Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: September 3, 2017

M. Andrews
ISC

March 2, 2017

A Common Operational Problem in DNS Servers - Failure To Respond.
draft-ietf-dnsop-no-response-issue-07

Abstract

The DNS is a query / response protocol. Failure to respond or to respond correctly to queries causes both immediate operational problems and long term problems with protocol development.

This document identifies a number of common kinds of queries to which some servers either fail to respond or else respond incorrectly. This document also suggests procedures for TLD and other zone operators to apply to help reduce / eliminate the problem.

The document does not look at the DNS data itself, just the structure of the responses.

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 3, 2017.

Table of Contents

1. Introduction

The DNS [RFC1034], [RFC1035] is a query / response protocol. Failure to respond to queries or to respond incorrectly causes both immediate operational problems and long term problems with protocol development.

Failure to respond to a query is indistinguishable from a packet loss without doing a analysis of query response patterns. Additionally failure to respond results in unnecessary queries being made by DNS clients, and delays being introduced to the resolution process.

Due to the inability to distinguish between packet loss and nameservers dropping EDNS [RFC6891] queries, packet loss is sometimes misclassified as lack of EDNS support which can lead to DNSSEC validation failures.

Servers which fail to respond to queries results in developers being hesitant to deploy new standards. Such servers need to be identified.

The DNS has response codes that cover almost any conceivable query response. A nameserver should be able to respond to any conceivable query using them. There should be no need to drop queries because a nameserver does not understand them.

Unless a nameserver is under attack, it should respond to all queries directed to it. Additionally, the nameserver should not assume that there isn't a delegation to the server even if it is not configured to serve the zone. Broken nameservers are a common occurrence in the DNS and receiving queries for zones that the server is not configured for is not necessarily an indication that the server is under attack. Parent zone operators are supposed to regularly check that the delegating NS records are consistent with those of the delegated zone and to correct them when they are not [RFC1034]. Doing this regularly should reduce the instances of broken delegations.

When a nameserver is under attack it may wish to drop packets. A common attack is to use a nameserver as a amplifier by sending spoofed packets. This is done because response packets are bigger than the queries and big amplification factors are available especially if EDNS is supported. Limiting the rate of responses is reasonable when this is occurring and the client should retry. This however only works if legitimate clients are not being forced to guess whether EDNS queries are accepted or not. While there is still a pool of servers that don't respond to EDNS requests, clients have no way to know if the lack of response is due to packet loss, EDNS packets not being supported or rate limiting due to the server being under attack. Misclassification of server behaviour is unavoidable when rate limiting is used until the population of servers which fail to respond to well formed queries drops to near zero.

2. Consequences

Not following the relevant DNS RFCs has multiple adverse consequences. Some resulting directly from the non-compliant behaviour and others as a result of work-arounds forced on recursive servers. Addressing known issues now will reduce future interoperability issues as the DNS protocol continues to evolve and clients make use of newly introduced DNS features.

Some examples of known consequences include:

- The AD flag bit in a response cannot be trusted to mean anything as many servers incorrectly copied the flag bit from the request to the response despite the prohibition.

- Widespread non response to EDNS queries has lead to recursive servers having to assume EDNS may not supported and that fallback to plain DNS is required. Servers get incorrectly diagnosed as not supporting EDNS and when they also serve signed zones DNSSEC validation fails.

- Widespread non response to EDNS options, requires recursive servers to have to decide whether to probe to see if it is the EDNS option or just EDNS that is causing the non response. In the limited amount of time required to resolve a query before the client times out this is not possible.

- Incorrectly returning FORMERR to a EDNS option being present, leads to the recursive server not being able to determine if the server is just broken in the handling of the EDNS option or doesn't support EDNS at all.

- Mishandling of unknown query types has contributed to the abandoning of the transition of the SPF type.

- Mishandling of unknown query types has slowed up the development of DANE and and result in additional rules being specified to reduce the probability of interacting with a broken server when making TLSA queries.

