DNS NOTIFY

Paul Vixie

Internet Software Consortium
Falls Church, Virginia

Problem Statement

- SOA REFRESH can’t be granular enough
- Would like real time slave updates
- Let’s not add any *new* security holes
- Keep it simple – BIND is a wreck

Push vs. Pull

- Pushing new data needs security
- When to update SOA? (Reliably?)
- Existing AXFR, proposed IXFR: “pull”
- Send only hints; query only masters

Message Format

- New opcode: NOTIFY (4)
- ID, QNAME, QCLASS, QTYPE
- No answers, authority, or additional
- Extensible, if we figure out how

Nameserver Definitions

- Primary Master: has *the* external data source
- Slave: uses AXFR/IXFR to fetch zone data
- Slave-Master (ick): as Slave, but is also an AXFR/IXFR server to other Slaves (deep tree)
- Unregistered: uses AXFR/IXFR but is not in NS RR
- Caching, Forwarding, Recursive: as before
- Server: receives and sends data on DNS (UDP/TCP) port

Notification

- Primary Master gets new zone (and new SOA)
- P.M. notifies all registered slaves (which are all those named in NS RR set except the one named in the SOA MNAME
- Optional: P.M. also notifies suspected Unregistered slaves, which are those Servers that have queried for the SOA within the last SOA REFRESH interval
- Each Slave-Master notifies all Slaves (and, optionally, suspected Unregistered slaves) that have fetched the SOA within the last SOA REFRESH interval.

Protocol

- Master -> Slave: NOTIFY, !QR
- (Retry until response or timeout)
- Slave -> Master: NOTIFY, QR
- Then Slave performs RRtype-specific action
- Only SOA is defined at this time