# TCP: DNS

D. Leeuw

6 december 2023
v.0.8.1

# Over dit Document

## 0.1 Leerdoelen

In dit document wordt DNS behandeld, je leert wat het Domain Name System is en waarvoor het dient. Als je dit document helemaal uit hebt ben je instaat om zelf een DNS-server op te zetten.

## 0.2 Voorkennis

Voor een goed begrip van de in dit document behandelde kennis is het noodzakelijk dat de volgende voorkennis aanwezig is:

- Kennis van IP-adressen
- Basiskennis van netwerken

# Inhoudsopgave

**Over dit Document** **i**
0.1 Leerdoelen . . . . . i
0.2 Voorkennis . . . . . i

**1 Inleiding** **1**

**2 Het Domain Name System** **3**
2.1 De hosts-file . . . . . 3
2.2 DNS . . . . . 4
2.3 De werking van DNS . . . . . 4
2.4 Root Hints . . . . . 5

**3 Forwarding DNS** **7**

**4 De DNS database** **9**
4.1 Serial . . . . . 9
4.2 NS record . . . . . 9
4.3 MX record . . . . . 10
4.4 A record . . . . . 10
4.5 PTR record . . . . . 10

**5 Opdrachten** **11**
5.1 nslookup . . . . . 11
5.2 DNS installatie op Windows . . . . . 11

# Hoofdstuk 1

# Inleiding

Computers zijn goed met getallen, maar wij mensen zijn beter met namen. Op een netwerk dat alleen uit IP-adressen zou bestaan zouden wij al snel de weg kwijt zijn. Het is voor ons makkelijker om te onthouden dat we bij google.com moeten zijn dan bij 142.251.36.46. Dit is precies de reden dat er een Domain Name System (DNS) is. DNS vertaald domeinnamen naar IP-adressen. Zo kunnen wij de naam gebruiken in onze browser en kan de computer het IP adres gebruiken om onze packetten over het netwerk te sturen.

# Hoofdstuk 2

# Het Domain Name System

## 2.1 De hosts-file

De eerste methode die werd gebruikt om mensen de mogelijkheid te geven om namen voor computers te gebruiken en machines een IP-adres was de hosts-file. Het bestand bestaat nog steeds om lokaal machines van een naam te voorzien. Het hosts-bestand is een simpel tekst bestand dat er bijvoorbeeld zo uit kan zien:

```
127.0.0.1       localhost
127.0.1.1       hcl01.localdomain       hcl01

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.181.65.42 my-test-host.example.com my-test-host
```

Je zou dit bestand kunnen zien als een kleine database met aan de linkerkant het IP-adres en rechts, gescheiden door wit (tab of spatie), de naam van de machine.

De hosts-file kan je op Linux of Mac OS X systemen terug vinden als `/etc/hosts` op een Windows systeem is het `C:\Windows\System32\Drivers\etc\hosts`. Het feit dat op een Windows systeem ook het laatste stukje `\etc\hosts` is heeft te maken met het feit dat Microsoft de BSD TCP/IP-stack heeft gebruikt als basis voor de TCP/IP-drivers in Windows.

Als je de laatste regel van het voorbeeld (wat begint met 10.181.65.42) toevoegt aan je eigen hosts file dan kan je met

```
ping my-test-host
```

zien dat de machine contact probeert te maken met 10.181.65.42. Het zal dit waarschijnlijk niet kunnen doen, maar je ziet dat hij de naam wel omzet naar het opgegeven IP-adres.

Voordat je verder gaat met dit document verwijder je eerst de toegevoegde regel weer uit je hosts-file.

## 2.2 DNS

Op een lokaal netwerk is het mogelijk om het hosts-bestand bij te houden, maar bij een wereldomvattend netwerk zoals het Internet is dat niet meer te doen. Er moest dus een wereldwijde database komen die op afstand geraadpleegd kan worden. Het nadeel van een enkele database is dat het tevens een single point of failure (SPOF) is. Als de database-server omvalt is er geen mogelijkheid meer om namen om te zetten naar IP-adressen. Ook en verbroken netwerkverbinding kan zorgen dat een deel van het netwerk niet meer bij de database kan. Om al deze problemen het hoofd te kunnen bieden is er gekozen voor een gedistribureerd systeem. Er is niet één enkele database dat de namen van de machines kent.

Zoals je misschien wel weet is net Internet opgedeeld in zogenaamde domeinen. Het adres www.google.com bestaat uit drie delen. Het eerste deel is www, dit is de host-naam. Het google deel is het domein en het com deel is het top-level-domain (TLD). De database-servers worden dan ook Domain Name Servers genoemd, afgekort DNS.

