Homenet D. Migault

Internet-Draft Ericsson

Intended status: Standards Track R. Weber

Expires: October 30, 2021 Nominum

M. Richardson

Sandelman Software Works

R. Hunter

Globis Consulting BV

April 28, 2021

Simple Provisioning of Public Names for Residential Networks

draft-ietf-homenet-front-end-naming-delegation-14

Abstract

Home owners often have IP devices that they wish to access from the

Internet using names. It has been possible to register and populate

a DNS Zone with names since DNS became a thing, but it has been an

activity typically reserved for experts. This document automates the

process through creation of a Homenet Naming Authority (HNA), whose

responsibility is to select, sign, and publish names to a set of

publicly visible servers.

The use of an outsourced primary DNS server deals with possible

renumbering of the home network, and with possible denial of service

attacks against the DNS infrastructure.

This document describes the mechanism that enables the HNA to

outsource the naming service to the DNS Outsourcing Infrastructure

(DOI) via a Distribution Master (DM).

In addition, this document deals with publication of a corresponding

reverse zone.

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 https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months

and may be updated, replaced, or obsoleted by other documents at any

Migault, et al. Expires October 30, 2021 [Page 1]

Internet-Draft public-names April 2021

time. It is inappropriate to use Internet-Drafts as reference

material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 30, 2021.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the

document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal

Provisions Relating to IETF Documents

(https://trustee.ietf.org/license-info) in effect on the date of

publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as

described in the Simplified BSD License.

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 3

1.1. Selecting Names to Publish . . . . . . . . . . . . . . . 5

1.2. Alternative solutions . . . . . . . . . . . . . . . . . . 6

2. Terminology . . . . . . . . . . . . . . . . . . . . . . . . . 7

3. Architecture Description . . . . . . . . . . . . . . . . . . 8

3.1. Architecture Overview . . . . . . . . . . . . . . . . . . 9

3.2. Distribution Master Communication Channels . . . . . . . 11

4. Control Channel between Homenet Naming Authority (HNA) and

Distribution Master (DM) . . . . . . . . . . . . . . . . . . 13

4.1. Information to build the Public Homenet Zone . . . . . . 13

4.2. Information to build the DNSSEC chain of trust . . . . . 13

4.3. Information to set the Synchronization Channel . . . . . 14

4.4. Deleting the delegation . . . . . . . . . . . . . . . . . 14

4.5. Messages Exchange Description . . . . . . . . . . . . . . 14

4.5.1. Retrieving information for the Public Homenet Zone. . 15

4.5.2. Providing information for the DNSSEC chain of trust . 16

4.5.3. Providing information for the Synchronization Channel 16

4.5.4. HNA instructing deleting the delegation . . . . . . . 17

4.6. Securing the Control Channel between Homenet Naming

Authority (HNA) and Distribution Master (DM) . . . . . . 17

4.7. Implementation Concerns . . . . . . . . . . . . . . . . . 18

5. DM Synchronization Channel between HNA and DM . . . . . . . . 19

5.1. Securing the Synchronization Channel between HNA and DM . 20

6. DM Distribution Channel . . . . . . . . . . . . . . . . . . . 20

7. HNA Security Policies . . . . . . . . . . . . . . . . . . . . 21

8. DNSSEC compliant Homenet Architecture . . . . . . . . . . . . 21

Migault, et al. Expires October 30, 2021 [Page 2]

Internet-Draft public-names April 2021

9. Homenet Reverse Zone Channels Configuration . . . . . . . . . 21

10. Homenet Public Zone Channel Configurations . . . . . . . . . 23

11. Renumbering . . . . . . . . . . . . . . . . . . . . . . . . . 24

11.1. Hidden Primary . . . . . . . . . . . . . . . . . . . . . 24

12. Privacy Considerations . . . . . . . . . . . . . . . . . . . 25

13. Security Considerations . . . . . . . . . . . . . . . . . . . 26

13.1. HNA DM channels . . . . . . . . . . . . . . . . . . . . 26

13.2. Names are less secure than IP addresses . . . . . . . . 27

13.3. Names are less volatile than IP addresses . . . . . . . 27

14. Information Model for Outsourced information . . . . . . . . 27

14.1. Outsourced Information Model . . . . . . . . . . . . . . 28

15. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 30

16. Acknowledgment . . . . . . . . . . . . . . . . . . . . . . . 30

17. Contributors . . . . . . . . . . . . . . . . . . . . . . . . 31

18. References . . . . . . . . . . . . . . . . . . . . . . . . . 31

18.1. Normative References . . . . . . . . . . . . . . . . . . 31

18.2. Informative References . . . . . . . . . . . . . . . . . 34

Appendix A. Envisioned deployment scenarios . . . . . . . . . . 36

A.1. CPE Vendor . . . . . . . . . . . . . . . . . . . . . . . 36

A.2. Agnostic CPE . . . . . . . . . . . . . . . . . . . . . . 36

Appendix B. Example: A manufacturer provisioned HNA product flow 37

Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 38

1. Introduction

The Homenet Naming Authority (HNA) is responsible for making devices

within the home network accessible by their name within the home network as

well as from outside the home network (e.g., the Internet). End users will be able to transparently make use of

this connectivity if they can use names to access the services they

want from their home network.

The use of a DNS zone for each home network is a reasonable and

scalable way to make the set of public names visible. There are a

number of ways to populate such a zone. This specification proposes

a method based on a number of assumptions about typical home networks:

1. The names of the devices accessible from the Internet are stored

in the Public Homenet Zone, served by a DNS authoritative server.

2. It is unlikely that home networks will contain sufficiently

robust platforms designed to host a service such as the DNS on

the Internet and as such would expose the home network to DDoS

attacks.

Migault, et al. Expires October 30, 2021 [Page 3]

Internet-Draft public-names April 2021

3. [RFC7368] emphasizes that the home network is subject to

connectivity disruptions with the ISP. But, names used within

the home MUST be resilient against such disruption.

This specification makes the public names resolvable within both the

home network and on the Internet, even when there are disruptions.

This is achieved by having a function inside the home network that

builds, signs, publishes, and manages a Public Homenet Zone. Doing so, thus

provides bindings between public names, IP addresses, and other RR

types.

The management of the names can be under the responsibility of the Customer Premises

Equipment (CPE). Other devices within the home network could

fulfill this role, e.g., a NAS server, but for simplicity, this

document assumes the function is located on one of the CPE devices.

The homenet architecture [RFC7368] makes it clear that a home network

may have multiple CPEs. The management of the Public Homenet Zone

involves DNS specific mechanisms that cannot be distributed over

multiple servers (primary server), when multiple nodes can

potentially manage the Public Homenet Zone, a single node needs to be

selected per outsourced zone. This selected node is designated as

providing the HNA function.

The process by which a single HNA is selected per zone is not in

the scope for this document.

CPEs, which may host the HNA function are usually low powered devices not designed for terminating

heavy traffic. As a result, hosting an authoritative DNS service

visible to the Internet may expose the home network to resource

exhaustion and other attacks. On the other hand, if the only copy of

the public zone is on the Internet, then Internet connectivity

disruptions would make the names unavailable within the homenet.

In order to avoid resource exhaustion and other attacks, this

document describes an architecture (Section 3.1) that outsources the authoritative

naming service of the home network. More specifically, the HNA

builds the Public Homenet Zone and outsources it to a DNS

Outsourcing Infrastructure (DOI) via a Distribution Master (DM). The

DOI is in charge of publishing the corresponding Public Homenet Zone

on the Internet. The transfer of DNS zone information is achieved

using standard DNS mechanisms involving primary and secondary DNS

servers, with the HNA hosted primary being a stealth primary, and the

DM a secondary.

Migault, et al. Expires October 30, 2021 [Page 4]

Internet-Draft public-names April 2021

In order to keep the Public

Homenet Zone up-to-date, Section 5 describes how the HNA and the DOI

synchronize the Pubic Homenet Zone.

The architecture is explicitly designed to enable fully

functional DNSSEC, and the Public Homenet Zone is expected to be

signed with a secure delegation. DNSSEC key management and zone

signing are handled by the HNA.

Section 10 discusses management and configuration of the Public

Homenet Zone. It shows that the HNA configuration of the DOI can

involve no or little interaction with the end user. More

specifically, it shows that the existence of an account in the DOI is

sufficient for the DOI to push the necessary configuration.

Section 9 discusses management of one or more reverse zones. It

shows that management of the reverse zones can be entirely automated

and benefit from a pre-established relation between the ISP and the

home network. Note that such scenarios may also be met for the

Public Homenet Zone.

