFC3775] describes how home agents can be dynamically discovered by mobile nodes that know the home network prefix. This scheme does not work when prefix information is not already available to the mobile node. One architecture to solve this problem is described in [I-D.ietf-mip6-bootstrapping-integrated-dhc]. This document specifies extensions to stateless DHCPv6 [RFC3736] [RFC3315] to deliver the home agent information to the mobile node in the form of the IP address of the home agent or the FQDN of the home agent. The information delivered to the mobile node may also include the home prefix for the mobile node. The solution involves defining a new DHCP option to carry home network prefix, home agent IP address and FQDN information. The mobile node MAY also use the home prefix to discover the list of home agents serving the home prefix using the Dynamic Home Agent Address Discovery mechanism specified in [RFC3775].

As part of configuring the initial TCP/IP parameters, a mobile node can find itself a suitable home agent. Such a home agent might reside in the access network that the mobile node connects to, or in a home network that the mobile node is associated with. A mobile node can indicate its home network identity when roaming to a visited network in order to obtain the MIP6 bootstrap parameters from the home network. As an example, the visited network may determine the home network of the mobile node based on the realm portion of the NAI (Network Access Identifier) [RFC4282] used in access authentication.

The mobile node may or may not be connected to the "home" network when it attempts to learn Mobile IPv6 home network information. This allows operators to centrally deploy home agents while being able to bootstrap mobile nodes that are already roaming. This scenario also occurs when HMIPv6 [I-D.ietf-mipshop-4140bis] is used, where the mobile node is required to discover the MAP (a special home agent) that is located multiple hops away from the mobile node's attachment point.

2. Terminology

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].

General mobility terminology can be found in [RFC3753]. The following additional terms, as defined in [RFC4640], are used in this document:

- Access Service Provider (ASP): A network operator that provides direct IP packet forwarding to and from the mobile node.

- Mobility Service Provider (MSP): A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile node must be authenticated and authorized to use the Mobile IPv6 service.

- Mobility Service Authorizer (MSA): A service provider that authorizes Mobile IPv6 service.

3. DHCP options for HA Dynamic Discovery

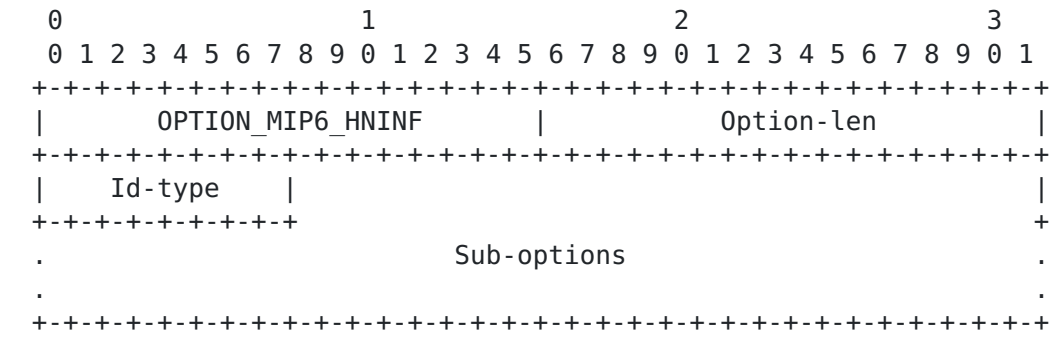
This section introduces new DHCP options and their sub-options which are used for dynamic discovery of the home agent's IPv6 address, IPv6 home network prefix, or FQDN information in Mobile IPv6. These options also carry an IPv4 address of the IPv6 home agent so that a mobile node can have access to Mobile IPv6 service over IPv4 as well. The detailed procedures are described in Section 2.3.2 of DSMIPv6 (Mobile IPv6 support for dual stack Hosts and Routers)[I-D.ietf-mip6-nemo-v4traversal].

The drafts [I-D.ietf-dime-mip6-integrated], [I-D.ietf-mip6-radius] and [I-D.ietf-mip6-bootstrapping-integrated-dhc] describe the complete procedure for home agent assignment among the mobile node, NAS (Network Access Server), DHCP and AAA entities for the bootstrapping procedure in the integrated scenario.

