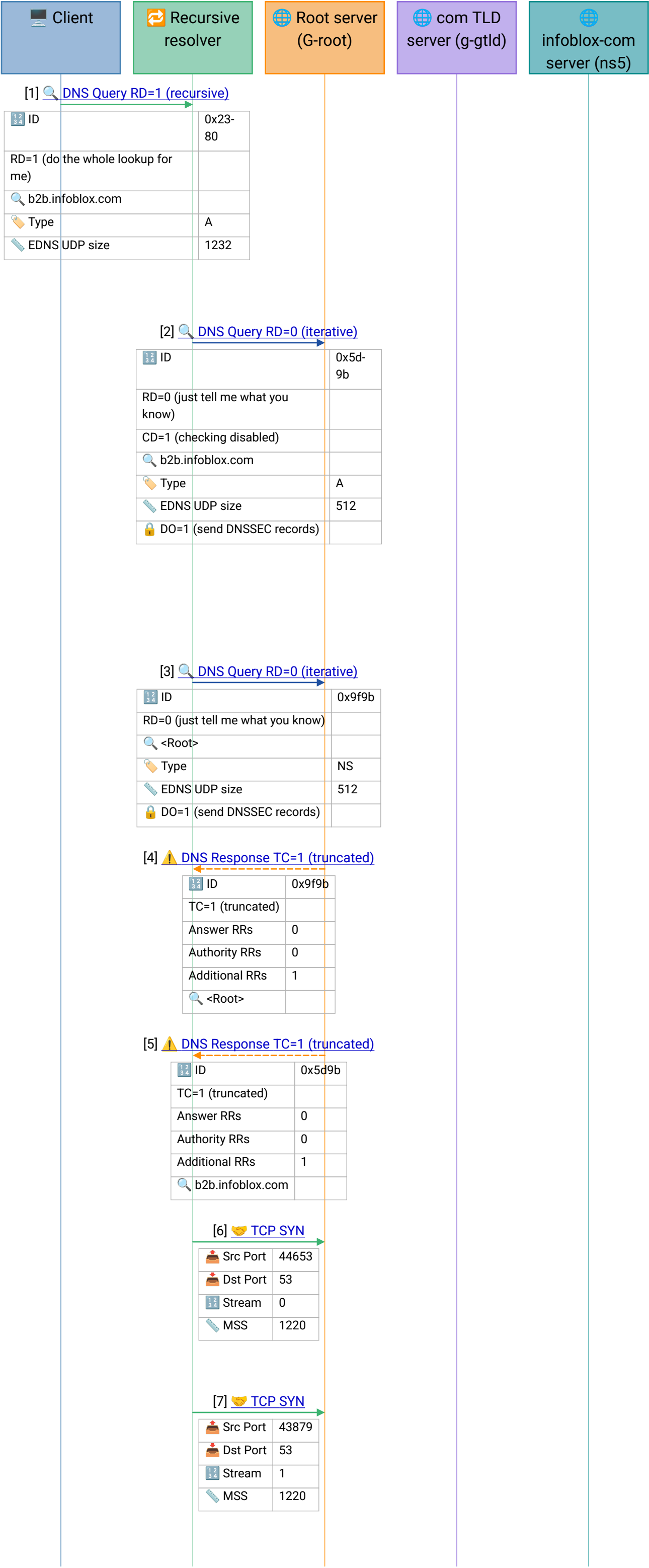




[Frame 1]

Phase 1: the client asks once

The client asks its resolver for the IPv4 address (A record) of b2b.infoblox.com. RD=1 (recursion desired) means "do the whole lookup for me": the client sends nothing else, and every frame until the answer in frame 31 is work the resolver does on its behalf, out of the client's sight.

The query also sets AD=1 , asking the resolver to report whether it validated the answer (RFC 6840), and carries an EDNS client cookie (RFC 7873). It advertises a 1,232-byte UDP buffer and leaves DO clear, so it does not want DNSSEC records back.

[Frame 2]

Phase 2: a cold resolver starts at the root

The resolver starts at the top of the DNS tree and asks a root server. The capture later proves this address is G-root (frame 15). Nothing in the capture supplied that address before this query, so it comes from the resolver's own built-in list of root server addresses (its root hints).

RD=0 : an iterative query. The root answers only from its own zone and will not chase the name further.

The resolver sends the full name b2b.infoblox.com to the root, not just com, so it is not using QNAME minimization (RFC 9156). Upstream traffic is IPv6, while the client side was IPv4. The query carries a fresh random ID (0x5d9b) and source port (51976), which makes spoofed replies hard to land.

Remember the advertised EDNS UDP size: 512 bytes, with DO=1 asking for DNSSEC records.

[Frame 3] A priming query (RFC 8109): "who are the root servers?" (NS for the root, <Root>) . It goes to the same server 0.1 ms after frame 2; the resolver does not wait for it before sending the real query.

Priming swaps the static hints list for the live, signed root NS set. This query also advertises 512 bytes with DO=1 .

[Frame 4] 27 ms later the root answers the priming query, but with TC=1 (truncated) and empty answer and authority sections. The full answer is 1,109 bytes (frame 15 shows it), far over the 512 bytes the resolver offered.

The truncated reply is just the header, the question, and the OPT record: 28 bytes, the same size as the query. AA=1 survives because the root is authoritative for its own NS set.

A resolver that gets TC=1 must retry over TCP, which is why RFC 7766 makes DNS over TCP mandatory.

[Frame 5] Same outcome for the real query: TC=1 and no answer. The full referral is 1,179 bytes (frame 19).

The CD bit from frame 2 is copied back, as RFC 4035 requires. Both answers would have fit in the 1,232-byte buffer the client itself used in frame 1. Offering only 512 bytes with DO=1 against the signed root zone makes this detour close to certain.

[Frame 6]

Phase 3: retry over TCP

0.4 ms after the truncated reply, the resolver opens a TCP connection to the same root server on port 53. This connection (source port 44653) will carry the priming query.

MSS 1220 is 1,280 bytes minus 40 for the IPv6 header and 20 for TCP: consistent with a 1,280-byte MTU (the IPv6 minimum) on the resolver's path.

[Frame 7] A second TCP connection (source port 43879) for the A query. This resolver opens one connection per outstanding query rather than sending both on one connection, which RFC 7766 would allow.

