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

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

October 20, 2013

IPv6 Home Network Naming Delegation
draft-mglt-homenet-front-end-naming-delegation-03.txt

Abstract

CPEs are designed to provide IP connectivity to home networks. Most CPEs assigns 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 results 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 associates to its home network, and outsource both DNSSEC management and naming service on the Internet to a third party designated as the Public Authoritative Servers.

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/.

This Internet-Draft will expire on April 23, 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. Introduction

IPv6 provides global end to end IP reachability from the Internet and into the Home Network. End Users to access services hosted in the Home Network with IPv6 addresses would 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 other words, the CPE is the natural candidate for setting the DNS(SEC) zone file.

CPEs are usually low powered devices designed for the Home Network, but not for heavy traffic. As a result, hosting the a 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. So, this document considers that the Naming Service SHOULD NOT be hosted on the CPE and SHOULD be outsourced to a third party.

In addition, the Naming Service of the Home Network is expected to be deployed with its security extension DNSSEC. DNSSEC comes with complex configurations as well as complex operation management like (DNSSEC secure delegation, DNSSEC key roll over, DNSSEC zone updates). These operations can hardly be understood by the average end user, and a misconfiguration MAY result in invalid naming resolutions that MAY make an host, or the whole home network unreachable. So, this document considers DNSSEC management operations SHOULD NOT be handled by the average end user, but SHOULD be outsourced to a third party.

This document describes an architecture where the CPE outsources the authoritative naming service and DNSSEC zone management to a third party designated as Public Authoritative Servers. It describes interactions between the CPE and the Public Authoritative Servers, that is to say the involved protocols and their respective configurations. More specifically, this document does not describe any new protocol. It provides a guide line to properly use the already existing protocols.

This document intends to efficiently deploy DNSSEC in the Home Networks in a standardized and highly flexible way. More specifically, the described Home Network Naming architecture is expected to lead to autoconfiguration facilities for most common users, as well as enabling advanced users to have their own specific settings. In fact, some end users MAY choose to host and expose a Naming service on their CPE. Others MAY sign the zone on the CPE. Although the document does not describe these scenarios, the described architecture only requires minor modifications - such as allowing incoming DNS queries from the Internet and adding the CPE in the list of Naming servers.

The document is organized as follows. Section 4 provides an overview of the homenet naming architecture and presents the CPE and the Public Authoritative Server that handles the authoritative naming service of the home network as well as DNSSEC management operations on behalf of the CPE. Section 5 describes in details protocols and configurations to set the homenet naming architecture. Section 6 sums up the various configuration parameters that MAY be filled by the end user on the CPE for example via a GUI. Finally Section 7 provides security considerations.

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 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 as public available name servers for the Registered Homenet Domain.

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

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

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

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

4. Architecture Overview

Figure 1 provides an overview of the homenet naming architecture.

The CPE is in charge of building the DNS Homenet Zone that contains all FQDN bindings of the home network. The home network is associated to a FQDN, the Registered Homenet Domain (example.com). Any node in the home network is associated to a FQDN (node1.example.com) that MAY be provided via DHCP or statically configured on the CPE via a GUI for example.

The goal of the homenet naming architecture is that the CPE does not handle any DNSSEC operations and does not host the authoritative naming service while FQDNs in the Homenet Zone can be resolved with DNSSEC by any node on the Internet.

In order to achieve this goal, when a node on the Internet sends a DNS(SEC) query like for node1.example.com, this DNS(SEC) query MUST be treated by a third party designated in figure 1 as the Public Authoritative Servers.

The Public Authoritative Servers are in charge of DNS(SEC) traffic for the Registered Homenet Domain (example.com) as well as all DNSSEC management operations like zone signing, key rollover. The DNSSEC zone hosted by the Public Authoritative Servers is called the DNSSEC Public Zone.

The purpose of our architecture is to describe how the CPE can outsource the DNS Homenet Zone hosted on the CPE to the DNSSEC Public Zone hosted on the Public Authoritative Servers. This includes description of the synchronization protocols between the CPE and the Public Authoritative Servers in Section 5.1 as well as configurations of the DNS Homenet Zone Section 5.2.