The consequences of servers not following the RFCs will only grow if measures are not put in place to remove non compliant servers from the ecosystem. Working around issues due to non RFC compliance is not sustainable.

Most, if not all, of these consequences could have been avoided if action had been taken to remove non compliant servers as soon as people were aware of them. To actively seek out broken implementations and servers and inform their developers and operators that they need to fix their servers.

3. Common queries kinds that result in non responses.

There are a number common query kinds that fail to respond today. They are: EDNS queries with and without extensions; queries for unknown (unallocated) or unsupported types; and filtering of TCP queries.

3.1. Basic DNS Queries

3.1.1. Zone Existence

Initially to test existence of the zone, an SOA query should be made. If the SOA record is not returned but some other response is returned, this is a indication of a bad delegation. If the server fails to get a response to a SOA query, the Operator should make an A query for the zone, as some nameservers fail to respond to SOA queries but will respond to A queries.

3.1.2. Unknown / Unsupported Type Queries

Identifying servers that fail to respond to unknown or unsupported types can be done by making an initial DNS query for an A record, making a number of queries for an unallocated type, then making a query for an A record again. IANA maintains a registry of allocated types.

If the server responds to the first and last queries but fails to respond to the queries for the unallocated type, it is probably

faulty. The test should be repeated a number of times to eliminate the likelihood of a false positive due to packet loss.

3.1.3. DNS Flags

Some servers fail to respond to DNS queries with various DNS flags set, regardless of whether they are defined or still reserved. At the time of writing there are servers that fail to respond to queries with the AD bit set to 1 and servers that fail to respond to queries with the last reserved flag bit set.

3.1.4. Unknown DNS opcodes

The use of previously undefined opcodes is to be expected. Since the DNS was first defined two new opcodes have been added, UPDATE and NOTIFY.

NOTIMP is the expected rcode to an unknown or unimplemented opcode.

Note: while new opcodes will most probably use the current layout structure for the rest of the message there is no requirement that anything other than the DNS header match.

3.1.5. Recursive Queries

A non-recursive server is supposed to respond to recursive queries as if the RD bit is not set.

3.1.6. TCP Queries

All DNS servers are supposed to respond to queries over TCP [RFC7766]. Firewalls that drop TCP connection attempts, they should reset the connect attempt or send a ICMP/ICMPv6 administratively prohibited message. Dropping TCP connections introduces excessive delays to the resolution process.

Whether a server accepts TCP connections can be tested by first checking that it responds to UDP queries to confirm that it is up and operating, then attempting the same query over TCP. An additional query should be made over UDP if the TCP connection attempt fails to confirm that the server under test is still operating.

3.2. EDNS Queries

3.2.1. EDNS Queries - Version Independent

Identifying servers that fail to respond to EDNS queries can be done by first identifying that the server responds to regular DNS queries, followed by a series of otherwise identical queries using EDNS, then making the original query again. A series of EDNS queries is needed as at least one DNS implementation responds to the first EDNS query with FORMERR but fails to respond to subsequent queries from the same address for a period until a regular DNS query is made. The EDNS query should specify a UDP buffer size of 512 bytes to avoid false classification of not supporting EDNS due to response packet size.

If the server responds to the first and last queries but fails to respond to most or all of the EDNS queries, it is probably faulty. The test should be repeated a number of times to eliminate the likelihood of a false positive due to packet loss.

Firewalls may also block larger EDNS responses but there is no easy way to check authoritative servers to see if the firewall is mis-configured.

3.2.2. EDNS Queries - Version Specific

Some servers respond correctly to EDNS version 0 queries but fail to respond to EDNS queries with version numbers that are higher than zero. Servers should respond with BADVERS to EDNS queries with version numbers that they do not support.

Some servers respond correctly to EDNS version 0 queries but fail to set QR=1 when responding to EDNS versions they do not support. Such answers are discarded or treated as requests.

3.2.3. EDNS Options

Some servers fail to respond to EDNS queries with EDNS options set. Unknown EDNS options are supposed to be ignored by the server [RFC6891].

