Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 26, 2019

T. Lemon
Nibbhaya Consulting
D. Migault
Ericsson
S. Cheshire
Apple Inc.

October 23, 2018

Homenet Naming and Service Discovery Architecture
draft-ietf-homenet-simple-naming-03

Abstract

This document describes how names are published and resolved on homenets, and how hosts are configured to use these names to discover services on homenets. It presents the complete architecture, and describes a simple subset of that architecture that can be used in low-cost homenet routers.

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 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 April 26, 2019.

Table of Contents

1. Introduction

This document is a homenet architecture document. The term 'homenet' refers to a set of technologies that allow home network users to have a local-area network (LAN) with more than one physical link and, optionally, more than one internet service provider. Home network users are assumed not to be knowledgeable in network operations, so homenets automatically configure themselves, providing connectivity and service discovery within the home with no operator intervention. This document describes the aspect of homenet automatic configuration that has to do with service discovery and name resolution.

This architecture provides a minimal set of features required to enable seamless service discovery on a multi-link home network, but does not attempt to provide feature parity with a managed LAN.

This document begins by presenting a motivational list of requirements and considerations, which should give the reader a clear idea of the scope of the problem being solved. It then explains how each requirement is addressed, and provides references for relevant standards documents describing the details of the implementation. Not all requirements are addressed by this architecture document, but the basic requirements are satisfied, and this document serves as a foundation upon which solutions to the remaining problems can be built.

2. Requirements

Name service on a local area network (LAN) requires the following:

- Name: a forward domain under which information about local services will be published

- Authority: a name server that is authoritative for at least one forward domain and one or two reverse domains that are applicable to that network and is capable of signing and publishing the zones using DNSSEC

- Resolution: a full-service caching DNS resolver that fully supports EDNS(0) and queries with the DO bit set

- Publication: a mechanism that

    * allows services on the LAN to publish information about the services they provide

    * allows services to publish information on how to reach them

    * manages the lifetime of such information, so that it persists long enough to prevent spoofing, but protects end users from seeing stale information

- Host configuration: one or more automatic mechanisms (e.g. DHCP or RA) that provide:

    * caching resolver information to hosts on the LAN

    * information about how services on the LAN can publish information

- Trust: some basis for trusting the information that is provided by the service discovery system

2.1. Managed LAN versus Homenet

A managed network is one that has a (human) manager, or operator. The operator has authority over the network, and the authority to publish names in a forward DNS tree, and reverse names in the reverse tree. The operator has the authority to sign the respective trees with DNSSEC, and acquire TLS certificates for hosts/servers within the network.

On a managed LAN, many of these services can be provided by operators. When a new printer is added to the network, it can be added to the service discovery system (the authoritative server) manually. When a printer is taken out of service, it can be removed. In this scenario, the role of "publisher" is filled by the network operator.

In many managed LANs, establishment of trust for service discovery is simply on the basis of a belief that the local resolver will give a correct answer. Once the service has been discovered and chosen, there may be some security (e.g., TLS) that protects the connection to the service, but the trust model is often just "you're connected to a network you trust, so you can trust the printer that you discovered on this network."

A homenet does not have an operator, so functions that would normally be performed by the operator have to happen automatically. This has implications for trust establishment--since there is no operator

controlling what services are published locally, some other mechanism is required for basic trust establishment.

2.1.1. Multiple Provisioning Domains

Additionally, whereas in a managed LAN with multiple links to the Internet, the network operator can configure the network so that multihoming is handled seamlessly, in a homenet, multihoming must be handled using multiple provisioning domains [RFC7556].

When a host on a homenet connects to a host outside the homenet, and the homenet is multihomed, the source address that the host uses for connecting determines which upstream ISP connection is used. In principle, this is not a problem, because the Internet is a fully connected network, so any host that is on the Internet can be reached by any host on the Internet, regardless of how that host connects to the Internet.

Unfortunately in practice this is not always the case. Some ISPs provide special services to their end users that are only accessible when connected through the ISP. When such a service is discovered using that ISP's name server, a response will be provided that will only work if the host connects using a prefix provided by that ISP. If another ISP's prefix is used, the connection will fail.

In the case of content delivery networks (CDNs), using the name service of one ISP and then connecting through a second ISP may seem to work, but may provide very poor service.