Section 11 discusses how renumbering should be handled. Finally,

Sections 12 and 13 respectively discuss privacy and security

considerations when outsourcing the Public Homenet Zone.

The Public Homenet Zone is expected to contain public information

only in a single universal view. This document does not define how

the information required to construct this view is derived.

It is also not in the scope of this document to define names for

exclusive use within the boundaries of the local home network.

Instead, local scope information is expected to be provided to the

home network using local scope naming services. mDNS [RFC6762] and DNS-SD

[RFC6763] are two examples of these services. Currently, mDNS is

limited to a single link network. However, future protocols and

architectures [I-D.ietf-homenet-simple-naming] are expected to

leverage this constraint as pointed out in [RFC7558].

1.1. Selecting Names to Publish

While this document does not create any normative mechanism by which

the selection of names to publish, this document anticipates that the

home network administrator, will be presented with a list

of current names and addresses present on the inside of the home

network.

Migault, et al. Expires October 30, 2021 [Page 5]

Internet-Draft public-names April 2021

The administrator would mark which devices (by name), are to be

published. The HNA would then collect the IPv6 address(es)

associated with that device, and put the name into the Public Homenet

Zone. The address of the device can be collected from a number of

places: mDNS [RFC6762], DHCP [RFC6644], UPnP, PCP [RFC6887], or

manual configuration.

A device may have a Global Unicast Address (GUA), a Unique Local IPv6

Address (ULA), as as well IPv6-Link-Local addresses, IPv4-Link-Local

Addresses, and RFC1918 addresses. Of these the link-local are never

useful for the Public Zone, and must be omitted. The IPv6 ULA and

the RFC1918 addresses may be useful to publish, if the home network

environment features a VPN that would allow the home owner to reach

the network.

The IPv6 ULA addressees are significantly safer to publish.

In general, one expects the GUA to be the default address to be

published. However, during periods when the home network has

connectivity problems, the ULA and RFC1918 addressees can be used

inside the home, and the mapping from public name to locally useful

location address would permit many services secured with HTTPS to

continue to operate.

1.2. An Alternative Solution

An alternative existing solution in IPv4 is to have a single zone,

where a host uses a RESTful HTTP service to register a single name

into a common public zone. This is often called "Dynamic DNS", and

there are a number of commercial providers.

These solutions were typically used by a host behind the CPE to make

its CPE IPv4 address visible, usually in order to enable incoming

connections.

For a very few number (one to three) of hosts, the use of such a system

provides an alternative to the architecture described in this

document.

The alternative does suffer from some limitations:

o the CPE/HNA router is unaware of the process, and cannot respond

to queries for these names when there are disruptions in

connectivity. This makes the home user or application dependent

on having to resolve different names in the event of outages or

disruptions.

Migault, et al. Expires October 30, 2021 [Page 6]

Internet-Draft public-names April 2021

o the CPE/HNA router cannot control the process. Any host can do

this regardless of whether or not the home network administrator

wants the name published or not. There is therefore no possible

audit trail.

o the credentials for the dynamic DNS server need to be securely

transferred to all hosts that wish to use it. This is not a

problem for a technical user to do with one or two hosts, but it

does not scale to multiple hosts and becomes a problem for non-

technical users.

o "all the good names are taken" - current services put everyone's

names into some small set of zones, and there are often conflicts.

Distinguishing similar names by delegation of zones was among the

primary design goals of the DNS system.

o The RESTful services do not always support all RR types. The

homenet user is dependent on the service provider supporting new

types. By providing full DNS delegation, this document enables

all RR types and also future extensions.

There is no technical reason why a RESTful cloud service could not

provide solutions to many of these problems, but this document

describes a DNS-based solution.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and

"OPTIONAL" in this document are to be interpreted as described in

BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all

capitals, as shown here.

Customer Premises Equipment: (CPE) is a router providing

connectivity to the home network.

Homenet Zone: is the DNS zone for use within the boundaries of the

home network: ‘home.arpa’ (see [RFC8375]). This zone is not

considered public and is out of the scope for this document.

Registered Homenet Domain: is the domain name that is associated with the

home network.

Public Homenet Zone: contains the names in the home network that are

expected to be publicly resolvable on the Internet.

Homenet Naming Authority (HNA): is a function that is responsible for

managing the Public Homenet Zone. This includes populating the

Migault, et al. Expires October 30, 2021 [Page 7]

Internet-Draft public-names April 2021

Public Homenet Zone, signing the zone for DNSSEC, as well as

managing the distribution of that Homenet Zone to the DNS

Outsourcing Infrastructure (DOI).

DNS Outsourcing Infrastructure (DOI): is the infrastructure

that is responsible for receiving the Public Homenet Zone and publishing

it on the Internet. It is mainly composed of a Distribution

Master and Public Authoritative Servers.

Public Authoritative Servers: are the authoritative name servers for

the Public Homenet Zone. Name resolution requests for the Homenet

Domain are sent to these servers. For resiliency the Public

Homenet Zone SHOULD be hosted on multiple servers.

Homenet Authoritative Servers: are authoritative name servers within

the Homenet network.

Distribution Master (DM): is the (set of) server(s) to which the HNA

synchronizes the Public Homenet Zone, and which then distributes

the relevant information to the Public Authoritative Servers.

Homenet Reverse Zone: The reverse zone file associated with the

Public Homenet Zone.

Reverse Public Authoritative Servers: equivalent to Public

Authoritative Servers specifically for reverse resolution.

Reverse Distribution Master: equivalent to Distribution Master

specifically for reverse resolution.

Homenet DNSSEC Resolver: a resolver that performs a DNSSEC

resolution on the home network for the Public Homenet Zone. The

resolution is performed requesting the Homenet Authoritative

Servers.

DNSSEC Resolver: a resolver that performs a DNSSEC resolution on the

Internet for the Public Homenet Zone. The resolution is performed

requesting the Public Authoritative Servers.

3. Architecture Description

This section provides an overview of the architecture for outsourcing

the authoritative naming service from the HNA to the DOI. Note that Section 14 defines necessary parameter to configure the

HNA.

Migault, et al. Expires October 30, 2021 [Page 8]

Internet-Draft public-names April 2021

3.1. Architecture Overview

Figure 1 illustrates the architecture where the HNA outsources the

publication of the Public Homenet Zone to the DOI.

The Public Homenet Zone is identified by the Registered Homenet

Domain Name - myhome.example. The ".local" as well as ".home.arpa"

are explicitly not considered as Public Homenet zones and represented

as Homenet Zone in Figure 1.

The HNA SHOULD build the Public Homenet Zone in a single view

populated with all resource records that are expected to be published

on the Internet. The HNA also

signs the Public Homenet Zone. The HNA handles all operations and

keying material required for DNSSEC, so there is no provision made in

this architecture for transferring private DNSSEC related keying

material between the HNA and the DM.

Once the Public Homenet Zone has been built, the HNA outsources it to

the DOI as described in Figure 1. The HNA acts as a hidden primary

while the DM behaves as a secondary responsible to distribute the

Public Homenet Zone to the multiple Public Authoritative Servers that

DOI is responsible for. The DM has three communication channels:

o a DM Control Channel (Section 4) to configure the HNA

and the DOI,

o a DM Synchronization Channel (Section 5) to synchronize

the Public Homenet Zone on the HNA and on the DM,

o one or more Distribution Channels (Section 6) that

distribute the Public Homenet Zone from the DM to the Public

Authoritative Server serving the Public Homenet Zone on the

Internet.

There might be multiple DM's, and multiple servers per DM. This text

assumes a single DM server for simplicity, but there is no reason why

each channel needs to be implemented on the same server or

use the same code base.

It is important to note that while the HNA is configured as an

authoritative server, it is not expected to answer to DNS requests

from the public Internet for the Public Homenet Zone. More

specifically, the addresses associated with the HNA SHOULD NOT be

mentioned in the NS records of the Public Homenet zone, unless

additional security provisions necessary to protect the HNA from

external attack have been taken.

Migault, et al. Expires October 30, 2021 [Page 9]

Internet-Draft public-names April 2021

The DOI is also responsible for ensuring the DS record has been

updated in the parent zone.

Resolution is performed by the DNSSEC resolvers. When the resolution

is performed outside the home network, the DNSSEC Resolver resolves

the DS record on the Global DNS and the name associated to the Public

Homenet Zone (myhome.example) on the Public Authoritative Servers.