3.2.4. EDNS Flags

Some servers fail to respond to EDNS queries with EDNS flags set. Server should ignore EDNS flags they do not understand and should not add them to the response [RFC6891].

3.2.5. Truncated EDNS Responses

Some EDNS aware servers fail to include a OPT record when a truncated response is sent. A OPT record is supposed to be included in a truncated response [RFC6891].

Some EDNS aware server fail to honour the advertised EDNS buffer size and send over sized responses.

3.2.6. DNSSEC

Servers should be checked to see if they support DNSSEC. Servers should also be checked to see if they support DNSSEC with EDNS.

3.2.7. EDNS over TCP

Some EDNS aware servers incorrectly limit the TCP response sizes to the advertised UDP response size.

4. Firewalls and Load Balancers

Firewalls and load balancers can affect the externally visible behaviour of a nameserver. Tests for conformance should to be done from outside of any firewall so that the system as a whole is tested.

Firewalls and load balancers should not drop DNS packets that they don't understand. They should either pass the packets or generate an appropriate error response.

Requests for unknown query types is normal client behaviour and should not be construed as an attack. Nameservers have always been expected to be able to handle such queries.

Requests for unknown query classes is normal client behaviour and should not be construed as an attack. Nameservers have always been expected to be able to handle such queries.

Requests with unknown opcodes is normal client behaviour and should not be construed as an attack. Nameservers have always been expected to be able to handle such queries.

Requests with unassigned flags set (DNS or EDNS) is expected client behaviour and should not be construed as an attack. The behaviour for unassigned flags is to ignore them in the request and to not set them in the response. Dropping DNS / EDNS packets with unassigned flags makes it difficult to deploy extensions that make use of them due to the need to reconfigure and update firewalls.

Requests with unknown EDNS options is expected client behaviour and should not be construed as an attack. The correct behaviour for unknown EDNS options is to ignore there presence when constructing a reply.

Requests with unknown EDNS versions is expected client behaviour and should not be construed as an attack. The correct behaviour for unknown EDNS versions is to return BADVERS along with the highest EDNS version the server supports. Dropping EDNS packet breaks EDNS version negotiation.

Firewalls should not assume that there will only be a single response message to a requests. There have been proposals to use EDNS to signal that multiple DNS messages be returned rather than a single UDP message that is fragmented at the IP layer.

However, there may be times when a nameserver mishandles messages with a particular flag, EDNS option, EDNS version field, opcode, type or class field or combination there of to the point where the integrity of the nameserver is compromised. Firewalls should offer the ability to selectively reject messages with an appropriately constructed response based on all these fields while awaiting a fix from the nameserver vendor.

DNS and EDNS in particular is designed to allow clients to be able to use new features against older servers without having to validate every option. Indiscriminate blocking of messages breaks that design.

5. Scrubbing Services

Scrubbing services, like firewalls, can affect the externally visible behaviour of a nameserver. If a operator uses a scrubbing service, they should check that legitimate queries are not being blocked.

Scrubbing services, unlike firewalls, are also turned on and off in response to denial of service attacks. One needs to take care when choosing a scrubbing service and ask questions like mentioned above.

Ideally, Operators should run these tests against a scrubbing service to ensure that these tests are not seen as attack vectors.

6. Whole Answer Caches

Whole answer caches take a previously constructed answer and return it to a subsequent query for the same qname, qtype and qclass, just updating the query id field and possibly the qname to match the incoming query to avoid constructing each response individually.

Whole answer caches can return the wrong response to a query if they do not take all of the attributes of the query into account, rather than just some of them e.g. qname, qtype and qclass. This has implications when testing and with overall protocol compliance.

Two current examples are:

- Whole answer caches that ignore the EDNS version field which results in incorrect answers to non EDNS version 0 queries being returned if they were preceded by a EDNS version 0 query for the same name and type.

