

CVO Antwerpen-Zuid
Graduaat Informatica

Docent : Chris van de Velde
Netwerken 1

DNS : Domain Name System

Hans Jonkers

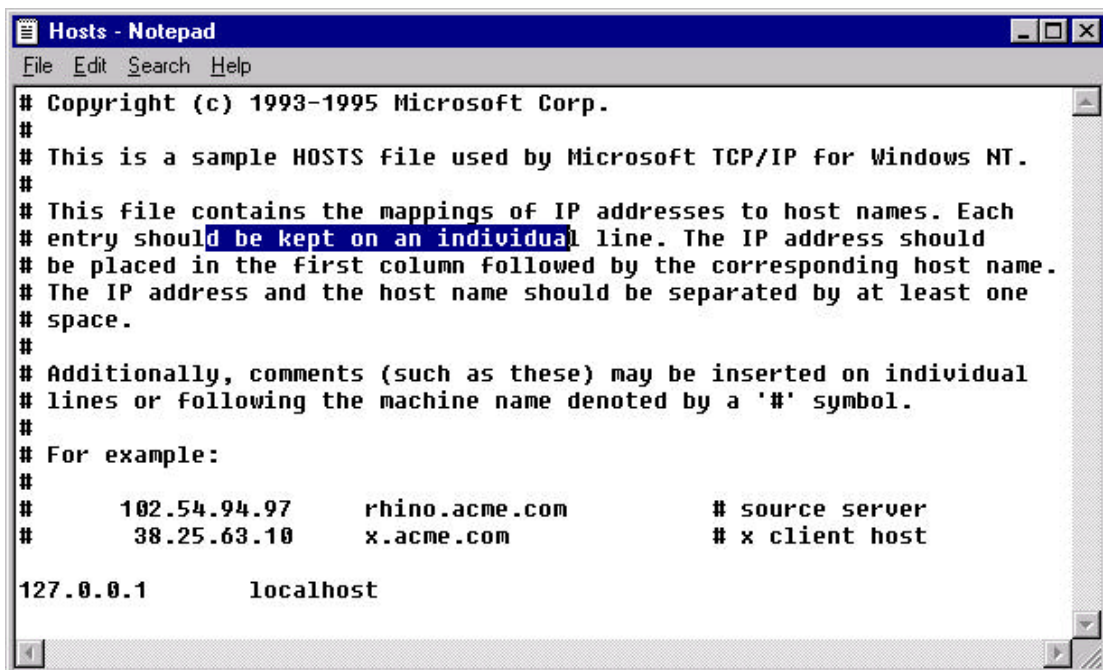
Schooljaar 2002-2003

DEEL 1 : DNS, de achterliggende theorie

1. Situering van DNS

TCP/IP is het standaard netwerkprotocol geworden, grotendeels dankzij het ontstaan en de groei van het internet. Omdat de adressering binnen TCP/IP gebruik maakt van getallen (IP-adressen), en mensen geneigd zijn getallen makkelijk te vergeten, moest een systeem uitgedacht worden dat gebruik maakt van namen - in plaats van de IP-adressen - om netwerkbronnen te vinden. De oplossing is naam-resolutie. Hierdoor konden gemakkelijk te onthouden namen (bv. www.yahoo.com) omgezet worden naar hun IP-adres (bv. 128.110.121.42).

In eerste instantie werd de naam-resolutie uitgevoerd aan de hand van hosts-files. Hosts-files zijn niet meer dan gewone ASCII-tekstfiles die een opsomming maken van objectnamen en IP-adressen, en een mapping tussen beide maakt. Een voorbeeld van een hostfile zie je hieronder :



```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com             # x client host

127.0.0.1       localhost
```

Het nadeel van het gebruik van hosts-files is dat iedere PC in het bezit moest zijn van een geupdate versie van de hosts-file om elke naam om te kunnen zetten naar een IP-adres. Dit wil zeggen dat wanneer een object aan het netwerk wordt toegevoegd of weggehaald, de hosts-file op alle PC's dient te worden aangepast. Naargelang netwerken groter worden wordt dit een onbeheerbare taak. Om dit probleem aan te pakken werd al snel gebruik gemaakt van de *Domain Name System* (DNS).

DNS is nu de standaard gebruikte manier binnen TCP/IP om adressen, die voor mensen makkelijk leesbaar zijn, om te zetten naar IP-adressen. DNS is een client/server protocol, wat wil zeggen dat een client een DNS-server zal contacteren om informatie over een bepaalde naam te bevroegen.

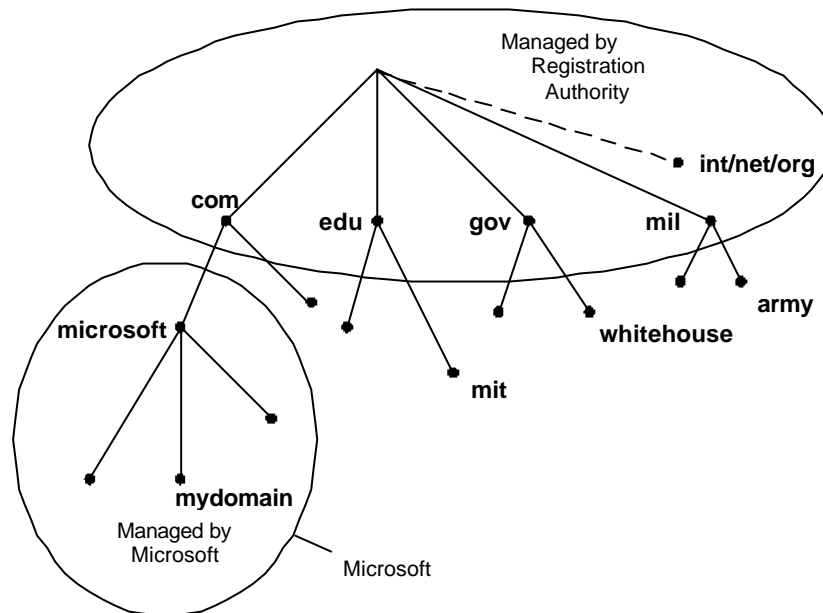
2. Werking van DNS

2.1. De DNS structuur

Het Domain Name System is een hiërarchische en gedistribueerde database die zich op DNS-servers bevindt en die een verscheidenheid aan data bijhoudt, waaronder hostnamen en domeinnamen. De namen in een DNS database vormen een hiërarchische boomstructuur die de domain name space genoemd wordt.

