MIP6 Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 4, 2012

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

March 3, 2012

DHCP Options for Home Information Discovery in MIPv6
draft-ietf-mip6-hiopt-18.txt

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.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on September 4, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction 4
2. Terminology 5
3. DHCP options for Home Network/Agent Dynamic Discovery 6
3.1. MIP6 Home Network ID FQDN Option 6
3.2. Home Network Information Options 7
3.2.1. MIP6 Visited Home Network Information Option 7
3.2.2. MIP6 Identified Home Network Information Option . . . 7
3.2.3. MIP6 Unrestricted Home Network Information Option . . 8
3.3. MIP6 Home Network Prefix Option 8
3.4. MIP6 Home Agent Address Option 9
3.5. MIP6 Home Agent FQDN Option 10
4. Option Usage 11
4.1. Mobile Node Behavior 11
4.1.1. Requesting MIP6 configuration 11
4.1.2. Processing MIP6 configuration information 12
4.2. Relay Agent Behavior 13
4.3. DHCP Server Behavior 14
4.4. Home agent discovery using a Network Access Server 14
5. Security Considerations 16
6. IANA Consideration 17
7. Acknowledgments 18
8. References 19
8.1. Normative References 19
8.2. Informative References 19
Authors' Addresses 21

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 [RFC6275] 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. This document specifies extensions to 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 Fully-qualified Domain Name (FQDN) [RFC1035] 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 [RFC6275].

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 [RFC5447].

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 [RFC5380] 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 Home Network/Agent Dynamic Discovery

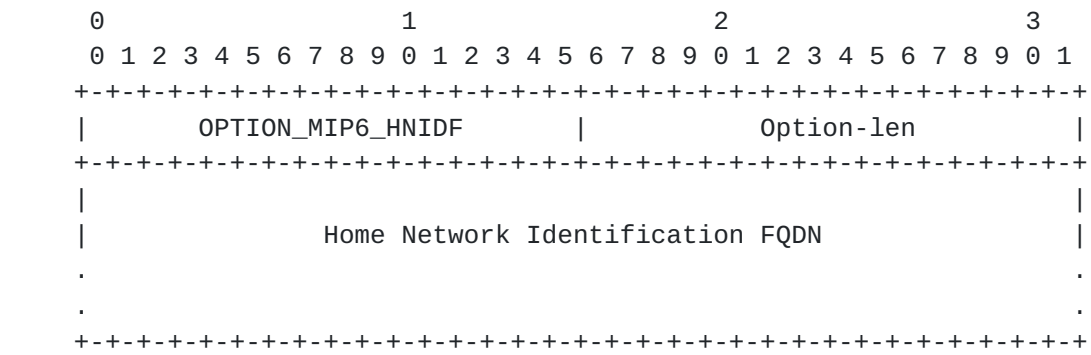
This section introduces new DHCP options which are used for dynamic discovery of the home agent's IPv6 address, IPv6 home network prefix, or FQDN information in Mobile IPv6. Transport to a home agent over IPv4 is also supported by specifying an IPv4-Embedded IPv6 address. The detailed procedures are described in Section 2.3.2 of Mobile IPv6 support for dual stack Hosts and Routers [RFC5555].

The names of options listed in this section all start with MIP6, in order to differentiate them from other DHCP options that might have similar names. However, throughout the rest of this document, the options are referred to by name without the MIP6 prefix, for brevity.

3.1. MIP6 Home Network ID FQDN Option

This option is used by mobile nodes to communicate to the DHCP server an FQDN that identifies the target home network for which the client is requesting configuration information. When the mobile nodes requests configuration for more than one target home network, this option is also used by the server to identify the target home network for each Identified Home Network Information option returned.

When a mobile node sends this option to request information about a specific home network, the option is simply included in the DHCP message from the mobile node. When a server responds with an Identified Home Network Information option, this option MUST be encapsulated in the Identified Home Network Information option that it identifies.