- Whole answer caches that ignore the EDNS options in the query resulting in options only working some of the time and/or options being returned when not requested.

7. Response Code Selection

Choosing the correct response code when responding to DNS queries is important. Just because a DNS qtype is not implemented does not mean that NOTIMP is the correct response code to return. Response codes should be chosen considering how clients will handle them.

For unimplemented opcodes NOTIMP is the expected response code. For example, a new opcode could change the message format by extending the header or changing the structure of the records etc. This may result in FORMERR being returned though NOTIMP would be more correct.

Unimplemented type codes, Name Error (NXDOMAIN) and NOERROR (no data) are the expected response codes. A server is not supposed to serve a zone which contains unsupported types ([RFC1034]) so the only thing left is return if the QNAME exists or not. NOTIMP and REFUSED are not useful responses as they force the clients to try the other authoritative servers for a zone looking for a server which will answer the query.

Meta queries may be the exception but these need to be thought about on a case by case basis.

If the server supports EDNS and receives a query with an unsupported EDNS version, the correct response is BADVERS [RFC6891].

If the server does not support EDNS at all, FORMERR and NOTIMP are the expected error codes. That said a minimal EDNS server implementation requires parsing the OPT records and responding with an empty OPT record. There is no need to interpret any EDNS options present in the request as unsupported EDNS options are expected to be ignored [RFC6891].

8. Testing

Testing is divided into two sections. Basic DNS which all servers should meet and Extended DNS which should be met by all servers that support EDNS (a server is deemed to support EDNS if it gives a valid EDNS response to any EDNS query). If a server does not support EDNS it should still respond to all the tests.

It is advisable to run all of the tests below in parallel so as to minimise the delays due to multiple timeouts when the servers do not respond. There are 16 queries directed to each nameserver assuming no packet loss testing different aspects of Basic DNS and EDNS.

The tests below use dig from BIND 9.11.0.

8.1. Testing - Basic DNS

This first set of tests cover basic DNS server behaviour and all servers should pass these tests.

8.1.1. Is The Server Configured For The Zone?

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set and without EDNS.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may also be set [RFC1034]. We do not expect a OPT record to be returned [RFC6891].

Verify the server is configured for the zone:

```
dig +noedns +noad +norec soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: flag: aa to be present
expect: flag: rd to NOT be present
expect: flag: ad to NOT be present
expect: the OPT record to NOT be present
```

8.1.2. Testing Unknown Types

Ask for the TYPE1000 record at the zone's name. This query is made with no DNS flag bits set and without EDNS. TYPE1000 has been chosen for this purpose as IANA is unlikely to allocate this type in the

near future and it is not in type space reserved for end user allocation.

We don't expect any records to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may also be set [RFC1034]. We do not expect a OPT record to be returned [RFC6891].

Check that queries for an unknown type work:

dig +noedns +noad +norec type1000 $zone @$server

expect: status: NOERROR
expect: an empty answer section.
expect: flag: aa to be present
expect: flag: rd to NOT be present
expect: flag: ad to NOT be present
expect: the OPT record to NOT be present

That new types are to be expected is specified in Section 3.6, [RFC1035]. Servers that don't support a new type are expected to reject a zone that contains a unsupported type as per Section 5.2, [RFC1035]. This means that a server that does load a zone can answer questions for unknown types with NOERROR or NXDOMAIN as per Section 4.3.2, [RFC1034]. [RFC6895] later reserved distinct ranges for meta and data types which allows servers to be definitive about whether a query should be answerable from zone content or not.

8.1.3. Testing Header Bits

8.1.3.1. Testing CD=1 Queries

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with only the CD DNS flag bit set and all other DNS bits clear and without EDNS.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response. We do not expect a OPT record to be returned.

If the server supports DNSSEC, CD should be set in the response [RFC4035] otherwise CD should be clear [RFC1034].

Check that queries with CD=1 work:

dig +noedns +noad +norec +cd soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: flag: aa to be present
expect: flag: rd to NOT be present
expect: flag: ad to NOT be present
expect: the OPT record to NOT be present

CD use in queries is defined in [RFC4035].

