Homenet
Internet-Draft
Intended status: Standards Track
Expires: 4 May 2023

D. Migault
Ericsson
R. Weber
Akamai
T. Mrugalski
Internet Systems Consortium, Inc.
31 October 2022

DHCPv6 Options for Home Network Naming Authority
draft-ietf-homenet-naming-architecture-dhc-options-24

Abstract

This document defines DHCPv6 options so a Homenet Naming Authority (HNA) can automatically proceed to the appropriate configuration and outsource the authoritative naming service for the home network. In most cases, the outsourcing mechanism is transparent for the end user.

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 https://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 4 May 2023.

Copyright Notice

Copyright (c) 2022 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The reader should be familiar with [I-D.ietf-homenet-front-end-naming-delegation].

2. Introduction

[I-D.ietf-homenet-front-end-naming-delegation] specifies how an entity designated as the Homenet Naming Authority (HNA) outsources a Public Homenet Zone to an DNS Outsourcing Infrastructure (DOI).

This document describes how a network can provision the HNA with a specific DOI. This could be particularly useful for a DOI partly managed by an ISP, or to make home networks resilient to HNA replacement. The ISP delegates an IP prefix to the home network as well as the associated reverse zone. The ISP is thus aware of the owner of that IP prefix, and as such becomes a natural candidate for hosting the Homenet Reverse Zone - that is the Reverse Distribution Manager (RDM) and potentially the Reverse Public Authoritative Servers.

In addition, ISPs often identify the line of the home network with a name. Such name is used for their internal network management operations and is not a name the home network owner has registered to. ISPs may leverage such infrastructure and provide the home network with a specific domain name designated as per [I-D.ietf-homenet-front-end-naming-delegation] a Homenet Registered Domain. Similarly to the reverse zone, ISPs are aware of who owns that domain name and may become a natural candidate for hosting the Homenet Zone - that is the Distribution Manager (DM) and the Public Authoritative Servers.

This document describes DHCPv6 options that enable an ISP to provide the necessary parameters to the HNA, to proceed. More specifically, the ISP provides the Registered Homenet Domain, necessary information on the DM and the RDM so the HNA can manage and upload the Public Homenet Zone and the Reverse Public Homenet Zone as described in [I-D.ietf-homenet-front-end-naming-delegation].

The use of DHCPv6 options may make the configuration completely transparent to the end user and provides a similar level of trust as the one used to provide the IP prefix - when provisioned via DHCP.

3. Procedure Overview

This section illustrates how a HNA receives the necessary information via DHCPv6 options to outsource its authoritative naming service to the DOI. For the sake of simplicity, and similarly to [I-D.ietf-homenet-front-end-naming-delegation], this section assumes that the HNA and the home network DHCPv6 client are colocated on the Customer Edge (CPE) router [RFC7368]. Note also that this is not mandatory and the DHCPv6 client may instruct remotely the HNA with a protocol that will be standardized in the future. In addition, this section assumes the responsible entity for the DHCPv6 server is provisioned with the DM and RDM information - associated with the requested Registered Homenet Domain . This means a Registered Homenet Domain can be associated with the DHCPv6 client.

This scenario is believed to be the most popular scenario. This document does not ignore scenarios where the DHCPv6 server does not have privileged relations with the DM or RDM. These cases are discussed in Appendix A. Such scenarios do not necessarily require configuration for the end user and can also be zero-config.

The scenario considered in this section is as follows:

1. The HNA is willing to outsource the Public Homenet Zone or Homenet Reverse Zone. The DHCPv6 client is configured to include in its Option Request Option (ORO) the Registered Homenet Domain Option (OPTION_REGISTERED_DOMAIN), the Forward Distribution Manager Option (OPTION_FORWARD_DIST_MANAGER) and the Reverse Distribution Manager Option (OPTION_REVERSE_DIST_MANAGER) option codes.

