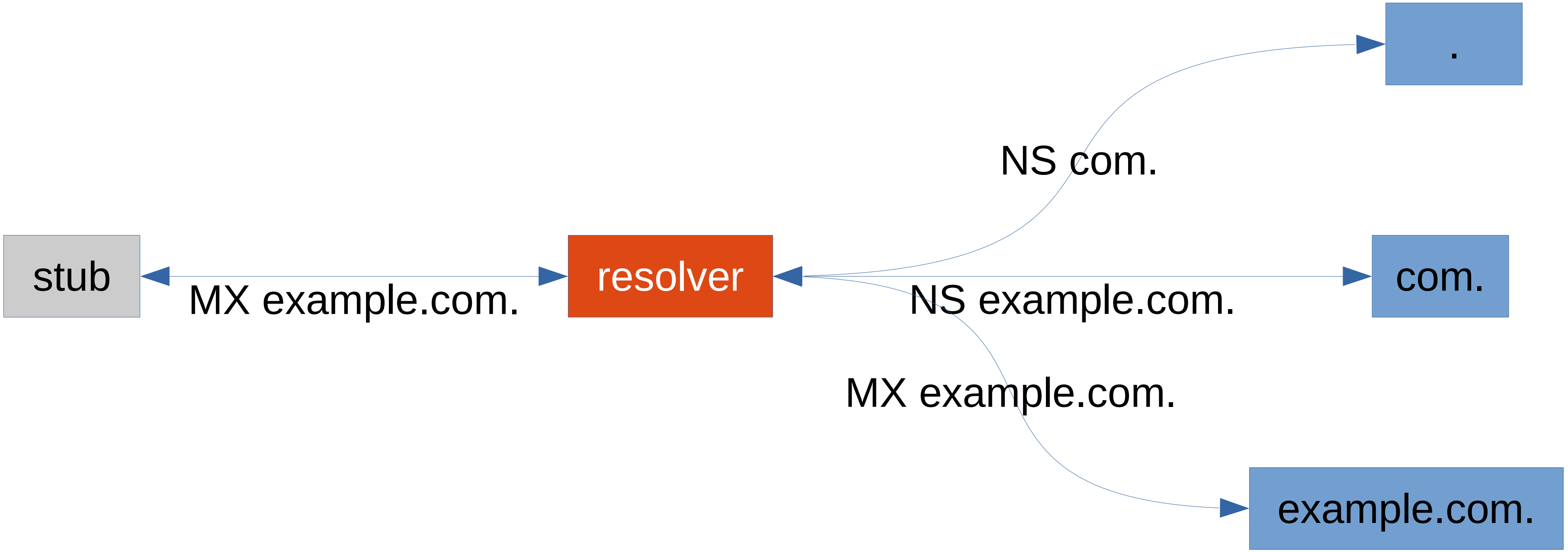
Query Name Minimisation

draft-ietf-dnsop-rfc7816bis-04

Stephane Bortzmeyer, **Ralph Dolmans**, Paul Hoffman

RFC7816



stub

MX example.com.

resolver

NS com.

NS example.com.

MX example.com.

.