2.2. De hiërarchy van DNS : domeinnamen

Domeinnamen bestaan uit een verzameling van individuele labels die gescheiden worden door een punt, bv. mydomain.microsoft.com. De positie van een host binnen de hiërarchische DNS structuur wordt uniek bepaald door de *Fully Qualified Domain Name* (FQDN). De FQDN is een opeenvolging van namen, gescheiden door een punt, die het pad aangeeft van de host tot aan de root. Onderstaande figuur geeft een voorbeeld van een DNS structuur waarbij de host "mydomain" deel uitmaakt van het microsoft.com domein. De FQDN van de host is in dit voorbeeld mydomain.microsoft.com.



2.3. DNS en internet

Het Internet Domain Name System wordt beheerd door onafhankelijke organisatie, waaronder Internic. Zij zijn verantwoordelijk voor de *top-level domains*. Top-level domains zijn de domeinen die iedereen wel kent vanop het internet. Voorbeelden zijn :

- .com : commerciële organisaties
- .edu : educatieve organisaties
- .gov : gouvernementele organisaties (behalve militaire)
- .mil : militaire organisaties
- .net : organisaties die iets van doen hebben met netwerken
- .org : non-profit organisaties
- .be : belgisch domein

2.4. Resource Records

De DNS database houdt alle informatie bij door middel van *Resource Records*. Ieder Resource Record identificeert een bepaalde netwerkbron binnen de database. Er zijn verschillende soorten Resource Records voor verschillende soorten informatie. De meest gebruikte zijn :

- **A** (Address Record) : Maakt het mogelijk dat DNS een naam omzet naar een IP-adres. Je zou een A record moeten hebben voor iedere netwerkbron op het TCP/IP netwerk met een vast IP-adres.
- **AAAA** (Address Record) : Is hetzelfde als het A record, maar voor gebruik bij IPv6.
- **SOA** (Start of Authority Record) : Verwijst naar de primary DNS server en zijn parameters voor een bepaalde zone. Het is het eerste record dat gezien wordt in een zone.
- **SRV** (Service Resource Record) : SRV records laten toe dat een server bevestigd wordt naargelang de service die hij levert. Hierdoor kan een lijst van bv. alle FTP servers in het domein opgevraagd worden. Het recordtype SRV is nieuw in Windows 2000, en wordt extensief gebruikt door Active Directory.
- **CNAME** (Alias of Canonical Name Record) : Laat toe dat computers kunnen bereikt worden aan de hand van verschillende namen door te verwijzen naar een ander DNS record. Hierdoor kan een computer tegelijk verschillende diensten aanbieden, zoals bv. DNS server, FTP server, Webserver,

... De diensten kunnen dan makkelijk naar een andere computer worden verplaatst door simpelweg het CNAME record aan te passen (en, vazelfsprekend, het verhuizen van de service zelf).

- **HINFO** (Host Information Record) : Houdt informatie over de computer bij, zoals CPU en operating systeem.
- **MX** (Mail Exchanger Record) : Specificeert de mailserver die instaat voor de internet mail van de computer. Het is mogelijk een mailserver te hebben die alle binnenkomende internet mail op het netwerk beschikbaar houdt voor de clients.
- **NS** (Name Server Record) : Beschrijft de DNS servers in een domein. Als er zich meerdere DNS servers in een netwerk bevinden, die elk een deel van het netwerk bedienen, kan je een top-level DNS server inrichten die records bevat voor alle lager gelegen DNS servers.
- **PTR** (Pointer Record) : Wordt gebruikt voor reverse DNS lookups (IP-adres naar naam). Het record wordt aangemaakt in het In-addr.arpa DNS domein.
- **RP** (Responsible Person Record) : Geeft de verantwoordelijke persoon voor de mail service aan.

2.5. De database distribueren : Zone files en delegatie

Een DNS database kan verdeeld worden in meerdere *zones*. Iedere zone hangt vast aan een welbepaalde domeinnaam, dat ook wel het *root domain* van die zone wordt genoemd. Een zone bevat informatie over alle namen die eindigen met de root domain naam van die zone, en wordt opgeslagen in een *zone-file*.

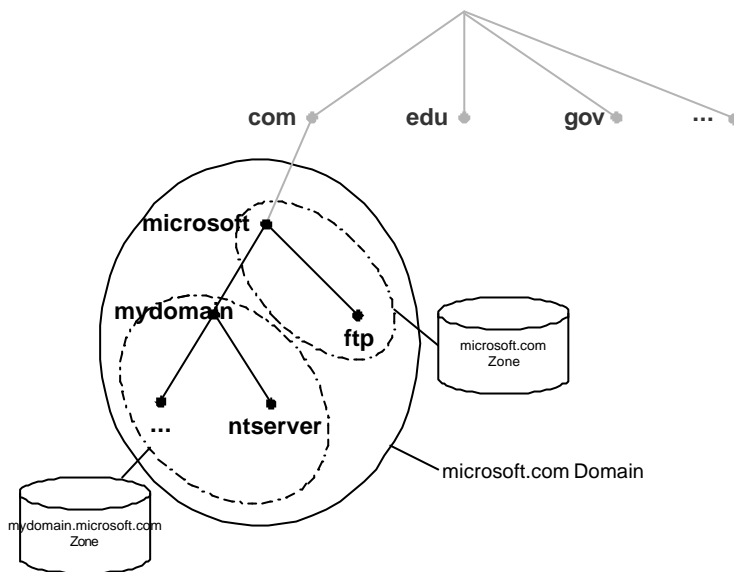
Het eerste resource record in een zone-file is een SOA-record. Het SOA-record identificeert de *primary DNS server* voor de zone. De primary DNS server is de beste informatiebron voor de data in de zone, en staat in voor het updaten van de data.

Namen binnen een zone kunnen ook gedelegeerd worden naar andere zones. *Delegatie* is een proces van verantwoordelijkheid over een deel van een DNS namespace toekennen aan een andere groep. Technisch gezien wil dit zeggen dat de verantwoordelijkheid over een bepaald deel van de DNS namespace wordt overgedragen op andere zones. Delegatie wordt in een zone-file aangegeven door het NS record, dat de gedelegeerde zone en de naam van de server die instaat voor die zone specificeert. Het delegeren over meerdere zones was een deel van de doelstelling van DNS. De belangrijkste redenen voor het delegeren van delen van een domain namespace zijn :

- Het verdelen van het beheer van een DNS domein over verschillende afdelingen binnen een organisatie.
- Het verdelen van de load van een DNS domein over verschillende DNS servers om een betere performantie en fout tolerantie te bekomen.
- Het weerspiegelen van de structuur van een organisatie door verschillende organisatieonderdelen onder te brengen in verschillende domeinen.

