DNS Catalog Zones

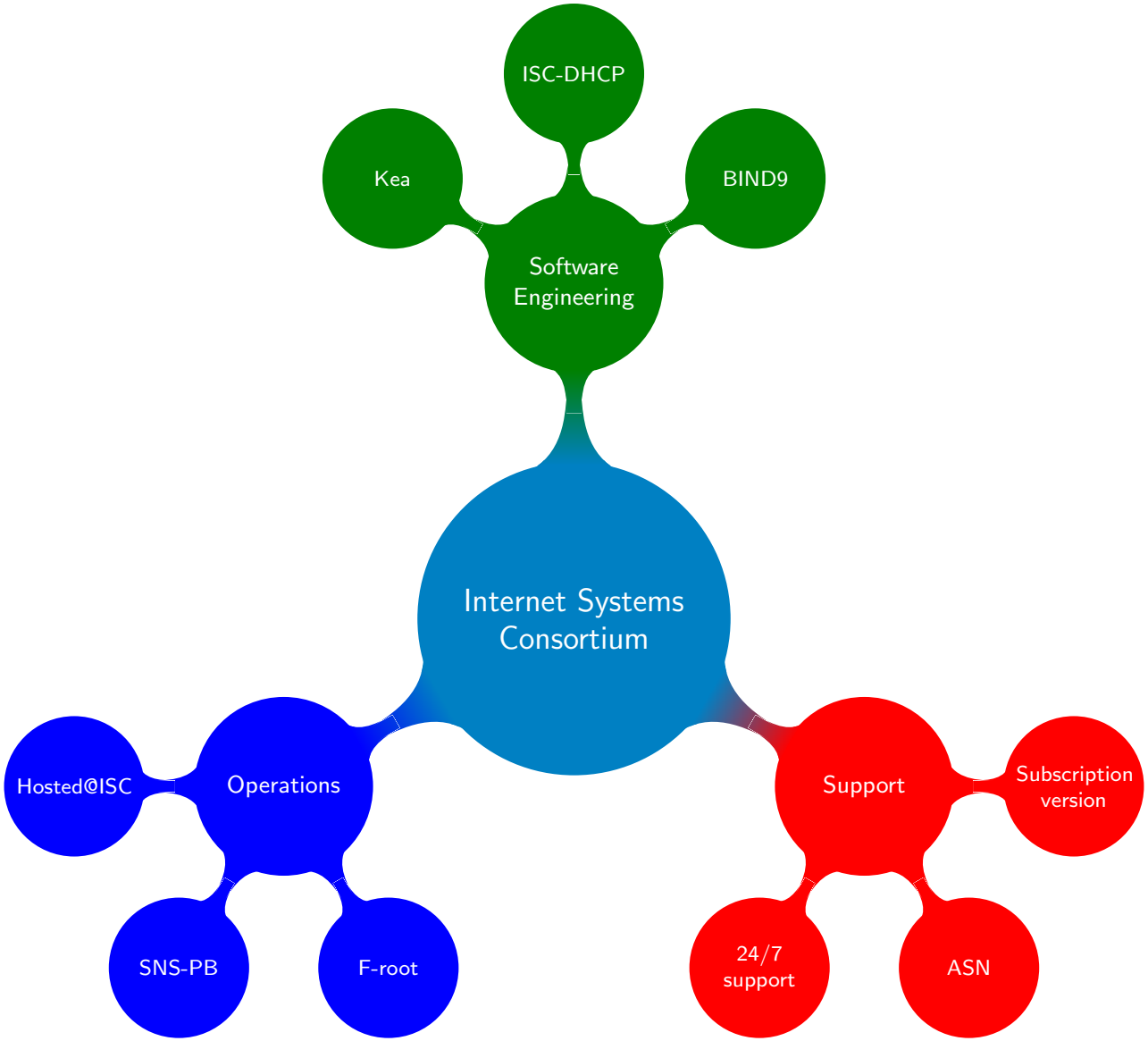
łatwe tworzenie i synchronizacja serwowanych stref