A NAS is assumed to be co-located with a DHCP relay agent or a DHCP server in this solution. In a network where the NAS is not co-located with a DHCP relay nor a server, the server may not be provided with the home network information from the NAS, and thereby it may either fail to provide information, or provide home information which has been preconfigured by the administrator or which is acquired through a mechanism that is not described in this document.

3.1. Home Network Information Option

This option is proposed to allow the exchange of home network information between the mobile node (DHCP client) and the DHCP server. It is used to indicate the target home network requested by the mobile node to the DHCP server in the Information-request message. In the Reply message, it conveys the home network information assigned by the DHCP server to the mobile node.



Option-code

OPTION_MIP6_HNINF (TBD)

Option-len

1 + length of Sub-options in units of octets.

Id-type

The type of Home Network Information.

0 Visited domain (local ASP)

1 Target MSP

2 No preference by the mobile node

Sub-options

A series of sub-options as specified in Section 3.3.

The Id-type in the request specifies the location of the home network requested by the mobile node as below:

- The Id-type 0 indicates the mobile node is interested in learning the home network information that pertains to the currently visited network. This type can be used to discover local home agents in the local ASP. In this case, the Option-len is set to 1.

- The Id-type 1 indicates the mobile node is interested in learning the home network information that pertains to the given realm. This type can be used to discover home agents that are hosted by a user's home domain or by any target domain. The option MUST carry a sub-option (defined in Section 3.3) whose Sub-opt-code is 1, which specifies the requested target MSP. The target MSP can be a mobile node's home MSP or any MSP which has a trusted roaming relationship with the mobile node's MSA.

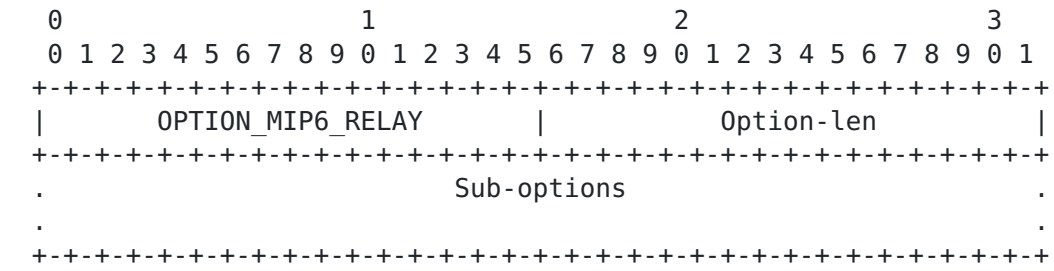
- If the mobile node has no preference, the Id-type is set to 2 and the Option-len field is set to 1. In this case, the assignment of the home network information is within the server's own discretion. For a detailed description, refer to Section 4.

The Id-type in the reply indicates the location of the home network information provided by the DHCP server which is carried in the following sub-options.

Multiple sub-options may exist in a Home Network Information option to carry more than one piece of home information.

3.2. MIP6 Relay Agent Option

This option carries the home network information for the mobile node (the NAS may know this, for instance, through AAA by using [I-D.ietf-mip6-radius] or [I-D.ietf-dime-mip6-integrated]) from the DHCP relay agent to the DHCP server. The DHCP relay agent sends this option to the DHCP server in the Relay-forward message.



Option-code

OPTION_MIP6_RELAY (TBD)

Option-len

The length of Sub-options in units of octets.

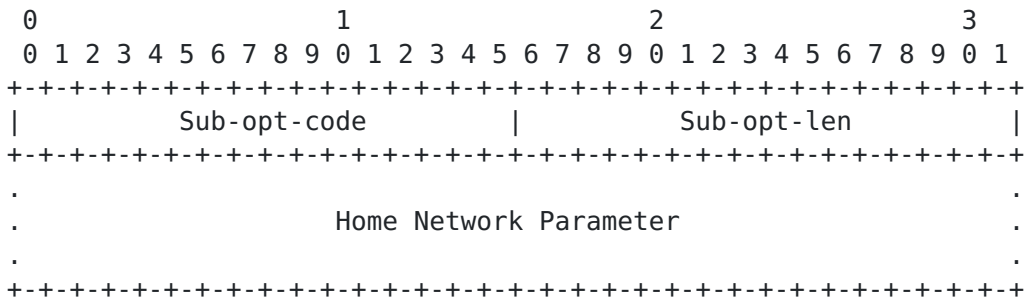
Sub-options

A series of sub-options as specified in Section 3.3.