2. The DHCPv6 server responds to the DHCPv6 client with the requested DHCPv6 options based on the identified homenet. The DHCPv6 client passes the information to the HNA.

3. The HNA is authenticated (see Section "Securing the Control Channel" of [I-D.ietf-homenet-front-end-naming-delegation]) by the DM and the RDM. The HNA builds the Homenet Zone (or the Homenet Reverse Zone) and proceed as described in [I-D.ietf-homenet-front-end-naming-delegation]. The DHCPv6 options provide the necessary non optional parameters described in Appendix B of [I-D.ietf-homenet-front-end-naming-delegation]. The HNA may complement the configurations with additional parameters via means not yet defined. Appendix B of [I-D.ietf-homenet-front-end-naming-delegation] describes such parameters that may take some specific non default value.

4. DHCPv6 Option

This section details the payload of the DHCPv6 options following the guidelines of [RFC7227].

4.1. Registered Homenet Domain Option

The Registered Domain Option (OPTION_REGISTERED_DOMAIN) indicates the FQDN associated with the home network.

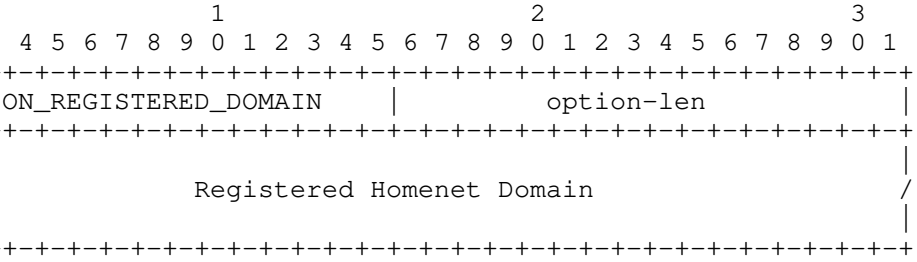

Figure 1: Registered Domain Option

* option-code (16 bits): OPTION_REGISTERED_DOMAIN, the option code for the Registered Homenet Domain (TBD1).

* option-len (16 bits): length in octets of the Registered Homenet Domain field as described in [RFC8415].

* Registered Homenet Domain (variable): the FQDN registered for the homenet encoded as described in Section 10 of [RFC8415].

4.2. Forward Distribution Manager Option

The Forward Distributed Manager Option (OPTION_FORWARD_DIST_MANAGER) provides the HNA with the FQDN of the DM as well as the transport protocols for the communication between the HNA and the DM. As opposed to IP addresses, the FQDN requires a DNS resolution before establishing the communication between the HNA and the DM. However, the use of a FQDN provides multiple advantages over IP addresses. Firstly, it makes the DHCPv6 Option easier to parse and smaller - especially when IPv4 and IPv6 addresses are expected to be provided. Then the FQDN can reasonably be seen as a more stable identifier than IP addresses, as well as a pointer to additional information that may be useful, in the future, to establish the communication between the HNA and the DM.

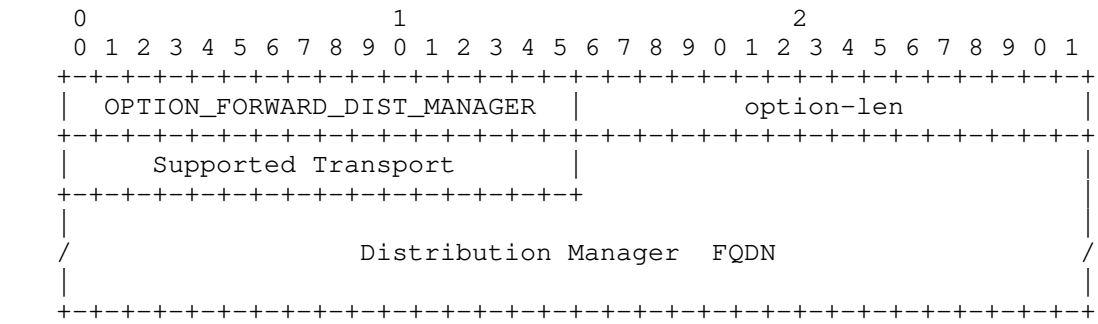

Figure 2: Forward Distribution Manager Option

* option-code (16 bits): OPTION_FORWARD_DIST_MANAGER, the option code for the Forward Distribution Manager Option (TBD2).

