Common configuration interface for DNS - YANG

P.Lexis, L.Lhotka, P.Spacek, N.Kowalewski, M.Vasko

IETF104 Hackathon

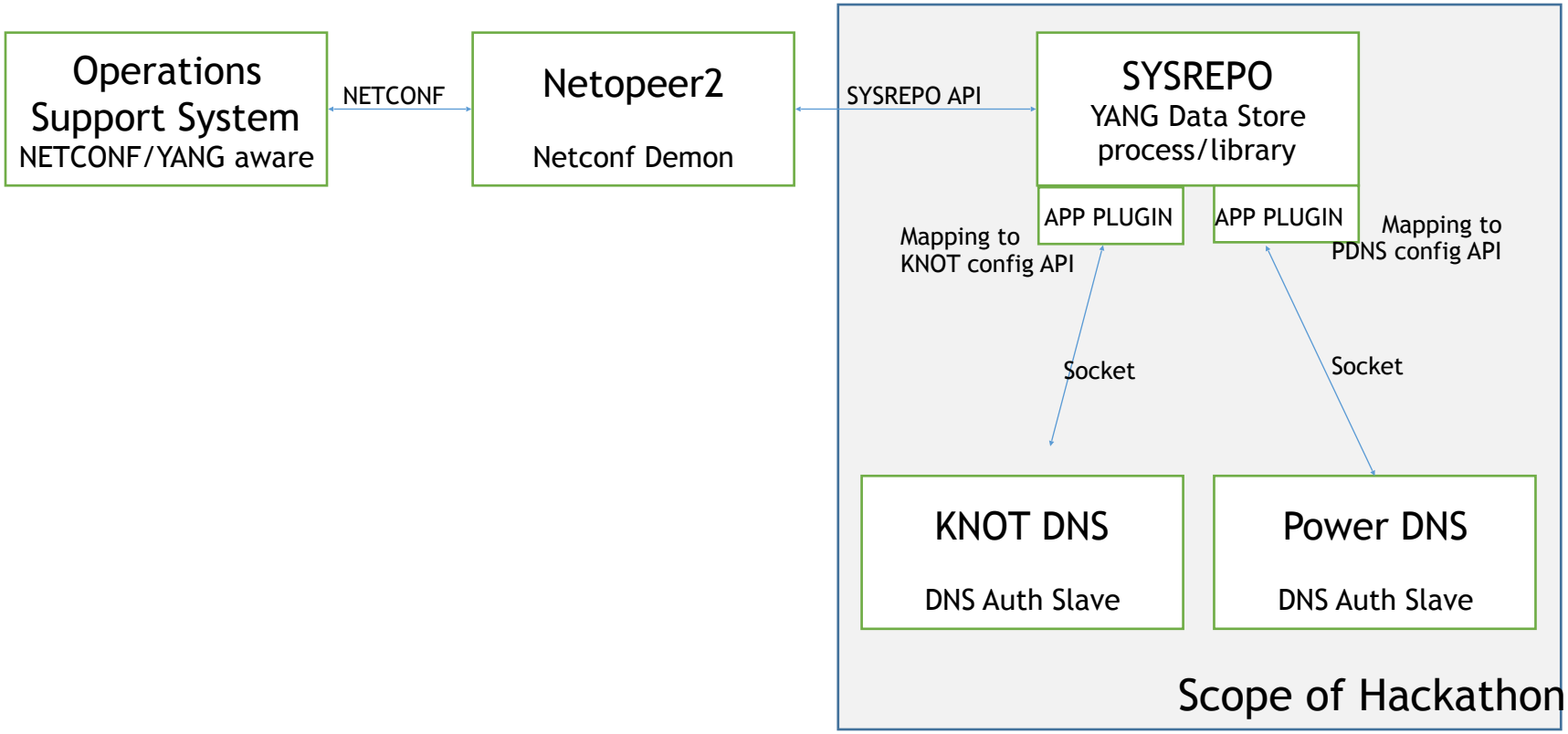
Why doing it?

- Motivated by a network in which everything that is NETCONF/YANG configurable today *is* indeed YANG modeled, and NETCONF configured
  - Network provides end-to-end “triple-play” capable consumer internet access
  - Functions encompass IPv6 transport - from IS-IS interconnect to Home Router, IPv4 runs as lwAFTR service, and baseline services NTP, DNS, DHCPv6
- Many aspects of this network are templated, follow well defined conventions, and configuration is computed and then applied
- Realtime customer self-signup, auto-configuring the full equipment path.
- Configuration for elements that yet have no NETCONF/YANG support yet is performed via wrapper functions hiding “traditional” config APIs
- DNS is an important element in this, and has no NETCONF/YANG support yet:
  - DNS Authoritative: masters/slave servers, zone descriptions, resource records, ACLs/policies
  - DNS Resolvers: servers, ACLs/policies

IETF104 Hackathon approach

- Create a minimal YANG model that can facilitate remote slave server zone management
- Find FOSS package SYSREPO that can store yang models, and can offer an API towards application specific configuration functions (Thank you !!!).
- Develop minimal SYSREPO/DNS Server API transcoding plugin
- Find FOSS DNS projects KNOT and PowerDNS (Thank you !!!) supporting the idea and be willing to experiment with having their DNS Auth servers as configuration targets
- Use cases:
  - Newly created zone at SYSREPO triggers its addition at slave
  - Works same, no matter if target is KNOT or PowerDNS

Hackathon context and scope



Hackathon insights and results

- PoC shown running:
  - Auth DNS slave come up with only its binding address configured
  - Small DNS specific demon listens to updates in SYSREPO config datastore, to then transcode that into config commands for this DNS
  - Config data store is changed to add zones „.“ and „.icann“
  - DNS auth slave is triggered to create zones and pulls in zone content
  - DNS can from here on deliver correct reply on respective DIG queries
- Conclusion: Leveraging Netconf/YANG in configuration management for DNS is feasible.
- Hackathon on site availability of non-DNS portion experts was pivotal to navigate around rough corners.
- Ongoing discussion on defining what to model as configuration and as operational state for DNS, and mappings to https://tools.ietf.org/html/rfc8342 Network Management Datastore Architecture (NMDA)
  - There was feedback with DNS server authors to see zone data that define resource records rather as operational state.
  - In this context, also the impact of Dynamic Updates in the Domain Name System (DNS UPDATE) https://tools.ietf.org/html/rfc2136, seems to require additonal analysis

Resources

- Experimental YANG model
  - https://github.com/CZ-NIC/yang-dns/tree/slave-only/ietf
- KNOT Project
  - https://gitlab.labs.nic.cz/knot/knot-dns
- PowerDNS Project
  - https://github.com/powerdns
- SYSREPO Project
  - http://www.sysrepo.org/

- Hackathon Participants
  - lhotka <at> nic <dot> cz (YANG)
  - mvasko <at> cesnet <dot> com (Sysrepo)
  - nbkowalewski <at> gmx <dot> net
  - petr.spacek <at> nic <dot> cz (KNOT DNS)
  - pieter.lexis <at> open-xchange <dot> com (PowerDNS)