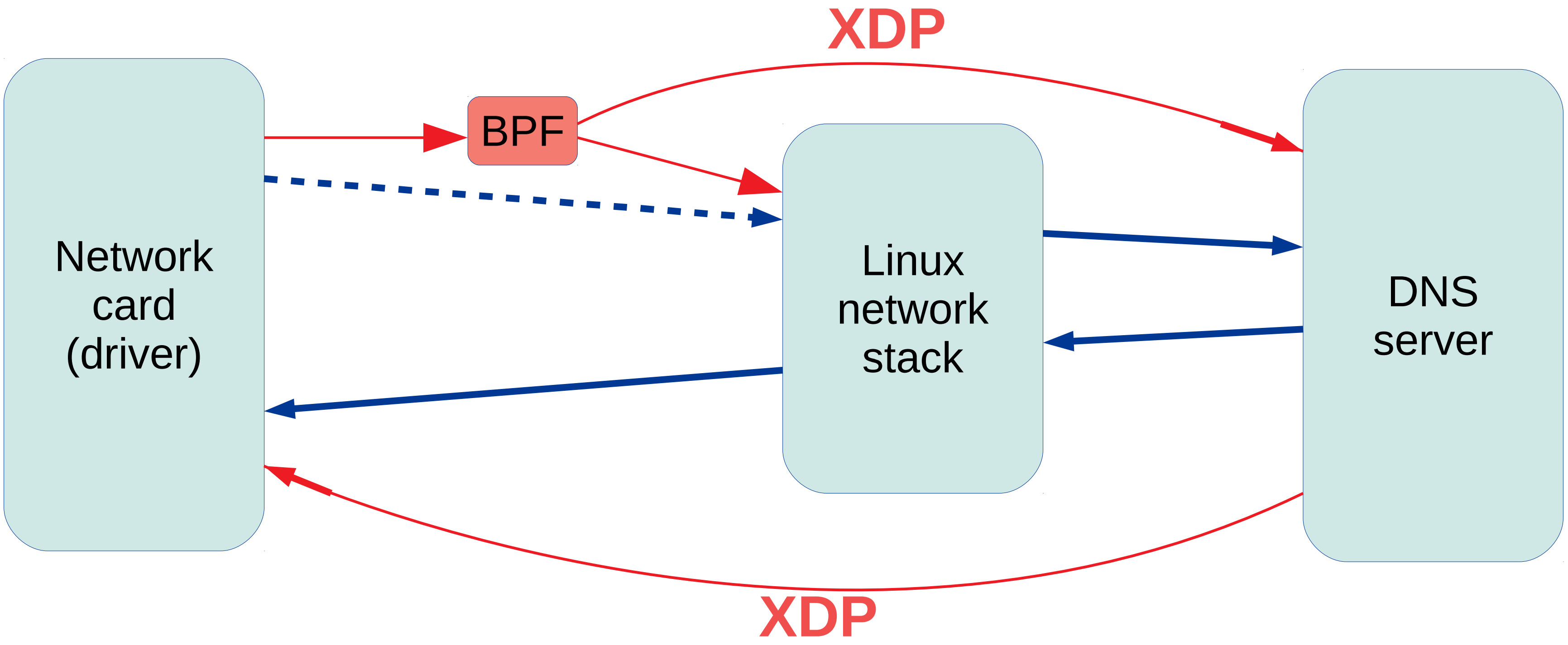
New in DNS
XDP & Catalog zones

Libor Peltan • libor.peltan@nic.cz • 2020-09-08

eXpress Data Path

- Packet I/O bypassing kernel
  - DNS over UDP only
- Performance +60% to +200%
  - Mitigate flood attacks
- Bypass routing
  - Same way back
- Bypass firewall

XDP packet handling



XDP Requirements

- Linux kernel 4.18+ (5.x recommended)
- XDP-compatible network card to achieve speed-up
- `CAP_SYS_ADMIN` during knotd startup