Multiple sub-options may exist in a MIP6 Relay Agent option to carry more than one piece of home information.

3.3. Common Sub-options

This sub-option is a container for a home network parameter in the Home Network Information option or in the MIP6 Relay Agent option.



Sub-opt-code

A 16-bit unsigned integer for the type of the following Home Network Parameter field. Possible values are:

0 Reserved

1 Home network identifier

2 IPv6 home network prefix

3 IPv6 home agent address

4 IPv4 address of the IPv6 home agent

5 Home agent FQDN

6 .. (2^16-1) Reserved

Sub-opt-len

The length of the Home Network Parameter field in units of octets.

Home Network Parameter

The provided home network information according to the Sub-opt-code. This is encoded as specified below.

While the Sub-opt-codes 1, 2, 3, 4, and 5 are available in the MIP6 Relay Agent option and the Home Network Information option returned by the DHCP server, a value of 1 is the only Sub-opt-code available in the requesting Home Network Information option by the mobile node.

When the Sub-opt-code is set to 1 in the request, the Home Network Parameter field MUST contain an identifier to specify the home network requested by the mobile node. This field MUST be set in the form of a FQDN [RFC1035], encoded as specified in Section 8 of

[RFC3315]. This sub-option in the request SHOULD be copied into the Home Network Information option returned in the reply.

When the Sub-opt-code is set to 2, the Home Network Parameter field MUST include the 8-bit Prefix-Len followed by the 128-bit IPv6 Home Network Prefix. The Prefix-Len information indicates the number of leading bits in the IPv6 Home Network Prefix that are valid. The prefix information is provided so that the mobile node can perform dynamic home agent discovery as defined in [RFC3775]. The information may also be used to allow the mobile node to determine whether the home agent information received via DHCPv6 corresponds to a home agent on-link or not.

When the Sub-opt-code is set to 3, the Home Network Parameter field MUST contain the 128-bit IPv6 address of the home agent.

When the Sub-opt-code is set to 4, the Home Network Parameter field MUST contain the 32-bit IPv4 address of the IPv6 home agent.

When the Sub-opt-code is set to 5, it MUST contain the FQDN of the home agent as described in Section 8 of [RFC3315].

4. Option Usage

The requesting and sending of the proposed DHCP options follow the rules for DHCPv6 options in [RFC3315].

4.1. Mobile Node Behavior

A mobile node does not need to perform the home information discovery procedure after every change in attachment. It may try to perform the home network information discovery when it lacks home network information for MIPv6 or needs to change the home agent for some reasons, for example, to recover from the single point of failure of the existing home agent or to use the local home agent located in the network where the mobile node is currently attached. Note that despite the home information discovery procedure the mobile node may decide to keep the old home agent still in use afterwards, in order to avoid losing the current sessions.

For acquiring the home network information, a mobile node MUST send an Information-request message including the Home Network Information option according to the stateless DHCPv6 procedures [RFC3736][RFC3315]. The mobile node MUST also include the Option code for the Home Network Information option in the Option Request option in the request.

During the process of requesting the bootstrapping information, the mobile node MUST clarify its preference about the requested home network with the Id-type in the Home Network Information option. If it does not care about the location of the home network where the home agent is to be assigned, it MUST clarify that fact by setting the Id-type to 2. Id-type 2 means that the mobile node has no preferred home network and is willing to use any information provided by the DHCP server. Once it decides where the home agent is to be assigned, the specific information to be assigned depends mainly on the server's policy or the server's knowledge.

When the mobile node sets the Id-type to 1 in the request, it MUST include a sub-option with Sub-opt-code 1 which carries the FQDN of the target network such as "example.com". Note that a single Home Network Information option can carry at most one sub-option with Sub-opt-code 1.

The mobile node MUST NOT include a Home Network Information option whose Id-type is other than 0, 1, and 2 as defined as Section 3.1.

A value of 1 is the only Sub-opt-code available in the request.

