

# Server Administration

## Inleiding DNS en Active Directory

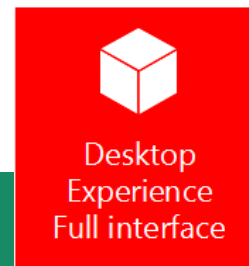
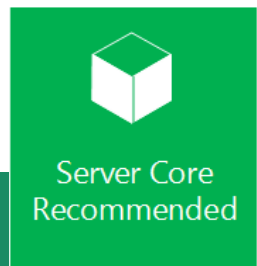
# WINDOWS SERVER

# Windows Server 2012 R2

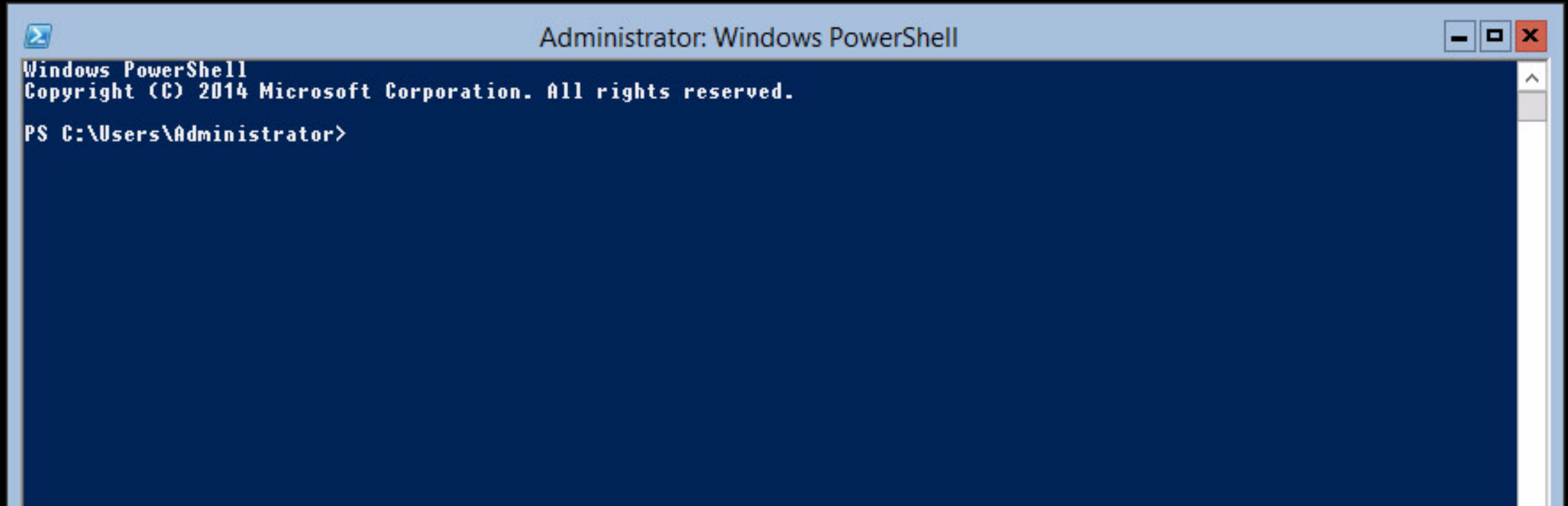
- ~ Windows 8.1 (client)
- Opvolger van Windows Server 2012 ~ Windows Server 2008
- Verbeteringen voor betrouwbaarheid, schaalbaarheid, veiligheid en beheer van grote netwerken
- Sinds 18 Oktober 2013

# Windows Server 2016

- ~ Windows 10 (client)
- Opvolger van Windows Server 2012 R2
- Meer beveiligingslagen, nieuwe implementatieopties, ingebouwde containers, software-gedefinieerde netwerken
- Sinds 26 September 2016
- Standaard zonder Gui of met “Desktop Experience” of Nano



