HOMENET
Internet-Draft
Intended status: Standards Track
Expires: August 17, 2014

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

February 13, 2014

DHCP Options for Homenet Naming Architecture
draft-mglt-homenet-naming-architecture-dhc-options-01.txt

Abstract

The home network naming architecture 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 August 17, 2014.

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.

- DNS Homenet Zone Template: The template used as a basis to generate the DNS Homenet Zone.

- DNS Homenet Reverse Zone: The reverse zone file associated to the DNS Homenet Zone.

- Public Authoritative Master(s): are the visible name server hosting the DNS Homenet 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.

- Reverse Public Authoritative Master(s): are the visible name server hosting the DNS Homenet Reverse Zone. End users'

resolutions for the Homenet Domain are sent to this server, and this server is a master for the zone.

- Reverse Public Authoritative Name Server Set: is the server the CPE synchronizes the DNS Homenet Reverse 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

[I-D.mglt-homenet-front-end-naming-delegation] defines a homenet naming architecture that enables CPE to outsource their naming service to Public Authoritative Masters. This document describes DHCP options that makes possible any CPE to configure automatically the homenet naming architecture.

More specifically, when the CPE is plugged, it downloads the DNS Homenet Zone Template. This template is used to generate the DNS Homenet Zone, for according to specific CPE configurations or to newly attached devices that need to be accessed from the outside Internet. Finally, the CPE uploads the DNS Homenet Zone file on the Public Authoritative Name Server Sets that are in charge of publishing the zone on the Internet - on the Public Authoritative Master(s). In the case, the DNS Homenet Zone is static, DNS update [RFC2136] [RFC3007] might be considered. However, [I-D.mglt-homenet-front-end-naming-delegation] recommends uploads is performed by setting a master / slave synchronization between the CPE and the Public Authoritative Name Server Sets, with a hidden master hosted by the CPE. This is actually the way to do when data MAY be subject to change, and this is the alternative we consider in this document.

In order to set the master / slave synchronization between the CPE and the Public Authoritative Name Server Sets, the CPE and the Public Authoritative Name Server Sets SHOULD agree on the 1) the zone to be synchronized, 2) the IP address used by both the CPE for the hidden master. In this document we assume that synchronization is performed on both side on port 53. The zone to be synchronized is the one associated to the Registered Homenet Domain and is mentioned in the DNS Homenet Zone Template. This means the Registered Homenet Domain provided in the DNS Homenet Zone Template MAY not be modified by the CPE and MAY be known by the Public Authoritative Name Server Sets. Although this is not mandatory, this document assumes so. When the CPE sends a NOTIFY [RFC1996] message to the Public Authoritative Name Server Sets reads the Registered Homenet Domain and check the NOTIFY is sent by the authorized master. This can be done using the shared secret (TSIG) or the public key (SIG(0)). Once the NOTIFY has been authenticated, the Public Authoritative Name Server Sets MAY consider

the source IP address of the NOTIFY query to configure the masters attributes.

[QUESTION Do we have to consider different port of port 53 is fine. I guess it is fine.]

Once the DNS Homenet Zone has been generated, the CPE generates the DNS Homenet Reverse Zone before uploading it on the Reverse Public Authoritative Name Server Sets. Note that the Reverse Public Master can be easily derived from the IP prefix delegated to the CPE. However, the DNS Homenet Reverse Zone may not be sent to the Reverse Public Master, but instead the Reverse Public Authoritative Name Server Sets that are in charge of publishing the zone on the Reverse Public Master.

Similarly, the CPE and the Reverse Public Authoritative Name Server Sets configure set a master / slave synchronization. Note that with the reverse zone, the domain name is agreed by both the CPE and the Reverse Public Authoritative Name Server Sets. More specifically, the zone is not modified by the CPE and is necessarily the one provided by the ISP.