The mobile node can request more than one instance of home

information by using multiple Home Network Information options in the request. For instance, if the mobile node wants to retrieve home network information from both the visited network (ASP) and the target MSP with a single transaction, it can request the information by using two Home Network Information options with Id-type 0 and Id-type 1. It can also request the home information for more than one target MSPs at the same time by including multiple Home Network Information options with Id-type 1. However, there MUST NOT be more than one Home Network Information option with Id-type 0 nor more than one Home Network Information option with Id-type 2 in the request.

On receiving the Reply message including a Home Network Information option, the mobile node SHOULD check whether the option is valid. It MUST ignore any option whose Id-type is other than 0, 1, and 2. It MUST also ignore any sub-option in the reply whose Sub-opt-code is other than 1, 2, 3, 4, and 5 as described in Section 3.3.

When the mobile node obtains a Home Network Information option with Id-type 1, it SHOULD check whether the returned option includes the home network identifier in its sub-options. If it is not provided in the sub-options, the Home Network Information option MUST be ignored and skipped. The home network identifiers provide a way to match the Home Network Information options in the request and the reply when the mobile node has sent the request with multiple Home Network Information options with the same Id-type 1 but with different home network identifiers.

As described later in Section 4.3, servers attempt to place multiple options and in the order of preference. When provided with multiple Home Network Information options having different id-types or with multiple sub-options for the same id-type, the mobile node SHOULD choose the first one that it can employ.

If the mobile node attempts to retrieve information in its current network but fails, it SHOULD employ previously retrieved information. If no information has been retrieved previously and there is no configuration that enables the mobile node to find and use a home agent, the mobile node SHOULD log an error and, depending on configured policy, revert to network access without a mobility protocol.

4.2. NAS/DHCP Relay Agent Behavior

As described in Section 3, a NAS is assumed to be co-located with a DHCP relay or a DHCP server. The NAS communicates with the mobile node during the network access authentication and typically also interacts with backend AAA systems. It is expected that the NAS is or becomes aware of the mobility related information for the mobile

node at this time using mechanisms such as Diameter attributes [I-D.ietf-dime-mip6-integrated] or RADIUS attributes [I-D.ietf-mip6-radius]. The NAS passes the information to the co-located DHCP relay agent or the server. The following describes the behavior of the DHCP relay agent when the NAS functions as a DHCP relay.

When receiving a DHCP message from the mobile node, the DHCP relay agent forwards the message to the All_DHCP_Servers multicast address, or other addresses configured by the network administrator as per [RFC3315]. If the relay determines that the NAS has passed home network information for this mobile node and has available home information for it, it SHOULD include the home network information in a MIP6 Relay Agent option, and attach this option in the Relay-forward message. When providing the home network information, the relay MUST include a sub-option whose Sub-opt-code is 1, and set the Home Network Parameter field to the FQDN of the network where the home information is assigned. That FQDN information will be compared with the target MSP requested by the mobile node when a DHCP server searches for the matching information.

The relay SHOULD include each home network parameter in a sub-option, and include all sub-options in a single MIP6 Relay Agent option. It MUST NOT include any sub-option whose Sub-opt-code is other than 1, 2, 3, 4, and 5 as described in Section 3.3.

In case the DHCP relay does not maintain any home network information for the requesting mobile node, it simply forwards the received message to the DHCP server according to the [RFC3315].

Upon receiving a Relay-reply message from the DHCPv6 server, the relay SHALL follow the guidelines defined in [RFC3315]. It extracts a Reply message from the Relay Message option in the Relay-reply message and relays it to the mobile node.

4.3. DHCP Server Behavior

When the server receives a Relay-forward message, it may include the MIP6 Relay Agent option in case there was home information available for the mobile node at the relay. The MIP6 Relay Agent option which does not include a sub-option with Sub-opt-code 1 MUST be ignored. Otherwise, the home network information received from the relay SHOULD be kept in the server so that the server can provide the information when it is requested by the mobile node. The server may carry this in the reply when the mobile node requested the home network information with an Id-type of 1.

The server MUST ignore any sub-option in a MIP6 Relay Agent option

whose Sub-opt-code is other than 1, 2, 3, 4, and 5, as described in Section 3.3.

