HOMENET
Internet-Draft
Intended status: Standards Track
Expires: April 23, 2014

D. Migault (Ed)
Francetelecom - Orange
W. Cloetens
SoftAtHome
C. Griffiths
Dyn
R. Weber
Nominum

October 20, 2013

DHCP DNS Public Authoritative Server Options
draft-mglt-homenet-naming-architecture-dhc-options-00.txt

Abstract

The home network naming architecture as described in [I-D.mglt-homenet-front-end-naming-delegation] requires a complex naming configuration on the CPE. This configuration MAY not be handled easily by the average end user. Furthermore, such misconfiguration MAY result in making home network unreachable.

This document proposes a DHCP options that provide the CPE all necessary parameters to set up the home network naming architecture.

First, this DHCP options provide automatic configuration and avoid most end users' misconfiguration. Most average end users may not require specific configuration, and their ISP default configuration MAY fully address their needs. In that case, the naming homenet architecture configuration will be completely transparent to the end users. Then, saving naming configuration outside the CPE, makes it resilient to change of CPE or CPE upgrades. Such configuration may also be configured by the end user, via the customer area of their ISP.

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 April 23, 2014.

Table of Contents

1. Requirements notation

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].

2. Terminology

- Customer Premises Equipment: (CPE) is the router providing connectivity to the home network. It is configured and managed by the end user. In this document, the CPE MAY also hosts services such as DHCPv6. This device MAY be provided by the ISP.

- Registered Homenet Domain: is the Domain Name associated to the home network.

- DNS Homenet Zone: is the DNS zone associated to the home network. This zone is set by the CPE and essentially contains the bindings between names and IP addresses of the nodes of the home network. In this document, the CPE does neither perform any DNSSEC management operations such as zone signing nor provide an authoritative service for the zone. Both are delegated to the Public Authoritative Server. The CPE synchronizes the DNS Homenet Zone with the Public Authoritative Server via a hidden master / slave architecture. The Public Authoritative Server MAY use specific servers for the synchronization of the DNS Homenet Zone: the Public Authoritative Name Server Set.

- Public Authoritative Server: performs DNSSEC management operations as well as provides the authoritative service for the zone. In this document, the Public Authoritative Server synchronizes the DNS Homenet Zone with the CPE via a hidden master / slave architecture. The Public Authoritative Server acts as a slave and MAY use specific servers called Public Authoritative Name Server Set. Once the Public Authoritative Server synchronizes the DNS Homenet Zone, it signs the zone and generates the DNSSEC Public Zone. Then the Public Authoritative Server hosts the zone as an authoritative server on the Public Authoritative Master(s).

- DNSSEC Public Zone: corresponds to the signed version of the DNS Homenet Zone. It is hosted by the Public Authoritative Server, which is authoritative for this zone, and is reachable on the Public Authoritative Master(s).

- Public Authoritative Master(s): are the visible name server hosting the DNSSEC Public Zone. End users' resolutions for the Homenet Domain are sent to this server, and this server is a master for the zone.

- Public Authoritative Name Server Set: is the server the CPE synchronizes the DNS Homenet Zone. It is configured as a slave

and the CPE acts as master. The CPE sends information so the DNSSEC zone can be set and served.

3. Introduction

With IPv6, nodes inside the home network are expected to be globally reachable. CPEs are already providing connectivity to the home network, and most of the time already assigns IP addresses to the nodes of the home network using for example DHCPv6.

This makes CPE good candidate for defining the DNS zone file of the home network. However, CPEs have not been designed to handle heavy traffic, nor heavy operations. As a consequence, CPE SHOULD neither host the authoritative naming service of the home network, nor handle DNSSEC operations such as zone signing. In addition, CPE are usually managed by end users, and the average end user is most likely not mastering DNSSEC to administrate its DNSSEC zone. As a result, CPE SHOULD outsource both the naming authoritative service and its DNSSEC management operations to a third party. This architecture, designated as the homenet naming architecture is described in [I-D.mglt-homenet-front-end-naming-delegation], and the third party is designated as the Public Authoritative Servers.

The home network naming architecture [I-D.mglt-homenet-front-end-naming-delegation] defines how the CPE and the Public Authoritative Servers interact together, to leverage some of the issues related to the CPE, and the DNSSEC understanding of the average end user. Even though most of the DNSSEC issues are outsourced to the Public Authoritative Servers, setting the homenet naming architecture still requires some configurations.

Configuration is fine as it provides the opportunity for advanced end users to make the naming architecture fit their specific needs. However most of the end users do not want to configure the homenet naming architecture. In most cases, the end users wants to subscribe and plug its CPE. The CPE is expected to be configured to set automatically and transparently the appropriated home network naming architecture.

Using DHCP options to provide the necessary parameters for setting the homenet naming architecture provides multiple advantages. Firstly, it makes the network configuration independent of the CPE. Any new plugged CPE configures itself according to the provided configuration parameters. Secondly, it saves the configuration outside the CPE, which prevents re-configuring the CPE when it is replaced or reset. Finally ISPs are likely to propose a default homenet naming architecture that may address most of the end users needs. For these end users, no configuration will be performed at

any time. This avoids unnecessary configurations or misconfiguration that could result in isolating the home network. For more advanced end users, the configuration MAY be provided also via the web GUI of the ISP's customer area for example. This configuration MAY enable third party Public Authoritative Servers. By doing so, these end users will also benefit from CPE-indepedent configuration and configuration backup.

This document considers the architecture described in [I-D.mglt-homenet-front-end-naming-delegation]. The DNS(SEC) zone related to the home network is configured and set by the CPE and hosted on a Public Authoritative Server. [I-D.mglt-homenet-front-end-naming-delegation] describes how the synchronization between the CPE and the Public Authoritative Server is performed. This document describes DHCP options that provide the necessary parameters to the CPE to set the architecture described in [I-D.mglt-homenet-front-end-naming-delegation].

Section 4 presents an overview of the DHCP options presented in this document and Section 5 describes the format of this option and Section 6, Section 7 and Section 8 details the behavior of respectively the DHCP Client, the DHCP Server and the DHCP Relay.

This document assumes the reader is familiar with [I-D.mglt-homenet-front-end-naming-delegation].

This document assumes that the communication between the CPE and the ISP DHCP Server is protected. This document does not specify which mechanism should be used. [RFC3315] proposes a DHCP authentication and message exchange protection, [RFC4301], [RFC5996] proposes to secure the channel at the IP layer.

This document only deals with IPv6 IP addresses and DHCPv6 [RFC3315]. When we mention DHCP, it MUST be understood as DHCPv6.

4. Protocol Overview

To properly configure the home network naming architecture defined in [I-D.mglt-homenet-front-end-naming-delegation], the CPE MUST:

- 1: Determine which Registered Domain are considered. Each Registered Domain is associated to a DNS Zone file. Note that a CPE MAY publish a single zone under different Registered Domain Names, or set different contents on different Registered Domain Names.

- 2: Properly generate the DNS Zone file and associate the corresponding authoritative Name Server (RRset NS) with

associated IP addresses (RRsets A or AAAA). The CPE derives the NS RRset from the Registered Domain and the Public Authoritative Master. Then it MAY derive the glue A or AAAA records from the Public Authoritative Master and associated IP addresses. These pieces of information are provided by the DHCP Zone Public Master Option (OPTION_ZONE_PUBLIC_MASTER).

- 3: Upload the Zone files to the Public Authoritative Master. Uploading the DNS Homenet Zone or the DNSSEC Homenet Zone may not be done directly from the CPE to the Public Authoritative Masters. In fact, the Public Authoritative Server MAY have a dedicated server for DNS zone uploads: the Public Authoritative Name Server Set. One of the reason is that the Public Authoritative Server MAY perform some extra operations such as the DNSSEC signing before publishing the DNSSEC Homenet Zone to on the Public Authoritative Masters. As a result, for each Public Authoritative Master a secure channel MUST be established between the CPE and the Public Authoritative Name Server Set. How to set, for each Public Authoritative Master, the secure channel to the Public Authoritative Name Server Set is provided by the DHCP Public Master Upload Option (OPTION_PUBLIC_MASTER_UPLOAD).

A common way for the CPE to collect these pieces of information is to send an Option Request DHCP Option (ORO) [RFC3315] for the DHCP DNS Public Authoritative Server Option and for the DNS Public Authoritative Name Server Set Option. If the DHCP Sever understand these options, it MAY send back one or multiple instance for each option. Then, the DHCP Client sets the naming architecture.

Similarly, the DHCP Server MAY provide the DHCP DNS Public Authoritative Server Option and for the DNS Public Authoritative Name Server Set Option without any request from the DHCP Client.