When the resolution is performed from within the home network, the

Homenet DNSSEC Resolver may proceed similarly. On the other hand, to

provide resilience to the Public Homenet Zone in case of WAN connectivity disruption,

the Homenet DNSSEC Resolver SHOULD be able to perform the resolution

on the Homenet Authoritative Servers. These servers are not expected

to be mentioned in the Public Homenet Zone, nor to be accessible from

the Internet. As such their information as well as the corresponding

signed DS record MAY be provided by the HNA to the Homenet DNSSEC

Resolvers, e.g., using HNCP [RFC7788]. Such configuration is outside

the scope of this document. Since the scope of the Homenet

Authoritative Servers is limited to the home network, these servers

are expected to serve the Homenet Zone as represented in Figure 1.

How the Homenet Authoritative Servers are provisioned is also out of

the scope of this specification. It could be implemented using primary

secondaries servers, or via rsync. In some cases, the HNA and

Homenet Authoritative Servers may be combined together which would

result in a common instantiation of an authoritative server on the

WAN and inner interface. Other mechanisms may also be used.

Migault, et al. Expires October 30, 2021 [Page 10]

Internet-Draft public-names April 2021

Home network | Internet

|

| +----------------------------+

| | DOI |

Control | | |

+-----------------------+ Channel | | +-----------------------+ |

| HNA |<-------------->| Distribution Master | |

|+---------------------+| | | |+---------------------+| |

|| Public Homenet Zone ||Synchronization || Public Homenet Zone || |

|| (myhome.example) || Channel | | || (myhome.example) || |

|+---------------------+|<-------------->|+---------------------+| |

+-----------^-----------+ | | +-----------------------+ |

. | | ^ Distribution |

. | | | Channel |

+-----------v-----------+ | | v |

| Homenet Authoritative | | | +-----------------------+ |

| Server(s) | | | | Public Authoritative | |

|+---------------------+| | | | Server(s) | |

||Public Homenet Zone || | | |+---------------------+| |

|| (myhome.example) || | | || Public Homenet Zone || |

|+---------------------+| | | || (myhome.example) || |

|| Homenet Zone || | | |+---------------------+| |

|| (home.arpa) || | | +-----------------------+ |

|+---------------------+| | +----------^---|-------------+

+----------^---|--------+ | | |

| | name resolution | |

| v | | v

+----------------------+ | +-----------------------+

| Homenet | | | Internet |

| DNSSEC Resolver | | | DNSSEC Resolver |

+----------------------+ | +-----------------------+

Figure 1: Homenet Naming Architecture

3.2. Distribution Master Communication Channels

This section details the DM channels, that is

the Control Channel, the Synchronization Channel, and the Distribution

Channel.

The Control Channel and the Synchronization Channel are the

interfaces used between the HNA and the DOI. The entity within the

DOI responsible to handle these communications is the DM.

The communications between the HNA and the DM SHOULD be protected and

mutually authenticated. While Section 4.6 discusses in more

depth the different security protocols that could be used to secure,

this specification RECOMMENDS the use of TLS with mutually

Migault, et al. Expires October 30, 2021 [Page 11]

Internet-Draft public-names April 2021

authentication based on certificates to secure the channel between

the HNA and the DM.

The Control Channel is used to set up the Synchronization Channel.

We assume that the HNA initiates the Control Channel connection with

the DM and as such has a prior knowledge of the DM identity (X509

certificate), the IP address and port number to use and protocol to set

secure session. We also assume the DM has knowledge of the identity

of the HNA (X509 certificate) as well as the Registered Homenet

Domain. For more detail to see how this can be achieved, please see

Section 10.

The information exchanged between the HNA and the DM uses DNS

messages protected by DNS over TLS (DoT) [RFC7858]. Other

specifications may consider protecting DNS messages with other

transport layers, among others, DNS over DTLS [RFC8094], or DNS over

HTTPs (DoH) [RFC8484] or DNS over QUIC [I-D.ietf-dprive-dnsoquic].

There was consideration to using a standard TSIG [RFC2845] or SIG(0)

[RFC2931] to perform a dynamic DNS update to the DM. There are a

number of issues with this. The first one is that TSIG or SIG(0)

make scenarios where the end user needs to interact via its web

browser more complex. More precisely, authorization and access

control granted via OAUTH would be unnecessarily complex with TSIG or

SIG(0).

The main issue is that the Dynamic DNS update would also update the

parent zone's (NS, DS and associated A or AAAA records) while the

goal is to update the DM configuration files. The visible NS records

SHOULD remain pointing at the cloud provider's anycast addresses.

Revealing the address of the HNA in the DNS is not desirable. Refer to Section 4.2 for more details.

This specification assumes:

o the DM serves both the Control Channel and Synchronization Channel

on a single IP address, single port and using a single transport

protocol.

o By default, the HNA uses a single IP address for both the Control

and Synchronization channel. However, the HNA MAY use distinct IP

addresses for the Control Channel and the Synchronization Channel

- see Section 5 and Section 4.3 for more details.

The Distribution Channel is internal to the DOI and as such is not

the primary concern of this specification.

Migault, et al. Expires October 30, 2021 [Page 12]

Internet-Draft public-names April 2021

4. Control Channel

The DM Control Channel is used by the HNA and the DOI to exchange

information related to the configuration of the delegation which

includes information to build the Public Homenet Zone (

Section 4.1), information to build the DNSSEC chain of trust (

Section 4.2), and information to set the Synchronization Channel (

Section 4.3).

4.1. Information to Build the Public Homenet Zone

When the HNA builds the Public Homenet Zone, it must include

information that it retrieves from the DM relating to how the zone is

to be published.

The information includes at least names and IP addresses of the

Public Authoritative Name Servers. In term of RRset information this

includes:

o the MNAME of the SOA,

o the NS and associated A and AAA RRsets of the name servers.

The DOI MAY also provide operational parameters such as

other fields of SOA (SERIAL, RNAME, REFRESH, RETRY, EXPIRE and

MINIMUM). As the information is necessary for the HNA to proceed and

the information is associated to the DOI, this information exchange

is mandatory.

4.2. Information to build the DNSSEC chain of trust

The HNA SHOULD provide the hash of the KSK (DS RRset), so the that

DOI provides this value to the parent zone. A common deployment use

case is that the DOI is the registrar of the Registered Homenet

Domain, and as such, its relationship with the registry of the parent

zone enables it to update the parent zone. When such relation

exists, the HNA should be able to request the DOI to update the DS

RRset in the parent zone. A direct update is especially necessary to

initialize the chain of trust.

Though the HNA may also later directly update the values of the DS

via the Control Channel, it is RECOMMENDED to use other mechanisms

such as CDS and CDNSKEY [RFC7344] for transparent updates during key

roll overs.

As some deployments may not provide a DOI that will be able to update

the DS in the parent zone, this information exchange is OPTIONAL.

Migault, et al. Expires October 30, 2021 [Page 13]

Internet-Draft public-names April 2021

By accepting the DS RR, the DM commits in taking care of advertising

the DS to the parent zone. Upon refusal, the DM clearly indicates it

does not have the capacity to proceed to the update.

4.3. Information to set the Synchronization Channel

The HNA works as a primary authoritative DNS server, while the DM

works like a secondary. As a result, the HNA MUST provide the IP

address the DM is using to reach the HNA. The synchronization

Channel will be set between that IP address and the IP address of the

DM. By default, the IP address used by the HNA in the Control

Channel is considered by the DM and the specification of the IP by

the HNA is only OPTIONAL. The transport channel (including port number) is

the same as the one used between the HNA and the DM for the Control

Channel.

4.4. Deleting the delegation

The purpose of the previous sections were to exchange information in

order to set a delegation. The HNA MUST also be able to delete a

delegation with a specific DM. Upon an instruction of deleting the

delegation, the DM MUST stop serving the Public Homenet Zone.

4.5. Messages Exchange Description

There are multiple ways this information could be exchanged between

the HNA and the DM. This specification defines a mechanism that re-

use the DNS exchanges format. The intention is to reuse standard

libraries especially to check the format of the exchanged fields as

well as to minimize the additional libraries needed for the HNA. The

re-use of DNS exchanges achieves these goals. Note that while

information is provided using DNS exchanges, the exchanged

information is not expected to be set in any zone file, instead this

information is expected to be processed appropriately.

The Control Channel is not expected to be a long term session. After

a predefined timer the Control Channel is expected to be terminated.

The Control Channel MAY be re-opened at any time later.

The provisioning process SHOULD provide a method of securing the

Control Channel, so that the content of messages can be

authenticated. This authentication MAY be based on certificates for

both the DM and each HNA. The DM may also create the initial

configuration for the delegation zone in the parent zone during the

provisioning process.

