Initializing a DNS Resolver with Priming Queries

draft-ietf-dnsop-resolver-priming-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on January 3, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document describes the initial queries a DNS resolver is supposed to emit to initialize its cache with a current NS RRSet for the root zone as well as the necessary address information.
1. Introduction

Domain Name System (DNS) resolvers need a starting point to resolve queries. [RFC1034], section 5.3.2, defines the SBELT structure in a full resolver as:

```
a "safety belt" structure of the same form as SLIST, which is initialized from a configuration file, and lists servers which should be used when the resolver doesn’t have any local information to guide name server selection. The match count will be -1 to indicate that no labels are known to match.
```

Section 5.3.3 of [RFC1034] adds

```
‘‘the usual choice is two of the root servers and two of the servers for the host’s domain’’
```

Today’s practice generally separates serving and resolving functionality, so the servers ‘‘for the host’s domain’’ might no longer be an appropriate choice, even if they were only intended to resolve ‘‘local’’ names, especially since the SBELT structure does not distinguish between local and global information. In addition, DNS server implementations have for a long time been seeded with not only two but an exhaustive list of the root servers’ addresses. This list is either supplied as a configuration file (root "hints", an excerpt of the DNS root zone) or even compiled into the software.

The list of root name servers has been rather stable over the last ten years. After the last four servers had been added and moved to their final (network) destinations in 1997, there have been only three address changes affecting the L, J, and B servers. Research is available for B [Mann2006] and J [BLKT2004], which shows that several months or even years after the change had become effective, traffic is still received on the old addresses. Therefore, it is important that resolvers be able to cope with change, even without relying upon configuration updates to be applied by their operator.

The recent work by the ICANN SSAC and RSSAC committees, [SSAC016] and [SSAC017], aiming at adding AAAA RRs for the root name servers’ names, deals with priming queries and so does a draft on DNSSEC Trust Anchor maintenance [I-D.larson-dnsop-trust-anchor]. However, it turned out that despite having been practiced for a long time, priming queries have not yet been documented as an important resolver feature.

The following sections cover parameters of both the priming query and the response to be sent by a root name server.
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Parameters of a Priming Query

This document only deals with QCLASS IN. A priming query SHOULD use a QNAME of "." and a QTYPE of NS. It SHOULD also use EDNS0 [RFC2671] and announce and handle a reassembly size of at least 1024 octets [RFC3226].

A priming query MUST be sent over UDP (section 6.1.3.2 of [RFC1123]). The RD bit MUST NOT be set in the query.

2.1. Target Selection

A resolver MUST select the target for a priming query randomly from its list of available addresses and it MUST ensure that all targets are selected with equal probability even upon startup. For resending the priming query to a different server the random selection SHOULD also be used.

2.2. DNSSEC with Priming Queries

The resolver MAY choose to use DNSSEC OK [RFC4033], in which case it MUST announce and handle a message size of at least 1220 octets.

Discussion: Delegations in referral responses are not signed, so following this model there would be no need to require a signed root NS RRSet and, equally important, signed A and AAAA RRSet for the root name servers’ names. On the other hand, a poisoned priming response could drastically influence the resolver’s operations. If the priming response should be secured by DNSSEC, then it should also be self contained, i.e., the whole validation chain should be present in the priming response. This might call for a different naming scheme (see section 5.1 of [I-D.koch-dns-glue-clarifications]).

2.3. Repeating Priming Queries

A resolver SHOULD NOT originate a priming query more often than once per day (or whenever it starts). It SHOULD adhere to the TTL values given in the priming response. To avoid amnesia, the resolver MAY proactively re-prime before the old root NS RRSet expires from the cache, but only after 75 percent of the NS RRSet’s TTL (or the A/AAAA RRSets’ TTL, whichever is lower) have passed.
3. Expected Properties of a Priming Response

The response can be expected to have an RCODE of NOERROR and the AA bit set. Also, there should be an NS RRSet in the answer section (since the NS RRSet originates from the root zone), an empty authority section and an additional section with A and AAAA RRSets for the root name servers pointed at by the NS RRSet. (Note that the number 13 does not appear here. It might be necessary to consider "internal" root server setups in split DNS configurations.)

3.1. Use of the Priming Response

A resolver MAY use the priming response as it would use any other data fed to its cache. However, it SHOULD NOT use the SBELT information directly in any responses it hands out.

3.2. Completeness of the Response

A resolver SHOULD consider the address information found in the additional section complete for any particular server that appears at all. In other words: if the additional section only has an A RRSet for a server, the resolver SHOULD assume that no AAAA RRSet exists. To ensure equal availability the A and AAAA RRSets should have identical TTL values at the authoritative source.

4. Root Name Server Requirements

The operational requirements for root name servers are described in [RFC2870].

All DNS root name servers need to be able to provide for all addresses of all root name servers. This can easily achieved by making all root name servers authoritative for the zone containing the servers’ names. (At the time of writing, all but one root name server were authoritative for ROOT-SERVERS.NET., even though only a subset received an official delegation.)

If the response packet does not provide for more than 512 octets due to lack of EDNS0 support, AAAA RRSets should be omitted from the response. (EDNS0 is used as an indication of AAAA understanding. What to do with small payload sizes indicated by EDNS0 is open to discussion.)

5. Security Considerations

This document deals with priming a DNS resolver’s cache. The usual
DNS caveats apply. Use of DNSSEC with priming queries is discussed in section 2.2

Spoofing a response to a priming query can be used to redirect all queries originating from a victim resolver, therefore any difference between the initial SBELT list and the priming response SHOULD be brought to the operators’ attention. There is also a chance that the random target selection chooses the address of a retired root name server. Operational measures to prevent reuse of these addresses are out of the scope of this document.

(This section needs more work.)

6.  IANA Considerations

This document does not propose any new IANA registry nor does it ask for any allocation from an existing IANA registry.

However, this document deals with requirements for the root zone and root server operations.

(This section needs more work.)

7.  References

7.1.  Normative References


7.2. Informative References

[BLKT2004]

[I-D.koch-dns-glue-clarifications]

[I-D.larson-dnsop-trust-anchor]

[Mann2006]
Manning, B., "persistent queries and phantom nameservers", WIDE/CAIDA Workshop, October 2006.


Appendix A. Document Revision History

This section is to be removed should the draft be published.

A.1. -00 WG Document

Reposted as WG document with minor edits.

Added re-priming proposal and A/AAAA TTL considerations.
A.2. Initial Document

First draft

Authors’ Addresses

Peter Koch
DENIC eG
Wiesenhettenplatz 26
Frankfurt  60329
DE

Phone: +49 69 27235 0
Email: pk@DENIC.DE

Matt Larson
VeriSign, Inc.
21345 Ridgetop Circle
Dulles, VA  20166-6503
USA

Email: mlarson@verisign.com