Note that how the CPE manage the multiple DNS Homenet Zones is implementation dependent. It MAY synchronize all DNS Homenet Zone with the Public Authoritative Servers, or use zone redirection mechanisms like like CNAME [RFC2181], [RFC1034], DNAME [RFC6672] or CNAME+DNAME [I-D.sury-dnsext-cname-dname]. In the first case, any update requires to update all zone, whereas redirection MAY require only updating a single DNS Homenet Zone.

5. Payload Description

5.1. DHCP Zone Public Master Option

The DHCP Zone Public Master Option (OPTION_ZONE_PUBLIC_MASTER) is used by the CPE to set the DNS Homenet Zone with the proper NS RRsets

and the associated IP addresses. The DHCP Zone Public Master Option provides bindings between Registered Domain Names and Public Authoritative Master.

Following Section 9 of [I-D.ietf-dhc-option-guidelines], the DHCP Zone Master Option encapsulates the DHCP Registered Domain Name Option (OPTION_REGISTERED_DOMAIN_NAMES) that contains a list of registered domain names and the Public Authoritative DHCP Master Option (OPTION_MASTER) that contains the FQDNs and IP addresses of each Public Authoritative Masters.

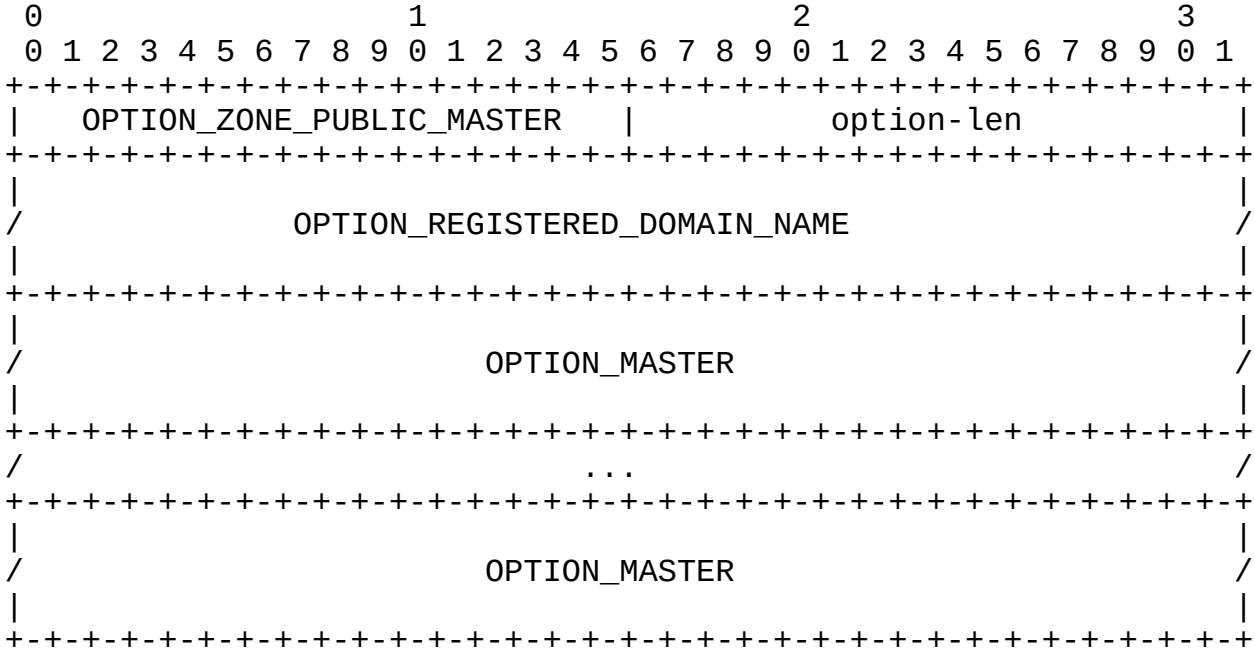


Fig 1: DHCP Zone Public Master Option

- OPTION_ZONE_PUBLIC_MASTER: the option code for the DHCP Zone Public Master Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- OPTION_REGISTERED_DOMAIN_NAME: the list of Registered Homenet Domains.

- OPTION_MASTER: the necessary information to configure properly the DNS Homenet Zone file with NS, A and AAA RRsets associated to the Public Authoritative Master(s).

5.1.1. Unpacking a DHCP Zone Public Master Option

When a DHCP Zone Public Master Option is received by the DHCP Client, if the DHCP Registered Domain Name Option does not exist or is void, the CPE ignores the DHCP Zone Public Master Option. It MAY indicate the DHCP Server supports these options but they are not properly configured. Otherwise, it selects all DNS Homenet Zone designated by the DHCP Registered Domain Name Option and adds the Public Authoritative NS, A and AAA records provided by the DHCP Master Option. If DHCP Master Option are missing, the CPE hosts the DNS Homenet Zone for the Registered Domains.

All DHCP Options are propositions. The CPE MAY chose a subset of these according to its policies.

Section 13 illustrates with pseudo code how this MAY be performed.

5.1.2. Packing a DHCP Zone Public Master Option

The DHCP Server sends a DHCP Zone Public Master Option to bind Registered Domain Names to a list of Public Authoritative Masters. How to collect these pieces of information is implementation dependent, and depends on the data structure that stores the information. However, we can reasonably assume that sending a DHCP Zone Public Master Option is composed of two phases:

- 1) First collect all Registered Domain with their associated list of Public Authoritative Masters. Basic implementation MAY build DHCP Zone Public Master Option for each Registered Domain. However, we recommend to group all Registered Domain with the same list of Public Authoritative Masters. This leads to a list of Registered Domain associated to a list of Public Authoritative Masters. Note that lists of Public Authoritative Masters are equals if they have the same Public Authoritative Masters, that is for each of them the same FQDN and the same list of IP addresses. The list is not ordered.

- 2) Then, for each binding build a new DHCP Zone Public Master Option, build DHCP Registered Domain Name Option from the list of Registered Domains, add it to the DHCP Zone Public Master Option. For each Public Authoritative Master of the list of Authoritative Masters, build a DHCP Master Option and add it to the DHCP Zone Public Master Option.

Section 13 illustrates with pseudo code how this MAY be performed.

5.1.3. DHCP Registered Domain Name Option

The DHCP Registered Domain Name Option (OPTION_REGISTERED_DOMAIN_NAME) contains a list of DNS domain names. It MAY have multiple FQDNs. This option follows the description of section 5.10 [I-D.ietf-dhc-option-guidelines].

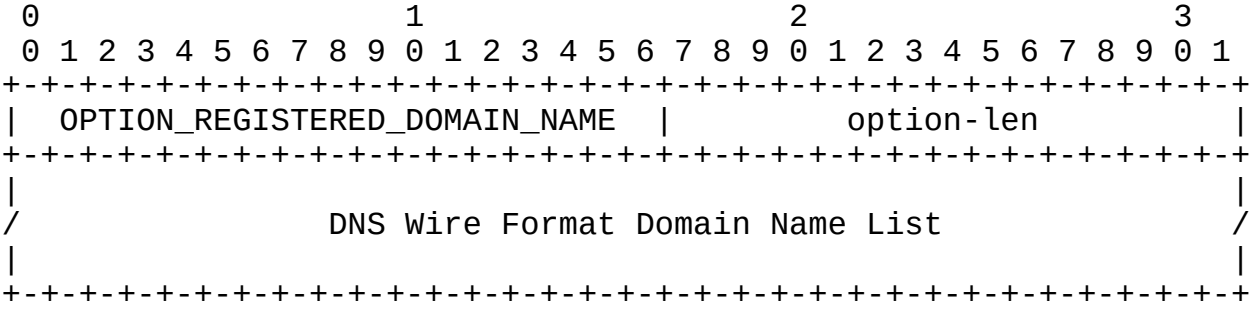


Fig 2: DHCP Registered Domain Name Option

- OPTION_REGISTERED_DOMAIN_NAME: the option code for the DHCP Registered Domain Name Option

- option-len: length in octets of the option-data field as described in [RFC3315].

- DNS Wire Format Domain Name List: The special encoding of this field supports carrying multiple instances of hosts or domain names in a single option, by terminating each instance with a byte of 0 value.

5.1.3.1. Unpacking a DHCP Registered Domain Name Option

The DHCP Registered Domain Name Option MAY return one or multiple Registered Domain Names. The DHCP Client MUST remove empty strings from the list.

5.1.3.2. Packing a DHCP Registered Domain Name Option

The DHCP Registered Domain Name Option is build from a list of non-empty strings.