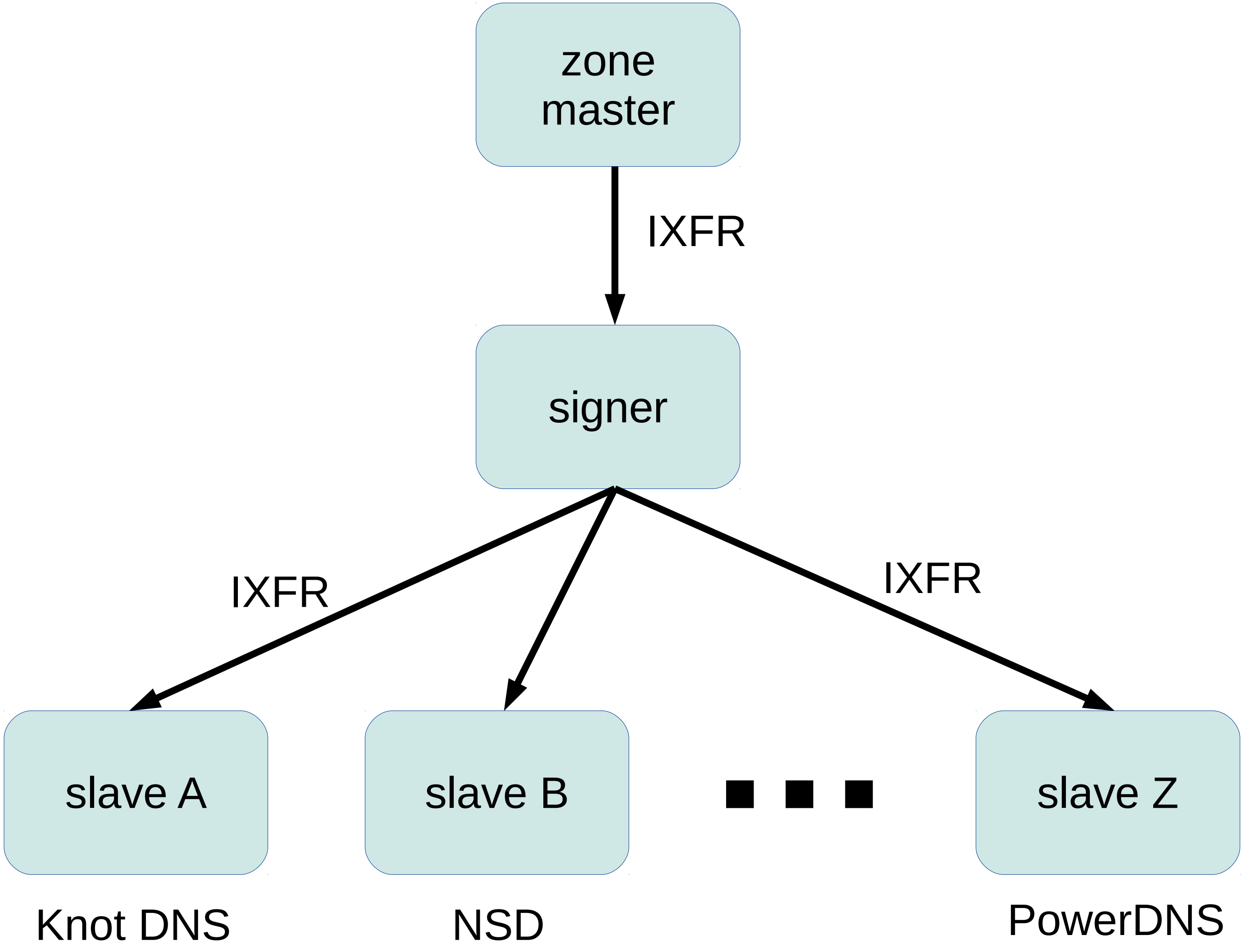
XDP in Knot DNS

- Released in version 3.0 **tomorrow**
- CZ.NIC already started deploying
- Open questions: IP filtering
  - “We won’t re-implement firewall!”
- BTW: kxdpgun benchmarking utility

