Cross-implementation configuration and provisioning management

Initiative coming from Afilias DNS Summit

`draft-toorop-dnsop-dns-catalog-zones`

Peter van Dijk
Libor Peltan
Ondřej Surý
Willem Toorop
Leo Vandewoestijne

`draft-toorop-dnsop-dns-zone-provisioning-yang`

Pieter Lexis
Ladislav Lhotka
Petr Špaček
Ondřej Surý
Willem Toorop

Genesis

- /me works for NLnet Labs
- Meet with operators at conferences
- Other Open Source DNS Software do the same
- A recurring topic:
  - Standard Configuration & Provisioning Management

Genesis

- Afilias one of those operators
  - Key is cross-implementation cooperation
  - Preferably standardized approaches and solutions
- Afilias DNS Summit
  - Friday prior to IETF105 in Montreal
  - Attendees from NLnet Labs, ISC and CZ.NIC
  - One of the topics:
    - Standard Configuration & Provisioning Management

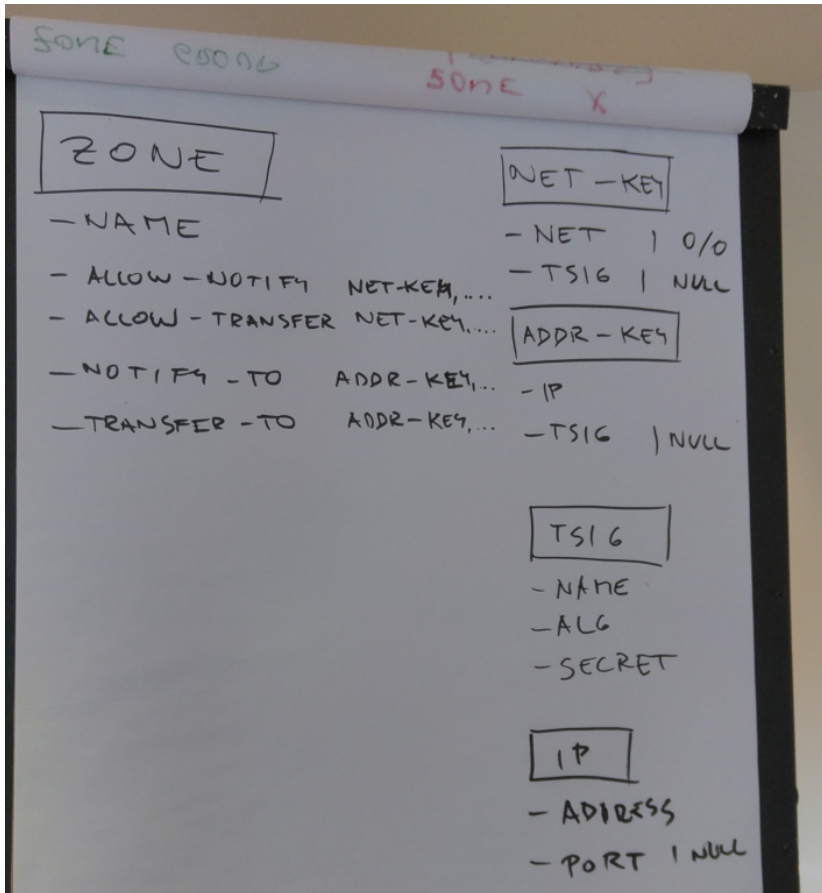
Standard Configuration & Provisioning Management

- Two candidates:

Catalog zones		NETCONF / YANG	
+	Provisioning infrastructure native to DNS	–	New infrastructure at least for DNS implementers
–	No feedback channel	+	Feedback on status
+	Implementations exist (ISC & PDNS) CZ.NIC is working on one	+	CZ.NIC & PDNS are working on it
+ –	(expired) draft exists (from ISC) draft lacks actual to configure properties	–	No draft yet for zone provisioning