In order to address this problem, the homenet naming architecture takes two approaches. First, for hosts that do not support provisioning domain separation, we make sure that all ISP name servers are consulted in such a way that Happy Eyeballs will tend to work. Second, for hosts that do support provisioning domain separation, we provide information to the hosts to identify provisioning domains, and we provide a mechanism that hosts can use to indicate which provisioning domain to use for a particular DNS query.

2.2. Homenet-specific considerations

A naming architecture for homenets therefore adds the following considerations:

- All of the operations mentioned here must reliably function automatically, without any user intervention or debugging.

- Because user intervention cannot be required, naming conflicts must be resolved automatically, and, to the extent possible, transparently.

- Devices that provide services must be able to publish those services on the homenet, and those services must be available from any part of the homenet, not just the link to which the device is attached.

- Homenets must address the problem of multiple provisioning domains, in the sense that the DNS may give a different answer depending on whether caching resolvers at one ISP or another are queried.

An additional requirement from the Homenet Architecture [RFC7556] is that hosts are not required to implement any homenet-specific capabilities in order to discover and access services on the homenet. This architecture may define optional homenet-specific features, but hosts that do not implement these features must work on homenets.

3. Terminology

This document uses the following terms and abbreviations:

HNR Homenet Router

SHNR Homenet Router implementing simple homenet naming architecture

AHNR Homenet Router implementing advanced homenet naming architecture

ISP Internet Service Provider

Forward Mapping A mapping between a host name or service name and some information about that host or service.

Reverse Mapping A mapping between an IP address and the host that has that IP address.

Homenet Domain A domain name that is used for publishing the names of devices and services that are present on the homenet. By default, 'home.arpa.'

4. Name

In order for names to be published on a homenet, it is necessary that there be a set of domain names under which such names are published. These domain names, together, are referred to as the "local domains."

By default, homenets publish names for forward lookups under the reserved domain 'home.arpa.' [RFC8375] publishing names.

So a host called 'example' that published its name on the homenet would publish its records on the domain name 'example.home.arpa.'. Because 'home.arpa.' is used by all homenets, it has no global meaning, and names published under the domain 'home.arpa' cannot be used outside of the homenet on which they are published.

How to publish names outside of the homenet is out of scope for this document. However, in order to address the problem of validating names published on the homenet using DNSSEC, it is necessary that the homenet have a globally valid delegation from the root. This allows hosts on the homenet to validate names published on the homenet using the DNS root trust anchor ([RFC4033] section 3.1).

It is not necessary that this delegation work for hosts off the homenet. HNRs implementing this specification do not answer queries from outside the homenet; however, when a validating resolver inside the homenet attempts to validate the chain of trust up to the root zone, the chain of trust will validate correctly, because the answer given for internally-available zones will be signed by a DS record that is present in the delegation externally.

If there is a valid delegation from the root, the homenet domain will be the name of the delegated domain. By default, there will be no delegation from the root; in this case, the homenet domainname will be 'home.arpa.'

In addition to the homenet domain, names are needed for reverse lookups. These names are dependent on the IP addressing used on the homenet. If the homenet is addressed with IPv4, a reverse domain corresponding to the IPv4 subnet [RFC1034] section 5.2.1 should be constructed. For example, if the homenet is allocating local IP addresses out of net 10 [RFC1918], a domain, '10.in-addr.arpa' would be required. Like 'home.arpa.', '10.in-addr.arpa' is a locally-served zone, and has no validity outside of the homenet.

If the homenet is addressed with IPv6, it is expected to have a unique local address prefix. The reverse mapping domain for hosts on any link in the subnet will be a subdomain of the reverse zone for the subset of the ULA prefix that is being advertised on that link. Every service on the homenet that supports IPv6 is expected to be reachable at an address that is configured using the ULA prefix. Therefore there is no need for any IPv6 reverse zone to be populated other than the ULA zone. So for example if the homenet's ULA prefix is fc00:2001:db8::/48, then the reverse domain name for the homenet would end in '8.b.d.0.1.0.0.2.0.0.d.f.ip6.arpa'.

5. Authority

There are two types of authoritative name service on the homenet. Every link on the homenet has a zone that is a subdomain of the homenet's primary domain. Authority for these zones is local to the HNR that is currently authoritative for that zone. The contents of these zones are served using DNSSD Discovery Proxy [I-D.ietf-dnssd-hybrid]. Consequently, there is no need for database replication in the case that a new HNR is elected; that HNR simply takes over the Discovery Relay function.

