Stream: Internet Engineering Task Force (IETF)
RFC: 9527
Category: Standards Track
Published: January 2024
ISSN: 2070-1721
Authors: D. Migault, *Ericsson*; R. Weber, *Akamai*; T. Mrugalski, *ISC*

RFC 9527
DHCPv6 Options for the Homenet Naming Authority

Abstract

This document defines DHCPv6 options so that a Homenet Naming Authority (HNA) can automatically set 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9527.

Table of Contents

1. Introduction

[RFC9526] specifies how an entity designated as the Homenet Naming Authority (HNA) outsources a Public Homenet Zone to a 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 and the associated reverse zone to the home network. 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 per a Registered Homenet Domain [RFC9526]. 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 and the 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 [RFC9526].

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.

2. 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 [RFC9526].

3. Procedure Overview

This section illustrates how an 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 [RFC9526], this section assumes that the HNA and the home network DHCPv6 client are colocated on the Customer Premises Equipment (CPE) router [RFC7368]. Also, note that this is not mandatory, and the DHCPv6 client may remotely instruct the HNA with a protocol that will be

standardized in the future. In addition, this section assumes that the responsible entity for the DHCPv6 server is provisioned with the DM and RDM information, which is 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 configuration.

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 "Securing the Control Channel" (Section 6.6) of [RFC9526]) by the DM and the RDM. The HNA builds the Homenet Zone (or the Homenet Reverse Zone) and proceeds as described in [RFC9526]. The DHCPv6 options provide the necessary non-optional parameters described in Appendix B of [RFC9526]. The HNA may complement the configurations with additional parameters via means not yet defined. Appendix B of [RFC9526] describes such parameters that may take some specific non-default value.

4. DHCPv6 Options

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 fully qualified domain name (FQDN) associated with the home network.

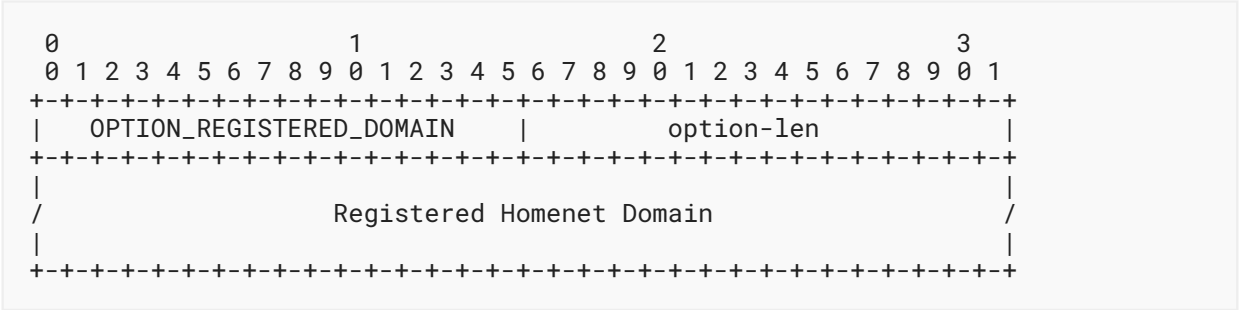


Figure 1: Registered Domain Option

option-code (16 bits): OPTION_REGISTERED_DOMAIN; the option code for the Registered Homenet Domain (145).

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 Distribution 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 an 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.

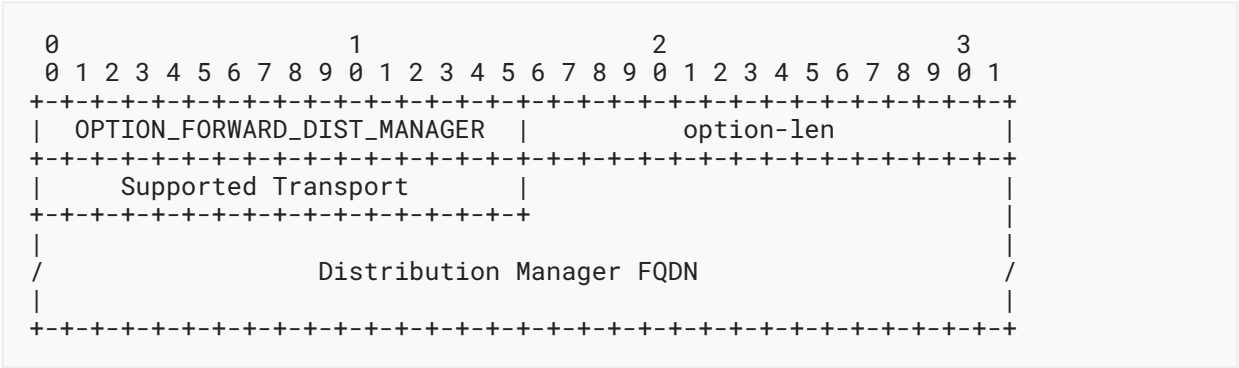


Figure 2: Forward Distribution Manager Option

option-code (16 bits): OPTION_FORWARD_DIST_MANAGER; the option code for the Forward Distribution Manager Option (146).