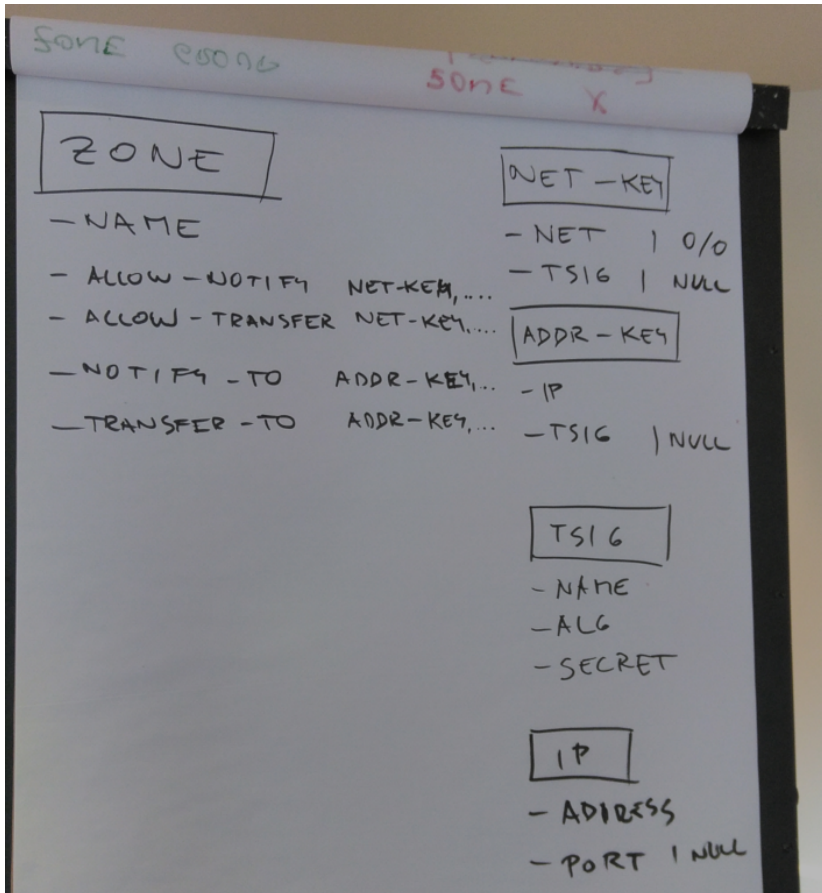
Standard Configuration & Provisioning Management

- Catalog zones lowest barrier to a working solution
- A new draft with minimal to configure properties



Standard Configuration & Provisioning Management

- Catalog zones lowest barrier to a working solution
- A new draft with minimal to configure properties defined in YANG



Catalog zones

draft-toorop-dnsop-dns-catalog-zones

- Presentation from Leo Vandewoestijne
  at FOSDEM2020
- Picked up from draft-muks-dnsop-dns-catalog-zones
- Authors from FOSDNSS implementations +Leo
  - Peter van Dijk – PowerDNS
  - Libor Peltan – CZ.NIC
  - Ondřej Surý – ISC
  - Willem Toorop – NLnet Labs
  - Leo Vandewoestijne