Name service for the homenet domain itself may be stateless or stateful. HNRs are not required to implement stateful service. If one or more HNRs on the homenet are capable of providing this service, then one of those HNRs is elected to act as the primary nameserver for the homenet domain; one or more HNRs may also act as secondary servers.

Name service for reverse mapping subdomains is only provided if one or more HNRs can provide stateful service. If no such server is present, the reverse mapping subdomains are not served. If stateful servers are present, the primary and secondary servers for these subdomains will be the same as for the homenet domain.

5.1. Reachability

Whether the homenet domain is a global domain name or not, HNRs answering queries for domains on the homenet do not respond to queries from off the homenet unless configured to do so. Exposing services on the homenet for browsing off the homenet creates many opportunities for security issues; as such, even an HNR configured to answer queries from prefixes off the homenet do not provide answers for names of devices on the homenet unless configured to do so. How reachability of names published on the homenet is managed is out of scope for this document: an HNR implementing only this document checks the source address of every query to see if it is within a prefix belonging to the homenet; if not, the HNR does not answer the query.

5.2. Link Names

Each link must have a name. These names are determined using HNCP. Each router will have zero or more wired links, each of which must be labeled. In addition, each router will have zero or more wireless links. Each of these links will be named by the frequency band the link supports, 2.4ghz or 5ghz.

The HNR is named using its manufacturer name. If, as is likely, two or more HNRs from the same manufacturer are present on a homenet, then the HNR name is made up of the manufacturer name plus as many hexadecimal digits as are required from the HNRs link layer addresses so as to disambiguate them.

When shipping multiple HNRs as a kit, manufacturers are advised to arrange that each HNR has a different number in the lowest four bits of the link-layer address. Manufacturers are also advised to print that link layer address, in full, somewhere on the outside of the HNR where it can be seen by the user. Since most HNRs will have more than one interface, the manufacturer should be consistent in choosing which link-layer address is printed on the outside and used to identify the router.

The name given to a link is the name of the HNR, plus a hyphen ('-'), plus name of the interface of that HNR that is attached to the link. In the event that this name must be displayed to the user, this should give the user enough information to figure out which link is being referenced. In the event that the HNR that is providing authoritative service for that link changes, the link name changes. This should only happen if the network topology changes.

If the appearance of a new HNR requires that the name of an existing HNR change, then the names of all the links managed by that existing HNR change to reflect the new name.

5.3. Authoritative name service for the homenet domain

All HNRs must be capable of providing authoritative name service for the homenet domain. HNRs that provide only stateless authoritative service publish the information that is required for hosts to do DNS Service Discovery over DNS, using the local resolver as a DNSSD Discovery Broker.

Some contents are required for the homenet domain, whether it is stateful or stateless.

- Every link on the homenet has a name that is a subdomain of the homenet domain. The zone associated with the homenet domain contains a delegation for each of these subdomains.

- In order for DNSSD service discovery to work, a default browsing domain must be published. The default browsing domain is simply the homenet domain.

- If DNSSD SRP is supported (that is, if stateful authoritative service is present), then an SRV record must be published, along

with a list of available registration zones containing exactly one entry, for the homenet domain ([I-D.sctl-service-registration] section 2).

- Also if DNSSD SRP is supported, then one or more A and/or AAAA records must be published under the name that the SRV record points to, which should be a single label subdomain of the homenet domain.

Both stateful and stateless authoritative servers provided by HNRs must support DNS Stateful Operations [I-D.ietf-dnsop-session-signal] and DNS Push [I-D.ietf-dnssd-push] for the names for which they are authoritative.

5.4. Authoritative name service for per-link subdomains of the homenet domain

Per-link subdomains of the homenet domain are served by DNSSD Discovery Proxies. Although these proxies generally do caching, no long-lived state is kept by them. DNSSD Discovery Proxies running on HNRs must support DNS Stateful Operations and DNS Push.

5.5. Authoritative name service for the ULA reverse mapping domain

The ULA reverse mapping domain itself is only published if stateful name service is available. It is represented as a single zone, which contains no delegations: every reverse mapping for an address in the ULA prefix is simply published in the ULA zone.

In order to permit registration of reverse mappings in this domain, it must contain an SRV record for the label _homenet-rrp._tcp at the top level, pointing to the primary server for the domain.