De NS records maken delegatie mogelijk door DNS servers te koppelen aan elke zone. Ze komen voor in alle *forward en reverse look-up zones*. Wanneer een DNS server een request moet doorsturen naar een gedelegeerde zone kan dit door gebruik te maken van NS records om een DNS server te vinden in de doelzone.

In onderstaande figuur is het beheer over het microsoft.com domein gedelegeerd over twee zones, namelijk microsoft.com en mydomain.microsoft.com.



Wanneer meerdere NS records bestaan voor een gedelegeerde zone zullen meerdere DNS servers voor die zone beschikbaar zijn. Een Windows 2000 DNS server zal in dit geval de dichtstbijzijnde DNS server in de gedelegeerde zone kiezen, gebaseerd op de tijdsinterval die nodig is voor een "round-trip".

2.6. Replicatie van de DNS database

Er kunnen meerdere zones bestaan die hetzelfde deel van de namespace representeren. Er bestaan 2 types:

- Primary zone
- Secondary zone

Een primary zone is een zone waarin alle updates van de records die to die zone behoren gemaakt worden. Een secondary zone wordt voorgesteld als een read-only kopie van de primary zone. De wijzigingen die worden gemaakt in de primary zone file worden gerepliceerd naar de secondary zone file.

Een DNS-server kan instaan voor meerdere zones. Hij kan daardoor een primary server zijn voor de ene zone en secondary voor een andere zone.

Het repliceren van een zone file naar meerdere DNS servers wordt een *zone transfer* genoemd. Een zone transfer wordt uitgevoerd door het kopiëren van de informatie in een zone file van de master server naar de secondary server.

Een *master server* is de server die de zone informatie doorstuurt. De master server kan zowel een primary als een secondary server zijn. Als de master server een primary server is dan komt de zone transfer rechtstreeks van de bron. Als de master server secondary is, is de zone transfer niet meer dan het doorsturen van een kopie van de read-only zone file van de master server naar de doelserver.

Een zone transfer kan op twee manieren in gang worden gezet:

- De master server zend een notificatie van een verandering in de zone naar de secondary server(s) (RFC1996).
- Wanneer een secondary server opstart, of het refresh interval op de secondary server bereikt is, dan zal deze nagaan of er veranderingen gemaakt zijn.

De Windows 2000 DNS server kent twee soorten zone file replicatie:

- Full zone transfer (AXFR): de gehele zone file wordt gerepliceerd.
- Incremental zone transfer (IXFR): enkel de ge-update records van de zone worden gerepliceerd.

2.7. Bevragen van de DNS database

DNS queries kunnen gestuurd worden van een client (*resolver*) naar een DNS server (*name server*), of tussen twee name servers afzonderlijk. Een query is niet meer dan een bevraging van records van een bepaald type met een bepaalde naam.

Er zijn twee soorten queries die naar een DNS server gestuurd kunnen worden:

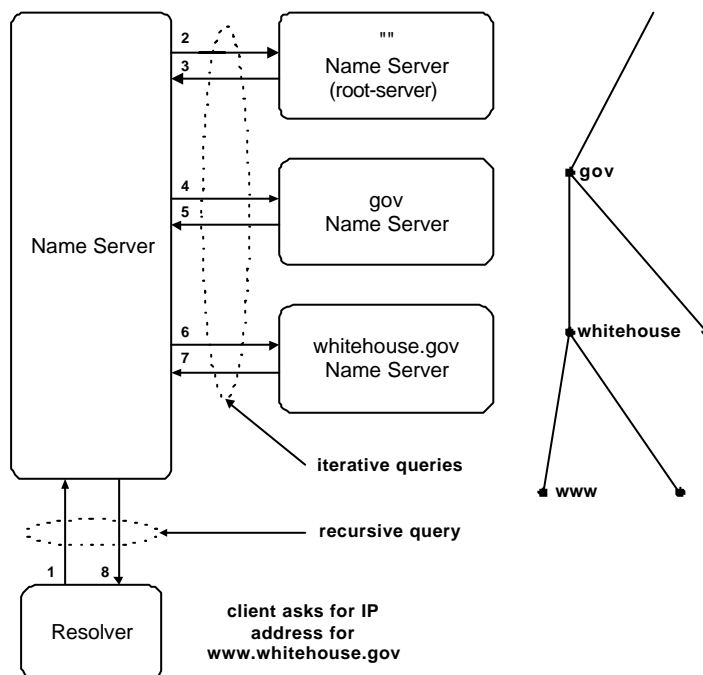
- Recursive queries
- Iterative queries

Een *recursive* query verplicht een DNS server te antwoorden, ofwel met een failure, ofwel met een succesvol antwoord. Resolvers doen vooral recursive queries. Bij een recursive query moet de DNS server indien nodig iedere andere DNS server contacteren om de bevraging succesvol af te ronden.

Wanneer een DNS server een recursive query behandelt, en de query kan niet worden opgelost aan de hand van de lokale zone files, dan moet de DNS server de query escaleren naar een root DNS server. Iedere op de standaard gebaseerde implementatie van DNS gebruikt een cache file (of root server hints) die de entrees van de root servers van de internet domains bevat. De meest recente versie van die file kan gedownload worden bij Internic op <http://rs.internic.net/domain/named.cache> (een afdruk van de file zit in bijlage).

Een *iterative* query is een query waarbij van de name server wordt verwacht dat hij de beste informatie geeft, gebaseerd op wat de server weet via local zone files of via caching. Als de name server geen beschikking heeft over informatie om te antwoorden op de bevraging, dan stuurt hij simpelweg een negatief antwoord. Een non-forwarding DNS server doet iterative queries wanneer hij namen tracht te vinden buiten zijn eigen lokale domeinen. Hij zal zelf een aantal externe DNS servers moeten bevragen om een naam te vertalen naar een IP-adres.