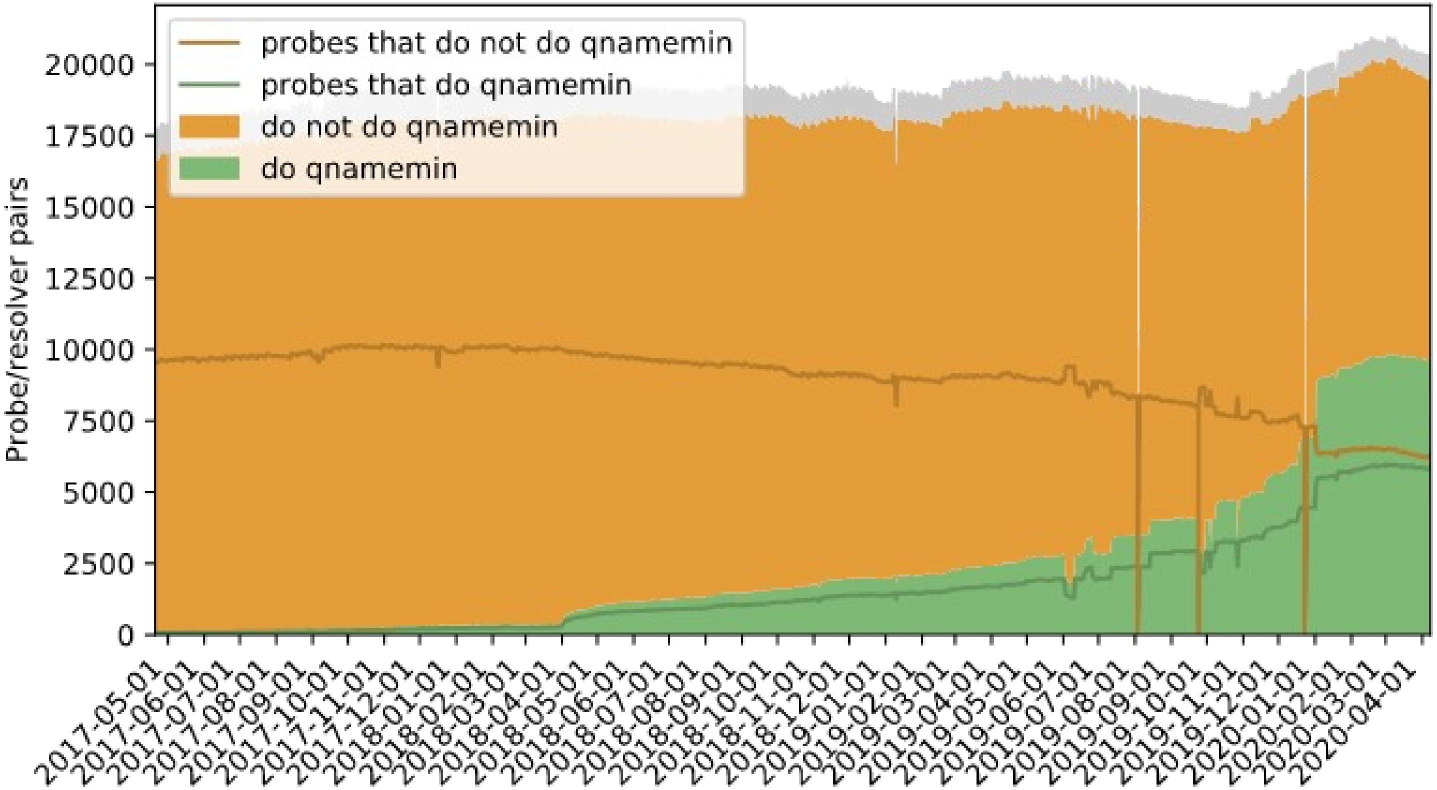
com.

example.com.

RFC7816bis goal

- Experimental → standards track
- Specify the standard in such a way that it can work on the real Internet
  - Document issues and solutions/workarounds
  - Using implementation experience

No longer experimental – enabled on 47% of tested resolvers



Source: https://dnsthought.nlnetlabs.nl/#qnamemin – 9 April 2020

Changes in -03 and -04

- Rework the algorithm
  - Better cache use
  - Get DS at parent
- Update examples
- Start documenting workarounds used per implementation
  - needs more work
- **Relax QTYPE recommendation**
- **Add text about danger of increased number of queries**
  - **Suggestion on how to handle this**

Relax QTYPE=NS recommendation

- QTYPE to use does not matter, server is not authoritative to answer anyway → return delegation
  - RFC7816 talks about prepending QNAME when using QTYPE=A, not needed
- All data TYPE RRTYPEs are fine as long as the authority lies below the zone cut
- There should not be a relation between incoming QTYPE and selection of QTYPE to use while minimising

Relax QTYPE=NS recommendation

- Using QTYPE=NS is still allowed
- Using QTYPE=A has some benefits
  - Not blocked
  - Less visible
  - Reduces number of queries
    - No delegation check needed for query to non-apex record for full QNAME when original QTYPE is same as minimising QTYPE
- Unbound uses QTYPE=A

Number of queries

- RFC7816 only mentions increased number of queries in performance context
- RFC7816bis also mentions DoS attack vector
  - Large number of labels answered using wildcard
- “*Resolvers supporting QNAME minimisation should implement a mechanism to limit the number of outgoing queries per user request.*”
  - SHOULD? MUST?

Number of queries

- One possible mechanism in draft (as implemented in Unbound)
- Limit number of qnamemin iterations to 10, append only 1 label for first 4 queries, divide rest of labels by rest of iterations, add remainder to last iterations.
  - Assumes bigger privacy gain higher in the name space
- E.g. QNAME with 18 labels; number of labels added per iteration are 1,1,1,1,2,2,2,2,3,3.

Forwarding

- Should queries be minimised when sending to forwarder?