5.1.4. DHCP Master Option

The DHCP Master Option provides the FQDN and associated IP addresses of the Public Authoritative Master. Following Section 9 of [I-D.ietf-dhc-option-guidelines], the DHCP Master Option encapsulates the DHCP Master FQDN Option (OPTION_MASTER_FQDN) that contains a single FQDN followed by a DHCP Master IP4 Option (OPTION_MASTER_IP4) or a DHCP Master IP6 Option (OPTION_MASTER_IP6) that contains the

associated IP addresses. Only a single DHCP Master IP6 Option or DHCP Master IP4 Option is expected.

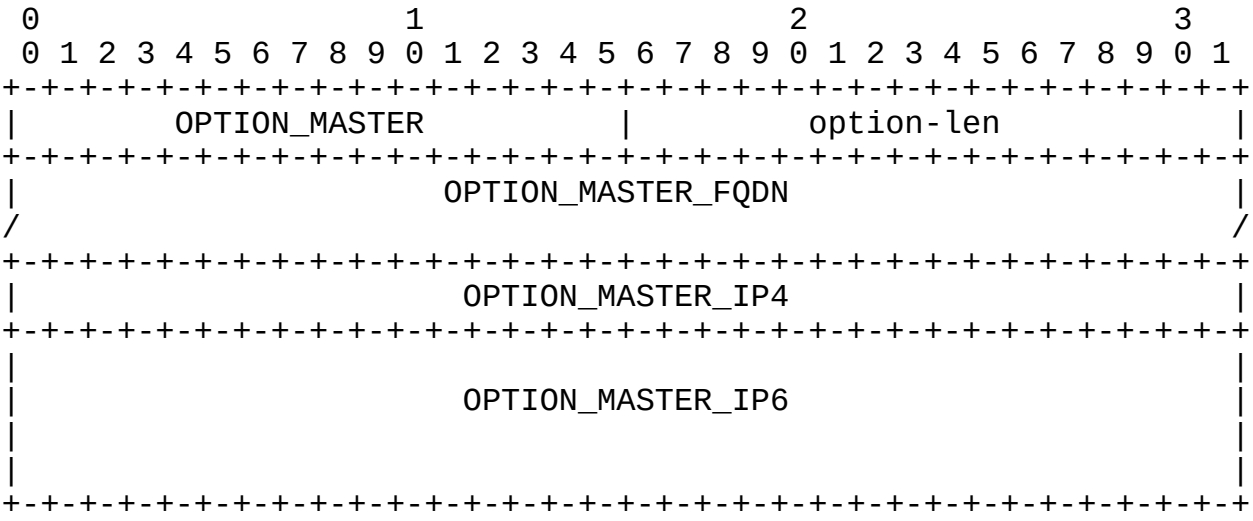


Fig 3: DHCP Master Option

- OPTION_MASTER: the option code for the DHCP Master Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- OPTION_MASTER_FQDN: the DHCP Master FQDN Option with FQDN associated to the Public Authoritative Server. This option is mandatory.

- OPTION_MASTER_IP4: the DHCP Master IP4 Option with IPv4 address associated to the Public Authoritative Server. This option is optional, however the DHCP server SHOULD provide at least one DHCP Master IP4 Option or one DHCP Master IP6 Option.

- OPTION_MASTER_IP6: the DHCP Master IP6 Option with IPv6 address associated to the Public Authoritative Server. This option is optional, however the DHCP server SHOULD provide at least one DHCP Master IP6 Option or one DHCP Master IP6 Option.

5.1.4.1. Unpacking a DHCP Master Option

The DHCP Master FQDN Option is mandatory, and a DHCP Master Option that do not encapsulate a DHCP Master FQDN Option MUST be ignored. An empty DHCP Master FQDN Option indicates the CPE and a FQDN MUST be provided by the CPE. DHCP Master IP4 Options and DHCP Master IP6 Options are optional. Following Section 8 of

[I-D.ietf-dhc-option-guidelines], providing IP addresses avoids DNS(SEC) resolutions which unnecessarily load the network and delay the configuration. As a result, it is recommended to provide the IP addresses. If at least a single non void DHCP Master IP4 Option or DHCP Master IP6 Option is provide, the DHCP Client MUST NOT perform any DNS(SEC) resolution. Otherwise, the DHCP Client SHOULD perform a DNSSEC resolution.

Section 13 illustrates with pseudo code how this MAY be performed.

5.1.4.2. Packing a DHCP Master Option

DHCP Master Options are built from the master object. If the FQDN of the Public Authoritative Master is empty, the DHCP Master Option MUST NOT be built. If no IP address has been provisioned, the DHCP Server SHOULD perform a DNS(SEC) resolution and provide the IP addresses.

Section 13 illustrates with pseudo code how this MAY be performed.

5.1.4.3. DHCP Master FQDN Option

The DHCP Master FQDN Option (OPTION_MASTER_FQDN) designates the FQDN of the Public Authoritative Server. Only one FQDN is expected. This option follows the description of section 5.10 [I-D.ietf-dhc-option-guidelines].

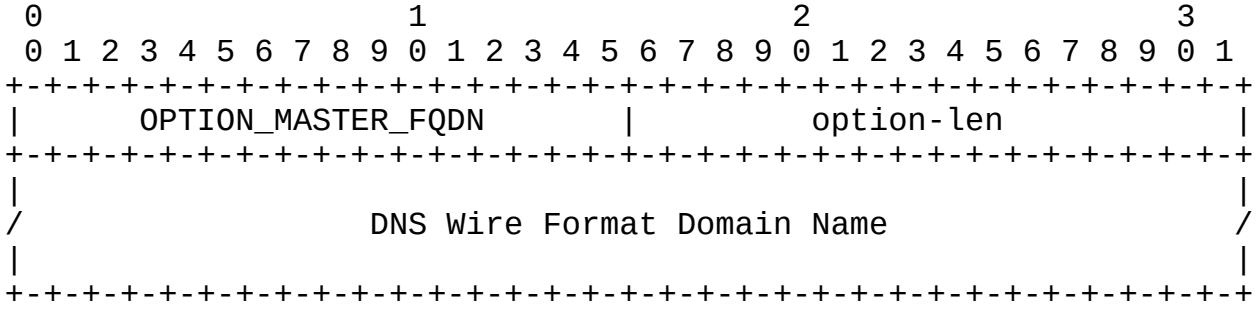


Fig 4: DHCP Master FQDN Option Format

- OPTION_MASTER_FQDN: the option code for the DHCP Master FQDN Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- DNS Wire Format Domain Name: A single FQDN.

5.1.4.4. DHCP Master IP4 Option

This section defines the IP addresses associated to the master. This option follows the recommendation of section 5.1 and 8 of [I-D.ietf-dhc-option-guidelines].