De onderstaande figuur toont een voorbeeld van zowel recursive als iterative queries:



In dit voorbeeld worden volgende queries gebruikt om het IP-adres van de URL `www.whitehouse.gov` te bekomen :

1. Recursive query naar `www.whitehouse.gov` (A RR)
2. Iterative query naar `www.whitehouse.gov` (A RR)
3. Referral naar de gov name server (NS RRs). Om de zaken te vereenvoudigen werd de iterative A queries die de DNS server doet om de IP-adressen van andere DNS servers te bekomen weggelaten.
4. Iterative query naar `www.whitehouse.gov` (A RR)
5. Referral naar de `whitehouse.gov` name server (NS RR)

6. Iterative query naar www.whitehouse.gov (A RR)
7. Antwoord van de whitehouse.gov server (IP-adres van www.whitehouse.gov)
8. Antwoord van de locale DNS server naar de resolver (IP-adres van www.whitehouse.gov).

2.8. Time to Live van Resource Records

Een resolver slaat de informatie, die hij krijgt via queries, op in een cache. Deze informatie kan dan gebruikt worden wanneer de resolver de informatie op een later tijdstip nodig heeft. De informatie heeft echter een beperkte levensduur, die gespecificeerd wordt in de *Time to Live* (TTL) parameter van het verkregen resultaat. De TTL parameter zorgt ervoor dat de DNS server de informatie niet te lang bijhoudt, zodat de informatie niet "verouderd" geraakt.

De TTL parameter van de cache kan gezet worden via de DNS database (per individueel resource record via het TTL veld van het record, en per zone via het minimum TTL veld van het SOA record), maar ook op de resolver zelf door de maximum TTL te specificeren die de resolver toelaat.

Er zijn twee zaken waar men rekening mee moet houden, als men de TTL parameter zet. Een eerste is de nauwkeurigheid van de gecachte informatie, een tweede de load op de DNS server en het netwerk. Als de TTL parameter laag gehouden wordt, dan is de kans dat de gecachte informatie verouderd is klein, maar zal de load op de DNS server en het netwerk hoger komen te liggen. Een hoge waarde voor de TTL parameter zal de kans op verouderde informatie verhogen, waardoor de DNS server eigenlijk verkeerde informatie doorgeeft, maar de load op netwerk en DNS server verlaagt wel.

2.9. Updaten van de DNS database

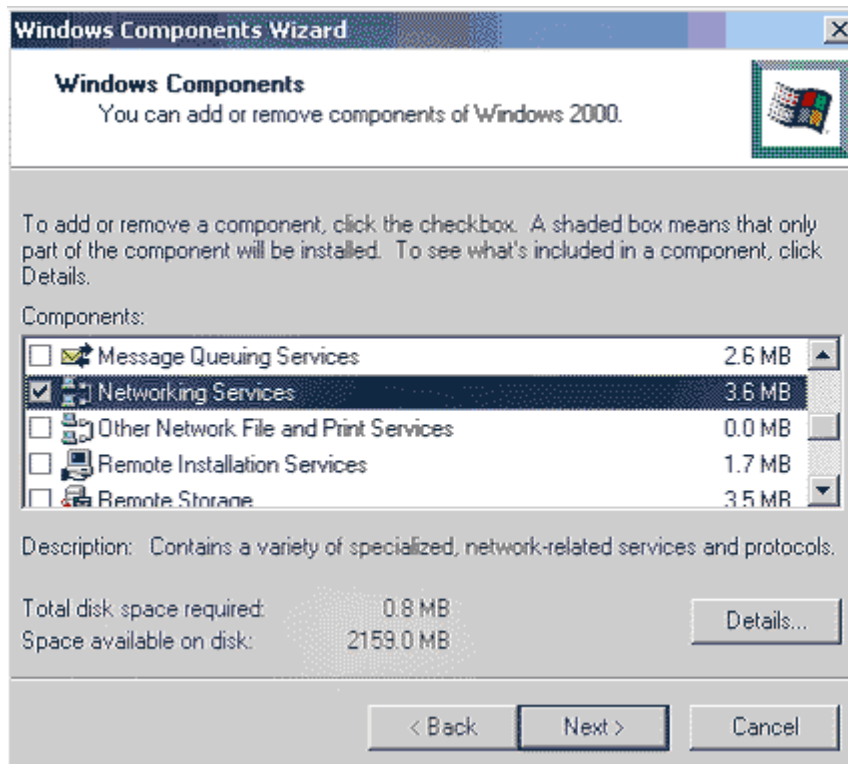
De resource records in de zone files dienen soms aangepast te worden. In Windows 2000 kan dit zowel statisch (manueel aanpassen van de zone files, vaste IP-adressen), als dynamisch (denk aan DHCP, geleaste IP-adressen) gebeuren.

DEEL 2 : DNS in Windows 2000

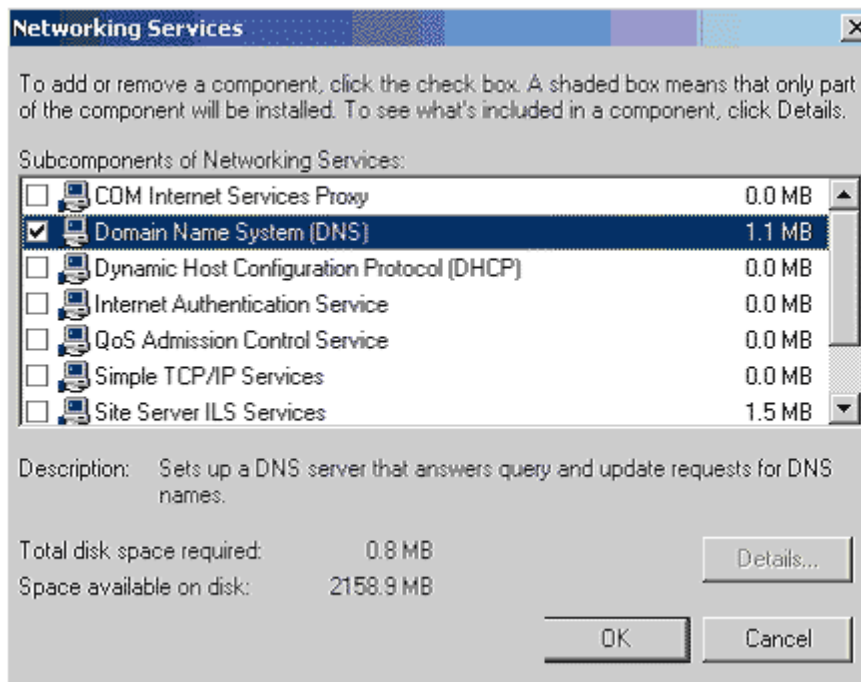
1. Installeren van DNS

Het installeren van een DNS server in Windows 2000 kan gebeuren via Control Panel, of door het promoveren van een member server naar een domain controller. Wanneer bij het promoveren geen DNS server gevonden wordt zal Windows de vraag stellen om er een te installeren.