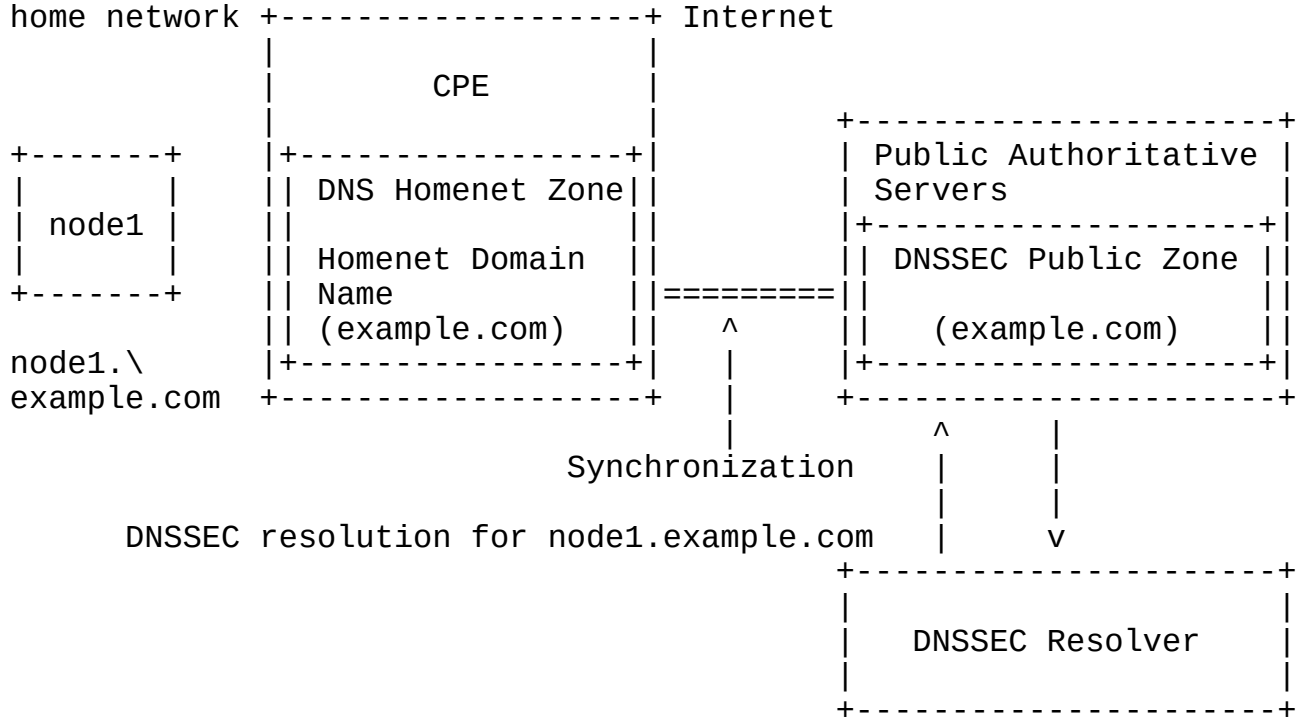

Figure 1: Homenet Naming Architecture Description

The content of the DNS Homenet Zone is out of the scope of this document. The CPE MAY host 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 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 Homenet Zone.

Because services or devices MAY only be reached from hosts in the home network, DNS resolution MAY be handled differently from inside the network and from outside the network.This is out of scope of this document. This document is focused on outsourcing the DNS Homenet Zone to the DNS Public Authoritative Servers that are visible from outside the home network. How to deal with a homenet view and a public view is out of the scope of this document. In order to deal with different views, some CPE MAY host DNS forwarders or use DNS view mechanisms.

This document does not make any other assumption on the DNS Homenet Zone that records MUST be made public. More specifically, the DNS Homenet Zone can be a regular or a reverse zone with PTR RRsets. A CPE SHOULD consider both the normal zone as well as the reverse zone and outsource them both to the designated Public Authoritative Servers.