Witold Kręcicki

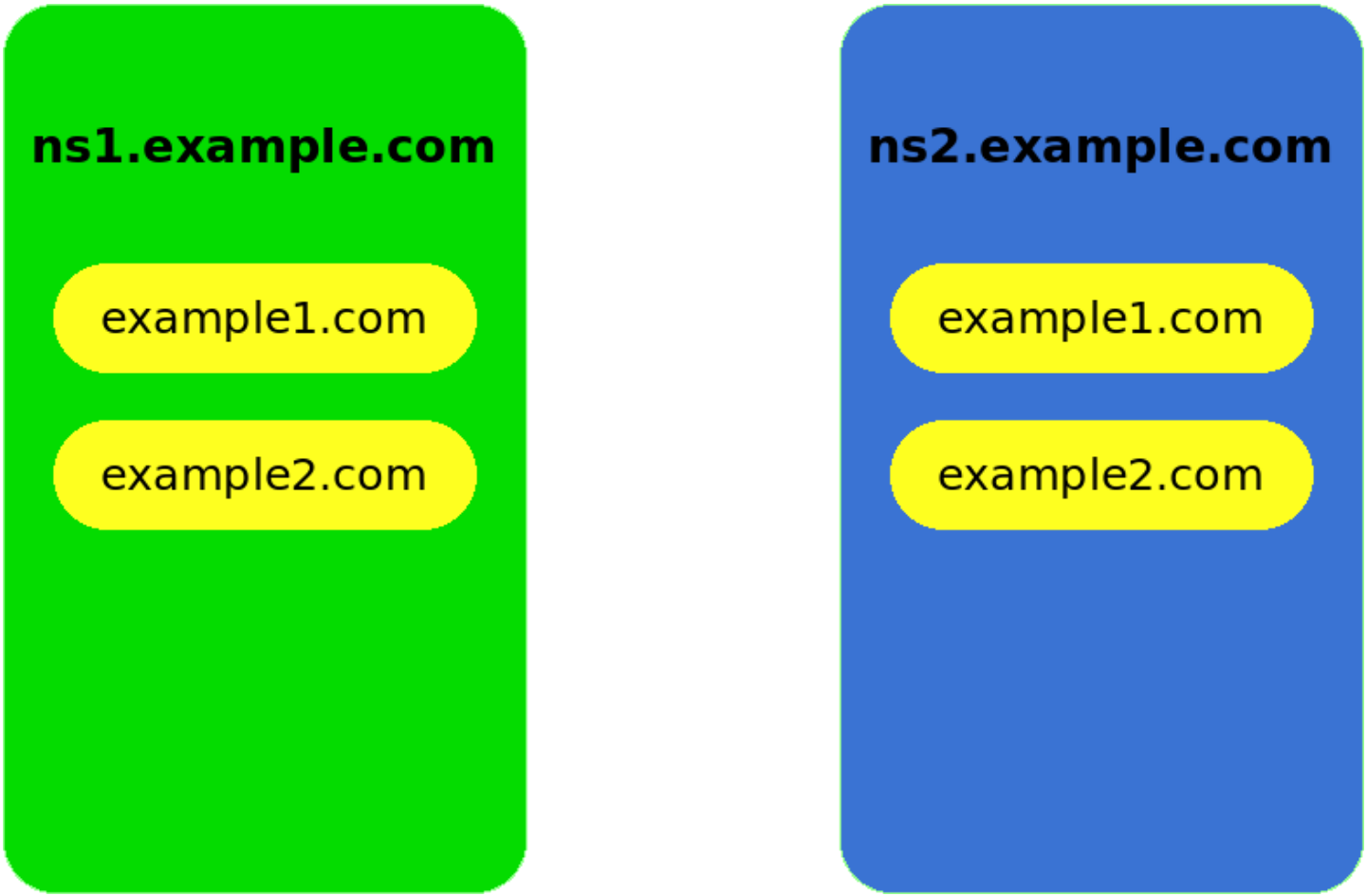
Internet Systems Consortium

23 lutego 2016

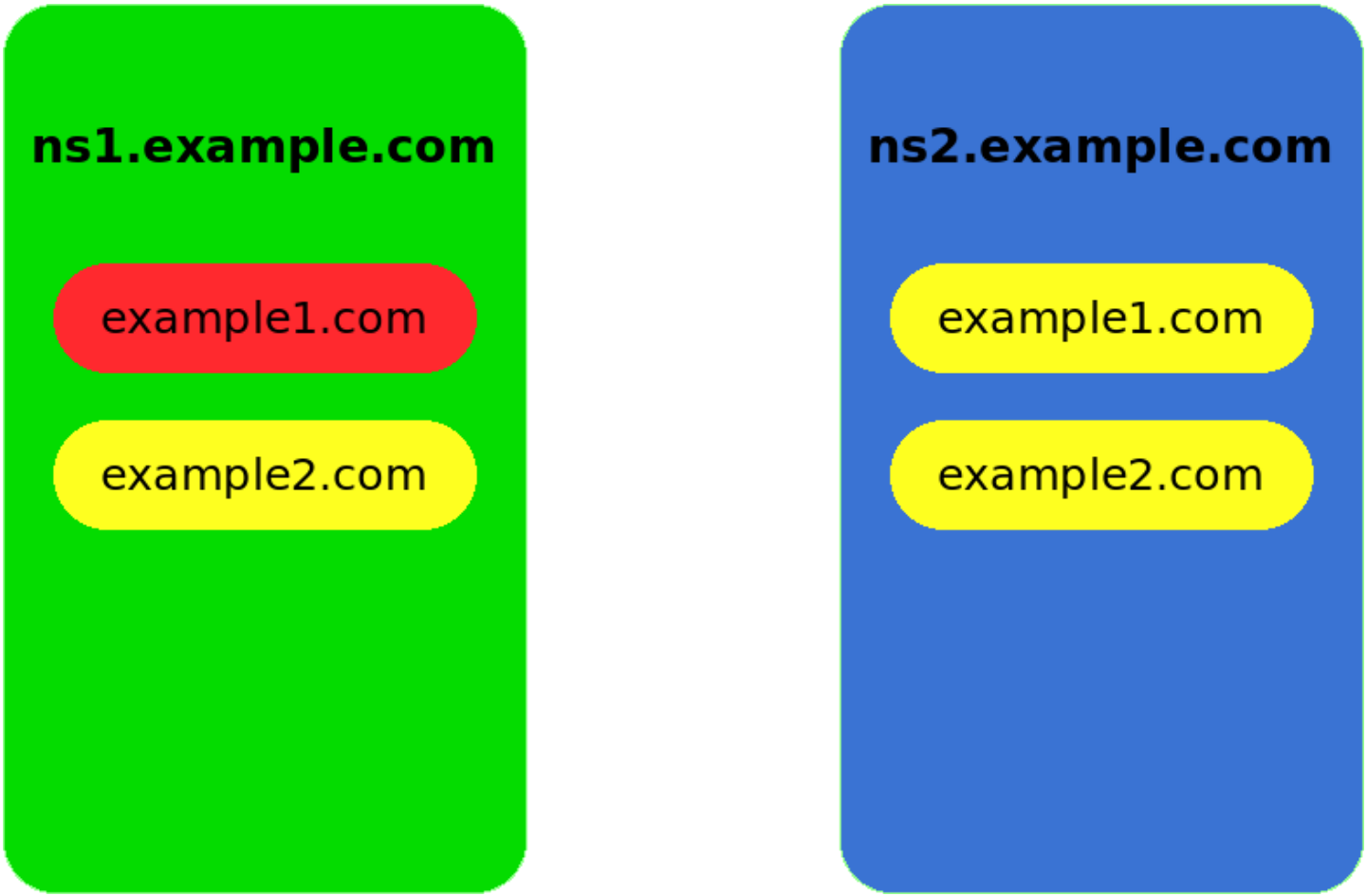
Internet Systems Consortium



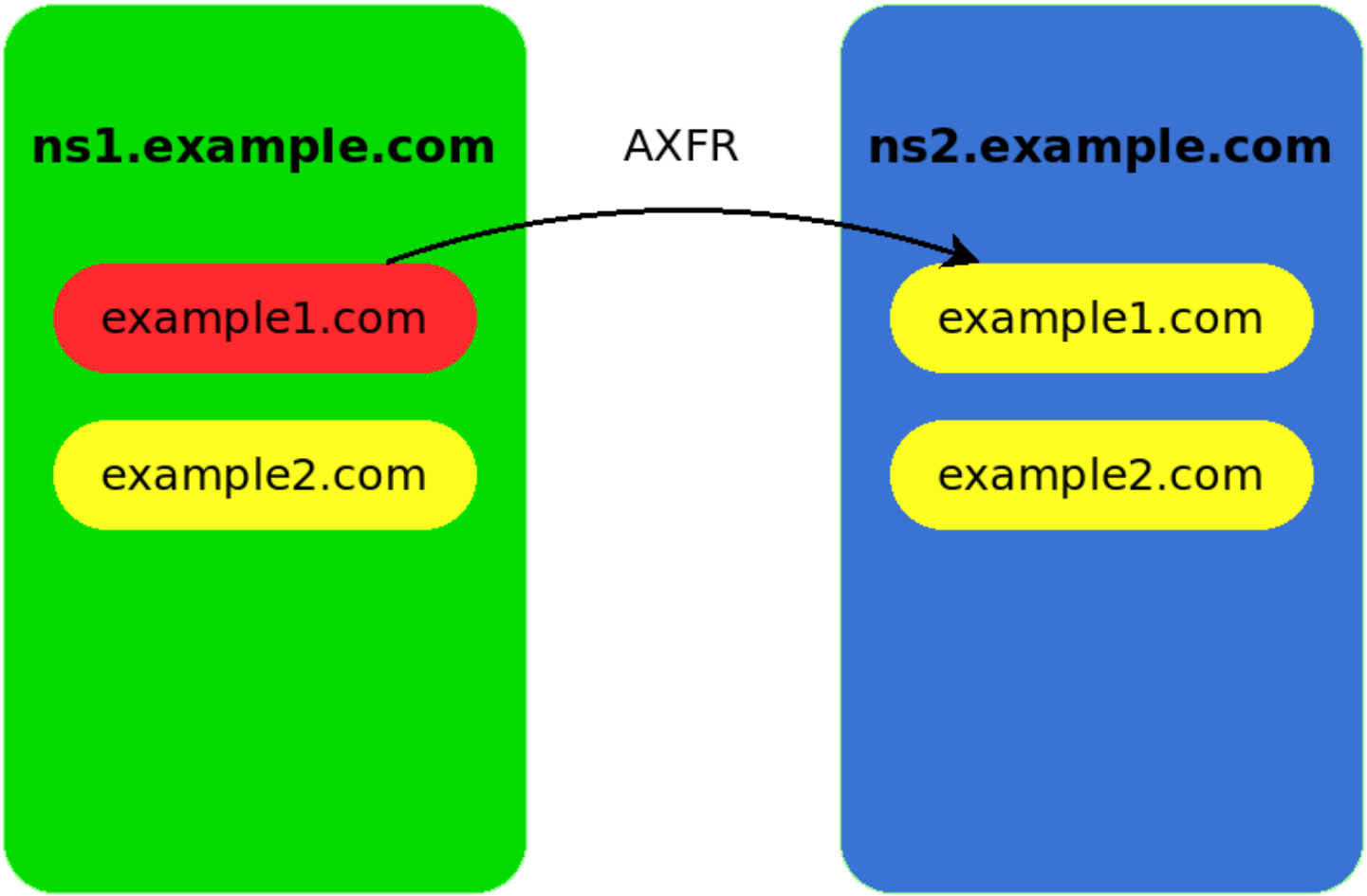
Problem?


ns1.example.com
example1.com
example2.com
ns2.example.com
example1.com
example2.com

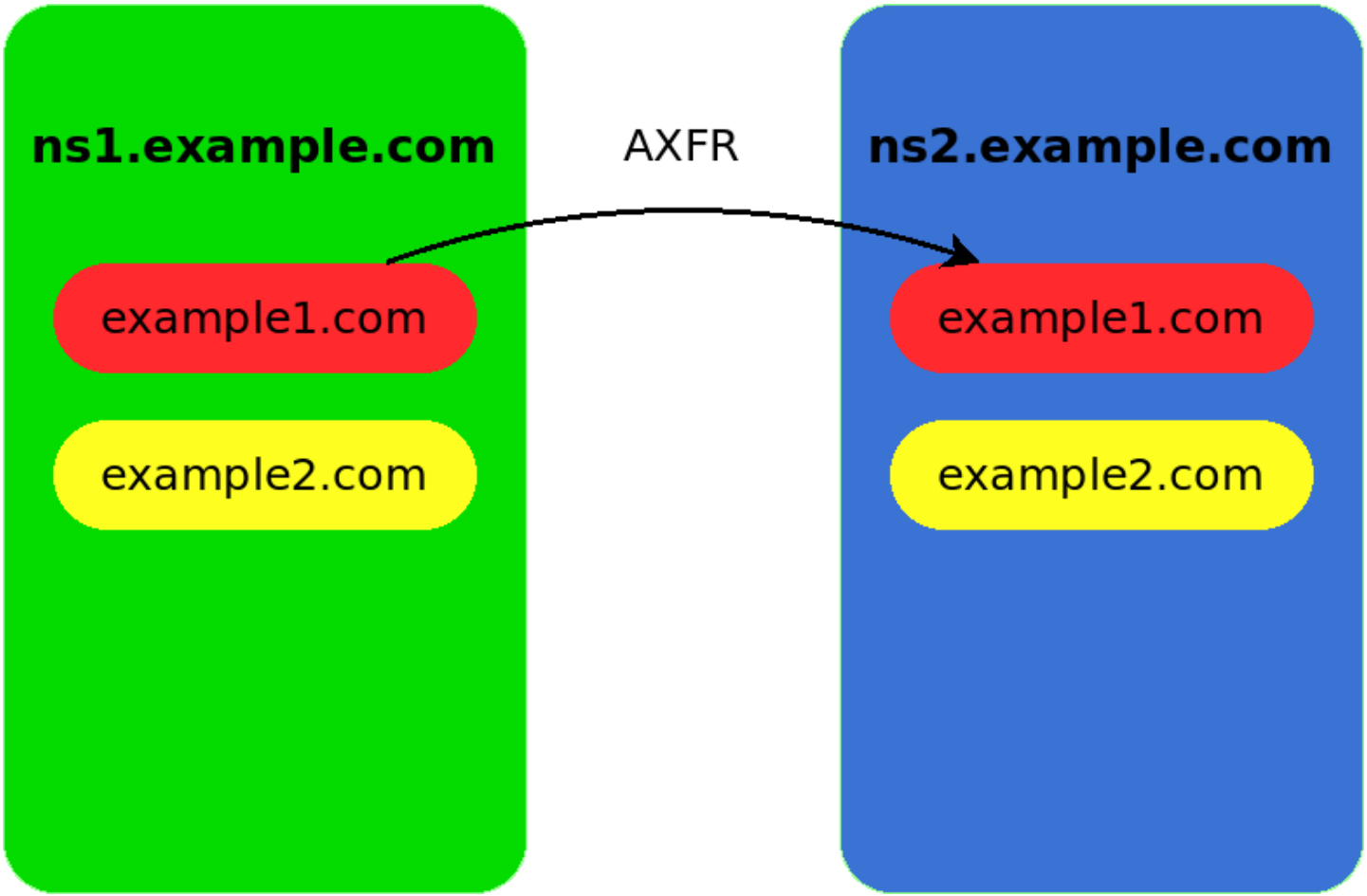
Problem?


ns1.example.com
example1.com
example2.com
ns2.example.com
example1.com
example2.com

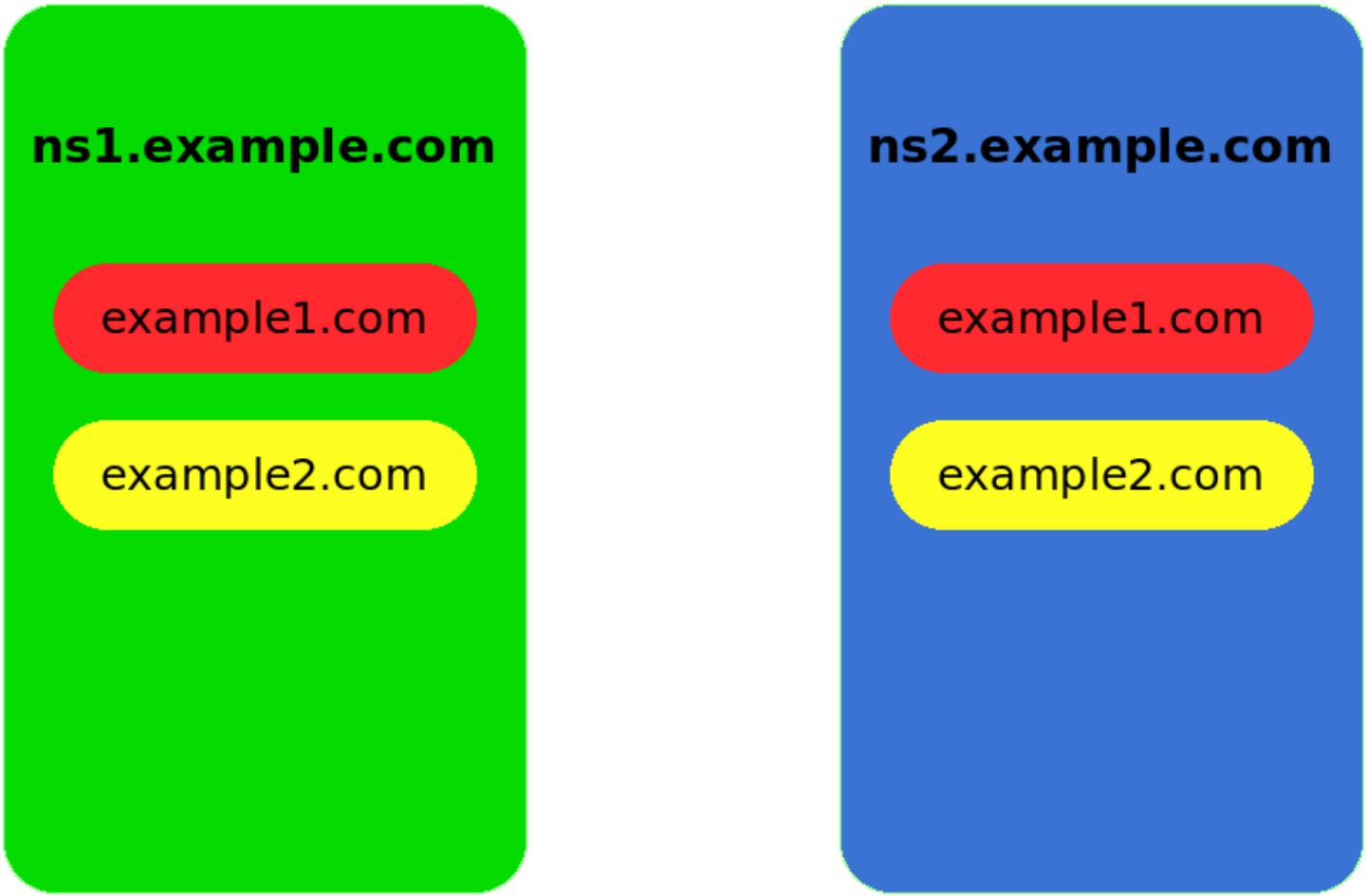
Problem?


ns1.example.com
example1.com
example2.com
AXFR
ns2.example.com
example1.com
example2.com

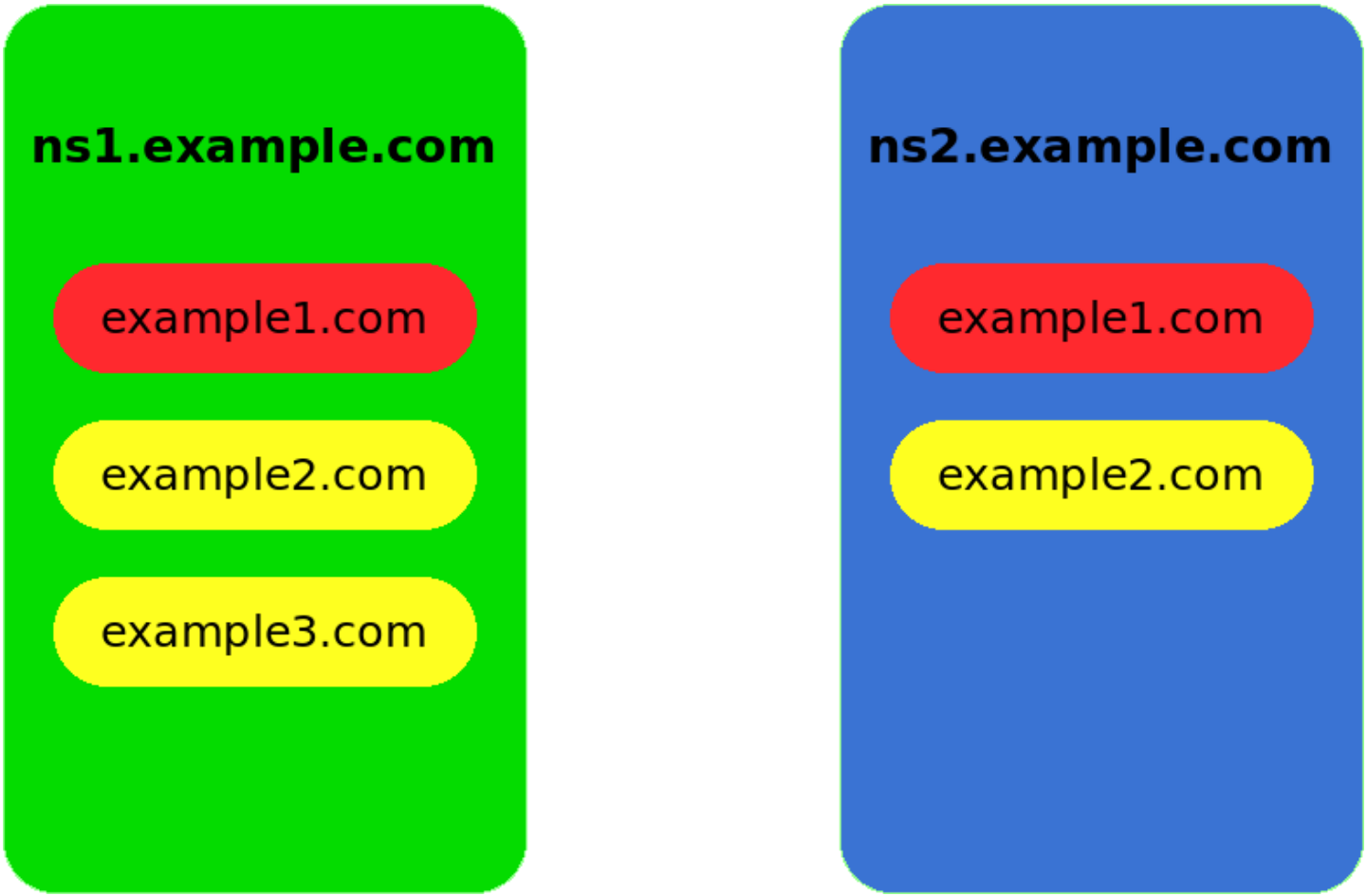
Problem?