Ga naar de Windows Component Wizard via Start > Settings > Control Panel > Add/Remove Programs, om zelf een DNS server te installeren:



Selecteer Networking Services en klik op de Details-knop, en selecteer in het volgende scherm Domain Name System (DNS):



Klik vervolgens op OK en op Next om DNS te installeren.

2. Configureren van DNS

Na de installatie kan de DNS console gevonden worden via start > Programs > Administrative Tools > DNS. Windows 2000 voorziet een wizard om de DNS server te configureren.

Vooraleer aan de configuratie te beginnen moet men op de hoogte zijn van volgende termen :

- Forward lookup zone
- Reverse lookup zone
- Zone types

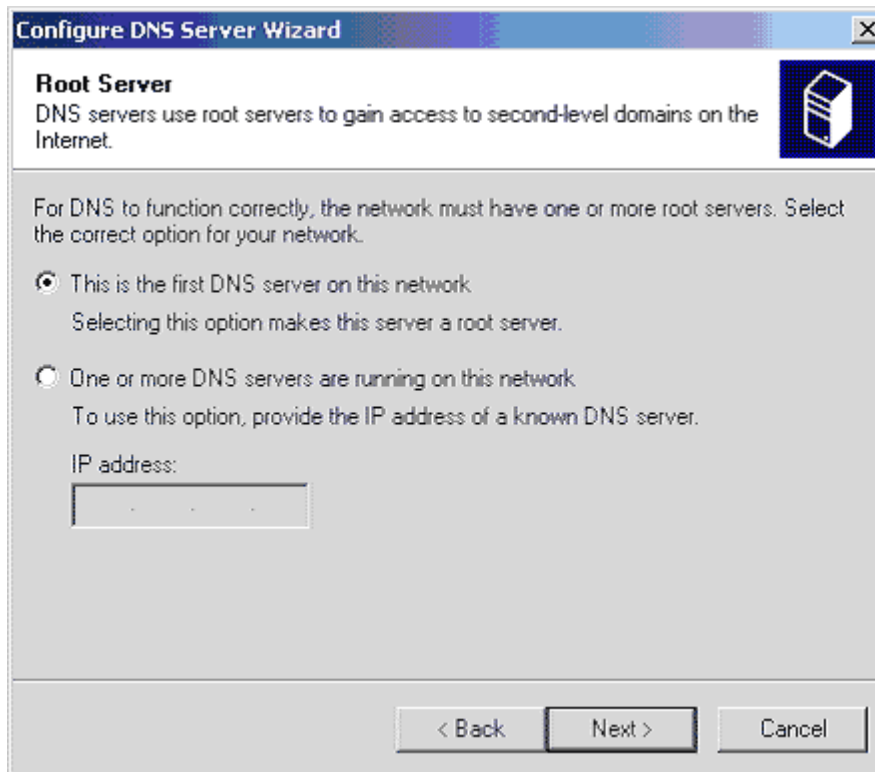
Een *forward lookup zone* vertaalt namen naar IP-adressen. Een *reverse lookup zone* laat een DNS server toe namen te vinden aan de hand van IP-adressen. Een reverse lookup zone is geen vereiste, maar is makkelijk te configureren en voorziet de Windows 2000 server van volledige DNS functionaliteit.

In Windows 2000 zijn er drie DNS zone types : Active Directory Integrated, Standard Primary en Standard Secondary.

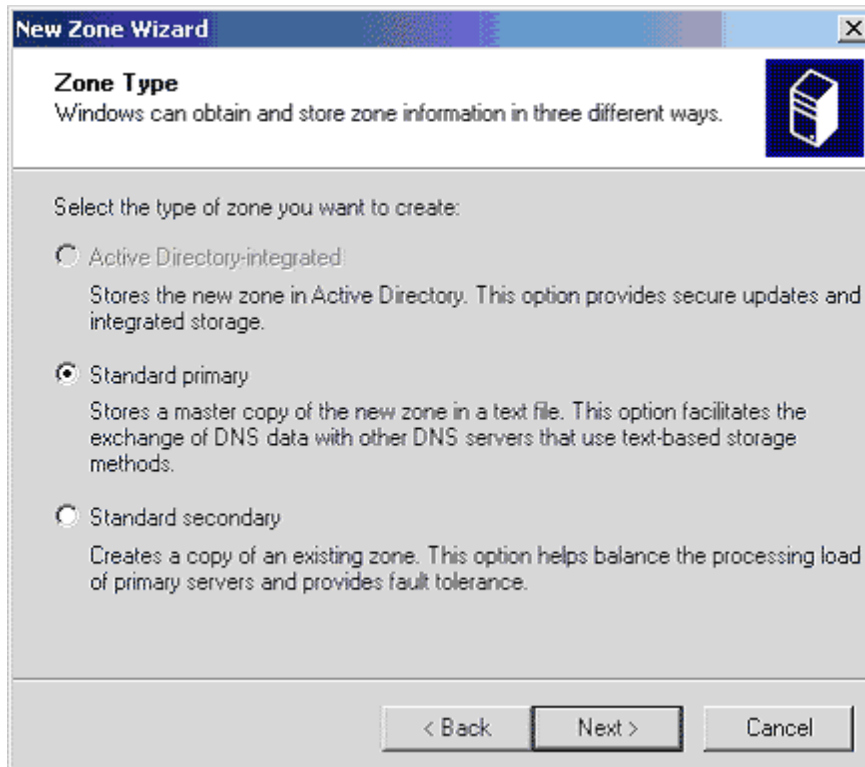
- AD Integrated slaat de database informatie op in de Active Directory en zorgt voor veilige opslag en updates van de database files. Deze optie is enkel voor handen als AD geconfigureerd is.
- Een Standard Primary Zone slaat de database op in een tekstbestand. Dit tekstbestand kan gedeeld worden met andere DNS servers die op zich hun informatie opslaan in een tekstbestand.
- Een Standard Secondary zone is gewoon een kopie van een bestaande database van een andere DNS server. Secondaries worden vooral gebruikt om aan load balancing te doen.

Om de wizard die helpt de DNS server te configureren te openen moet men DNS selecteren in Administrative Tools en vervolgens de server selecteren en klikken op Choose Action > Configure The Server.