* option-len (16 bits): length in octets of the enclosed data as described in [RFC8415].

* Supported Transport (16 bits): defines the supported transport by the DM (see Section 4.4). Each bit represents a supported transport, and a DM MAY indicate the support of multiple modes. The bit for DNS over mutually authenticated TLS (DomTLS) MUST be set.

* Distribution Manager FQDN (variable): the FQDN of the DM encoded as described in Section 10 of [RFC8415].

It is worth noticing that the DHCP Option specifies the Supported Transport without specifying any explicit port. Unless the HNA and the DM have agreed on using a specific port - for example by configuration, or any out of band mechanism -, the default port is used and must be specified. The specification of such default port may be defined in the specification of the designated Supported Transport or in any other document. In the case of DNS over mutually authenticated TLS (DomTLS), the default port value is 853 as per DNS over TLS [RFC7858] and DNS Zone Transfer over TLS [RFC9103].

The need to associate in the DHCP Option the port value to each Supported Transport has been balanced with the difficulty of handling a list of tuples (transport, port) as well as the possibility to use a dedicated IP address for the DM in case the default port was already in use.

4.3. Reverse Distribution Manager Server Option

The Reverse Distribution Manager Option (OPTION_REVERSE_DIST_MANAGER) provides the HNA with the FQDN of the DM as well as the transport protocols for the communication between the HNA and the DM.

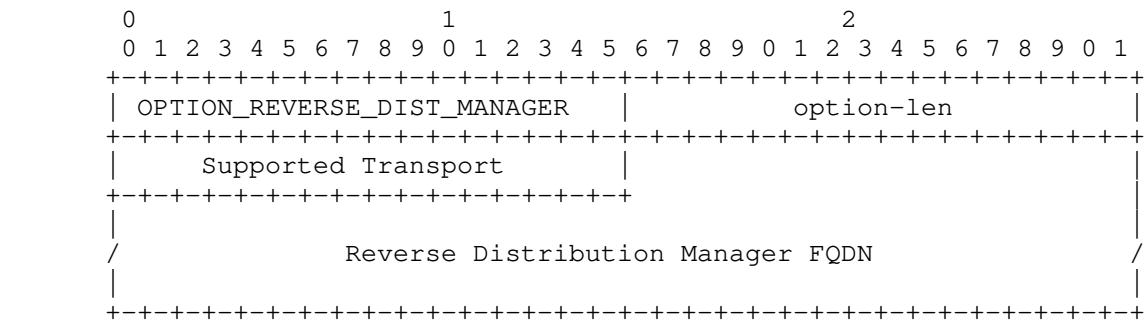

Figure 3: Reverse Distribution Manager Option

* option-code (16 bits): OPTION_REVERSE_DIST_MANAGER, the option code for the Reverse Distribution Manager Option (TBD3).

* option-len (16 bits): length in octets of the option-data field as described in [RFC8415].

* Supported Transport (16 bits): defines the supported transport by the RDM (see Section 4.4). Each bit represents a supported transport, and a RDM MAY indicate the support of multiple modes. The bit for DNS over mutually authenticated TLS [RFC7858] MUST be set.

* Reverse Distribution Manager FQDN (variable): the FQDN of the RDM encoded as described in section 10 of [RFC8415].

For the port number associated to the Supported Transport, the same considerations as described in Section 4.2 holds.

