RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Expired RRSIG… Answer or not?

Anand Buddhdev | 9 Feb 2024 | OARC 42

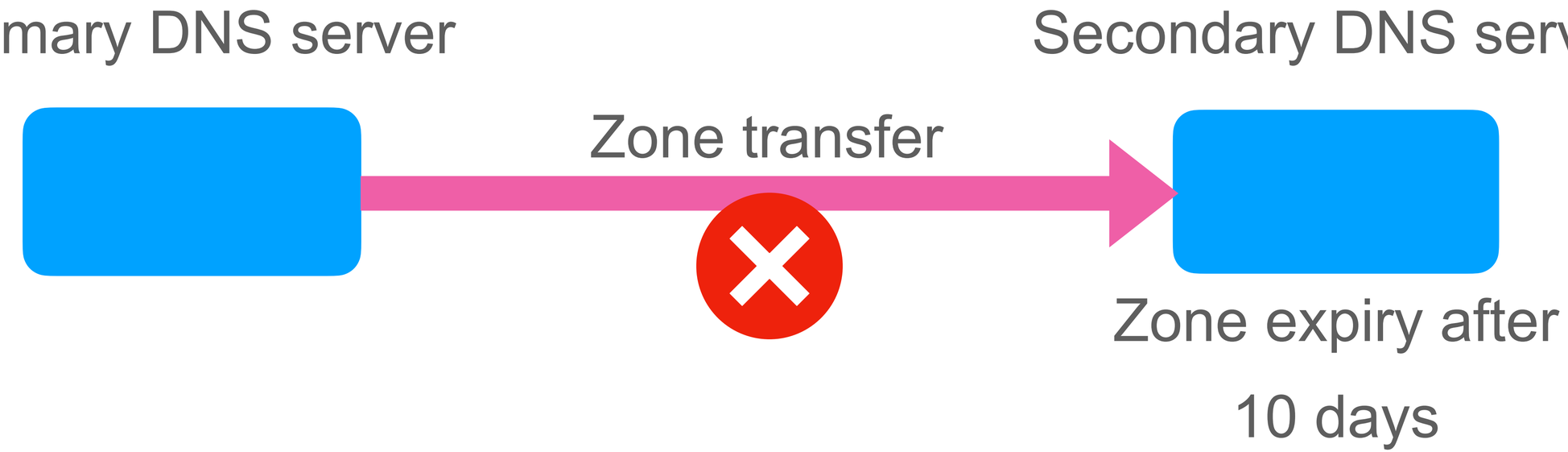
Zone propagation incident

- One of our secondaries was serving older versions of two RIPE NCC reverse DNS zones
- DNSSEC signatures in the zones had expired
  - DNSSEC validation failures
  - Worse than SERVFAIL

Expiry timers

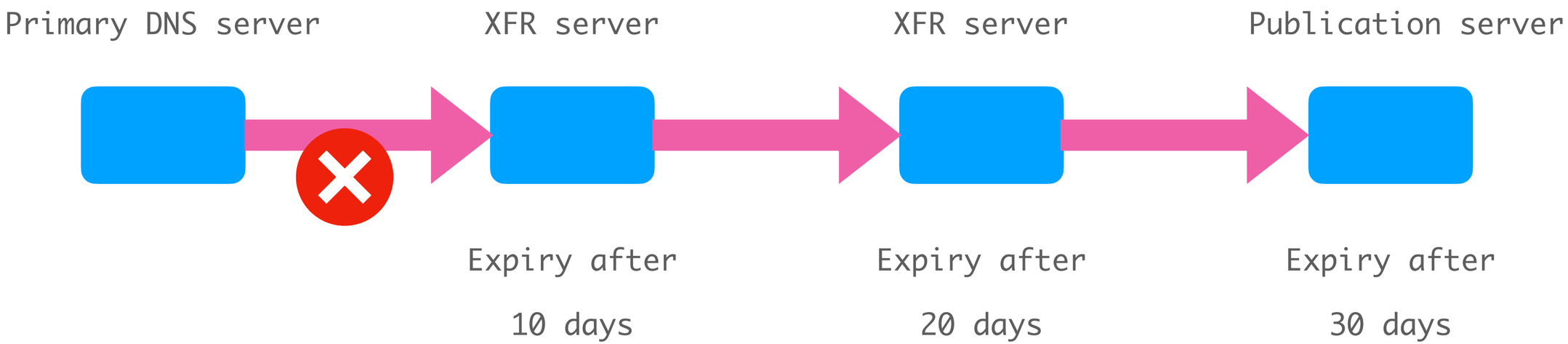
```
25.in-addr.arpa. SOA pri.authdns.ripe.net. dns.ripe.net. (
                                1684926122 ; serial
                                3600       ; refresh (1 hour)
                                600        ; retry (10 minutes)
                                864000     ; expire (10 days)
                                3600       ; minimum (1 hour)
                                )
25.in-addr.arpa. RRSIG SOA 13 3 3600 20230607110202 20230524093202 (
                                3096 25.in-addr.arpa.
                                F6PixyE86N…
                                )
```

Simple DNS infrastructure



- Secondary DNS server responds with SERVFAIL
- DNS resolvers try other servers

Tiered zone transfer infrastructure



Zone is served, with expired DNSSEC signatures for 16 days!

The solution

- EDNS EXPIRE option
- RFC 7314
  - EXPIRE option valid in SOA and XFR queries and responses
  - Primary server sets zone’s expiry timer from zone’s SOA record
  - Primary server responds with this expiry value in the EXPIRE field of the response
  - XFR client uses this value for the zone lifetime
  - Intermediate XFR server passes on this value to downstream XFR clients
  - Only works if all servers in the chain support the EXPIRE option

Example using EXPIRE option

```
dig @manus.authdns.ripe.net ripe.net soa +noall +comments +answer +expire +norec +multi
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48134
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; EXPIRE: 861439 (1 week 2 days 23 hours 17 minutes 19 seconds)
;; ANSWER SECTION:
ripe.net.       3600 IN SOA manus.authdns.ripe.net. dns.ripe.net. (
                1684949195 ; serial
                3600       ; refresh (1 hour)
                600        ; retry (10 minutes)
                864000     ; expire (1 week 3 days)
                3600       ; minimum (1 hour)
                )
```

EXPIRE support in software

- BIND 9 (including dig)
- Knot DNS since version 3.2 (including kdig)
- NSD - not yet
  - https://github.com/NLnetLabs/nsd/issues/274

Expired RRSIG - answer or not?

Questions

anandb@ripe.net