DNSOP
Internet-Draft
Updates: 1035 (if approved)
Intended status: Standards Track
Expires: September 10, 2015

O. Gudmundsson
M. Majkowski
CloudFlare Inc.
J. Abley
Dyn, Inc.

March 9, 2015

DNS Meta-Queries restricted. draft-ogud-dnsop-acl-metaqueries-00

Abstract

Some DNS types have special meaning and are classified as meta queries, this includes ANY, AXFR, IXFR. These queries frequently return larger answers than queries for other types.

This document defines a standard way for Authoritative-Only servers how to refuse to serve these and other similar queries, with the expectation that resolvers honor that, by not asking followup queries.

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 http://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 September 10, 2015.

Copyright Notice

Table of Contents

1. Introduction

The DNS Specification [RFC1035] meta queries where defined for use either zone maintainance AXFR, full zone transfer, IXFR [RFC1995], incremental zone transfer. For security reasons Authoritative name servers frequently only respond to these queries if a TSIG [RFC2845] key is presented or the query comes from an approved address.

The ANY meta query was defined for debugging purposes mainly against resolvers. There have been widespread misunderstanding as to what the query is supposed to do and when it is approriate. The query is intented for testing what records for a particular name a resolver has in its cache. There are security implications related to information leaks and use in DoS attacks that strongly argue for restricting its use like the other Meta Queries.

RRSIG [RFC4034] type used in a query can also return large answers as the server attempts to put all RRSIG records at that one name into one answer. This type was envisioned as deployment tool for validators to overcome DNSSEC ignorant resolvers and/or servers. For all practical purposes this is never needed.

Queries yielding large answers are known to be widely abused by attackers carrying out reflection attacks, since they provide a convenient way to elicit large responses from small queries, and hence exhibit significant amplification potential. A similar reaction to an operational security problem can be observed in the advice contained within [RFC5358].

The data model used by some authoritative-only DNS server implementations does not align easily with the zone structure described in [RFC1035], and responding accurately to meta queries involves significant processing overhead. The ability to refuse meta queries can simplify the implementation with corresponding benefits to performance and code correctness.

Recursive Resovlers frequently treat REFUSED as a temporary denial. In the case of policy statement that certain queries will not answered, having a more explicit statment is beneficial. There are two chocies as how more permanent semantics can be expressed, reusing an exisiting RCODE or define a new one. This docuemnt proposes reusing the NOTIMP rcode. This feels like the right choice as as far as the querier is concerned it makes no difference if the meta type is implemented or the authoritative server has no interest in providing that service to the client. There are other options like defining new RCODE or place stronger semantics on REFUSED.

Various DNS operators have chosen to refuse various meta queries including QTYPE=ANY in the past, using a variety of approaches, including rate-limiting of queries and responses, returning TC=1 on qeries received via UDP transport and silently dropping queries before they reach the DNS server. Consistency in approach would provide a more predictable outcome for DNS resolvers and clients.

2. Requirements Notation

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].

3. Protocol Changes

DNS processing entities SHOULD support authenticated meta queries, and process them when appropriate as defined by policy. By default the implemenations SHOULD be restrict it to localhost via ACL. For all rejected meta-queries the behavior specified below SHOULD be used. The types where this behavior is appropriate includes ANY, AXFR, IXFR, RRSIG.

An authoritative-only DNS server MAY reject meta queries received by returning RCODE=4 (NOTIMP).

An iterative resolver MUST NOT forward a meta-query when the query arrives with RD=0, even when it has no types for that name. An iterative resolver SHOULD ignore RD=1 on a meta query, i.e. it SHOULD NOT forward them upstream.

An iterative resolver that sends a query to an authoritative DNS server and receives a response with RCODE=4 SHOULD remember that upstream server's behaviour, for that qclass, qname, qtype combination. It SHOULD suppress any subsequent qeries for that qclass, qname, qtype to that server for at least one day (??? better value needed).

4. IANA Considerations

No actions are requested of the IANA.

5. Security Considerations

In the original Internet where everyone behaved nicely had different secrity and operating model than todays Internet. This document is defining how DNS servers can express that they will never answer a particular query from a given address.

RCODE=REFUSED is frequently treated as temporary thus resolver may repeat queries in the hope of getting an answer.

An on-path attacker[RFC3833] can forge these answers easily, but as that document explains the attacker can anyway inject any lies it wants to.

6. Implementation Experience

TBD

7. Acknowledgements

Editors want to thank following people, in random order, for useful feedback: Paul Vixie, Tony Finch, Ralph Weber, Mark Andrews, Stephane ortzmeyre, Filippo Valsodra, Edward Lewis, and we forgot someone.

8. References

8.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, August 1996.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC5358] Damas, J. and F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks", BCP 140, RFC 5358, October 2008.

Appendix A. Document history

This section (and sub-sections) should be removed before publication.

A.1. Venue

An appropriate venue to discuss this draft is the dnsop working group mailing list.

A.2. Abridged Revision History

A.2.1. draft-ogud-dnsop-any-notimp-00

Initial draft.

A.2.2. draft-ogud-dnsop-acl-metaqueries-00

Wordsmithing; add jabley as co-author; normalise normative language in protocol changes section.

Based on feeback from dnsop mailing list, we Expaned the scope of the document to cover "META" types in general, and express that RCODE=NOTIMP should be cached by resolvers. Changed language so it is more neutral to as what path this work takes.

Authors' Addresses

Olafur Gudmundsson
CloudFlare Inc.
San Francisco, CA 94107
USA

Email: olafur@cloudflare.com

Marek Majkowski
CloudFlare Inc.
London
UK

Email: marek@cloudflare.com

Joe Abley
Dyn, Inc.
103-186 Albert Street
London, ON N6A 1M1
Canada

Email: jabley@dyn.com