DHC
Internet-Draft
Intended status: Standards Track
Expires: January 06, 2014

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

July 05, 2013

DHCP DNS Public Authoritative Server Option
draft-mglt-dhc-public-authoritative-server-option-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 option that provides the CPE all necessary parameters to set up the home network naming architecture.

First, this DHCP option provides automatic configuration and avoids most end users' misconfigurations. 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.

Copyright Notice

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 defines how the CPE and the Public Authoritative Servers interact together, so 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 the DNS Public Authoritative Server DHCP option (DNS_PUBLIC_AUTHORITATIVE_SERVER) that provides 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 DNS Public Authoritative Server DHCP option (DNS_PUBLIC_AUTHORITATIVE_SERVER) and Section 5 describes the format of this option and Section 6 details the exchange between the CPE and the DHCPv6 Server.

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

The CPE requests the necessary parameters to set its home network naming configuration to the DHCP server. The DHCP server MAY be, for example, the one of its ISP, that already provides the IPv6 prefix to the CPE.

The CPE sends an Option Request DHCP Option (ORO) [RFC3315] for the DHCP DNS Public Authoritative Server Option (DNS_PUBLIC_AUTHORITATIVE_SERVER)

If available, the DHCP server sends back one or more DHCP DNS Public Authoritative Server Option (DNS_PUBLIC_AUTHORITATIVE_SERVER), depending if the end user has registered to one or multiple Public Authoritative Servers.

A CPE MAY be associated to one or multiple Registered Homenet Domain and one or multiple Public Authoritative Servers. The CPE builds a zone for each Registered Homenet Domain. These zones are uploaded / synchronized with their associated Public Authoritative Servers. Note that synchronization is performed through master / slave configuration of the DNS servers, thus Public Authoritative Servers are configured to host specific Registered Homenet Domains. On the other hand, a given Homenet Zone MAY be hosted by multiple Public Authoritative Servers. The CPE MUST build properly the DNS Homenet Zone and synchronize properly the hidden master and slaves for the synchronizations.

In order to configure properly the DNS Homenet Zone, the CPE SHOULD collect the list of Registered Homenet Domain and their associated Public Authoritative Servers. For each Registered Homenet Domain, the CPE lists the Public Authoritative Servers FQDN and set them as authoritative Name Server (RRset NS) for the zone. The CPE MAY also add in the DNS Homenet Zone their IP addresses (RRsets A or AAAA). This FQDN and IP addresses associated are designated as the Public Authoritative Master(s).

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.

In order to synchronize the DNS Homenet Zone with a Public Authoritative Server, the CPE needs to know how to establish a secure channel with the Public Authoritative Server. The Public Authoritative Server MAY have dedicated servers working as slave to synchronize the DNS Homenet Zone with the CPE. These servers are called Public Authoritative Name Server Set. In addition to these servers, the CPE MUST know which security protocol can be used to secure the channel as well as the security credential. In this document, we only considered Pre-Shared Key (PSK).

As a result, the DHCP DNS Public Authoritative Server Option (DNS_PUBLIC_AUTHORITATIVE_SERVER) carries:

- Registered Homenet Domain List: the list of Registered Homenet Domain the Public Authoritative Server hosts.

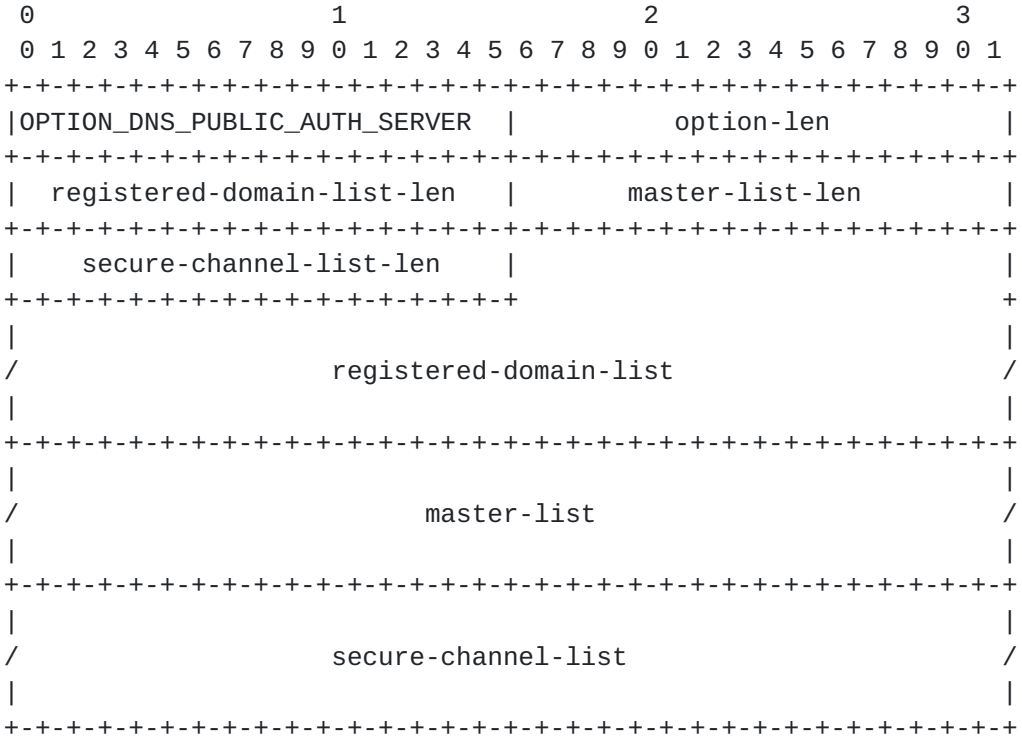
- Master : the Public Authoritative Master(s), that is to say the FQDNs provided in the NS RRsets of the Homenet Zones associated to each of the Registered Homenet Domains. IP addresses are derived by the CPE thanks to a DNS(SEC) resolutions.