8.1.3.2. Testing AD=1 Queries

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with only the AD DNS flag bit set and all other DNS bits clear and without EDNS.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response. We do not expect a OPT record to be returned.

If the server supports DNSSEC, AD may be set in the response [RFC6840] otherwise AD should be clear [RFC1034].

Check that queries with AD=1 work:

dig +noedns +norec +ad soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: flag: aa to be present
expect: flag: rd to NOT be present
expect: the OPT record to NOT be present

AD use in queries is defined in [RFC6840].

8.1.3.3. Testing Reserved Bit

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with only the final reserved DNS flag bit set and all other DNS bits clear and without EDNS.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may be set. The final reserved bit must not

be set [RFC1034]. We do not expect a OPT record to be returned [RFC6891].

Check that queries with the last unassigned DNS header flag work and that the flag bit is not copied to the response:

dig +noedns +noad +norec +zflag soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: MBZ to NOT be in the response
expect: flag: aa to be present
expect: flag: rd to NOT be present
expect: flag: ad to NOT be present
expect: the OPT record to NOT be present

MBZ (Must Be Zero) presence indicates the flag bit has been incorrectly copied. See Section 4.1.1, [RFC1035] "Z Reserved for future use. Must be zero in all queries and responses."

8.1.4. Testing Unknown Opcodes

Construct a DNS message that consists of only a DNS header with opcode set to 15 (currently not allocated), no DNS header bits set and empty question, answer, authority and additional sections.

Check that new opcodes are handled:

dig +noedns +noad +opcode=15 +norec +header-only @$server

expect: status: NOTIMP
expect: SOA record to NOT be present
expect: flag: aa to NOT be present
expect: flag: rd to NOT be present
expect: flag: ad to NOT be present
expect: the OPT record to NOT be present

As unknown opcodes have no definition, including packet format other than there must be a DNS header present (QR, OPCODE and RCODE are the only header fields that need to be common across all opcodes, everything else in the header can potentially be redefined), there is only one possible rcode that make sense to return to a request with a unknown opcode and that is NOTIMP.

8.1.5. Testing Recursive Queries

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with only the RD DNS flag bit set and without EDNS.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA, QR and RD bits to be set in the response, RA may also be set [RFC1034]. We do not expect a OPT record to be returned [RFC6891].

Check that recursive queries work:

dig +noedns +noad +rec soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: flag: aa to be present
expect: flag: rd to be present
expect: flag: ad to NOT be present
expect: the OPT record to NOT be present

8.1.6. Testing TCP

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set and without EDNS. This query is to be sent using TCP.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may also be set [RFC1034]. We do not expect a OPT record to be returned [RFC6891].

Check that TCP queries work:

dig +noedns +noad +norec +tcp soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: flag: aa to be present
expect: flag: rd to NOT be present
expect: flag: ad to NOT be present
expect: the OPT record to NOT be present

The requirement that TCP be supported is defined in [RFC7766].

8.2. Testing - Extended DNS

The next set of test cover various aspects of EDNS behaviour. If any of these tests succeed, then all of them should succeed. There are servers that support EDNS but fail to handle plain EDNS queries correctly so a plain EDNS query is not a good indicator of lack of EDNS support.

8.2.1. Testing Minimal EDNS

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 0 is used without any EDNS options or EDNS flags set.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags present in the response. The EDNS version field should be zero and there should be no EDNS options present [RFC6891].

Check that plain EDNS queries work:

```
dig +nocookie +edns=0 +noad +norec soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: a OPT record to be present in the additional section
expect: EDNS Version 0 in response
expect: flag: aa to be present
expect: flag: ad to NOT be present
```

+nocookie disables sending a EDNS COOKIE option in which is on by default in BIND 9.11.0.

8.2.2. Testing EDNS Version Negotiation

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 1 is used without any EDNS options or EDNS flags set.