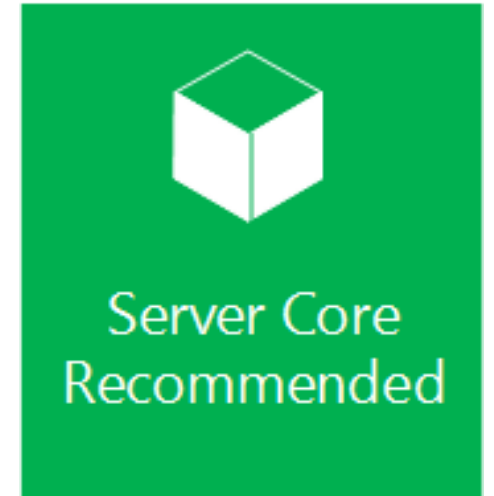
# Windows Server Core



# Windows Server Core

## Voordelen

- Kleiner OS
- Bedoeld voor specifieke, vaste taken
- Verkleint onderhoud en management
- Verkleint risico op security holes en dus ook op aanvallen
- Verbruikt een stuk minder resources



# Windows Server 2016 - Nano Server

- Nieuwe installatieoptie
- Minimaal gebruik van resources
- Geen grafische interface, geen console, geen RDP  
=> Alleen extern beheer
- Bedoeld voor in cloud omgevingen



# Windows Server 2012 R2

	Aanbevolen systeemspecificaties	Minimale systeemspecificaties
Architectuur	x86-64 (64 bit)	x86-64 (64 bit)
Processor	3,1 GHz	1,4 GHz
Geheugen (RAM)	16 GB	512 MB
Vrije ruimte op harde schijf	32 GB	32 GB



# Windows Server 2016

	Minimale systeemspecificaties	
Architectuur	x64 (64 bit)	
Processor	1,4 GHz	
Geheugen (RAM)	512 MB	2GB voor Desktop Experience
Vrije ruimte op harde schijf	32 GB	+4GB voor Desktop Experience

# Windows Server 2012 R2

	Foundation	Essentials	Standard	Datacenter
<b>Processors</b>	1	2	64	64
<b>RAM</b>	32 GB	64 GB	4 TB	4 TB
<b>Gebruikers</b>	15	25	$\infty$	$\infty$
<b># VM's</b>	0	1VM of 1 fysieke server	2 processors / licentie 2 VM's per fysieke server	2 processors / licentie $\infty$
<b>Active Directory</b>	Enkel als root	Enkel als root	Geen beperking	Geen beperking

Processors = aantal processor chips

Enige verschil is de licentie

# Windows Server 2016

- Licenties op basis van aantal cores ipv aantal processors
- Prijzen afhankelijk van aantal fysieke cores en aantal VM's die er op draaien

# Server Roles

Typische functies waarvoor de server kan ingezet worden

- Active Directory Certificate Services
- **Active Directory Domain Services**
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- DHCP Server
- **DNS Server**
- Fax Server
- **File Services**
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- **Remote Desktop Services**
- **Web Services (IIS)**
- Windows Deployment Services
- Windows Server Update Services (WSUS)

# Server Features

Ondersteunen de server rollen of bieden gewoon extra functionaliteit voor de server

## Voorbeeld van features bij de File Service Role

- File Server
- Distributed File System
- DFS Namespaces
- DFS Replication
- File Server Resource Manager
- Services for Network File System
- Windows Search Service
- Windows Server 2003 File Services
- Indexing Service
- BranchCache for Network Files

## Voorbeelden van extra losse features

- .NET Framework 3.5.1 Features
- Background Intelligent Transfer Service (BITS)
- BitLocker Drive Encryption
- BranchCache
- Connection Manager Administration Kit
- Desktop Experience
- DirectAccess Management Console
- Failover Clustering



# Unieke machine

- Indien machines gekopieerd of gekloond worden, dan moeten deze eerst terug “uniek” gemaakt worden
- Dit proces wordt meestal mbv **sysprep.exe** gedaan
- Het zorgt er voor dat de machine terug een unieke SID (Security ID) en computernaam krijgt bij de eerstvolgende opstart
- Indien men dit niet doet dan kan later b.v. Active Directory de PC niet uniek identificeren
- Toepassen bij elke vorm van kopiëren (kloon of kopie, WDS deployment,...)

