Dynamic Domain Name Zone Provisioning

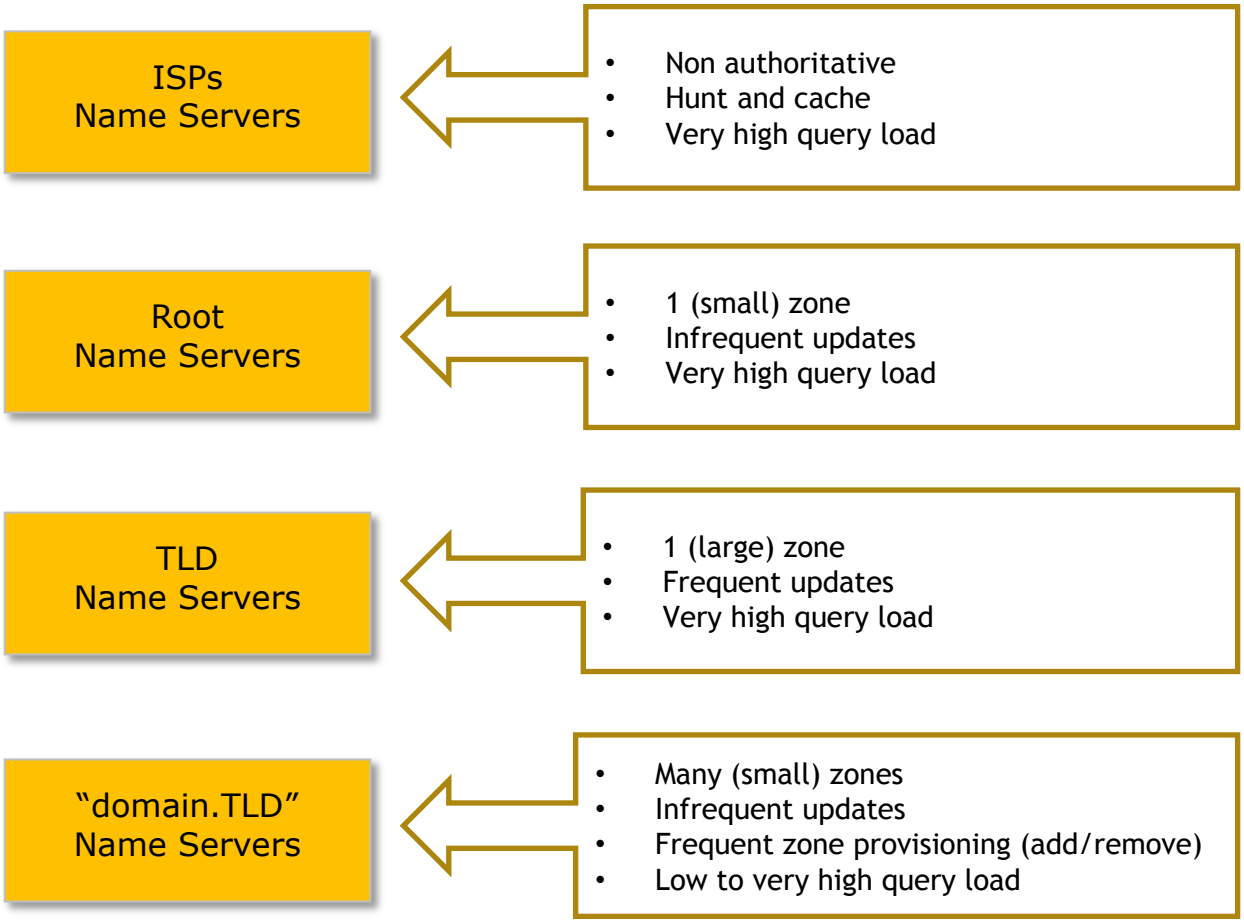
Peter Janssen

Technical Manager @ the .eu Registry

EURid vzw/asbl

.eu
Your European Identity

DNS servers everywhere



DNS provisioning (BIND)