- Secure Channel: the Public Authoritative Name Server Set , that is the FQDN the CPE MUST securely synchronize its DNS Homenet Zone with. This field MUST also specify, the security protocol as well as the security material.

5. Payload Description

5.1. DNS Public Authoritative Server Option

The DHCP DNS Public Authoritative Server Option is constituted of three ordered sub payloads: the registered-domain-list, the master-list and the secure-channel-list payload.



- option-code: OPTION_DNS_PUBLIC_AUTH_SERVER

- option-len: length of the OPTION_DNS_PUBLIC_AUTH_SERVER field, the option-code and the option-message in octets.

- registered-domain-list-len: Length in octets of the list of Registered Homenet Domains field.

- master-list-len: Length in octets of the list of the master-list field.

- secure-channel-list-len: Length in octets of the Secure Channels field.

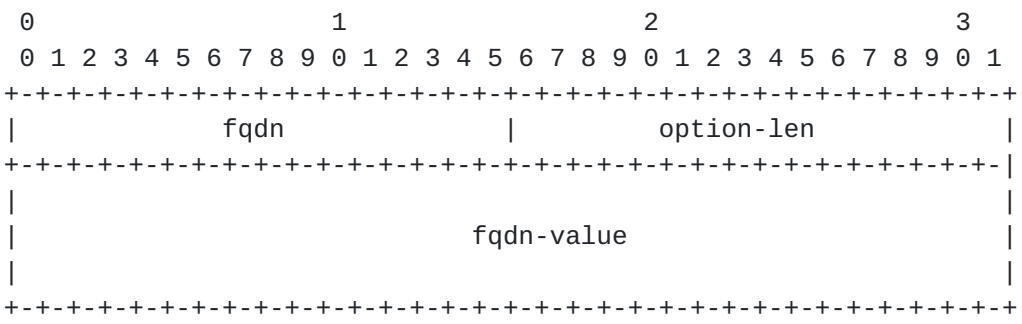
- registered-domain-list: The list of Registered Homenet Domains.

- master-list: The list of Public Authoritative Master(s).

- secure-channel-list: The list of Secure Channels

5.2. registered-domain-list

The registered-domain-list contains a list of fqdn payloads. The fqdn payload is as described below:



- payload-code: fqdn

- option-len: length of the fqdn field, the payload-code and the payload-message in octets.

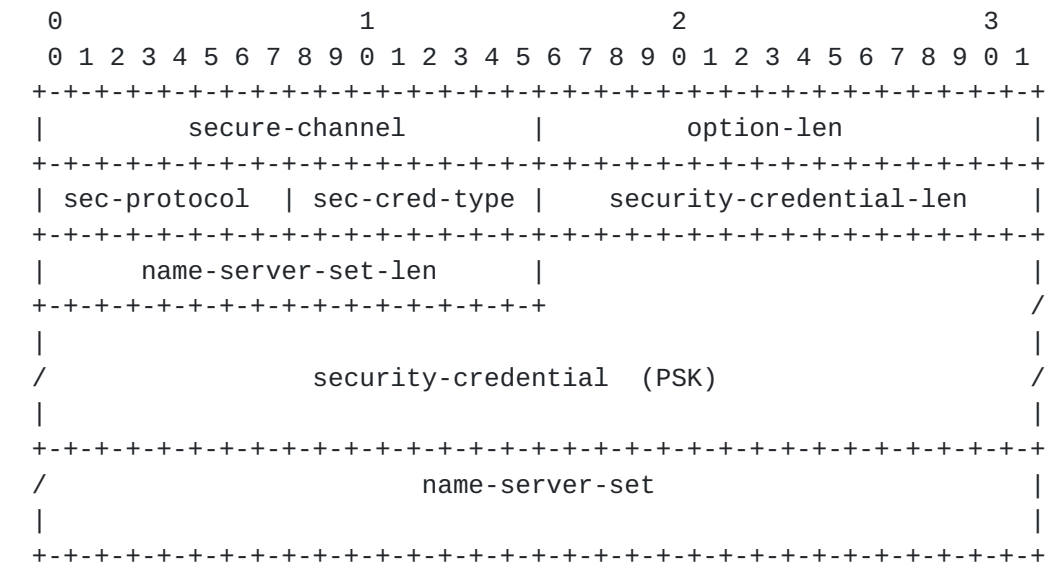
- fqdn-value: fqdn value as specified in [RFC1035]

