draft-fujiwara-dnsop-additional-answers-00

K. Fujiwara

IETF 100 dnsop WG

Differences from draft-wkumari-dnsop-multiple-responses

- Authoritative name server software developers choose additional records
  - Without configuration
  - or system wide config: like “minimal-responses”
  - Like MX, SRV responses on BIND 9, NSD
    - They add mail exchange A/AAAA in additional sec.
- Aggressive appending NSEC/NSEC3 RRs
  - To generate NODATA/NXDOMAIN responses by RFC 8198

Background

- DNS standards allow for supplemental information to be included in the “additional” section of the DNS response
  - Existing implementations already add MX mail exchange A/AAAA or SRV Target A/AAAA
  - Developers know well
- DNSSEC guarantees that these additional records will be accepted/cached (RFC 2181)
- Validating resolvers can synthesize NODATA/NXDOMAIN responses using cached NSEC* RRs (RFC 8198)

Proposal of additional-answers

- Authoritative name server software developers choose query/answer and additional records pairs
  - The draft proposes good pairs
- To increase the probability that these extra data will actually be useful for resolvers,
  - The query has DNSSEC OK bit set
  - Additional records are signed by DNSSEC
  - Additional records may contain NSEC* RRs for the query and other related names
  - Responses with additional records fit in required response size

Additional answer pairs

Query:	additional answers
• name A:	name AAAA/NSEC*
• name AAAA:	name A/NSEC*
• name MX:	mail_exchange A/AAAA/NSEC*
• name SRV:	target_host A/AAAA/NSEC*
• name A/AAAA:	_443._tcp.name TLSA/NSEC*
• _443._tcp.name TLSA:	name A/AAAA/NSEC*

TLSA / MX / SRV pairs have different names.

NSEC* means NSEC or matching NSEC3

Experimental implementation

- http://member.wide.ad.jp/~fujiwara/files/nsd-always-add-a_aaaa_nsec.diff
- Add a code at add_rrset() in nsd/query.c

```
add_rrset(…) {
….
    switch (rrset_rrtype(rrset)) {
…
    case TYPE_A:
                rrset2 = domain_find_rrset(owner, query->zone, TYPE_AAAA);
                if (rrset2) {
                    answer_add_rrset(answer, ADDITIONAL_A_SECTION, owner, rrset2);
                } else {
                    answer_nodata(query, answer, owner); // add NSEC* (and SOA)
                }
                break;
….
```

Multiple response proposals

- draft-vavrusa-dnsop-aaaa-for-free
  - Additional AAAA in **answer section**
- draft-wkumari-dnsop-multiple-responses
  - **Pseudo RR** controls additional RRs
- draft-fujiwara-additional-answers
  - **Developers** choose additional RRs (+**NSEC***)
- draft-bellis-dnsext-multi-qtypes
  - New EDNS option carries additional **qtypes**
- draft-yao-dnsop-accompanying-questions
  - New EDNS option carries additional **qnames, qtypes, rcodes**

Comparison of proposals

Draft	additional answers	multiple responses	aaaa for free	multi qtypes	Accompanying questions
Protocol change	No	No	Yes?	Yes	Yes
Code size	little	some	little	large?	large?
Resolver modification	No	No	Yes?	Yes	Yes
Config complexity	No	Yes	No	No	No
Multiple names	Yes	Yes	No	No	Yes
Multiple types	Yes	Yes	AAAA	Yes	Yes
Multiple rcodes	(NSEC*)	---	---	---	Yes
Negative response	Yes	No	No	Yes	Yes
Fat response if	always	config	always	query	query
Stub support ?	No	No	?	possible	possible
Deployment	easy	easy	gradual	gradual	gradual