Catalog zones

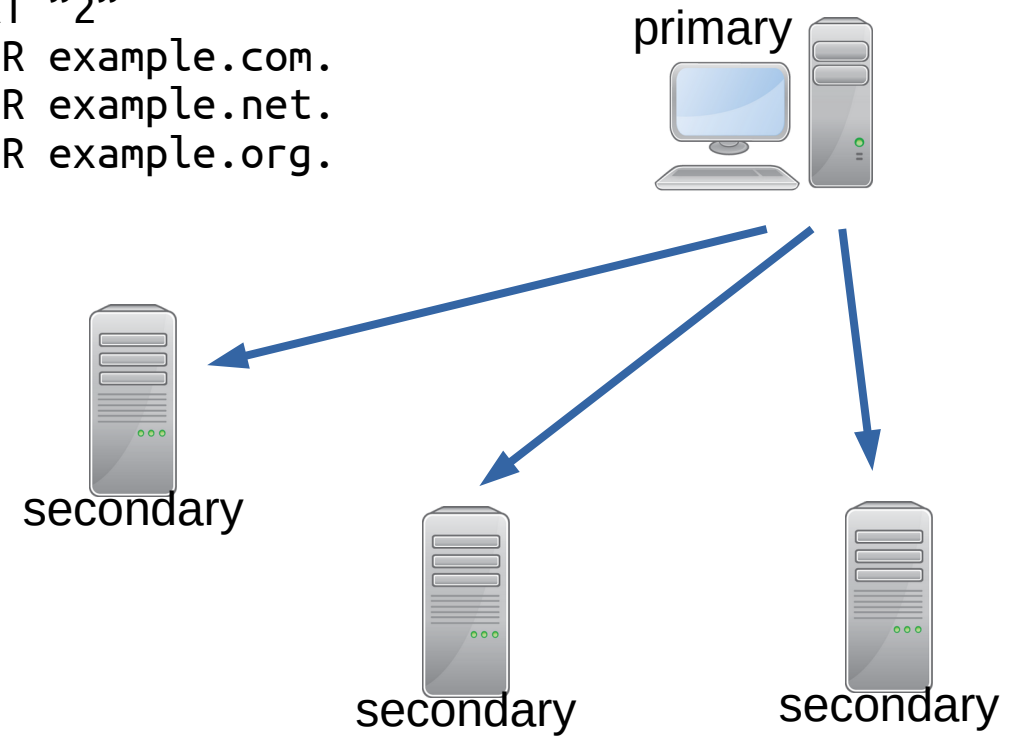
draft-toorop-dnsop-dns-catalog-zones

- Abstract
  - “a method for automatic DNS zone provisioning
    by storing and transferring
    the catalog of zones to be provisioned
    as one or more regular DNS zones.”

Catalog zones

draft-toorop-dnsop-dns-catalog-zones

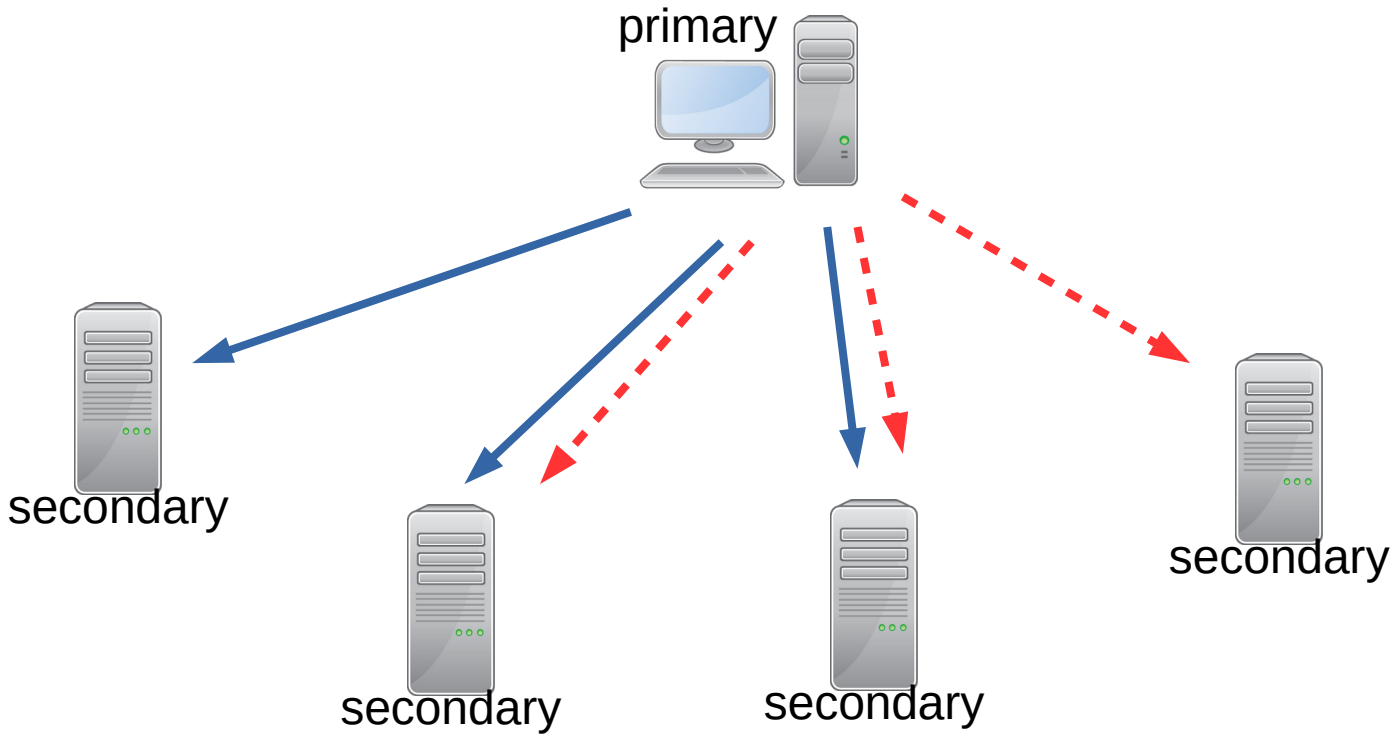
```
$ORIGIN catzone.
@                    IN  SOA . . 1552507036 86400 14400 86400 0
@                    IN  NS  invalid.
version              IN  TXT ”2”
<unique-id-1>.zones IN  PTR example.com.
<unique-id-2>.zones IN  PTR example.net.
<unique-id-3>.zones IN  PTR example.org.
```



