Upper limit values for DNS

draft-fujiwara-dnsop-dns-upper-limit-values-01

https://datatracker.ietf.org/doc/draft-fujiwara-dnsop-dns-upper-limit-values/

Kazunori Fujiwara, JPRS

OARC 43 Lightning talks

Upper limit values: Problem Statement

- Some parameters in DNS don't have clear upper limits
  - Number of Resource Records in an RRset
    - Number of RRSIG/DNSKEY/DS RRs in an RRSet
    - Number of NS, glue, …
  - Number of CNAME/DNAME chains
  - Number of levels of unrelated only delegations
  - DNS packet size (≦65535)
- Without upper limits,
  - Easy to attack DNS aimed at resource depletion or DoS
    - Just prepare long CNAME chains, large RRSets (many RRs) in a zone
  - Several attack methods have been reported
    - KeyTrap, Tsuname, several DoS attacks
- This draft proposes reasonable upper limits for DNS protocols
- Intended status is "Best Current Practice"

Possible (proposed) upper limits

Name	proposal	use cases	implementation
DNS message size (without PQC)	≦ 1400		≦ 1232 on UDP
Number of Resource Records in a RRSet	≦ 13	. / com NS	≦100 (BIND)
Number of NS RRs at a delegation	≦ 13	. / com NS	
Number of glue RRs at a delegation	≦ 26	com glue	
Number of DS RRs at a delegation	≦ 3	need research	
Number of DNSKEY RRs in a DNSKEY RRSet	≦ 6	need research	
Number of RRSIG RRs for each name and type	≦ 2	need research	≦8 (Unbound)
Number of levels of unrelated only delegations	≦ 2	need research	
Number of CNAME/DNAME chains	≦ 3	10	≦11 (Unbound)

Recursive resolvers MAY/SHOULD respond with a name resolution error (Server Failure)
if they receive responses from authoritative servers that exceed these limits.

Request

- This draft proposes aggressive upper limits in order to advance discussions on determining upper limit values in DNS protocol.

- This proposal is one countermeasure to yesterday's "Security Discussion Panel 1"

- Please read draft-fujiwara-dnsop-dns-upper-limit-values-01 and comment to dnsop@ietf.org
  - https://datatracker.ietf.org/doc/draft-fujiwara-dnsop-dns-upper-limit-values/