HOMENET
Internet-Draft
Intended status: Standards Track
Expires: November 5, 2015

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

May 4, 2015

Outsourcing Home Network Authoritative Naming Service
draft-ietf-homenet-front-end-naming-delegation-02.txt

Abstract

CPEs are designed to provide IP connectivity to home networks. Most CPEs assign IP addresses to the nodes of the home network which makes it a good candidate for hosting the naming service. With IPv6, the naming service makes nodes reachable from the home network as well as from the Internet.

However, CPEs have not been designed to host such a naming service exposed on the Internet. This may expose the CPEs to resource exhaustion which would make the home network unreachable, and most probably would also affect the home network inner communications.

In addition, DNSSEC management and configuration may not be well understood or mastered by regular end users. Misconfiguration may also result in naming service disruption, thus these end users may prefer to rely on third party naming providers.

This document describes a homenet naming architecture where the CPEs manage the DNS zone associated to its home network, and outsources the naming service and eventually the DNSSEC management on the Internet to a third party designated as the Public Authoritative Servers.

Status of This Memo

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. Introduction

IPv6 provides global end to end IP reachability. To access services hosted in the home network with IPv6 addresses, end users prefer to use names instead of long and complex IPv6 addresses.

CPEs are already providing IPv6 connectivity to the home network and generally provide IPv6 addresses or prefixes to the nodes of the home network. This makes the CPEs a good candidate to manage binding between names and IP addresses of the nodes. In addition, [RFC7368] recommends that home networks be resilient to connectivity disruption from the ISP. This requires that a dedicate device inside the home network manage bindings between names and IP addresses of the nodes and builds the DNS Homenet Zone. All this makes the CPE the natural candidate for setting the DNS(SEC) zone file of the home network.

CPEs are usually low powered devices designed for the home network, but not for heavy traffic. As a result, hosting an authoritative DNS service on the Internet may expose the home network to resource exhaustion, which may isolate the home network from the Internet and affect the services hosted by the CPEs, thus affecting the overall home network communications.

In order to avoid resource exhaustion, this document describes an architecture that outsources the authoritative naming service of the home network. More specifically, the DNS(SEC) Homenet Zone built by the CPE is outsourced to Public Authoritative Servers. These servers publish the corresponding DN(SEC) Public Zone on the Internet. Section 4.1 describes the architecture. In order to keep the DNS(SEC) Public Zone up-to-date Section 5 describes how the DNS(SEC) Homenet Zone and the DN(SEC) Public Zone can be synchronized. The proposed architecture aims at deploying DNSSEC and the DNS(SEC) Public Zone is expected to be signed with a secure delegation. The zone signing and secure delegation can be performed either by the CPE or by the Public Authoritative Servers. Section 6 discusses these two alternatives. Section 7 discusses multiple views aspects and provide guidance to avoid them. Section 8 discusses the case of the reverse zone. Section 9 discusses how renumbering should be handled. Finally, Section 10 and Section 11 respectively discuss privacy and security considerations when outsourcing the DNS Homenet Zone.

3. 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 host 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 primary / secondary architecture. The Public Authoritative Server MAY use specific servers for the synchronization of the DNS Homenet Zone: the Public Authoritative Name Server Set as public available name servers for the Registered Homenet Domain.

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

- 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 primary / secondary architecture. The Public Authoritative Server acts as a secondary 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 Primary(ies).

- 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 Primary(ies).

- Public Authoritative Primary(ies): 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 primary for the zone.

- Public Authoritative Name Server Set: is the server the CPE synchronizes the DNS Homenet Zone. It is configured as a secondary and the CPE acts as primary. The CPE sends information so the DNSSEC zone can be set and served.

- Reverse Public Authoritative Primary(ies): 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 primary 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 secondary and the CPE acts as primary. The CPE sends information so the DNSSEC zone can be set and served.

4. Architecture Description

This section describes the architecture for outsourcing the authoritative naming service from the CPE to the Public Authoritative Primary(ies). Section 4.1 describes the architecture, Section 4.2 and Section 4.3 illustrate this architecture and shows how the DNS(SEC) Homenet Zone should be built by the CPE, as well as lists the necessary parameters the CPE needs to outsource the authoritative naming service. These two section are informational and non normative.

4.1. Architecture Overview

Figure 1 provides an overview of the architecture.

The home network is designated by the Registered Homenet Domain Name -- example.com in Figure 1. The CPE builds the DNS(SEC) Homenet Zone associated to the home network. How the DNS(SEC) Homenet Zone is built is out of the scope of this document. The CPE may host and involve multiple services like a web GUI, DHCP [RFC6644] or mDNS [RFC6762]. These services may coexist and may be used to populate the DNS Homenet Zone. This document assumes the DNS(SEC) Homenet Zone has been populated with domain names that are intended to be publicly published and that are publicly reachable. More specifically, names associated to services or devices that are not expected to be reachable from outside the home network or names bound to non globally reachable IP addresses MUST NOT be part of the DNS(SEC) Homenet Zone.

Once the DNS(SEC) Homenet Zone has been built, the CPE does not host the authoritative naming service for it, but instead outsources it to the Public Authoritative Servers. The Public Authoritative Servers take the DNS(SEC) Homenet as an input and publishes the DNS(SEC) Public Zone. In fact the DNS(SEC) Homenet Zone and the DNS(SEC) Public Zone have different names as they may be different. If the CPE does not sign the DNS Homenet Zone, for example, the Public Authoritative Servers may instead sign it on behalf of the CPE. Figure 1 provides a more detailed description of the Public Authoritative Servers, but overall, it is expected that the CPE provides the DNS(SEC) Homenet Zone, the DNS(SEC) Public Zone is derived from the DNS(SEC) Homenet Zone and published on the Internet.