4.4. Supported Transport

The Supported Transport field of the DHCPv6 option indicates the supported transport protocols. Each bit represents a specific transport mechanism. A bit sets to 1 indicates the associated transport protocol is supported. The corresponding bits are assigned as described in Figure 4 and Section 6.

Bit Position left to right	Transport Protocol Description	Mnemonic	Reference
0	DNS over mutually authenticated TLS	DomTLS	This-RFC
1-15	unallocated	-	-

Figure 4: Supported Transport

DNS over mutually authenticated TLS (DomTLS): indicates the support of DNS over TLS [RFC7858], DNS Zone Transfer over TLS [RFC9103] as described in [I-D.ietf-homenet-front-end-naming-delegation].

5. DHCPv6 Behavior

5.1. DHCPv6 Server Behavior

Sections 17.2.2 and 18.2 of [RFC8415] govern server operation regarding option assignment. As a convenience to the reader, we mention here that the server will send option foo only if configured with specific values for foo and if the client requested it. In particular, when configured the DHCPv6 server sends the Registered Homenet Domain Option, Distribution Manager Option, the Reverse Distribution Manager Option when requested by the DHCPv6 client by including necessary option codes in its ORO.

5.2. DHCPv6 Client Behavior

The DHCPv6 client includes Registered Homenet Domain Option, Distribution Manager Option, the Reverse Distribution Manager Option in an ORO as specified in Sections 18.2.1, 18.2.2, 18.2.4, 18.2.5, 18.2.6, and 21.7 of [RFC8415].

Upon receiving a DHCPv6 option described in this document in the Reply message, the HNA SHOULD proceed as described in [I-D.ietf-homenet-front-end-naming-delegation].

5.3. DHCPv6 Relay Agent Behavior

There are no additional requirements for the DHCPv6 Relay agents.

6. IANA Considerations

6.1. DHCPv6 Option Codes

IANA is requested to assign the following new DHCPv6 Option Codes in the registry maintained in: https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2.

Value	Description	Client ORO	Singleton Option	Reference
TBD1	OPTION_REGISTERED_DOMAIN	Yes	No	[This-RFC] Section 4.1
TBD2	OPTION_FORWARD_DIST_MANAGER	Yes	Yes	[This-RFC] Section 4.2
TBD3	OPTION_REVERSE_DIST_MANAGER	Yes	Yes	[This-RFC] Section 4.3

6.2. Supported Transport parameter

IANA is requested to maintain a new registry of Supported Transport parameter in the Distributed Manager Option (OPTION_FORWARD_DIST_MANAGER) or the Reverse Distribution Manager Option (OPTION_REVERSE_DIST_MANAGER). The different parameters are defined in Figure 4 in Section 4.4.

The Name of the registry is: Supported Transport parameter

The registry description is: The Supported Transport field of the DHCPv6 option is a two octet field that indicates the supported transport protocols. Each bit represents a specific transport mechanism.

The parent grouping is Dynamic Host Configuration Protocol for IPv6 (DHCPv6) at https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2.

New entry MUST specify the bit position, the Transport Protocol Description a Mnemonic and a Reference as defined in Figure 5.

The initial registry is as specified in Figure 5.

Changes of the format or policies of the registry is left to the IETF via the IESG.

Future code points are assigned under RFC Required as per [RFC8126].

Bit Position left to right	Transport Protocol Description	Mnemonic	Reference
0	DNS over mutually authenticated TLS	DomTLS	This-RFC
1-15	unallocated	-	-

Figure 5: Supported Transport

7. Security Considerations

The security considerations in [RFC8415] are to be considered. The trust associated with the information carried by the DHCPv6 Options described in this document is similar to the one associated with the IP prefix - when configured via DHCPv6.

In some cases, the ISP MAY identify the HNA by its wire line, that is to say physically which may not require to rely on TLS to authenticate the HNA. As TLS is mandatory to be used, it is expected the HNA is provisioned with a certificate. In some cases, the HNA may use a self signed certificate.

