DNS Push Notifications

IETF 92, March 2015, Dallas TX

Tom Pusateri, Stuart Cheshire

LLQ is dead.

Long Live DNS Push!

Review Design Goals

- Solution should be more timely & more resource efficent than polling
- Minimize changes to existing DNS servers
- Ensure client return reachability
- Resilience to packet loss
- Reduce DDoS attacks and client packet storms

DNS Push Notifications

- Simplify LLQ by using DNS UPDATE as a notification from server to client
- Add SUBSCRIBE, UNSUBSCRIBE for client to register / deregister with server
- Require TCP to simplify state & cleanup
- Require TLS for confidentiality, integrity, authentication

Discovery

- Client sends SOA query for RR or RRSet
- Receives back `<zone>` in SOA response

- Client sends SRV for `_dns-push._tcp.<zone>`
- Receives targets, priorities, weights, ports
- Client follows DANE SRV to authenticate

DANE SRV

- SRV records MUST be secured with DNSSEC
- Ordering & selection based on priority & weight
- DNSSEC validation of A and/or AAAA records
- TLSA query for SRV target / proto / port

  ← `_dns-push._tcp.<zone>. 86400 IN SRV 10 0 53 foo.<zone>.`

  → `_53._tcp.foo.<zone>. IN TLSA ?`

- SRV, A, AAAA, & TLSA queries MAY happen in parallel

SUBSCRIBE

- Similar to a Query but flag bits, ID all set to `0`
- QR bit cleared in SUBSCRIBE Request, RCODE `0`
- QTYPE, QCLASS may be specific or ANY
- Must contain ONE and only ONE resource record
- QR bit set in SUBSCRIBE Response, No Answers included
- Response indicates sucess in RCODE
- Valid until revoked (UNSUBSCRIBE) or connection closed

UNSUBSCRIBE

- Almost identical to SUBSCRIBE
- Must match an existing subscription
  - Close connection on error
- No response sent by server

UPDATE

- UPDATEs follow a successful SUBSCRIBE
- QR, ID, Z, and RCODE must be `0`
- UPCOUNT contains number of records
- Resource record fields indicate ADD or DELETE variants using CLASS, TTL, RDLEN, etc.
- Server UPDATE optimization is encouraged
- Client doesn’t use TTL to expire received records
- No response is sent by the client upon reception of UPDATE

TODO

- Clarify use of term “wildcarding” in Section 6.2
- Document fallback procedures for DANE SRV
- TLS Server Name Indication (SNI) handling
- Discuss user authentication
- Simultaneous client connections
- DANE SRV a MUST (for Markus)
- Do we need a teardown message or is TCP RST ok?