SANOG XIV

15-23 July 2009, Chennai, India

EDNS Fun

Gaurab Raj Upadhaya

- EDNS is an extension of the DNS protocol which allows DNS messages larger than 512 bytes over UDP, and expands the number of flags, label types and return codes available to the protocol. The version of EDNS specified by RFC 2671 is known as EDNS0

So..

```
; <<>> DiG 9.4.3-P1 <<>> +dnssec soa sanog.org
;; global options:  printcmd
;; connection timed out; no servers could be reached
Gaurab-Upadhayas-MacBook-Air:~ gaurab$ dig +dnssec soa sanog.org

; <<>> DiG 9.4.3-P1 <<>> +dnssec soa sanog.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 925
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;sanog.org.                     IN      SOA

;; ANSWER SECTION:
sanog.org.              3600    IN      SOA     ns-int.isc.org. hostmaster.isc.org. 2009071900 7200 3600 604800 3600
sanog.org.              3600    IN      RRSIG   SOA 5 2 3600 20090817233351 20090718233351 23988 sanog.org.
HQe7TPQcsOQIbuYfe1ymgRDbVusyVWV1tPY1PITRci/Gi4KGtdNAE2TU 3xjP4tfybH3/LDsMR5gBcTj/R/UFteKAgWTCdKoSzUMqwb/OlOuJ+c5d
JUOtaiBpPg642WY20HxkMEFiTwN6sGrBBngD61eLcuRxByqU8GbQ+szw W14=

;; AUTHORITY SECTION:
sanog.org.              3600    IN      NS      ns-ext.nrt1.isc.org.
sanog.org.              3600    IN      NS      ams.sns-pb.isc.org.
sanog.org.              3600    IN      NS      sfba.sns-pb.isc.org.
sanog.org.              3600    IN      NS      ord.sns-pb.isc.org.
sanog.org.              3600    IN      RRSIG   NS 5 2 3600 20090817233351 20090718233351 23988 sanog.org.
pzBvOxRSRHSiFKKSxaEwLwlufFOsdxdC38zg+1Tdkco2OSBfkgfQ3EPI SZ1xypNOFHQSavtrSyUuDvC/tSEDKTlDBExb+oVaZvcyb11dvc0XWsMc
XX77XzJLoGMBR5Y4UrV4+r4gGH64Ou5TznNShp5uXflGlN8Ycqmuml/O E98=

;; ADDITIONAL SECTION:
ams.sns-pb.isc.org.     24077   IN      A       199.6.1.30
ord.sns-pb.isc.org.     24077   IN      A       199.6.0.30
sfba.sns-pb.isc.org.    24077   IN      A       149.20.64.3
sfba.sns-pb.isc.org.    24077   IN      AAAA    2001:4f8:0:2::19
ams.sns-pb.isc.org.     24077   IN      RRSIG   A 5 4 43200 20090820204821 20090721204821 27624 isc.org.
tG9kPaiQa8KRuhJKJAe3iWR96jKpERoxhwfhGMPCQDs96ZjRsZ6HAlu9 TO7fEPOac/tWEjrzrhdRDshZS2/guhkuPfCA3zM4it2bErA1jRNB/huu
tnopsXmIzHjd3NbRITTMA1atxVMDDxprE6HIRcBE9vgteqvWZGJdMc4C whs=
ord.sns-pb.isc.org.     24077   IN      RRSIG   A 5 4 43200 20090820204821 20090721204821 27624 isc.org.
y58klMsz9S6lomseUIqewcxo1H9SxAmhAVpCBNWnBg4sKx67meuOruSZ dxoiBVXQCp+y4iEMtp7rWJa6Jto4pBDj6CeezAUzvnVjea3HC/D1NPgN
q4aOvLFNMc9AlC4UlEg82PalAAWDP1YT02uMP00DxrDFH4rd9ZZ4dBVd yWk=
sfba.sns-pb.isc.org.    24077   IN      RRSIG   A 5 4 43200 20090820204821 20090721204821 27624 isc.org. mp+zn01Lgf/
CikxOyV8YFGfusUKBrUWb50ET+xe5j1KhEs25dujCQNCj yRSGO6g2VgILw3Rid6nXgJmV7V8zkLsyzpHWXkXYG3F5LnVJ2we5jBpu +wIFPZdgsHr33DsK8y66vGd/
xO7pTckH+oiRDs1I9Q/TbcAFBPlhtTf0 zi0=
sfba.sns-pb.isc.org.    24077   IN      RRSIG   AAAA 5 4 43200 20090820204821 20090721204821 27624 isc.org.
HfUKSo2n5ZL1f6HpVCbISPrs4951ccrrq1pKvQ3y9XnQz0fmF6Gyz+on hp/E6MLGtWsYBQdrAxdzThWZBQ60T+yFuEL4lBPRmqqxQ+Y6VAlTbtZL
q4VM7TF7avEpht1aO8Was62eosMXQ2FA0+PBcHQushTGaBPTgchMYWiw uts=

;; Query time: 245 msec
;; SERVER: 204.152.184.76#53(204.152.184.76)
;; WHEN: Wed Jul 22 10:09:01 2009
;; MSG SIZE  rcvd: 1266
```

```
; <<>> DiG 8.3 <<>> +dnssec soa sanog.org
;; res options: init recurs defnam dnsrch dnssec
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44729
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1
;; QUERY SECTION:
;;      sanog.org, type = SOA, class = IN

;; ANSWER SECTION:
sanog.org.              1H IN SOA       ns-int.isc.org. hostmaster.isc.org. (
                                        2009071900      ; serial
                                        2H              ; refresh
                                        1H              ; retry
                                        1W              ; expiry
                                        1H )            ; minimum


;; AUTHORITY SECTION:
sanog.org.              1H IN NS        ord.sns-pb.isc.org.
sanog.org.              1H IN NS        sfba.sns-pb.isc.org.
sanog.org.              1H IN NS        ns-ext.nrt1.isc.org.
sanog.org.              1H IN NS        ams.sns-pb.isc.org.

;; ADDITIONAL SECTION:
; EDNS: version: 0, udp=4096, flags=0000

;; Total query time: 143 msec
;; FROM: ns.lahai.com to SERVER: default -- 127.0.0.1
;; WHEN: Wed Jul 22 09:17:04 2009
;; MSG SIZE  sent: 38  rcvd: 184
```

dig +short rs.dns-oarc.net txt

```
;; Truncated, retrying in TCP mode.
rst.x3997.rs.dns-oarc.net.
rst.x3985.x3997.rs.dns-oarc.net.
rst.x4023.x3985.x3997.rs.dns-oarc.net.
"204.152.184.14 sent EDNS buffer size 4096"
"204.152.184.14 DNS reply size limit is at least 4023 bytes"

--------------------------- Vs. ---------------------------------

rst.x486.rs.dns-oarc.net.
rst.x454.x486.rs.dns-oarc.net.
rst.x384.x454.x486.rs.dns-oarc.net.
"62.206.1.43 DNS reply size limit is at least 486 bytes"
"62.206.1.43 lacks EDNS, defaults to 512"
```

Look for EDNS blocking

- thanks