As a result, DNS(SEC) queries from the DNS(SEC) Resolvers on the Internet are answered by the Public Authoritative Server and do not reach the CPE. Figure 1 illustrates the case of the resolution of node1.example.com.

```
   home network +-------------------+ Internet
                |                   |
                |        CPE        |
                |                   |         +----------------------+
   +-------+    |+-----------------+|         | Public Authoritative |
   |       |    || DNS(SEC) Homenet||         | Servers              |
   | node1 |    || Zone            ||         |+--------------------+|
   |       |    ||                 ||         ||DNS(SEC) Public Zone||
   +-------+    || Homenet Domain  ||=========||                    ||
                || Name            ||   ^     ||   (example.com)    ||
   node1.\      || (example.com)   ||   |     |+--------------------+|
   example.com  |+-----------------+|   |     +----------------------+
                +-------------------+   |          ^     |
                                Synchronization    |     |
                                                   |     |
         DNSSEC resolution for node1.example.com   |     v
                                              +----------------------+
                                              |                      |
                                              |   DNSSEC Resolver    |
                                              |                      |
                                              +----------------------+
```

Figure 1: Homenet Naming Architecture Description

The Public Authoritative Servers are described in Figure 2. The Public Authoritative Name Server Set receives the DNS(SEC) Homenet Zone as an input. The received zone may be transformed to output the DNS(SEC) Public Zone. Various operations may be performed here, however this document only considers zone signing as potential operation. This could occur only when the CPE outsources this operation to the Public Authoritative Name Server Set. On the other hand, if the CPE signs the DNSSEC Homenet Zone itself, the zone it collected by the Public Authoritative Name Server Set and directly transferred to the Public Authoritative Primary. Implications of such policy are detailed in Section 6 and Section 7.

```
                                      Internet

             +--------------------------------------------------------+
             |              Public Authoritative Servers              |
             +--------------------------------------------------------+

             +----------------------+         +----------------------+
             |                      |         |                      |
             | Public Authoritative |         | Public Authoritative |
             | Name Server Set      |         | Primaries            |
             |                      |         |                      |
             | +------------------+ |    X    | +------------------+ |
             | | DNS(SEC) Homenet | |    ^    | | DNS(SEC) Public  | |
   =========>| | Zone             | |    |    | | Zone             | |
       ^     | |                  | |    |    | |                  | |
       |     | | (example.com)    | |    |    | | (example.com)    | |
       |     | +------------------+ |    |    | +------------------+ |
       |     +----------------------+    |    +----------------------+
       |                         Homenet to Public Zone
   Synchronization                   transformation
   from the CPE
```

Figure 2: Public Authoritative Servers Description

4.2. Example: DNS(SEC) Homenet Zone

This section is not normative and intends to illustrate how the CPE builds the DNS(SEC) Homenet Zone.

As depicted in Figure 1 and Figure 2, the DNS(SEC) Public Zone is hosted on the Public Authoritative Primaries, whereas the DNS(SEC) Homenet Zone is hosted on the CPE. Motivations for keeping these two zones identical are detailed in Section 7, and this section considers that the CPE builds the zone that will be effectively published on the Public Authoritative Primaries. In other words "Homenet to Public Zone transformation" is the identity.

In that case, the DNS Homenet Zone should configure its Name Server RRset (NS) and Start of Authority (SOA) with the ones associated to the Public Authoritative Primaries. This is illustrated in Figure 3. public.primary.example.net is the FQDN of the Public Authoritative Primaries, and IP1, IP2, IP3, IP4 are the associated IP addresses. Then the CPE should add the different new nodes that enter the home network, remove those that should be removed and sign the DNS Homenet Zone.

```
$ORIGIN example.com
$TTL 1h

@  IN  SOA  public.primary.example.net
            hostmaster.example.com. (
      2013120710 ; serial number of this zone file
      1d         ; secondary refresh
      2h         ; secondary retry time in case of a problem
      4w         ; secondary expiration time
      1h         ; maximum caching time in case of failed
                 ; lookups
      )

@   NS  public.authoritative.servers.example.net

public.primary.example.net   A @IP1
public.primary.example.net   A @IP2
public.primary.example.net   AAAA @IP3
public.primary.example.net   AAAA @IP4
```

Figure 3: DNS Homenet Zone

The SOA RRset is defined in [RFC1033], [RFC1035] and [RFC2308]. This SOA is specific as it is used for the synchronization between the Hidden Primary and the Public Authoritative Name Server Set and published on the DNS Public Authoritative Primary.

- MNAME: indicates the primary. In our case the zone is published on the Public Authoritative Primary, and its name MUST be mentioned. If multiple Public Authoritative Primaries are involved, one of them MUST be chosen. More specifically, the CPE MUST NOT place the name of the Hidden Primary.

- RNAME: indicates the email address to reach the administrator. [RFC2142] recommends to use hostmaster@domain and replacing the '@' sign by '.'.

- REFRESH and RETRY: indicate respectively in seconds how often secondaries need to check the primary and the time between two refresh when a refresh has failed. Default value indicated by [RFC1033] are 3600 (1 hour) for refresh and 600 (10 minutes) for retry. This value MAY be long for highly dynamic content. However, Public Authoritative Primaries and the CPE are expected to implement NOTIFY [RFC1996]. Then short values MAY increase the bandwidth usage for secondaries hosting large number of zones. As a result, default values looks fine.

EXPIRE: is the upper limit data SHOULD be kept in absence of refresh. Default value indicated by [RFC1033] is 3600000 about 42 days. In home network architectures, the CPE provides both the DNS synchronization and the access to the home network. This device MAY be plugged and unplugged by the end user without notification, thus we recommend large period.

MINIMUM: indicates the minimum TTL. Default value indicated by [RFC1033] is 86400 (1 day). For home network, this value MAY be reduced, and 3600 (1 hour) seems more appropriated.

4.3. Example: CPE necessary parameters for outsourcing

This section specifies the various parameters required by the CPE to configure the naming architecture of this document. This section is informational, and is intended to clarify the information handled by the CPE and the various settings to be done.

Public Authoritative Name Server Set may be defined with the following parameters. These parameters are necessary to establish a secure channel between the CPE and the Public Authoritative Name Server Set:

- Public Authoritative Name Server Set: The associated FQDNs or IP addresses of the Public Authoritative Server. IP addresses are optional and the FQDN is sufficient. To secure the binding name and IP addresses, a DNSSEC exchange is required. Otherwise, the IP addresses should be entered manually.

- Authentication Method: How the CPE authenticates itself to the Public Server. This MAY depend on the implementation but we should consider at least IPsec, DTLS and TSIG

- Authentication data: Associated Data. PSK only requires a single argument. If other authentication mechanisms based on certificates are used, then, files for the CPE private keys, certificates and certification authority should be specified.