We expect the SOA record for the zone to NOT be returned in the answer section with the extended rcode set to BADVERS and the QR bit to be set in the response, RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags present in the response. The EDNS version field should be zero as EDNS versions other than 0 are yet to be specified and there should be no EDNS options present [RFC6891].

Check that EDNS version 1 queries work (EDNS supported):

dig +nocookie +edns=1 +noednsneg +noad +norec soa $zone @$server

expect: status: BADVERS
expect: the SOA record to NOT be present in the answer section
expect: a OPT record to be present in the additional section
expect: EDNS Version 0 in response
expect: flag: aa to NOT be present
expect: flag: ad to NOT be present

Only EDNS Version 0 is currently defined so the response should always be a 0 version. This will change when EDNS version 1 is defined. BADVERS is the expected rcode if EDNS is supported as per Section 6.1.3, [RFC6891].

8.2.3. Testing Unknown EDNS Options

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 0 is used without any EDNS flags. A EDNS option is present with a value from the yet to be assigned range. The unassigned value chosen is 100 and will need to be adjusted when IANA assigns this value formally.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags present in the response. The EDNS version field should be zero as EDNS versions other than 0 are yet to be specified and there should be no EDNS options present as unknown EDNS options are supposed to be ignored by the server [RFC6891].

Check that EDNS queries with an unknown option work (EDNS supported):

dig +nocookie +edns=0 +noad +norec +ednsopt=100 soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: a OPT record to be present in the additional section
expect: OPT=100 to NOT be present
expect: EDNS Version 0 in response
expect: flag: aa to be present
expect: flag: ad to NOT be present

Unknown EDNS options are supposed to be ignored, Section 6.1.2, [RFC6891].

8.2.4. Testing Unknown EDNS Flags

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 0 is used without any EDNS options. A unassigned EDNS flag bit is set (0x40 in this case).

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags present in the response as unknown EDNS flags are supposed to be ignored. The EDNS version field should be zero and there should be no EDNS options present [RFC6891].

Check that EDNS queries with unknown flags work (EDNS supported):

dig +nocookie +edns=0 +noad +norec +ednsflags=0x40 soa $zone @$server

expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: a OPT record to be present in the additional section
expect: MBZ not to be present
expect: EDNS Version 0 in response
expect: flag: aa to be present
expect: flag: ad to NOT be present

MBZ (Must Be Zero) presence indicates the flag bit has been incorrectly copied as per Section 6.1.4, [RFC6891].

8.2.5. Testing EDNS Version Negotiation With Unknown EDNS Flags

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 1 is used without any EDNS options. A unassigned EDNS flag bit is set (0x40 in this case).

We expect the SOA record for the zone to NOT be returned in the answer section with the extended rcode set to BADVERS and the QR bit to be set in the response, RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags present in the response as unknown EDNS flags are supposed to be ignored. The EDNS version field should be zero as EDNS versions other than 0 are yet to be specified and there should be no EDNS options present [RFC6891].

Check that EDNS version 1 queries with unknown flags work (EDNS supported):

```
dig +nocookie +edns=1 +noednsneg +noad +norec +ednsflags=0x40 soa \
    $zone @$server
```

```
expect: status: BADVERS
expect: SOA record to NOT be present
expect: a OPT record to be present in the additional section
expect: MBZ not to be present
expect: EDNS Version 0 in response
expect: flag: aa to NOT be present
expect: flag: ad to NOT be present
```

+noednsneg disables EDNS version negotiation in DiG; MBZ (Must Be Zero) presence indicates the flag bit has been incorrectly copied.

8.2.6. Testing EDNS Version Negotiation With Unknown EDNS Options

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 1 is used. A unknown EDNS option is present (option code 100 has been chosen).

We expect the SOA record for the zone to NOT be returned in the answer section with the extended rcode set to BADVERS and the QR bit to be set in the response, RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags present in the response. The EDNS version field should be zero as EDNS versions other than 0 are yet to be specified and there should be no EDNS options present [RFC6891].

