DNS

Linuxnijmegen

Oscar Buse

13 jan 2015

Inhoudsopgave

Inleiding

Dit praatje is niet om te beschrijven hoe DNS technisch (op unix systemen) geïmplementeerd is.
Hoewel dit onvermijdelijk is ligt de nadruk op een uitleg van DNS zonder ons (al te) druk te maken over de technische implementatie.

DNS?

- DNS = Domain Name System.

  Grootste gedistrubueerde database ter wereld?

Voornamelijk voor:

- Hostnaam naar IP-adres vertaling (en andersom).

  Mensen zijn goed in namen (strings), computers goed in nummers.

  Naam <–> nummer vertaling kom je vaker tegen, bv:

  - username <–> uid
  - filename <–> inode

Maar ook:

- Opzoeken mailserver ("MX-record" (later meer))
- "Sender Policy Framework"

"**Here at First National, you're not just a number - you're two numbers, a dash, three more numbers, another dash, and another number.**"

Waarom

Vóór DNS: HOSTS.TXT (bijgehouden en te verkrijgen (ftp) op host "SRI-NIC.ARPA")
Nadelen:

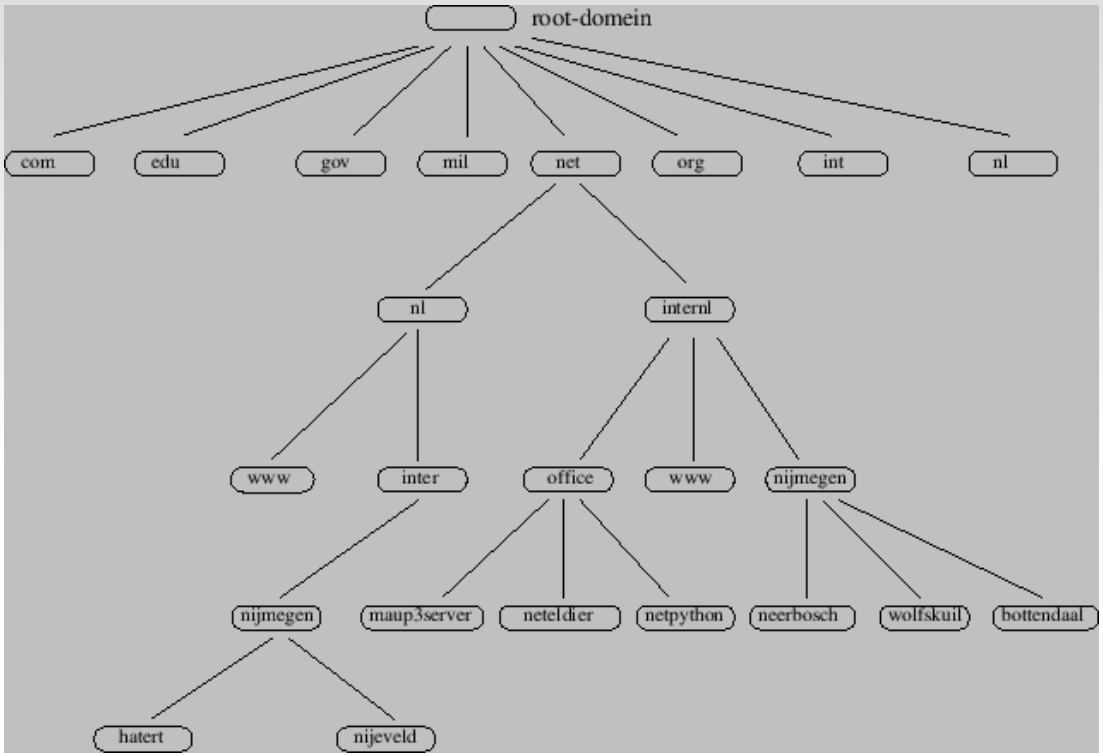
- *Flat namespace*, uniekheid van namen moeilijk te waarborgen.
- Belasting.
- Traag: verouderde info

Een nieuw systeem moest voldoen aan de volgende eisen:

- Hiërarchisch zijn
- Decentralisatie van autoritiet
- Up-2-date

DNS voldoet hieraan.

domeinen en zones



domein: 1 tak met alle bijbehordende vertakkingen. Bv. internl.net
zone: hetzelfde zonder de *gedelegeerde* delen. Bv. internl.net zonder nijmegen.internl.net
Nameserver: verantwoordelijk voor zijn stukje (zone) van de boom.

client (*resolver*) en server (*nameserver*)

Hoe wordt het IP-adres behorende bij een naam gevonden?