- /etc/named.conf (master server)

```
zone “somedomain.eu" {
        type master;
        file "/var/bind/somedomain.eu”;
        allow-transfer { @ip_secondary; };
};
```

- /etc/named.conf (slave server)

```
zone “somedomain.eu" {
        type slave;
        file "/var/bind/somedomain.eu";
        masters { @ip_master; };
};
```

DNS provisioning (BIND)

- /var/bind/somedomain.eu
  - …
  - somedomain.eu. NS ns1.somedomain.eu.
  - somedomain.eu. NS ns2.somedomain.eu.
  - ns1.somedomain.eu. A 192.168.0.1
  - ns2.somedomain.eu. A 192.168.0.2
  - somedomain.eu. MX smtp.somedomain.eu.
  - www A 192.168.0.3
  - smtp A 192.168.0.4

DNS provisioning (powerdns)

- pdns.conf
  - launch=gmysql
  - gmysql-host=127.0.0.1
  - gmysql-user=root
  - gmysql-dbname=pdns
  - gmysql-password=C@n@nyb0dyR3@dTh1s?
- Database tables
  - Domains (id, name, master, type, …)
  - Records (id, domain_id, name, type, content, ttl, …)

Provisioning

- Config files
  - Generation
  - Distribution
- Database backend
  - Inserting/updating
  - Replication
- Is it configuration or is it just data?

Dynamic provisioning of DNS

- Goals
  - Performance
  - Easy provisioning of zones
  - Implementation flexibility (different vendors)
  - Security
    - Protocol security
    - As few as possible “entry points”
  - Support for DNSSEC
  - “Simplicity” of software setup

Config file based provisioning

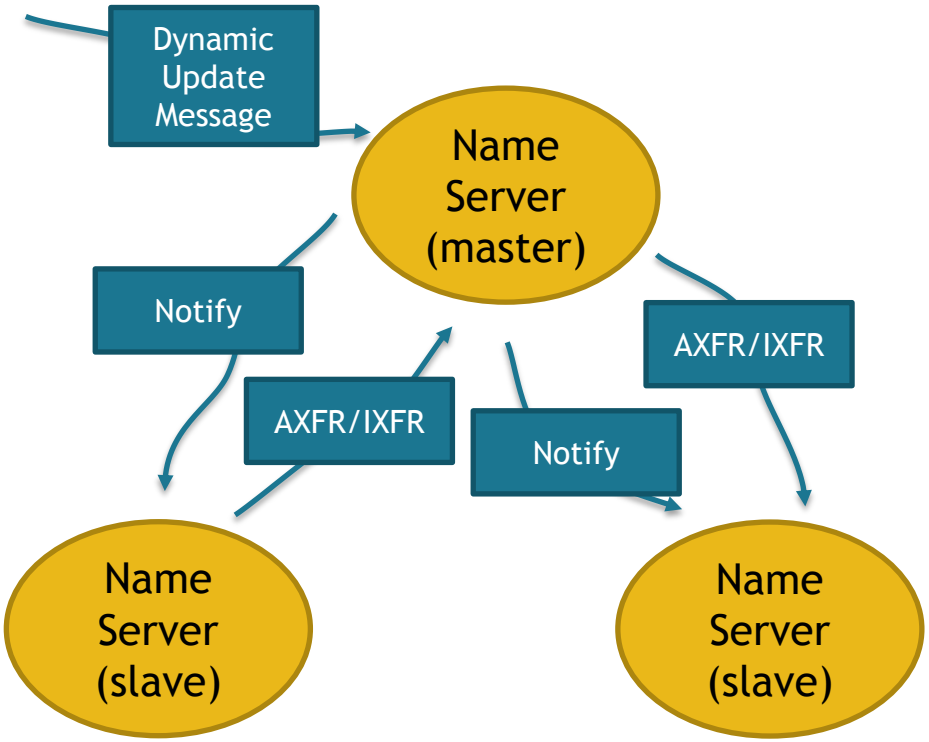
- Flow
  - Generate config files
  - Distribute config files
    - Chef, Puppet, CFEngine, rsync, …
  - Reload config files
    - cron, gearman, …
    - Signals, socket interface, …
- Challenges
  - Config file “layout” per name server implementation
  - “Reload” command per name server implementation
  - Reload without stopping answering queries
  - Extra “layer” of software for distribution and command

