

AllKnowingDNS

Reverse DNS für 2^{64} IPv6-Adressen

sECuRE, 2012-03-13

Reverse DNS?

- Man möchte wissen, welcher Name zu einer IP-Adresse gehört:

```
$ host 192.168.1.24
24.1.168.192.in-addr.arpa domain name pointer midna.lan.
```

- Bei IPv6 ist jeder Nibble eine Einheit:

```
$ host 2001:4d88:100e:23:3a60:77ff:feab:d3ea
a.e.3.d.b.a.e.f.f.f.7.7.0.6.a.3.3.2.0.0.e.0. \
0.1.8.8.d.4.1.0.0.2.ip6.arpa domain name pointer midna.lan.
```

Server-seitig: Zonefile

```
; Reverse lookup 1.168.192.in-addr.arpa
;ORIGIN TTL                Authoritative Server      Email
$TTL 172800
@          172800  IN SOA  dns.lan.      hostmaster.lan. (
                2010120201 ; Serial (YYYYMMDDnn)
                172800   ; Refresh      48 Stunden
                43200   ; Retry        12 Stunden
                1209600  ; Expire       2 Wochen
                172800 ) ; Minimum TTL   2 Tage
; DNS server
                IN NS   dns.lan.
; PTR records
24             IN PTR  midna.lan.
```

Problem

- RaumZeitLabor: 2001:4d88:100e:ccc0::/64
→ $2^{48} = 281474976710656$ potenzielle Adressen (autoconf)
- selbst bei 1 Byte/Adresse wäre ein Zonefile 256 TiB groß
- **ICH WILL ABER!**

Lösung

- DNS-Server, der Antworten aus der Anfrage generiert
- Anfrage: 2001:4d88:100e:ccc0:216:eaff:feeb:826
Antwort: ipv6-0216eafffeeb0826.nutzer.raumzeitlabor.de
- Da gibts doch bestimmt schon was?
- Aber was ist mit DNS für Hosts wie
2001:4d88:100e:ccc0:219:dbff:fe43:2ec5
(blackbox.raumzeitlabor.de)?

AllKnowingDNS

- Net::DNS::Nameserver + ein paar Zeilen Perl (~ 400 SLOC)
- Binnen zwei Stunden entstanden
- Nochmal ein Tag für Konfiguration, Refactoring

AllKnowingDNS: Konfiguration

```
$ cat /etc/all-knowing-dns.conf
# Configuration file for AllKnowingDNS v1.0

# RaumZeitLabor
network 2001:4d88:100e:ccc0::/64
    resolves to ipv6-%DIGITS%.nutzer.raumzeitlabor.de
    with upstream 2001:4d88:100e:1::2

listen 2001:4d88:100e:1::3
listen 79.140.39.197
```

AllKnowingDNS: Reverse-Delegation

```
$ORIGIN .
$TTL 604800      ; 1 week
e.0.0.1.8.8.d.4.1.0.0.2.ip6.arpa IN SOA
    infra.in.zekjur.net. hostmaster.zekjur.net. (
        20          ; serial
        604800     ; refresh (1 week)
        86400      ; retry (1 day)
        2419200    ; expire (4 weeks)
        604800     ; minimum (1 week)
    )
    NS      libri.sur5r.net.
    NS      infra.in.zekjur.net.

; net for RaumZeitLabor
0.c.c.c.e.0.0.1.8.8.d.4.1.0.0.2.ip6.arpa.
    IN     NS      ipv6-rdns.zekjur.net.
```

AllKnowingDNS: Forward-Delegation

```
$TTL      6h
raumzeitlabor.de IN SOA ns1.jpru.de. hostmaster.jpru.de.
                        2012030701
                        3h
                        30m
                        7d
                        1d )
    IN  NS  ns1.jpru.de.
    IN  NS  ns2.jpru.de.

nutzer.raumzeitlabor.de. IN NS ipv6-rdns.zekjur.net.
```

AllKnowingDNS: Query-Log

2012-03-09 11:40:40 +0100 - 178.7.42.88 - query for \
ipv6-021075ffffe1adf8f.nutzer.raumzeitlabor.de (AAAA)

2012-03-09 12:20:40 +0100 - 178.7.42.88 - query for \
f.8.f.d.a.1.e.f.f.f.5.7.0.1.2.0.0.c.c.c.e.0.0.1.8.8.d.4.1.0.0.2.ip6.ar

2012-03-09 12:40:17 +0100 - 188.40.25.2 - query for \
8.d.a.e.0.6.e.f.f.f.4.b.8.8.2.a.0.c.c.c.e.0.0.1.8.8.d.4.1.0.0.2.ip6.ar

2012-03-09 12:40:17 +0100 - 2a01:4f8:0:a111::add:9898 - \
query for ipv6-a288b4ffffe60ead8.nutzer.raumzeitlabor.de (AAAA)

EOF

- <http://all-knowing-dns.zekjur.net/>
- <http://code.stapelberg.de/git/all-knowing-dns/>
- michael+akd@stapelberg.de
- Fragen?