- Public Authoritative Primary(ies): The FQDN or IP addresses of the Public Authoritative Primary. It MAY correspond to the data that will be set in the NS RRsets and SOA of the DNS Homenet Zone. IP addresses are optional and the FQDN is sufficient. To secure the binding name and IP addresses, a DNSSEC exchange is required. Otherwise, the IP addresses should be entered manually.

- Registered Homenet Domain: The domain name the Public Authoritative is configured for DNS secondary, DNSSEC zone signing and DNSSEC zone hosting.

Setting the DNS(SEC) Homenet Zone requires the following information.

- Registered Homenet Domain: The Domain Name of the zone. Multiple Registered Homenet Domain may be provided. This will generate the creation of multiple DNS Homenet Zones.

- Public Authoritative Primaries: The public authoritative servers associated to the Registered Homenet Domain. Multiple public authoritative server may be provided.

5. Synchronization between CPE and Public Authoritative Name Server Sets

The DNS(SEC) Homenet Reverse Zone and the DNS Homenet Zone can be updated either with DNS update [RFC2136] or using a primary / secondary synchronization. The primary / secondary mechanism is preferred as it better scales and avoids DoS attacks: First the primary notifies the secondary the zone must be updated, and leaves the secondary to proceed to the update when possible. Then, the NOTIFY message sent by the primary is a small packet that is less likely to load the secondary. At last, the AXFR query performed by the secondary is a small packet sent over TCP (section 4.2 [RFC5936]) which makes unlikely the secondary to perform reflection attacks with a forged NOTIFY. On the other hand, DNS updates can use UDP, packets require more processing then a NOTIFY, and they do not provide the server the opportunity to post-pone the update.

This document recommends the use of a primary / secondary mechanism instead of the use of nsupdates. This section details the primary / secondary mechanism.

5.1. Synchronization with a Hidden Primary

Uploading and dynamically updating the zone file on the Public Authoritative Name Server Set can be seen as zone provisioning between the CPE (Hidden Primary) and the Public Authoritative Name Server Set (Secondary Server). This can be handled either in band or out of band.

The Public Authoritative Name Server Set is configured as a secondary for the Homenet Domain Name. This secondary configuration has been previously agreed between the end user and the provider of the Public Authoritative Name Server Sets. In order to set the primary/ secondary architecture, the CPE acts as a Hidden Primary Server,

which is a regular Authoritative DNS(SEC) Server listening on the WAN interface.

The Hidden Primary Server is expected to accept SOA [RFC1033], AXFR [RFC1034], and IXFR [RFC1995] queries from its configured secondary DNS servers. The Hidden Primary Server SHOULD send NOTIFY messages [RFC1996] in order to update Public DNS server zones as updates occur. Because, DNS Homenet Zones are likely to be small, CPE MUST implement AXFR and SHOULD implement IXFR.

Hidden Primary Server differs from a regular authoritative server for the home network by:

- Interface Binding: the Hidden Primary Server listens on the WAN Interface, whereas a regular authoritative server for the home network would listen on the home network interface.

- Limited exchanges: the purpose of the Hidden Primary Server is to synchronizes with the Public Authoritative Name Server Set, not to serve zone. As a result, exchanges are performed with specific nodes (the Public Authoritative Name Server Sets). Then exchange types are limited. The only legitimate exchanges are: NOTIFY initiated by the Hidden Primary and IXFR or AXFR exchanges initiated by the Public Authoritative Name Server Set. On the other hand regular authoritative servers would respond any hosts on the home network, and any DNS(SEC) query would be considered. The CPE SHOULD filter IXFR/AXFR traffic and drop traffic not initiated by the Public Authoritative Name Server Set. The CPE MUST listen for DNS on TCP and UDP and at least allow SOA lookups to the DNS Homenet Zone.

5.2. Securing Synchronization

Exchange between the Public Authoritative Name Server Sets and the CPE MUST be secured, at least for integrity protection and for authentication.

TSIG [RFC2845] or SIG(0) [RFC2931] can be used to secure the DNS communications between the CPE and the Public DNS(SEC) Servers. TSIG uses a symmetric key which can be managed by TKEY [RFC2930]. Management of the key involved in SIG(0) is performed through zone updates. How to roll the keys with SIG(0) is out-of-scope of this document. The advantage of these mechanisms is that they are only associated with the DNS application. Not relying on shared libraries ease testing and integration. On the other hand, using TSIG, TKEY or SIG(0) requires these mechanisms to be implemented on the DNS(SEC) Server's implementation running on the CPE, which adds codes.

Another disadvantage is that TKEY does not provide authentication mechanism.

Protocols like TLS [RFC5246] / DTLS [RFC6347] can be used to secure the transactions between the Public Authoritative Name Server Sets and the CPE. The advantage of TLS/DTLS is that this technology is widely deployed, and most of the boxes already embeds a TLS/DTLS libraries, eventually taking advantage of hardware acceleration. Then TLS/DTLS provides authentication facilities and can use certificates to authenticate the Public Authoritative Name Server Set and the CPE. On the other hand, using TLS/DTLS requires to integrate DNS exchange over TLS/DTLS, as well as a new service port. This is why we do not recommend this option.

IPsec [RFC4301] IKEv2 [RFC7296] can also be used to secure the transactions between the CPE and the Public Authoritative Servers. Similarly to TLS/DTLS, most CPE already embeds a IPsec stack, and IKEv2 provides multiple authentications possibilities with its EAP framework. In addition, IPsec can be used to protect the DNS exchanges between the CPE and the Public Authoritative Servers without any modifications of the DNS Servers or client. DNS integration over IPsec only requires an additional security policy in the Security Policy Database. One disadvantage of IPsec is that it hardly goes through NATs and firewalls. However, in our case, the CPE is connected to the Internet, and IPsec communication between the CPE and Public Authoritative Name Server Set SHOULD NOT be impacted by middle boxes.

How the PSK can be used by any of the TSIG, TLS/DTLS or IPsec protocols: Authentication based on certificates implies a mutual authentication and thus requires the CPE to manage a private key, a public key or certificates as well as Certificate Authorities. This adds complexity to the configuration especially on the CPE side. For this reason, we recommend that CPE MAY use PSK or certificate base authentication and that Public Authoritative Servers Servers MUST support PSK and certificate based authentication.