Database backend provisioning

- Flow
  - Insert/update in database tables
- Challenges
  - Database running on all nodes
  - Replication
  - Performance?
  - Interoperability?

Dynamic DNS

- Updating zone somedomain.eu



- In band communication
- Self managed
- No other software
- Interoperable
  - Dynamic Update : RFC2136
  - AXFR/IXFR : RFC1995/RFC5936
- No “downtime” when updating

Dynamic DNS provisioning

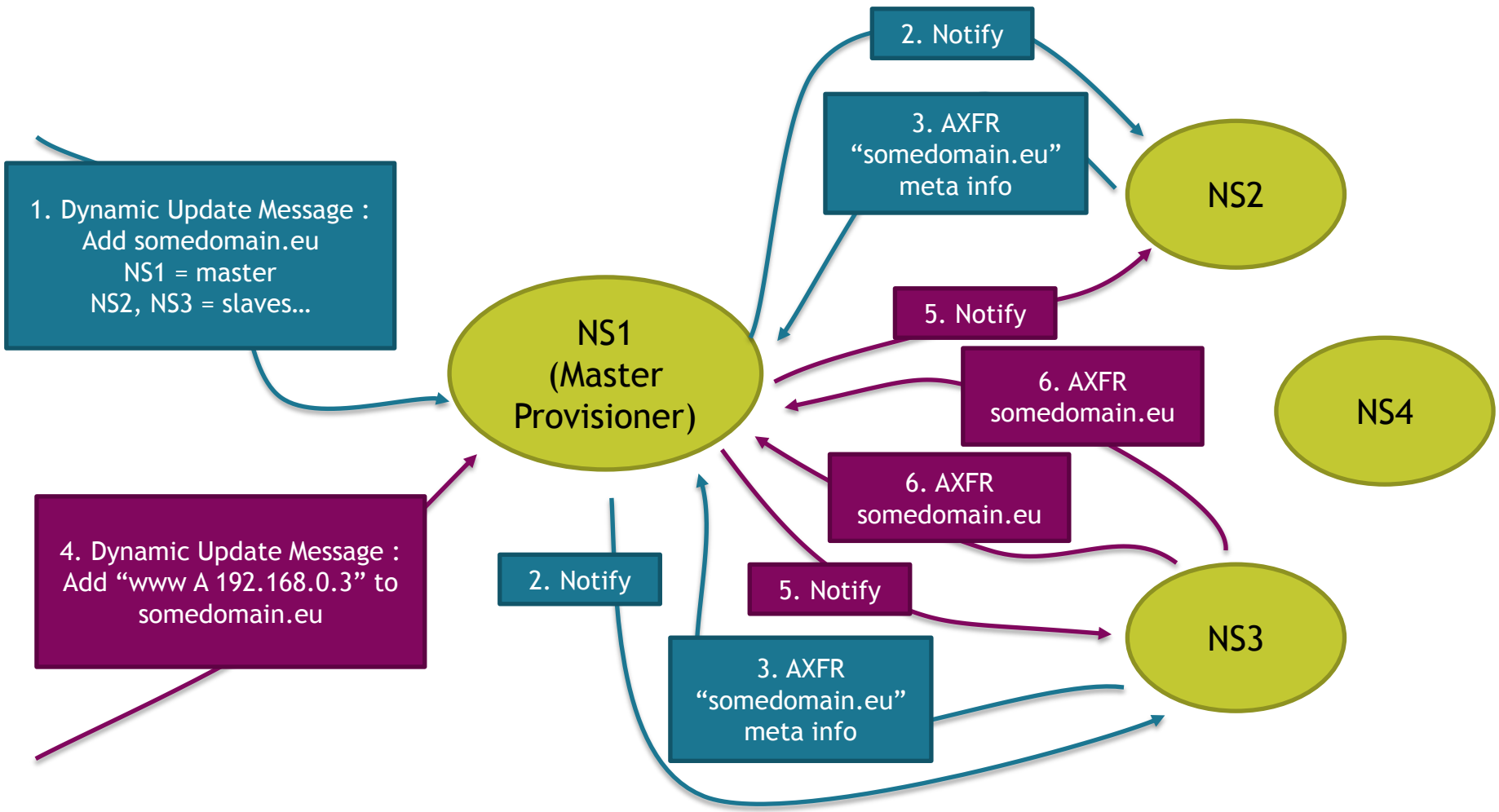
- Configuration data (zones)
  - Data in a (meta) zone

```
www.somedomain.eu.
        A       192.168.0.3
```