When a DHCP server receives an Information-request message either directly or encapsulated in a Relay-forward message, it SHOULD check whether the Information-request includes the Home Network Information option. If the mobile node included a Home Network Information option and a Home Network Information option is requested by the Option Request option in the Information-request, the server MUST include a Home Network Information option in the Reply message.

The server MUST ignore any Home Network Information option in the request whose Id-type is other than 0, 1, and 2 as described in Section 3.1. It MUST also ignore any sub-option in the request whose Sub-opt-code is not 1.

It MUST construct the Home Network Information option(s) according to the following logic, and include it or them in the Reply. In case the Information-request message includes:

- A. Home Network Information option with Id-type 0

  The DHCP server MUST include each configured local home network parameter in a sub-option, and include all sub-options in a single Home Network Information option. It MUST set the Id-type to 0 in the Home Network Information option to be returned.

- B. Home Network Information option with Id-type 1

  Any Home Network Information option which carries more than one target MSP or which does not carry any target MSP MUST be ignored. Otherwise, the DHCP server searches its database by using the received target MSP as a key. If the DHCP server has home network information for the target MSP, it MUST include each home network parameter in a sub-option, and include all these sub-options in a single Home Network Information option. It MUST set the Id-type to 1 in the Home Network Information option to be returned, and copy the sub-option of the request which includes the target MSP into the Home Network Information option to be returned.

- C. Home Network Information option with Id-type 2

  In this case, the assignment of home information relies on the server's local policy, and the DHCP server is required to have its own policy so that it can reply with the proper information in the Home Network Information option. The policy can be determined based on several factors such as home agent availability and the authorization information of the mobile node. However, the specific policy setting is not in the scope of this document. For each instance of home network information selected, the DHCP server MUST include each home network parameter in a sub-option, and include all these sub-options in a Home Network Information option with Id-type 0 or 1 in the reply.

The server MUST NOT include a Home Network Information option in the reply whose Id-type is other than 0, 1, and 2. It also MUST NOT include a sub-option in the reply whose Sub-opt-code is other than 1, 2, 3, 4, and 5 as described in Section 3.3.

The Reply message can carry multiple Home Network Information options. The provided multiple options SHOULD be listed in order of preference. Multiple sub-options also SHOULD be listed in order of preference within a single Home Network Information option.

Note that there MUST NOT be more than one Home Network Information option with Id-type 0 nor more than one Home Network Information option with Id-type 2 in the reply. The value of Id-type 2 is valid in the reply only when the server received the option with Id-type 2 but has no data to be returned to the mobile node.

In case the server cannot find any home information, it must proceed as follows:

- For Id-type 0 or 2, it MUST return a Home Network Information option with the Id-type set to the requested Id-type and the Option-len set to 1.

- In case of Id-type 1 in the request, it MUST return a Home Network Information option by setting the Id-type to 1, include the Home Network Information sub-option with the target MSP, and set the Option-len to 1 + the length of this sub-option.

There is no requirement that the server return this option and its data in a Relay message as another Relay Agent option [RFC4580][RFC4649].

The DHCP server should provide all of the matching home information in Home Network Information option(s) based on its policy. While searching for the home network information by using the target MSP as a key, it may return the results when the key is partially matched. For example, on receipt of a Home Network Information option which specifies "xxx.example.com" as the target network, it may return the home network information assigned for "example.com" to the mobile node. Note that the detailed rule for returning partially matched instances of home network information follows the server's own policy and is outside the scope of this document.

There can be several ways that the DHCP server knows the requested home network information. For instance, as described in [I-D.ietf-mip6-radius] and [I-D.ietf-dime-mip6-integrated], a NAS can learn the information via RADIUS or Diameter, respectively, during network access authentication, and the DHCP relay co-located with the NAS can transfer it to the DHCP server by using the DHCP option specified in Section 3.2 and Section 3.3. Or the home information may have been configured statically in the DHCP server by the administrator. However, the mechanism by which the DHCP server is provisioned with the home network information or obtains it dynamically is outside the scope of this document.

5. Security Considerations

Secure delivery of home agent and home network information from a DHCP server to the mobile node (DHCP client) relies on the same security as DHCP. The particular option defined in this draft does not have additional impact on DHCP security.

Aside from the DHCP client to server interaction, an operator must also ensure secure delivery of mobile IP information to the DHCP server. This is outside the scope of DHCP and the newly defined option.