Catalog zones

draft-toorop-dnsop-dns-catalog-zones

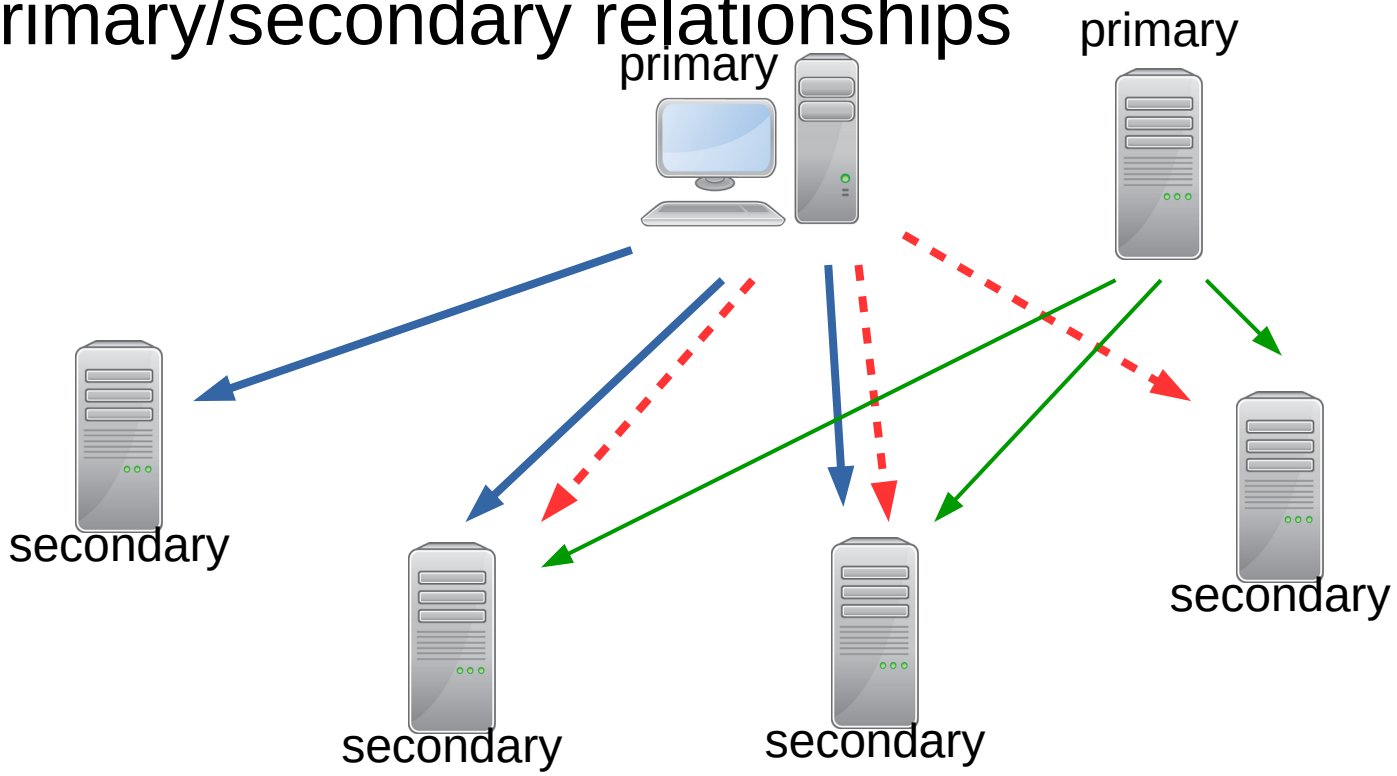
- Multiple catalog zones



Catalog zones

