Status of this memo

This memo provides information to the Internet community. It does not specify an Internet standard of any kind. This memo is in full conformance with all provisions of Section 10 of RFC2026

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Abstract

This memo summarizes DNS related issues when transitioning a network to IPv6. Consensus and open issues are presented.

1. Representing IPv6 addresses in DNS records

In the direct zones, according to [RFC3363], IPv6 addresses are represented using AAAA records [RFC1886]. In the reverse zone, IPv6 addresses are represented using PTR records in nibble format under the ip6.arpa. tree [RFC3152].

2. IPv4/IPv6 name space

2.1 Terminology

The phrase "IPv4 name server" indicates a name server available over IPv4 transport. It does not imply anything about what DNS data is served. Likewise, "IPv6 name server" indicates a name server available over IPv6 transport.

2.2 Introduction to the problem of name space fragmentation: following the referral chain

The caching resolver that tries to lookup a name starts out at the root, and follows referrals until it is referred to a nameserver that
is authoritative for the name. If somewhere down the chain of referrals it is referred to a nameserver that is only accessible over a type of transport that is unavailable, a traditional nameserver is unable to finish the task.

When the Internet moves from IPv4 to a mixture of IPv4 and IPv6 it is only a matter of time until this starts to happen and the complete DNS hierarchy starts to fragment into a graph where authoritative nameservers for certain nodes are only accessible over a certain transport. What is feared is that a node using only a particular version of IP, querying information about another node using the same version of IP can not do it because, somewhere in the chain of servers accessed during the resolution process, one or more of them will only be accessible with the other version of IP.

With all DNS data only available over IPv4 transport everything is simple. IPv4 resolvers can use the intended mechanism of following referrals from the root and down while IPv6 resolvers have to work through a "translator", i.e. they have to use a second name server on a so-called "dual stack" host as a "forwarder" since they cannot access the DNS data directly.

With all DNS data only available over IPv6 transport everything would be equally simple, with the exception of old legacy IPv4 name servers having to switch to a forwarding configuration.

However, the second situation will not arise in a foreseeable time. Instead, it is expected that the transition will be from IPv4 only to a mixture of IPv4 and IPv6, with DNS data of theoretically three categories depending on whether it is available only over IPv4 transport, only over IPv6 or both.

The latter is the best situation, and a major question is how to ensure that it as quickly as possible becomes the norm. However, while it is obvious that some DNS data will only be available over v4 transport for a long time it is also obvious that it is important to avoid fragmenting the name space available to IPv4 only hosts. I.e. during transition it is not acceptable to break the name space that we presently have available for IPv4-only hosts.

2.3 Policy based avoidance of name space fragmentation.

Today there are only a few DNS "zones" on the public Internet that are available over IPv6 transport, and they can mostly be regarded as "experimental". However, as soon as there is a root name server available over IPv6 transport it is reasonable to expect that it will become more common to have zones served by IPv6 servers over time.

Having those zones served only by IPv6-only name server would not be a good development, since this will fragment the previously unfragmented IPv4 name space and there are strong reasons to find a mechanism to avoid it.

The RECOMMENDED approach to maintain name space continuity is to use administrative policies:
- every recursive DNS server SHOULD be either IPv4-only or dual stack,
- every single DNS zone SHOULD be served by at least one IPv4 reachable DNS server.
This rules out IPv6-only recursive DNS servers and DNS zones served only by IPv6-only DNS servers. This approach could be revisited if/when translation techniques between IPv4 and IPv6 were to be widely deployed.

In order to enforce the second point, the zone validation process SHOULD ensure that there is at least one IPv4 address record available for the name servers of any child delegations within the zone.

3. Local Scope addresses.

[IPv6ADDRARCH] define three scopes of addresses, link local, site local and global.

3.1 Link local addresses

Local addresses SHOULD NOT be published in the DNS, neither in the forward tree nor in the reverse tree.

3.2 Site local addresses

Note: There is an ongoing discussion in the IPv6 wg on the usefulness of site local addresses that may end up deprecating or limiting the use of Site Local addresses.

Site local addresses are an evolution of private addresses [RFC1918] in IPv4. The main difference is that, within a site, nodes are expected to have several addresses with different scopes. [ADDRSELEC] recommends to use the lowest possible scope possible for communications. That is, if both site local & global addresses are published in the DNS for node B, and node A is configured also with both site local & global addresses, the communication between node A and B has to use site local addresses.

For reasons illustrated in [DontPublish], site local addresses SHOULD NOT be published in the public DNS. They MAY be published in a site view of the DNS if two-face DNS is deployed.

For a related discussion on how to handle those "local" zones, see [LOCAL].

3.3 Reverse path DNS for site local addresses.

The main issue is that the view of a site may be different on a stub resolver and on a fully recursive resolver it points to. A simple scenario to illustrate the issue is a home network deploying site local addresses. Reverse DNS resolution for site local addresses has to be done within the home network and the stub resolver cannot simply point to the ISP DNS resolver.