Migault, et al. Expires October 30, 2021 [Page 14]

Internet-Draft public-names April 2021

4.5.1. Retrieving information for the Public Homenet Zone.

The information provided by the DM to the HNA is retrieved by the HNA

with an AXFR exchange [RFC1034]. AXFR enables the response to

contain any type of RRsets. The response might be extended in the

future if additional information will be needed. Alternatively, the

information provided by the HNA to the DM is pushed by the HNA via a

DNS update exchange [RFC2136].

To retrieve the necessary information to build the Public Homenet

Zone, the HNA MUST send a DNS request of type AXFR associated to the

Registered Homenet Domain. The DM MUST respond with a zone template.

The zone template MUST contain a RRset of type SOA, one or multiple

RRset of type NS and zero or more RRset of type A or AAAA.

o The SOA RR indicates to the HNA the value of the MNAME

of the Public Homenet Zone.

o The NAME of the SOA RR MUST be the Registered Homenet Domain.

o The MNAME value of the SOA RDATA is the value provided by the DOI

to the HNA.

o Other RDATA values (RNAME, REFRESH, RETRY, EXPIRE and MINIMUM) are

provided by the DOI as suggestions.

The NS RRsets carry the Public Authoritative Servers of

the DOI. Their associated NAME MUST be the Registered Homenet

Domain.

The TTL and RDATA are those expected to be published on the Public

Homenet Zone. The RRsets of Type A and AAAA MUST have their NAME

matching the NSDNAME of one of the NS RRsets.

Upon receiving the response, the HNA MUST validate format and

properties of the SOA, NS and A or AAAA RRsets. If an error occurs,

the HNA MUST stop proceeding and MUST report an error. Otherwise,

the HNA builds the Public Homenet Zone by setting the MNAME value of

the SOA as indicated by the SOA provided by the AXFR response. The

HNA SHOULD set the value of NAME, REFRESH, RETRY, EXPIRE and MINIMUM

of the SOA to those provided by the AXFR response. The HNA MUST

insert the NS and corresponding A or AAAA RRset in its Public Homenet

Zone. The HNA MUST ignore other RRsets. If an error message is

returned by the DM, the HNA MUST proceed as a regular DNS resolution.

Error messages SHOULD be logged for further analysis. If the

resolution does not succeed, the outsourcing operation is aborted and

the HNA MUST close the Control Channel.

Migault, et al. Expires October 30, 2021 [Page 15]

Internet-Draft public-names April 2021

4.5.2. Providing information for the DNSSEC chain of trust

To provide the DS RRset to initialize the DNSSEC chain of trust the

HNA MAY send a DNS update [RFC2136] message.

The DNS update message is composed of a Header section, a Zone

section, a Pre-requisite section, and Update section and an

additional section. The Zone section MUST set the ZNAME to the

parent zone of the Registered Homenet Domain - that is where the DS

records should be inserted. As described [RFC2136], ZTYPE is set to

SOA and ZCLASS is set to the zone's class. The Pre-requisite section

MUST be empty. The Update section is a DS RRset with its NAME set to

the Registered Homenet Domain and the associated RDATA corresponds to

the value of the DS. The Additional Data section MUST be empty.

Though the pre-requisite section MAY be ignored by the DM, this value

is fixed to remain coherent with a standard DNS update.

Upon receiving the DNS update request, the DM reads the DS RRset in

the Update section. The DM checks ZNAME corresponds to the parent

zone. The DM SHOULD ignore non empty the Pre-requisite and

Additional Data section. The DM MAY update the TTL value before

updating the DS RRset in the parent zone. Upon a successful update,

the DM should return a NOERROR response as a commitment to update the

parent zone with the provided DS. An error indicates the MD does not

update the DS, and other method should be used by the HNA.

The regular DNS error message SHOULD be returned to the HNA when an

error occurs. In particular a FORMERR is returned when a format

error is found, this includes when unexpected RRSets are added or

when RRsets are missing. A SERVFAIL error is returned when a

internal error is encountered. A NOTZONE error is returned when

update and Zone sections are not coherent, a NOTAUTH error is

returned when the DM is not authoritative for the Zone section. A

REFUSED error is returned when the DM refuses to proceed to the

configuration and the requested action.

4.5.3. Providing information for the Synchronization Channel

To provide a non default IP address used by the HNA for the

Synchronization Channel, the HNA MAY send a DNS Update message.

Similarly to the Section 4.5.2, the HNA MAY specify the IP

address using a DNS update message. The Zone section sets its ZNAME

to the parent zone of the Registered Homenet Domain, ZTYPE is set to

SOA and ZCLASS is set to the zone's type. Pre-requisite is empty.

The Update section is a RRset of type NS. The Additional Data

Migault, et al. Expires October 30, 2021 [Page 16]

Internet-Draft public-names April 2021

section contains the RRsets of type A or AAAA that designates the IP

addresses associated to the primary (or the HNA).

The reason to provide these IP addresses is that it is NOT

RECOMMENDED to publish these IP addresses. As a result, it is not

expected to resolve them.

Upon receiving the DNS update request, the DM reads the IP addresses

and checks the ZNAME corresponds to the parent zone. The DM SHOULD

ignore a non empty Pre-requisite section. The DM configures the

secondary with the IP addresses and returns a NOERROR response to

indicate it is committed to serve as a secondary.

Similarly to Section 4.5.2, DNS errors are used and an error

indicates the DM is not configured as a secondary.

4.5.4. HNA instructing deleting the delegation

To instruct to delete the delegation, the HNA SHOULD send a DNS UPDATE

Delete message.

The Zone section sets its ZNAME to the Registered Homenet Domain, the

ZTYPE to SOA and the ZCLASS to zone's type. The Pre-requisite

section is empty. The Update section is a RRset of type NS with the

NAME set to the Registered Domain Name. As indicated by [RFC2136]

section 2.5.2 the delete instruction is set by setting the TTL to 0,

the Class to ANY, the RDLENGTH to 0 and the RDATA MUST be empty. The

Additional Data section is empty.

Upon receiving the DNS update request, the DM checks the request and

removes the delegation. The DM returns a NOERROR response to

indicate the delegation has been deleted. Similarly to

Section 4.5.2, DNS errors are used and an error indicates the

delegation has not been deleted.

4.6. Securing the Control Channel

The control channel between the HNA and the DM MUST be secured at

both the HNA and the DM.

Secure protocols (like TLS [RFC8446] SHOULD be used to secure the

transactions between the DM and the HNA.

The advantage of TLS is that this technology is widely deployed, and

most of the devices already embed TLS libraries, possibly also taking

advantage of hardware acceleration. Further, TLS provides

authentication facilities and can use certificates to mutually

Migault, et al. Expires October 30, 2021 [Page 17]

Internet-Draft public-names April 2021

authenticate the DM and HNA at the application layer, including

available API. On the other hand, using TLS requires implementing

DNS exchanges over TLS, as well as a new service port.

The HNA SHOULD authenticate inbound connections from the DM using

standard mechanisms, such as a public certificate with baked-in root

certificates on the HNA, or via DANE [RFC6698]. The HNA is expected

to be provisioned with a connection to the DM by the manufacturer, or

during some user-initiated onboarding process, see Section 10.

The DM SHOULD authenticate the HNA and check that inbound messages

are from the appropriate client. The DM MAY use a self-signed CA

certificate mechanism per HNA, or public certificates for this

purpose.

IPsec [RFC4301] and IKEv2 [RFC7296] were considered. They would need

to operate in transport mode, and the authenticated end points would

need to be visible to the applications, and this is not commonly

available at the time of this writing.

A pure DNS solution using TSIG and/or SIG(0) to authenticate message

was also considered. Section 10 envisions one mechanism would

involve the end user, with a browser, signing up to a service

provider, with a resulting OAUTH2 token to be provided to the HNA. A

way to translate this OAUTH2 token from HTTPS web space to DNS SIG(0)

space seems overly problematic, and so the enrollment protocol using

web APIs was determined to be easier to implement at scale.

Note also that authentication of message exchanges between the HNA

and the DM SHOULD NOT use the external IP address of the HNA to index

the appropriate keys. As detailed in Section 11, the IP addresses of

the DM 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 SHOULD NOT be indexed using the IP

address, and SHOULD be resilient to IP address changes.

4.7. Implementation Concerns

The Hidden Primary Server on the HNA differs from a regular

authoritative server for the home network due to:

Interface Binding: the Hidden Primary Server will almost certainly

listen on the WAN Interface, whereas a regular Homenet

Authoritative Servers would listen on the internal home network

interface.

Migault, et al. Expires October 30, 2021 [Page 18]

Internet-Draft public-names April 2021

Limited exchanges: the purpose of the Hidden Primary Server is to

synchronize with the DM, not to serve any zones to end users, or

the public Internet.

