Homenet
Internet-Draft
Intended status: Standards Track
Expires: October 30, 2021

D. Migault
Ericsson
R. Weber
Akamai
T. Mrugalski
Internet Systems Consortium, Inc.
April 28, 2021

DHCPv6 Options for Home Network Naming Authority
draft-ietf-homenet-naming-architecture-dhc-options-12

Abstract

This document defines DHCPv6 options so an agnostic 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.

Commenté [BMT1]: What is an “agnostic” HNA?

Commenté [BMT2]: I’m not this is useful in the abstract as more elaboration is needed to assess which are these “most cases”.

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 ~~is expected to~~should be familiar with concepts and terms defined in [I-D.ietf-homenet-front-end-naming-delegation]~~ and its terminology section~~.

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 Outsourcing DNS Infrastructure (DOI).

This document ~~shows~~ describes how ~~an ISP~~a network can provision ~~automatically~~ the HNA with a specific DOI. Most likely the DOI will be - at least partly be - managed or provided by its ISP, but other cases may envision the ISP storing some configuration so the homenet becomes resilient to HNA replacement.

The ISP delegates an IP prefix to the home network ~~an IP prefix it owns~~ as well as the associated reverse zone. The ISP is ~~well~~ 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 Master (RDM) and potentially the Reverse Public Authoritative Servers.

In addition, ~~the~~ ISPs often identifies the home network with a name. ~~In most cases, t~~Such as~~he~~ name is used by ~~the~~ ISPs for ~~its~~ their internal network management operations and is not a name the home network owner has registered to. ~~The~~ ISPs may ~~thus~~ leverage such infrastructure and provide the homenet 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, ~~the~~ ISPs ~~is~~ are ~~well~~ aware of who owns that domain name and may become a natural candidate for hosting the Homenet Zone - that is the Distribution Master (DM) and the Public Authoritative Servers.

This document describes DHCPv6 options that ~~enables~~ enable ~~the~~ 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 makes the configuration completely transparent to the end user and provides a similar level of trust as the one used to provide the IP prefix.

3. ~~Protocol~~ 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 [I-D.ietf-homenet-front-end-naming-delegation], this section assumes that the HNA and the home network DHCPv6 client are collocated on the CPE. Note also that this is not mandatory and only specific

Commenté [BMT3]: I'm not sure I would maintain this sentence.

Mis en forme : Surlignage

Mis en forme : Surlignage

Commenté [BMT4]: Not the home network but a line.

Commenté [BMT5]: This is not "naturally". This is a consequence of what is indicated in the second sentence.

Commenté [BMT6]: The abstract says "most cases".

Commenté [BMT7]: The prefix can be obtained by other means for IPv6. You may tweak this accordingly.

Commenté [BMT8]: Having a figure would be helpful.

Commenté [BMT9]: Please note that RFC7368 uses "CE router".

communications between the HNA and the DHCPv6 client ~~only~~ are needed. In addition, this section assumes that the ~~responsible entity for the~~ DHCPv6 server is ~~able to~~ configured with the DM and RDM. In our case, this means a Registered Homenet Domain can be associated to the DHCPv6 client.

This scenario has been chosen as it is believed to be the most popular scenario. This document does not ignore scenarios where the DHCPv6 ~~Server~~ server does not have privileged relations with the DM or RDM.

These cases are discussed ~~latter~~ 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. ~~and configures its~~The DHCPv6 ~~Client~~ client is configured to include in its Option Request Option (ORO) the Registered Homenet Domain Option (OPTION_REGISTERED_DOMAIN), the Distribution Master Option (OPTION_DIST_MASTER), and the Reverse Distribution Master Option (OPTION_REVERSE_DIST_MASTER) option codes.

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

3. The HNA is able to get authenticated by the DM and the RDM. The HNA builds the Homenet Zone (~~resp.~~or the Homenet Reverse Zone) and proceed as described in [I-D.ietf-homenet-front-end-naming-delegation]. The DHCPv6 options provide the necessary and ~~non~~ non-optional parameters described in ~~section~~ Section 14 of [I-D.ietf-homenet-front-end-naming-delegation]. The HNA ~~MAY set~~may complement the configurations with additional parameters. Section 14 of [I-D.ietf-homenet-front-end-naming-delegation] describes such parameters that MAY take a default value.

4. ~~Payload~~ DHCPv6 Option~~Description~~

This section details the payload of the DHCPv6 options.

4.1. Registered Homenet Domain Option

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

Commenté [BMT10]: If they are not collocated, how communication takes place?

Commenté [BMT11]: Which one?

Mis en forme : Surlignage

Mis en forme : Surlignage

Mis en forme : Surlignage

Commenté [BMT12]: You may rename to "OPTION_V6_xx" as this was the practice for recent DHCPv6 options.

Commenté [BMT13]: How?

Commenté [BMT14]: You may indicate the specific section where this is discussed.

Mis en forme : Surlignage

Commenté [BMT15]: Do you mean the additional parameters?

Commenté [BMT16]: Not sure what is meant here.