5.6. Authoritative name service for the RFC1918 reverse mapping domains

If IPv4 service is being provided on the homenet, and if stateful name service is being provided on the homenet, then either one or sixteen reverse mapping zones for the RFC1918 prefix in use must be provided. If more than one RFC1918 prefix is in use, reverse mapping zones for all such prefixes must be provided.

Like the ULA reverse mapping zone, the RFC1918 reverse mapping zones must each contain an SRV record on the label _homenet-rrp._tcp at the top level, pointing to the name of the primary server for the zone.

The RFC1918 reverse mapping zone contains the entire address space of the RFC1918 prefix that is in use on the homenet. Section 3 of RFC1918 defines three prefixes that may be used. The homenet will

use all of one of these three prefixes. Of these, the 172.16.0.0 prefix is subdivided on a 12-bit boundary, and therefore must be represented as 16 separate zones. The 10.0.0.0/8 and 192.168.0.0/16 prefixes are each represented as a single zone.

The zone to be updated is therefore the 10.in-addr.arpa zone for all addresses in 10.0.0.0/8, and the 168.192.in-addr.arpa zone for all addresses in 192.168.0.0/16. For addresses in the 172.16.0.0/12 prefix, the zone to be updated is the subdomain of 172.in-addr.arpa that corresponds to bits 8-11 of the prefix: a number between 16 and 31, inclusive.

Also like the ULA zone, the RFC1918 reverse mapping zones contain no delegations: if there is a single zone, then every reverse mapping published for an address in the RFC1918 prefix in use on the homenet is published directly under this zone. If there are sixteen zones, each address is published in its respective zone. Because the zone 172.in-addr.arpa is not available to be served locally, its locally served subdomains are simply served individually with no delegation.

6. Resolution

Name resolution on the homenet must accomplish two tasks: resolving names that are published on the homenet, and resolving names that are published elsewhere. This is accomplished by providing several functional layers.

1. The set of caching nameservers provided by the ISP or ISPs through which the homenet gains access to the global internet, if any (homenets can operate standalone as well).

2. The set of stateful name servers on the homenet that are authoritative for the homenet domain as a whole, and for any reverse mapping zones that are provided by the homenet. This layer is optional, and may or may not be present. If present, it is provided by one or more HNRs on the homenet that support stateful service.

3. The set of stateless name servers on the homenet that are authoritative for the homenet domain as a whole. These are not used if one or more stateful servers are present.

4. The set of stateless DNSSD Discovery Proxies that are authoritative for each of the links in the homenet.

5. A DNS routing proxy. Hereafter we refer to this as the DNS proxy.

The reason that these are described as layers is that it's quite possible that all of the DNS services on the homenet might be provided by a single service listening on port 53; how the request is routed then depends on the question being asked. So the services described as running on HNRs are treated as functional blocks which may be connected internally, if the question being asked can be answered directly by the HNR that received it, or they may be separate name servers running on different HNRs, if the question can be answered within the homenet, or it may be that the HNR receiving the query forwards it to an ISP caching name server.

The routing works as follows. When a request is received (opcode=0, Q/R=0), the DNS proxy looks at the owner name in the question part of the message.

- If the name is a subdomain of the homenet domain, the query is local.
- If the name is a subdomain of a locally-valid ULA reverse mapping domain, the query is local.
- If the name is a subdomain of a locally valid RFC1918 reverse mapping zone, the query is local.
- If the name is a subdomain of any locally-served zone, as defined in Locally Served DNS Zones [localzones], but is not otherwise identified as local, the response is NXDOMAIN.
- Otherwise, the query is not local.

Local queries are further divided. If the query is for a link subdomain, the DNS proxy consults the table that maps per-link subdomains to the HNRs that serve them. Either the HNR that serves this link subdomain is the HNR that received the question, or not. If it is, then the DNS proxy passes the query directly to the local DNSSD Discovery Proxy. Otherwise, it forwards the query to the DNSSD Discovery Proxy on the HNR that is providing Discovery Proxy service for that link.

If the query is for the homenet subdomain, and stateful authoritative service for the homenet subdomain is present on the homenet, then either the HNR receiving the query provides stateful authoritative service, or not. If it does, then the query is passed directly to the local authoritative server. If not, then the HNR looks in the table of authoritative servers generated by HNCP and forwards the request to one of these servers. Queries for the reverse mapping zones are handled the same way.