ns1.example.com
AXFR
ns2.example.com
example1.com
example2.com
example1.com
example2.com

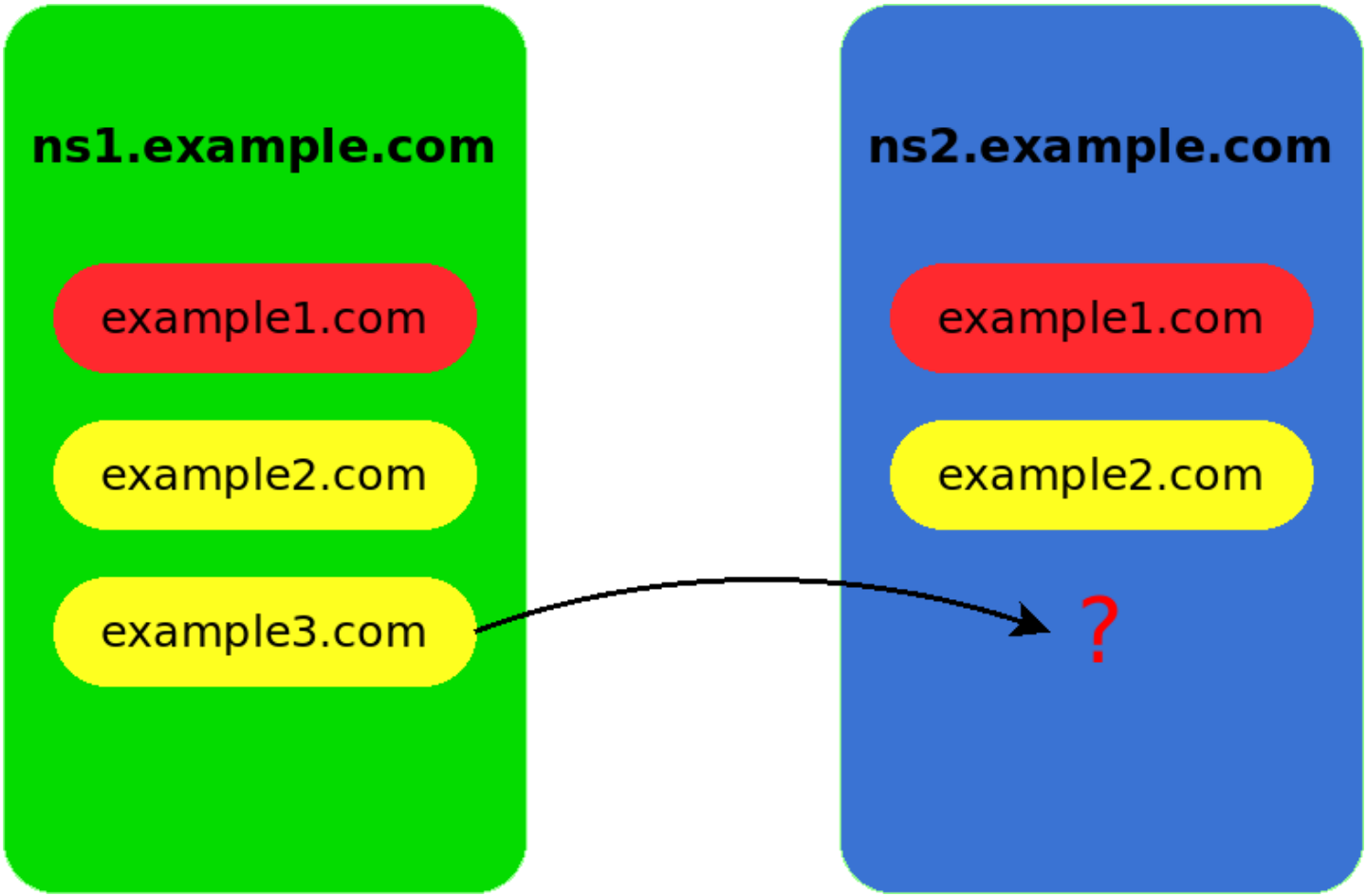
Problem?


ns1.example.com
example1.com
example2.com
ns2.example.com
example1.com
example2.com

Problem?


ns1.example.com
example1.com
example2.com
example3.com
ns2.example.com
example1.com
example2.com

Problem?


ns1.example.com
example1.com
example2.com
example3.com
ns2.example.com
example1.com
example2.com
?

Historia

- *1983* - RFC882, RFC883 - pierwsze podejście, już z XFR!
- *1986* - RFC1034, RFC1035 - DNS jaki mamy dziś
- *2010* - RFC5963 - oczyszczenie AXFR
- w 1986 roku domen było kilkaset, dodanie nowej było 'wydarzeniem', nikt nie potrzebował automatyzacji
- zone catalog - dziura...

Co mamy teraz

- Generowanie na podstawie bazy danych
- SCP (jak XFR u DJB)
- 'supermaster' w PowerDNS - notify tworzy domenę, nie można usunąć
- skrypty, hacki, śrubokręty
- brak rozwiązania systemowego
- brak interoperability
- out-of-band

Czego potrzebują użytkownicy?

90% definicji stref to:

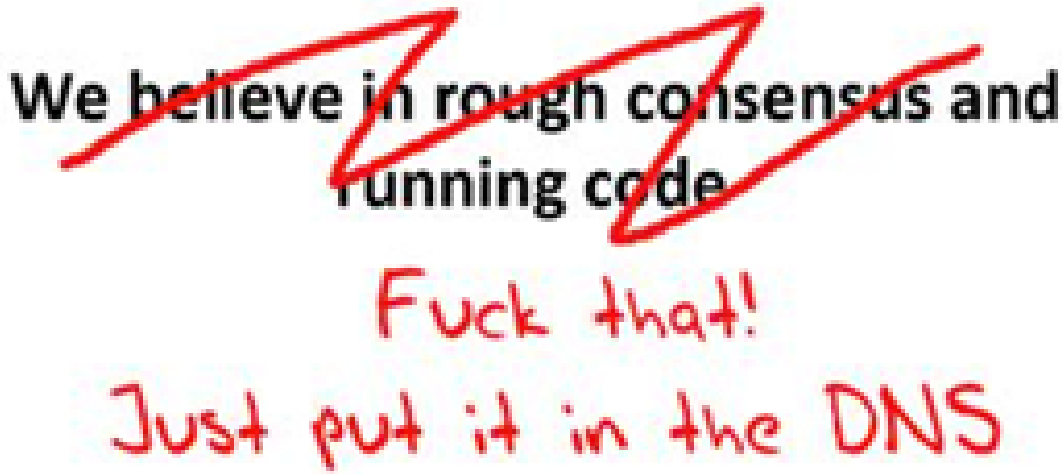
```
zone "foo.com" { masters "1.2.3.4"; };
zone "bar.com" { masters "1.2.3.4"; };
zone "baz.com" { masters "1.2.3.4"; };
```

Z pozostałych 10% - 90% to:

```
zone "lor.com" { masters "5.6.7.8"; };
zone "emi.com" { masters "9.10.11.12"; };
zone "psu.com" { masters "13.14.15.16"; };
```

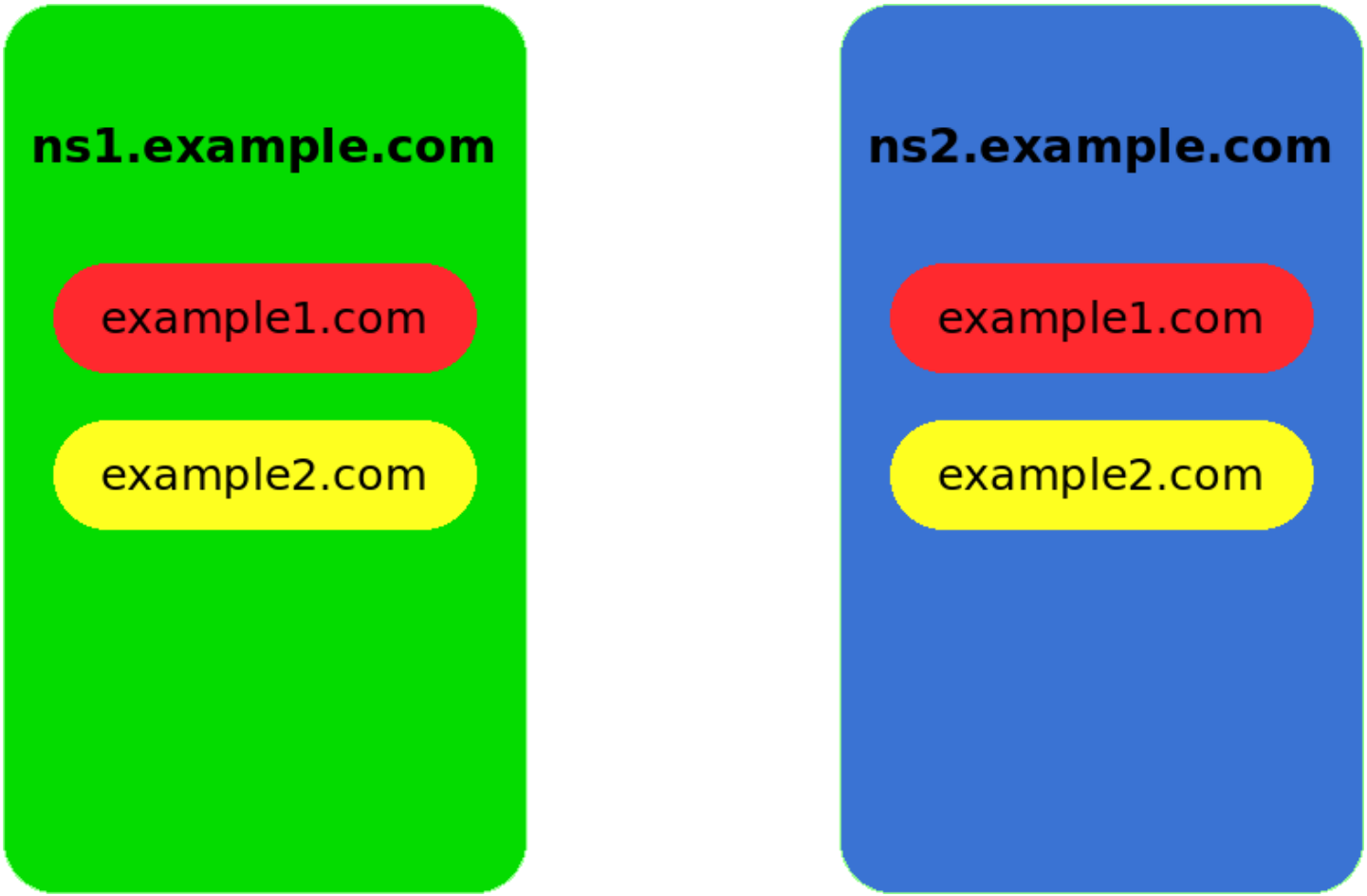
Czasami zdarza się allow-query, allow-transfer