DNS is client-server georienteerd:

resolver	de client die de vraag stelt
nameserver	de server die het antwoord gaat geven

resolver 1/2

- Wat is een resolver?
  Veelal simpelweg een bibliotheek routine (functie gethostbyname()), ingebakken in client toepassingen als bv. firefox, thunderbird etc...
- Hoe weet een resolver nu welke name-server te vragen?
  - Configuratie in /etc/resolv.conf:
    `search internl.net nijmegen.internl.net`
    `nameserver 202.219.13.156`
    `nameserver 202.67.14.144` (**IP adressen!**)
  - Op desktop-clients (bv. bij ubuntu) zie je:
    `nameserver 127.0.1.1`
    `search localhost`
    Dan wordt de vraag doorgegeven aan "NetworkManager"

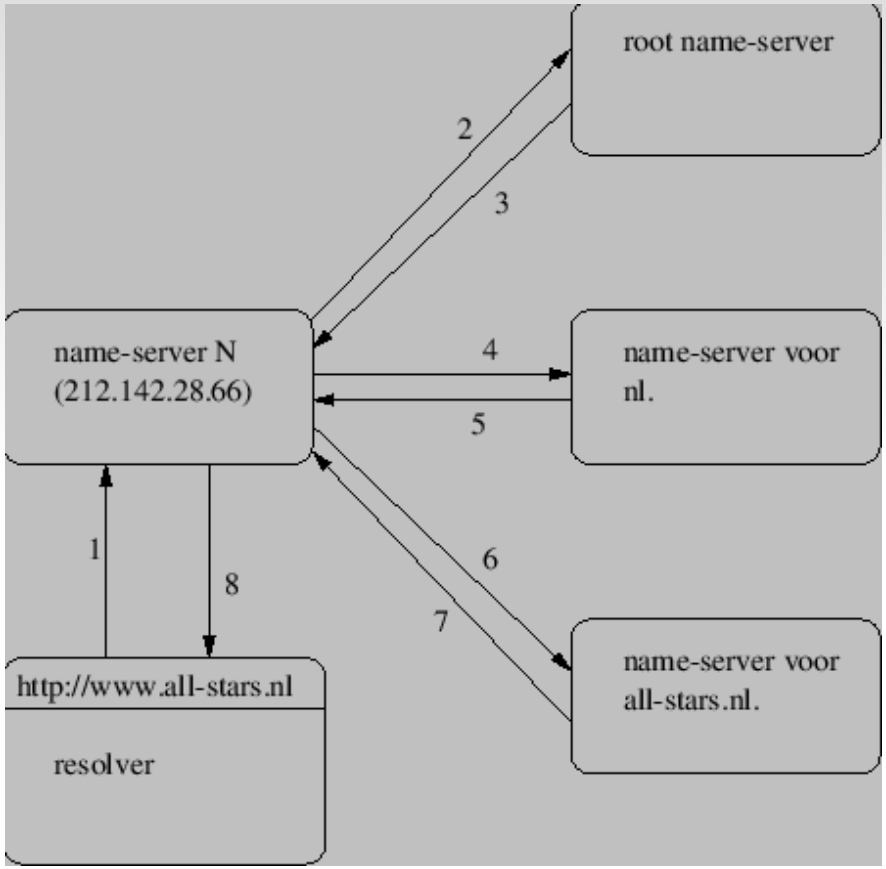
resolver 2/2

- Een resolver overhandigt altijd een FQDN (*Fully Qualified Domain Name*):
  - Bij een enkele naam vult de resolver deze aan met het default domein.
  - Indien de naam uit 2 of meer labels bestaat (dus in elk geval 1 punt bevat) wordt deze naam beeindigt met een punt. Levert dit niets op dan wordt alsnog de naam aangevuld met het default domein.
- **Geen** goed idee om zelf de laatste punt toe te voegen..
- **Geen** goed idee om bv. een *toplevel* domainnaam te kiezen vóór een lager domein:
  bv. `www.org.internl.net`

nameserver

- Werkpaard
- Verschil in functionaliteit tussen nameservers (straks meer)
- In tegenstelling tot een resolver gewoon zichtbaar: een daemon (veelal *named* (package *bind9* (ubuntu)))

een voorbeeld van de werking



Dit SCHREEUWT om het herinvoeren van HOSTS.TXT.. Maar:

