Network Working Group
Internet-Draft
Updates: RFC7788 (if approved)
Intended status: Standards Track
Expires: March 5, 2018

P. Pfister
Cisco Systems
T. Lemon
Nominum, Inc.

September 1, 2017

# Special Use Domain 'home.arpa.' draft-ietf-homenet-dot-14

## Abstract

This document specifies the behavior that is expected from the Domain Name System with regard to DNS queries for names ending with '.home.arpa.', and designates this domain as a special-use domain name. 'home.arpa.' is designated for non-unique use in residential home networks. Home Networking Control Protocol (HNCP) is updated to use the 'home.arpa.' domain instead of '.home'.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 5, 2018.

## Copyright Notice

Table of Contents



## 1. Introduction

Users and devices within a home network (hereafter "homenet") require devices and services to be identified by names that are unique within the boundaries of the homenet [RFC7368]. The naming mechanism needs to function without configuration from the user. While it may be possible for a name to be delegated by an ISP, homenets must also function in the absence of such a delegation. This document reserves the name 'home.arpa.' to serve as the default name for this purpose, with with a scope limited to each individual homenet.

This document corrects an error in [RFC7788], replacing '.home' with 'home.arpa.' as the default domain-name for homenets. '.home' had been selected as the most user-friendly option. However, there are existing uses of '.home' that may be in conflict with this use: evidence indicates that '.home' queries frequently leak out and reach the root name servers [ICANN1] [ICANN2].

In addition, it's necessary, for compatibility with DNSSEC (Section 6), that an insecure delegation ([RFC4035] section 4.3) be present for the name. There is an existing process for allocating names under '.arpa.' [RFC3172]. No such process is available for requesting a similar delegation in the root at the request of the IETF, which does not administer that zone. As a result, all unregistered uses of '.home' (that is, all current uses at the time

of this document's publication), particularly as specified in RFC7788, are deprecated.

This document registers the domain 'home.arpa.' as a special-use domain name [RFC6761] and specifies the behavior that is expected from the Domain Name System with regard to DNS queries for names whose rightmost non-terminal labels are 'home.arpa.'. Queries for names ending with '.home.arpa.' are of local significance within the scope of a homenet, meaning that identical queries will result in different results from one homenet to another. In other words, a name ending in '.home.arpa.' is not globally unique.

Although this document makes specific reference to RFC7788, it is not intended that the use of 'home.arpa.' be restricted solely to networks where HNCP is deployed; it is rather the case that 'home.arpa.' is the correct domain for uses like the one described for '.home' in RFC7788: local name service in residential homenets.

## 2. Requirements Language

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.

## 3. General Guidance

The domain name 'home.arpa.' is to be used for naming within residential homenets. Names ending with '.home.arpa.' reference a locally-served zone, the contents of which are unique only to a particular homenet, and are not globally unique. Such names refer to nodes and/or services that are located within a homenet (e.g., a printer, or a toaster).

DNS queries for names ending with '.home.arpa.' are resolved using local resolvers on the homenet. Such queries MUST NOT be recursively forwarded to servers outside the logical boundaries of the homenet.

Some service discovery user interfaces that are expected to be used on homenets conceal information such as domain names from end users. However, it is still expected that in some cases, users will need to see, remember, and even type, names ending with '.home.arpa.'. The working group hopes that this name will in some way indicate to as many readers as possible that such domain names are referring to devices in the home, but we recognize that it is an imperfect solution.

## 4. Domain Name Reservation Considerations

This section specifies considerations for systems involved in domain name resolution when resolving queries for names ending with '.home.arpa.'. Each item in this section addresses some aspect of the DNS or the process of resolving domain names that would be affected by this special use allocation. Detailed explanations of these items can be found in [RFC6761], Section 5.

1. Users can use names ending with '.home.arpa.' just as they would use any other domain name. The 'home.arpa.' name is chosen to be readily recognized by users as signifying that the name is addressing a service on the homenet to which the user's device is connected.

2. Application software SHOULD NOT treat names ending in '.home.arpa.' differently than other names. In particular, there is no basis for trusting names that are subdomains of 'home.arpa.' (see Section 6).

3. Name resolution APIs and libraries MUST NOT recognize names that end in '.home.arpa.' as special and MUST NOT treat them as having special significance, except that it may be necessary that such APIs not bypass the locally configured recursive resolvers.

   One or more IP addresses for recursive DNS servers will usually be supplied to the client through router advertisements or DHCP. For an administrative domain that uses subdomains of 'home.arpa.', such as a homenet, the recursive resolvers provided by that domain will be able to answer queries for subdomains of 'home.arpa.'; other resolvers will not, or will provide answers that are not correct within that administrative domain.

   A host that is configured to use a resolver other than one that has been provided by the local network may be unable to resolve, or may receive incorrect results for, subdomains of 'home.arpa.'. In order to avoid this, it is permissible that hosts use the locally-provided resolvers for resolving 'home.arpa.' even when they are configured to use other resolvers.

4.