Klik op Next en geef de gepaste root server in :



Klik op Next om een forward lookup zone te creëren.
Selecteer het gepaste zone type:



Klik Next en geef de naam in van de zone die je aanmaakt.
Klik Next en klik Yes om een reverse lookup zone aan te maken.
Klik Next om de gegevens van de reverse lookup zone in te geven :

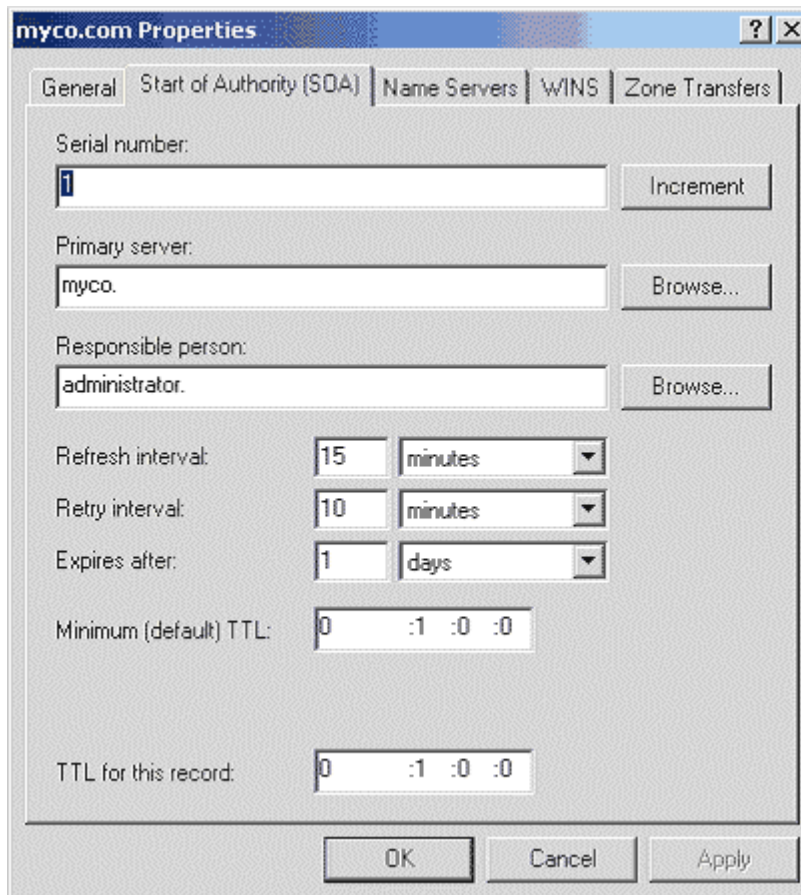
The screenshot shows a Windows dialog box titled "New Zone Wizard" with a close button in the top right corner. The main heading is "Reverse Lookup Zone" with a sub-heading: "A reverse lookup zone is an address-to-name database that helps computers translate IP addresses into DNS names." To the right of this text is a small icon of a server rack. Below the heading, there is a text instruction: "To identify the reverse lookup zone, type the network ID or the name of the zone." There are two radio button options. The first is "Network ID:" with a text box containing "192.168.1.". Below this is a paragraph of explanatory text: "If you use a zero in the network ID, it will appear in the zone name. For example, network ID 169 would create zone 169.in-addr.arpa, and network ID 169.0 would create zone 0.169.in-addr.arpa." The second radio button option is "Reverse lookup zone name:" with a text box containing "1.168.192.in-addr.arpa". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Klik Next en Finish.

3. Beheren van DNS records

3.1. SOA records (Start of Authority)

Het SOA record is altijd het eerste record in een standaard zone. De SOA tab maakt het mogelijk veranderingen aan te brengen aan het SOA record.



3.2. NS records (Name Servers)

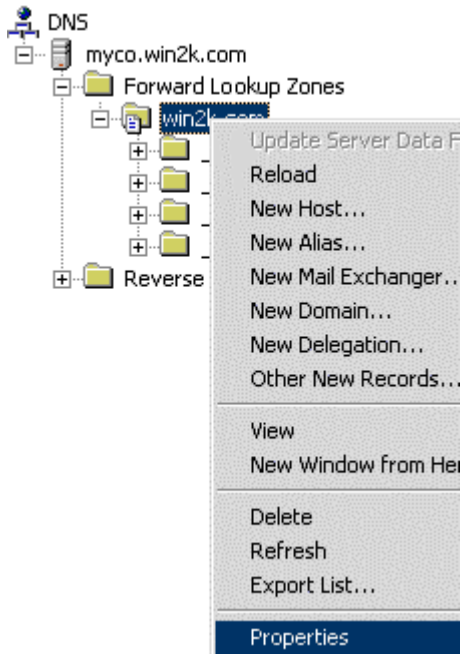
NS records specificeren alle name servers voor een bepaald domein.

Om een NS record aan te maken moet men volgende stappen volgen :

Selecteer DNS in de Administrative Tools om de DNS console te openen.

Dubbelklik op de Forward Lookup zone.

Klik rechts op het domein en kies properties:



Selecteer de Name Servers tab en klik op Add.
Geef de geschikte FQDN en het IP-adres van de server die je wilt toevoegen.

3.3. H records (Host) en PTR records (Pointer)

Host records staan in voor het omzetten van namen naar IP-adressen, pointer records voor het omzetten van IP-adressen naar namen. Bij het aanmaken van een host record kan men gelijktijdig een pointer record aanmaken.

Om een host record aan te maken :

Ga naar Administrative Tools > DNS om de DNS Console te openen.

