EDNS Compliance Status of Resolvers

Jeisson Sanchez
jeisson@niclabs.cl
What is EDNS?

Extension mechanisms for DNS: RFC 6891 in 2013

Defines a backward-compatible mechanisms to deploy new DNS features

- Extra data space for additional flags
- DNS messages larger than 512 bytes
- Extended response codes
- Among others…
Problem – Solution with EDNS

But there are some operational workarounds with EDNS…

• Poorly firewall rules blocking valid traffic
• Obsolete DNS software

Summary: Bad implementations of DNS not following standards
CONTRIBUTION

What is EDNS status resolvers before and after DNS Flagday?

TEST

• 19061 Resolvers
• VMs: Ubuntu 16.04
• Dig and Pydig [1]: DNS query tool written in Python
• Each test was performed 5 times
• Tests 1 & 2 are based on I-D “A Common Operational Problem in DNS Servers - Failure To Respond”

[1]. Author: Shumon Huque. Source: https://github.com/shuque/pydig
Basic Test

1

Tests

- Chaos: version.bind
  - Whois: ASN, ISP & location
    - -x: Name server

  Queries
    - +edns
    - +noedns
    - +edns=0
    - +edns=1

  EDNS

  Version EDNS0

  Yes
  - Answer without additional OPT code. Analysis of rCODE & flags

  No
  - Answer OPT code, rCODE, no EDNS compliance dismiss other tests

- Whois
  - -x

A
Edns aware

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

- NOERROR
- REFUSED
- FORMERR
- SERVFAIL
- NXDOMAIN
- NOTIMP

Number of servers
Algorithm EDNS classification

Number of servers

- EDNS0
- OK
- NOEDNS0
- TIMEOUT
1. Basic Test
   - Normal operation of resolvers and basic information

2. Edns and DNSSEC
   - Edns version and complete chain of validation

3. Some extensions
   - Client Subnet, Chain query, EDNS TCP Keepalive, among others

4. DNSFlag Day
EDNS and DNSSEC test
Testing Edns1

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

- OK
- BADVERSION
- REFUSED
- NOERROR
- NOOPT
- TIMEOUT

Number of servers
Testing DNSSEC

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

Number of servers

- REFUSED: 9000
- NOERROR: 9000
- TIMEOUT: 2000
- FORMERR: 0
- SERVFAIL: 0
- NXDOMAIN: 0
- NOTIMP: 0
1. Basic Test
   Normal operation of resolvers and basic information
2. Edns and DNSSEC
   Edns version, negotiation and chain of validation
3. Some extensions
   Client Subnet, Chain query, expire option, among others
4. DNSFlag Day
Chain query in DNS - RFC 7901

pydig +tcp +chainquery soa $zone @$server

Number of servers

- REFUSED
- NORESPONSE
- NOERROR
- FORMERR
- SERVFAIL
- NXDOMAIN
- NOTIMP
Client Subnet in DNS- RFC 7871

```
pydig +subnet=addr $zone @$server
```

![Graph showing the number of servers for different DNS responses](image-url)

- **REFUSED**: The highest number of servers, indicating a high number of refused responses.
- **NORESPONSE**: Moderate number of servers, indicating some non-response.
- **NOERROR**: Number of servers is close to REFUSED, suggesting a substantial number of correct responses.
- **FORMERR**: Lowest number of servers, indicating few form errors.
- **SERVFAIL**: Significantly fewer servers, indicating a smaller number of service failures.
- **NXDOMAIN**: Little to no servers, indicating no records for domain names.
- **NOTIMP**: Least number of servers, indicating a low occurrence of not implemented responses.
EDNS comparison

DNS FLAG DAY
Comparison Minimal Edns

- NOERROR
- REFUSED
- FORMERR
- SERVFAIL
- NXDOMAIN
- NOTIMP

Number of Servers:

- AFTER
- BEFORE
Client Subnet in DNS - RFC 7871

- REFUSED
- NORESPONSE
- NOERROR
- FORMERR
- SERVFAIL
- NXDOMAIN
- NOTIMP

Number of servers

- AFTER
- BEFORE

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

NIC CHILE
RESEARCH LABS
### OPTcodes comparison

<table>
<thead>
<tr>
<th>OPTcode</th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>170 serv</td>
<td>413 serv</td>
</tr>
<tr>
<td>8</td>
<td>265 serv</td>
<td>631 serv</td>
</tr>
<tr>
<td>12</td>
<td>478 serv</td>
<td>792 serv</td>
</tr>
</tbody>
</table>

### Summary Algorithm classification

<table>
<thead>
<tr>
<th>Classification</th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>714 serv</td>
<td>1084 serv</td>
</tr>
<tr>
<td>Warnings</td>
<td>15813 serv</td>
<td>16518 serv</td>
</tr>
<tr>
<td>Not EDNS</td>
<td>2534 serv</td>
<td>1459 serv</td>
</tr>
</tbody>
</table>
Thanks!

Questions?

https://github.com/niclabs/testResolvers/tree/edns/resolvertests

jeisson@niclabs.cl