EDNS0 Deployment

Shane Kerr <shane@ca.afilias.info>
Joe Abley <jabley@ca.afilias.info>

DNSOP, IETF 72
Baile Átha Cliath, Éire
EDNS0

- Specified in RFC 2671, published in August 1999
- Provides an extension mechanism for DNS
- Widely deployed thanks to implementation in software such as BIND9, NSD
- Notably not supported in DJBDNS, PowerDNS
Deployment

• DNS operations folklore suggests that EDNS0 deployment is far from complete, and that serious proposals relating to the DNS cannot rely on its existence

• We decided to look at a sample of authority-only servers and see what we could see

• Work in Progress! Interim Results! Many Improvements Possible!
More Details

• draft-kerr-dnsop-edns0-penetration-00

• Work in Progress! Interim Results! Many Improvements Possible!
Methodology

• Take a number of TLD and TLD-ish zones, and harvest nameservers from the NS RRsets contained within

• list of zones in draft, includes some large gTLDs and a small collection of ccTLDs

• 13 million delegations, around 4000 unique servers
Methodology

• Send a query with EDNS0 to each server
• Look for an OPT record in the additional section of the response
  • if present, “EDNS0-capable”
  • if absent, “EDNS0-incapable”
  • if no reply, “unresponsive”
Methodology

- For those servers which we classified as “EDNS0-incapable”:
  - test to see whether a query with TCP transport succeeds
Methodology

• For those servers which were classified as “unresponsive”:
  • test UDP with no EDNS0
  • test TCP with no EDNS0
Interim Observations

- Of 407,011 nameservers tested
  - 332,992 (82%) were EDNS0-capable
  - 19,030 (4.7%) were EDNS0-incapable
  - 64,989 (16%) were unresponsive
Interim Observations

• Of the 19,030 servers which were EDNS0-incapable
  • 14,991 (79%) provided answers to queries sent over TCP
  • 4,039 (21%) did not respond to a query over TCP
Interim Observations

- Of the 64,989 unresponsive servers:
  - 807 (1.2%) responded to UDP queries without EDNS0, but not TCP
  - 919 (1.4%) responded to TCP queries without EDNS0, but not UDP
  - 5,326 (8.2%) respond over both UDP and TCP queries without EDNS0
Tentative Conclusion

• Of servers that are sufficiently non-broken that they will provide some kind of answer to some kind of client \((332,992 + 19,030 + 807 + 919 + 5,326 = 359,074)\)

• \(332,992 \text{ (92.7\%)}\) support UDP/EDNS0

• \(4,039 \text{ (1.1\%)}\) don’t support UDP/EDNS0, but support TCP without EDNS0

• \(22,043 \text{ (6.1\%)}\) support neither UDP/EDNS0 nor TCP
Further Work

• We can see many areas where the methodology here can be improved

• Several areas in which we think we can improve are shown in the draft

• Offers of additional source data, ideas, coffee, beer, most welcome