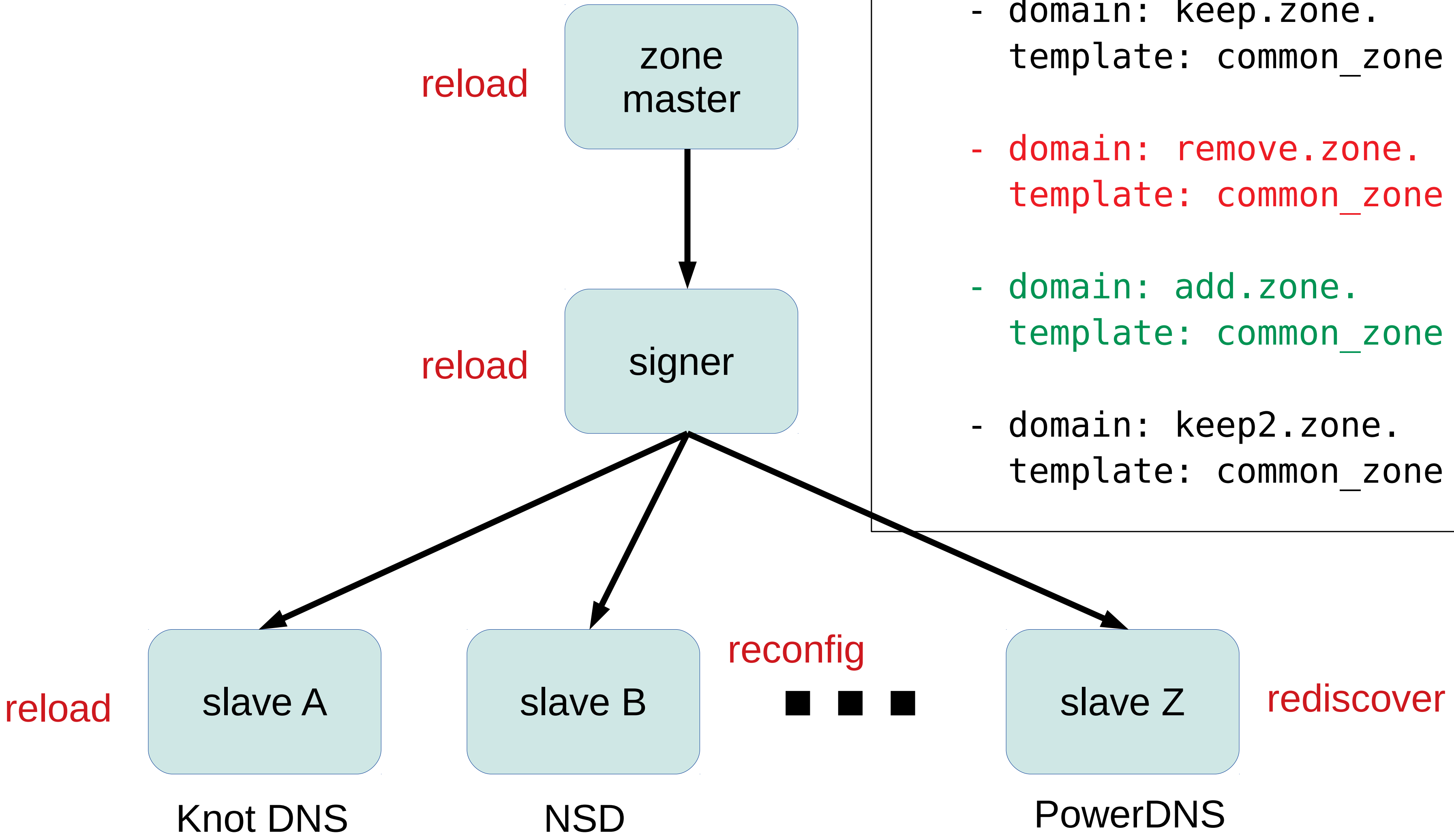
XDP configuration

```
server:
     listen: "217.31.205.1@53"
     listen-xdp: "ens3f0@53"
```

Zone propagation



Zone set propagation



```
zone:
 - domain: keep.zone.
   template: common_zone

 - domain: remove.zone.
   template: common_zone

 - domain: add.zone.
   template: common_zone

 - domain: keep2.zone.
   template: common_zone
```