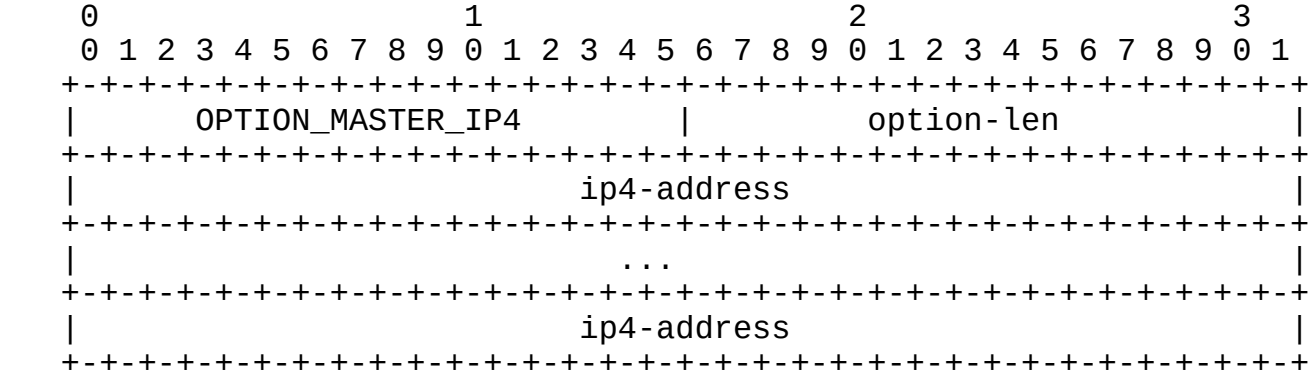


Fig 5: DHCP Master IP4 Option Format

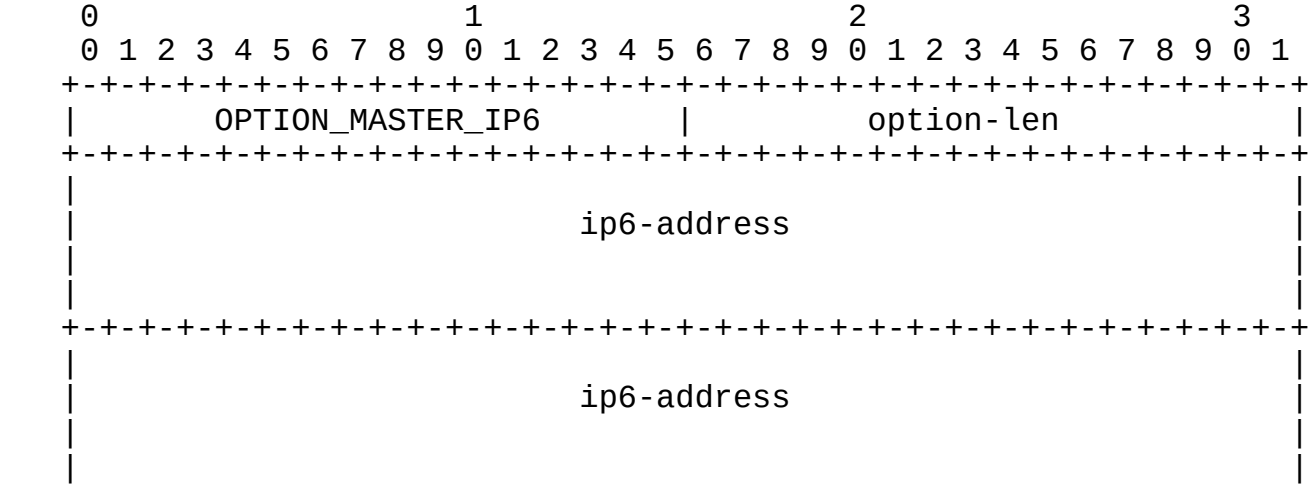
- OPTION_MASTER_IP4: the option code for the DHCP Master IP4 Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- ip4-address: the 32 bit value of the IPv4 address.

5.1.4.5. DHCP Master IP6 Option

This section defines the IP addresses associated to the master. This option follows the recommendation of section 5.1 and 8 of [I-D.ietf-dhc-option-guidelines].



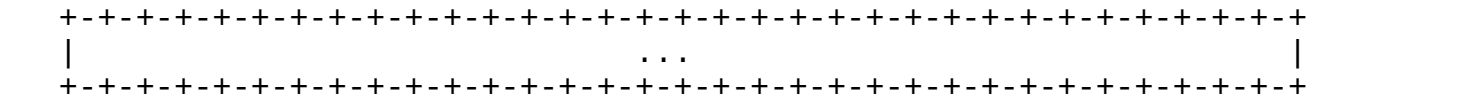


Fig 6: DHCP Master IP6 Option Format

- OPTION_MASTER_IP6: the option code for the DHCP Master IP6 Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- ip6-address: the 128 bit value of IPv6 address.

5.2. DHCP Public Master Upload Option

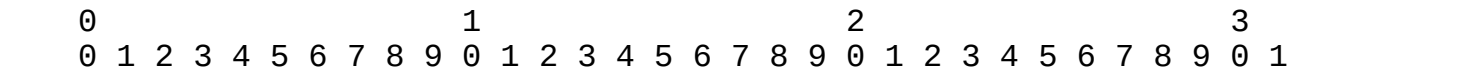
The DHCP Public Master Upload Option (OPTION_PUBLIC_MASTER_UPLOAD) is used to associate a secure channel for each Public Authoritative Master.

More specifically, to publish a DNS Homenet Zone on a given Public Authoritative Master, the CPE establish a secure channel with the Public Authoritative Name Server Set and upload the DNS Homenet Zone using master / slave mechanisms. It is then the responsibility of the Public Authoritative Name Server Set to publish the DNS Homenet Zone to its associated Public Authoritative Masters.

The DHCP Public Master Upload Option enables the CPE to set an address book where the key is the Public Authoritative and the value is a set of Secure Channels. For each DNS(SEC) Homenet Zone, the CPE is expect to list the Public Authoritative Master and for each of them upload the DNS(SEC) Homenet Zone file to the Public Authoritative Name Server Set via a Secure Channel.

Following Section 9 of [I-D.ietf-dhc-option-guidelines], the DHCP Public Master Upload Option encapsulates a DHCP Master FQDN List Option (OPTION_MASTER_FQDN_LIST) that contains the list of the FQDNs of the Public Authoritative Master and a list of DHCP Secure Channel Options (OPTION_SECURE_CHANNEL) that list how the CPE can upload the DNS(SEC) Homenet Zone. For each of the mentioned Public Authoritative Master, the CPE is expected to consider one of the DHCP Secure Channel Options to upload the Zone.

The DHCP Master FQDN List Option is mandatory and MUST be unique. At least one DHCP Secure Channel Options MUST be encapsulated.



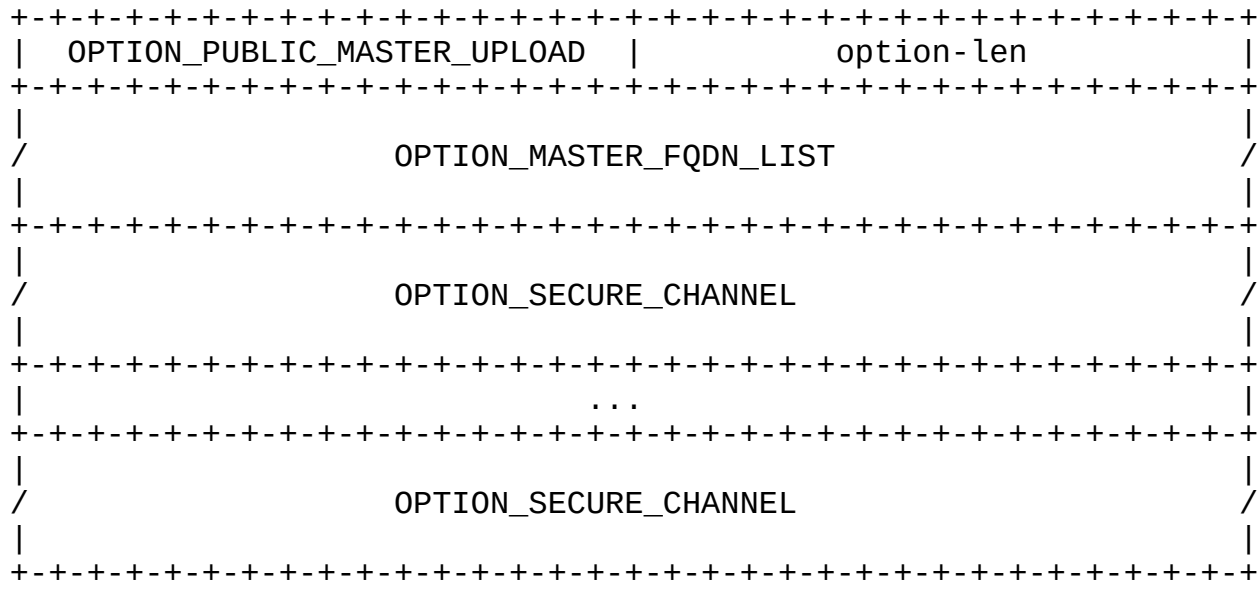


Fig 7: DHCP Public Master Upload Option Format

- OPTION_PUBLIC_MASTER_UPLOAD: the option code that corresponds to the DHCP Public Master Upload Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- OPTION_MASTER_FQDN_LIST: The DHCP Master FQDN List Option. A single DHCP Master FQDN List Option MUST be encapsulated in the DHCP Public Master Upload Option.

- OPTION_SECURE_CHANNEL: The DHCP Secure Channel Option. One or multiple DHCP Secure Channel Option MUST be encapsulated in the DHCP Public Master Upload Option.

5.2.1. Unpacking a DHCP Public Master Upload Option

When the DHCP Client receives a DHCP Public Master Upload Option, it builds a dictionary between, Public Authoritative Master FQDN and possible Secure Channels. Secure Channel that do not correspond to the CPE policy, MAY be discarded.

This binding will be used latter when the CPE uploads the DNS(SEC) Homenet Zone files. Section 13 illustrates with pseudo code how this MAY be performed.

5.2.2. Packing a DHCP Public Master Upload Option

The DHCP Server SHOULD send at least a Secure Channel for each of the Public Authoritative Master. All Public Authoritative Masters associated to the DHCP Client that are provided in a DHCP Zone Public Master Option MUST be mentioned in an DHCP Public Master Upload Option.