draft-toorop-dnsop-dns-catalog-zones

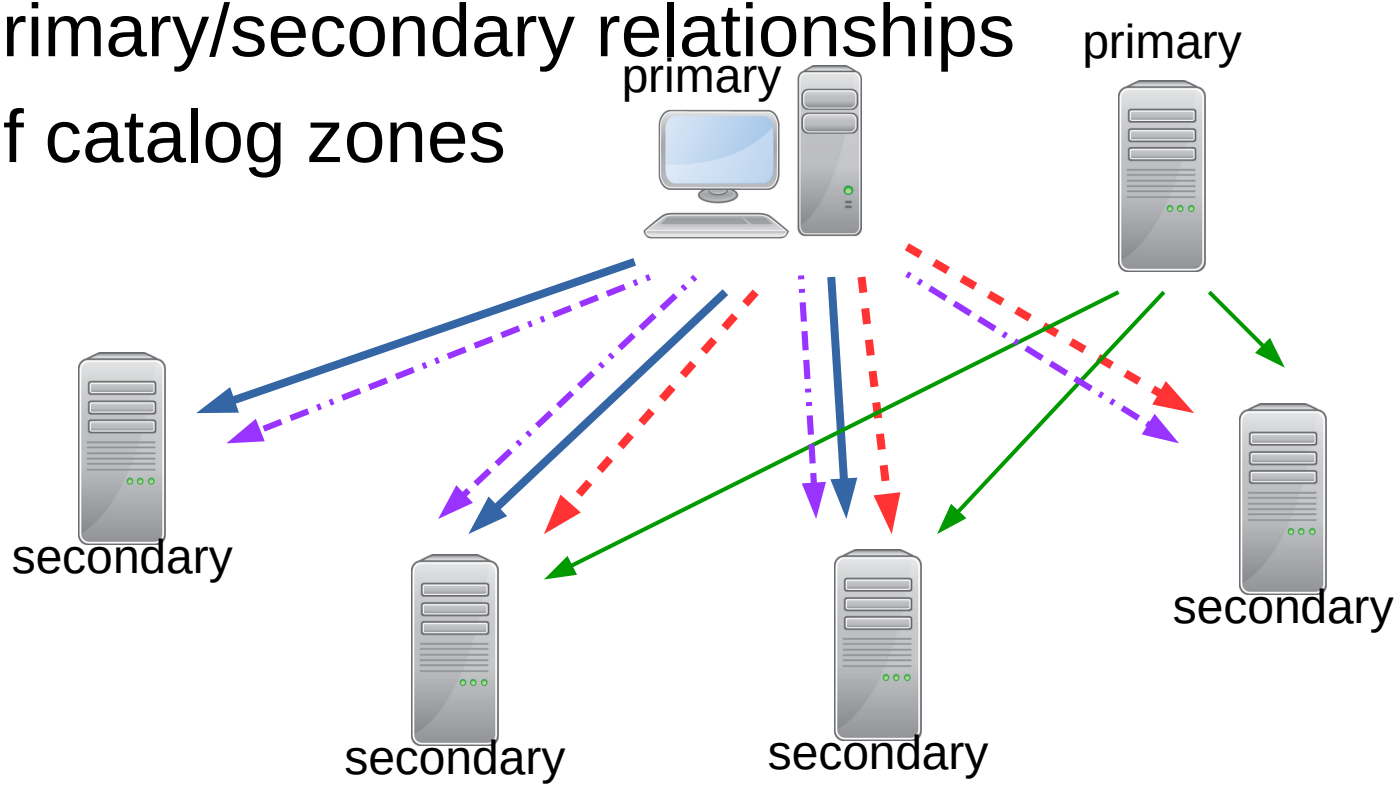
- Multiple catalog zones
- With different primary/secondary relationships