Option-code OPTION_MIP6_HNIDF (TBD)

Option-len Length of option, per RFC3315

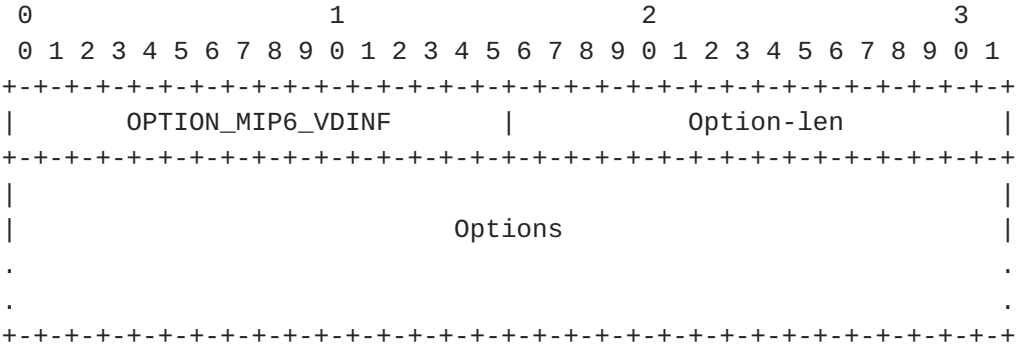
Home Network Identification FQDN A fully-qualified domain name that identifies a mobile IP home network for which the client is seeking configuration information. This is encoded in accordance with RFC3315, section 8, "Representation and Use of Domain Names."

3.2. Home Network Information Options

There are three different options that specify home network information. Which of these options is used depends on what kind of home network information the client needs. Each of these options is used to encapsulate options containing prefix and home agent information about the home network for which configuration information was requested.

3.2.1. MIP6 Visited Home Network Information Option

This option is used by relay agents and DHCP servers to provide information about the local home network.



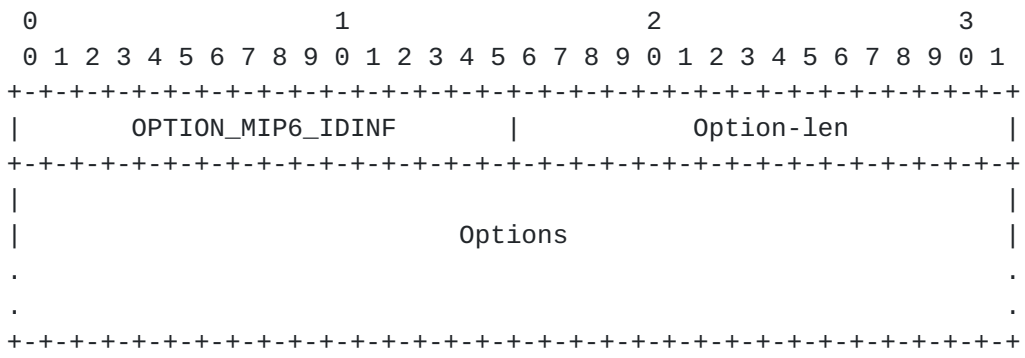
Option-code OPTION_MIP6_VDINF (TBD)

Option-len Length of option, per RFC3315

Suboptions One or more suboptions, specifying information about the local ASP (visited domain).

3.2.2. MIP6 Identified Home Network Information Option

This option is used by relay agents and DHCP servers to provide information about the the home network identified by a Home Network Identifier FQDN option.



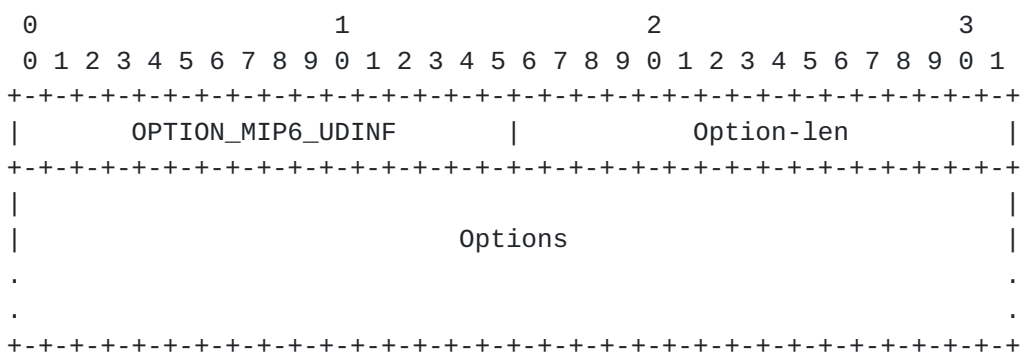
Option-code OPTION_MIP6_IDINF (TBD)

Option-len Length of option, per RFC3315

Suboptions One or more suboptions, specifying information about the home network identified by a Home Network Identifier FQDN option sent by a mobile node.