Otherwise, the query is examined to see if it contains an EDNS(0) Provisioning Domain option. If not, it round-robined across the resolvers provided by each ISP in such a way that each ISP is tried in succession, and the same ISP is not asked the same question repeatedly. If the query does contain the EDNS(0) Provisioning Domain option, then that option is used to select which ISP's resolvers are used for the round robin.

6.1. Round Robining

There are several cases above where there may be a choice of servers to which to forward queries. It's assumed that when the query can be satisfied by the HNR that received it, round robining is not required. If there is a specific HNR that is responsible for a particular link, then round robining is likewise not required. However, if the query is for a stateful authoritative server, and the HNR that received it does not provide this service, and there is more than one HNR on the homenet that does provide the service, the HNR that received the query round robins it across the available set of HNRs that could answer it.

Similarly, if the query is to be sent to an ISP's resolver, and the ISP has provided more than one resolver, round robining is done across the set of resolvers provided by that ISP. If the query is to be attempted at every ISP, then that is accomplished by round-robining in such a way that each ISP is tried in succession, rather than all the resolvers at one ISP, and then all the resolvers at the next ISP, and so on.

6.2. Retransmission

For queries that can't be resolved locally by the HNR that received them, retransmission as described in [RFC1035] is performed.

6.3. DNS Stateful Operations and DNS Push

DNS proxies on HNRs are required to support DNS Stateful Operations and DNS Push. When a DNS Push operation is requested on a name that can be satisfied by the HNR that received it, it is handled locally. When such an operation is requested on a name that is local to the homenet, but can't be satisfied by the HNR that received it, a DNS Stateful operation is started with the HNR that is responsible for it.

6.4. Multicast DNS

In addition to consulting the local resolver, hosts on the homenet may attempt to discover services directly using Multicast DNS. HNRs may filter out incoming Multicast DNS queries, forcing the client to do service discovery using the DNS protocol. If such filtering is not done, the client will be able to discover services on the link to which it is attached, but will not be able to discover services elsewhere.

It is believed that all currently-available hosts support DNSSD using the DNS protocol. Support for mDNS on the local link is therefore not required. However, if an mDNS query returns the same answer as the DNS protocol query, this is not expected to be a problem.

6.5. Host behavior

Hosts that support the RA Provisioning Domain option direct queries to the name server(s) of the provisioning domain they will use for communication using the EDNS(0) provisioning domain option. In practice this means that a host that supports PvDs will keep a set of provisioning information for each prefix that it received from the router, and will either choose a prefix to use based on its own criteria, or will attempt to connect using every PvD at once or in sequence. Answers to queries sent for a particular provisioning domain will only be used with source addresses for prefixes that are in that provisioning domain.

7. Publication

Names are published either using Multicast DNS Service Discovery [RFC6762] or DNSSD Service Registration Protocol ([I-D.sctl-service-registration]). Reverse mappings are published using Homenet Reverse Mapping Update Protocol Section 7.2.

7.1. DNSSD Service Registration Protocol

HNRs that provide stateful authoritative service also publish information acquired using DNSSD Service Registration Protocol [I-D.sctl-service-registration]. DNSSD SRP does not explicitly support population of the reverse zone; hosts that wish to provide reverse mapping information must first establish their hostname using DNSSD SRP; once established, the key used to authenticate the DNSSD SRP update is also used to update the reverse name.

Support for SRP provides several advantages over DNSSD Discovery Proxy. First, DNSSD SRP provides a secure way of claiming service names. Second, a claimed name is valid for the entire network

covered by the SRP service, not just an individual link, as is the case with mDNS. Third, SRP does not use multicast, and is therefore more reliable on links with constrained multicast support [I-D.ietf-mboned-ieee802-mcast-problems].

Support for the DNSSD SRP service is not sufficient to achieve full deployment of DNSSD SRP: it is also necessary that services advertise using DNSSD SRP. Requiring such support is out of scope for this document; our goal is simply to specify a way in which DNSSD SRP can be supported on homenets, so that that as adoption of SRP increases on devices providing service, it can actually be used.

7.2. Homenet Reverse Mapping Update Protocol

This is an extension to the DNSSD Service Registration protocol. The purpose is to allow for updates of reverse mappings. Hosts wishing to publish reverse mappings first publish their hostname using DNSSD SRP. When this process has successfully completed, the host can add reverse mappings to the ULA reverse mapping domain and to the RFC1918 reverse mapping domain, if present.