Zone catalog zone

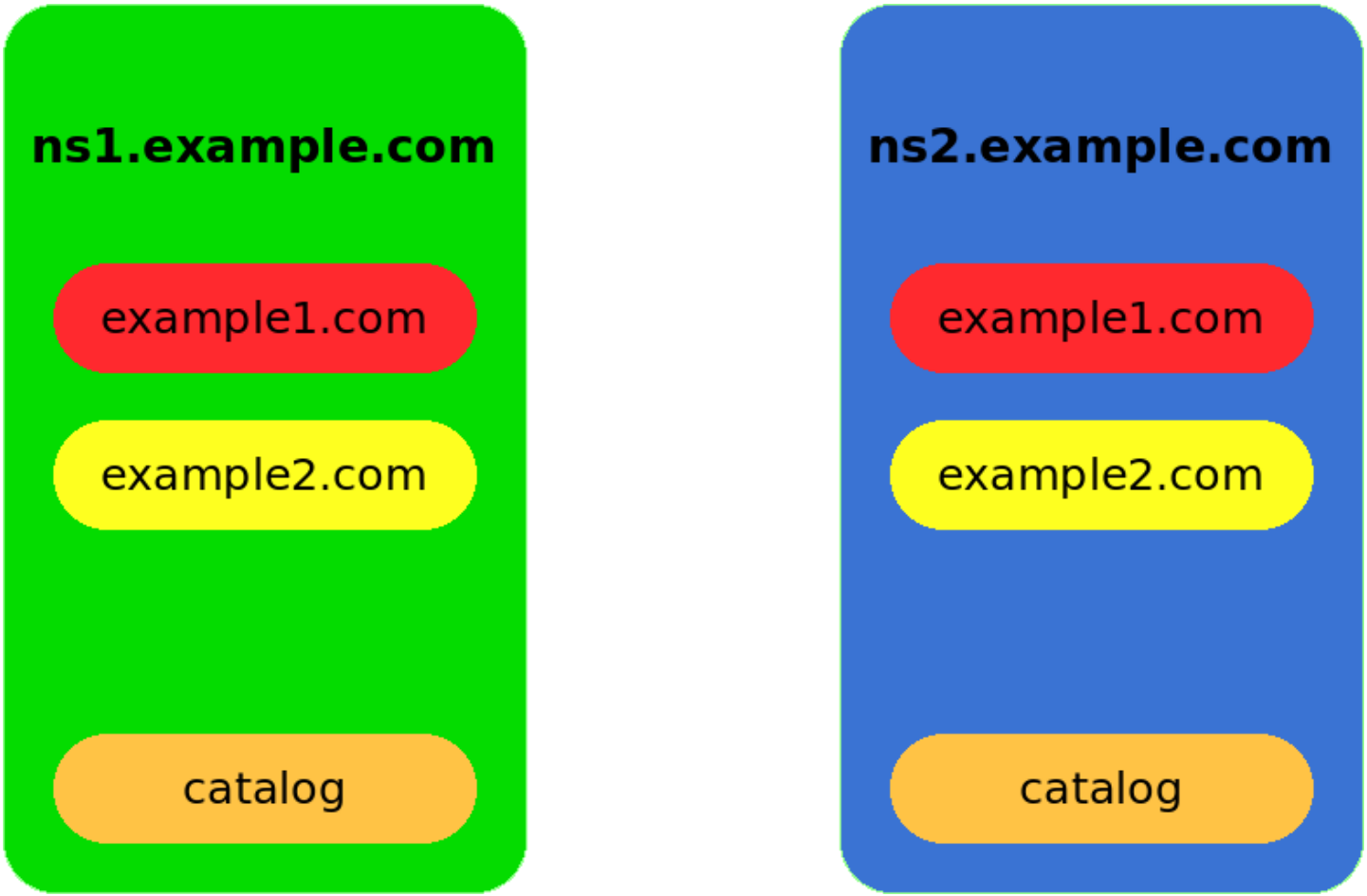


- Pierwsze podejście - Paul Vixie - Metazones (2005)
- Wbudowane w serwer
- Ustandaryzowane w ramach IETF - draft w DNSOP
- Docelowo obsługiwane przez różne implementacje

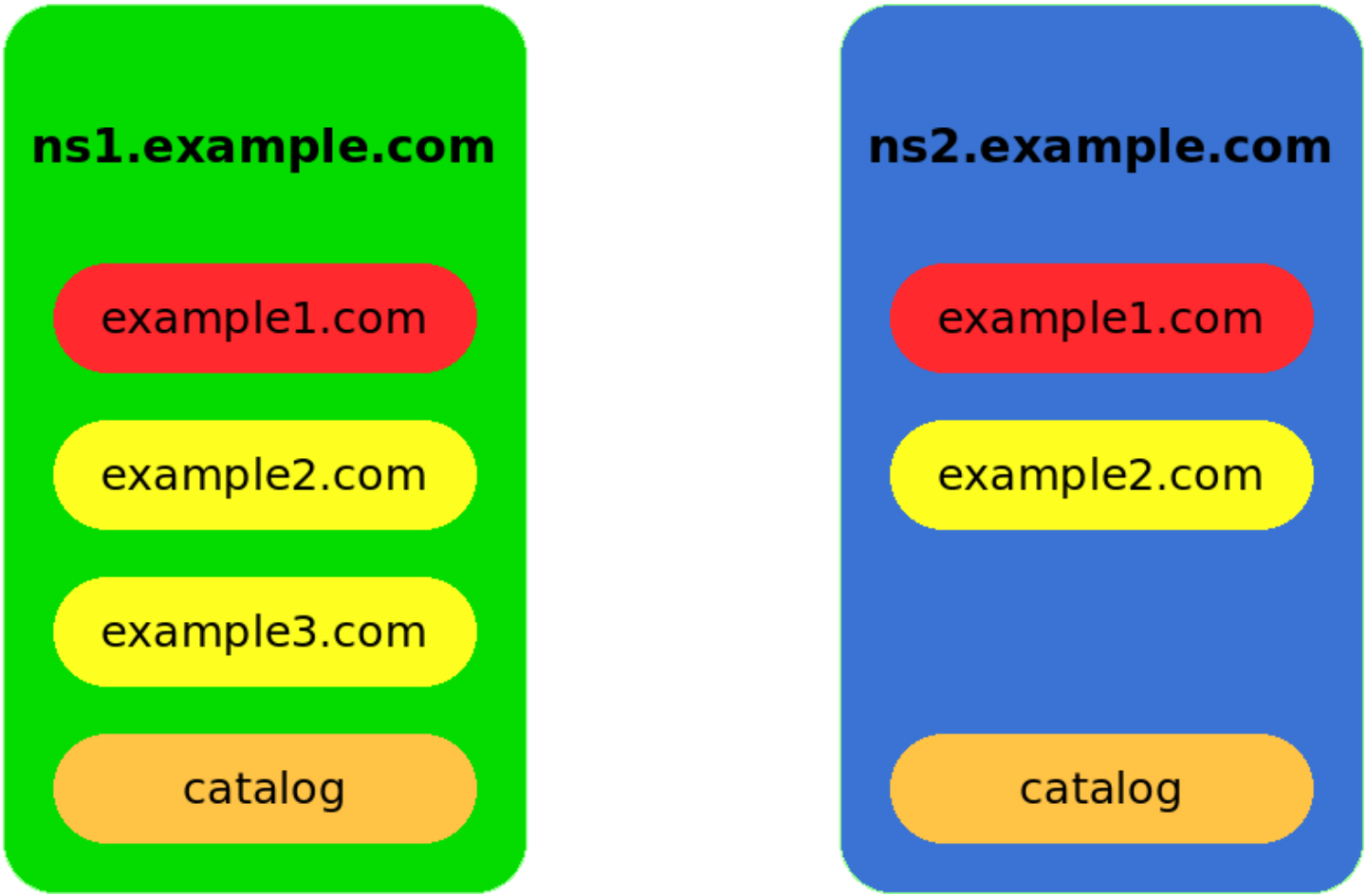
Rozwiązanie!



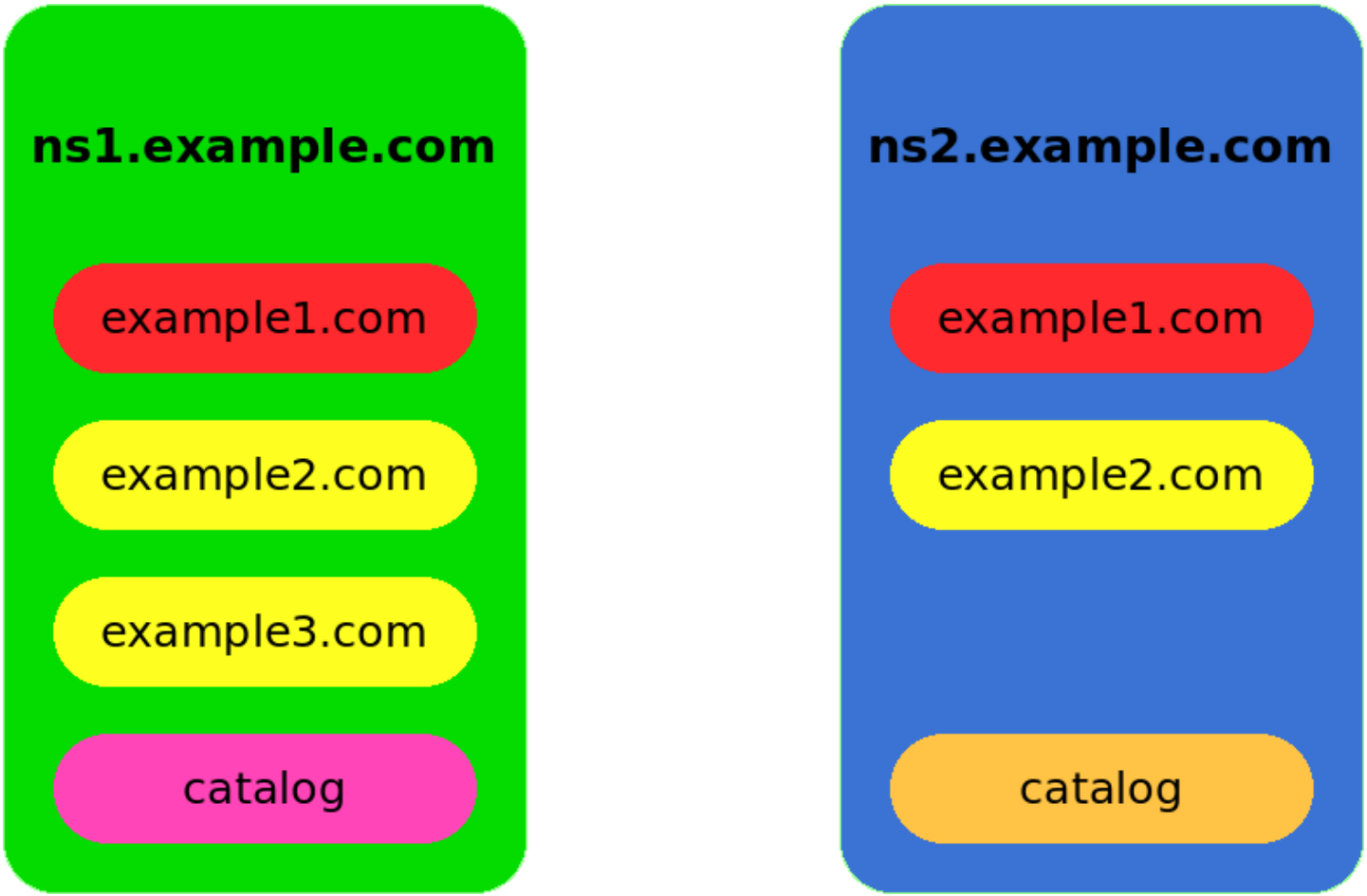
Rozwiązanie!