Check that EDNS version 1 queries with unknown options work (EDNS supported):

```
dig +nocookie +edns=1 +noednsneg +noad +norec +ednsopt=100 soa \
    $zone @$server
```

```
expect: status: BADVERS
expect: SOA record to NOT be present
expect: a OPT record to be present in the additional section
expect: OPT=100 to NOT be present
expect: EDNS Version 0 in response
expect: flag: aa to be present
expect: flag: ad to NOT be present
```

+noednsneg disables EDNS version negotiation in DiG.

8.2.7. Testing DNSSEC Queries

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 0 is used without any EDNS options. The only EDNS flag set is DO.

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, AD may be set in the response if the server supports DNSSEC otherwise it should be clear. RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags other than DO present in the response which should be present if the server supports DNSSEC. The EDNS version field should be zero and there should be no EDNS options present [RFC6891].

Check that a DNSSEC queries work (EDNS supported):

```
dig +nocookie +edns=0 +noad +norec +dnssec soa $zone @$server
```

```
expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: a OPT record to be present in the additional section
expect: DO=1 to be present if a RRSIG is in the response
expect: EDNS Version 0 in response
expect: flag: aa to be present
```

DO=1 should be present if RRSIGs are returned as they indicate that the server supports DNSSEC. Servers that support DNSSEC are supposed to copy the DO bit from the request to the response as per [RFC3225].

8.2.8. Testing EDNS Version Negotiation With DNSSEC

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 1 is used without any EDNS options. The only EDNS flag set is DO.

We expect the SOA record for the zone to NOT be returned in the answer section with the rcode set to BADVERS and the only the QR bit and possibly the RA bit to be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags other than DO present in the response which should be present if the server supports DNSSEC. The EDNS version field should be zero and there should be no EDNS options present [RFC6891].

Check that EDNS version 1 DNSSEC queries work (EDNS supported):

```
dig +nocookie +edns=1 +noednsneg +noad +norec +dnssec soa \
    $zone @$server
```

```
expect: status: BADVERS
expect: SOA record to NOT be present
expect: a OPT record to be present in the additional section
expect: DO=1 to be present if the EDNS version 0 DNSSEC query test
        returned DO=1
expect: EDNS Version 0 in response
expect: flag: aa to NOT be present
```

+noednsneg disables EDNS version negotiation in DiG.

8.2.9. Testing With Multiple Defined EDNS Options

Ask for the SOA record of the zone the server is nominally configured to serve. This query is made with no DNS flag bits set. EDNS version 0 is used. A number of defined EDNS options are present (NSID [RFC5001], DNS COOKIE [RFC7873], EDNS Client Subnet [RFC7871] and EDNS Expire [RFC7314]).

We expect the SOA record for the zone to be returned in the answer section with the rcode set to NOERROR and the AA and QR bits to be set in the response, RA may also be set [RFC1034]. We expect a OPT record to be returned. There should be no EDNS flags present in the response. The EDNS version field should be zero. Any of the requested EDNS options supported by the server and permitted server configuration may be returned [RFC6891].

Check that EDNS queries with multiple defined EDNS options work:

```
dig +edns=0 +noad +norec +cookie +nsid +expire +subnet=0.0.0.0/0 \
    soa $zone @$server
```

```
expect: status: NOERROR
expect: the SOA record to be present in the answer section
expect: a OPT record to be present in the additional section
expect: EDNS Version 0 in response
expect: flag: aa to be present
expect: flag: ad to NOT be present
```

8.3. When EDNS Is Not Supported

If EDNS is not supported by the nameserver, we expect a response to all the above queries. That response may be a FORMERR or NOTIMP error response or the OPT record may just be ignored.

Some nameservers only return a EDNS response when a particular EDNS option or flag (e.g. DO=1) is present in the request. This behaviour is not compliant behaviour and may hide other incorrect behaviour from the above tests. Re-testing with the triggering option / flag present will expose this misbehaviour.