7.2.1. Adding ULA reverse mappings

The host first determines the ULA prefix. If there is more than one ULA prefix active, the ULA prefix with the longest preferred lifetime is used. A ULA prefix can be identified because it matches the prefix fc00::/7 ([RFC4193] section 3.1). The actual prefix is then the first 48 bits of the advertised prefix or the IP address in that prefix.

Because the ULA reverse mapping zone contains no delegations, all updates go to that one zone. To determine where to send the updates, the host first queries the SRV record under the label _homenet-rrp._tcp at the top of the ULA reverse mapping zone. It then uses the name contained in the SRV record to look up A and/or AAAA records to which to send the update.

The update is then signed using SIG(0) with the key that was used for the DNSSD SRP registration. The update is then sent using DNS Update [RFC2136] to one of the IP addresses received during the A/AAAA resolution step. The update is sent using TCP; if a TCP connection to one of the addresses fails, each subsequent address is tried in succession; if none of the addresses is reachable, the update fails, and may be retried after a reasonable period (on the order of an hour) has elapsed.

7.2.2. Adding RFC1918 reverse mappings

RFC1918 reverse mapping updates use the same mechanism as ULA reverse mapping updates. The host must first determine which zone to update, as described earlier in Section 5.6. Once the zone has been determined, the reverse mapping is updated as described in Section 7.2.1.

8. Host Configuration

Each HNR provides a Homenet DNS Proxy. When an HNR provides the DNS resolver IP address to hosts on the link using RA, DHCPv4 or DHCPv6, it provides its own address. The IPv4 address that it provides is a valid IPv4 address on the link to which the host is attached. The IPv6 address it provides is an address in the homenet's ULA prefix that is valid on the link to which the host is attached.

When sending router advertisements, the homenet includes the PvD ID RA option [I-D.ietf-intarea-provisioning-domains] in each RA. Because the PvD ID RA option can only be sent once per RA message, if the homenet is connected to more than one ISP, the prefixes for each ISP must be advertised in different RA options. In this case, the prefix for the ULA should also be sent in a separate RA.

If the configuration received from the ISP includes a Domain Name (DHCPv4) or Domain Search List (DHCPv4 or DHCPv6) option, the domain name provided is used to identify the PvD. In the case of Domain Search List options, if there is more than one, the first one is used. For the ULA prefix, the homenet domain is used to identify the PvD.

In order to facilitate DNSSD bootstrapping, any DHCPv4, DHCPv6 or RA Domain Search List options contain only a single domain name, the homenet domain. This allows hosts to quickly bootstrap DNS Service Discovery using the local domain name, as descried in [RFC6763] section 11.

9. Globally Unique Names

Homenets are not required to have globally unique names. Homenets operating according to this specification do not publish names in such a way that they can be resolved by hosts that aren't on the homenet. However, such names are useful for DNSSEC validation.

There are three ways that homenets can get global names:

1. They can be manually configured by the user. How this is done is out of scope for this document.

2. They can publish a delegation with the ISP, using a Homenet Delegation Registration Protocol Section 11.

3. They can publish a delegation with some other provider, using Homenet Delegation Registration Protocol Section 11. How this is configured is out of scope for this document.

Homenets are also not required to support global delegations for reverse mapping of global IPv4 and IPv6 addresses. How this would be done is out of scope for this document.

10. DNSSEC Validation

DNSSEC validation for 'home.arpa' requires installing a per-homenet trust anchor on the host, and is therefore not practical. Validation for locally-served reverse zones for the ULA and RFC1918 addresses would likewise require a trust anchor to be installed on the host, and likewise are not practical.

If DNSSEC validation is to be done for the homenet, the homenet must acquire a global name, and must be provided with a secure delegation. Secure delegations must also be provided from the homenet domain to each of the per-link subdomains.

Each HNR on a homenet generates its own private/public key pair that can serve as a trust anchor. These keys are shared using HNCP [RFC7788]. HNRs MUST NOT use pre-installed keys: each HNR MUST generate its own key. The HNR responsible for authoritative Discovery Proxy service on a particular link signs the zone for that link; delegations from the homenet domain zone to each per-link subdomain zone include a DS record signed by the ZSK of the homenet zone.