As a result, exchanges are performed with specific nodes (the DM).

Further, exchange types are limited. The only legitimate exchanges

are: NOTIFY initiated by the Hidden Primary and IXFR or AXFR

exchanges initiated by the DM.

On the other hand, regular authoritative servers would respond to any

hosts, and any DNS query would be processed. The HNA SHOULD filter

IXFR/AXFR traffic and drop traffic not initiated by the DM. The HNA

MUST at least allow SOA lookups of the Homenet Zone.

5. DM Synchronization Channel

The DM Synchronization Channel is used for communication between the

HNA and the DM for synchronizing the Public Homenet Zone. Note that

the Control Channel and the Synchronization Channel are by

design different channels even though there they may use the

same IP address. The Control Channel is set between the HNA

working as a client using port number YYYY (a high range port) toward a

service provided by the DM at port number XX (well-known port number).

On the other hand, the Synchronization Channel is set between the DM

working as a client using port ZZZZ ( a high range port) toward a

service a service provided by the HNA at port XX.

As a result, even though the same couple of IP addresses may be

involved the Control Channel and the Synchronization Channel are

always distinct channels.

Uploading and dynamically updating the zone file on the DM can be

seen as zone provisioning between the HNA (Hidden Primary) and the DM

(Secondary Server). This can be handled via AXFR + DNS Update.

This document RECOMMENDS use of a primary / secondary mechanism

instead of the use of DNS Update. The primary / secondary mechanism

is RECOMMENDED as it scales better and avoids DoS attacks. Note that

even when UPDATE messages are used, these messages are using a

distinct channel as those used to set the configuration.

Note that there is no standard way to distribute a DNS primary

between multiple devices. As a result, if multiple devices are

candidate for hosting the Hidden Primary, some specific mechanisms

should be designed so the home network only selects a single HNA for

the Hidden Primary. Selection mechanisms based on HNCP [RFC7788] are

good candidates.

Migault, et al. Expires October 30, 2021 [Page 19]

Internet-Draft public-names April 2021

The HNA acts as a Hidden Primary Server, which is a regular

authoritative DNS Server listening on the WAN interface.

The DM is configured as a secondary for the Registered Homenet Domain

Name. This secondary configuration has been previously agreed

between the end user and the provider of the DOI as part of either

the provisioning or due to receipt of DNS Update messages on the DM

Control Channel.

The Homenet Reverse Zone MAY also be updated either with DNS UPDATE

[RFC2136] or using a primary / secondary synchronization.

5.1. Securing the Synchronization Channel

The Synchronization Channel uses standard DNS requests.

First, the primary notifies the secondary that the zone must be

updated and eaves the secondary to proceed with the update when

possible/convenient.

Then, a NOTIFY message is sent by the primary, which is a small

packet that is less likely to load the secondary.

Finally, the AXFR [RFC1034] or IXFR [RFC1995] query performed by the

secondary is a small packet sent over TCP (Section 4.2 [RFC5936]),

which mitigates reflection attacks using a forged NOTIFY.

The AXFR request from the DM to the HNA SHOULD be secured and the use

of TLS is RECOMMENDED [I-D.ietf-dprive-xfr-over-tls]

When using TLS, the HNA MAY authenticate inbound connections from the

DM using standard mechanisms, such as a public certificate with

baked-in root certificates on the HNA, or via DANE [RFC6698]. In

addition, to guarantee the DM remains the same across multiple TLS

session, the HNA and DM MAY implement [RFC8672].

The HNA SHOULD apply an ACL on inbound AXFR requests to

ensure they only arrive from the DM Synchronization Channel. In this

case, the HNA SHOULD regularly check (via DNS resolution) that the

address of the DM in the filter is still valid.

6. DM Distribution Channel

The DM Distribution Channel is used for communication between the DM

and the Public Authoritative Servers. The architecture and

communication used for the DM Distribution Channels is outside the

scope of this document, and there are many existing solutions

available, e.g., rsynch, DNS AXFR, REST, DB copy.

Migault, et al. Expires October 30, 2021 [Page 20]

Internet-Draft public-names April 2021

7. HNA Security Policies

This section details security policies related to the Hidden Primary

/ Secondary synchronization.

The HNA, as Hidden Primary SHOULD drop any queries from the home

network. This could be implemented via port binding and/or firewall

rules. The precise mechanism deployed is out of scope of this

document. The Hidden Primary SHOULD drop any DNS queries arriving on

the WAN interface that are not issued from the DM. 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, depending on how the

synchronization is secured.

8. DNSSEC compliant Homenet Architecture

[RFC7368] in Section 3.7.3 recommends DNSSEC to be deployed on both

the authoritative server and the resolver. The resolver side is out

of scope of this document, and only the authoritative part of the

server is considered.

This document assumes the HNA signs the Public Homenet Zone.

Secure delegation is achieved only if the DS RRset is properly set in

the parent zone. Secure delegation is performed by the HNA or the

DOIs.

The DS RRset can be updated manually with nsupdate for example. This

requires the HNA or the DOI to be authenticated by the DNS server

hosting the parent of the Public Homenet Zone. Such a trust channel

between the HNA and the parent DNS server may be hard to maintain

with HNAs, and thus may be easier to establish with the DOI. In

fact, the Public Authoritative Server(s) may use Automating DNSSEC

Delegation Trust Maintenance [RFC7344].

9. Homenet Reverse Zone Channels Configuration

The Public Homenet Zone is associated to a Registered Homenet Domain

and the ownership of that domain requires a specific registration

from the end user as well as the HNA being provisioned with some

authentication credentials. Such steps are mandatory unless the DOI

has some other means to authenticate the HNA. Such situation may

occur, for example, when the ISP provides the Homenet Domain as well

as the DOI.

Migault, et al. Expires October 30, 2021 [Page 21]

Internet-Draft public-names April 2021

In this case, the HNA may be authenticated by the physical link

layer, in which case the authentication of the HNA may be performed

without additional provisioning of the HNA. While this may not be so

common for the Public Homenet Zone, this situation is expected to be

quite common for the Reverse Homenet Zone.

More specifically, a common case is that the upstream ISP provides

the IPv6 prefix to the Homenet with a IA\_PD [RFC8415] option and

manages the DOI of the associated reverse zone.

This leave place for setting up automatically the relation between

HNA and the DNS Outsourcing infrastructure as described, e.g., in

[I-D.ietf-homenet-naming-architecture-dhc-options].

In the case of the reverse zone, the DOI authenticates the source of

the updates by IPv6 Access Control Lists. In the case of the reverse

zone, the ISP knows exactly what addresses have been delegated. The

HNA SHOULD therefore always originate Synchronization Channel updates

from an IP address within the zone that is being updated.

For example, if the ISP has assigned 2001:db8:f00d::/64 to the WAN

interface (by DHCPv6, or PPP/RA), then the HNA should originate

Synchronization Channel updates from 2001:db8:f00d::2.

An ISP that has delegated 2001:db8:babe::/56 to the HNA via

DHCPv6-PD, then HNA should originate Synchronization Channel updates

an IP within that subnet, such as 2001:db8:babe:0001::2.

With this relation automatically configured, the synchronization

between the Home network and the DOI happens similarly as for the

Public Homenet Zone described earlier in this document.

Note that for home networks connected to by multiple ISPs, each ISP

provides only the DOI of the reverse zones associated to the

delegated prefix. It is also likely that the DNS exchanges will need

to be performed on dedicated interfaces as to be accepted by the ISP.

More specifically, the reverse zone associated to prefix 1 will not

be possible to be performs by the HNA using an IP address that

belongs to prefix 2. Such constraints does not raise major concerns

either for hot standby or load sharing configuration.

With IPv6, the domain space for IP addresses is so large that reverse

zone may be confronted with scalability issues. How the reverse zone

is generated is out of scope of this document.

[I-D.howard-dnsop-ip6rdns] provides guidance on how to address

scalability issues.

Migault, et al. Expires October 30, 2021 [Page 22]

Internet-Draft public-names April 2021

10. Homenet Public Zone Channel Configurations

This document does not deal with how the HNA is provisioned with a

trusted relationship to the Distribution Master for the forward zone.

This section details what needs to be provisioned into the HNA and

serves as a requirements statement for mechanisms.

The HNA needs to be provisioned with:

o the Registered Domain (e.g., myhome.isp.example )

o the contact info for the Distribution Master (DM), including the

DNS name (FQDN), possibly including the IP literal, and a

certificate (or anchor) to be used to authenticate the service

o the DM transport protocol and port (the default is DNS over TLS,

on port 853)

o the HNA credentials used by the DM for its authentication.