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 noting that the DHCPv6 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 DomTLS, the default port value is 853 per DNS over TLS [RFC7858] and DNS Zone Transfer over TLS [RFC9103].

The need to associate the port value to each Supported Transport in the DHCPv6 option has been balanced with the difficulty of handling a list of tuples (transport, port) and the possibility of using a dedicated IP address for the DM in case the default port is 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.

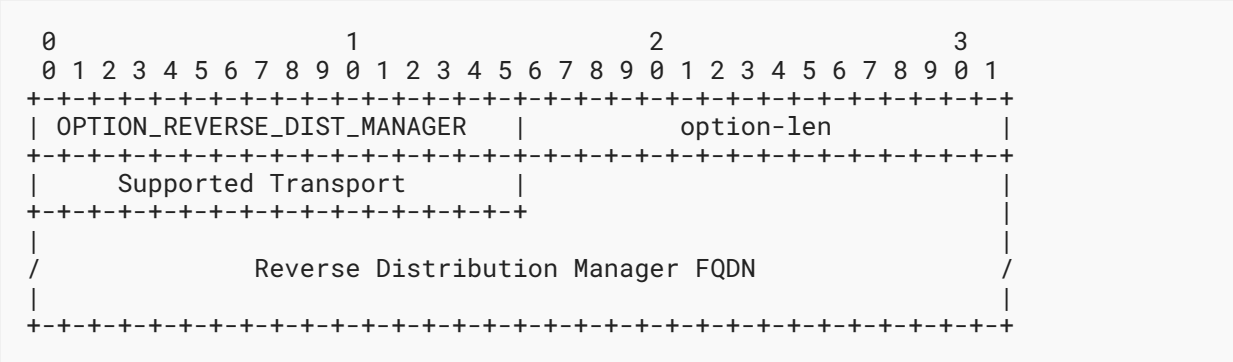


Figure 3: Reverse Distribution Manager Option

option-code (16 bits): OPTION_REVERSE_DIST_MANAGER; the option code for the Reverse Distribution Manager Option (147).

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 an RDM **MAY** indicate the support of multiple modes. The bit for DomTLS [RFC7858] **MUST** be set.

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

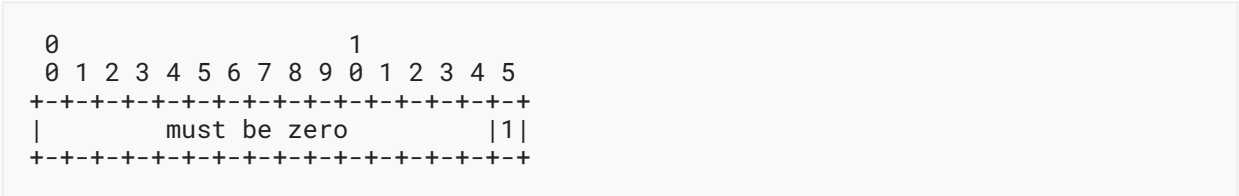
For the port number associated to the Supported Transport, the same considerations as described in Section 4.2 apply.

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 set to 1 indicates the associated transport protocol is supported. The corresponding bits are assigned as described in Table 2.

DNS over mutually authenticated TLS (DomTLS): Indicates the support of DNS over TLS [RFC7858] and DNS Zone Transfer over TLS [RFC9103] as described in [RFC9526].

As an example, the Supported Transport field expressing support for DomTLS looks as follows and has a numeric value of 0x0001:



5. DHCPv6 Behavior

5.1. DHCPv6 Server Behavior

Section 18.3 of [RFC8415] governs 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, and 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 the Registered Homenet Domain Option, Distribution Manager Option, and Reverse Distribution Manager Option in an ORO as specified in Sections 18.2 and 21.7 of [RFC8415].

Upon receiving a DHCPv6 option, as described in this document, in the Reply message, the HNA **SHOULD** proceed as described in [RFC9526].

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 has assigned the following new DHCPv6 Option Codes in the "Option Codes" registry maintained at <https://www.iana.org/assignments/dhcpv6-parameters>.