The DNS Homenet Zone Template, is provided to the CPE by the DHCP server via the DHCP Zone Template Option (OPTION_DNS_ZONE_TEMPLATE). This option contains a FQDN. In order to download the DNS Homenet Zone Template, the CPE sends a DNS query with type AXFR [RFC5936]. If this exchange needs to be protected or authenticated, TSIG [RFC2845], [RFC2930] or SIG(0) [RFC2931]may be used. The DHCP Zone Template Option indicates which security mechanisms are supported by the DNS authoritative server. Note that integrity protection may be performed by DNSSEC [RFC4033], [RFC4034], [RFC4035] only and may not require additional protections.

The DHCP Public Authoritative Name Server Set Option (OPTION_NAME_SERVER_SET) provides the Public Authoritative Name Server Set the DNS Homenet Zone is uploaded to. This operation SHOULD be done in a secure way, and this option specifies the supported security mechanisms used by the Public Authoritative Name Server (TSIG or SIG(0) [RFC3007]).

This document considers that uploading the DNS Homenet Zone is performed using a master / slave architecture between the CPE and the Public Authoritative Name Server Set. The CPE gets the Registered Homenet Domain from the DNS Homenet Zone Template and the IP address of the Public Authoritative Name Server Set from the DHCP Public Authoritative Name Server Set Option (OPTION_NAME_SERVER_SET). This IP address is used to send a NOTIFY query, protected with TSIG or SIG(0). This identifies the Registered Homenet Domain as well as the

sender. Then the Public Authoritative Name Server Set can finalize its slave configuration by considering the IP address of the NOTIFY query.

Similarly, the DHCP Reverse Public Authoritative Name Server Set Option (OPTION_REVERSE_NAME_SERVER_SET) provides the Reverse Public Authoritative Name Server Set the Reverse DNS Homenet Zone is uploaded to. This operation SHOULD be done in a secure way, and this option specifies the supported security mechanisms used by the Public Authoritative Name Server (TSIG or SIG(0)).

In case TSIG is used to secure the exchanges between the CPE and the Public Authoritative Name Server Sets or the Reverse Public Authoritative Name Server Sets. The CPE MAY request and get this shared secret from the DHCP Server via the DHCP TSIG Public Authoritative Name Server Set Option (OPTION_TSIG_NAME_SERVER_SET) and DHCP TSIG Reverse Public Authoritative Name Server Set Option (OPTION_TSIG_REVERSE_NAME_SERVER_SET). Note that sending this information has significant security issues and SHOULD be done in a controlled and cautious way.

3.1. DNS Homenet Zone Template Considerations

The DNS Homenet Zone Template contains at least the related fields of the Public Authoritative Master(s) as well as the Homenet Registered Domain, that is SOA, and NS fields. This template MAY be generated automatically by the owner of the DHCP Server. For example, an ISP MAY provide a default Homenet Registered Domain as well as default Public Authoritative Master(s). This default settings SHOULD provide the CPE the necessary pieces of information to set the homenet naming architecture.

If the DNS Homenet Zone Template is not subject to modifications or updates, the owner of the template MAY only use DNSSEC to enable integrity check.

The DNS Homenet Zone Template MAY be subject to modification by the CPE. The advantage of using the standard DNS zone format is that standard DNS update mechanisms [RFC2136], [RFC3007] can be used to perform updates. This updates MAY be accepted or rejected by the owner of the DNS Homenet Zone Template. Policies that defines what is accepted or rejected is out of scope of this document. However, in this document we assume the Registered Homenet Domain is used as an index by the Public Authoritative Name Server Set, and SIG(0), TSIG are used to authenticate the CPE. As a result, the Registered Homenet Domain MUST NOT be modified unless the Public Authoritative Name Server Set can handle with it.

If updates on the DNS Homenet Zone Template are considered, then they SHOULD be performed using an authenticated and secure channel. This document lists TSIG and SIG(0) as mechanisms to secure the transactions. Bootstrap mechanisms as those described in [I-D.andrews-dnsop-pd-reverse] for SIG(0) or using the DHCP TSIG Public Authoritative Name Server Set Option (OPTION_TSIG_NAME_SERVER_SET) as described in this document.