5.3. master-list payload

The master-list payload contains a list of fqdn payloads. The fqdn payload is defined in Section 5.2.

5.4. secure-channel-list payload

The registered-domain-list contains a list of secure-channel payloads. The secure-channel payload is described below.



- payload-code: secure-channel-list. Although not necessary, since payloads are ordered, we provide this code to ease implementation and future options.

- option-len: Length of the delegated-naming-action-list field, the status-code and the status-message in octets.

- sec-protocol: the protocol that secures the exchanges between the CPE and the Public Authoritative Server. Possible protocols are NONE, TSIG, IPSEC.

- sec-cred-type: the type of credential used between the CPE and the Public Authoritative Server. The current document considers only PSK that can be used with any of the sec-protocol.

- security-credential-len: length of the delegated-naming-action-list field, the sec-cred-type and the security-credential-len in octets.

- security-credential: the security credential. In this document, the security credential is of type PSK.

- name-server-set-len: length of the name-server-set field and the name-server-set-len in octets.

- name-server-set: Public Authoritative Name Server Set encoded as specified in [RFC1035]. Only the FQDN representation is considered in this document.

6. Exchange Details

This section details the DHCPv6 exchange between the DHCPv6 server and the CPE.

6.1. DHCPv6 Server

The DHCPv6 server MUST NOT send a DHCP DNS Public Authoritative Server Option (DNS_PUBLIC_AUTHORITATIVE_SERVER) if not requested by the CPE through the DHCP Option Request Option (ORO).

In the remaining of this section we suppose the DHCPv6 Server has received a DHCP Option Request Option (ORO) from the CPE for a DHCP DNS Public Authoritative Server Option (DNS_PUBLIC_AUTHORITATIVE_SERVER).

If the DHCPv6 Server does not understand the DHCP DNS Public Authoritative Server Option, it ignores the Option as specified in [RFC3315].

If the DHCPv6 has no specific configuration, it MUST return a DHCP DNS Public Authoritative Server Option with the len registered-domain-list-len, master-list-len and secure-channel-list-len set to zero. This response is called the Zero Response and indicates that there are not enough arguments to set the home network architecture.

The registered-domain-list is mandatory. If it does not exists, and Zero Response MUST be sent.

A zero length for master-list indicates the CPE hosts the zone. In this case, a zero length secure-channel-list is expected.

6.2. CPE

In this section we assume the CPE has sent a DHCP Option Request Option (ORO) from the CPE for a DHCP DNS Public Authoritative Server Option (DNS_PUBLIC_AUTHORITATIVE_SERVER).

An Zero Response indicates the DHCPv6 Server has not a specific configuration for the CPE.

A response with an registered-domain-list set to zero MUST be ignored.

A zero length for master-list indicates the CPE hosts the zone. A non zero length secure-channel-list MUST be ignored.

7. IANA Considerations

The DHCP options detailed in this document is:

- OPTION_DNS_PUBLIC_AUTH_SERVER: TBD

The payload detailed in this document are:

- fqdn: TBD

- secure-channel: TBD

The security-protocol detailed in this document are:

- NONE: TBD

- TSIG: TBD

- IPSEC: TBD

The security-credential detailed in this document are:

- NONE: TBD

- PSK: TBD

8. Security Considerations

8.1. 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.

8.2. 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.

8.3. 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].

9. Acknowledgment

10. References

10.1. Normative References

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

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

[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.

10.2. Informational References

[I-D.mglt-homenet-front-end-naming-delegation] Migault, D., Cloetens, W., Lemordant, P., and C. Griffiths, "IPv6 Home Network Front End Naming Delegation", draft-mglt-homenet-front-end-naming-delegation-01 (work in progress), November 2012.

[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