Note also that authentication of the messages exchanged between the CPE and the Public Authoritative Name Server Set should not involve the IP address to index the appropriated keys. As detailed in Section 9, the IP addresses of the Public Authoritative Name Server Set and the Hidden Primary are subject to change, for example while the network is being renumbered. This means that the necessary keys to authenticate transaction must not be indexed using the IP and be resilient to IP updates.

5.3. CPE Security Policies

This section details security policies related to the Hidden Primary / Secondary synchronization.

The Hidden Primary, as described in this document SHOULD drop any queries from the home network. This can be performed with port binding and/or firewall rules.

The Hidden Primary SHOULD drop on the WAN interface any DNS queries that is not issued from the Public Authoritative Name Server Set.

The Hidden Primary SHOULD drop any outgoing packets other than DNS NOTIFY query, SOA response, IXFR response or AXFR responses.

The Hidden Primary SHOULD drop any incoming packets other than DNS NOTIFY response, SOA query, IXFR query or AXFR query.

The Hidden Primary SHOULD drop any non protected IXFR or AXFR exchange. This depends how the synchronization is secured.

6. DNSSEC compliant Homenet Architecture

[RFC7368] in Section 3.7.3 recommends DNSSEC to be deployed on the both the authoritative server and the resolver. The resolver side is out of scope of this document, and only the authoritative part is considered.

Deploying DNSSEC requires signing the zone and configuring a secure delegation. As described in Section 4.1, signing can be performed by the CPE or by the Public Authoritative Name Server Sets. Section 6.1 details the implications of these two alternatives. Similarly, the secure delegation can be performed by the CPE or by the Public Authoritative Servers. Section 6.2 discusses these two alternatives.

6.1. Zone Signing

This section discusses the pros and cons when zone signing is performed by the CPE or by the Public Authoritative Name Servers Set. It is recommended the CPE signs the zone unless there is a strong argument against it, like a CPE that is not able to sign the zone. In that case zone signing may be performed by the Public Authoritative Name Servers Set on behalf of the CPE.

Reasons for signing the zone by the CPE are:

- 1: Keeping the Homenet Zone and the Public Zone equals to securely optimize DNS resolution. As the Public Zone is signed with

DNSSEC, RRsets are authenticated and thus DNS responses can be validated even though they are not provided by the authoritative server. This provides the CPE the ability to respond on behalf of the Public Authoritative Primary. This could be useful for example if, in the future, the CPE could announce to the home network that the CPE can act a a local authoritative primary or equivalent for the Homenet Zone. Currently the CPE is not expected to receive authoritative DNS queries as its IP address is not mentioned in the Public Zone. On the other hand most CPEs host a resolving function, and could be configured to perform a local lookup to the Homenet Zone instead of initiating a DNS exchange with the Public Authoritative Primary. Note that outsourcing the zone signing operation requires that all DNSSEC queries be cached to perform a local lookup, otherwise a resolution with the Public Authoritative Primary is performed.

- 2: Keeping the Homenet Zone and the Public Zone equals to securely address the connectivity disruption independence exposed in [RFC7368] section 4.4.1 and 3.7.5. As local lookups are possible in case of network disruption, communications within the home network can still rely on the DNSSEC service. Note that outsourcing the zone signing operation does not address connectivity disruption independence with DNSSEC. Instead local lookup would provide DNS as opposed to DNSSEC responses provided by the Public Authoritative Primaries.

- 3: Keeping the Homenet Zone and the Public Zone equals to guarantee coherence between DNS(SEC) responses. Using a unique zone is one way to guarantee uniqueness of the responses among servers and places. Issues generated by different views are discussed in more details in Section 7.

- 2: Privacy and Integrity of the DNS Zone are better guaranteed. When the Zone is signed by the CPE, it makes modification of the DNS data -- for example for flow redirection -- not possible. As a result, signing the Homenet Zone by the CPE provides better protection for the end user privacy.

Reasons for signing the zone by the Public Authoritative Servers are:

- 1: The CPE is not able to sign the zone, most likely because its firmware does not make it possible. However the reason is expected to be less and less valid over time.

- 2: Outsourcing DNSSEC management operations. Management operations involve key-roll over which can be done automatically by the CPE and transparently for the end user.

As result avoiding DNSSEC management is mostly motivated by bad software implementations.

- 3: Reducing the impact of CPE replacement on the Public Zone. Unless the CPE private keys are backuped, CPE replacement results in a emergency key roll over. This can be mitigated also by using relatively small TTLs.

- 4: Reducing configuration impacts on the end user. Unless there are some zero configuration mechanisms to provide credentials between the new CPE and the Public Authoritative Name Server Sets. Authentications to Public Authoritative Name Server Set should be re-configured. As CPE replacement is not expected to happen regularly, end users may not be at ease with such configuration settings. However, mechanisms as described in [I-D.ietf-homenet-naming-architecture-dhc-options] use DHCP Options to outsource the configuration and avoid this issue.

- 5: Public Authoritative Servers are more likely to handle securely private keys than the CPE. However, having all private information at one place may also balance that risk.

6.2. Secure Delegation

The secure delegation is set if the DS RRset is properly set in the parent zone. Secure delegation can be performed by the CPE or the Public Authoritative Servers.

The DS RRset can be updated manually by the CPE or the Public Authoritative Servers. This can be used then with nsupdate for example but requires the CPE or the Public Authoritative Server to be authenticated by the Parent Zone Server. Such a trust channel between the CPE and the Parent Zone server may be hard to maintain, and thus may be easier to establish with the Public Authoritative Server. On the other hand, [RFC7344] may mitigate such issues.

7. Handling Different Views

The DNS Homenet Zone provides information about the home network and some user may be tempted to have different information regarding the origin of the DNS query. More specifically, some users may be tempted to provide a different view for DNS queries originating from the home network and for DNS queries coming from the wild Internet. Each view can be associated to a dedicated Homenet Zone. Note that this document does not specify how DNS queries coming from the home network are addressed to the DNS(SEC) Homenet Zone. This could be done via the DNS resolver hosted on the CPE for example.