   A. Recursive resolvers at sites using 'home.arpa.' MUST transparently support DNSSEC queries: queries for DNSSEC records and queries with the DO bit set ([RFC4035] section 3.2.1). While validation is not required, it is strongly encouraged: a caching recursive resolver that does not validate answers that can be validated may cache invalid

data. This in turn will prevent validating stub resolvers from successfully validating answers.

B. Unless configured otherwise, recursive resolvers and DNS proxies MUST behave as described in Locally Served Zones ([RFC6303] Section 3). That is, queries for 'home.arpa.' and subdomains of 'home.arpa.' MUST NOT be forwarded, with one important exception: a query for a DS record with the DO bit set MUST return the correct answer for that question, including correct information in the authority section that proves that the record is nonexistent.

So for example a query for the NS record for 'home.arpa.' MUST NOT result in that query being forwarded to an upstream cache nor to the authoritative DNS server for '.arpa.'. However, as necessary to provide accurate authority information, a query for the DS record MUST result in whatever queries are necessary being forwarded; typically, this will just be a query for the DS record, since the necessary authority information will be included in the authority section of the response if the DO bit is set.

C. In addition to the behavior specified above, recursive resolvers that can be used in a homenet MUST be configurable to forward queries for 'home.arpa.' and subdomains of 'home.arpa.' to an authoritative server for 'home.arpa.'. This server will provide authoritative data for 'home.arpa.' within a particular homenet. The special handling for DS records for the 'home.arpa.' delegation is still required.

It is permissible to combine the recursive resolver function for general DNS lookups with an authoritative resolver for 'home.arpa.'; in this case, rather than forwarding queries for subdomains of 'home.arpa.' to an authoritative server, the resolver answers them authoritatively. The behavior with respect to forwarding queries specifically for 'home.arpa.' remains the same.

5. No special processing of 'home.arpa.' is required for authoritative DNS server implementations. It is possible that an authoritative DNS server might attempt to check the authoritative servers for 'home.arpa.' for a delegation beneath that name before answering authoritatively for such a delegated name. In such a case, because the name always has only local significance there will be no such delegation in the 'home.arpa.' zone, and so the server would refuse to answer authoritatively for such a zone. A server that implements this sort of check MUST be

configurable so that either it does not do this check for the ’home.arpa.’ domain, or it ignores the results of the check.

6. DNS server operators MAY configure an authoritative server for ’home.arpa.’ for use in homenets and other home networks. The operator for the DNS servers authoritative for ’home.arpa.’ in the global DNS will configure any such servers as described in Section 7.

7. ’home.arpa.’ is a subdomain of the ’arpa’ top-level domain, which is operated by IANA under the authority of the Internet Architecture Board according to the rules established in [RFC3172]. There are no other registrars for .arpa.

## 5. Updates to Home Networking Control Protocol

The final paragraph of Home Networking Control Protocol [RFC7788], section 8, is updated as follows:

OLD:

> Names and unqualified zones are used in an HNCP network to provide naming and service discovery with local significance. A network-wide zone is appended to all single labels or unqualified zones in order to qualify them. ".home" is the default; however, an administrator MAY configure the announcement of a Domain-Name TLV (Section 10.6) for the network to use a different one. In case multiple are announced, the domain of the node with the greatest node identifier takes precedence.

NEW:

> Names and unqualified zones are used in an HNCP network to provide naming and service discovery with local significance. A network-wide zone is appended to all single labels or unqualified zones in order to qualify them. ’home.arpa.’ is the default; however, an administrator MAY configure the announcement of a Domain-Name TLV (Section 10.6) for the network to use a different one. In case multiple are announced, the domain of the node with the greatest node identifier takes precedence.
>
> The ’home.arpa.’ special-use name does not require a special resolution protocol. Names for which the rightmost two labels are ’home.arpa.’ are resolved using the DNS protocol [RFC1035].

## 6. Security Considerations

### 6.1. Local Significance

A DNS record that is returned as a response to a query for an FQDN that is a subdomain of 'home.arpa.' is expected to have local significance. It is expected to be returned by a server involved in name resolution for the homenet the device is connected in. However, such response MUST NOT be considered more trustworthy than would be a similar response for any other DNS query.

Because 'home.arpa.' is not globally scoped and cannot be secured using DNSSEC based on the root domain's trust anchor, there is no way to tell, using a standard DNS query, in which homenet scope an answer belongs. Consequently, users may experience surprising results with such names when roaming to different homenets.

To prevent this from happening, it could be useful for the resolver on the host to securely differentiate between different homenets, and between identical names on different homenets. However, a mechanism for doing this has not yet been standardized, and doing so is out of scope for this document. It is expected that this will be explored in future work.

Locally Served Zones ([RFC6303] section 7) recommends installing trust anchors for locally served zones. However, in order for this to be effective, there must be some way of configuring the trust anchor in the host. Homenet currently specifies no mechanism for configuring such trust anchors. As a result, while this advice sounds good, it is not practicable.

Also, although in principle it might be useful to install a trust anchor for a particular instance of 'home.arpa.', it's reasonable to expect that a host with such a trust anchor might from time to time connect to more than one network with its own instance of 'home.arpa.'. Such a host would be unable to access services on any instance of 'home.arpa.' other than the one for which a trust anchor was configured.