Packing a DHCP Public Master Upload Option is performed in a similar way as the DHCP Zone Public Master Option. A binding between the Public Authoritative Master and the Secure Channels is performed. Then, this dictionary is factorized as described in Section 5.1.2. More specifically, all keys with the same value are grouped.

5.2.3. DHCP Master FQDN List Option

The DHCP Master FQDN List Option is similar to the DHCP Master FQDN Option except that it can indicate multiple Master FQDNs.

5.2.4. DHCP Secure Channel Options

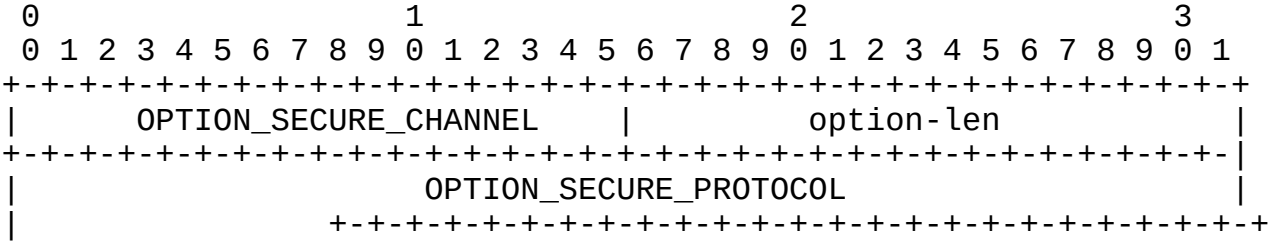
The DHCP Secure Channel Option (OPTION_SECURE_CHANNEL) indicates:

- 1: How to secure the channel, that is to say which protocols are used to secure the channel. This is indicated by the DHCP Secure Protocol Option (OPTION_SECURE_PROTOCOL).

- 2: The security credential used to set up the secure channel, that is to say the cryptographic material to authenticate the CPE and the Public Authoritative Name Server Set. This is carried by the DHCP Secure Credential Option (OPTION_SECURE_CREDENTIAL).

- 3: The Public Authoritative Name Server Set the secure channel is established with, that is to say its IP addresses. These IP addresses are carried by the DHCP Server Set Option (OPTION_SERVER_SET).

Following Section 9 of [I-D.ietf-dhc-option-guidelines], the DHCP Secure Channel Option encapsulates the DHCP Secure Protocol Option, the DHCP Secure Credential Option and the DHCP Server Set Option. Each of these options is mandatory and MUST appear only once.



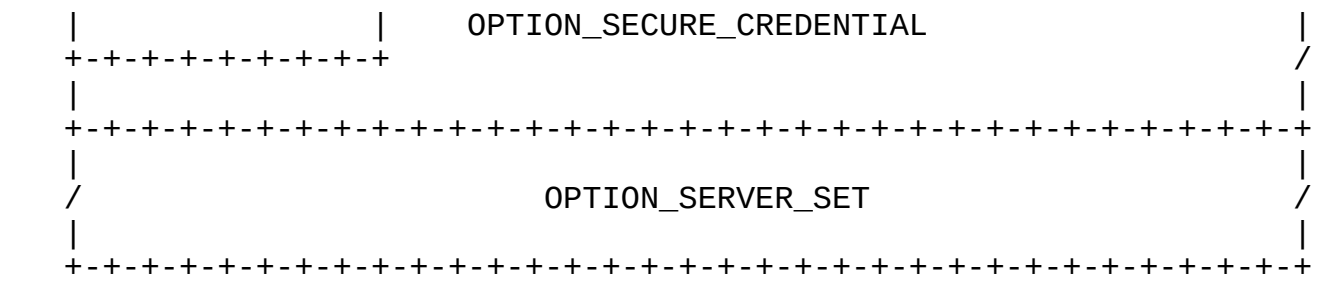


Fig 8: DHCP Secure Channel Option Format

- OPTION_SECURE_CHANNEL: The option code for the DHCP Secure Channel Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- OPTION_SECURE_PROTOCOL: the DHCP Secure Protocol Option. This option is mandatory and MUST appear only once.

- OPTION_SECURE_CREDENTIAL: the DHCP Secure Credential Option. This option is mandatory and MUST appear only once.

- OPTION_SERVER_SET: the DHCP Server Set Option. This option is mandatory and MUST appear only once.

5.2.4.1. Unpacking a DHCP Secure Channel Option

When the DHCP Secure Channel Option is received, the DHCP Client MUST check that DHCP Secure Protocol Option, DHCP Secure Credential Option and DHCP Server Set Option are unique. If not, the DHCP Client MUST ignore the DHCP Secure Channel Option.

The DHCP Client MUST also check proposition match its policies and Secure Credentials match the Secure Protocol.

Section 13 illustrates with pseudo code how this MAY be performed.

5.2.4.2. Packing a DHCP Secure Channel Option

Packing the DHCP Secure Channel Option from the Secure_channel object is straight forward.

5.2.4.3. DHCP Secure Protocol Option

The DHCP Secure Protocol Option (OPTION_SECURE_PROTOCOL) is a 8-bit integer option that fills recommendation of section 5.6 of [I-D.ietf-dhc-option-guidelines].

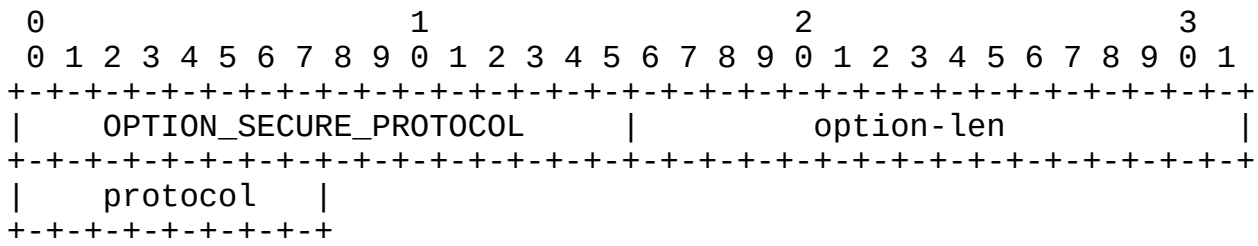


Fig 9: DHCP Secure Protocol Option Format

- OPTION_SECURE_PROTOCOL: The opcode for the DHCP Secure Protocol Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- protocol: the 8 bit value that indicates which protocol MUST be used between the CPE and the Name Server Set for this secure channel.

The protocol detailed in this document are:

- NONE: TBD

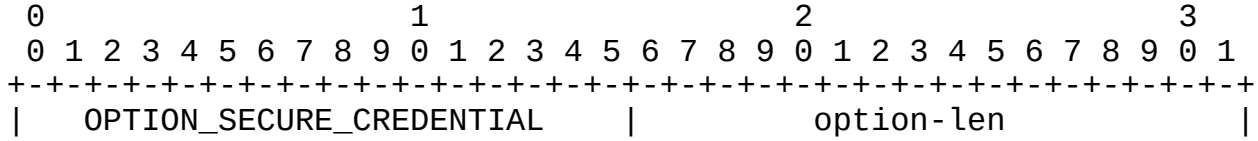
- TSIG: TBD

- IPSEC: TBD

- SIG(0): TBD

5.2.4.4. DHCP Secure Credential Option

The DHCP Secure Credential Option encapsulates the necessary element to authenticate and set up the secure channel. Currently, only the DHCP PSK Credential Option (OPTION_PSK_CREDENTIAL) is defined in this document but the use of DHCP Secure Credential Option enables makes possible the use of different credential in the future.



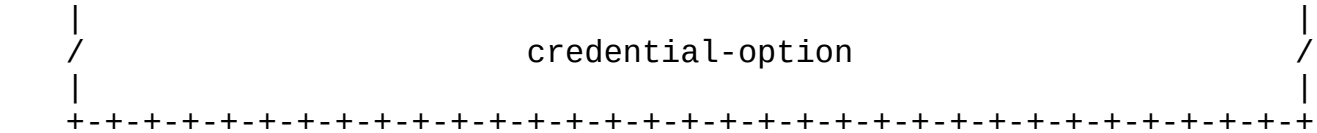


Fig 10: DHCP Secure Credential Option Format

- OPTION_SECURE_CREDENTIAL: The option code for the DHCP Secure Credential Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

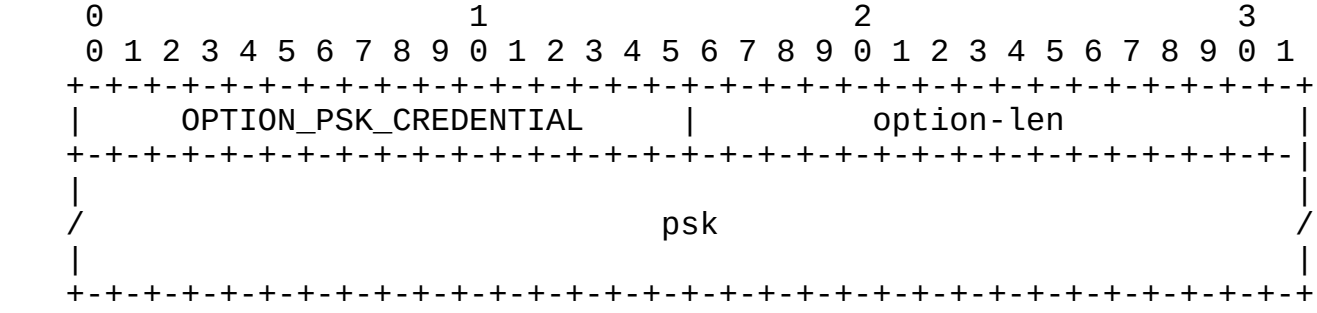
- credential-option: A DHCP Credential Option.