This section is not normative. Section 7.1 details why some nodes may only be reachable from the home network and not from the global Internet. Section 7.2 briefly describes the consequences of having distinct views such as a "home network view" and a "Internet view". Finally, Section 7.3 provides guidance to on how to resolve names that are only significant in the home network without creating different views.

7.1. Misleading Reasons for Local Scope DNS Zone

The main motivation to handle different views is to provide different information depending on the location the DNS query is emitted. Here are a few motivations for doing so:

- 1: An end user may want to have services not published on the Internet. Services like the CPE administration interface that provides the GUI to administrate your CPE may not be published on the Internet. Similarly services like the mapper that registers the devices of your home network may not be published on the Internet. In both case, these services should only be known/used by the network administrator. To restrict the access of such services, the home network administrator may chose to publish these information only within the home network, where it may suppose users are more trustable then on the Internet. Even though, this assumption may not be valid, at least, this reduces the surface of attack.

- 2: Services within the home network may be reachable using non global IP addresses. IPv4 and NAT may be one reason. On the other hand IPv6 may favor link-local or site-local IP addresses. These IP addresses are not significant outside the boundaries of the home network. As a result, they may be published in the home network view, and should not be published in the Internet.

- 3: If the CPE does not sign the Homenet Zone and outsource the signing process, the two views are at least different since, one is protected with DNSSEC whereas the other is not.

7.2. Consequences

Enabling different views leads to a non-coherent naming system. Basically, depending on where resolution is performed, some services will not be available. This may be especially inconvenient with devices with multiple interfaces that are attached both to the Internet via a 3G/4G interface and to the home network via a WLAN interface.

Regarding local-scope IP addresses, such device may end up with poor connectivity. Suppose, for example, the DNS resolution is performed via the WLAN interface attached to the CPE, the response provides local-scope IP addresses and the communication is initiated on the 3G/4G interface. Communications with local-scope addresses will be unreachable on the Internet, thus aborting the communication. The same situation occurs if a device is flip / flopping between various WLAN networks.

Regarding DNSSEC, devices with multiple interfaces will have difficulties to secure the naming resolution as responses emitted from the home network may not be signed.

For devices with all its interfaces attached to a single administrative domain, that is to say the home network or the Internet. Incoherence between DNS responses may also happen if the device is able to perform DNS resolutions. DNS resolutions performed via the CPE resolver may be different then those performed over the Internet.

7.3. Guidance and Recommendations

As exposed in Section 7.2, it is recommended to avoid different views. If network administrators chose to implement multiple views, impacts on devices' resolution should be evaluated.

A consequence the DNS(SEC) Homenet Zone is expected to be the exact copy of the DNS(SEC) Public Zone. As a result, services that are not expected to be published on the Internet should not be part of the DNS(SEC) Homenet Zone, local-scope address should not be part of the DNS(SEC) Homenet Zone, and when possible, the CPE should sign the DNS(SEC) Homenet Zone.

The DNS(SEC) Homenet Zone is expected to host public information. It is not to the DNS service to define local home networks boundaries. Instead, local scope information is expected to be provided to the home network using local scope naming services. mDNS [RFC6762] DNS-SD [RFC6763] are one of these services. Currently mDNS is limited to a single link network. However, future protocols are expected to leverage this constraint as pointed out in [I-D.ietf-dnssd-requirements].

8. Reverse Zone

Most of the description considered the DNS Homenet Zone as the non-Reverse Zone. This section is focused on the Reverse Zone.

First, all considerations for the DNS Homenet Zone apply to the Reverse Homenet Zone. The main difference between the Reverse DNS Homenet Zone and the DNS Homenet Zone is that the parent zone of the Reverse Homenet Zone is most likely managed by the ISP. As the ISP also provides the IP prefix to the CPE, it may be able to authenticate the CPE. If the Reverse Public Authoritative Name Server Set is managed by the ISP, credentials to authenticate the CPE for the zone synchronization may be set automatically and transparently to the end user. [I-D.ietf-homenet-naming-architecture-dhc-options] describes how automatic configuration may be performed.

With IPv6, the domain space for IP address is so large, that reverse zone may be confronted to a scalability issue. How to reverse zone is generated is out of scope of this document. [I-D.howard-dnsop-ip6rdns] provides guidance on how to address the scalability issue.

9. Renumbering

This section details how renumbering is handled by the Hidden Primary server or the Public Authoritative Name Server Set which acts as a secondary server. Both types of renumbering also designated as "make-before-break" or "break-before-make" are discussed.

In the make-before-break renumbering scenario, the new prefix is advertised, the network is configured to prepare the transition to the new prefix. During a period of time, the two prefixes old and new coexist, before the old prefix is completely removed. In the break-before-make renumbering scenario, the new prefix is advertised making the old prefix obsolete.

Renumbering has been extensively described in [RFC4192] and analyzed in [RFC7010] and the reader is expected to become familiar with them.

9.1. Hidden Primary

In a renumbering scenario, the Hidden Primary is informed it is being renumbered. In most cases, it occurs as the whole home network is being renumbered. As a result, the DNS(SEC) Homenet Zone will also be updated. Although the new and old IP addresses may be stored in the DNS(SEC) Homenet Zone, we recommend that only the newly reachable IP addresses be mentioned.

To avoid reachability disruption, IP connectivity information provided by the DNS should be coherent with the IP plane. In our case, this means the old IP address should not be provided via the DNS, when it is not reachable anymore. Let for example TTL be the

TTL associate to a RRset of the Homenet Zone, it may be cache during TTL seconds. Let T_NEW be the time the new IP address replaces the old IP address in the DNS, and T_OLD_UNREACHABLE the time the old IP is not reachable anymore. In the case of the make-before-break, seamless reachability is provided as long as T_OLD_UNREACHABLE - T_NEW > 2 * TTL. If this is not satisfied, then devices associated to the old IP address in the home network may become unreachable for 2 * TTL - (T_OLD_UNREACHABLE - T_NEW). In the case of a break-before-make, T_OLD_UNREACHABLE = T_NEW, and the device may become non reachable up to 2 * TTL.