3.2. DNS Homenet Zone Considerations

The DNS Homenet Zone is generated from the DNS Homenet Zone Template. How the DNS Homenet Zone is generated is out of scope of this document. In some cases, the DNS Homenet Zone MAY be the exact copy of the DNS Homenet Zone Template. In other cases, it MAY be generated from the DNS Homenet Zone Template with additional RRsets. In some other cases, the DNS Homenet Zone MAY be generated without considering the DNS Homenet Zone Template, but only considering specific configuration rules.

In the current document the CPE only sets a single zone that is associated with one single Homenet Registered Domain. The domain MAY be assigned by the owner of the DNS Homenet Zone Template. This constrain does not prevent the CPE to use multiple domain names. How additional domains are considered is out of scope of this document. One way to handle these additional zones is to configure static redirections to the DNS Homenet Zone using CNAME [RFC2181], [RFC1034], DNAME [RFC6672] or CNAME+DNAME [I-D.sury-dnsext-cname-dname].

4. Payload Description

4.1. DHCP Zone Template Option

The DHCP Zone Template Option (OPTION_DNS_ZONE_TEMPLATE) Option provides the FQDN the CPE SHOULD query with a DNS query of type AXFR. The option also specifies which security protocols are available on the authoritative server. In addition, in order to limit the number of DNS resolutions, the option follows recommendations of Section 8 of [I-D.ietf-dhc-option-guidelines] and provide an IPv6 address of the dns authoritative server. In case the IPv6 address is not compatible with the CPE, or that the IPv6 address happens to be unreachable, the CPE SHOULD resolve the Zone Template FQDN using a resolver.

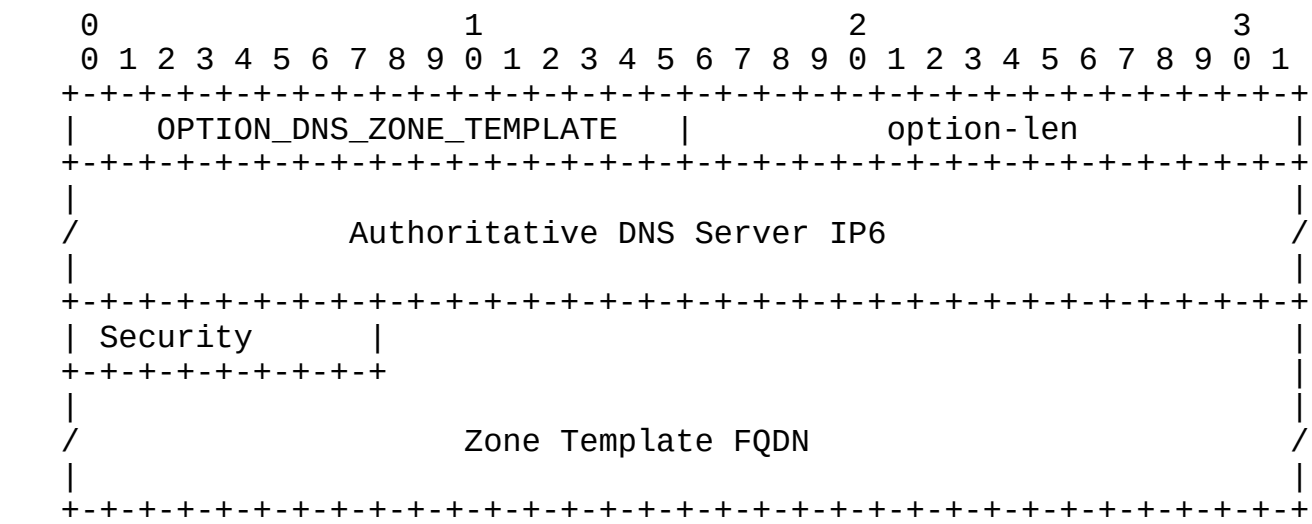

Fig 1: DHCP Zone Template Option

- OPTION_DNS_ZONE_TEMPLATE (variable): the option code for the DHCP Zone Template Option.

- option-len (16 bits): length in octets of the option-data field as described in [RFC3315].

- Authoritative DNS Server IP6 (128 bits): the IP address the AXFR DNS query is sent to.