The HNA will need to select an IP address for communication for the

Synchronization Channel. This is typically the WAN address

of the RG router, but could be an IPv6 LAN address in the case of a home

with multiple ISPs (and multiple border routers). This is

communicated in Section 4.5.3 when the NS and A or AAAA

RRsets are communicated.

The above parameters MUST be provisioned for ISP-specific reverse

zones, as per [I-D.ietf-homenet-naming-architecture-dhc-options].

ISP-specific forward zones MAY also be provisioned using

[I-D.ietf-homenet-naming-architecture-dhc-options], but zones which

are not related to a specific ISP zone (such as with a DNS provider)

must be provisioned through other means.

Similarly, if the HNA is provided by a registrar, the HNA may be

given configured to end user.

In the absence of specific pre-established relation, these pieces of

information may be entered manually by the end user. In order to

ease the configuration from the end user the following scheme may be

implemented.

The HNA may present the end user a web interface where it provides

the end user the ability to indicate the Registered Homenet Domain or

the registrar for example a preselected list. Once the registrar has

been selected, the HNA redirects the end user to that registrar in

order to receive a access token. The access token will enable the

Migault, et al. Expires October 30, 2021 [Page 23]

Internet-Draft public-names April 2021

HNA to retrieve the DM parameters associated to the Registered

Domain. These parameters will include the credentials used by the

HNA to establish the Control and Synchronization Channels.

Such architecture limits the necessary steps to configure the HNA

from the end user.

11. Renumbering

This section details how renumbering is handled by the Hidden Primary

server or the DM. Both types of renumbering are discussed i.e.

"make-before-break" and "break-before-make" (aka flash renumbering).

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 be familiar with them

before reading this section.

11.1. Hidden Primary

In a renumbering scenario, the HNA or Hidden Primary is informed it

is being renumbered. In most cases, this occurs because the whole

home network is being renumbered. As a result, the Public Homenet

Zone will also be updated. Although the new and old IP addresses may

be stored in the Public Homenet Zone, we recommend that only the

newly reachable IP addresses be published.

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

associated with a RRset of the Public Homenet Zone, it may be cached

for TTL seconds. Let T\_NEW be the time the new IP address replaces

the old IP address in the Homenet Zone, 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 with 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 =

Migault, et al. Expires October 30, 2021 [Page 24]

Internet-Draft public-names April 2021

T\_NEW, and the device may become unreachable up to 2 \* TTL. Of

course if T\_NEW >= T\_OLD\_UNREACHABLE, the disruption is increased.

Once the Public Homenet Zone file has been updated on the Hidden

Primary, the Hidden Primary needs to inform the DOI that the Public

Homenet Zone has been updated and that the IP address to use to

retrieve the updated zone has also been updated. Both notifications

are performed using regular DNS exchanges. Mechanisms to update an

IP address provided by lower layers with protocols like SCTP

[RFC4960], MOBIKE [RFC4555] are not considered in this document.

Instead the IP address of the HNA is updated using the

Synchronization Channel as described in Section 4.3.

12. Privacy Considerations

Outsourcing the DNS Authoritative service from the HNA to a third

party raises a few privacy related concerns.

The Public Homenet Zone lists the names of services hosted in the

home network. Combined with blocking of AXFR queries, the use of

NSEC3 [RFC5155] (vs NSEC [RFC4034]) prevents an attacker from being

able to walk the zone, to discover all the names. However, the

attacker may be able to walk the reverse DNS zone, or use other

reconnaissance techniques to learn this information as described in

[RFC7707].

In general a home network owner is expected to publish only names for

which there is some need to be able to reference externally.

Publication of the name does not imply that the service is

necessarily reachable from any or all parts of the Internet.

[RFC7084] mandates that the outgoing-only policy [RFC6092] be

available, and in many cases it is configured by default. A well

designed User Interface would combine a policy for making a service

public by a name with a policy on who may access it.

In many cases, the home network owner wishes to publish names for

services that only they will be able to access. The access control

may consist of an IP source address range, or access may be

restricted via some VPN functionality. The purpose of publishing the

name is so that the service may be access by the same name both

within the home, and outside the home. Sending traffic to the

relevant IPv6 address causes the relevant VPN policy to be enacted

upon.

While the problem of getting access to internal names has been solved

in Enterprise configurations with a split-DNS, and such a thing could

be done in the home, many recent improvements to VPN user interfaces

make it more likely that an individual might have multiple

Migault, et al. Expires October 30, 2021 [Page 25]

Internet-Draft public-names April 2021

connections configured. For instance, an adult child checking on the

state of a home automation system for a parent.

In addition to the Public Homenet Zone, pervasive DNS monitoring can

also monitor the traffic associated with the Public Homenet Zone.

This traffic may provide an indication of the services an end user

accesses, plus how and when they use these services. Although,

caching may obfuscate this information inside the home network, it is

likely that outside your home network this information will not be

cached.

13. Security Considerations

This document exposes a mechanism that prevents the HNA from being

exposed to the Internet and served DNS request from the Internet.

These requests are instead served by the DOI. While this limits the

level of exposure of the HNA, the HNA remains exposed to the Internet

with communications with the DOI. This section analyses the attack

surface associated to these communications. In addition, the DOI

exposes data that are related to the home network. This section also

analyses the implication of such exposure.

13.1. HNA DM channels

The channels between HNA and DM are mutually authenticated and

encrypted with TLS [RFC8446] and its associated security

considerations apply. To ensure the multiple TLS session are

continuously authenticating the same entity, TLS may take advantage

of second factor authentication as described in [RFC8672].

At the time of writing TLS 1.2 or TLS 1.3 can be used and TLS 1.3 (or

newer) SHOULD be supported.

The DNS protocol is subject to reflection attacks, however, these

attacks are largely applicable when DNS is carried over UDP. The

interfaces between the HNA and DM are using TLS over TCP, which

prevents such reflection attacks. Note that Public Authoritative

servers hosted by the DOI are subject to such attacks, but that is

out of scope of our document.

Note that in the case of the Reverse Homenet Zone, the data is less

subject to attacks than in the Public Homenet Zone. In addition, the

DM and RDM may be provided by the ISP - as described in

[I-D.ietf-homenet-naming-architecture-dhc-options], in which case DM

and RDM might be less exposed to attacks - as communications within a

network.

Migault, et al. Expires October 30, 2021 [Page 26]

Internet-Draft public-names April 2021

13.2. Names are less secure than IP addresses

This document describes how an end user can make their services and

devices from his home network reachable on the Internet by using

names rather than IP addresses. This exposes the home network to

attackers, since names are expected to include less entropy than IP

addresses. In fact, with IP addresses, the Interface Identifier is

64 bits long leading to up to 2^64 possibilities for a given

subnetwork. This is not to mention that the subnet prefix is also of

64 bits long, thus providing up to 2^64 possibilities. On the other

hand, names used either for the home network domain or for the

devices present less entropy (livebox, router, printer, nicolas,

jennifer, ...) and thus potentially exposes the devices to dictionary

attacks.

13.3. 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 a time

invariant prefix by ISPs. As a result, observing IP addresses only

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 than logging IP addresses, especially to profile an 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 end users may choose not to respond to PTR DNS queries

and MAY instead return a NXDOMAIN response.

14. Information Model for Outsourced information

This section is non-normative for the front-end protocol. It

specifies an optional format for the set of parameters required by

the HNA to configure the naming architecture of this document.

In cases where a home router has not been provisioned by the

manufacturer (when forward zones are provided by the manufacturer),

or by the ISP (when the ISP provides this service), then a home user/

owner will need to configure these settings via an administrative

interface.

By defining a standard format (in JSON) for this configuration

information, the user/owner may be able to just copy and paste a

configuration blob from the service provider into the administrative

interface of the HNA.

Migault, et al. Expires October 30, 2021 [Page 27]

Internet-Draft public-names April 2021

This format may also provide the basis for a future OAUTH2 [RFC6749]

flow that could do the setup automatically.