5.2.4.4.1. DHCP PSK Credential Option

The DHCP PSK Credential Option (OPTION_PSK_CREDENTIAL) contains the pre-shared key. It can be used with IPsec, TSIG. If SIG(0) is selected as a protocol, the DHCP server MUST NOT provide this option, and it MUST be ignored by the DHCP Client.

Note that PSK MUST NOT be sent by the DHCP Server over an non trusted channel. In addition a DHCP Server SHOULD NOT provide the PSK unless requested explicitly by the DHCP Client. Similarly, the DHCP Client MUST NOT request the PSK if the channel between the DHCP Client and the DHCP Server is not trusted.

This option follows recommendation of section 5.9 of [I-D.ietf-dhc-option-guidelines].



- OPTION_PSK_CREDENTIAL: The opcode for the DHCP PSK Credential Option.

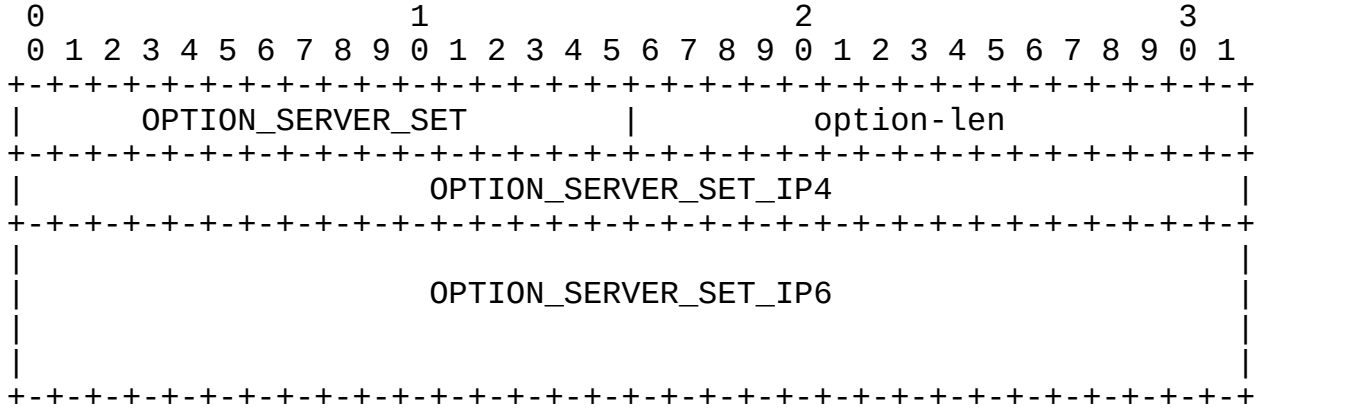
- option-len: length in octets of the option-data field as described in [RFC3315].

- psk: raw preshared key.

5.2.4.5. DHCP Server Set Option

The DHCP Server Set Option (OPTION_SERVER_SET) carries the IP addresses of the Public Authoritative Name Server Set. It is recommended to have one IP address, and eventually two if the Public Authoritative Server is dual stack. In any case no more than one IP address of each family is expected. The use of IP addresses instead of FQDN follows recommendation of [I-D.ietf-dhc-option-guidelines] section 8.

The DHCP Server Set Option encapsulates the DHCP Server Set IP4 Option (OPTION_SERVER_SET_IP4) and the DHCP Server Set IP6 Option (OPTION_SERVER_SET_IP6).



- OPTION_SERVER_SET: The option code for the DHCP Server Set Option.

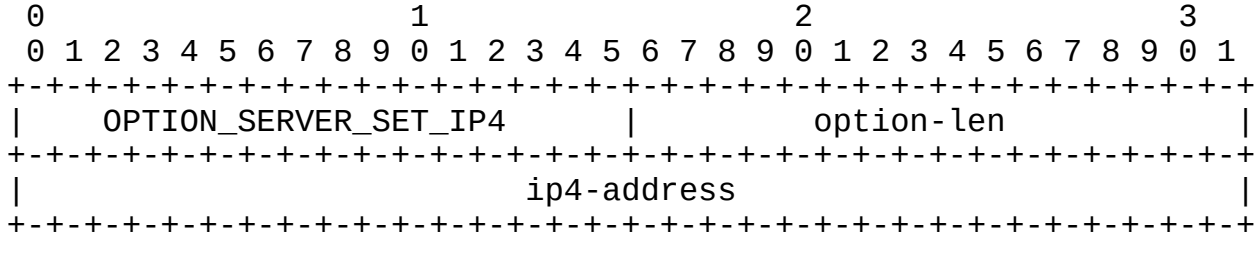
- option-len: length in octets of the option-data field as described in [RFC3315].

- OPTION_SERVER_SET_IP4: DHCP Server Set IP4 Option with IPv4 address associated to the Public Authoritative Name Server Set. This option is optional, however the DHCP server SHOULD provide at least one DHCP Server Set IP4 Option or one DHCP Server Set IP6 Option.

- OPTION_SERVER_SET_IP6: DHCP Server Set IP6 Option with IPv4 address associated to the Public Authoritative Name Server Set. This option is optional, however the DHCP server SHOULD provide at least one DHCP Server Set IP4 Option or one DHCP Server Set IP6 Option.

5.2.4.5.1. DHCP Server Set IP4 Option

The DHCP Server Set IP4 Option (OPTION_SERVER_SET_IP4) carries the IP address of the Public Authoritative Name Server Set. This option follows the recommendation of section 5.1 and 8 of [I-D.ietf-dhc-option-guidelines].



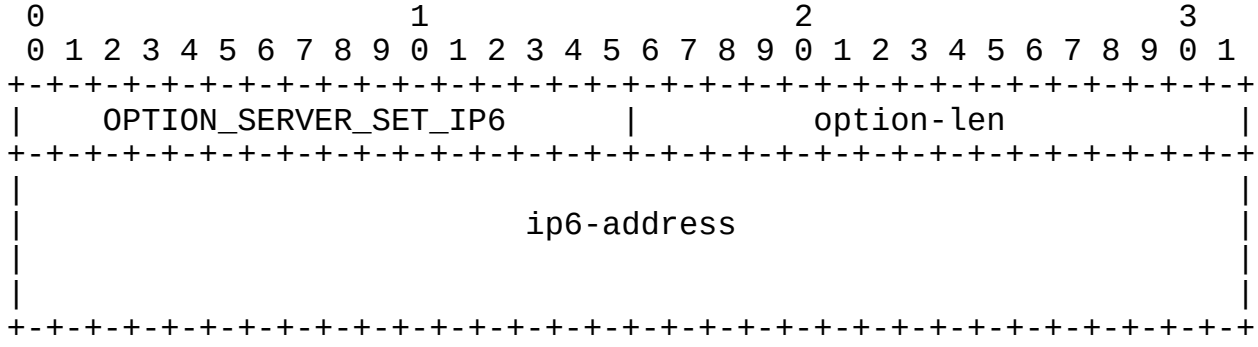
- OPTION_SERVER_SET_IP4: The option code for the DHCP Server Set IP4 Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- ip4-address: the 32 bit value of the IPv4 address.

5.2.4.5.2. DHCP Server Set IP6 Option

The DHCP Server Set IP6 Option (OPTION_SERVER_SET_IP6) carries the IP address of the Public Authoritative Name Server Set. This option follows the recommendation of section 5.1 and 8 of [I-D.ietf-dhc-option-guidelines].



- OPTION_SERVER_SET_IP6: The option code for the DHCP Server Set IP6 Option.

- option-len: length in octets of the option-data field as described in [RFC3315].

- ip6-address: the 128 bit value of the IPv6 address.

