IETF 101 DNS Hackathon

Minimal IXFR (MIXFR)

Matthijs Mekking, Shane Kerr
This document proposes extensions to the DNS protocol to provide an incremental zone transfer (IXFR) mechanism to keep IXFRs (that deal with DNSSEC) small.
Hacking Implicit RRSIG Deletion into Knot DNS
IETF 101 DNS Hackathon: Results

Commits (33)
9 changed files...
...with 695 additions and 50 deletions
2 issues
IETF 101 DNS Hackathon: Results

Commits (33)
9 changed files...
...with 695 additions and 50 deletions
2 issues
IETF 101 DNS Hackathon: Results

MIXFR: 1217 bytes (saved 888 bytes)

Domain Name System (response)

[Request In: 18]
[Time: 0.000713631 seconds]
Length: 1215
Transaction ID: 0x3bee

Flags: 0x8000 Standard query response, No error
Questions: 1
Answer RRs: 9
Authority RRs: 0
Additional RRs: 1

Queries

Answers
- mixfr.nl: type SOA, class IN, mname dns-master.mixfr.nl
- mixfr.nl: type SOA, class IN, mname dns-master.mixfr.nl
- mixfr.nl: type SOA, class IN, mname dns-master.mixfr.nl
- mixfr.nl: type MX, class IN, preference 999, mx smtp2.mixfr.nl
- mixfr.nl: type A, class IN, addr 46.19.37.145
- mixfr.nl: type RRSIG, class IN
- mixfr.nl: type RRSIG, class IN
- mixfr.nl: type RRSIG, class IN
- mixfr.nl: type SOA, class IN, mname dns-master.mixfr.nl

Additional records
DNSSEC re-sign:
22390 bytes of IXFR
RSASHA256: Saved ~300 bytes / RRSIG
ECDSAP256SHA256: Saved ~100 bytes / RRSIG

For each RRSIG per changed/re-signed RRset
SOA RRset will always change
Improving DNS replication:
* Packet size
* Disk space, disk I/O
* Secondary server features signaling, for example online signing
* (M)IXFR-ONLY
* Separate protocol
IETF 101 DNS Hackathon: Thoughts

Improving DNS replication, something we should work on?

Dealing with the Camel:
rm -rf RFC1995 (IXFR)
rm -rf RFC2931 (SIG(0))

Thanks for your support: Petr Špaček
Blog: TBD on RIPE LABS
Draft: https://datatracker.ietf.org/doc/draft-mekking-mixfr/
GitLab https://gitlab.labs.nic.cz/matje/knot-dns/tree/mixfr