9. Remediation

Name server operators are generally expected to test their own infrastructure for compliance to standards. The above tests should be run when new systems are brought online, and should be repeated periodically to ensure continued interoperability.

Domain registrants who do not maintain their own DNS infrastructure are entitled to a DNS service that conforms to standards and interoperates well. Registrants who become aware that their DNS operator does not have a well maintained or compliant infrastructure should insist that their service provider correct issues, and switch providers if they do not.

In the event that an operator experiences problems due to the behaviour of name servers outside their control, the above tests will help in narrowing down the precise issue(s) which can then be reported to the relevant party.

If contact information for the operator of a misbehaving name server is not already known, the following methods of communication could be considered:

- the RNAME of the zone authoritative for the name of the misbehaving server
- the RNAME of zones for which the offending server is authoritative
- administrative or technical contacts listed in the registration information for the parent domain of the name of the misbehaving server, or for zones for which the name server is authoritative
- the registrar or registry for such zones
- DNS-specific operational fora (e.g. mailing lists)

Operators of parent zones may wish to regularly test the authoritative name servers of their child zones. However, parent operators can have widely varying capabilities in terms of notification or remediation depending on whether they have a direct relationship with the child operator. Many TLD registries, for example, cannot directly contact their registrants and may instead

need to communicate through the relevant registrar. In such cases it may be most efficient for registrars to take on the responsibility for testing the name servers of their registrants, since they have a direct relationship.

When notification is not effective at correcting problems with a misbehaving name server, parent operators can choose to remove NS record sets (and glue records below) that refer to the faulty server. This should only be done as a last resort and with due consideration, as removal of a delegation can have unanticipated side effects. For example, other parts of the DNS tree may depend on names below the removed zone cut, and the parent operator may find themselves responsible for causing new DNS failures to occur.

10. Security Considerations

Testing protocol compliance can potentially result in false reports of attempts to break services from Intrusion Detection Services and firewalls. None of the tests listed above should break nominally EDNS compliant servers. None of the tests above should break non EDNS servers. All the tests above are well formed, though not necessarily common, DNS queries.

Relaxing firewall settings to ensure EDNS compliance could potentially expose a critical implementation flaw in the nameserver. Nameservers should be tested for conformance before relaxing firewall settings.

When removing delegations for non-compliant servers there can be a knock on effect on other zones that require these zones to be operational for the nameservers addresses to be resolved.

11. IANA Considerations

There are no actions for IANA.

12. References

12.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <http://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC3225] Conrad, D., "Indicating Resolver Support of DNSSEC", RFC 3225, DOI 10.17487/RFC3225, December 2001, <http://www.rfc-editor.org/info/rfc3225>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <http://www.rfc-editor.org/info/rfc4035>.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, DOI 10.17487/RFC6840, February 2013, <http://www.rfc-editor.org/info/rfc6840>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <http://www.rfc-editor.org/info/rfc6891>.

[RFC6895] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 6895, DOI 10.17487/RFC6895, April 2013, <http://www.rfc-editor.org/info/rfc6895>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <http://www.rfc-editor.org/info/rfc7766>.

12.2. Informative References

[RFC5001] Austein, R., "DNS Name Server Identifier (NSID) Option", RFC 5001, DOI 10.17487/RFC5001, August 2007, <http://www.rfc-editor.org/info/rfc5001>.

[RFC7314] Andrews, M., "Extension Mechanisms for DNS (EDNS) EXPIRE Option", RFC 7314, DOI 10.17487/RFC7314, July 2014, <http://www.rfc-editor.org/info/rfc7314>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <http://www.rfc-editor.org/info/rfc7871>.

[RFC7873] Eastlake 3rd, D. and M. Andrews, "Domain Name System (DNS) Cookies", RFC 7873, DOI 10.17487/RFC7873, May 2016, <http://www.rfc-editor.org/info/rfc7873>.

Author's Address

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

Email: marka@isc.org