Catalog zone

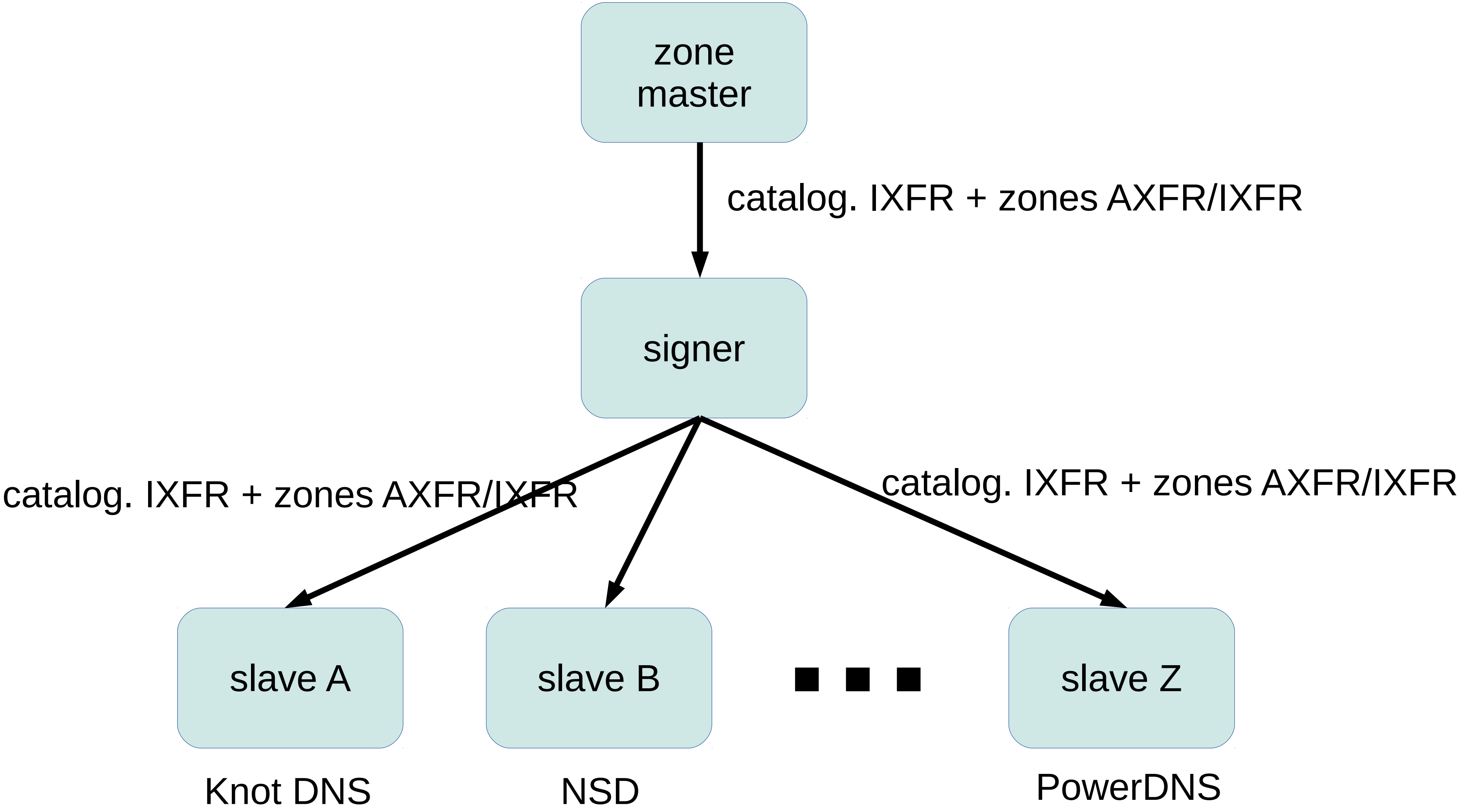
- Not part of global DNS tree
- PTR records <=> member zones
- + SOA, version, ...

Catalog zone

```
catalog. 0 SOA ns1.example.com. mail.example.com. (
       1594285472 ; serial eg unixtime
       7200       ; refresh
       1800       ; retry
       86400      ; expire
       0 )        ; minTTL == TTL == 0
catalog. 0 NS invalid.
version.catalog. 0 TXT "2"
c105364f1a847c07860ad7bd.zones.catalog. 0 PTR neci-maly-bussiness.eu.
703c55bbda045c1a91d0947a.zones.catalog. 0 PTR esop-vobchod.org.
```

Change owner iff re-registered

Zone propagation


zone master
catalog. IXFR + zones AXFR/IXFR
signer
catalog. IXFR + zones AXFR/IXFR
catalog. IXFR + zones AXFR/IXFR
slave A
slave B
...
slave Z
Knot DNS
NSD
PowerDNS

Implementations of Catalog

- 2016: BIND9 + first draft
  - incl detailed settings
  - “too slow” (Leo Vandewoestijne)
- 2020: second draft
  - only list of zones
  - https://tools.ietf.org/html/draft-toorop-dnsop-dns-catalog-zones-01
- Knot DNS 3.0
  - catalog **interpretation**
  - config → catalog postponed to 3.1(?)

Catalog zone configuration

```
template:
  - id: member_zones
    dnssec-signing: on
    master: hidden_master01
    ...

zone:
  - domain: catalog.
    file: /var/lib/knot/zones/catalog.zone
    catalog-role: interpret
    catalog-template: member_zones
```