# NAME RESOLVING

# Name Resolving

Naam omzetten naar IP-adres

- Verschillende soorten namen
  - NetBIOS naam (vooral bij Windows)
  - *hosts* bestand
    - /etc/hosts (Linux) 
    - %SystemRoot%\System32\drivers\etc\hosts (Windows) 
  - Internet Host Name

Vroeger: enkel HOSTS bestand met alle hostnames



# NetBIOS

- Network Basic Input Output System
- Geen protocol maar API
- In een LAN
- Meestal over TCP/IP via het NetBIOS over TCP/IP (NBT) protocol
- NetBIOS: 16 ASCII tekens
  - Meestal 15 ASCII tekens voor naam
  - Meestal 1 ASCII teken voor suffix = type resource
- Resolving door broadcast of WINS server (NetBIOS Name Server)

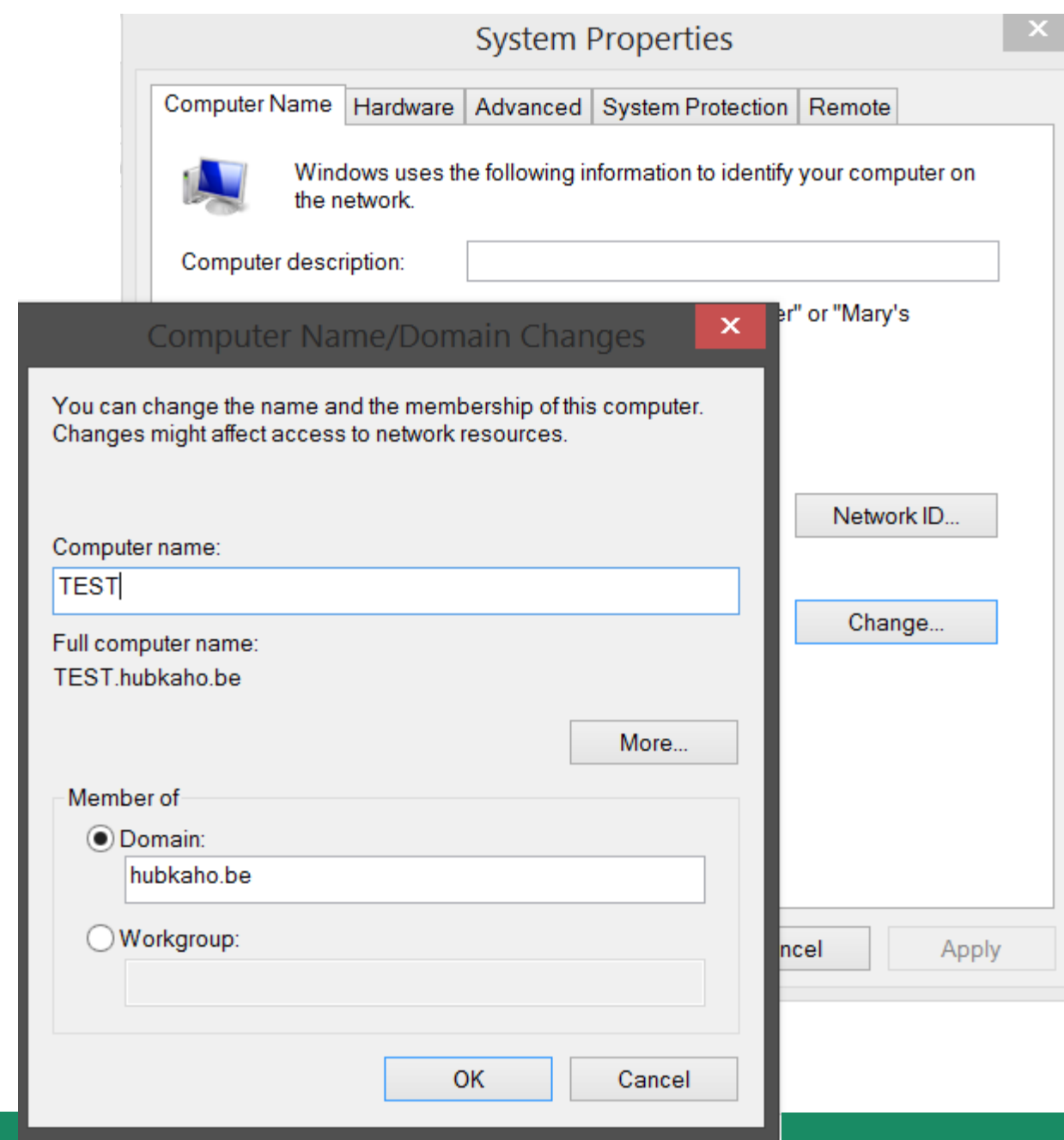
# NetBIOS



- Windows
  - Geïmplementeerd in TCP/IP stack door Microsoft
  - Normaal standaard ondersteund