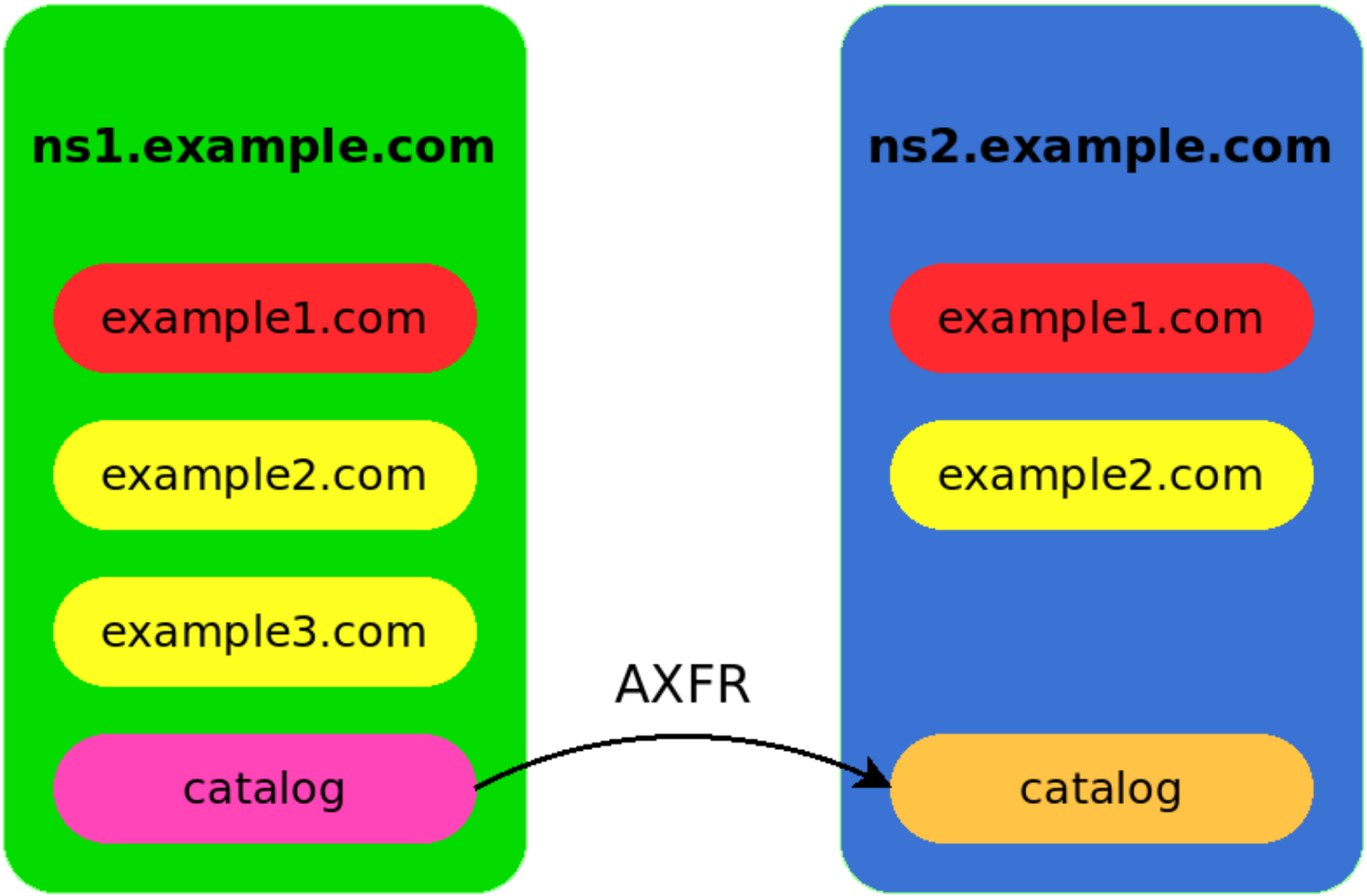
Rozwiązanie!



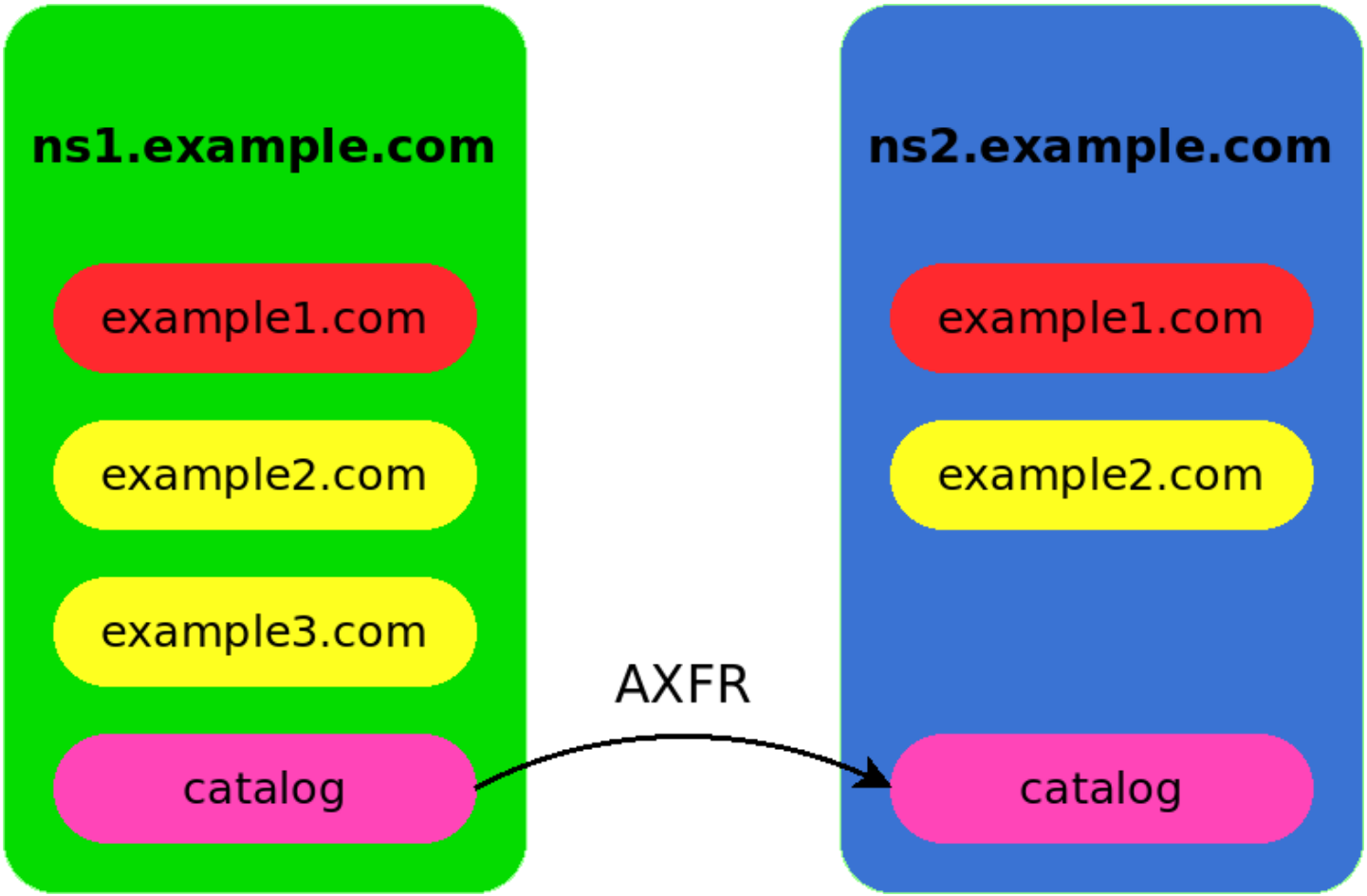
Rozwiązanie!



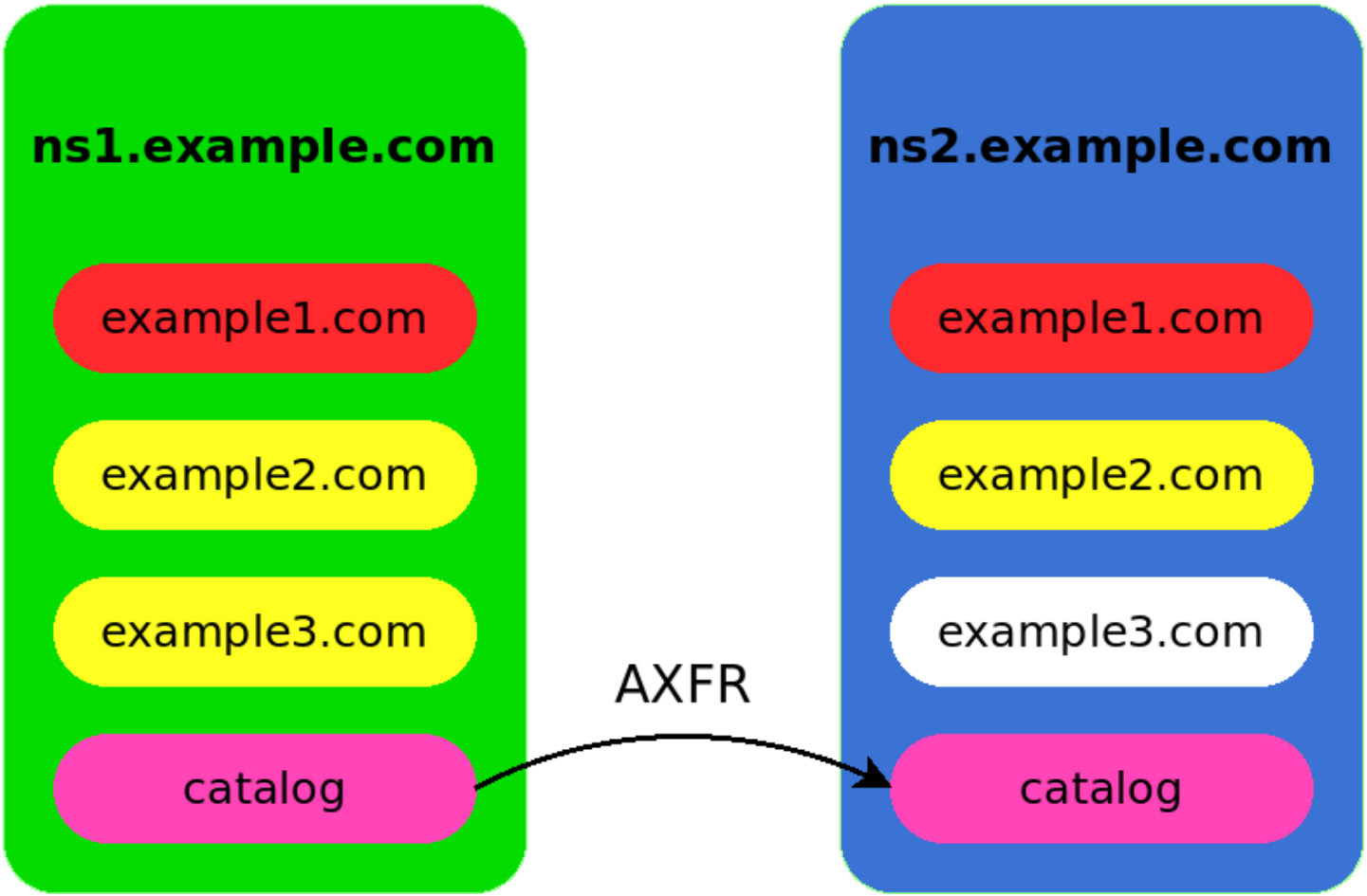
Rozwiązanie!



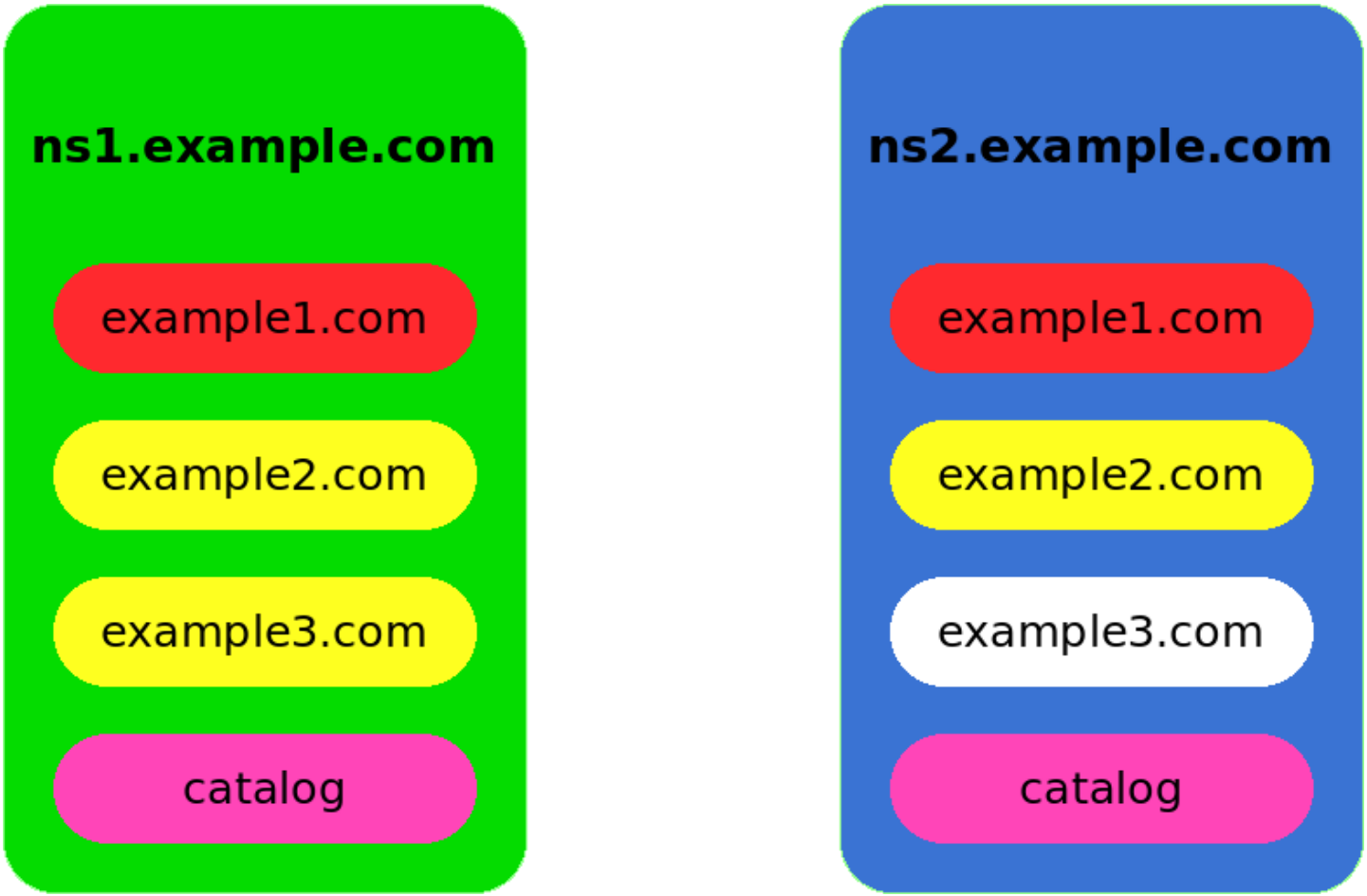
Rozwiązanie!