8. Acknowledgments

We would like to thank Marcin Siodelski, Bernie Volz and Ted Lemon for their comments on the design of the DHCPv6 options. We would also like to thank Mark Andrews, Andrew Sullivan and Lorenzo Colliti for their remarks on the architecture design. The designed solution has been largely been inspired by Mark Andrews's document [I-D.andrews-dnsop-pd-reverse] as well as discussions with Mark. We also thank Ray Hunter and Michael Richardson for its reviews, its comments and for suggesting an appropriated terminology.

9. Contributors

The co-authors would like to thank Chris Griffiths and Wouter Cloetens that provided a significant contribution in the early versions of the document.

10. References

10.1. Normative References

[I-D.ietf-homenet-front-end-naming-delegation] Migault, D., Weber, R., Richardson, M., and R. Hunter, "Simple Provisioning of Public Names for Residential Networks", Work in Progress, Internet-Draft, draft-ietf-homenet-front-end-naming-delegation-22, 31 October 2022, <https://datatracker.ietf.org/api/v1/doc/document/draft-ietf-homenet-front-end-naming-delegation/>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC9103] Toorop, W., Dickinson, S., Sahib, S., Aras, P., and A. Mankin, "DNS Zone Transfer over TLS", RFC 9103, DOI 10.17487/RFC9103, August 2021, <https://www.rfc-editor.org/info/rfc9103>.

10.2. Informative References

[I-D.andrews-dnsop-pd-reverse]
Andrews, M., "Automated Delegation of IP6.ARPA reverse zones with Prefix Delegation", Work in Progress, Internet-Draft, draft-andrews-dnsop-pd-reverse-02, 4 November 2013, <https://www.ietf.org/archive/id/draft-andrews-dnsop-pd-reverse-02.txt>.

[I-D.sury-dnsext-cname-dname]
Sury, O., "CNAME+DNAME Name Redirection", Work in Progress, Internet-Draft, draft-sury-dnsext-cname-dname-00, 15 April 2010, <https://www.ietf.org/archive/id/draft-sury-dnsext-cname-dname-00.txt>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, DOI 10.17487/RFC2181, July 1997, <https://www.rfc-editor.org/info/rfc2181>.

[RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", RFC 6672, DOI 10.17487/RFC6672, June 2012, <https://www.rfc-editor.org/info/rfc6672>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <https://www.rfc-editor.org/info/rfc7227>.

[RFC7368] Chown, T., Ed., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", RFC 7368, DOI 10.17487/RFC7368, October 2014, <https://www.rfc-editor.org/info/rfc7368>.

Appendix A. Scenarios and impact on the End User

This appendix details various scenarios and discuss their impact on the end user. This appendix is not normative and limits the description of a limited scope of scenarios that are assumed to be representative. Many other scenarios may be derived from these.

A.1. Base Scenario

The base scenario is the one described in Section 3 in which an ISP manages the DHCPv6 server, the DM and RDM.

The end user subscribes to the ISP (foo), and at subscription time registers for foo.example as its Registered Homenet Domain foo.example.

In this scenario, the DHCPv6 server, DM and RDM are managed by the ISP so the DHCPv6 server and as such can provide authentication credentials of the HNA to enable secure authenticated transaction with the DM and the Reverse DM.

The main advantage of this scenario is that the naming architecture is configured automatically and transparently for the end user. The drawbacks are that the end user uses a Registered Homenet Domain managed by the ISP and that it relies on the ISP naming infrastructure.

A.2. Third Party Registered Homenet Domain

This appendix considers the case when the end user wants its home network to use example.com not managed by her ISP (foo) as a Registered Homenet Domain. This appendix still considers the ISP manages the home network and still provides foo.example as a Registered Homenet Domain.