Once the DNS(SEC) Homenet Zone file has been updated on the Hidden Primary, the Hidden Primary needs to inform the Public Authoritative Naming Server Set that the DNS(SEC) Homenet Zone has been updated and that the IP address to use to retrieve the updated zone has also been updated. Both information are updated using the regular DNS exchanges. More specifically, mechanisms to update a IP address provided by lower layers with for protocols like SCTP [RFC4960], MOBIKE [RFC4555] are not considered in this document.

The Hidden Primary informs the Public Authoritative Name Server Set the DNS(SEC) Homenet Zone has been updated by sending a NOTIFY payload with the new IP address. In addition, this NOTIFY payload is authenticated using SIG(0) or TSIG. When the Public Authoritative Name Server Set receives the NOTIFY payload, it MUST authenticate it. Note that the cryptographic key used for the authentication should be indexed by the Homenet Domain Name contained in the NOTIFY payload as well as the RRSIG. In other words, the IP address should not be used as an index. If authentication succeeds, the Public Authoritative Name Server Set MUST also notice the IP address has been modified and perform a reachability check before updating its primary configuration. The routability check is performed by sending a SOA request to the Hidden Primary using the source IP address of the NOTIFY. This exchange is also secured, and if an authenticated response is received from the Hidden Primary with the new IP address, the Public Authoritative Name Server Set updates its configuration file and retrieve the DNS(SEC) Homenet Zone using an AXFR or a IXFR exchange.

Note that the primary reason for providing the IP address is that the Hidden Primary is not publicly announced in the DNS. If the Hidden Primary were publicly announced in the DNS, then the IP address update could have been performed using the DNS as described in Section 9.2.

9.2. Public Authoritative Name Server Set

Renumbering of the Public Authoritative Name Server Set results in the Public Authoritative Name Server Set to change its IP address. The Public Authoritative Name Server Set is a secondary, so its renumbering does not impact the DNS(SEC) Homenet Zone. In fact, exchanges to the Public Authoritative Name Server Set are restricted to the DNS(SEC) Homenet Zone synchronization. In our case, the Hidden Primary MUST be able to send NOTIFY payloads to the Public Authoritative Name Server Set.

If the Public Authoritative Name Server Set is configured in Hidden Primary configuration file with a FQDN, then the update of the IP address is performed by the DNS(SEC). More specifically, before sending the NOTIFY, the Hidden Primary performs a DNS(SEC) resolution to retrieve the IP address of the secondary.

As described in Section 9.1, the Public Authoritative Name Server Set DNS information should be coherent with the IP plane. Let TTL be the TTL associated to the Public Authoritative Name Server Set FQDN, T_NEW the time the new IP address replaces the old one and T_OLD_UNREACHABLE the time the Public Authoritative Name Server Set is not reachable anymore with its old IP address. Seamless reachability is provided as long as T_OLD_UNREACHABLE - T_NEW > 2 * TTL. If this condition is not met, the Public Authoritative Name Server Set may be unreachable during 2 * TTL - (T_OLD_UNREACHABLE - T_NEW). In the case of a break-before-make, T_OLD_UNREACHABLE = T_NEW, and it may become non reachable up to 2 * TTL.

Some DNS infrastructure uses the IP address to designate the secondary, in which case, other mechanisms must be found. The reason for using IP addresses instead of names is generally, to reach an internal interface that is not designated by a FQDN. Such scenarios are considered as out of scope in the case of home networks.

10. Privacy Considerations

Outsourcing the DNS Authoritative service from the CPE to a third entity comes with a few privacy related concerns.

First the DNS Homenet Zone contains a full description of the services hosted in the network. These services may not be expected to be publicly shared although their names remains accessible though the Internet. Even though DNS makes information public, the DNS does not expect to make the complete list of service public. In fact, making information public still requires the key (or FQDN) of each service to be known by the resolver in order to retrieve information of the services. More specifically, making mywebsite.example.com

public in the DNS, is not sufficient to make resolvers aware of the existence web site.

In order to prevent the complete DN(SEC) Homenet Zone to be published on the Internet, one should prevent AXFR queries on the Public Authoritative Primaries. Similarly, to avoid zone-walking one should prefer NSEC3 [RFC5155] over NSEC [RFC4034].

When the DNS Homenet Zone is outsourced the end user must be aware that it provides a complete description of the services available on the home network. More specifically, names usually provides a clear indication of the service and eventually the device, by as the DNS Homenet Zone contains the IP addresses associated to the service, they limit the scope of the scan.

In addition to the DNS Homenet Zone, the third party can also monitor the traffic associated to the DNS Homenet Zone. This traffic may provide indication of the services you use, how and when you use these services. Although, cache may alter this information inside the home network, it is likely that outside your home network this information will not be cached.

11. Security Considerations

The Homenet Naming Architecture described in this document solves exposing the CPE's DNS service as a DoS attack vector.

11.1. Names are less secure than IP addresses

This document describes how an End User can make his services and devices from his home network reachable on the Internet with Names rather than IP addresses. This exposes the home network to attackers since names are expected to provide less randomness than IP addresses. The naming delegation protects the End User's privacy by not providing the complete zone of the home network to the ISP. However, using the DNS with names for the home network exposes the home network and its components to dictionary attacks. In fact, with IP addresses, the Interface Identifier is 64 bit length leading to 2^64 possibilities for a given subnetwork. This is not to mention that the subnet prefix is also of 64 bit length, thus providing another 2^64 possibilities. On the other hand, names used either for the home network domain or for the devices present less randomness (livebox, router, printer, nicolas, jennifer, ...) and thus exposes the devices to dictionary attacks.

11.2. Names are less volatile than IP addresses

IP addresses may be used to locate a device, a host or a Service. However, home networks are not expected to be assigned the same Prefix over time. As a result observing IP addresses provides some ephemeral information about who is accessing the service. On the other hand, Names are not expected to be as volatile as IP addresses. As a result, logging Names, over time, may be more valuable that logging IP addresses, especially to profile End User's characteristics.

PTR provides a way to bind an IP address to a Name. In that sense responding to PTR DNS queries may affect the End User's Privacy. For that reason we recommend that End Users may choose to respond or not to PTR DNS queries and may return a NXDOMAIN response.

