EDNS (in) Compatibility

October, 2015
DNS-OARC, Montreal, Canada
Vicky Risk, ISC
New Applications introduce new (unknown) options

---

*IETF Draft of edns-client-subnet*

Below is a copy of the most recent IETF draft for edns-client-subnet.

dnsop
Internet-Draft
Intended status: Informational
Expires: May 19, 2015
EDNS Version 1 (expired draft)

“It is impracticable to deploy new EDNS options, with EDNS version 0, on a global scale due to inconsistent server behaviour in deployed servers when a EDNS option is present in the query.”
Experiment surveyed ...

1. Root and TLD servers using a series of dig queries
2. DNS servers for Alexa Top 1000 sites
3. DNS servers for Alexa Bottom 1000 of the top 1M sites see ednscomp.isc.org for details of queries + expected results
4. GOV servers in the Alexa Top 1M sites
5. AU servers in the Alexa Top 1M sites
EDNS Aware Servers
(Sept 30, 2015)

90%++ Awareness = Success!!

© 2015 ISC

http://ednscomp.isc.org/compliance/summary.html
EDNS Aware Servers and Full EDNS Compliance
(Sept 30, 2015)

60%++ Compliance = Not Success

<table>
<thead>
<tr>
<th>Category</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLD</td>
<td>100%</td>
</tr>
<tr>
<td>Alexa Top</td>
<td>96%</td>
</tr>
<tr>
<td>Alexa Bottom</td>
<td>90%</td>
</tr>
<tr>
<td>GOV</td>
<td>98%</td>
</tr>
<tr>
<td>AU</td>
<td>97%</td>
</tr>
</tbody>
</table>

http://ednscomp.isc.org/compliance/summary.html
Problems seen

- OPT only returned when DO=1 is present in the request
- BADVER not returned to EDNS (1)
- NOTIMP, FORMERR, BADVERS returned when a EDNS option is present
- NOTIMP, FORMERR, BADVERS returned when a EDNS Z flag is present
- EDNS (1) queries being dropped
- EDNS queries with a Z bit being dropped
- EDNS Z bits in queries echoed back
- TCP response size limited to EDNS UDP response size
- DO=1 not returned by DNSSEC aware servers
“dropping packets is just plain anti-social and always has been”
Unknown option -> disable EDNS

Signals that EDNS is not supported
Which breaks DNSSEC validation
TRENDS

September 2014 vs September 2015
Historical Data

Percentage of EDNS aware servers that handled unknown EDNS(0) flags correctly

Percentage of EDNS aware servers that handled unknown FQDN

Alexa .GOV Servers Response Rates

Percentage of EDNS aware servers that passed plain EDNS(0) check

© 2015 ISC
2014

EDNS Compliance by Function of EDNS Aware Servers - 21 Sep 2014

© 2015 ISC
EDNS Compliance by Function of EDNS Aware Servers - 30 Sep 2015

Data Subset

© 2015 ISC
# Trend by Problem

<table>
<thead>
<tr>
<th>Issue</th>
<th>Trend 2014 - 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDNS0</td>
<td>flat, slight decline in .AU</td>
</tr>
<tr>
<td>Truncated Response</td>
<td>4 of 5 improved slightly</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>all improved</td>
</tr>
<tr>
<td>Unknown Option</td>
<td>3 of 5 improved slightly</td>
</tr>
<tr>
<td>Unknown Flag</td>
<td>significant improvement – esp in TLDs by 8%</td>
</tr>
<tr>
<td>EDNS1</td>
<td>significant recent improvement</td>
</tr>
<tr>
<td>Fully Compliant</td>
<td>significant improvement est. in TLD and Alexa top 1000</td>
</tr>
</tbody>
</table>
August 7th

Percentage of EDNS aware servers that handled unknown EDNS(0) flags correctly

firewall blocking EDNS fixed
Sept 30th

Percentage of EDNS aware servers that passed all EDNS compliance tests

servers that were ignoring the EDNS version field
Why should you care?

1. Most recursive resolvers now support EDNS. Lack of EDNS support in authoritative servers results in additional queries being made as the recursive servers need to retry with plain DNS and results in slower DNS resolution.

2. Not answering EDNS queries is particularly bad as that is indistinguishable from packet loss.

3. Incorrect EDNS behaviour when presented with unknown EDNS versions and EDNS options can result in DNS resolution failures and/or DNSSEC validation failures.

4. Failure to run fully EDNS compliant nameservers will make it hard to deploy developments like DNS COOKIES.
What we have done so far

- Put up a self-test web site at www.ednscomp.isc.org
- Contacted various operators who seemed to have problems, based on our testing
- Asked Casey Deccio to add this test to DNSViz – https://github.com/dnsviz/dnsviz/releases/tag/v0.4.0-beta4
- Presented at IETF on this problem (3/15)
- NOW – presenting at OARC and NANOG
Please

Test your nameserver to ensure it:

1. Supports EDNS version negotiation.
2. Handles unknown EDNS options.
3. Handles unknown EDNS flags.

(Switch has put up a site to measure compliance in .ch and .li)
Summary

- DNS cookies are disabled by default in BIND 9.10. We plan to enable them in 9.11, by default.
- Is there anything further the community wants to do to prevent DNSSEC failures?
References

- http://ednscomp.isc.org