Catalog zones

draft-toorop-dnsop-dns-catalog-zones

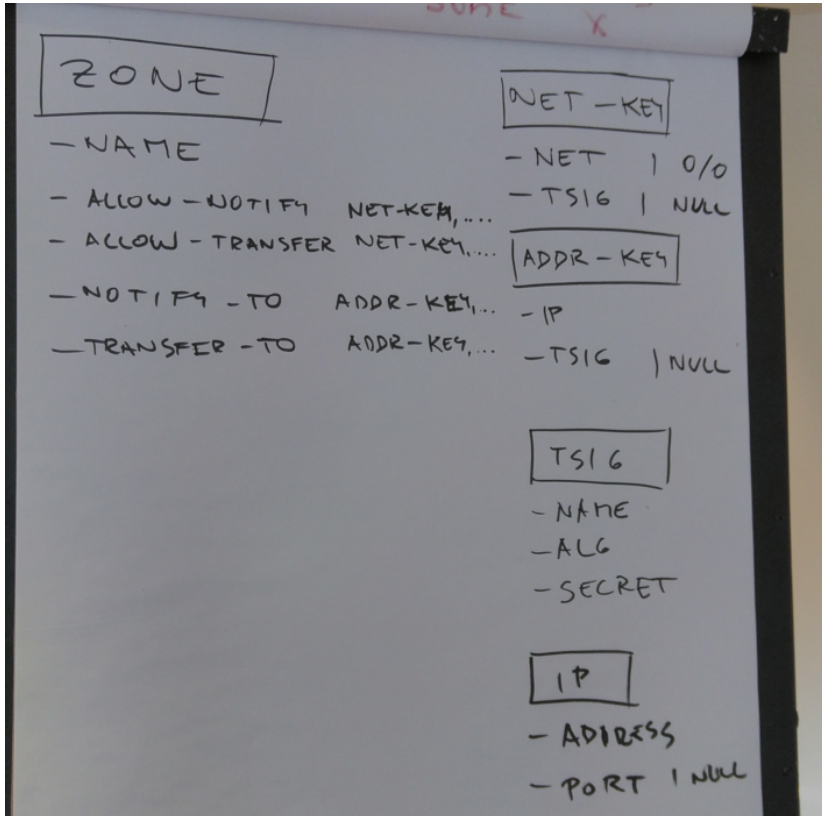
- Multiple catalog zones
- With different primary/secondary relationships
- Catalog zone of catalog zones



Catalog zones

draft-toorop-dnsop-dns-catalog-zones

- Changes since draft-muks-dnsop-dns-catalog-zones
  - Just the catalog, **no properties**



Catalog zones

draft-toorop-dnsop-dns-catalog-zones

- Changes since draft-muks-dnsop-dns-catalog-zones
  - Just the catalog, **no properties**
  - Changing unique id resets zone state

```
$ORIGIN catzone.
@                       IN  SOA . . 1552507036 86400 14400 86400 0
@                       IN  NS  invalid.
version                 IN  TXT ”2”
<unique-id-1>.zones IN  PTR example.com.
<unique-id-2>.zones IN  PTR example.net.
<unique-id-3>.zones IN  PTR example.org.
```

Catalog zones

draft-toorop-dnsop-dns-catalog-zones

- Idea from Leo
  - Make the list enumerable
  -
```
$ORIGIN catzone.
@                       IN  SOA . . 1552507036 86400 14400 86400 0
@                       IN  NS  invalid.
version                 IN  TXT ”2”
$ORIGIN zones.catzone.
@                       IN  HINFO   ”0”             <unique-id-1>
<unique-id-1>           IN  PTR     example.com.
                        IN  HINFO   ”1552507036”    <unique-id-2>
<unique-id-2>           IN  PTR     example.net.
                        IN  HINFO   ”1552501234”    <unique-id-3>
<unique-id-3>           IN  PTR     example.org.
                        IN  HINFO   ”1552505432”    @
```