The mechanisms in this specification could be used by attackers to learn the addresses of home agents in the home network, or to feed incorrect information to mobile nodes.

The ability to learn addresses of nodes may be useful to attackers because brute-force scanning of the address space is not practical with IPv6. Thus, they could benefit from any means which make mapping the networks easier. For example, if a security threat targeted at routers or even home agents is discovered, having a simple mechanism to easily find out possible targets may prove to be an additional security risk.

Apart from discovering the address(es) of home agents, attackers will not be able to learn much from this information, and mobile nodes cannot be tricked into using wrong home agents, as the actual communication with the home agents employs mutual authentication.

The mechanisms from this specification may also leak interesting information about network topology and prefixes to attackers, and where there is no security to protect DHCP, even modify this information. Again, the mobile nodes and home agents employ end-to-end security when they communicate with each other. The authentic source of all information is that communication, not the information from DHCP.

However, attacks against the information carried in DHCP may lead to denial-of-service if mobile nodes are unable to connect to any home agent, or choose a home agent that is not the most preferred one.

6. IANA Consideration

IANA is requested to assign the following new DHCPv6 Option Codes, DHCPv6 Sub-option Codes, and Id-type Codes in the registry maintained in http://www.iana.org/assignments/dhcpv6-parameters:

IANA is requested to assign the following new DHCPv6 Option Codes:

- OPTION_MIP6_HNINF for the Home Network Information option
- OPTION_MIP6_RELAY for the MIP6 Relay Agent option

The Sub-option Codes for the Home Network Information option and the MIP6 Relay Agent option share a common namespace, and should be placed under the same registry. These Sub-option Codes should be placed in a new name space "DHCPv6 Mobile IPv6 Sub-option Codes".

o Reserved	0
o Home network identifier	1
o IPv6 Home network prefix	2
o IPv6 Home agent address	3
o IPv4 address of the IPv6 home agent	4
o Home agent FQDN	5
o Reserved	6 .. (2^16-1)

IANA is requested to create a new registry for the Home Network Information Option Id-type Codes.

o Visited domain (local ASP)	0
o Target MSP	1
o No preference by the mobile node	2

New Codes for these name spaces can be allocated using Standards Action or IESG approval according to [RFC2434].

7. Acknowledgments

The authors would like to thank Kilian Weniger, Domagoj Premec, Basavaraj Patil, Vijay Devarapalli, Gerardo Giaretta, Bernie Volz, David W. Hankins, Behcet Sarikaya, Vidya Narayanan, Francis Dupont, Sam Weiler, Jari Arkko, Alfred Hoenes, Suresh Krishnan, and Miguel A. Diaz for their valuable feedback.

8. References

8.1. Normative References

[I-D.ietf-mip6-bootstrapping-integrated-dhc]
Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-06 (work in progress), April 2008.

[I-D.ietf-mip6-nemo-v4traversal]
Soliman, H., "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mip6-nemo-v4traversal-06 (work in progress), November 2007.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[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.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC4580] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option", RFC 4580, June 2006.

[RFC4649] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option", RFC 4649, August 2006.

8.2. Informative References

[I-D.ietf-dime-mip6-integrated]
Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", draft-ietf-dime-mip6-integrated-08 (work in progress), February 2008.

[I-D.ietf-mip6-radius]
Chowdhury, K., "RADIUS Mobile IPv6 Support", draft-ietf-mip6-radius-04 (work in progress), February 2008.

[I-D.ietf-mipshop-4140bis]
Castelluccia, C., "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", draft-ietf-mipshop-4140bis-02 (work in progress), April 2008.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC4640] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

Authors' Addresses

Heejin Jang
Samsung Advanced Institute of Technology
P.O. Box 111
Suwon 440-600
Korea

Email: heejin.jang@samsung.com

Alper E. Yegin
Samsung Electronics
Istanbul
Turkey

Email: a.yegin@partner.samsung.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
US

Email: kchowdhury@starentnetworks.com

JinHyeock Choi
Samsung Advanced Institute of Technology
P.O. Box 111
Suwon 440-600
Korea

Email: jinchoe@samsung.com

Full Copyright Statement

Intellectual Property