A Mechanism to Reduce the junky queries to Authoritative Name Servers Serving Small Size Zones
draft-yao-dnsop-smallzone-junk-query-00

Abstract

Some zones are small, public and stable, but very important. They might deal with millions of queries every day. But many of the queries are junky. For examples, many queries DNS root servers receive are junky. The queried junky names are not in the root, but the root servers have to waste a lot of resources to deal with them. It has been an obstacle to increase the performance of DNS root query. In order to save the resource caused by the DNS junky queries, this document proposes a new mechanism by aggressive use of the owner name list of the DNS zone.

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 January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
Some zones are small, public and stable, but very important. They might deal with millions of queries every day. But many of the queries are junky. For examples, many queries DNS root servers receive are junky. The queried junky names are not in the root, but the root servers have to waste a lot of resources to deal with them. It has been an obstacle to increase the performance of DNS root query.

In order to save the resource caused by the DNS junky queries, this document proposes a new mechanism by aggressive use of the owner name list of the DNS zone. This document proposes an owner name list of
the DNS zone, and introduces a new RR type that serves as a
cryptographic message digest of the owner name list of the DNS zone.
The digest allows a receiver of the owner name list of the zone to
verify the owner name list.

2. Terminology

The basic key words such as "MUST", "MUST NOT", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "MAY", and "MAYNOT" are to be interpreted as
described in [RFC2119] [RFC8174].

The basic DNS terms used in this specification are defined in the
documents [RFC1034] and [RFC1035].

3. Design Overview

This document introduces a new mechanism which uses the owner name
list of a zone to produce the negative response. When the resolver
receives the query for the specific zone, it checks its owner name
list of that zone before doing further query. If the name queried is
in the owner name list, it will be sent to that zone for further
query; otherwise, the responder will generate the negative response
if it is not in the owner name list. This document introduces a new
Resource Record type designed to convey a message digest of the owner
name list of a zone. The digest is calculated at the time of zone
publication. Ideally the zone is signed with DNSSEC to guarantee
that any modifications of the digest can be detected. The procedures
for digest calculation and DNSSEC signing are similar, which require
the similar ordering of RRs. Many small zones’ owner name list keeps
stable, although the DNS RR’s type or RDATA may change day by day.
The mechanism is designed to be used on zones that are relatively
stable and have infrequent updates. As currently specified, the
digest is re-calculated over the entire zone when the owner names are
updated. It is expected that verification of digest of owner name
list of a zone would be implemented in name servers and the
resolvers. That is, a name server can verify the zone owner name
list it was given and refuse to serve a zone which fails
verification; a resolver can verify the zone owner name list it was
given and refuse to serve a zone owner name list which fails
verification. For signed zones, the name server needs a trust anchor
to perform DNSSEC validation. A server for a specific zone can
publish the owner name list or the full zone. A resolver can get the
owner name list for a specific zone or get the full zone and create
the owner name list for this zone according to the rules set by this
document.

The goal of our design is that the junk-queried names can be
recognized as soon as possible before sending to the specified zone.
The mechanism proposed by this document will decrease the work load of authoritative name servers serving the specific zone efficiently.

4. Onldigest Resource Record

This record is designed for the cryptographic message digest of the owner name list of the DNS zone. The Onldigest RDATA wire format is encoded as follows:

```
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------------------------------+
|  Digest Type |                                               |
+---------------------------------------------------------------------+
|  ++          |                                               |
| /            |                                               |
| /            |                                               |
+---------------------------------------------------------------------+
```

Figure 1. Onldigest RDATA Wire Format

- The Digest Type field is an 8-bit unsigned integer that identifies the algorithm used to construct the digest.
- The Digest field is a variable-length sequence of octets containing the message digest. The Digest field MUST NOT be empty.

5. Create the Owner Name list and Calculate the Digest

The owner name list digest is calculated by concatenating the canonical on-the-wire form (without name compression) of all RRs in the zone, and then applying the digest algorithm. Some rules are:

- All of owner names of RRs with NS type should be prefixed with "." before putting into the owner name list. It means that if example.com has NS type, the owner name will become ".example.com".
- For ordering of owner names in the zone, this document adopts DNSSEC's canonical ordering for names (Section 6.1 of [RFC4034]),
- It is meaningless for an owner name list to have multiple same owner names. In the interest of consistency and interoperability, such duplicate owner names MUST NOT be included in the owner name list.
6. Requirements for the resolver

In order to implement the mechanism described in this document:

- The resolver should get the owner name list for a specific zone either in band or out of band. It can also get a full zone and create the owner name list for a specific zone.
- The resolver should verify the zone owner name list using the Onldigest record.
- The resolver should refresh the Onldigest record before it expires. When the Onldigest record’s Digest field is updated, it means that the owner name list was updated and the resolve should get a new one.
- For a non DNSSEC query, if the queried name is not on the owner name list for the specific zone, it means that that name is not on that zone or its sub-zone and the resolver can create a nonexistent name response to the query.
- For a DNSSEC query, if the queried name is not on the owner name list for the specific zone, it means that that name is not on that zone or its sub-zone and the resolver can create a nonexistent name response to the query. The resolver can verify the Onldigest record’s relative RRSIG and the owner name list with the Onldigest record. If it is successful, it can be regarded as the DNSSEC verification.

7. Requirements for the Authoritative Name Servers

In order to reduce the workload and get the faster response, the Authoritative Name Servers may choose the similar strategies adopted by the resolvers. For a non DNSSEC query, if the queried name is not on the owner name list for the specific zone, it means that that name is not on that zone or its sub-zone and the servers can create a nonexistent name response to the query. For a DNSSEC query, if the
queried name is not on the owner name list for the specific zone, the servers need to find the NSEC or NSEC3 records before responding.

8. Use Cases

The mechanism proposed in this document has the following use cases (you can help to add more):

- **Root Zone**: The root zone are small, public and stable where the owner name are not likely to be changed for a long time.

- **Important Companies’ zone**: These company’s zones are small and where the owner name are not likely to be changed for a period of time. For examples, CNNIC’s owner name list for cnnic.cn are kept stable for a long time. But sometimes, the attacker may choose name server serving cnnic.cn zone for random name DDOS attack. CNNIC also runs a resolver which can be configured to use this mechanism to help to deduce the flooding to the CNNIC’s authoritative name server.

- **Public DNS Resolver**: The public DNS resolver can provide the value-added service to some specific companies’ zone. Some online company may choose to coporate with some public DNS resolvers to reduce the possible DDOS attack to their companies’ authoritative name servers.

9. IANA Considerations

This document defines a new DNS RR type, Onldigest, whose value ** has been allocated by IANA from the "Resource Record (RR) TYPEs" subregistry of the "Domain Name System (DNS) Parameters" registry:

Type: Onldigest

Value: **

Meaning: Owner name list digest

Reference: This document

10. Security Considerations

The mechanism design in this document is useful for small, public and stable zone, where owner names are likely to kept stable. It is not useful for big, private and dynamic zone, where owner names are too many or likely to kept dynamical.
The resolver needs to know the owner name list via the public zones or the one published by the zone owners.

11. Change History

RFC Editor: Please remove this section.

11.1. draft-yao-dnsop-smallzone-junk-query: Version 00

- Help to reduce the workload of junk-query to the authoritative name servers.

12. Normative References


Author’s Address

Jiankang Yao
CNNIC
4 South 4th Street, Zhongguancun, Haidian District
Beijing, Beijing 100190
China

Phone: +86 10 5881 3007
Email: yaojk@cnnic.cn