Dubbelklik op Forward Lookup Zone

Vanuit het Action-menu, klik op New Host

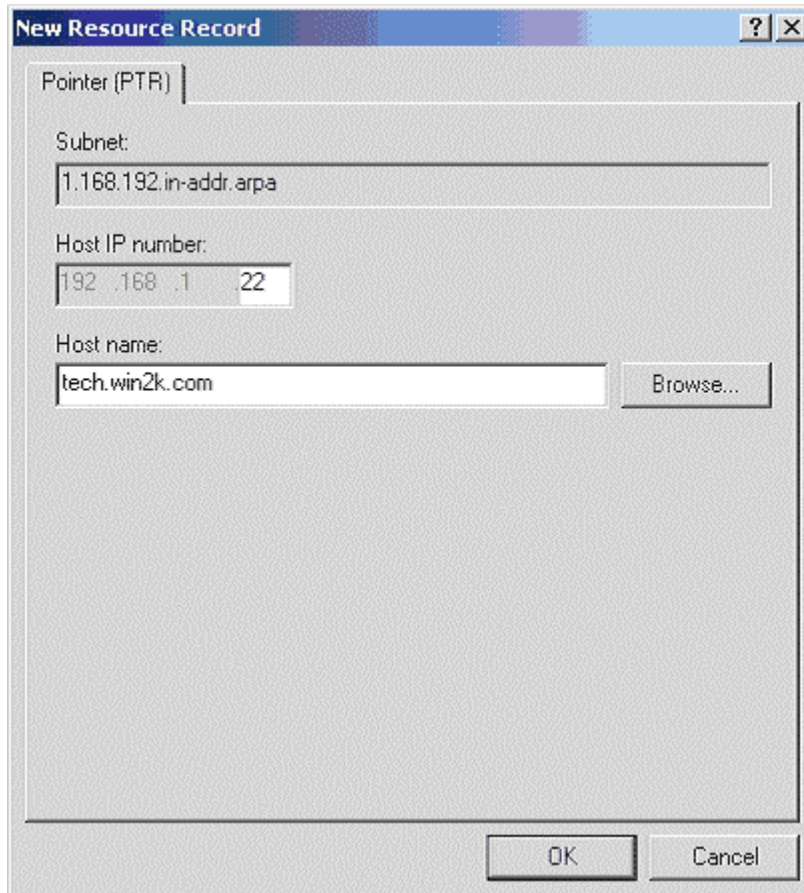
Vul naam en IP-adres in van de host die je toevoegt, en selecteer de checkbox indien een PTR record dient aangemaakt te worden :

Klik op Add Host om de records toe te voegen.

3.4. PTR records (Pointer)

In 3.3. hebben we al gezien hoe een PTR record aan te maken tijdens het aanmaken van een H record. Indien geen PTR record was aangemaakt, kan dat nog steeds. Om dit te doen:

Ga naar Administrative Tools > DNS om de DNS Console te openen.
Dubbelklik op de Reverse Lookup Zone waarin je het PTR record wil aanmaken.
Kies vanuit het Action menu om een nieuw PTR record aan te maken.
Geef het IP-adres en de naam in:



The image shows a Windows dialog box titled "New Resource Record". The "Resource Record Type" is set to "Pointer (PTR)". The "Subnet" field contains "1.168.192.in-addr.arpa". The "Host IP number" field contains "192 .168 .1 .22". The "Host name" field contains "tech.win2k.com" and has a "Browse..." button next to it. At the bottom of the dialog are "OK" and "Cancel" buttons.

Klik op OK om het record aan te maken.

3.5. CNAME records (Canonical Name of Alias)

Een Canonical Name laat toe meerdere namen te hebben voor dezelfde host. Om een DNS alias aan te maken:

Ga naar Administrative Tools > DNS om de DNS Console te openen.
Dubbelklik op de Forward Lookup Zone en selecteer het domein.
Vanuit het Action menu, selecteer New Alias.
Vul de Alias name in en de FQDN:

New Resource Record

Alias (CNAME) |

Parent domain:
win2k.com

Alias name (uses parent domain if left blank):
www

Fully qualified name for target host:
webserver.win2k.com Browse...

OK Cancel

Klik op OK om het CNAME record aan te maken.

3.6. MX Records (Mail exchange)

Mail exchange records kunnen helpen bij het identificeren van mail servers binnen een zone in de DNS database. Aan de hand van deze records kunnen prioriteiten tussen mail verschillende mailservers opgezet worden. MX records kunnen ook helpen bij het bijhouden van de locaties van de mailservers. Om MX records aan te maken:

Ga naar Administrative Tools > DNS om de DNS Console te openen.
Dubbelklik op de Forward Lookup Zone en selecteer het domein.
Vanuit het Action menu, selecteer New Mail Exchanger.
Vul Host of Domain, Mail Server en Mail Server Priority in:

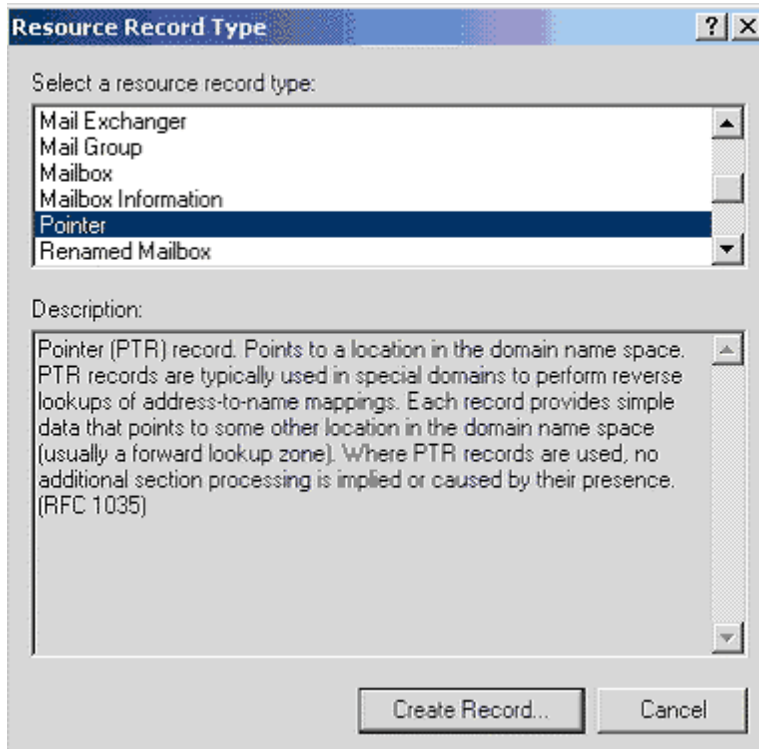
The image shows a Windows-style dialog box titled "New Resource Record" with a question mark and close button in the title bar. The dialog is for creating a Mail Exchanger (MX) record. It contains the following fields and controls:

- Mail Exchanger (MX)**: A label at the top of the dialog.
- Parent domain:** A text input field containing "win2k.com".
- Deliver mail addressed to the following host or domain to the mail server specified below (uses parent domain if left blank).**: A descriptive instruction.
- Host or domain:** A text input field containing "corpmail".
- Mail server:** A text input field containing "corpmail.myco.win2k.com" and a "Browse..." button to its right.
- Mail server priority:** A text input field containing "10".
- OK** and **Cancel**: Buttons at the bottom of the dialog.

