Internet Engineering Task Force
INTERNET-DRAFT
June, 23, 2002
Expires December, 24, 2002

Alain Durand
SUN Microsystems,inc.

IPv6 DNS transition issues
<draft-durand-ngtrans-dns-issues-00.txt.

Status of this memo

Abstract

This memo summarizes DNS related issues when transitioning a network to IPv6. Those issues have been discussed in the NGtrans, IPv6, DNSext and DNSop working group. Wherever consensus has been reached, it is presented. When consensus has not yet been reached, a list of open issues is presented.

1. DNS records

In the direct zones, the consensus is to use AAAA [RFC1886] records. In the reverse zone, the consensus is to use PTR records in nibble format under the ip6.arpa. tree.

2. IPv4/IPv6 name space

There is consensus that keeping the Internet name space unfragmented is a good thing. This covers IPv4 and IPv6. It means that any record in the public Internet should be available to any nodes, IPv4 or IPv6. See [FRAGMENTATION] and [DNS-OPS-REQ] for details. One possible approach is to maintain name space continuity with administrative procedures: ask every full DNS resolver to be dual stack and ask that every single DNS zone has to be served by at least an IPv4 reachable DNS server. The other avenue to approach this problem is to design a 'bridging system' enabling direct communication between and IPv6 only DNS resolver and an IPv4 only DNS server or an IPv4 only resolver talking to an IPv6 only DNS server. NAT-PT [RFC2766] does not work for that purpose because of the DNS-ALG built-in. Other issues surrounding NAT-PT are discussed in [NAT-PTissues]. [NAT64] as a potential replacement for NAT-PT could be a better fit, at least for the case of the IPv6 only DNS resolver talking to an IPv4 only DNS server.

3. Local Scope addresses.

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

3.1 Link local addresses

There is consensus not to publish link local addresses in the DNS.

3.2 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. This means that 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.

3.3 Reverse path DNS for site local.

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.

4. Reverse 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
```

Its not clear today if something similar need to be done in IPv6. 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
```

5. 6to4

6to4 addresses can be published in the forward DNS, however special care is needed in the reverse tree. See [6to4ReverseDNS] for details. 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.

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 Inernet. 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.

6. DNS resolver discovery

[DNSdiscovery] has been proposed to reserved 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 DHCPv6 extensions.

7. DNSsec

There is nothing specific to IPv6 or IPv4 in DNSsec.

8. Security considerations

A certain number of security considerations are not completely solved.

- If a 'bridging system' based on translation is designed to enable seamless interoperation between IPv4 & IPv6 DNS resolvers & servers, this system should not introduce any new security issues.
- If DNS resolver discovery is done using the 'well known address' approach, the stub resolver will not know exactly which resolver it is talking to and thus may or may not be able establish a cryptographically verified association with it.

9. Author addresses

Alain Durand
SUN Microsystems, Inc
901 San Antonio Road MPK17-202
Palo Alto, CA 94303-4900
USA
Mail: Alain.Durand@sun.com

10. References

[RFC1918] Address Allocation for Private Internets. Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear. February 1996.

[RFC2766] Network Address Translation - Protocol Translation (NAT-PT). G. Tsirtsis, P. Srisuresh. February 2000.

[NAT-PTissues] Issues with NAT-PT DNS ALG in RFC2766, A. Durand, draft-durand-natpt-dns-alg-issues-00.txt, work in progress.

[NAT64] NAT64 - NAT46, A. Durand, draft-durand-ngtrans-nat64-nat46-00.txt, work in progress.

[FRAGMENTATION] IPv4-to-IPv6 migration and DNS namespace fragmentation, J. Ihren, draft-ietf-dnsop-v6-name-space-fragmentation-01.txt, work in progress.

[DNS-OPS-REQ] NGtrans IPv6 DNS operational requirements and roadmap, A. Durand, J. Ihren, draft-ietf-ngtrans-dns-ops-req-04.txt, work in progress.

[IPv6ADDRARCH] IP Version 6 Addressing Architecture, R. Hinden,

draft-ipngwg-addr-arch-v3-07.txt, work in progress.

[6to4ReverseDNS] 6to4 and DNS, K. Moore, draft-ietf-ngtrans-6to4-dns-00.txt, work in progress.

[DNSdiscovery] Well known site local unicast addresses for DNS resolver, A. Durand, J. hagano, D. Thaler, draft-ietf-ipv6-dns-discovery-05.txt, work in progress.

10. Full Copyright Statement