It is in principle possible to attach an identifier to an instance of 'home.arpa.' that could be used to identify which trust anchor to rely on for validating names in that particular instance. However, the security implications of this are complicated, and such a mechanism, as well as a discussion of those implications, is out of scope for this document.

### 6.2. Insecure Delegation

It is not possible to install a trust anchor (a DS RR) for this zone in the '.arpa' zone. The reason for this is that in order to do so, it would be necessary to have the key-signing key for the zone ([RFC4034] Section 5). Since the zone is not globally unique, no one key would work.

An alternative would be to provide a authenticated denial of existence ([RFC4033] Section 3.2). This would be done simply by not having a delegation from the 'arpa.' zone. However, this requires the validating resolver to treat 'home.arpa.' specially. If a validating resolver that doesn't treat 'home.arpa.' specially attempts to validate a name in 'home.arpa.', an authenticated denial of existence of 'home' as a subdomain of 'arpa.' would cause the validation to fail. Therefore, the only delegation that will allow names under 'home.arpa.' to be resolved by all validating resolvers is an insecure delegation as in [RFC6303] section 7.

Consequently, unless a trust anchor for the particular instance of the 'home.arpa.' zone being validated is manually configured on the validating resolver, DNSSEC signing and validation of names within the 'home.arpa.' zone is not possible.

### 6.3. Bypassing Manually Configured Resolvers

In Section 4, item 3, an exception is made to the behavior of stub resolvers allowing them to query local resolvers for subdomains of 'home.arpa.' even when they have been manually configured to use other resolvers. This behavior obviously has security and privacy implications, and may not be desirable depending on the context. It may be better to simply ignore this exception and, when one or more recursive resolvers are configured manually, simply fail to provide correct answers for subdomains of 'home.arpa.'. At this time we do not have operational experience that would guide us in making this decision; implementors are encouraged to consider the context in which their software will be deployed when deciding how to resolve this question.

## 7. Delegation of 'home.arpa.'

In order to be fully functional, there must be a delegation of 'home.arpa.' in the '.arpa.' zone [RFC3172]. This delegation MUST NOT include a DS record, and MUST point to one or more black hole servers, for example 'blackhole-1.iana.org.' and 'blackhole-2.iana.org.'. The reason that this delegation must not be signed is that not signing the delegation breaks the DNSSEC chain of trust,

which prevents a validating stub resolver from rejecting names published under 'home.arpa.' on a homenet name server.

## 8. IANA Considerations

IANA is requested to record the domain name 'home.arpa.' in the Special-Use Domain Names registry [SUDN]. IANA is requested, with the approval of IAB, to implement the delegation requested in Section 7.

IANA is further requested to create a new subregistry within the "Locally-Served DNS Zones" registry [LSDZ], titled "Transport-Independent Locally-Served DNS Zones", with the same format as the other subregistries. IANA is requested to add an entry in this new registry for 'home.arpa.' with the description "Homenet Special-Use Domain", listing this document as the reference. The registration procedure for this subregistry should be the same as for the others, currently "IETF Review" ([RFC8126] Section 4.8).

## 9. Acknowledgments

The authors would like to thank Stuart Cheshire for his prior work on '.home', as well as the homenet chairs: Mark Townsley and Ray Bellis. We would also like to thank Paul Hoffman for providing review and comments on the IANA considerations section, Andrew Sullivan for his review and proposed text, and Suzanne Woolf and Ray Bellis for their very detailed review comments and process insights. Thanks to Mark Andrews for providing an exhaustive reference list on the topic of insecure delegations. Thanks to Dale Worley for catching a rather egregious mistake and for the Gen-Art review, and to Daniel Migault for a thorough SecDir review. Thanks to Warren Kumari for catching some additional issues, and to Adam Roach for some helpful clarifications.

## 10. References

### 10.1. Normative References

[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>.

[RFC3172] Huston, G., Ed., "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")", BCP 52, RFC 3172, DOI 10.17487/RFC3172, September 2001, <https://www.rfc-editor.org/info/rfc3172>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC6303] Andrews, M., "Locally Served DNS Zones", BCP 163, RFC 6303, DOI 10.17487/RFC6303, July 2011, <https://www.rfc-editor.org/info/rfc6303>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

[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>.

## 10.2. Informative References

[ICANN1] "New gTLD Collision Risk Mitigation", October 2013, <https://www.icann.org/en/system/files/files/new-gtld-collision-mitigation-05aug13-en.pdf>.

[ICANN2] "New gTLD Collision Occurence Management", October 2013, <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-1-07oct13-en.pdf>.

[LSDZ] "Locally-Served DNS Zones Registry", July 2011, <https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xhtml>.

[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>.

[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>.

[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>.

[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>.

[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>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[SUDN] "Special-Use Domain Names Registry", July 2012, <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml>.

## Authors' Addresses

Pierre Pfister
Cisco Systems
Paris
France

Email: pierre.pfister@darou.fr

Ted Lemon
Nominum, Inc.
800 Bridge Parkway
Redwood City, California 94065
United States of America

Phone: +1 650 381 6000
Email: ted.lemon@nominum.com