- Security (8 bits): defines which security protocols are supported by the Authoritative DNS server. Bit 0 is set to indicate the AXFR query can be done with DNS without any additional security mechanisms. Bit 1 is set to mention TSIG is available to secure the transaction. Bit 2 is set to indicate SIG(0) is available to secure the DNS transaction.

- Zone Template FQDN FQDN (variable): the FQDN of the DNS server hosting the DNS Homenet Zone Template.

4.2. DHCP Public Authoritative Name Server Set Option

The DHCP Public Authoritative Name Server Set Option (OPTION_NAME_SERVER_SET) provides information so the CPE can upload the DNS Homenet Zone to the Public Authoritative Name Server Set. In order to limit the number of DNS resolutions, the option follows recommendations of Section 8 of [I-D.ietf-dhc-option-guidelines] and provide an IPv6 address of the Public Authoritative Name Server Set. If this IPv6 cannot be used by the CPE or is unreachable, the option provides the FQDN of the Public Authoritative Name Server Set. Finally, the option provides the security mechanisms that are

available to perform the upload. The upload is performed via a DNS master / slave architecture or DNS updates.

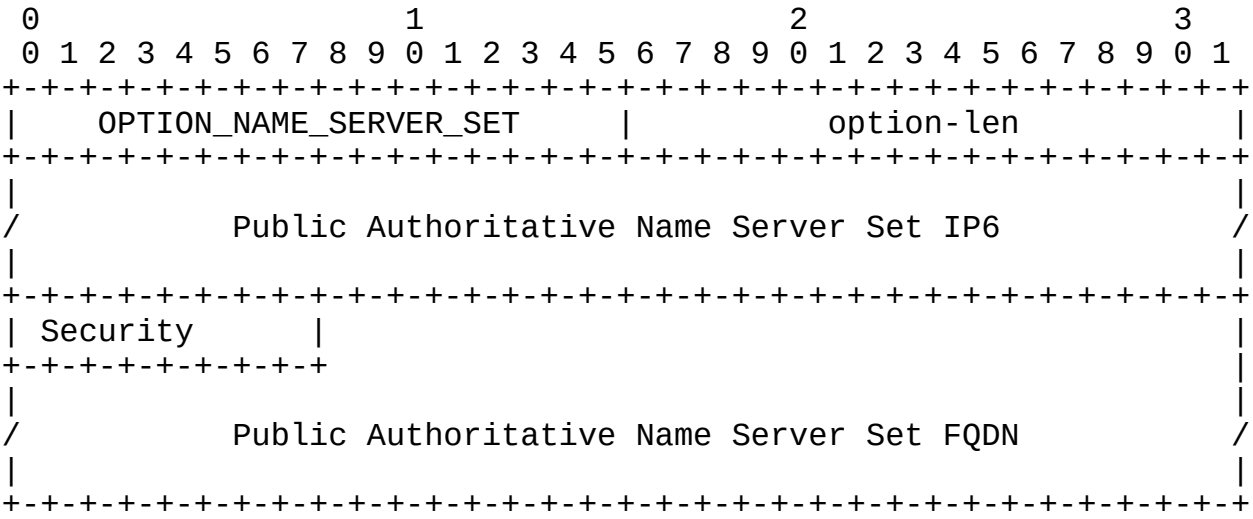

Fig 2: DHCP Public Authoritative Name Server Set Option

- OPTION_NAME_SERVER_SET (16 bits): the option code for the DHCP Public Authoritative Name Server Set Option.

- option-len (16 bits): length in octets of the option-data field as described in [RFC3315].

- Public Authoritative Name Server Set IP6 (128 bits): the IP address of the Public Authoritative Name Server Set. The DNS master / slave synchronization or DNS update query is performed between the CPE and this IP address.

- Security (8 bits): defines which security protocols are supported by the Public Authoritative Name Server Set. Bit 0 is set to indicate the AXFR query can be done with DNS without any additional security mechanisms. Bit 1 is set to mention TSIG is available to secure the transaction. Bit 2 is set to indicate SIG(0) is available to secure the DNS transaction.

- Public Authoritative Name Server Set FQDN (variable): The FQDN of the Public Authoritative Name Server Set.