Er zijn verschillende TLD's op de wereld. Elk land heeft zijn eigen TLD, die voor Nederland is nl, voor Duitsland de en die voor België be. Zo heeft elk land zijn eigen TLD. Daarnaast zijn er vele generieke TLD's zoals com voor commerciële bedrijven, org voor organisaties en edu voor educatieve instellingen. Elke TLD heeft zijn eigen name-server wat al zorgt voor een enorme wereldwijde spreiding.

Een organisatie als Google heeft zijn eigen domein (google.com) en daarmee ook zijn eigen domein-database (DNS). Dus als je wilt weten wat het adres is dat hoort bij www.google.com dan vraag je dat aan de DNS van Google.

## 2.3 De werking van DNS

Hoe zorgt een client, bijvoorbeeld je browser, dat je bij de domeinnaam een IP adres krijgt?

Je browser geeft aan de TCP/IP stack door dat hij bijvoorbeeld verbinding wil maken met www.microsoft.com. Het eerste dat je TCP/IP stack dan gaat doen is kijken of het weet welke name servers er zijn. Deze name server moet je handmatig hebben geconfigureerd of ze moeten door DHCP aan je machine zijn gegeven.

Je machine neemt contact op met een DNS op port 53 en vraagt aan de server of hij weet wat het IP-adres is van www.microsoft.com.

De kans is natuurlijk klein dat jouw name server de IP-adressen van Microsoft kent. Dus je name server neemt contact op met een root name server. Een root name server kent de Top Level Domains (TLDs) van het Internet. De root server kan onze server verwijzen naar de name server voor het .com domain. Die name server kan ons verwijzen naar het IP-adres van de name server van het .microsoft.com domein.

Als we het IP-adres hebben van de name server van Microsoft dan kan onze name server aan de name server van Microsoft vragen wat het IP adres is voor www.microsoft.com en dat antwoord kan onze server dan weer aan onze machine gegeven. Daarna kunnen we een verbinding leggen met de web-server van Microsoft.

Om toekomstige DNS queries te versnellen, kunnen de gevonden oplossing tijdelijk opslaan (cache) zodat we een volgende query sneller kunnen beantwoorden. Voor veel gebruikte domeinen helpt dit om het proces te versnellen. Het nadeel is natuurlijk wel dat als er in de DNS bij Microsoft een wijziging plaats vindt wij die niet meteen medelen aan onze gebruikers. Pas als de cache rijd verlopen is zullen we bij Microsoft controleren of het gevonden IP nog geldig is en tot de conclusie komen dat dit niet het geval is. Pas daarna weten ook onze gebruikers het.

## 2.4 Root Hints

De InterNIC is verantwoordelijk voor het bijhouden van de root van de name servers van het Internet. Dit is een kort lijstje van alle servers wereldwijd die alle TLDs kennen. Dit is een lijstje dat je af en toe eens moet updaten om te zorgen dat je de laatste versie hebt. Het is beschikbaar op `https://www.internic.net/domain/named.cache`. Het is bekend onder de naam "hints-file".

Het bestandje heeft allemaal regels die vertellen waar root servers gevonden kunnen worden. De root van een domein is de . (punt). Eigenlijk zou je een domein naam dus moeten schrijven als wwww.microsoft.com. met een punt aan het einde. Maar omdat die punt er altijd moet staan laten we hem weg en nemen we aan dat die er is. In de hints-file komen we deze punt weer

tegen:

```
.                       3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:ba3e::2:30
```

We zien hier dat voor de root (.) we de name server (NS record) A.ROOT-SERVERS.NET. moeten gebruiken en dat die server het IPv4 adres (A record) 198.41.0.4 heeft. Ook een IPv6 adres (AAAA record) is gegeven voor de name server.

# Hoofdstuk 3

# Forwarding DNS

De meest simpele vorm van DNS is het forwarden van een request aan een volgende DNS. Dit gebeurd vaak in de wat kleinere netwerken. In interne DNS server wordt door alle clients gebruikt om hun requests naar toe te sturen en de interne DNS forward de request naar de DNS van de provider. De interne DNS werkt dan alleen als cache zodat veel voorkomende queries niet allemaal bij de DNS van de provider terecht komen. Dus hoewel het toevoegen van een extra DNS een extra stap is en dus vertraging oplevert kan het door de caching uiteindelijk toch een verbetering zijn.