Catalog zones

draft-toorop-dnsop-dns-catalog-zones

- We’d like to discuss and develop this further on list

Zone provisioning definitions in YANG

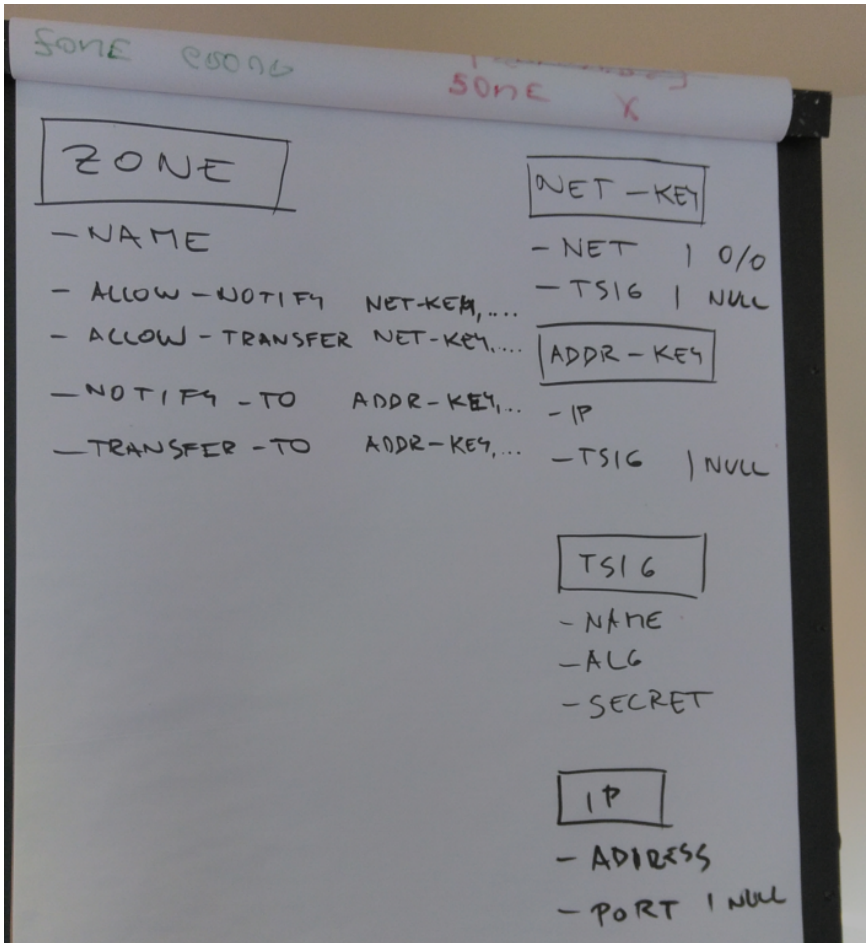
draft-toorop-dnsop-dns-zone-provisioning-yang

- YANG : A Data Modeling Language for the Network Configuration Protocol (NETCONF) RFC6020, RFC7950
- IANA maintains a registry for IETF yang models:
  https://www.iana.org/assignments/yang-parameters/yang-parameters.xhtml
- Abstract:
  - “A data model for configuring DNS Zone provisioning.
    This data model includes definitions
    for configuration of primary and secondary relationships.”

Zone provisioning definitions in YANG

draft-toorop-dnsop-dns-zone-provisioning-yang

- Gathered authors:
  - Pieter Lexis – PowerDNS
  - Ladislav Lhotka – CZ.NIC
  - Petr Špaček – CZ.NIC
  - Ondřej Surý – ISC
  - Willem Toorop – NLnet Labs
- Quick translation of our sketch to YANG.



Zone provisioning definitions in YANG

draft-toorop-dnsop-dns-zone-provisioning-yang

- From discussions with Pieter Lexis
  - type inet:domain-name could use re-evaluation
    - type dns:domain-name
  - introduce new types inheriting from domain-name:
    - type dns:host-name
  - Make translations for IANA parameters to YANG
    - type dns:tsig-algorithm

Zone provisioning definitions in YANG

draft-toorop-dnsop-dns-zone-provisioning-yang

- Maybe review initial model internally first…

  after that

- Is DNSOP a good place to develop these models?