The HNA needs to be configured with the following parameters as

described by this CDDL [RFC8610]. These are the parameters are

necessary to establish a secure channel between the HNA and the DM as

well as to specify the DNS zone that is in the scope of the

communication.

hna-configuration = {

"registered\_domain" : tstr,

"dm" : tstr,

? "dm\_transport" : "DoT"

? "dm\_port" : uint,

? "dm\_acl" : hna-acl / [ +hna-acl ]

? "hna\_auth\_method": hna-auth-method

? "hna\_certificate": tstr

}

hna-acl = tstr

hna-auth-method /= "certificate"

For example:

{

"registered\_domain" : "n8d234f.r.example.net",

"dm" : "2001:db8:1234:111:222::2",

"dm\_transport" : "DoT",

"dm\_port" : 4433,

"dm\_acl" : "2001:db8:1f15:62e:21c::/64"

or [ "2001:db8:1f15:62e:21c::/64", ... ]

"hna\_auth\_method" : "certificate",

"hna\_certificate" : "-----BEGIN CERTIFICATE-----\nMIIDTjCCFGy....",

}

14.1. Outsourced Information Model

Registered Homenet Domain (zone) The Domain Name of the zone.

Multiple Registered Homenet Domains may be provided. This will

generate the creation of multiple Public Homenet Zones. This

parameter is MANDATORY.

Distribution Master notification address (dm) The associated FQDNs

or IP addresses of the DM to which DNS notifies should be sent.

This parameter is MANDATORY. IP addresses are optional and the

FQDN is sufficient and preferred. If there are concerns about the

security of the name to IP translation, then DNSSEC should be

employed.

Migault, et al. Expires October 30, 2021 [Page 28]

Internet-Draft public-names April 2021

As the session between the HNA and the DM is authenticated with TLS,

the use of names is easier.

As certificates are more commonly emitted for FQDN than for IP

addresses, it is preferred to use names and authenticate the name of

the DM during the TLS session establishment.

Supported Transport (dm\_transport) The transport that carries the

DNS exchanges between the HNA and the DM. Typical value is "DoT"

but it may be extended in the future with "DoH", "DoQ" for

example. This parameter is OPTIONAL and by default the HNA uses

DoT.

Distribution Master Port (dm\_port) Indicates the port used by the

DM. This parameter is OPTIONAL and the default value is provided

by the Supported Transport. In the future, additional transport

may not have default port, in which case either a default port

needs to be defined or this parameter become MANDATORY.

Note that HNA does not defines ports for the Synchronization Channel.

In any case, this is not expected to part of the configuration, but

instead negotiated through the Configuration Channel. Currently the

Configuration Channel does not provide this, and limits its agility

to a dedicated IP address. If such agility is needed in the future,

additional exchanges will need to be defined.

Authentication Method ("hna\_auth\_method"): How the HNA authenticates

itself to the DM within the TLS connection(s). The authentication

meth of can typically be "certificate", "psk" or "none". This

Parameter is OPTIONAL and by default the Authentication Method is

"certificate".

Authentication data ("hna\_certificate", "hna\_key"): : The certificate

chain used to authenticate the HNA. This parameter is OPTIONAL and

when not specified, a self-signed certificate is used.

Distribution Master AXFR permission netmask (dm\_acl): The subnet

from which the CPE should accept SOA queries and AXFR requests. A

subnet is used in the case where the DNS Outsourced Infrastructure

consists of a number of different systems. An array of addresses

is permitted. This parameter is OPTIONAL and if unspecified, the

CPE the IP addresses specified in the dm\_notify parameters or the

IP addresses that result from the DNS(SEC) resolution when

dm\_notify specifies a FQDN.

For forward zones, the relationship between the HNA and the forward

zone provider may be the result of a number of transactions:

Migault, et al. Expires October 30, 2021 [Page 29]

Internet-Draft public-names April 2021

1. The forward zone outsourcing may be provided by the maker of the

Homenet router. In this case, the identity and authorization

could be built in the device at manufacturer provisioning time.

The device would need to be provisioned with a device-unique

credential, and it is likely that the Registered Homenet Domain

would be derived from a public attribute of the device, such as a

serial number (see Appendix B or

[I-D.richardson-homerouter-provisioning] for more details ).

2. The forward zone outsourcing may be provided by the Internet

Service Provider. In this case, the use of

[I-D.ietf-homenet-naming-architecture-dhc-options] to provide the

credentials is appropriate.

3. The forward zone may be outsourced to a third party, such as a

domain registrar. In this case, the use of the JSON-serialized

YANG data model described in this section is appropriate, as it

can easily be copy and pasted by the user, or downloaded as part

of a web transaction.

For reverse zones, the relationship is always with the upstream ISP

(although there may be more than one), and so

[I-D.ietf-homenet-naming-architecture-dhc-options] is always the

appropriate interface.

The following is an abbridged example of a set of data that

represents the needed configuration parameters for outsourcing.

15. IANA Considerations

This document has no actions for IANA.

16. 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

HNA 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, and Ray Bellis for their feedback on handling different

views as well as clarifying the impact of outsourcing the zone

signing operation outside the HNA; Mark Andrew and Peter Koch for

clarifying the renumbering.

Migault, et al. Expires October 30, 2021 [Page 30]

Internet-Draft public-names April 2021

17. Contributors

The co-authors would like to thank Chris Griffiths and Wouter

Cloetens that provided a significant contribution in the early

versions of the document.

18. References

18.1. Normative References

[I-D.ietf-dprive-xfr-over-tls]

Toorop, W., Dickinson, S., Sahib, S., Aras, P., and A.

Mankin, "DNS Zone Transfer-over-TLS", draft-ietf-dprive-

xfr-over-tls-11 (work in progress), April 2021.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities",

STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987,

<https://www.rfc-editor.org/info/rfc1034>.

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

DOI 10.17487/RFC1995, August 1996,

<https://www.rfc-editor.org/info/rfc1995>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", BCP 14, RFC 2119,

DOI 10.17487/RFC2119, March 1997,

<https://www.rfc-editor.org/info/rfc2119>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound,

"Dynamic Updates in the Domain Name System (DNS UPDATE)",

RFC 2136, DOI 10.17487/RFC2136, April 1997,

<https://www.rfc-editor.org/info/rfc2136>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S.

Rose, "Resource Records for the DNS Security Extensions",

RFC 4034, DOI 10.17487/RFC4034, March 2005,

<https://www.rfc-editor.org/info/rfc4034>.

[RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for

Renumbering an IPv6 Network without a Flag Day", RFC 4192,

DOI 10.17487/RFC4192, September 2005,

<https://www.rfc-editor.org/info/rfc4192>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the

Internet Protocol", RFC 4301, DOI 10.17487/RFC4301,

December 2005, <https://www.rfc-editor.org/info/rfc4301>.

Migault, et al. Expires October 30, 2021 [Page 31]

Internet-Draft public-names April 2021

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol

(MOBIKE)", RFC 4555, DOI 10.17487/RFC4555, June 2006,

<https://www.rfc-editor.org/info/rfc4555>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol",

RFC 4960, DOI 10.17487/RFC4960, September 2007,

<https://www.rfc-editor.org/info/rfc4960>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS

Security (DNSSEC) Hashed Authenticated Denial of

Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008,

<https://www.rfc-editor.org/info/rfc5155>.

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol

(AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010,

<https://www.rfc-editor.org/info/rfc5936>.

[RFC6092] Woodyatt, J., Ed., "Recommended Simple Security

Capabilities in Customer Premises Equipment (CPE) for

Providing Residential IPv6 Internet Service", RFC 6092,

DOI 10.17487/RFC6092, January 2011,

<https://www.rfc-editor.org/info/rfc6092>.

[RFC6644] Evans, D., Droms, R., and S. Jiang, "Rebind Capability in

DHCPv6 Reconfigure Messages", RFC 6644,

DOI 10.17487/RFC6644, July 2012,

<https://www.rfc-editor.org/info/rfc6644>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication

of Named Entities (DANE) Transport Layer Security (TLS)

Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August

2012, <https://www.rfc-editor.org/info/rfc6698>.

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

DOI 10.17487/RFC6762, February 2013,

<https://www.rfc-editor.org/info/rfc6762>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service

Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013,

<https://www.rfc-editor.org/info/rfc6763>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and

P. Selkirk, "Port Control Protocol (PCP)", RFC 6887,

DOI 10.17487/RFC6887, April 2013,

<https://www.rfc-editor.org/info/rfc6887>.

Migault, et al. Expires October 30, 2021 [Page 32]

Internet-Draft public-names April 2021

[RFC7010] Liu, B., Jiang, S., Carpenter, B., Venaas, S., and W.

George, "IPv6 Site Renumbering Gap Analysis", RFC 7010,

DOI 10.17487/RFC7010, September 2013,

<https://www.rfc-editor.org/info/rfc7010>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic

Requirements for IPv6 Customer Edge Routers", RFC 7084,

DOI 10.17487/RFC7084, November 2013,

<https://www.rfc-editor.org/info/rfc7084>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.