3.2.3. MIP6 Unrestricted Home Network Information Option

This option is used by relay agents and DHCP servers to provide information about the a home network specified by the DHCP server administrator.



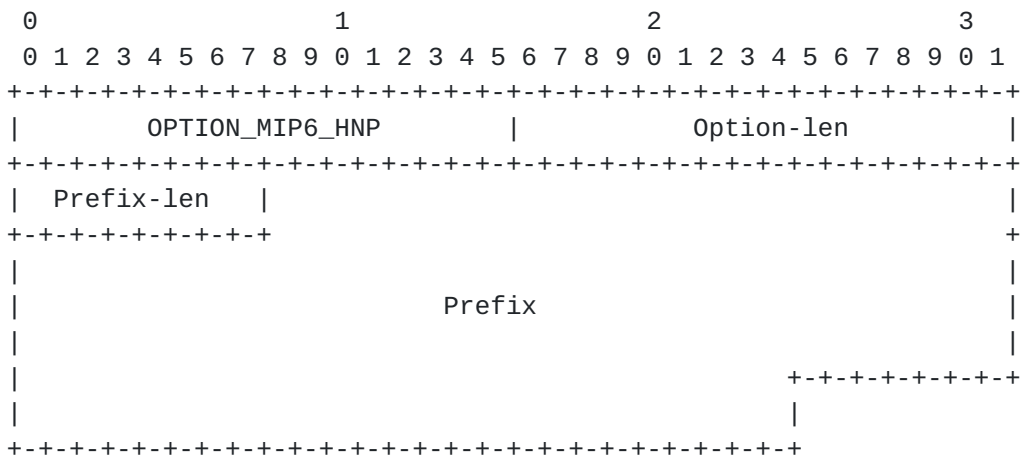
Option-code OPTION_MIP6_UDINF (TBD)

Option-len Length of option, per RFC3315

Suboptions One or more suboptions, specifying information about some home network as specified by the DHCP server administrator.

3.3. MIP6 Home Network Prefix Option

This option is used by DHCP servers and relay agents to define the prefix for a home network. This option should only appear in one of the Home Network Information options.



Option-code OPTION_MIP6_HNP (TBD)

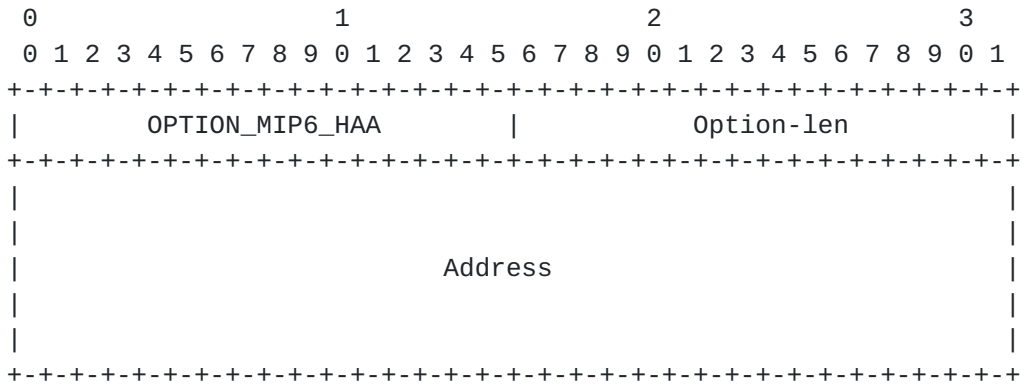
Option-len Length of option, per RFC3315

Prefix-len Length of prefix

Prefix Home Network Prefix

3.4. MIP6 Home Agent Address Option

This option is used by DHCP servers and relay agents to specify the home agent IP address. In cases where the home agent must be contacted over an IPv4-only infrastructure, the IPv4 address is specified as an IPv4-Embedded IPv6 address using the Well-Known prefix [RFC6052]. This option should only appear in one of the Home Network Information options.