By outsourcing to Public Authoritative Servers, services or devices mentioned in the DNS Homenet Zone MAY be not reachable in case the home network has no internet connectivity. How to keep the naming service within the home network when the it is disconnected from the public internet is out of scope of this document. CPE MAY chose for example to host an authoritative naming server for the home network or use a DNS forwarders.

Similarly, CPE MAY host a DNS(SEC) resolution service for nodes in the home network. There are multiple ways to configure the resolver service on the CPE. Detailing these various configurations is out of the scope of this document, and is considered as an implementation issue. Some implementers MAY chose to forward DNS(SEC) queries from the home network to the resolving server of its ISP or any other public resolver. In that case, the DNS(SEC) response from the Public Authoritative Servers is forwarded to the home network, which provide DNS and DNSSEC resolution for the home network. Note also that in this case, the naming service depends on the connectivity with the resolving servers. In case the home network is disconnected, the naming service MAY not be available. Alternative implementations MAY

chose to take advantage of forwarders and lookup in the DNS Homenet Zone. This MAY provide only DNS responses in the home network if the CPE does not sign the DNS Homenet Zone. Other implementation MAY chose to synchronize the DNSSEC Public Zone on the CPE either using DNS master slave mechanisms, or by caching the whole zone. This latest option MAY require some additional configuration the Public Authoritative Servers.

5. Architecture Description

This section describes how the CPE and the Public Authoritative Servers SHOULD be configured to outsource authoritative naming service as well as DNSSEC management operations. Section 5.1 describes how a secure synchronization between the CPE and the Public Authoritative server is set. Section 5.2 provides guide lines for the DNS Homenet Zone set in the CPE and uploaded on the Public Authoritative Servers. Section 5.3 describes DNSSEC settings on the Public Authoritative Servers. Finally, Section 5.4 provides the security policies that SHOULD be set on the CPE.

5.1. CPE and Public Authoritative Servers Synchronization

5.1.1. Synchronization with a Hidden Master

Uploading and dynamically updating the zone file on the Public Servers can be seen as zone provisioning between the CPE (Hidden Master) and the Public Server (Slave Server). This can be handled either in band or out of band. DNS dynamic update [RFC2136] may be used. However, in this section we detail how to take advantage of the DNS slave / master architecture to deploy updates to public zones.

The Public Authoritative Server is configured as a slave for the Homenet Domain Name. This slave configuration has been previously agreed between the end user and the provider of the Public Authoritative Servers. In order to set the master/ slave architecture, the CPE acts as a Hidden Master Server, which is a regular Authoritative DNS(SEC) Server listening on the WAN interface.

The Hidden Master Server is expected to accept SOA [RFC1033], AXFR [RFC1034], and IXFR [RFC1995] queries from its configured slave DNS servers. The Hidden Master 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 Master Server differs from a regular authoritative server for the home network by:

- Interface Binding: the Hidden Master 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 Master Server is to synchronizes with the Public Authoritative Servers, not to serve zone. As a result, exchanges are performed with specific nodes (the Public Authoritative Servers). Then exchange types are limited. The only legitimate exchanges are: NOTIFY initiated by the Hidden Master and IXFR or AXFR exchanges initiated by the Public Authoritative Servers. 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 Server. The CPE MUST listen for DNS on TCP and UDP and at least allow SOA lookups to the DNS Homenet Zone.

5.1.2. Securing Synchronization

Exchange between the Public Servers and the CPE MUST be secured, at least for integrity protection and for authentication. This is the case whatever mechanism is used between the CPE and the Public Authoritative DNS(SEC) Servers.

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 that 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 provides authentication mechanism.

Protocols like TLS [RFC5246] / DTLS [RFC6347] can be used to secure the transactions between the Public Authoritative Servers 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 Server 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 [RFC5996] 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 Server SHOULD NOT be impacted by middle boxes.

As mentioned above, TSIG, IPsec and TLS/DTLS may be used to secure transactions between the CPE and the Public Authentication Servers. The CPE and Public Authoritative Server SHOULD implement TSIG and IPsec.