6. DHCPv6 Server Behavior

The DHCPv6 server MAY send DHCP Zone Public Master Option and/or DHCP Public Master Upload Option upon receiving or not a DHCP Option Request Option (ORO) by the DHCP Client.

The DHCP Server MAY send zero, one or multiple DHCP Zone Public Master Option or DHCP Public Master Upload Option.

The DHCP Server MUST send these option over a trusted channel. The PSK MUST NOT be sent over a non trusted channel.

If the DHCP Server is not provisioned properly, it SHOULD send empty DHCP Zone Public Master Option or DHCP Public Master Upload Option to indicate it supports the options, but they are not provisioned properly.

Although DHCP Zone Public Master Option and DHCP Public Master Upload Option are different options, they MAY be used together by the DHCP Client. Unless there are good reasons, DHCP Servers SHOULD provide in their DHCP Public Master Upload Option a Secure Channel for all Public Authoritative Masters mentioned in the DHCP Zone Public Master Option. In other words, for all Public Authoritative Masters mentioned in the DHCP Zone Public Master Option, the DHCP Server SHOULD send a DHCP Public Master Upload Option that provides a Secure Channel.

7. DHCPv6 Client Behavior

7.1. Sending an ORO

The DHCPv6 Client MAY enable different policies to configure the Home Network Naming Architecture. More specifically, it MAY allow an end user to set manually a specific naming configuration, which may disable automatic configuration of the Home Network Naming Architecture. If automatic configuration of the Home Network is not considered, the CPE SHOULD NOT send a DHCP Option Request Option (ORO) from the CPE for a DHCP DNS Public Authoritative Server Option or for a DHCP Public Master Upload Option. This would otherwise unnecessarily load the DHCPv6 Server of the ISP and the network.

The DHCP Client SHOULD NOT send and ORO for a DHCP Zone Public Master Option or a DHCP Public Master Upload Option if the channel between the DHCP Client and the DHCP Server is not trusted.

By sending an DHCP Option Request Option (ORO) for a DHCP Zone Public Master Option or a DHCP Public Master Upload Option, the CPE indicates that the response received from the DHCP Server will define how the Naming Architecture of the CPE is configured. However, this does not necessarily mean that the CPE will automatically configure its Naming Architecture according to according to the elements provided by the DHCPv6 Server. In fact the CPE MAY implement various policies to configure the Naming Architecture. Some policies MAY merge configuration manually provided by the end user and those provided by the DHCPv6 Server, others MAY only accept a subset of Public Authoritative Name Servers provided by the DHCPv6 Server. Defining the selection policies of the CPE is how of scope of this document.

The remaining of the section describes how the DHCPv6 Client handles information received by the DHCPv6 Server to configure the Naming Architecture. We assume that all information are considered. Although this document restricts the description to a single use case, we believe this will be the most common and basic use case. In addition, other uses cases implementing different configuration policies only requires small modifications to the use case considered in this section.

7.2. Receiving no DHCP Options

If the DHCPv6 Client does not receive any DHCP Zone Public Master Option or DHCP Public Master Upload Option from the DHCPv6 Server. The DHCPv6 Client assumes the DHCPv6 Server does not support the option. In this case, the Naming Architecture can only be set from local settings.

7.3. Receiving empty DHCP Options

By receiving empty DHCP Zone Public Master Option or empty DHCP Public Master Upload Option. The DHCP Client assumes the DHCP Server supports these options, but they are not or badly provisioned.

7.4. Receiving multiple DHCP Options

The DHCPv6 Client MAY receive one or multiple DHCP Zone Public Master Option and/or DHCP Public Master Upload Option. From these Option the CPE is expected to :

- 1: Collect all DHCP Zone Public Master Options.

- 2: Set the DNS Homenet Zone with the Public Authoritative Servers associated to each Registered Homenet Domain. This includes setting NS and Public Authoritative Server A/AAA RRsets. The

CPE is expected to proceed to some checks so these RRSets are valid.

- 3: Collect all DHCP Public Master Upload Option.

- 4: Build the master_secure_channel_dict dictionary that associates to each Public Authoritative Master a list of possible secure channels.

- 5: Upload the DNS Homenet Zone to the Public Authoritative Name Server Set so the zone can be published on the corresponding Public Authoritative Servers. The DNS(SEC) Homenet Zone is considered uploaded if for all Public Authoritative Masters of the DNS(SEC) Homenet Zone, upload (i.e. master/slave synchronization) succeeded at least with one Secure Channel. If for a given Public Authoritative Master, upload fails with all its Secure Channel, it MUST be removed from the DNS(SEC) Homenet Zone and upload MUST restarted. In other words synchronization MUST be performed again with all Public Authoritative Masters of the DNS(SEC) Homenet Zone (not only the remaining ones).

8. DHCPv6 Relay Behavior

DHCP Relay behavior are not modified by this document.

9. IANA Considerations

The DHCP options detailed in this document is:

- OPTION_ZONE_PUBLIC_MASTER: TBD

- OPTION_REGISTERED_DOMAIN_NAME: TBD

- OPTION_MASTER: TBD

- OPTION_MASTER_IP4: TBD

- OPTION_MASTER_IP6: TBD

- OPTION_MASTER_FQDN: TBD

- OPTION_PUBLIC_MASTER_UPLOAD: TBD

- OPTION_MASTER_FQDN_LIST: TBD

- OPTION_SECURE_CHANNEL: TBD

- OPTION_SECURE_PROTOCOL: TBD

- OPTION_SECURE_CREDENTIAL: TBD

- OPTION_SERVER_SET: TBD

- OPTION_SERVER_SET_IP4: TBD

- OPTION_SERVER_SET_IP6: TBD

The security-protocol detailed in this document are:

- NONE: TBD

- TSIG: TBD

- IPSEC: TBD

- SIG(0): TBD

The security-credential detailed in this document are:

- NONE: TBD

- PSK: TBD

10. Security Considerations

10.1. DNSSEC is recommended to authenticate DNS hosted data

The document describes how the Secure Delegation can be set between the Delegating DNS Server and the Delegated DNS Server.

Deploying DNSSEC is recommended since in some cases the information stored in the DNS is used by the ISP or an IT department to grant access. For example some Servers may performed a PTR DNS query to grant access based on host names. With the described Delegating Naming Architecture, the ISP or the IT department MUST take into consideration that the CPE is outside its area of control. As such, with DNS, DNS responses may be forged, resulting in isolating a Service, or not enabling a host to access a service. ISPs or IT department may not base their access policies on PTR or any DNS information. DNSSEC fulfills the DNS lack of trust, and we recommend to deploy DNSSEC on CPEs.

10.2. Channel between the CPE and ISP DHCP Server MUST be secured

In the document we consider that the channel between the CPE and the ISP DHCP Server is trusted. More specifically, we suppose the CPE is authenticated and the exchanged messages are protected. The current document does not specify how to secure the channel. [RFC3315] proposes a DHCP authentication and message exchange protection, [RFC4301], [RFC5996] propose to secure the channel at the IP layer.

In fact, the channel MUST be secured because the CPE provides necessary information for the configuration of the Naming Delegation. Unsecured channel may result in setting the Naming Delegation with an non legitimate CPE. The non legitimate CPE would then be redirected the DNS traffic that is intended for the legitimate CPE. This makes the CPE sensitive to three types of attacks. The first one is the Deny Of Service Attack, if for example DNS traffic for a lot of CPEs are redirected to a single CPE. CPE are even more sensitive to this attack since they have been designed for low traffic. The other type of traffic is the DNS traffic hijacking. A malicious CPE may redirect the DNS traffic of the legitimate CPE to one of its server. In return, the DNS Servers would be able to provide DNS Responses and redirect the End Users on malicious Servers. This is particularly used in Pharming Attacks. A third attack may consists in isolating a Home Network by misconfiguring the Naming Delegation for example to a non-existing DNS Server, or with a bad DS value.

10.3. CPEs are sensitive to DoS

The Naming Delegation Architecture involves the CPE that hosts a DNS Server for the Home Network. CPE have not been designed for handling heavy load. The CPE are exposed on the Internet, and their IP address is publicly published on the Internet via the DNS. This makes the Home Network sensitive to Deny of Service Attacks. The Naming Delegation Architecture described in this document does not address this issue. The issue is addressed by [I-D.mglt-homenet-front-end-naming-delegation].

11. Acknowledgment

We would like to thank Tomasz Mrugalski and Bernie Volz for their comments on the design of the DHCP Options.

12. Document Change Log

[RFC Editor: This section is to be removed before publication]

-00: version published in the homenet WG. Major modifications are:

- Reformatting of DHCP Options: Following options guide lines

- DHCPv6 Client behavior: Following options guide lines

- DHCPv6 Server behavior: Following options guide lines

-00: First version published in dhc WG.