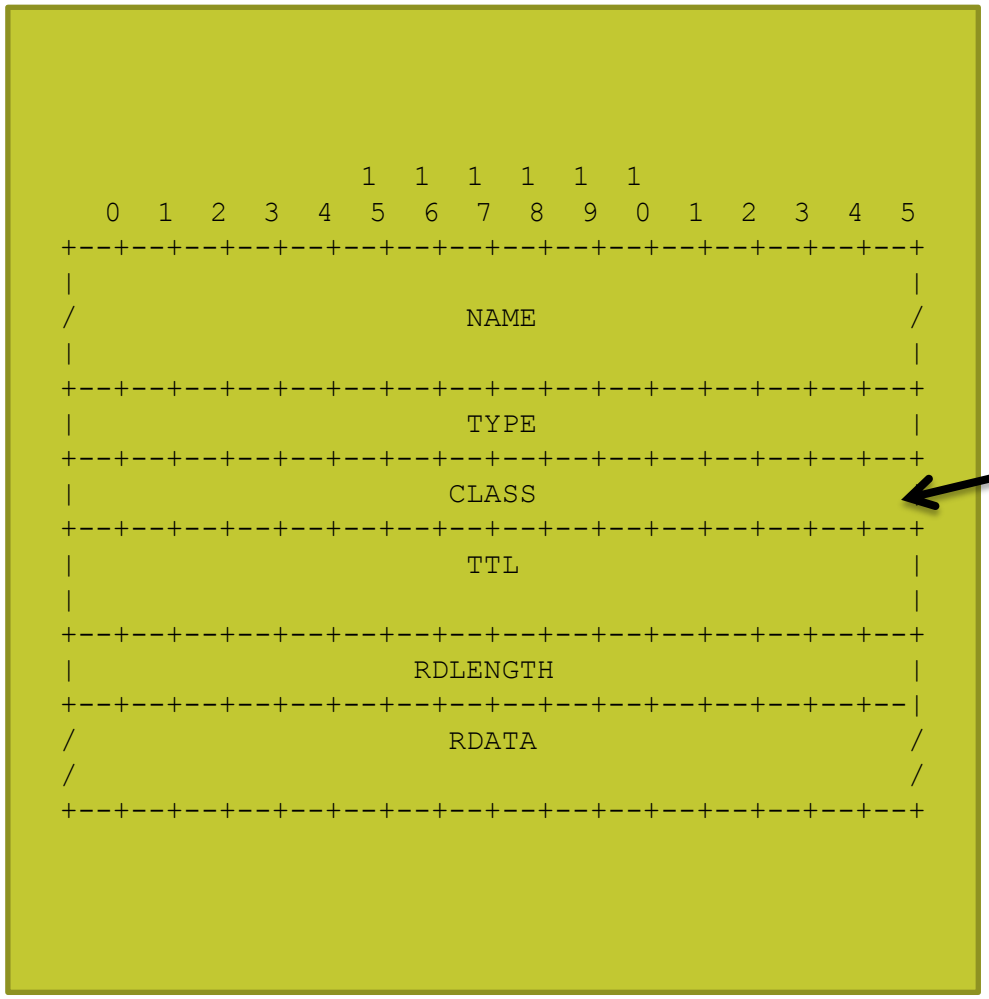
```
zone “somedomain.eu" {
   type master;
   file "/var/bind/somedomain.eu”;
   allow-transfer { @ip_secondary; }
};
```