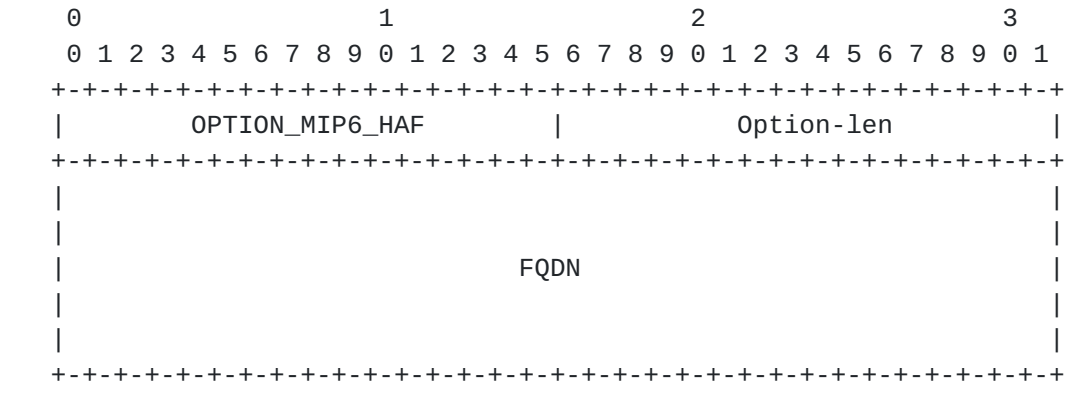
Option-code OPTION_MIP6_HAA (TBD)

Option-len Length of option, per RFC3315

Address IP Address of home agent

3.5. MIP6 Home Agent FQDN Option

This option is used by DHCP servers and relay agents to specify the home agent FQDN. This FQDN is used to look up one or more A or AAAA records containing IPv4 or IPv6 addresses for the home agent, as needed. This option should only appear in one of the Home Network Information options.



Option-code OPTION_MIP6_HAF (TBD)

Option-len Length of option, per RFC3315

Address FQDN resolving to one or more IPv4 and/or IPv6 addresses for the home agent. This is encoded in accordance with RFC3315, section 8, "Representation and Use of Domain Names."

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

Mobile nodes MAY obtain MIP6 configuration information either during a stateful configuration exchange [RFC3315] or a stateless configuration exchange [RFC3736].

Mobile nodes that obtain MIP6 configuration information using a stateful configuration exchange SHOULD include the same options in every message they send to the DHCP server.

Mobile nodes that obtain MIP6 configuration using a stateless exchange MAY omit MIP6 configuration from some exchanges, but SHOULD reconfigure whenever a change in the attached network is detected. If the DHCP server responds to a MIP6-related stateless configuration request with an Information Request Timer option, the mobile node SHOULD attempt to reconfigure when the IRT expires.

A mobile node using stateless configuration may try to perform home network information discovery when it lacks home network information for MIPv6 or needs to change the home agent for some reason. For example, this may be necessary to recover from the failure of an 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 continue to use the old home agent, in order to avoid losing current sessions.

4.1.1. Requesting MIP6 configuration

Mobile nodes signal that they are interested in being configured with MIP6 home agent information by requesting one or more of the three Home Network Information options--the Visited Home Network Information option, the Identified Home Network Information option, or the Unrestricted Home Network Information option. To request these options, the client lists them in the Option Request Option. A client that requests any of these three options in the ORO MUST also request the Home Network Identification FQDN option, the Home Network Prefix option, the Home Agent Address Option, and the Home Agent FQDN option.

If the mobile node requests the Visited Home Network Information option, this indicates that it 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.

If the mobile node requests the Identified Home Network Information option, this indicates that it is interested in learning the home network information that pertains to a specified realm. This type can be used to discover home agents that are hosted by a user's home domain or by any target domain. A mobile node requesting the Identified Home Network Information option MUST include a Client Home Network ID FQDN option identifying the MSP being identified. 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 as to the home network with which it should be configured, it SHOULD request the Unrestricted Home Network Information option, and SHOULD NOT request either the Visited Home Network Information option or the Identified Home Network Information option.

A client that wishes to be configured with both the Visited Home Network Information option and the Identified Home Network Information option may request both options in the Option Request Option. A client may request information about more than one identified domain by requesting the Identified Home Network Information option in the ORO and including more than one Home Network ID FQDN option. A client that sends more than one Home Network ID FQDN option MUST request the Home Network ID option in the ORO.

4.1.2. Processing MIP6 configuration information

DHCP Clients on mobile nodes should be prepared to receive any MIP6 Home Network Information options they request. If more than one Home Network ID FQDN option was sent, the client should be prepared to handle zero or more Identified Home Network Information options in response; the DHCP server may not have configuration information for all targeted domains, or, indeed, for any. If a misconfigured server returns an Identified Home Network option that does not contain a Home Network ID FQDN option corresponding to one that the client requested, the client MUST silently discard that Identified Home Network option.