When the end user buys the domain name example.com, it may request to redirect the name example.com to foo.example using static redirection with CNAME [RFC2181], [RFC1034], DNAME [RFC6672] or CNAME+DNAME [I-D.sury-dnsext-cname-dname]. The only information the end user needs to know is the domain name assigned by the ISP. Once the redirection has been configured, the HNA may be changed, the zone can be updated as in Appendix A.1 without any additional configuration from the end user.

The main advantage of this scenario is that the end user benefits from the Zero Configuration of the Base Scenario Appendix A.1. Then, the end user is able to register for its home network an unlimited number of domain names provided by an unlimited number of different third party providers. The drawback of this scenario may be that the end user still rely on the ISP naming infrastructure. Note that the only case this may be inconvenient is when the DNS servers provided by the ISPs results in high latency.

A.3. Third Party DNS Infrastructure

This scenario considers that the end user uses example.com as a Registered Homenet Domain, and does not want to rely on the authoritative servers provided by the ISP.

In this appendix we limit the outsourcing to the DM and Public Authoritative Server(s) to a third party. The Reverse Public Authoritative Server(s) and the RDM remain managed by the ISP as the IP prefix is managed by the ISP.

Outsourcing to a third party DM can be performed in the following ways:

1. Updating the DHCPv6 server Information. One can imagine a GUI interface that enables the end user to modify its profile parameters. Again, this configuration update is done once-for-ever.

2. Upload the configuration of the DM to the HNA. In some cases, the provider of the CPE router hosting the HNA may be the registrar and provide the CPE router already configured. In other cases, the CPE router may request the end user to log into the registrar to validate the ownership of the Registered Homenet Domain and agree on the necessary credentials to secure the communication between the HNA and the DM. As described in [I-D.ietf-homenet-front-end-naming-delegation], such settings could be performed in an almost automatic way as to limit the necessary interactions with the end user.

A.4. Multiple ISPs

This scenario considers a HNA connected to multiple ISPs.

Suppose the HNA has been configured each of its interfaces independently with each ISPS as described in Appendix A.1. Each ISP provides a different Registered Homenet Domain.

The protocol and DHCPv6 options described in this document are fully compatible with a HNA connected to multiple ISPs with multiple Registered Homenet Domains. However, the HNA should be able to handle different Registered Homenet Domains. This is an implementation issue which is outside the scope of the current document.

If a HNA is not able to handle multiple Registered Homenet Domains, the HNA may remain connected to multiple ISP with a single Registered Homenet Domain. In this case, one entity is chosen to host the Registered Homenet Domain. This entity may be one of the ISP or a third party. Note that having multiple ISPs can be motivated for bandwidth aggregation, or connectivity fail-over. In the case of connectivity fail-over, the fail-over concerns the access network and a failure of the access network may not impact the core network where the DM and Public Authoritative Primaries are hosted. In that sense, choosing one of the ISP even in a scenario of multiple ISPs may make sense. However, for sake of simplicity, this scenario assumes that a third party has been chosen to host the Registered Homenet Domain. Configuration is performed as described in Appendix A.2 and Appendix A.3.

With the configuration described in Appendix A.2, the HNA is expected to be able to handle multiple Homenet Registered Domain, as the third party redirect to one of the ISPs servers. With the configuration described in Appendix A.3, DNS zone are hosted and maintained by the third party. A single DNS(SEC) Homenet Zone is built and maintained by the HNA. This latter configuration is likely to match most HNA implementations.

The protocol and DHCPv6 options described in this document are fully compatible with a HNA connected to multiple ISPs. To configure or not and how to configure the HNA depends on the HNA facilities. Appendix A.1 and Appendix A.2 require the HNA to handle multiple Registered Homenet Domain, whereas Appendix A.3 does not have such requirement.

Authors' Addresses

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint Laurent, QC 4S 0B6
Canada
Email: daniel.migault@ericsson.com

Ralf Weber
Akamai
Email: ralf.weber@akamai.com

Tomek Mrugalski
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, 94063
United States of America
Email: tomasz.mrugalski@gmail.com