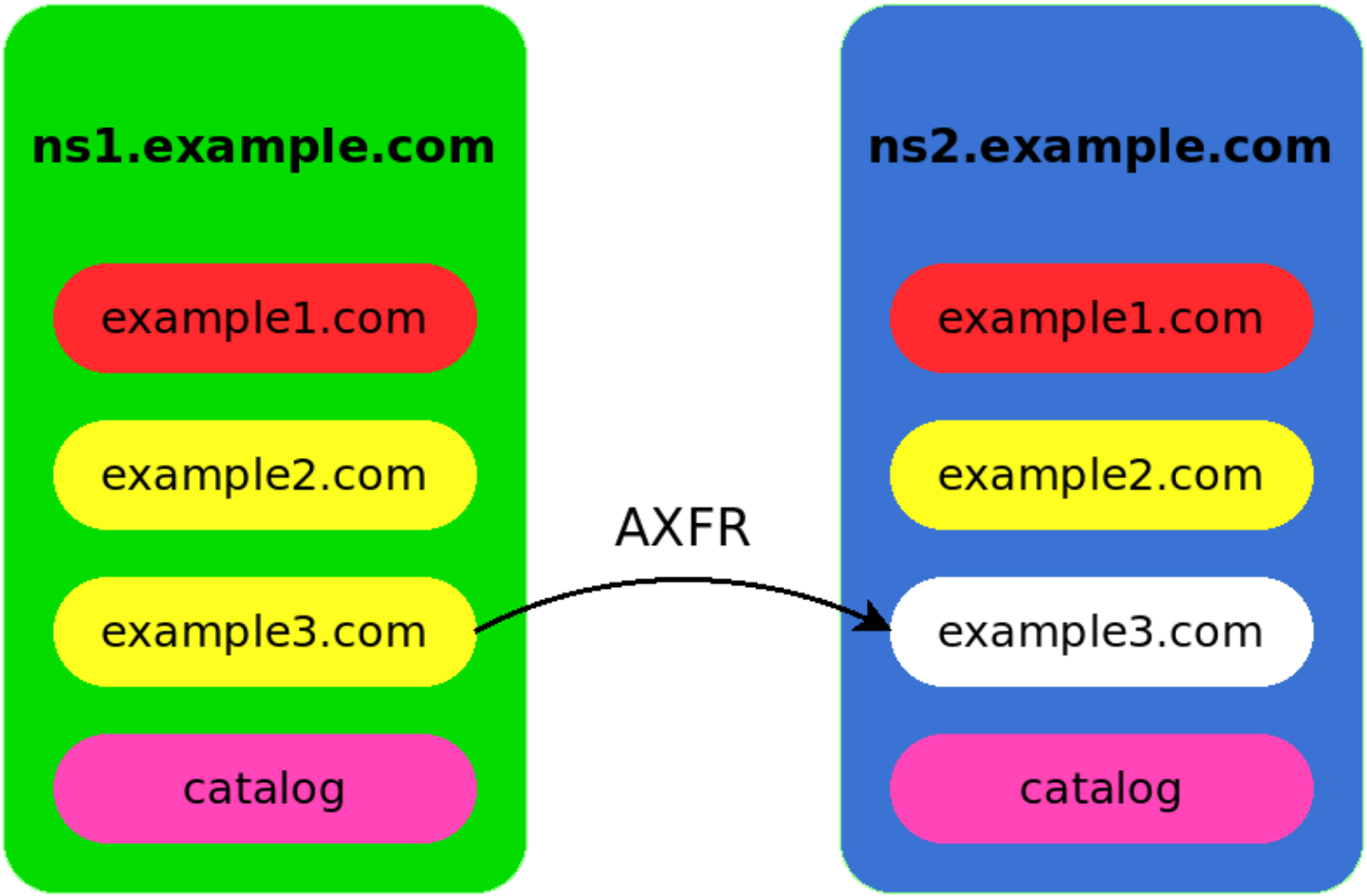
Rozwiązanie!



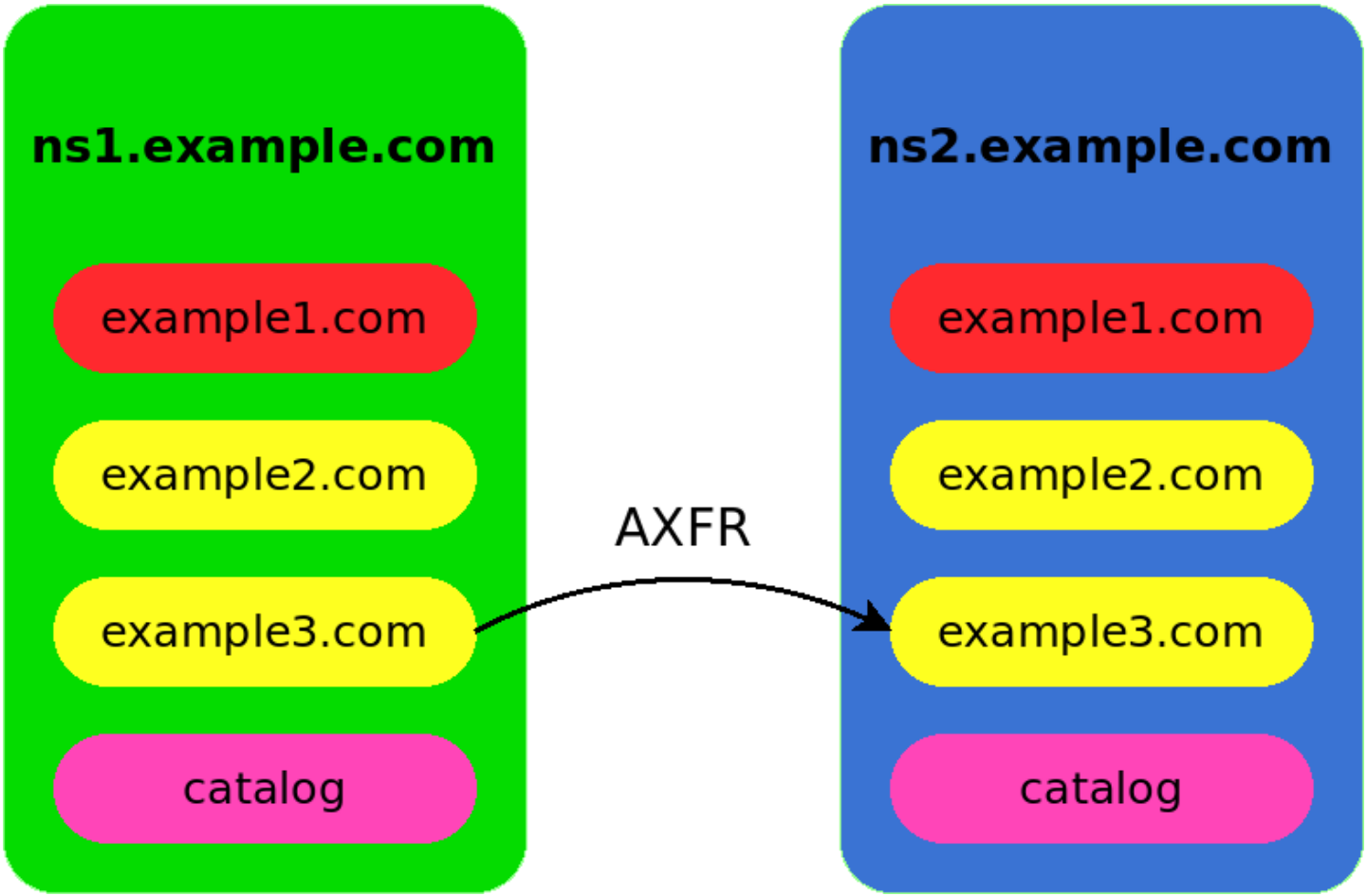
Rozwiązanie!



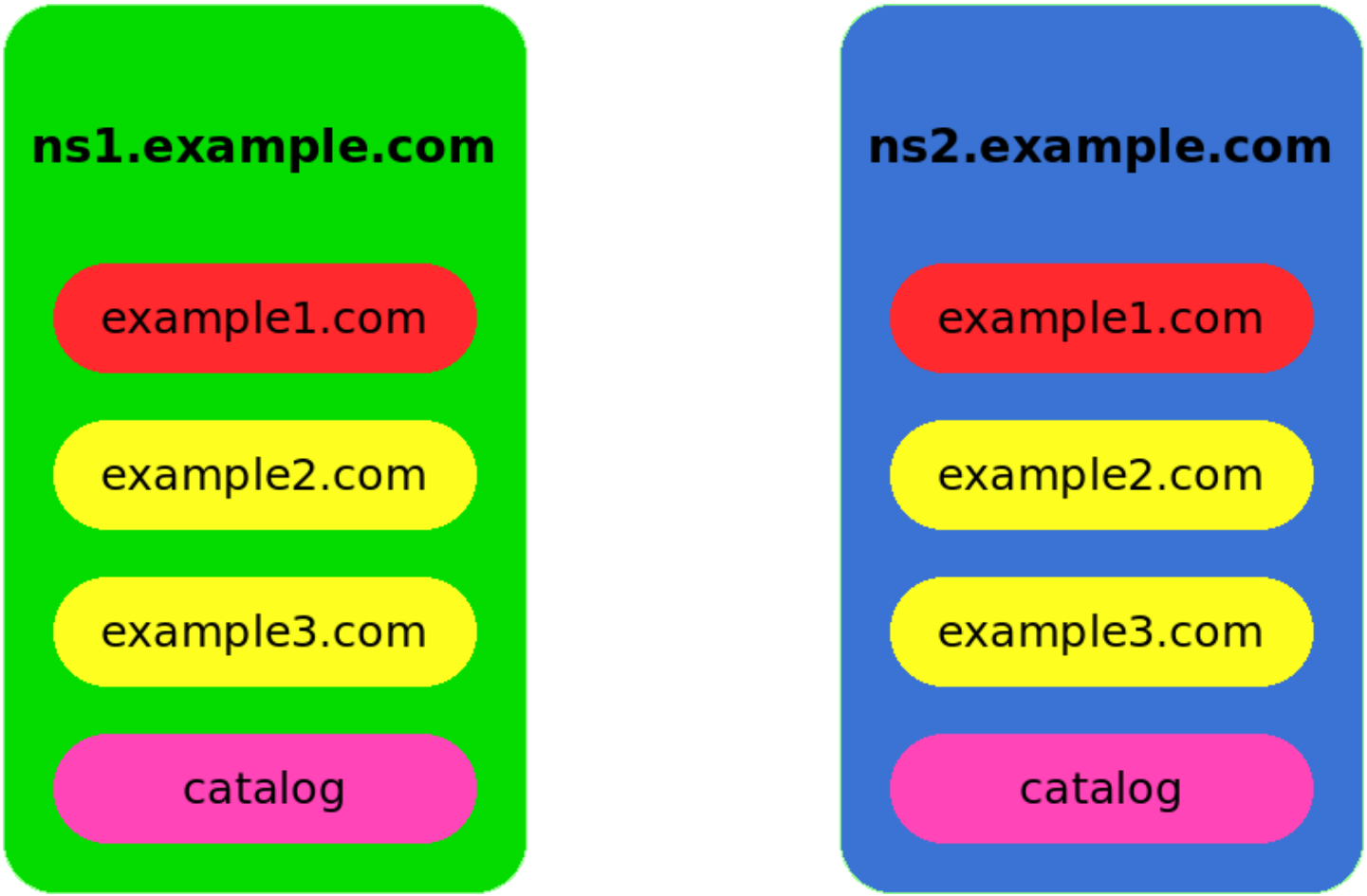
Rozwiązanie!