Site local addresses SHOULD NOT be populated in the public reverse tree. If two-face DNS is deployed, site local addresses MAY be populated in the local view of reverse tree.
4. Automatic population of the Reverse path DNS

Getting the reverse tree DNS populated correctly in IPv4 is not an easy exercise and very often the records are not really up to date or simply are just not there. As IPv6 addresses are much longer than IPv4 addresses, the situation of the reverse tree DNS will probably be even worse.

A fairly common practice from IPv4 ISP is to generate PTR records for home customers automatically from the IPv4 address itself. Something like:

```
1.2.3.4.in-addr.arpa. IN PTR 4.3.2.1.local-ISP.net
```

It is not clear today if something similar need to be done in IPv6, and, if yes, what is the best approach to this problem.

As the number of possible PTR records would be huge \((2^{80})\) for a /48 prefix, a possible solution would be to use wildcards entries like:

```
*.0.1.2.3.4.5.6.7.8.9.a.b.c.ip6.arpa. IN PTR customer-42.local-ISP.net
```

However, the use of wildcard is generally discouraged and this may not be an acceptable solution.

An alternative approach is to dynamically synthetize PTR records, either on the server side or on the resolver side. This approach is discussed at length in [DYNREVERSE].

Other solutions like the use of ICMP name lookups [ICMPNL] have been proposed but failed to reach consensus. It would work if and only the remote host is reachable at the time of the request and one can somehow trust the value that would be returned by the remote host.

A more radical approach would be not to pre-populate the reverse tree at all. This approach claims that applications that misuse reverse DNS for any kind of access control are fundamentally broken and should be fixed without introducing any kludge in the DNS. There is a certain capital of sympathy for this, however, ISP who who pre-generate statically PTR records for their IPv4 customers do it for a reason, and it is unlikely that this reason will disappear with the introduction of IPv6.

5. Privacy extension addresses

[RFC3041] defines privacy extensions for IPv6 stateless autoconfiguration where the interface ID is a random number. As those addresses are designed to provide privacy by making it more difficult to log and trace back to the user, it makes no sense to in the reverse tree DNS to have them pointing to a real name.

[RFC3041] type addresses SHOULD NOT be published in the reverse tree DNS pointing to meaningful names. A generic, catch-all name MAY be acceptable. An interesting alternative would be to use dynamic synthesis as in [DYNREVERSE].
6. 6to4

6to4 addresses can be published in the forward DNS, however special care is needed in the reverse tree. See [6to4ReverseDNS] for details. The delegation of 2.0.0.2.ip6.arpa. is suggested in [6to4ARPA], however, delegations in the reverse zone under 2.0.0.2.ip6.arpa are the core of the problem. Delegating the next 32 bits of the IPv4 address used in the 6to4 domain won’t scale and delegating on less may require cooperation from the upstream IPSs. The problem here is that, especially in the case of home usage of 6to4, the entity being delegated the x.y.z.t.2.0.0.2.ip6.arpa. zone (the ISP) may not be the same as the one using 6to4 (the end customer). The

Another problem with reverse DNS for 6to4 addresses is that the 6to4 prefix may be transient. One of the usage scenario of 6to4 is to have PCs connected via dial-up use 6to4 to connect to the IPv6 Internet. In such a scenario, the lifetime of the 6to4 prefix is the same as the DHCP lease of the IPv4 address it is derived from. It means that the reverse DNS delegation is only valid for the same duration.

A possible approach is not to populate the reverse tree DNS for 6to4 addresses. Another one is to use dynamic synthesis as described in [DYNREVERSE].

7. Recursive DNS server discovery

[DNSdiscovery] has been proposed to reserve a well known site local unicast address to configure the DNS resolver as a last resort mechanism, when no other information is available. Another approach is to use a DHCPv6 extensions [DHCPv6DNS].

8. DNSsec

There is nothing specific to IPv6 or IPv4 in DNSsec. However, translation tools such as NAT-PT [RFC2766] introduce a DNS-ALG that will break DNSsec by imposing a change in the trust model. See [DNS-ALG] for details.

9. Security considerations

Using wildcard DNS records in the reverse path tree may have some implication when used in conjunction with DNSsec. Security considerations for referenced documents are described in those memos and are not replicated here.

10. Author addresses

Alain Durand
SUN Microsystems, Inc
17 Network circle UMPK17-202
Menlo Park, CA, 94025
11. References


[RFC3041] Privacy Extensions for Stateless Address Autoconfiguration in IPv6,


[ICMPNL] Use of ICMPv6 node information query for reverse DNS lookup, Jun-ichiro itojun Hagino, draft-itojun-ipv6-nodeinfo-revlookup-00.txt, work in progress.


[6to4ARPA] Delegation of 2.0.0.2.ip6.arpa, Bush, R., Damas, J., draft-ymbk-6to4-arpa-delegation-00.txt, work in progress.

[6to4ReverseDNS] 6to4 and DNS, K. Moore, draft-moore-6to4-dns-03.txt, work in progress.

[DNSdiscovery] Well known site local unicast addresses for DNS resolver,

[DHCPv6DNS] DNS Configuration options for DHCPv6, Droms, R.
12. Full Copyright Statement

"Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."