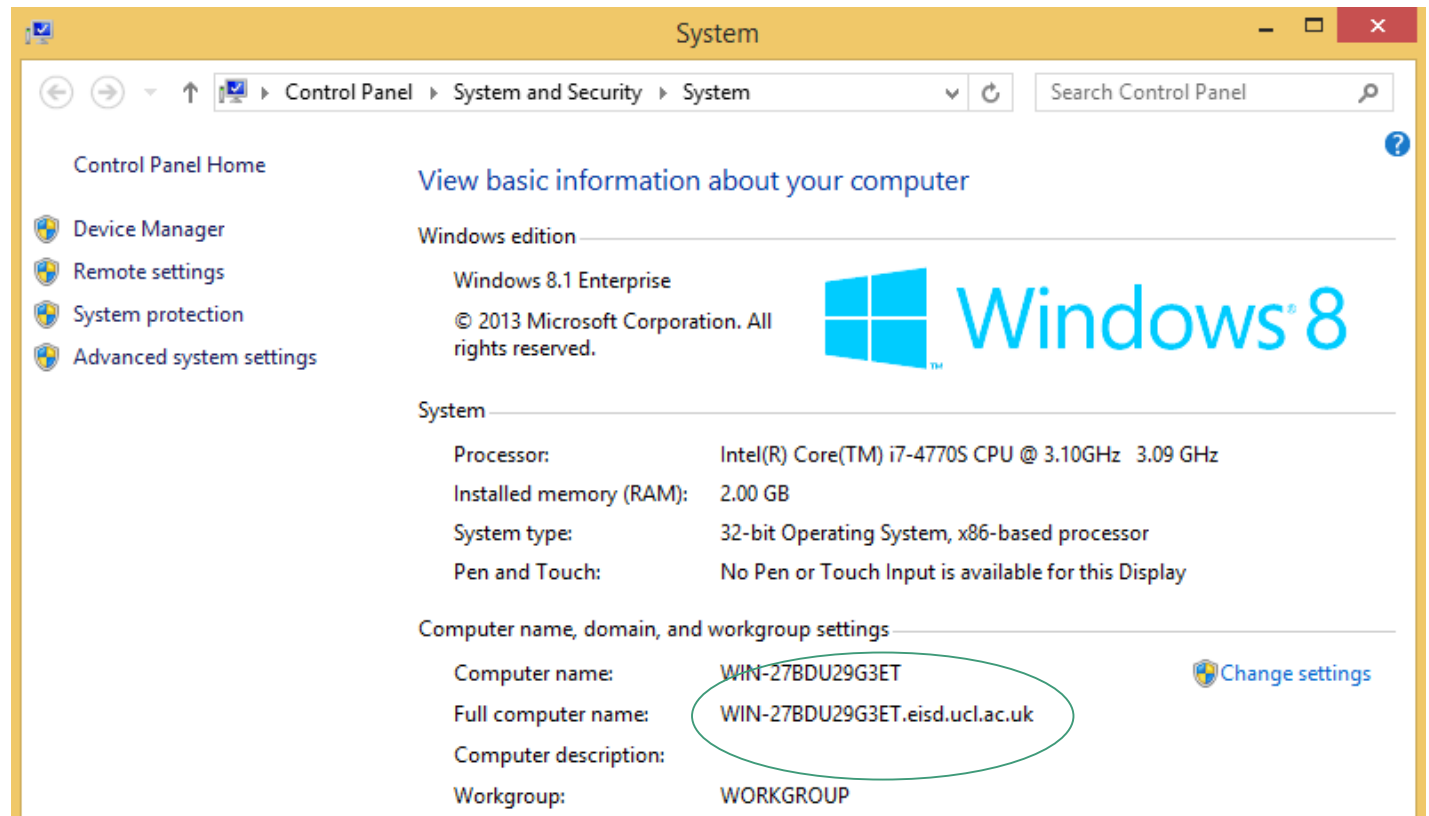


- Linux
  - Geïmplementeerd in Samba (winbind)
  - Standaard niet actief
  - In `/etc/samba/smb.conf`  
*netbios name = something*



# Internet Host Name

- Als toestel ook Internet Protocollen ondersteunt
- Meestal NetBIOS naam + Primary DNS Suffix



# Name resolving in Linux



Verschillende bronnen in /etc/nsswitch.conf

```
hosts:      files dns wins
```

1. files: Domein naam in /etc/hosts
2. dns: Gebruikte dns uit /etc/network/interfaces
3. wins: Samba configuratie

# /etc/hosts



- Bestand dat adressen mapt op namen
  - Eigen adressen en namen automatisch
  - Anderen kunnen ook manueel toegevoegd worden

```
127.0.0.1    localhost
192.168.0.1  srv1.ikdoeict.be  srv1
```

Meerdere namen mogelijk



# Name resolving in Windows

1. Controle of gelijk aan eigen naam
2. Zoeken in Hosts file
3. Domain Name System (DNS)
4. NetBIOS (als backup)

# Name resolving in Windows



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 254

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

# DNS



# DNS

- **Domain Name System**
- Hiërarchische database met namen en IP-adressen
- Legt relatie tussen een IP-adres en een (hiërarchische) naam
- Belangrijk voor bijna alle huidige netwerk-communicatie (incl Active Directory,...)

# DNS Database

- Gedistribueerde database die een deel van een (grotere) naamruimte onderhoudt
- ==> data storage en query loads zijn verdeeld over het netwerk
- Geconstrueerd voor redundantie
- De hiërarchische structuur laat toe dat elk toestel een unieke naam krijgt als deel van de DNS-namespace.

# Structuur en naamgeving

- DNS namen zijn opgedeeld en verdeeld adhv “.”
- Elk deel dns-suffix max. 63 karakters lang zijn
- Gehele DNS-naam max. 255 karakters

server.research.odisee.be.

Toestelnaam

domeinnaam of DNS-suffix

- Let op met de toeselnaam! In samenwerking met NetBIOS enkel 15 karakters.

# Structuur en naamgeving

server . research . odisee . be .