11.3. DNS Reflection Attacks

An attacker uses a reflection attack when it sends traffic to an intermediary node that in turn sends back some traffic to the victim. Motivations for using an intermediary node might be anonymity of the attacker as wells as amplification of the traffic. Typically, when the intermediary node is a DNSSEC server, the attacker sends a DNSSEC query and the victim is likely to receive a DNSSEC response. This section analyzes how the different components may be involved in a reflection attack. Section 11.3.1 considers the Hidden Primary, Section 11.3.2 the Public Authoritative Name Server Set, and Section 11.3.3 the Public Authoritative Primary.

11.3.1. Reflection Attack involving the Hidden Primary

With the current architecture, the Hidden Primary is only expected to receive DNS queries of type SOA, AXFR or IXFR. This section analyzes how these DNS queries may be used by an attacker to perform a reflection attack.

At first, DNS queries of type AXFR and IXFR uses TCP and as such a less subject to reflection attacks. This makes SOA query the only remaining vector of attacks for reflection based on UDP.

Firstly, SOA queries are not associated with a large amplification factor compared to queries of type "ANY" or to query of non existing FQDNs. This reduces the probability a DNS query of type SOA is involved in a DDoS attack. In addition, SOA queries are expected to follow a very specific pattern which makes rate limiting techniques an efficient way to limit such attacks, with a limited impact on the naming service of the home network.

This paragraph analyzes how a Hidden Primary could mitigate a flood of SOA requests. Motivations for such flood might be a reflection attack, but could be also an attack performed against the Hidden Primary for resource exhaustion. At first, the Hidden Primary only expects traffic from the Public Authoritative Name Server Set that is its associated secondary. Even though secondary servers may be renumbered, as exposed in Section 9, the Hidden Primary is likely to perform a DNSSEC resolution and find out the associated secondary's IP addresses in use. As a result, the Hidden Primary is likely to limit the origin of its incoming traffic based on the origin IP address.

With filtering rules base on the IP address, SOA flooding attacks are limited to forged packets with the IP address of the secondary server. In other words, the only victims are the Hidden Primary itself or the secondary. There is a need for the Hidden Primary to limit that flood to limit the impact of the reflection attack on the secondary, and to limit the resource needed to carry on the traffic by the CPE hosting the Hidden Primary. On the other hand, mitigation should be appropriately done, as to limit the impact on the legitimate SOA sent by the secondary.

The main reason for the Public Authoritative Name Server Set to send a SOA query is to update the SOA RRset after the TTL expires, to check serial number upon the receipt of a NOTIFY query from the Hidden Primary or to re-send the SOA request when the response has not been received. When a flood of SOA queries is received by the Hidden Primary, the Hidden Primary can assume it is involved in an attack. There are a few legitimate time slot the secondary is expected to send a SOA query. These times may be specific times like T_NOTIFY the emission of a NOTIFY query, T_SOA + 2/3 TTL, T_SOA + TTL, T_SOA + T_REFRESH where TTL designates the SOA TTL value, T_REFRESH the refresh time defined in the SOA RRset, and T_SOA the last time the SOA has been queried. Outside a few minutes following these specific time, the probability the CPE discard a legitimate SOA query is very low. Within these time slots, the probability the secondary may have its legitimate query rejected is higher. If a legitimate SOA is discarded, the secondary will re-send SOA query every "retry time" second until "expire time" seconds occurs, where "retry time" and "expire time" have been defined in the SOA.

As a result, it is recommended to set rate limiting policies to preserve the CPE resource. If a flood lasts more than the expired time defined by the SOA, it is recommended to re-initiate a synchronization between the Hidden Primary and the secondaries.

11.3.2. Reflection Attacks involving the Public Authoritative Name Server Set

The Public Authoritative Name Server Set acts as a secondary toward the Hidden Primary. The secondary expects to receive NOTIFY query, SOA responses, AXFR and IXFR responses from the Hidden Primary.

Sending NOTIFY query to the secondary generates a NOTIFY response as well as an SOA query to the Hidden Primary. As mentioned in [RFC1996], this is a "known benign denial of service attack". As a result, the Public Authoritative Name Server Set should enforce rate limiting on the SOA queries and NOTIFY responses that are sent to the Hidden Primary. Most likely, when the secondary is flooded with valid and signed NOTIFY queries it is under a replay attack which is discussed in Section 11.5. The key thing here is that the secondary is likely to be designed to address much traffic than the Hidden Primary hosted on a CPE.

This paragraph details how the secondary may limit the NOTIFY queries. Because the Hidden Primary may be renumbered, the secondary may not proceed to IP filtering based on the IP address. In addition, a given secondary may be shared among multiple Hidden Primaries which makes filtering rules based on IP harder to set. At last, time at which a NOTIFY is sent by the Hidden Primary is not predictable. However, a flood of NOTIFY may be easily detected as a NOTIFY for a given DNS Homenet Zone is expected to have a very limited number of different IP addresses even though renumbering occurs. As a result, the secondary, can rate limit incoming NOTIFY queries.

It is recommended the Hidden Primary sends NOTIFY as long as the zone has not been updated by the secondary. Multiple SOA queries may indicate the secondary is under attack.

11.3.3. Reflection Attacks involving the Public Authoritative Primary

The Public Authoritative Primary implication of reflection attacks is similar as any public authoritative server. These is not specific to the architecture described in this document, and thus considered as out of scope.

In fact, one of the motivation of the architecture described in this document was to expose the Public Authoritative Primary to attacks instead of the CPE.

11.4. Flooding Attack

The purpose of flooding attacks is mostly resource exhaustion where the resource can be bandwidth or CPU for example.

One of the goal of the architecture described in the document is to limit the surface of attack for the CPE. This is done, by outsourcing the DNS service to the Public Authoritative Primaries. By doing so, the CPE limits its DNS interactions between the Hidden Primary and the Public Authoritative Name Server Set. This limits the number of entity the CPE interacts with as well as the scope of DNS exchanges - basically NOTIFY, SOA, AXFR, IXFR.

The use of an authenticated channel with SIG(0) or TSIG between the CPE and the Public Authoritative Name Server Set, enables to detect illegitimate DNS queries, and take appropriated actions - like dropping the queries. If signatures are validated, then most likely, the CPE is under a replay attack, as detailed in Section 11.5

In order to limit the resource required for authentication, it is recommended to use TSIG that uses symmetric cryptography over SIG(0) that uses asymmetric cryptography.