4.3. DHCP Reverse Public Authoritative Name Server Set Option

The DHCP Reverse Public Authoritative Name Server Set Option (OPTION_REVERSE_NAME_SERVER_SET) provides information so the CPE can upload the DNS Homenet Zone to the Public Authoritative Name Server Set. In order to limit the number of DNS resolutions, the option

follows recommendations of Section 8 of [I-D.ietf-dhc-option-guidelines] and provide an IPv6 address of the Public Authoritative Name Server Set. If this IPv6 cannot be used by the CPE or is unreachable, the option provides the FQDN of the Public Authoritative Name Server Set. Finally, the option provides the security mechanisms that are available to perform the upload. The upload is performed via a DNS master / slave architecture or DNS updates.

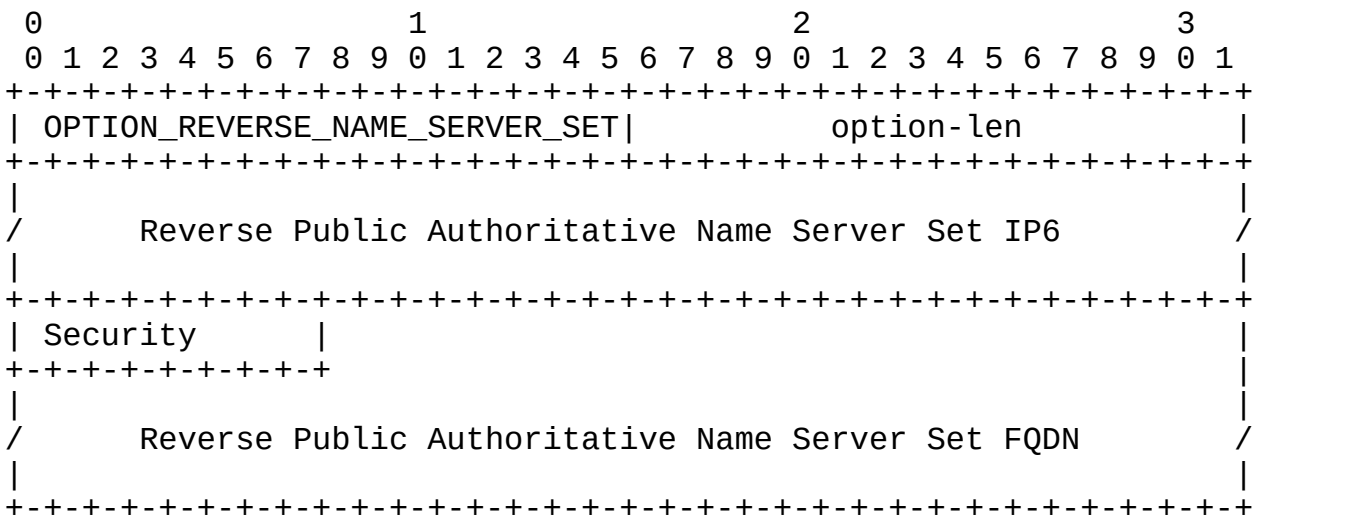

Fig 3: DHCP Reverse Public Authoritative Name Server Set Option

- OPTION_REVERSE_NAME_SERVER_SET (16 bits): the option code for the DHCP Reverse Public Authoritative Name Server Set Option.

- option-len (16 bits): length in octets of the option-data field as described in [RFC3315].

- Reverse Public Authoritative Name Server Set IP6 (128 bits): the IP address of the Reverse Public Authoritative Name Server Set. The DNS master / slave synchronization or DNS update query is performed between the CPE and this IP address.

- Security (8 bits): defines which security protocols are supported by the Public Authoritative Name Server Set. Bit 0 is set to indicate the AXFR query can be done with DNS without any additional security mechanisms. Bit 1 is set to mention TSIG is available to secure the transaction. Bit 2 is set to indicate SIG(0) is available to secure the DNS transaction.

- Reverse Public Authoritative Name Server Set FQDN (variable): The FQDN of the Reverse Public Authoritative Name Server Set.