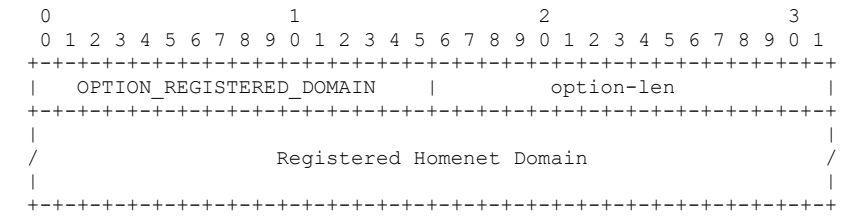

Figure 1: Registered Domain Option

- option-code (16 bits): OPTION_REGISTERED_DOMAIN, the option code for the Registered Homenet Domain (~~TBD2~~TBD1).

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

- Registered Homenet Domain (variable): the FQDN registered for the homenet. It is encoded as described in ~~section~~ Section 10 of [RFC8415].

4.2. Distribution Master Option

The Distributed Master Option (OPTION_DIST_MASTER) provides the HNA ~~to~~ with the FQDN of the DM as well as the transport ~~protocol~~ protocols for the transaction between the HNA and the DM.

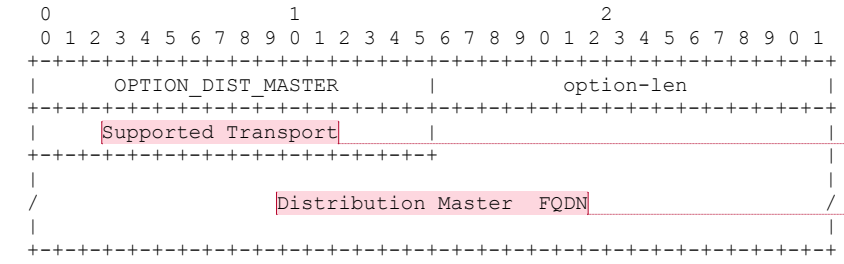

Figure 2: Distribution Master Option

- option-code (16 bits): OPTION_DIST_MASTER, the option code for the DM Option (~~TBD3~~TBD2).

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

Commenté [BMT17]: Do you assume that default ports are used? If not, how this is discovered?

Commenté [BMT18]: Why not returning a list of IP addresses? Or do you need it for authentication?

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

- Distribution Master FQDN (variable): the FQDN of the DM encoded as described in ~~section~~ Section 10 of [RFC8415].

4.2.1. Supported Transport

The Supported Transport ~~filed~~ field of the DHCPv6 option indicates the supported transport ~~protocol~~protocols. Each bit represents a specific transport mechanism. ~~The~~ A bit sets to 1 indicates the associated transport protocol is supported. The corresponding bits are assigned as described in Figure 3.

Bit Position	Transport Protocol	Reference
0	DNS over TLS	This-RFC
1-15	unallocated	

~~Figure~~ Table 3: Supported Transport

- DNS over TLS: indicates the support of DNS over TLS as described in [RFC7858].

4.3. Reverse Distribution Master Server Option

The Reverse Distribution Master Server Option (OPTION_REVERSE_DIST_MASTER) provides the HNA with ~~to~~ the FQDN of the DM as well as the transport ~~protocol~~ protocols for the transaction between the HNA and the DM.

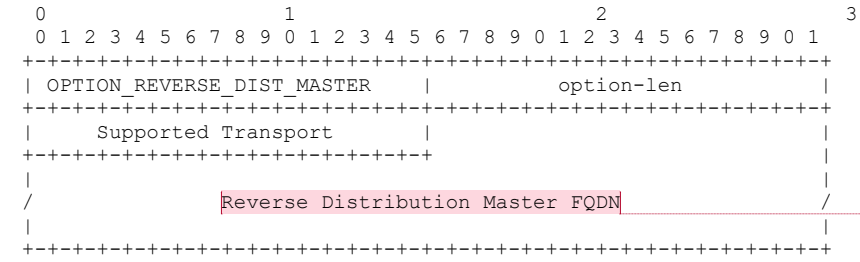

Figure 4: Reverse Distribution Master Option

Commenté [BMT19]: Please add a pointer to Section 4.2.1

Commenté [BMT20]: When more than one bit is set, how the client selects the transport?

Commenté [BMT21]: Please add a pointer to the IANA section where the behavior to associate a meaning with a bit is defined.

Commenté [BMT22]: What is a “transaction”?

Commenté [BMT23]: Idem as for DM.

- option-code (16 bits): OPTION_REVERSE_DIST_MASTER, the option code for the Reverse Distribution Master Option (TBD3~~TBD4~~).

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

- Supported Transport (16 bits): defines the supported transport by the DM. Each bit represents a supported transport, and a DM MAY indicate the support of multiple modes. The DoT bit ~~for DoT~~ MUST be set.

- Reverse Distribution Master FQDN (variable): Includes the FQDN of the RDM . It is encoded as described in section 10 of [RFC8415].