Kivinen, "Internet Key Exchange Protocol Version 2

(IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October

2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating

DNSSEC Delegation Trust Maintenance", RFC 7344,

DOI 10.17487/RFC7344, September 2014,

<https://www.rfc-editor.org/info/rfc7344>.

[RFC7368] Chown, T., Ed., Arkko, J., Brandt, A., Troan, O., and J.

Weil, "IPv6 Home Networking Architecture Principles",

RFC 7368, DOI 10.17487/RFC7368, October 2014,

<https://www.rfc-editor.org/info/rfc7368>.

[RFC7558] Lynn, K., Cheshire, S., Blanchet, M., and D. Migault,

"Requirements for Scalable DNS-Based Service Discovery

(DNS-SD) / Multicast DNS (mDNS) Extensions", RFC 7558,

DOI 10.17487/RFC7558, July 2015,

<https://www.rfc-editor.org/info/rfc7558>.

[RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6

Networks", RFC 7707, DOI 10.17487/RFC7707, March 2016,

<https://www.rfc-editor.org/info/rfc7707>.

[RFC7788] Stenberg, M., Barth, S., and P. Pfister, "Home Networking

Control Protocol", RFC 7788, DOI 10.17487/RFC7788, April

2016, <https://www.rfc-editor.org/info/rfc7788>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D.,

and P. Hoffman, "Specification for DNS over Transport

Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May

2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC

2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,

May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Migault, et al. Expires October 30, 2021 [Page 33]

Internet-Draft public-names April 2021

[RFC8375] Pfister, P. and T. Lemon, "Special-Use Domain

'home.arpa.'", RFC 8375, DOI 10.17487/RFC8375, May 2018,

<https://www.rfc-editor.org/info/rfc8375>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A.,

Richardson, M., Jiang, S., Lemon, T., and T. Winters,

"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)",

RFC 8415, DOI 10.17487/RFC8415, November 2018,

<https://www.rfc-editor.org/info/rfc8415>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol

Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018,

<https://www.rfc-editor.org/info/rfc8446>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J.

Kasten, "Automatic Certificate Management Environment

(ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019,

<https://www.rfc-editor.org/info/rfc8555>.

18.2. Informative 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-dprive-dnsoquic]

Huitema, C., Mankin, A., and S. Dickinson, "Specification

of DNS over Dedicated QUIC Connections", draft-ietf-

dprive-dnsoquic-02 (work in progress), February 2021.

[I-D.ietf-homenet-naming-architecture-dhc-options]

Migault, D., Weber, R., Mrugalski, T., Griffiths, C., and

W. Cloetens, "DHCPv6 Options for Home Network Naming

Authority", draft-ietf-homenet-naming-architecture-dhc-

options-11 (work in progress), April 2021.

[I-D.ietf-homenet-simple-naming]

Lemon, T., Migault, D., and S. Cheshire, "Homenet Naming

and Service Discovery Architecture", draft-ietf-homenet-

simple-naming-03 (work in progress), October 2018.

[I-D.richardson-homerouter-provisioning]

Richardson, M., "Provisioning Initial Device Identifiers

into Home Routers", draft-richardson-homerouter-

provisioning-00 (work in progress), November 2020.

Migault, et al. Expires October 30, 2021 [Page 34]

Internet-Draft public-names April 2021

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B.

Wellington, "Secret Key Transaction Authentication for DNS

(TSIG)", RFC 2845, DOI 10.17487/RFC2845, May 2000,

<https://www.rfc-editor.org/info/rfc2845>.

[RFC2931] Eastlake 3rd, D., "DNS Request and Transaction Signatures

( SIG(0)s )", RFC 2931, DOI 10.17487/RFC2931, September

2000, <https://www.rfc-editor.org/info/rfc2931>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework",

RFC 6749, DOI 10.17487/RFC6749, October 2012,

<https://www.rfc-editor.org/info/rfc6749>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram

Transport Layer Security (DTLS)", RFC 8094,

DOI 10.17487/RFC8094, February 2017,

<https://www.rfc-editor.org/info/rfc8094>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS

(DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018,

<https://www.rfc-editor.org/info/rfc8484>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data

Definition Language (CDDL): A Notational Convention to

Express Concise Binary Object Representation (CBOR) and

JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610,

June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC8672] Sheffer, Y. and D. Migault, "TLS Server Identity Pinning

with Tickets", RFC 8672, DOI 10.17487/RFC8672, October

2019, <https://www.rfc-editor.org/info/rfc8672>.

Migault, et al. Expires October 30, 2021 [Page 35]

Internet-Draft public-names April 2021

Appendix A. Envisioned deployment scenarios

A number of deployment have been envisioned, this section aims at

providing a brief description. The use cases are not limitations and

this section is not normative.

A.1. CPE Vendor

A specific vendor with specific relations with a registrar or a

registry may sell a CPE that is provisioned with provisioned domain

name. Such domain name does not need to be necessary human readable.

One possible way is that the vendor also provisions the HNA with a

private and public keys as well as a certificate. Note that these

keys are not expected to be used for DNSSEC signing. Instead these

keys are solely used by the HNA to proceed to the authentication.

Normally the keys should be necessary and sufficient to proceed to

the authentication. The reason to combine the domain name and the

key is that DOI are likely handle names better than keys and that

domain names might be used as a login which enables the key to be

regenerated.

When the home network owner plugs the CPE at home, the relation

between HNA and DM is expected to work out-of-the-box.

A.2. Agnostic CPE

An CPE that is not preconfigured may also take advantage to the

protocol defined in this document but some configuration steps will

be needed.

1. The owner of the home network buys a domain name to a registrar,

and as such creates an account on that registrar

2. Either the registrar is also providing the outsourcing

infrastructure or the home network needs to create a specific

account on the outsourcing infrastructure. \* If the DOI is the

registrar, it has by design a proof of ownership of the domain

name by the homenet owner. In this case, it is expected the DOI

provides the necessary parameters to the home network owner to

configure the HNA. A good way to provide the parameters would be

the home network be able to copy/paste a JSON object - see

Section 14. What matters at that point is the DOI being able to

generate authentication credentials for the HNA to authenticate

itself to the DOI. This obviously requires the home network to

provide the public key generated by the HNA in a CSR.

Migault, et al. Expires October 30, 2021 [Page 36]

Internet-Draft public-names April 2021

o If the DOI is not the registrar, then the proof of ownership needs

to be established using protocols like ACME [RFC8555] for example

that will end in the generation of a certificate. ACME is used

here to the purpose of automating the generation of the

certificate, the CA may be a specific CA or the DOI. With that

being done, the DOI has a roof of ownership and can proceed as

above.

Appendix B. Example: A manufacturer provisioned HNA product flow

This scenario is one where a homenet router device manufacturer

decides to offer DNS hosting as a value add.

[I-D.richardson-homerouter-provisioning] describes a process for a

home router credential provisioning system. The outline of it is

that near the end of the manufacturing process, as part of the

firmware loading, the manufacturer provisions a private key and

certificate into the device.

In addition to having a assymmetric credential known to the

manufacturer, the device also has been provisioned with an agreed

upon name. In the example in the above document, the name

"n8d234f.r.example.net" has already been allocated and confirmed with

the manufacturer.

The HNA can use the above domain for itself. It is not very pretty

or personal, but if the owner wishes a better name, they can arrange

for it.

The configuration would look like:

{

"dm\_notify" : "2001:db8:1234:111:222::2",

"dm\_acl" : "2001:db8:1234:111:222::/64",

"dm\_ctrl" : "manufacturer.example.net",

"dm\_port" : "4433",

"ns\_list" : [ "ns1.publicdns.example", "ns2.publicdns.example"],

"zone" : "n8d234f.r.example.net",

"auth\_method" : "certificate",

"hna\_certificate":"-----BEGIN CERTIFICATE-----\nMIIDTjCCFGy....",

}

The dm\_ctrl and dm\_port values would be built into the firmware.

Migault, et al. Expires October 30, 2021 [Page 37]

Internet-Draft public-names April 2021

Authors' Addresses

Daniel Migault

Ericsson

8275 Trans Canada Route

Saint Laurent, QC 4S 0B6

Canada

EMail: daniel.migault@ericsson.com

Ralf Weber

Nominum

2000 Seaport Blvd

Redwood City 94063

US

EMail: ralf.weber@nominum.com

Michael Richardson

Sandelman Software Works

470 Dawson Avenue

Ottawa, ON K1Z 5V7

Canada

EMail: mcr+ietf@sandelman.ca

Ray Hunter

Globis Consulting BV

Weegschaalstraat 3

Eindhoven 5632CW

NL

EMail: v6ops@globis.net

Migault, et al. Expires October 30, 2021 [Page 38]