10.1. How trust is established

Every HNR has its own public/private key pair. A DS record for each such public key is published in the delegation for the homenet domain. If stateless authoritative service for the homenet zone is being provided, then each HNR signs its own homenet zone. The signed zone should be very stable, although the delegations may change when the network topology changes. The HNR can therefore sign the zone using its private key whenever it changes. Each HNR will have a copy of the zone signed with a different key, but since all of the ZSKs are present in the DS RRset at the delegation point, validation will succeed.

If stateful authoritative service is being provided, the HNR that is acting as primary signs the zone, and all the secondaries serve

copies acquired using zone transfers. If the HNR that is primary goes away, then a secondary becomes primary and signs the zone before beginning to provide service. Again, since all of the HNR's public keys exist in the DS RRset at the delegation, the zone can be validated.

11. Homenet Delegation Registration Protocol

Homenet Delegation Registration Protocol (HDeRP) operates similarly to DNSSD Service Registration Protocol. When a homenet is not connected to an ISP that supports HDeRP, and then an ISP connection becomes available, the HNR that is connected to the ISP determines whether HDeRP is available. This is done by first determining the ISP domain.

If the connection to the ISP is IPv4-only, this will be either the DHCPv4 Domain Name option or, if not present, the only domain name in the DHCPv4 Domain Name Search List option. If the Domain Name Search List option contains more than one name, HDeRP is not supported by the ISP.

If the connection to the ISP is dual-stack or IPv6-only, then the DHCPv6 Domain Search List option obtained through DHCPv6 Prefix Delegation is used. If it is not present, or if it contains more than one domain name, HDeRP is not supported by the ISP.

Once the ISP domain has been discovered, the HNR looks for an SRV record owned by the name _homenet-derp._tcp under the ISP domain. If this is not present, HDeRP is not supported. If the SRV record is present, then the HNR looks for A and AAAA records on the hostname provided in the HNR. If present, these are used when attempting the update.

The HNR then constructs a DNS update. The DNS update creates a delegation for the zone home.arpa, with a DS record for each HNR on the homenet, containing that HNR's public key. The HNR doing the update lists its key as the first key in the DS RRset. The update is signed using SIG(0) with the private key of the HNR that is constructing it. As with DNSSD SRP, the update includes an Update Lease EDNS(0) option, specifying a key lifetime of a week.

The HNR then attempts to connect to the hostname provided in the SRV record, in a round-robin fashion across the set of IP addresses discovered during the A/AAAA lookup phase. When it has successfully connected, it sends the DNS update.

The HDeRP server validates the update by checking the SIG(0) signature of the update against the first key in the DS RRset. If

the update is successfully validated, then the server generates a domain name and sends a reply back to the HNR on the same TCP connection, including the NOERROR (0) RCODE, and including in the query section the actual domain name that was generated.

This domain name then becomes the homenet name. Subsequent updates use the homenet name rather than 'home.arpa'. It is not necessary that the same HNR do the update; if a different HNR does the update, it lists its public key first in the DS RRset, and signs the update using its private key.

The HDeRP is responsible for removing the delegation if it is not refreshed for the length of its lifetime. HNRs should attempt to refresh the delegation when half the lifetime has experienced, then again at 5/8ths, and again at 7/8ths of the lifetime. If the ISP becomes unavailable, and a different ISP becomes available that supports HDeRP, the homenet should migrate to the new ISP.

12. Using the Local Namespace While Away From Home

This document does not specify a way for service discovery to be performed on the homenet by devices that are not directly connected to a link that is part of the homenet.

13. Expected Host Behavior

It is expected that hosts will fall into one of two categories: hosts that are able to discover DNS-SD browsing domains, and hosts that are not. Hosts that can discover DNS-SD browsing domains can be expected to successfully use service discovery across the entire homenet. Hosts that do not will only be able to discover services on the particular local subnet of the homenet to which they happen to be attached at any given time.

This is not considered to be a problem, since it is understood by the authors that the vast majority of hosts that are capable of doing mDNS discovery are also capable of doing DNS-SD discovery as described in [RFC6763].

14. Management Considerations

This architecture is intended to be self-healing, and should not require management. That said, a great deal of debugging and management can be done simply using the DNS Service Discovery protocol.

15. Privacy Considerations

Privacy is somewhat protected in the sense that names published on the homenet are only visible to devices connected to the homenet. This may be insufficient privacy in some cases.