5. DHCP Behavior

5.1. DHCPv6 Server Behavior

Sections 17.2.2 and 18.2 of [RFC8415] govern server operation in regards to 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 DHCP Server sends the Registered Homenet Domain Option, Distribution Master Option, the Reverse Distribution Master Option when requested by the DHCPv6 client by including necessary option codes in its ORO.

5.2. DHCPv6 Client Behavior

The DHCPv6 client ~~sends a ORO with the necessary option codes~~includes~~:~~ Registered Homenet Domain Option, Distribution Master Option, the Reverse Distribution Master 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 DHCP 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 DHCP Relay agents.~~

6. IANA Considerations

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.

Commenté [BMT24]: Please add a pointer to 4.2.1

Commenté [BMT25]: I'm not sure I would keep this section. Only the DHCPv6 client behavior should be normative.

Commenté [BMT26]: This is more a behavior of I-D.ietf-homenet-front-end-naming-delegation. This section should focus on the behavior of the **DHCPv6 client**.

Value	Description	Client ORO	Singleton Option
TBD1	OPTION_REGISTERED_DOMAIN	Yes	Yes
TBD2	OPTION_DIST_MASTER	Yes	Yes
TBD3	OPTION_REVERSE_DIST_MASTER	Yes	Yes

IANA is requested to maintain a new number space of Supported Transport parameter in the Distributed Master Option (OPTION_DIST_MASTER) or the Reverse Distribution Master Server Option (OPTION_REVERSE_DIST_MASTER). The different parameters are defined in Figure 3 in Section 4.2.1. Future code points are assigned under Specification Required as per [RFC8126].

7. Security Considerations

The security considerations in [RFC2131] and [RFC8415] are to be considered. The use of DHCPv6 options provides a similar level of trust as the one used to provide the IP prefix. The link between the HNA and the DHCPv6 server may benefit from additional security for example by using [I-D.ietf-dhc-sedhcpv6].

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 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

[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>.

Commenté [BMT27]: There will be always one registered domain?

Commenté [BMT28]: Why this one is cited here?

Commenté [BMT29]: What about the scenario where the HNA and DHCPv6 client are not colocatted?

Commenté [BMT30]: This was expired since 2017.

Commenté [BMT31]: Why is this normative?

[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>.

~~[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.~~

[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>.

[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>.

[I-D.ietf-homenet-front-end-naming-delegation] Migault, D., Weber, R., Richardson, M., Hunter, R., Griffiths, C., and W. Cloetens, "Simple Provisioning of Public Names for Residential Networks", draft-ietf-homenet-front-end-naming-delegation-13 (work in progress), March 2021.

10.2. Informative References

[I-D.andrews-dnsop-pd-reverse] Andrews, M., "Automated Delegation of IP6.ARPA reverse zones with Prefix Delegation", draft-andrews-dnsop-pd-reverse-02 (work in progress), November 2013.

[I-D.ietf-dhc-sedhcpv6] Li, L., Jiang, S., Cui, Y., Jinmei, T., Lemon, T., and D. Zhang, "Secure DHCPv6", draft-ietf-dhc-sedhcpv6-21 (work in progress), February 2017.

Commenté [BMT32]: This is not a normative ref.

Commenté [BMT33]: This is not a normative ref.

[I-D.ietf-homenet-front-end-naming-delegation]
Migault, D., Weber, R., Richardson, M., Hunter, R., Griffiths, C., and W. Cloetens, "Simple Provisioning of Public Names for Residential Networks", draft-ietf-homenet-front-end-naming-delegation-13 (work in progress), March 2021.

[I-D.sury-dnsext-cname-dname]
Sury, O., "CNAME+DNAME Name Redirection", draft-sury-dnsext-cname-dname-00 (work in progress), April 2010.

Appendix A. Scenarios and impact on the End User

This section details various scenarios and discuss their impact on the end user. This section 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.

Appendix B. Base Scenario

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

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

In this scenario, the DHCP Server, DM and RDM are managed by the ISP so the DHCP 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.

B.1. Third Party Registered Homenet Domain

This section 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 section still consider the ISP manages the home network and still provides example.foo 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 example.foo using static redirection with CNAME [RFC2181], [RFC1034], DNAME [RFC6672] or CNAME+DNAME [I-D.sury-dnsext-cname-dname].

This configuration is performed once when the domain name example.com is registered. The only information the end user needs to know is the domain name assigned by the ISP. Once this configuration is done no additional configuration is needed anymore. More specifically, the HNA may be changed, the zone can be updated as in Appendix B 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 B. 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.

B.2. 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 section 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 DHCP 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 hosting the HNA may be the registrar and provide the CPE already configured. In other cases, the CPE 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.

B.3. 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 B. 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 Server 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 B.1 and Appendix B.2.

With the configuration described in Appendix B.1, the HNA is expect 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 B.2, 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 B and Appendix B.1 require the HNA to handle multiple Registered Homenet Domain, whereas Appendix B.2 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
US

EMail: tomasz.mrugalski@gmail.com