4.4. DHCP TSIG Public Authoritative Name Server Set Option

The DHCP TSIG Public Authoritative Name Server Set Option carries the shared secret used for TSIG with the Public Authoritative Name Server Set.

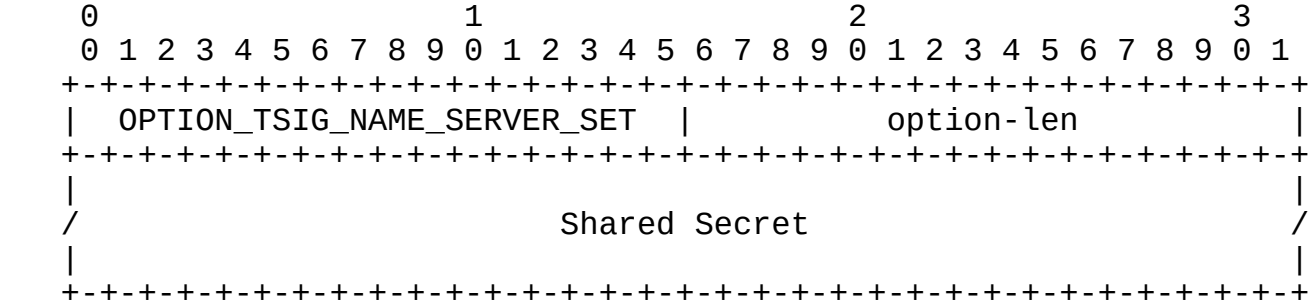

Fig 4: DHCP TSIG Public Authoritative Name Server Set Option

- OPTION_TSIG_NAME_SERVER_SET (16 bits): the option code for the DHCP TSIG Public Authoritative Name Server Set Option.

- option-len (16 bits): length in octets of the option-data field as described in [RFC3315].

- Shared Secret (variable): the Shared Secret used for TSIG.

4.5. DHCP TSIG Reverse Public Authoritative Name Server Set Option

The DHCP TSIG Reverse Public Authoritative Name Server Set Option carries the shared secret used for TSIG with the Reverse Public Authoritative Name Server Set.

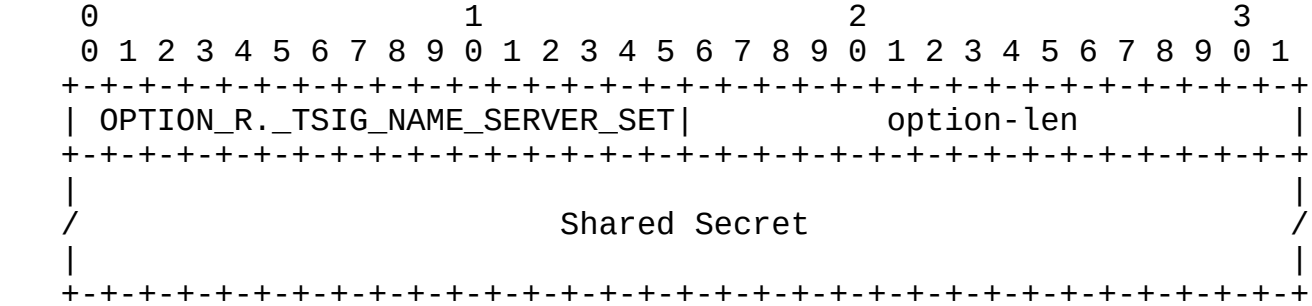

Fig 5: DHCP TSIG Reverse Public Authoritative Name Server Set Option

- OPTION_TSIG_REVERSE_NAME_SERVER_SET (16 bits): the option code for the DHCP TSIG Reverse Public Authoritative Name Server Set Option.

- option-len (16 bits): length in octets of the option-data field as described in [RFC3315].

- Shared Secret (variable): the Shared Secret used for TSIG.