13. Pseudo Code

This section is informational. It aims at illustrating how options MAY be handled by the DHCP Client or the DHCP Server. Not all the DHCP Options described in the document are considered. This section is not normative and implementation MAY differ.

13.1. DHCP Zone Public Master Option

13.1.1. Unpacking a DHCP Zone Public Master Option

```
## We consider the following object for the CPE:
## Class cpe
##    self.ip4_list
##    self.ip6_list
##    self.fqdn

receive_dhcp_zone_public_master_option(OPTION_ZONE_PUBLIC_MASTER):
    ## Checking existence of Registered Domains
    if OPTION_REGISTERED_DOMAIN_NAME is empty or missing:
        ignore OPTION_ZONE_PUBLIC_MASTER
    ## Checking existence of Public Authoritative Masters
    if OPTION_ZONE_PUBLIC_MASTER has no OPTION_MASTER options:
        build_option_master(cpe.fqdn, cpe.ip4_list, cpe.ip6_list)

    ## select each DNS Homenet Zone
    for zone_name in OPTION_REGISTERED_DOMAIN_NAME:
        ## adds Public Authoritative Master information to the
        ## zone_name. Typically this may consists in adding the
        ## lines:
        ## zone_name   NS master_fqdn
        ## master_fqdn A ip4
        ## master_fqdn A ip6
        for each OPTION_MASTER:
            (fqdn, ip4_list, ip6_list) = \
                get_master_option_info(OPTION_MASTER)
            add_ns(fqdn, zone_name)
            add_a(fqdn, ip4_list, zone_name)
            add_aaa(fqdn, ip6_list, zone_name)
```

Fig 11: Pseudo code for receiving a DHCP Zone Public Master Option

13.1.2. Packing a DHCP Zone Public Master Option

The pseudo code for sending a DHCP Zone Public Master Option is presented below. It is informational and intedns to illustrates text above. Implementation MAY be different.

```
## We consider the following objects for Public Authoritative Master
## Class master
##    self.ip4_list
##    self.ip6_list
##    self.fqdn


build_dhcp_zone_public_master_option():
    ## Collect all Registered Domain and associate the list of
```

```
      ## Public Authoritative Master. One way it to build the
      ## registered_domain_dict = {registered_domain:[master_list]}
      tmp_rd_dict = build_registered_domain_dict()

      ## Remove void registered domain names,
      ## Factorize registered_domain_dict and output
      rd_dict = factorize_registered_domain_dict(tmp_rd_dict)

      ## Build DHCP Zone Public Master Option
      for registered_domain_list, master_list in rd_dict.items():
          ## Builds the DHCP Zone Public Master Option Data Payload
          data = \
          build_registered_domain_name_option(registered_domain_list)
          ## Concatenation with DHCP Public Authoritative Master
          ## Options
          for master in master_list:
              data += build_master_option(master)

          ## Build the  DHCP Zone Public Master Option
          return build_header_zone_public_master(data) + data
```

Fig 12: Pseudo code for sending DHCP Zone Public Master Option

13.1.3. DHCP Master Option

13.1.3.1. Unpacking a DHCP Master Option

```
   def get_master_option_info(OPTION_MASTER):
       if OPTION_MASTER is empty:
           ## Consider the CPE for the Public Authoritative Master
           ## or ignore the option
           ## build_option_master(cpe.fqdn, cpe.ip4_list, cpe.ip6_list)
           ignore OPTION_MASTER

       if OPTION_MASTER_FQDN is empty or missing:
           ignore OPTION_MASTER
       if multiple OPTION_MASTER_IP4 or\
          multiple OPTION_MASTER_IP4:
           ignore OPTION_MASTER

       fqdn = get_fqdn(OPTION_MASTER_FQDN)
       ip4_list = []
       ip6_list = []
       ## collect Public Authoritative Master's IP addresses
       if OPTION_MASTER_IP4 exists:
           append(ip4_list, get_ip4(OPTION_MASTER_IP4))
```

```
    if OPTION_MASTER_IP6 exists:
        append(ip4_list, get_ip4(OPTION_MASTER_IP4))

    ## if no IP addresses are provided perform a DNSSEC
    ## resolution
    if len(ip4_list) == 0 and len(ip6_list) == 0:
        ip4_list = dig(fqdn, A)
        ip6_list = dig(fqdn, AAAA)
```

Fig 13: Pseudo code for Unpacking DHCP Master Option

13.1.3.2. Packing a DHCP Master Option

The pseudo code illustrates how the DHCP Server builds a DHCP Master Option.

```
def build_master_option(fqdn, ip4_list, ip6_list):
    ## Do not build the data payload of the  DHCP Master Option
    ## if fqdn is empty or a null string
    if fqdn is empty or fqdn has more than one fqdn:
        return error
    data = build_master_fqdn_option(fqdn)
    if ip4_list is empty:
        ip4_list = dig(fqdn, A)
    if ip6_list is empty:
        ip6_list = dig(fqdn, AAAA)
    if ip4_list is empty and ip6_list is empty:
        return error
    if  ip4_list is not empty:
        data += build_master_ip4_option(ip4_list)
    if  ip6_list is not empty:
        data += build_master_ip6_option(ip6_list)
    return build_header_master(data) + data
```

Fig 14: Pseudo code for Packing DHCP Master Option

13.2. DHCP Public Master Upload Option

13.2.1. Unpacking a DHCP Public Master Upload Option

The pseudo code for building the binding between Public Authoritative Master and Secure Channel MAY be as follows:

```
## We consider the master_secure_channel_dict that associates
## for each master a list of Secure Channel
```

```
   ## master_secure_channel_dict = {master: [secure_channel], ..., }

   ## This function is used to add an entry to the
   ## master_secure_channel_dict
   def get_master_upload_option_info(OPTION_PUBLIC_MASTER_UPLOAD):
       if OPTION_MASTER_FQDN_LIST is not unique or\
          OPTION_SECURE_CHANNEL does not exist:
           ignore OPTION_PUBLIC_MASTER_UPLOAD

       secure_channel_list = []
       for all OPTION_SECURE_CHANNEL:
           sc = get_secure_channel_info(OPTION_SECURE_CHANNEL)
           secure_channel_list.append(sc)

       for each master in OPTION_MASTER_FQDN_LIST:
           master_secure_channel_dict[master] = secure_channel_list
```

Fig 15: Pseudo code for receiving a DHCP Public Master Upload Option

13.2.2. DHCP Secure Channel Options

13.2.2.1. Unpacking a DHCP Secure Channel Option

```
   ## We consider the secure_channel object
   ## Class Secure_channel:
   ##    self.protocol
   ##    self.credential
   ##    self.server_set_ip4
   ##    self.server_set_ip6

   def get_secure_channel_option_info(OPTION_SECURE_CHANNEL):

       if OPTION_SECURE_PROTOCOL is not unique or \
          OPTION_SECURE_CREDENTIAL is not unique or\
          OPTION_SERVER_SET is not unique:
           ignore OPTION_SECURE_CHANNEL

       protocol = \
           get_secure_protocol_option_info(OPTION_SECURE_PROTOCOL)
       credential = \
           get_secure_credential_option_info(OPTION_SECURE_CREDENTIAL)
       ip4, ip6 = \
          get_server_set_option_info(OPTION_SERVER_SET)

       return(Secure_channel(protocol, credential, ip4, ip6))
```

Fig 16: Pseudo code for receiving a DHCP Secure Channel Option

14. References

14.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

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

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 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.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", RFC 6672, June 2012.

14.2. Informational References

[I-D.ietf-dhc-option-guidelines] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", draft-ietf-dhc-option-guidelines-14 (work in progress), September 2013.

[I-D.mglt-homenet-front-end-naming-delegation] Migault, D., Cloetens, W., Griffiths, C., and R. Weber, "IPv6 Home Network Naming Delegation", draft-mglt-homenet-front-end-naming-delegation-02 (work in progress), July 2013.

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

Authors' Addresses

Daniel Migault
Francetelecom - Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: mglt.ietf@gmail.com

Wouter Cloetens
SoftAtHome
vaartdijk 3 701
3018 Wijgmaal
Belgium

Email: wouter.cloetens@softathome.com

Chris Griffiths
Dyn
150 Dow Street
Manchester, NH 03101
US

Email: cgriffiths@dyn.com
URI: http://dyn.com

Ralf Weber
Nominum
2000 Seaport Blvd #400
Redwood City, CA 94063
US

Email: ralf.weber@nominum.com
URI: http://www.nominum.com