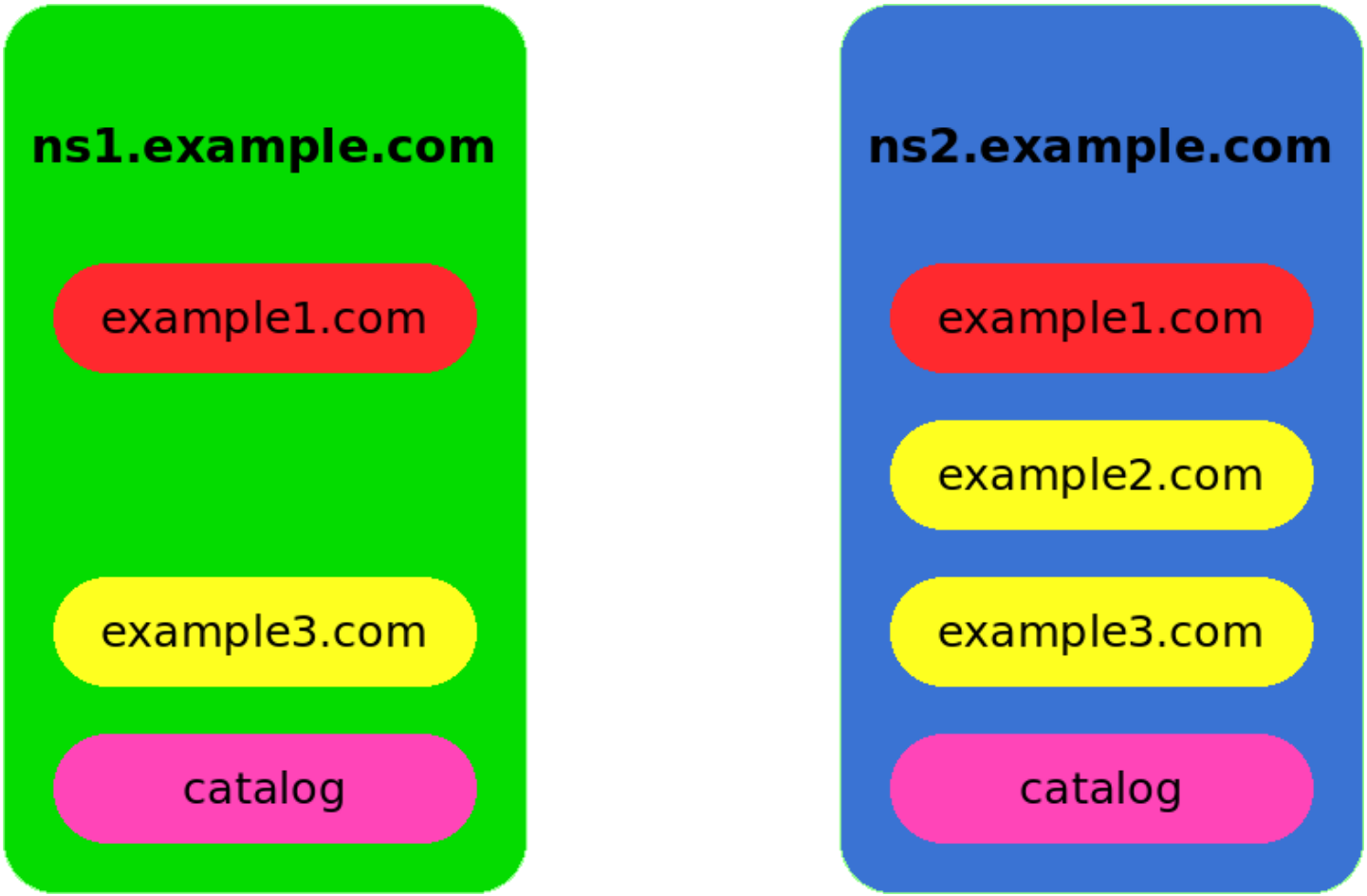
Rozwiązanie!



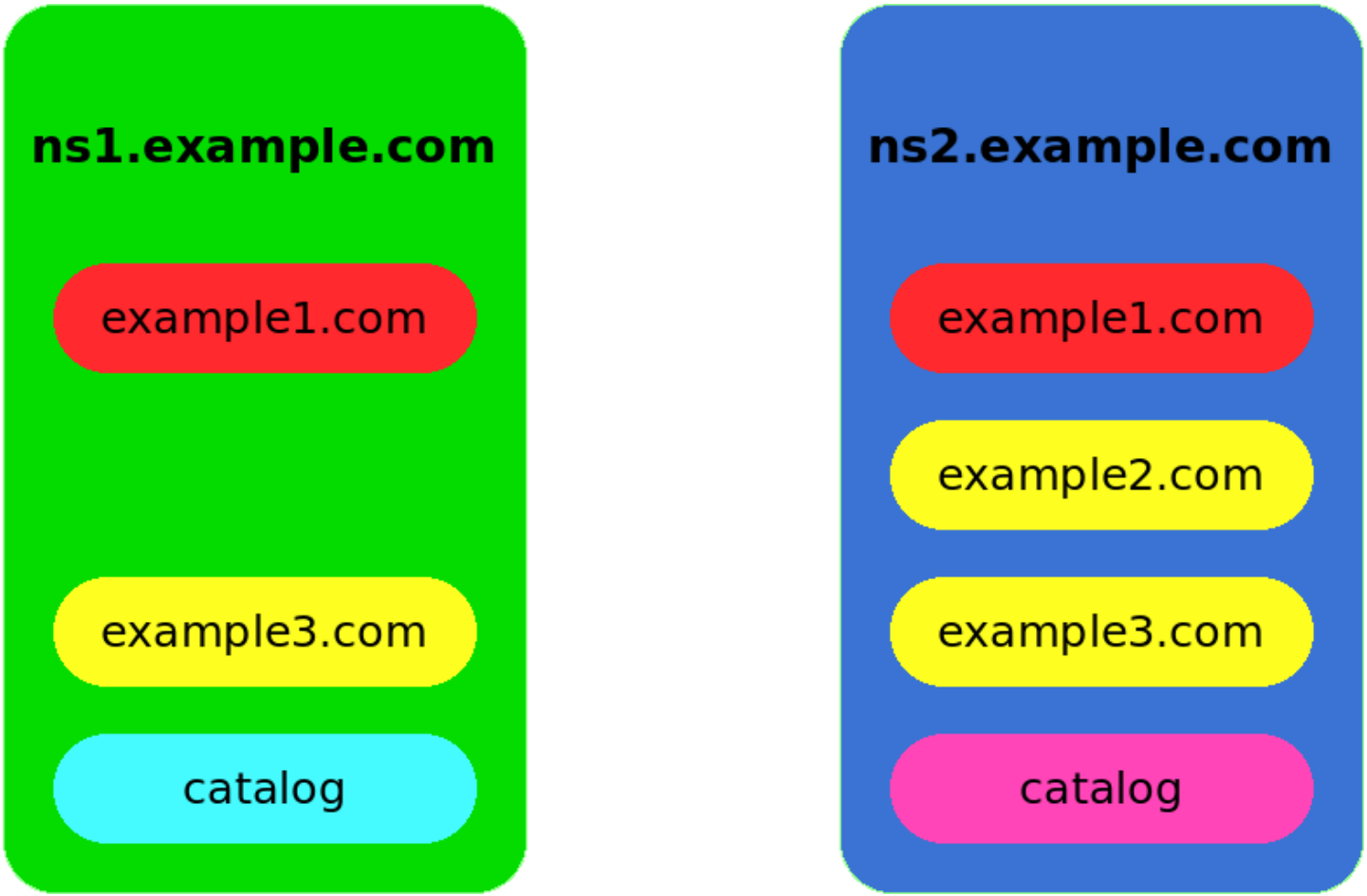
Rozwiązanie!



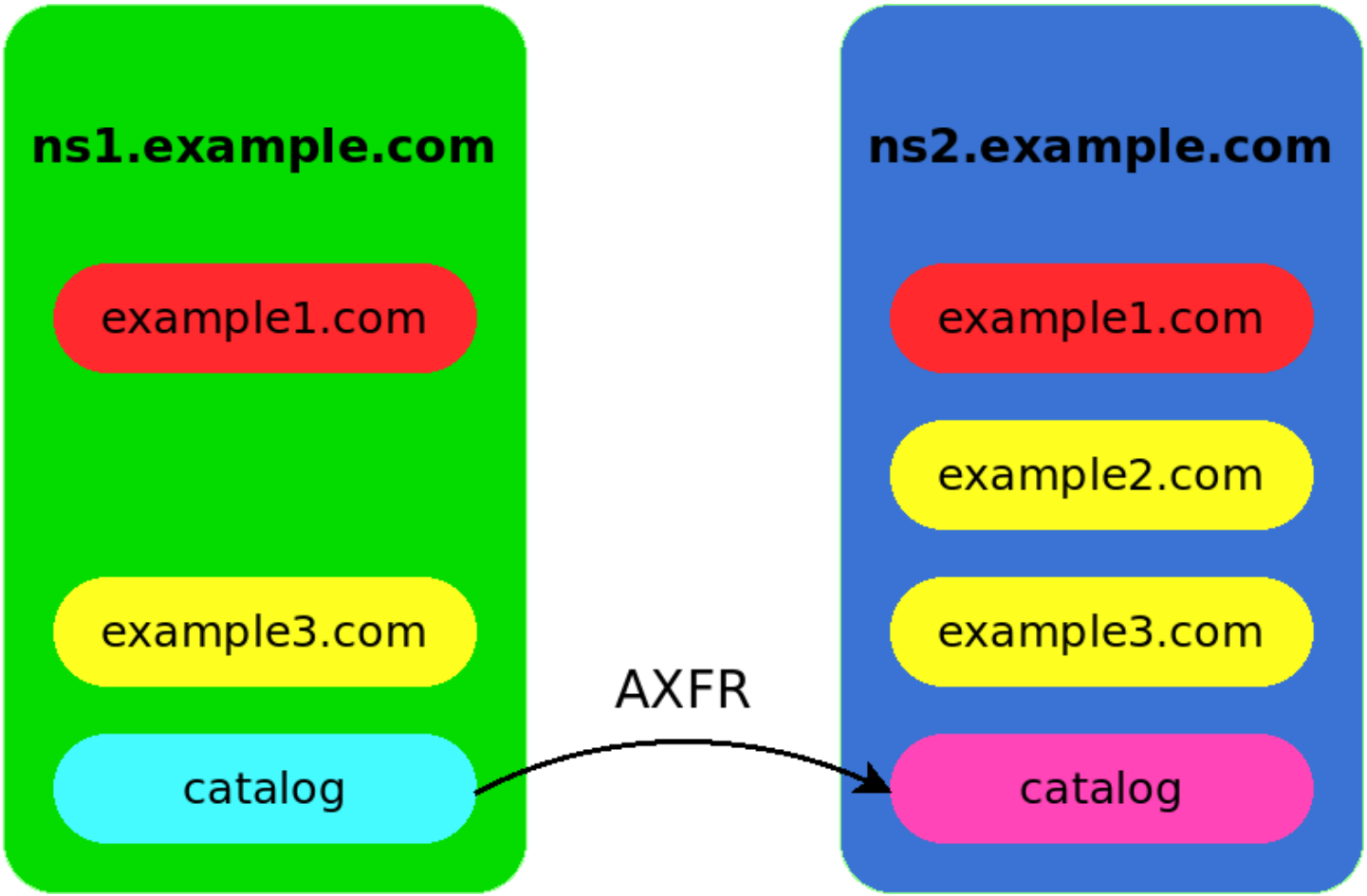
Rozwiązanie!



