DNS Start of Authority Discovery

draft-andrews-dnsext-soa-discovery-00

Abstract

Sometimes it is necessary to discover the Start of Authority points in the DNS, otherwise known as zone cuts, without causing negative entries to be recorded in caches. This document describes how to achieve this.
Table of Contents

1. Introduction ................................................. 3
1.1. Reserved Words ........................................... 3
2. Why Choose SOA over NS Queries .............................. 3
3. Authoritative Server Behaviour ............................... 4
4. Caching Server Behaviour ................................... 4
5. Client Behaviour ............................................ 4
6. IANA Considerations ........................................ 5
7. Security Considerations ..................................... 5
8. References .................................................. 5
  8.1. Normative References ................................... 5
  8.2. Informative References ................................ 5
Author’s Address ................................................ 6
Intellectual Property and Copyright Statements ................ 7
1. Introduction

When performing a DNS UPDATE RFC 2136 [RFC2136] it is necessary to send the request to the nameservers for the zone. Often, however, all you have is the name of the record to be updated. From this you need to discover the zone and the authoritative nameservers to which the DNS UPDATE request should be addressed to.

One method would be to query for the root nameservers then have the client follow the delegation path talking to each set of nameservers in turn. In practice this does not work due to firewalls and because not all names in the DNS actually have a delegation path from the root. The later is especially true with split DNS configurations and with sites using private addressing RFC 1918 [RFC1918].

The next method is just to query for the SOA or NS records (both being present only at zone cuts) at the query name, removing labels until a answer is returned. This works well if the initial query happens to be at a zone cut and reasonably well if the query name exists in the DNS. It does not work well if name does not exist in the DNS as the negative cache entry obscures the changes that are about to be made.

This document describes changes to nameserver behaviour which remove the undesired side effects of making a SOA query.

1.1. Reserved Words

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 RFC 2119 [RFC2119].

2. Why Choose SOA over NS Queries

As the primary motivation for this was to support UPDATE requests and these are supposed to be preferentially directed at the SOA MNAME, the SOA query was required. SOA queries will also usually return the corresponding NS RRset in the additional section where as the NS query will not return the SOA RRset at zone cuts.

SOA queries are not part of the normal query mix. Not negatively caching the SOA response is unlikely to have a detrimental impact.

SOA queries do not interfere with any benefits of caching the NODATA response to NS queries made by nameservers performing DNSSEC validations RFC 4035, Section 4.2 [RFC4035].
3. Authoritative Server Behaviour

When returning a negative answer to a SOA query, the nameserver sets the TTL of the SOA record in the authority section of the response to zero rather than the SOA MINIMUM as described in RFC 2308 [RFC2308].

An implementation SHOULD do this by default but MUST allow it to be overridden on a per zone basis. Some zones which are not updateable, TLDs in particular, have "unregistered" children which attempt to update them. Returning a negative response with a non-zero TTL can reduce the load on the authoritative servers.

4. Caching Server Behaviour

When a resolver receives a negative answer to a SOA query it MAY set the negative cache TTL to zero. It MAY also set the TTL of the SOA record in the authority section to zero.

This is useful when the authoritative servers do not follow this documents and there are update clients using the cache.

5. Client Behaviour

Clients start by issuing a recursive query for a SOA resource record at <QNAME,QCLASS>. If we get one as an answer that matches the <SOA,QNAME,QCLASS> tuple we have found the containing zone name.

If a referral is returned then fail.

If a CNAME or DNAME is returned in the answer section the QNAME does not correspond to a zone name and any SOA record present may not be for the desired zone. The client SHOULD re-query removing the leftmost (least significant) label from QNAME.

If we get a SOA record in the authority section this record should refer to the enclosing zone, RFC 2308 [RFC2308].

If the answer section is empty and there is not SOA record in the authority section the client needs to re-query with the leftmost label removed.

If a client performs an UPDATE it should not immediately perform an action that depends on the updated data being returned to the resolver. UPDATEs, even when NOTIFY RFC 1996 [RFC1996] is in use, take some time to propagate to the authoritative servers. Immediately querying for the updated data using a caching server will
often defeat the steps taken here.

Polling each of the nameservers for the zone to see if it has the new
data and waiting if it doesn’t should prevent this occurring. If you
do this use exponential back-off when polling.

6. IANA Considerations

This document has no actions for IANA.

7. Security Considerations

As with all answers from the DNS, clients need to be aware that
answers may be spoofed. It is advised that that clients use DNSSEC,
TSIG, SIG(0) or some other cryptographic mechanism to detect such
spoofed responses.

8. References

8.1. Normative References

[ RFC2119 ] Bradner, S., "Key words for use in RFCs to Indicate

[ RFC2308 ] Andrews, M., "Negative Caching of DNS Queries (DNS
NCACHE)", RFC 2308, March 1998.

8.2. Informative References

[ RFC1918 ] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G.,

[ RFC1996 ] Vixie, P., "Mechanism for Prompt Notification of Zone

[ RFC2136 ] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound,
"Dynamic Updates in the Domain Name System (DNS UPDATE)",
RFC 2136, April 1997.

Rose, "Protocol Modifications for the DNS Security
Author’s Address

Mark P. Andrews
Internet Systems Consortium
950 Charter Street
Redwood City, CA  94063
US

Email: Mark_Andrews@isc.org
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.