If any of the three Home Network Information options is returned, configuration information will be included within it. The client must be prepared to handle home agent addresses either in the form of the Home Agent Address option or the Home Agent FQDN option.

If the client finds a v4-embedded IPv6 address in a Home Agent Address option, it may only use this address to communicate over

IPv4. If a Home Network Information option does not contain complete configuration information, the client MUST silently discard that Home Network Information option.

If the client receives any Home Network ID FQDN options, Home Network Prefix options, Home Agent Address options, or Home Agent FQDN options that are not encapsulated in one of the three types of Home Network Information options, it MUST silently discard these options.

The DHCP client must pass whatever configuration information it receives to the appropriate mobile IP implementation on the mobile node. How this is done, and what the mobile IP implementation on the mobile node does with this information, is outside the scope of this document.

As described later in this section, servers may provide more than one Home Network Information option, or multiple Home Agent Prefix, Home Agent Address or Home Agent FQDN options. When provided with multiple Visited Home Network Information options or Unrestricted Home Network Information options of the same type, or with multiple sub-options within such an option, the mobile node SHOULD choose the first one that it can employ.

If the DHCP client on a mobile node receives any MIP6 Home Network Prefix options, MIP6 Home Agent Address option, or MIP6 Home Agent FQDN option that are not contained within Home Network Information options, the DHCP client MUST silently discard these options.

4.2. Relay Agent Behavior

DHCP relay agents may in some cases have access to configuration information for the mobile node. In such cases, relay agents MAY send Visited Home Network Information options, Identified Home Network Information options, and/or Unrestricted Home Network Information options to the DHCP server. To do so, the Relay agent MUST encapsulate these options in a Relay Supplied Options option [RFC6422]. If the DHCP Relay Agent includes any Identified Home Network Information options, these options MUST correspond to home networks identified in Home Network ID FQDN options in the client request. In addition, each Identified Home Network option must contain a Home Network ID FQDN option identical to the one sent by the client, to identify the network to the client.

No special handling is required when processing relay-reply messages.

4.3. DHCP Server Behavior

DHCP servers generally can simply be configured with Visited Network Information options, Identified Network Information options, and Unrestricted Network Information options. In the case of Visited Network Information options and Unrestricted Network Information options, which clients get what options depends on operator configuration.

A DHCP server MAY maintain a table of Home Network ID FQDNs. For each such FQDN, a server that maintains such a table SHOULD include an Identified Network Information option. Such a server would look up the FQDN from any Home Network ID FQDN options provided by the client in its table, and for each match, include the Identified Network Information option configured in the table entry for that FQDN.

If a DHCP server does not implement the Home Network ID FQDN table, or some similar functionality, it is an error for the operator to configure it with any Identified Network Information options. These options could be erroneously forwarded to the client, which would have no use for them, and is required to discard them.

DHCP servers that implement the Home Network ID FQDN table must, when sending an Identified Network Information option to the client, include a Home Network ID option within the Identified Network Information option that identifies the home network for which configuration information is being sent.

Aside from the Home Network ID FQDN table, the actual behavior of the DHCP server with respect to MIP6 configuration is simply in accordance with the DHCPv6 protocol specification [RFC3315] and depends on operator configuration. No special processing is required for Visited Home Network Information options or Unrestricted Home Network Information options.

4.4. Home agent discovery using a Network Access Server

[RFC5447] describes 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.

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_HNIDF for the Home Network ID FQDN option
- OPTION_MIP6_VDINF for the Visited Home Network Information option
- OPTION_MIP6_IDINF for the Identified Home Network Information option
- OPTION_MIP6_UDINF for the Unrestricted Home Network Information option
- OPTION_MIP6_HNP for the Home Network Prefix option
- OPTION_MIP6_HAA for the Home Agent Address option
- OPTION_MIP6_HAF for the Home Agent FQDN option

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

[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.

[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.

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

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6422] Lemon, T. and Q. Wu, "Relay-Supplied DHCP Options", RFC 6422, December 2011.

8.2. Informative References

[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.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC5447] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for

Network Access Server to Diameter Server Interaction",
RFC 5447, February 2009.

Authors' Addresses

Heejin Jang
Samsung Electronics
416 Maetan-3dong, Yeongtong-gu
Suwon 443-742
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

Ted Lemon
Nominum
2000 Seaport Blvd
Redwood City, CA 94063
USA

Phone: +1 650 381 6000
Email: mellon@nominum.com