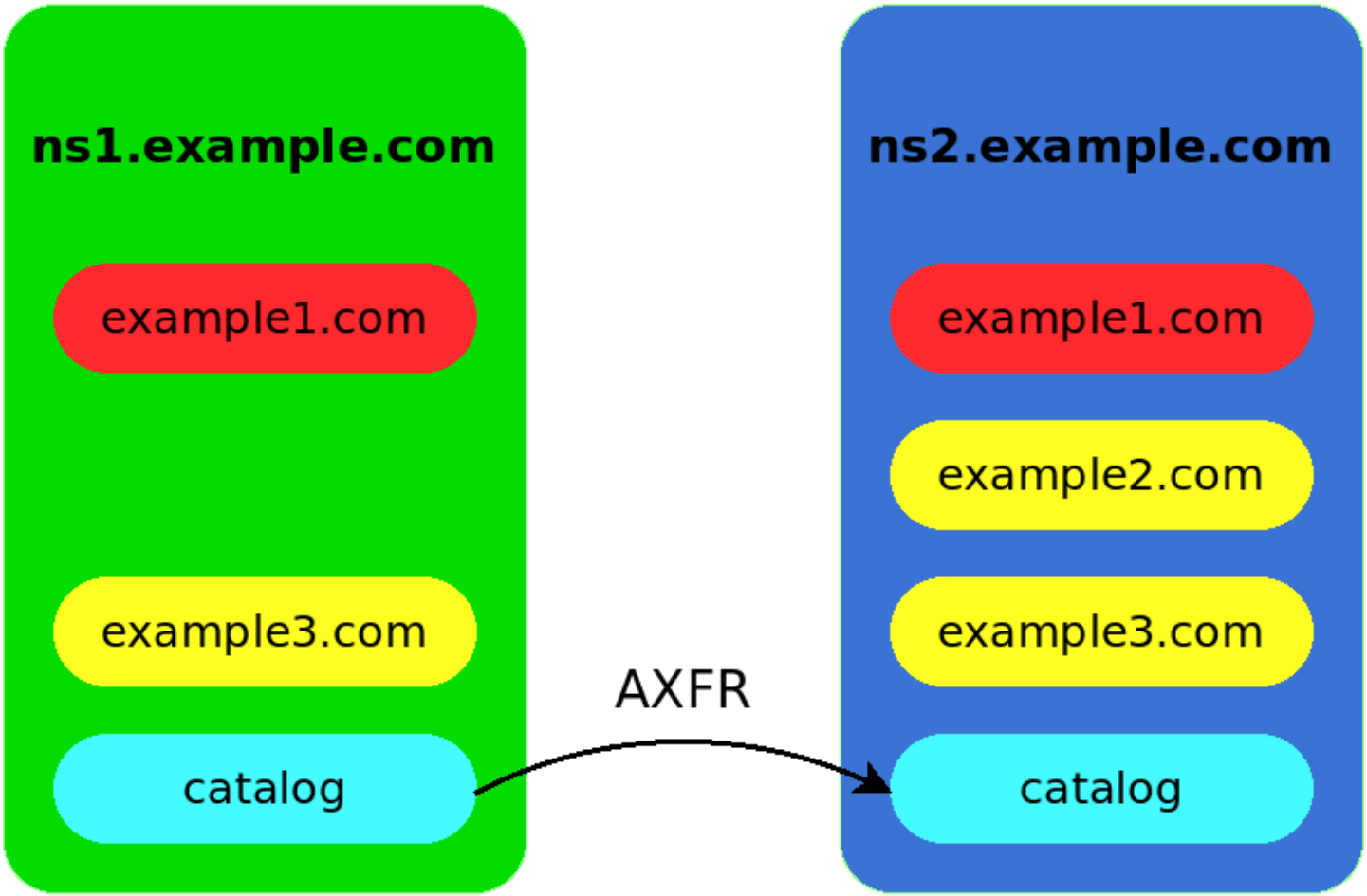
Rozwiązanie!



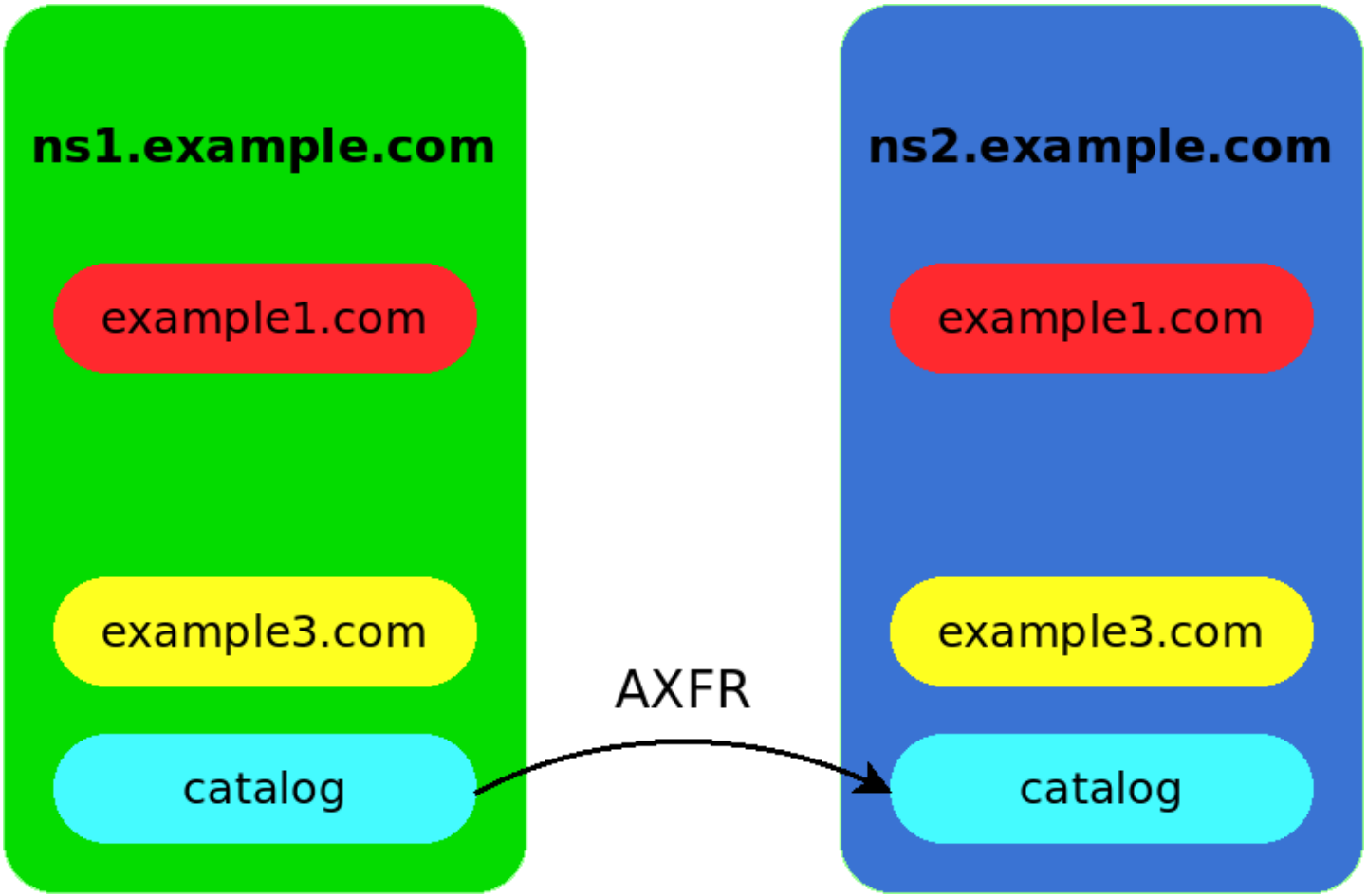
Rozwiązanie!



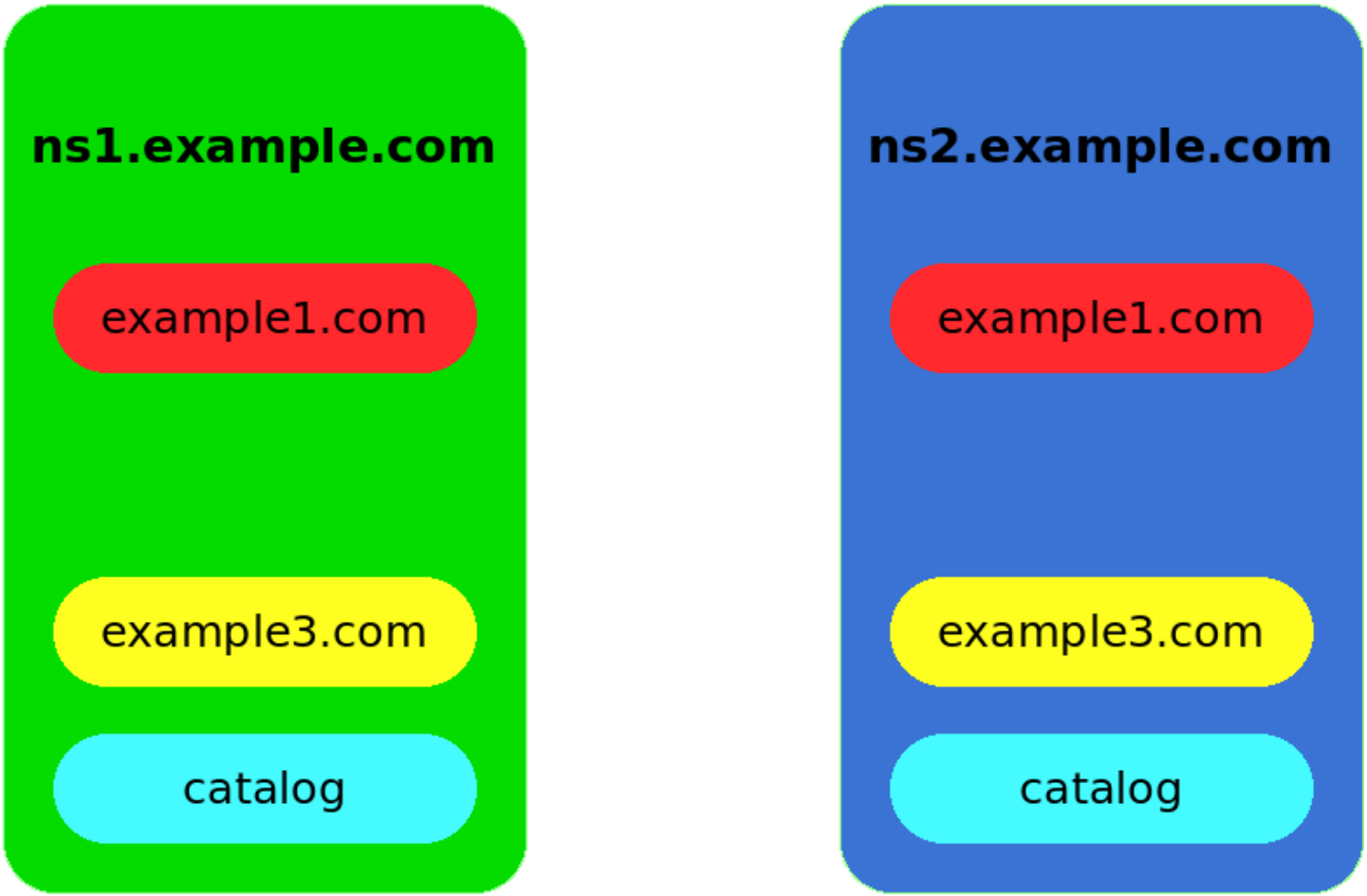
Rozwiązanie!



Rozwiązanie!



Rozwiązanie!



Najprostsza strefa

```
catz.isc.org.                          IN SOA . . 2016022901 900 600 86400 1
catz.isc.org.                          IN NS master.isc.org.
catz.isc.org.                          IN NS slave.isc.org.
version.catz.isc.org.                  IN TXT "1"

masters.catz.isc.org.                  IN A 149.20.64.3
masters.catz.isc.org.                  IN AAAA 2001:500:2c::254

5ce8b9...c9.zones.catz.isc.org.        IN PTR mojadome.na

f47be8...16.zones.catz.isc.org.        IN PTR drugadome.na
masters.f47be8...16.catz.isc.org.      IN A 199.254.63.254

4f1be1...67.catz.isc.org.              IN PTR trzeciadome.na
allow-query.4f1be1...67.catz.isc.org.  IN APL 1:10.0.0.0/8 !1:10.10.0.0/16
masters.4f1be1...67.catz.isc.org.      IN MX 0 mojmaster.servers.catz.isc.org.

mojmaster.servers.catz.isc.org.        IN A 199.6.0.30
mojmaster.servers.catz.isc.org.        IN TXT "tsigkey"
```

Konfiguracja

master.conf

```
options {
  listen-on {
   10.53.0.1;
  };
  allow-new-zones yes;
};

zone "catz.isc.org" {
  type master;
  file "catz.isc.org.db";
  allow-transfer {
   10.53.0.2;
  };
};
```

slave.conf

```
options {
  listen-on {
    10.53.0.2;
  };
  allow-new-zones yes;
  catalog-zones {
    zone "catz.isc.org";
  };
};

zone "catz.isc.org" {
  type slave;
  masters {
   10.53.0.1;
  };
};
```

Sposób użycia

- rndc addzone:

```
$ rndc addzone dome.na { type master; file "domena.db"; allow-transfer { 10.53.0.2; }; }
```

- nsupdate:

```
$ cat <<_EOF |nsupdate
server 10.53.0.1
update add 345f0ef372cb4f8fa1df416e5edc4b6be7c162b7.catz.isc.org. 3600 IN PTR dome.na
send
_EOF
```

Finalnie

- Wykorzystujemy istniejącą infrastrukturę
- Wszystko jest przesyłane po DNS
- Brak haków, zewnętrznych skryptów
- Docelowo - RFC, wspierane przez różne implementacje

Koniec.
Pytania?
wpk@isc.org