5. DHCPv6 Server Behavior

The DHCP Server sends the DHCP Zone Template Option (OPTION_DNS_ZONE_TEMPLATE), DHCP Public Authoritative Name Server Set Option (OPTION_NAME_SERVER_SET), DHCP Reverse Public Authoritative Name Server Set Option (OPTION_REVERSE_NAME_SERVER_SET), DHCP TSIG Public Authoritative Name Server Set Option (OPTION_TSIG_NAME_SERVER_SET), DHCP TSIG Reverse Public Authoritative Name Server Set Option (OPTION_TSIG_REVERSE_NAME_SERVER_SET) upon request by the DHCP Client.

The DHCP Server MUST NOT send DHCP a TSIG Public Authoritative Name Server Set Option (OPTION_TSIG_NAME_SERVER_SET) or a DHCP TSIG Reverse Public Authoritative Name Server Set Option (OPTION_TSIG_REVERSE_NAME_SERVER_SET) over a channel that is not trusted.

6. DHCPv6 Client Behavior

The DHCP Client sends a DHCP Option Request Option (ORO) with the necessary DHCP options.

A CPE that does not use information provided by the network SHOULD NOT send any ORO for options described in this document. It MAY be for example a CPE that uses alternate Public Authoritative Name Server Set. In that case it SHOULD only send the an ORO request for the necessary options related to the Reverse Public Authoritative Name Server Set. Another example is when the CPE has already up-to date information.

A CPE that uses TSIG and has the Shared Secret stored on the device SHOULD NOT request any of the DHCP TSIG Public Authoritative Name Server Set Option (OPTION_TSIG_NAME_SERVER_SET) or the DHCP TSIG Reverse Public Authoritative Name Server Set Option (OPTION_TSIG_REVERSE_NAME_SERVER_SET).

Once the CPE has the necessary information to generate the DNS Homenet Zone and DNS Homenet Reverse Zone, as recommended by [I-D.mglt-homenet-front-end-naming-delegation], it MAY set the hidden master that synchronizes with the Public Authoritative Name Server Sets and Reverse Public Authoritative Name Server Sets. Alternatively, for very static zones, the CPE MAY use DNS update.

7. DHCPv6 Relay Behavior

DHCP Relay behavior are not modified by this document.

8. IANA Considerations

The DHCP options detailed in this document is:

- OPTION_DNS_ZONE_TEMPLATE: TBD

- OPTION_NAME_SERVER_SET: TBD

- OPTION_REVERSE_NAME_SERVER_SET: TBD

- OPTION_TSIG_NAME_SERVER_SET: TBD

- OPTION_TSIG_REVERSE_NAME_SERVER_SET: TBD

9. Security Considerations

9.1. 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.

9.2. Sending TSIG over the network is not recommended

Sending a DHCP TSIG Public Authoritative Name Server Set Option (OPTION_TSIG_NAME_SERVER_SET) or a DHCP TSIG Reverse Public Authoritative Name Server Set Option (OPTION_TSIG_REVERSE_NAME_SERVER_SET) is generally not recommended.

In non trusted environments, sending DHCP TSIG Options MUST NOT be performed.

If the DHCP Server identify the request from a device that is not expected to manage the DNS Homenet Zone, the DHCP TSIG Options MUST NOT be sent back.

In any case, sending these options MUST NOT be systematic. It MAY be performed at first boot, and then stored in the CPE. This would enable to perform a leaf-of-faith security.

9.3. 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.

9.4. 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].

10. Acknowledgment

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

11. Document Change Log

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

-02: Working Version Major modifications are:

- Redesigning options/scope: As suggested by Bernie Volz

-01: Working Version Major modifications are:

- Remove the DNS Zone file construction: As suggested by Bernie Volz

- DHCPv6 Client behavior: Following options guide lines

- DHCPv6 Server behavior: Following options guide lines

-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.

12. References

12.1. Normative References

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

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, August 1996.

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

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC2930] Eastlake, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[RFC2931] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[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.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

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

[RFC5936] Lewis, E. and A. Hoenes, "DNS Zone Transfer Protocol (AXFR)", RFC 5936, June 2010.

[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.

12.2. Informational 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-option-guidelines]
Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", draft-ietf-dhc-option-guidelines-17 (work in progress), January 2014.

[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-03 (work in progress), October 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
Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: daniel.migault@orange.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