De root

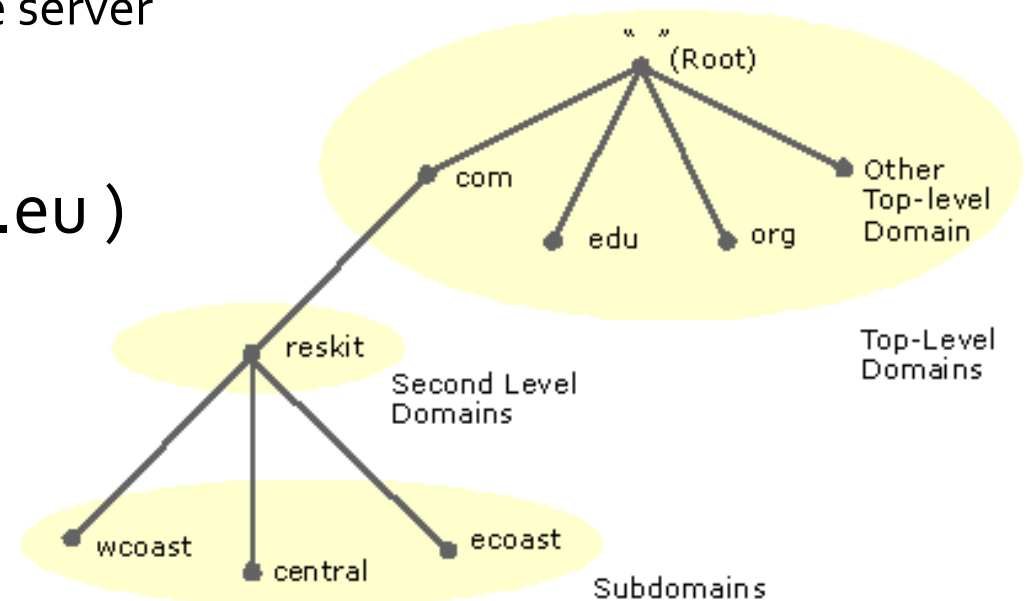
- **server**: naam van de server/host
- **research**: is subdomein van odisee
- **odisee**: is subdomein van be
- **be**: is subdomein van "." (de root)!!!
- Let op de **laatste punt!** (officiële schrijfwijze)
- ==> **Fully Qualified Domain Name (FQDN)**  
is een volledig unieke, eenduidige notatie/locatie van een machine in de DNS naamruimte

# Structuur en naamgeving

- Om een subdomein te creëren moet telkens “toestemming” gekregen worden van het “parent” domein. (**delegeren** van domeinen)

De parent delegeert een subdomein naar een andere server

- De root wordt beheerd door ICANN  
(.com .net .be .fr .info .vlaanderen .eu )



ICANN = Internet Corporation for Assigned Names and Numbers



# Structuur en naamgeving

- Honderden root servers met 13 IP-adressen wereldwijd
- Per IP-adres verschillende fysieke servers (anycast)
- Op elke server cluster

a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::dod	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project



# DNS Name resolving

`server.research.odisee.be.`

Stappen bij het opzoeken:

1. Browser richt vraag aan DNS-server die verantwoordelijk is voor domein "research.odisee.be."
2. Hoe vinden we die? ==> We kunnen de DNS-server "research.odisee.be." vinden door dit te vragen aan de DNS-server die verantwoordelijk is voor domein "odisee.be."
3. Hoe vinden we die? ==> We kunnen de DNS-server "odisee.be." vinden door dit te vragen aan de DNS-server die verantwoordelijk is voor "be".
4. Hoe vinden we die? ==> We kunnen de DNS-server "be." vinden door dit te vragen aan de DNS-server die verantwoordelijk is voor ".".
5. Hoe vinden we die? ==> ROOT HINT FILE => lijst van IP-adressen waarin de 13 root-servers wereldwijd te vinden zijn