# Hoofdstuk 4

# De DNS database

## 4.1 Serial

De database van de verschillende DNSen kan wijzigen. Het kan bijvoorbeeld gebeuren dat de web-server op een andere machine komt te draaien en dat dus het IP-adres wijzigt. Dit willen we in het name-server database wijzigen, zolang de andere name-servers aan ons systeem vragen wat het IP adres is gaat het goed, dan is de wijziging onmiddelijk, maar als een name-server een cache heeft aangelegd, dan zal die voorlopig zijn cache blijven gebruiken. Het kan dus enige tijd duren voordat een wijziging op het gehele Internet bekend is.

De manier om caches te laten verlopen is het updaten van de "serial". De serial is een numeriek ID. Een hogere serial betekent een nieuwere versie. Voor de serial wordt meestal de datum + een versie nummer genomen: 2023120603. Deze serial staat voor 6 december 2023 de derde wijziging. Je kan zo maximaal 99 wijzigingen op een dag doen (01 tot 99).

Een DNS kan dus de serial opvragen om te weten te komen of het opnieuw een query moet doen naar een IP-adres of dat hij de huidige cache kan laten bestaan.

## 4.2 NS record

Het name server (NS) record vertelt wat de name-servers zijn voor een domein. Let op dat je bij dit record niet 127.0.0.1 invult, maar altijd het externe IP-adres van je server, daar waar iedereen bij kan. Als je je eigen Internet domein hebt, moet je name server ook werkelijk aan het Internet hangen.

## 4.3 MX record

De wereld wil ook graag weten hoe e-mail naar een organisatie verstuurd kan worden. Hiervoor is er een speciaal veld in de DNS database, het zogenaam de MX ofwel Mail eXchange record. Het MX-record verwijst naar de hostname (plus domainname) van de mail server en geeft tevens een prioriteit mee. De mail-server met de laagste prioriteit moet gebruikt worden, de andere mag alleen gebruikt worden als de eerste niet bereikbaar is of als deze aangeeft dat hij niet gebruikt mag worden.

## 4.4 A record

Het A record in de DNS database staat voor een adres-record. In dit veld wordt de hostname opgegeven met het bijbehorende IP-adres.

## 4.5 PTR record

Het kan voorkomen dat we ook bij een IP-adres willen weten welk domein erbij hoort. Stel bijvoorbeeld dat iemand op ons systeem inlogt vanaf 142.251.36.46. Om dat mogelijk te maken met de tree-werking van DNS moeten we ook een reverse tree hebben. De oplossing die gekozen is om een apart domein te maken voor reverse lookups. Het domein is in-addr.arpa. Het TLD is dus .arpa. en de daarbij behorende functionele domein is in-addr (Internet Address).

Domeinen zoeken we op van TLD naar domein naar host. Om IP-adressen te resolven moeten we dat ook omgekeerd doen, dus voor 142.251.36.46 moet dat worden eerst 142, dan 251, vervolgens 36 om uit te komen bij 42. Dus de query zou moeten zijn 46.36.251.142.in-addr.arpa. Dat is een moeilijke om elke keer goed te doen, dus lossen de tools die we gebruiken om DNS-queries uit te voeren dit zelf op. Ook de DNS database lost dit zelf op, maar we moeten hem wel vertellen dat het een reverse-database is.

De reverse database is dus een andere database dan de forward database. In de reverse database hebben we dan ook geen A-records, maar PTR records. Het Pointer-record zegt hij dus behoort tot het in-addr.arpa domain.

# Hoofdstuk 5

# Opdrachten

## 5.1 nslookup

Een tool die je op bijna elk operating system kan gebruiken om vragen te stellen aan DNS is `nslookup`. In de meest eenvoudige vorm kan `nslookup` gebruikt worden om een IP-adres bij een domeinnaam op te vragen:

```
nslookup www.google.com
```

Je kan ook specifiek om het IPv4 adres vragen door alleen het A-record op te vragen:

```
nslookup -type=A www.google.com
```

We weten dat DNS aan de root van de DNS-tree begint en langzaam verder gaat. Dat gaan wij nu ook doen:

1. Gebruik `nslookup` om een met lijst name-servers op te vragen die behoren bij het com domain.

2. Vraag aan één van de gevonden name-servers wat de name-servers zijn voor google.com.

3. Vraag aan één van de name-servers van Google wat de IP-adressen zijn van de mail-servers van Google (2 queries).

## 5.2 DNS installatie op Windows

Voor het opzetten van een DNS op Windows is een document van Microsoft dat je kan vinden op https://learn.microsoft.com/en-us/windows-server/networking/dns/quickstart-install-configure-dns-server?t

abs=powershell. De installatie kan je doen op een fysiek systeem of op een virtual machine.