Klik op OK om het MX record toe te voegen.

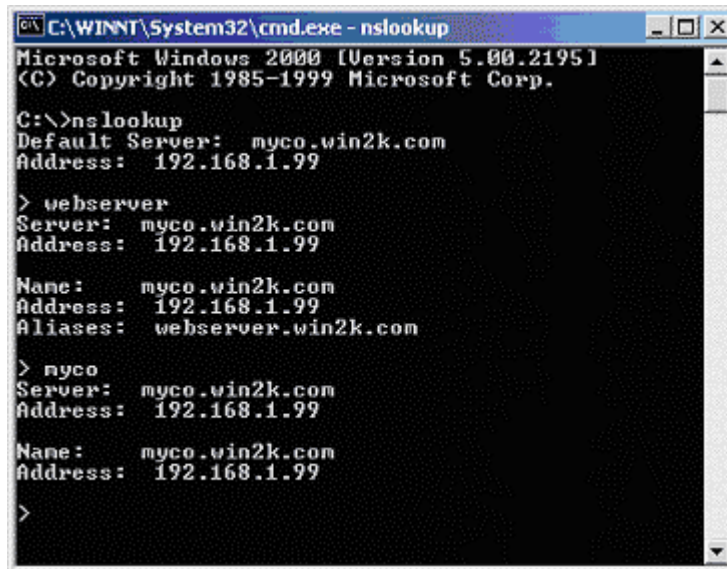
3.7. Aanmaken van andere records

Een hele hoop records van andere types kunnen ook aangemaakt worden. Ga naar Action > Other New Records om een beschrijving te zien van de verschillende records:



4. Troubleshooting

Een handige tool om DNS servers te troubleshooten is nslookup. Nslookup is een command line tooltje dat makkelijk te gebruiken is. Geef ? in in de commandline van nslookup om meer over de werking te leren.



DEEL 3 : Bijlagen

BIJLAGE 1 : Root Server Hints

File die de entries van de root servers van de internet domains bevat. De meest recente versie van de file kan gedownload worden bij Internic op <ftp://rs.internic.net/domain/named.cache>.

```
;      This file holds the information on root name servers needed
to
;      initialize cache of Internet domain name servers
;      (e.g. reference this file in the "cache . <file>"
;      configuration file of BIND domain name servers).
;
;      This file is made available by InterNIC registration services
;      under anonymous FTP as
;      file          /domain/named.root
;      on server     FTP.RS.INTERNIC.NET
;      -OR- under Gopher at RS.INTERNIC.NET
;      under menu    InterNIC Registration Services (NSI)
;      submenu       InterNIC Registration Archives
;      file          named.root
;
;      last update:   Aug 22, 1997
;      related version of root zone: 1997082200
;
;
; formerly NS.INTERNIC.NET
;
.          3600000  IN  NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000      A      198.41.0.4
;
; formerly NS1.ISI.EDU
;
.          3600000      NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000      A      128.9.0.107
;
; formerly C.PSI.NET
;
.          3600000      NS      C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000      A      192.33.4.12
;
; formerly TERP.UMD.EDU
;
.          3600000      NS      D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000      A      128.8.10.90
;
; formerly NS.NASA.GOV
;
.          3600000      NS      E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000      A      192.203.230.10
;
; formerly NS.ISC.ORG
;
.          3600000      NS      F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000      A      192.5.5.241
```

```

;
; formerly NS.NIC.DDN.MIL
;
.           3600000      NS      G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.  3600000      A      192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.           3600000      NS      H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.  3600000      A      128.63.2.53
;
; formerly NIC.NORDU.NET
;
.           3600000      NS      I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.  3600000      A      192.36.148.17
;
; temporarily housed at NSI (InterNIC)
;
.           3600000      NS      J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.  3600000      A      198.41.0.10
;
; housed in LINX, operated by RIPE NCC
;
.           3600000      NS      K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.  3600000      A      193.0.14.129
;
; temporarily housed at ISI (IANA)
;
.           3600000      NS      L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.  3600000      A      198.32.64.12
;
; housed in Japan, operated by WIDE
;
.           3600000      NS      M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.  3600000      A      202.12.27.33
; End of File

```

BIJLAGE 2 : Bronnen

MCSE: NT® Server 4 Study Guide Second Edition
Mathew Strebe
Charles Perkins
With James Chellis
ISBN : 0-7821-2222-1

DNS, DDNS and DHCP
<http://www.mcmcse.com/win2k/guides/dns2000.shtml>

Microsoft Windows 2000 DNS White Paper
<http://www.microsoft.com/windows2000/docs/w2kdns.doc>

Installing and configuring a DNS server in Win2K
Steven Warren
http://www.techrepublic.com/article.jhtml?id=r00220010514wrr01.htm&src=bc&_requestid=206623

<u>DEEL 1 : DNS, de achterligende theorie</u>	1
1. <u>Situering van DNS</u>	1
2. <u>Werking van DNS</u>	1
2.1. <u>De DNS structuur</u>	1
2.2. <u>De hiërarchy van DNS : domeinnamen</u>	2
2.3. <u>DNS en internet</u>	2
2.4. <u>Resource Records</u>	2
2.5. <u>De database distribueren : Zone files en delegatie</u>	3
2.6. <u>Replicatie van de DNS database</u>	4
2.7. <u>Bevragen van de DNS database</u>	4
2.8. <u>Time to Live van Resource Records</u>	6
2.9. <u>Updaten van de DNS database</u>	6
<u>DEEL 2 : DNS in Windows 2000</u>	7
1. <u>Installeren van DNS</u>	7
2. <u>Configureren van DNS</u>	8
3. <u>Beheren van DNS records</u>	10
3.1. <u>SOA records (Start of Authority)</u>	10
3.2. <u>NS records (Name Servers)</u>	11
3.3. <u>H records (Host) en PTR records (Pointer)</u>	12
3.4. <u>PTR records (Pointer)</u>	13
3.5. <u>CNAME records (Canonical Name of Alias)</u>	13
3.6. <u>MX Records (Mail exchange)</u>	14
3.7. <u>Aanmaken van andere records</u>	15
4. <u>Troubleshooting</u>	16
<u>DEEL 3 : Bijlagen</u>	17
<u>BIJLAGE 1 : Root Server Hints</u>	17
<u>BIJLAGE 2 : Bronnen</u>	19