- Use DNS channel to communicate configuration data to DNS servers
- Name servers at startup
  - Have no configuration
  - ACL/TSIG key (one key to trust them all)

Dynamic DNS provisioning



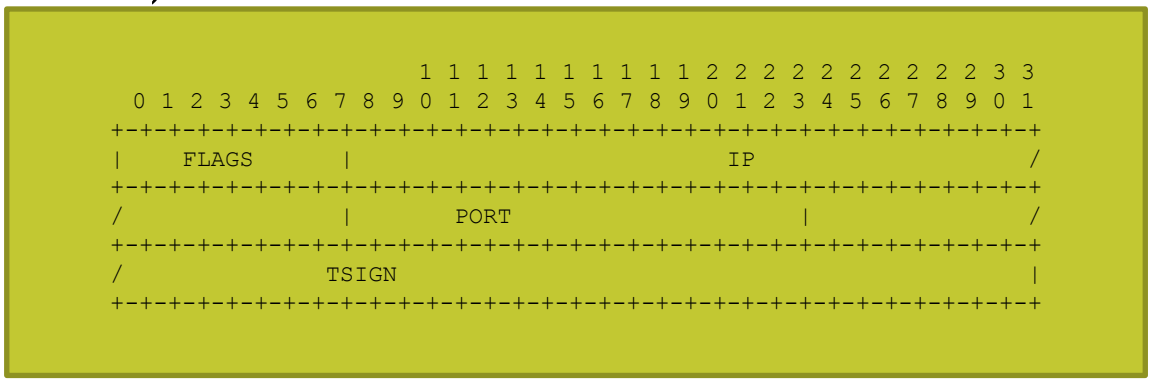
Resource Record



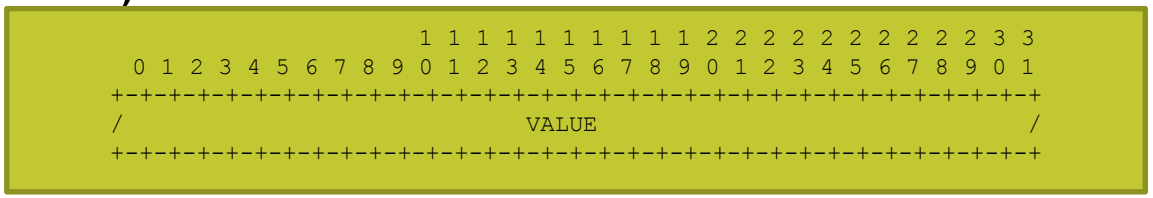
CTRL
(0x002a)
(preliminary)

RR Type (preliminary)

- MASTER (0x2a04)
  - RRDATA



- NTRFC (0x2a0b)
  - RRDATA



YADIFA (in our labs)

- Efficient handling of (very) high number of zones
- Dynamic provisioning extension
- Command line tools
- Libraries/API
- Defined the protocol

Conclusion

A standards based, interoperable, DNS message based, dynamic zone provisioning protocol.

YADIFA

- http://www.yadifa.eu
- info@yadifa.eu

EURid, the .eu registry

- http://www.eurid.eu
- info@eurid.eu