- Bovenstaand voorbeeld is een *worst case scenario*
- Praktijk: caching

caching nameservers

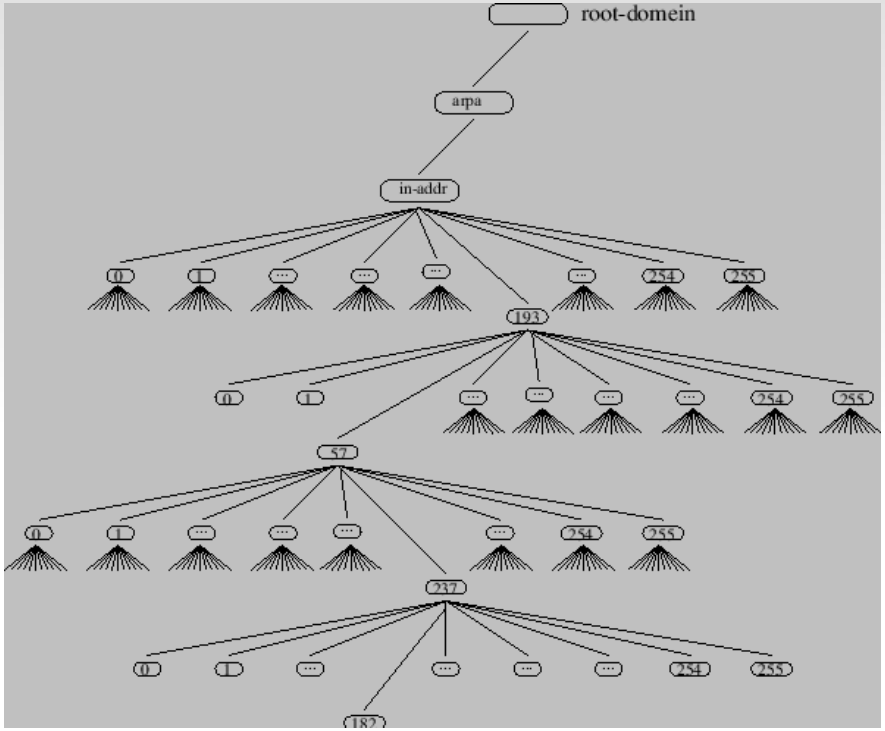
- Vrijwel nergens *autoritair* voor: ze bevatten geen *zone-data*.
- Ook wel *recursive* nameservers genoemd.
- Veelal meer dan 1 geconfigged voor een client PC (DNS is belangrijk!!).
- Worden door je provider beschikbaar gesteld:
  Geef je vaak op als "DNS-servers" in je netwerk-configuratie van je PC.
- Ook vrij te gebruiken caching nameservers: OpenDNS, Google Public DNS, ...

authoritative name-servers

- Autoritair voor 1 of meerdere zones
- Veelal master met 1 of meerdere slaves (vroeger ook wel primary master en secondary masters genoemd, alleen Microsoft houdt hardnekkig vast aan deze namen (nog steeds?))
- Meerdere servers: *redundancy*, spreiding drukte
- Administratie zonedata op 1 plek (master)
- Kunnen evt. ook recursie doen

De omgekeerde wereld

"Reverse DNS":



- Elk domein heeft 256 subdomeinen
- Op 1 na de grootste tak in de boom (alle IPv4 adressen)
- Naam begint ook onderaan maar IP-adres formuleer je andersom (!)
- Autoriteit voor DNS en reserve DNS kan prima verschillen (komt zelfs vaak voor)

Resource Records (RRs)