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 Authentication Servers MUST support PSK and certificate based authentication.

5.2. DNS Homenet Zone configuration

As depicted in figure 1, he DNSSEC Public Zone is hosted on the Public Authoritative Server, whereas the DNS Homenet Zone is hosted on the CPE. As a result, the CPE MUST configure the DNS Homenet Zone as if the DNS Homenet Zone were hosted by the Public Authoritative Servers instead of the CPE.

If one considers the case where the CPE has a single Homenet Domain Name and has an agreement with a single Public Authoritative Server. In that case, the DNS Homenet Zone SHOULD configure its Name Server RRset and Start of Authority with the ones associated to the Public Authoritative Servers. This is illustrated in figure 2. public.autho.servers.example.net is the domain name associated to the Public Authoritative Server, and IP1, IP2, IP3, IP4 are the IP addresses associated.

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

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

@   NS  public.authoritative.servers.example.net

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

Figure 2: DNS Homenet Zone

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

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

- 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 slaves need to check the master 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 Masters and the CPE are expected to implement NOTIFY [RFC1996]. Then short values MAY increase the bandwidth usage for slaves 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 plug / 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 (1hour) seems more appropriated.

When the end user considers multiple Public Authoritative Servers for a given Registered Homenet Domain, the DNS Homenet Zone MAY contain all associated Name Servers and IP addresses.

Some additional verification can check whether the CPE IP address is mentioned in the Public Zone file, and raise a warning to the End User.

5.3. DNSSEC outsourcing configuration

In this document we assumed that the Public Authoritative Server signs the DNS Homenet Zone. Multiple variants MAY be proposed by the Public Authoritative Servers. Public Authoritative Servers MAY propose to sign the DNS Homenet Zone with keys generated by the Public Authoritative Servers and unknown to the CPE. Alternatively some MAY propose the end user to provide the private keys. Although not considered in this document some end user MAY still prefer to sign their zone with their own keys they do not communicate to the Public Authoritative Servers. All these alternatives result from a negotiation between the end user and the Public Authoritative Servers. This negotiation is performed out-of-band and is out of scope of this document.

In this document, we consider that the Public Authoritative Server has all the necessary cryptographic elements to perform zone signing and key management operations.

Note that Public Authoritative Servers described in this document accomplish different functions, and thus different entities MAY be involved.

- DNS Slave function synchronizes the DNS Homenet Zone between the CPE and the Public Authoritative Servers. The DNS Homenet Zone on the Public Authoritative Servers is not available, and the Public Authoritative Server MUST NOT address any DNS queries for that zone. As a result, the Public Authoritative Servers MAY chose a dedicated set of servers to serve the DNS Homenet Zone: the Public Authoritative Name Server Set.

- DNS Zone Signing function signs the DNS Zone Homenet Zone to generate an DNSSEC Public Zone.

- DNSSEC Authoritative Server hosts the naming service for the DNSSEC Public Zone. Any DNS(SEC) query associated to the Homenet Zone SHOULD be done using the specific servers designated as the Public Authoritative Master(s).

5.4. CPE Security Policies

This section details security policies related to the Hidden Master / Slave synchronization.

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

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

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

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

6. Homenet Naming Configuration

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 Servers MAY be defined with the following parameters. These parameters are necessary to establish a secure channel between the CPE and the Public Authoritative Server, and to set the appropriated DNS Homenet Zone file:

- 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 Master(s): The FQDN or IP addresses of the Public Authoritative Master. 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 slave, DNSSEC zone signing and DNSSEC zone hosting.

Setting the DNS 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 Server: The Public Authoritative Servers associated to the Registered Homenet Domain. Multiple Public Authoritative Server MAY be provided.

7. Security Considerations

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

7.1. 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.

7.2. 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.

8. IANA Considerations

This document has no actions for IANA.

9. 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.

10. References

10.1. Normative References

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

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

[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.

[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.

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

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

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

10.2. Informational References

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

Appendix A. Document Change Log

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

-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 Master(s)". "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 Master / Slave functions with CPE as Hidden Master/Homenet Server.

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

-00: First version published.

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: 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