11.5. Replay Attack

Replay attacks consist in sending a message that has already been sent. As the Hidden Primary and the Public Authoritative Name Server Set use an authenticated channel, replay attacks are mostly expected to used over forged DNS queries in order to provide valid traffic.

On an attacker points of view, using a correctly authenticated DNS query, may not be detected as an attack, and thus may generate the corresponding response. Generating and sending a response consumes more resources then dropping the query and thus could be used for resource exhaustion attacks. In addition, as the authentication is performed at the DNS layer, the IP address could be impersonated in order to perform a reflection attack.

Section 11.3 details how to mitigate reflection attacks and Section 11.4 details how to mitigate resource exhaustion. Both section assumes a context of DoS with a flood of DNS queries. This section address replay attack as a way to limit the surface of these attacks.

As SIG(0) and TSIG uses inception and expiration time, the time frame for replay attack is limited. SIG(0) and TSIG recommends a fudge value of 5 minutes. This value has been set as a compromise between loose time synchronization of the devices and short live time for the

message. As a result, better time synchronization policies could reduce the time window of the attack.

12. IANA Considerations

This document has no actions for IANA.

13. Acknowledgment

The authors wish to thank Philippe Lemordant for its contributions on the early versions of the draft; Ole Troan for pointing out issues with the IPv6 routed home concept and placing the scope of this document in a wider picture; Mark Townsley for encouragement and injecting a healthy debate on the merits of the idea; Ulrik de Bie for providing alternative solutions; Paul Mockapetris, Christian Jacquenet, Francis Dupont and Ludovic Eschard for their remarks on CPE and low power devices; Olafur Gudmundsson for clarifying DNSSEC capabilities of small devices; Simon Kelley for its feedback as dnsmasq implementer; Andrew Sullivan, Mark Andrew, Ted Lemon, Mikael Abrahamson, Michael Richardson and Ray Bellis for their feed backs on handling different views as well as clarifying the impact of outsourcing the zone signing operation outside the CPE; Ray Hunter, Mark Andrew and Peter Koch for clarifying the renumbering.

14. References

14.1. 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.

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, August 1996.

[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.

[RFC2142] Crocker, D., "MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS", RFC 2142, May 1997.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998.

[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.

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

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

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

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

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6644] Evans, D., Droms, R., and S. Jiang, "Rebind Capability in DHCPv6 Reconfigure Messages", RFC 6644, July 2012.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, October 2014.

14.2. Informational References

[I-D.howard-dnsop-ip6rdns]
Howard, L., "Reverse DNS in IPv6 for Internet Service Providers", draft-howard-dnsop-ip6rdns-00 (work in progress), June 2014.

[I-D.ietf-dnssd-requirements]
Lynn, K., Cheshire, S., Blanchet, M., and D. Migault, "Requirements for Scalable DNS-SD/mDNS Extensions", draft-ietf-dnssd-requirements-06 (work in progress), March 2015.

[I-D.ietf-homenet-naming-architecture-dhc-options]
Migault, D., Cloetens, W., Griffiths, C., and R. Weber, "DHCP Options for Homenet Naming Architecture", draft-ietf-homenet-naming-architecture-dhc-options-01 (work in progress), February 2015.

[RFC1033] Lottor, M., "Domain administrators operations guide", RFC 1033, November 1987.

[RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005.

[RFC7010] Liu, B., Jiang, S., Carpenter, B., Venaas, S., and W. George, "IPv6 Site Renumbering Gap Analysis", RFC 7010, September 2013.

[RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating DNSSEC Delegation Trust Maintenance", RFC 7344, September 2014.

[RFC7368] Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", RFC 7368, October 2014.

Appendix A. Document Change Log

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

-06:

Ray Hunter is added in acknowledgment.

Adding Renumbering section with comments from Dallas meeting

Replacing Master / Primary - Slave / Secondary

Security Consideration has been updated with Reflection attacks, flooding attacks, and replay attacks.

-05:

*Clarifying on handling different views:

- 1: How the CPE may be involved in the resolution and responds without necessarily requesting the Public Primaries (and eventually the Hidden Primary)

- 2: How to handle local scope resolution that is link-local, site-local and NAT IP addresses as well as Private domain names that the administrator does not want to publish outside the home network.

Adding a Privacy Considerations Section

Clarification on pro/cons outsourcing zone-signing

Documenting how to handle reverse zones

Adding reference to RFC 2308

-04:

*Clarifications on zone signing

*Rewording

*Adding section on different views

*architecture clarifications

-03:

*Simon's comments taken into consideration

*Adding SOA, PTR considerations

*Removing DNSSEC performance paragraphs on low power devices

*Adding SIG(0) as a mechanism for authenticating the servers

*Goals clarification: the architecture described in the document 1) does not describe new protocols, and 2) can be adapted to specific cases for advance users.

-02:

*remove interfaces: "Public Authoritative Server Naming Interface" is replaced by "Public Authoritative Primary(ies)". "Public Authoritative Server Management Interface" is replaced by "Public Authoritative Name Server Set".

-01.3:

*remove the authoritative / resolver services of the CPE. Implementation dependent

*remove interactions with mdns and dhcp. Implementation dependent.

*remove considerations on low powered devices

*remove position toward homenet arch

*remove problem statement section

-01.2:

* add a CPE description to show that the architecture can fit CPEs

* specification of the architecture for very low powered devices.

* integrate mDNS and DHCP interactions with the Homenet Naming Architecture.

* Restructuring the draft. 1) We start from the homenet-arch draft to derive a Naming Architecture, then 2) we show why CPE need mechanisms that do not expose them to the Internet, 3) we describe the mechanisms.

* I remove the terminology and expose it in the figures A and B.

* remove the Front End Homenet Naming Architecture to Homenet Naming

-01:

* Added C. Griffiths as co-author.

* Updated section 5.4 and other sections of draft to update section on Hidden Primary / Slave functions with CPE as Hidden Primary/ Homenet Server.

* For next version, address functions of MDNS within Homenet Lan and publishing details northbound via Hidden Primary.

-00: First version published.

Authors' Addresses

Daniel Migault
Ericsson
8400 boulevard Decarie
Montreal, QC H4P 2N2
Canada

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