- Een authoritative nameserver beheerd de data voor 1 of meer zones: de zonedata
- Zonedata bestaat uit gewone ASCII regels: de *resource records* (vaak aangeduid in de leteratuur als RRs).
- Verschillende soorten resource records:
  - SOA-record: Start Of Authority, administratieve data
  - NS-records: de authoritative nameservers
  - MX-records: wat zijn de mailservers voor dit domein?
  - A-records: wat is het IP-adres (default, meest voorkomend)
  - CNAME-records: wat is de **echte** (Canonical) naam?
  - PTR-records: wat is de naam? (in *.addr.arpa. zones)

Voorbeelden RR's

linuxnijmegen.nl. 86400 IN SOA ns1.am13.siteground.biz.
root.serv01.am13.siteground.biz. 2014112706 86400 7200 3600000 86400

linuxnijmegen.nl. 86400 IN NS ns1.am13.siteground.biz.
linuxnijmegen.nl. 86400 IN NS ns2.am13.siteground.biz.

linuxnijmegen.nl. 3600 IN MX 30 mx30.mailspamprotection.com.
linuxnijmegen.nl. 3600 IN MX 10 mx10.mailspamprotection.com.
linuxnijmegen.nl. 3600 IN MX 20 mx20.mailspamprotection.com.

www.linuxnijmegen.nl. 14400 IN CNAME linuxnijmegen.nl.
linuxnijmegen.nl. 14400 IN A 109.73.229.96

96.229.73.109.in-addr.arpa. 86400 IN PTR ip-109-73-229-96.siteground.com.

229.73.109.in-addr.arpa. 172800 IN NS ns1.clev1.net.

229.73.109.in-addr.arpa. 172800 IN NS ns2.clev1.net.

dig 1/2

Het commando *dig* is onderdeel van het package "dnsutils" (ubuntu)

Voorbeelden:
Wat is het IP-adres van www.linuxnijmegen.nl?

- `dig www.linuxnijmegen.nl`

Wat zijn de nameservers voor linuxnijmegen.nl?

- `dig ns linuxnijmegen.nl`

Wat zijn de mailservers voor linuxnijmegen.nl? Vraag het aan een authoritative nameserver.

- `dig mx linuxnijmegen.nl @ns1.am13.siteground.biz`

Wat is de naam van 109.73.229.96?

- `dig -x linuxnijmegen.nl`

dig 2/2

Wat is het IPv6-adres van colo.all-stars.nl?

- `dig AAAA colo.all-stars.nl`

  (verwar niet met `dig -6 colo.all-stars.nl` !)

Wat is de naam van het IPv6-adres: 2a01:3a8:100:16:1:cafe:0:80?

- `dig -x 2a01:3a8:100:16:1:cafe:0:80`

Gehele zone opvragen (*zone transfer*):

- `dig axfr linuxnijmegen.nl @ns1.am13.siteground.biz`

  Dit is bv. wat de slaves doen (en mogen).

Vermijd caching (alleen voor "debug" doeleinden): +trace

- `dig +trace +nodnssec linuxnijmegen.nl`

geoip

Onderstaande heeft niets met DNS te maken (maar is wel leuk :-))

Een naam zegt niet altijd waar een host zich bevind.
Bv.: is de host die luistert naar `www.linuxnijmegen.nl` in Nederland?
Kun je achterhalen met commando geoiplookup (package "geoip-bin" (ubuntu))

```
geoiplookup 109.73.229.96
```

Ook leuk:

```
sudo traceroute -I www.triplej.com.au
```

Nog leuker:

```
sudo traceroute -I www.triplej.com.au | tail -n +2 |
   sed 's/^.*(\(.*\)).*$/\1/'| grep -v '\*' |
   xargs -n1 geoiplookup | grep -v 'Address not found' |
   cut -d, -f2 | sed 's/^ //' | uniq -c
```

Configuratie van bind

- *bind* meest gebruikte nameserver software
- Configfile veelal /etc/named.conf (meestal chrooted)
- Rest config veelal onder /var/named (meestal chrooted)