The privacy of host information on the homenet is left to hosts. Various mechanisms are available to hosts to ensure that tracking does not occur if it is not desired. However, devices that need to have special permission to manage the homenet will inevitably reveal something about themselves when doing so.

16. Security Considerations

There are some clear issues with the security model described in this document, which will be documented in a future version of this section. A full analysis of the avenues of attack for the security model presented here have not yet been done, and must be done before the document is published.

17. IANA considerations

17.1. Homenet Reverse Registration Protocol

IANA is requested to add a new entry to the Service Names and Port Numbers registry for homenet-rrp with a transport type of tcp. No port number is to be assigned. The reference should be to this document, and the Assignee and Contact information should reference the authors of this document. The Description should be as follows:

Availability of Homenet Reverse Registration Protocol service for a given domain is advertised using an SRV record with an owner name of "_homenet-rrp._tcp.<domain>." in that domain, which gives the target host and port where Homenet Reverse Registration service is provided for the named domain.

17.2. Homenet Delegation Registration Protocol

IANA is requested to add a new entry to the Service Names and Port Numbers registry for homenet-derp with a transport type of tcp. No port number is to be assigned. The reference should be to this document, and the Assignee and Contact information should reference the authors of this document. The Description should be as follows:

Availability of Homenet Delegation Registration Protocol service for a given domain is advertised using an SRV record with an owner name of "_homenet-derp._tcp.<domain>." in that domain, which gives the

target host and port where Homenet Delegation Registration service is provided for the named domain.

17.3. Unique Local Address Reserved Documentation Prefix

IANA is requested to add an entry to the IPv6 Special-Purpose Address Registry for the prefix fc00:2001:db8::/48. The Name shall be "Unique Local Address Documentation Prefix." The reference RFC will be this document, once published. The date will be the date the entry was added. All other fields will be the same as for the Documentation prefix, 2001:db8::/32.

18. References

18.1. Normative References

[I-D.ietf-dnsop-session-signal]
Bellis, R., Cheshire, S., Dickinson, J., Dickinson, S., Lemon, T., and T. Pusateri, "DNS Stateful Operations", draft-ietf-dnsop-session-signal-16 (work in progress), September 2018.

[I-D.ietf-dnssd-hybrid]
Cheshire, S., "Discovery Proxy for Multicast DNS-Based Service Discovery", draft-ietf-dnssd-hybrid-08 (work in progress), March 2018.

[I-D.ietf-dnssd-push]
Pusateri, T. and S. Cheshire, "DNS Push Notifications", draft-ietf-dnssd-push-15 (work in progress), September 2018.

[I-D.ietf-intarea-provisioning-domains]
Pfister, P., Vyncke, E., Pauly, T., Schinazi, D., and W. Shao, "Discovering Provisioning Domain Names and Data", draft-ietf-intarea-provisioning-domains-03 (work in progress), October 2018.

[I-D.sctl-service-registration]
Cheshire, S. and T. Lemon, "Service Registration Protocol for DNS-Based Service Discovery", draft-sctl-service-registration-02 (work in progress), July 2018.

[localzones]
Internet Assigned Numbers Authority, "Locally-Served DNS Zones", n.d., <https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xhtml>.

[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>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[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>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[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>.

[RFC7336] Peterson, L., Davie, B., and R. van Brandenburg, Ed., "Framework for Content Distribution Network Interconnection (CDNI)", RFC 7336, DOI 10.17487/RFC7336, August 2014, <https://www.rfc-editor.org/info/rfc7336>.

[RFC7556] Anipko, D., Ed., "Multiple Provisioning Domain Architecture", RFC 7556, DOI 10.17487/RFC7556, June 2015, <https://www.rfc-editor.org/info/rfc7556>.

[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>.

[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>.

18.2. Informative References

[I-D.ietf-mboned-ieee802-mcast-problems] Perkins, C., McBride, M., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-ietf-mboned-ieee802-mcast-problems-02 (work in progress), August 2018.

Authors' Addresses

Ted Lemon
Nibbhaya Consulting
P.O. Box 958
Brattleboro, Vermont 05301
United States of America

Email: mellon@fugue.com

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

Email: daniel.migault@ericsson.com

Stuart Cheshire
Apple Inc.
1 Infinite Loop
Cupertino, California 95014
USA

Phone: +1 408 974 3207
Email: cheshire@apple.com