Value	Description	Client ORO	Singleton Option	Reference
145	OPTION_REGISTERED_DOMAIN	Yes	No	RFC 9527, Section 4.1
146	OPTION_FORWARD_DIST_MANAGER	Yes	Yes	RFC 9527, Section 4.2
147	OPTION_REVERSE_DIST_MANAGER	Yes	Yes	RFC 9527, Section 4.3

Table 1: Option Codes Registry

6.2. Supported Transport Parameter

IANA has created and maintains a new registry called "Supported Transport" under the "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" registry at <https://www.iana.org/assignments/dhcpv6-parameters>. This registry contains Supported Transport parameters 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 Table 2 (Section 6.2).

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.

New entries **MUST** specify the bit position, the transport protocol description, a mnemonic, and a reference as shown in Table 2.

Changes to the format or policies of the registry are managed by the IETF via the IESG.

Future code points are assigned under RFC Required per [RFC8126]. The initial registry is as specified in Table 2 below.

Bit Position (least to most significant)	Transport Protocol Description	Mnemonic	Reference
0	DNS over mutually authenticated TLS	DomTLS	RFC 9527

Bit Position (least to most significant)	Transport Protocol Description	Mnemonic	Reference
1-15	Unassigned		

Table 2: Supported Transport Registry

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 (i.e., physically), which may not require relying on TLS to authenticate the HNA. As the use of TLS is mandatory, it is expected that the HNA will be provisioned with a certificate. In some cases, the HNA may use a self-signed certificate.

8. References

8.1. Normative References

[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>.

[RFC9526] Migault, D., Weber, R., Richardson, M., and R. Hunter, "Simple Provisioning of Public Names for Residential Networks", RFC 9526, DOI 10.17487/RFC9526, January 2024, <https://www.rfc-editor.org/info/rfc9526>.

8.2. Informative References

[CNAME-PLUS-DNAME] Surý, O., "CNAME+DNAME Name Redirection", Work in Progress, Internet-Draft, draft-sury-dnsop-cname-plus-dname-01, 15 July 2018, <https://datatracker.ietf.org/doc/html/draft-sury-dnsop-cname-plus-dname-01>.

[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, 5 November 2013, <https://datatracker.ietf.org/doc/html/draft-andrews-dnsop-pd-reverse-02>.

[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 discusses 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, as described in Section 3, is one in which an ISP manages the DHCPv6 server, DM, and RDM.

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

In this scenario, the DHCPv6 server, DM, and RDM are managed by the ISP, so the DHCPv6 server and 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 where the end user wants its home network to use example.com but does not want it to be managed by the ISP (foo) as a Registered Homenet Domain, and 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 example.com to foo.example using static redirection with CNAME [RFC1034] [RFC2181], DNAME [RFC6672], or CNAME+DNAME [CNAME-PLUS-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, and the zone can be updated as described 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 in Appendix A.1. Then, the end user is able to register an unlimited number of domain names provided by an unlimited number of different third-party providers for its home network. The drawback of this scenario may be that the end user still needs to rely on the ISP naming infrastructure. Note that this may be inconvenient in the case where the DNS servers provided by the ISPs result in high latency.

A.3. Third-Party DNS Infrastructure

This scenario involves the end user using example.com as a Registered Homenet Domain and not relying on the authoritative servers provided by the ISP.

In this appendix, we limit the outsourcing of 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 only needs to be performed one time.
2. Uploading 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 the registrar may 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 [RFC9526], 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 involves an HNA connected to multiple ISPs.

Suppose the HNA has configured each of its interfaces independently with each ISP 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 an 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 this document.

If an HNA is not able to handle multiple Registered Homenet Domains, the HNA may remain connected to multiple ISPs with a single Registered Homenet Domain. In this case, one entity is chosen to host the Registered Homenet Domain. This entity may be an ISP or a third party. Note that having multiple ISPs can be motivation for bandwidth aggregation or connectivity failover. In the case of connectivity failover, the failover 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 ISPs even in a scenario of multiple ISPs may make sense. However, for the 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 Appendices A.2 and A.3.

With the configuration described in Appendix A.2, the HNA is expected to be able to handle multiple Registered Homenet Domains as the third-party redirect to one of the ISP's servers. With the configuration described in Appendix A.3, DNS zones 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 an HNA connected to multiple ISPs. Whether to configure the HNA or not, and how to configure the HNA, depends on the HNA facilities. Appendices A.1 and A.2 require the HNA to handle multiple Registered Homenet Domains, whereas Appendix A.3 does not have such a requirement.

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 inspired by Mark Andrews's document [PD-REVERSE] as well as discussions with Mark. We also thank Ray Hunter and Michael Richardson for their reviews and comments and for suggesting appropriate terminology.

Contributors

The coauthors would like to thank Chris Griffiths and Wouter Cloetens for providing significant contributions to the early draft versions of this document.

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.
PO Box 360
Newmarket, NH 03857
United States of America
Email: tomasz.mrugalski@gmail.com