Voorbeeld inhoud file /etc/named.conf (heel summier) voor de authoritative nameserver voor kwalinux.nl:

```
options {
allow-query     { any; };
allow-transfer  { 188.142.103.98; 149.210.136.182;};
recursion no;
}
zone "." IN {
        type hint;
        file "named.ca";
};
include "/etc/named.rfc1912.zones";
// for which zones are we authoritative?
include "/etc/named.conf.master";
```

/etc/named.conf.master

```
zone "kwalinux.nl" {
        type master;
        file "/var/named/master/kwalinux.nl";
};
zone "linuversity.nl" {
        type master;
        file "/var/named/master/linuversity.nl";
};
zone "reisavonturen.net" {
        type master;
        file "/var/named/master/reisavonturen.net";
};
zone "travelstories.net" {
        type master;
        file "/var/named/master/travelstories.net";
};
```

/var/named/master/kwalinux.nl

```
@           IN      SOA     auth1.dns.kwalinux.nl. hostmaster.kwalinux.nl. (
                            30              ; serial
                            6H              ; refresh
                            30M             ; retry
                            1d            ; expiry
                            1H )            ; minimum


@           IN      NS      auth1.dns.kwalinux.nl.
@           IN      NS      auth2.dns.kwalinux.nl.

@           IN      A       78.31.117.114
@           IN      AAAA    2001:7b8:634:4100:20c:29ff:feb4:fce2

@           IN      MX      0 mail.kwalinux.nl.
@           IN      TXT     "v=spf1 mx a ~all"

localhost   IN      A       127.0.0.1

auth1.dns   IN      A       78.31.117.114
auth1.dns   IN      AAAA    2001:7b8:634:4100:20c:29ff:feb4:fce2
auth2.dns   IN      A       188.142.103.98
mail        IN      A       78.31.117.114
www         IN      A       78.31.117.114
www         IN      AAAA    2001:7b8:634:4100:20c:29ff:feb4:fce2
ww6         IN      AAAA    2001:7b8:634:4100:20c:29ff:feb4:fce2
doc         IN      A       78.31.117.114
m           IN      A       78.31.117.114
```

gevorderde technieken

- *dynamic updates*. Vooral handig bij het gebruik van IP-adressen verkregen met DHCP voor hosts met vaste hostnamen.
- *incremental zone transfers*. Alleen de zone-data die gewijzigd is wordt opgehaald door de slaves.
- Secure DNS (DNSSEC): zekerheid gewenst dat de verkregen DNS informatie ook werkelijk de juiste is.
  Heikele punten m.b.t. DNSSEC:
  - Extra resource records nodig, o.a.:
    - SIG-record. Dit record bevat een cryptografische *signature* voor resource records.
    - KEY-record. Dit is een record met public keys van SIG-records.
  - Meer complexiteit: bijhouden van DNS niet meer "met de hand" maar met tooling.
  - De performance van DNSSEC laat nog te wensen over.

vragen en antwoorden

Eerst een **Tip:** Sluit netwerk-issues uit door eerst met IP-adressen te werken.

Q "We willen ons domein graag verhuizen maar blijft onze mailserver dan bereikbaar?"

A "Geen probleem. Zolang de zonedata gewoon meeverhuisd wordt."

Q "We willen het IP-adres van onze webserver veranderen. Hoelang duurt het dan voordat alle name-servers het nieuwe IP-adres weten?"

A "Wanneer geenéén caching nameserver de oude data nog in de cache heeft. Check voor jezelf met dig "naam webstite".

Q "Wij hebben een eigen mail-server maar we ontvangen geen mail!"

A "Check de MX records voor het domein."

Q "Ik kan pingen naar de ftp-server maar zodra ik ernaar probeer te ftp-en wordt de verbinding direct verbroken?"

A "Waarschijnlijk gaat de reverse lookup van je eigen IP-adres fout: sommige ftp daemons willen dat."

Q "Ik wil mijn nieuw gemaakte website testen met de echte url, kan dat zomaar?"

A "Edit op je client je eigen hosts-file (/etc/hosts)."

Q "Ik heb geen internet!"

A "Als pingen naar IP-adressen wel werkt: misschien heeft je provider een probleem.. (zelden)"

Q "Waarom zijn er maar 13 root nameservers?"

A "Meer past(te) er niet in een UDP pakket. Overigens zijn er dankzij *anycast* veel meer dan 13."