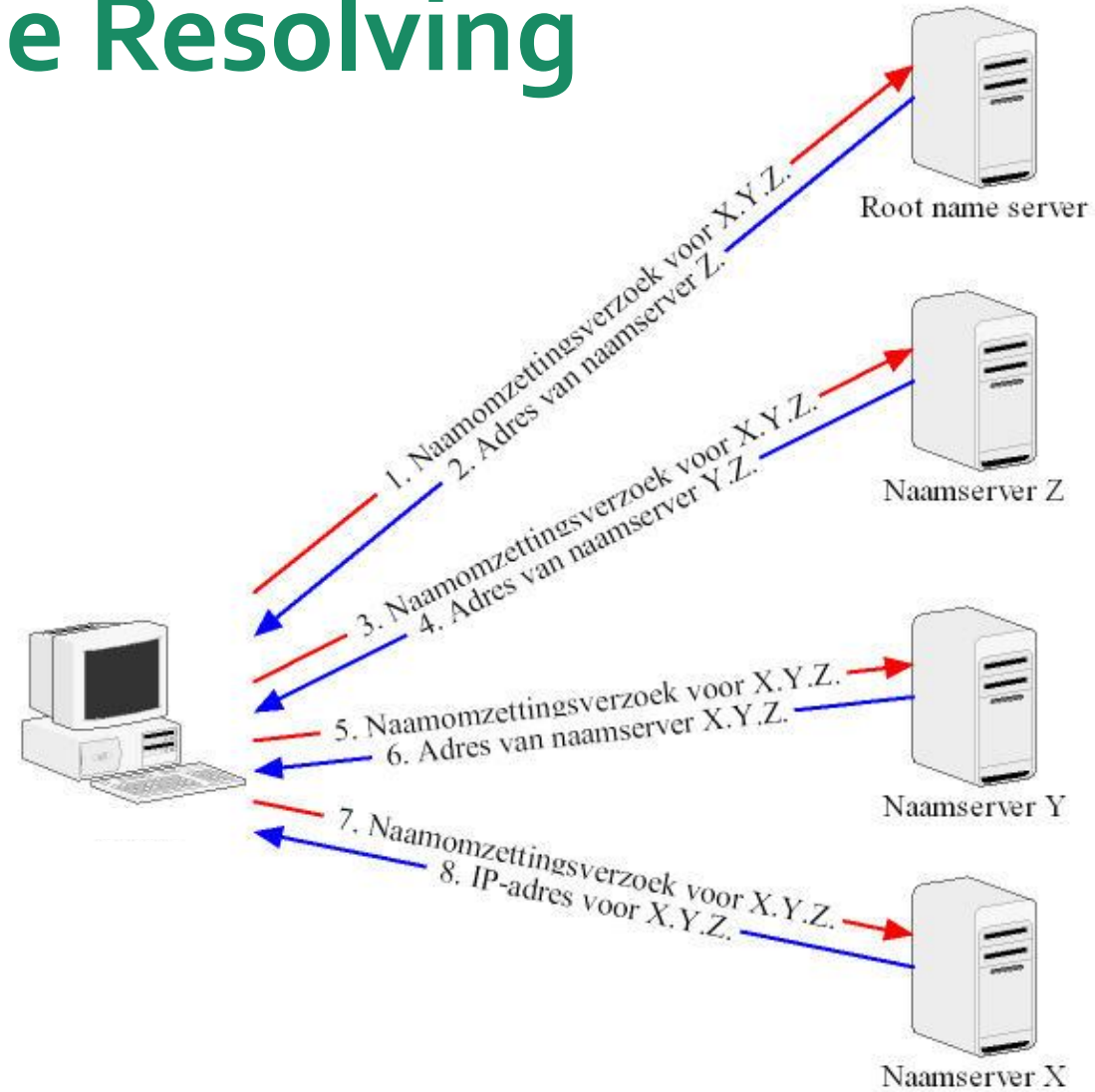
Eigenlijk worden bovenstaande stappen onmiddellijk en in omgekeerde volgorde uitgevoerd.

# DNS Name resolving

- Je computer (DNS-client) gaat uiteraard efficiënter tewerk en gaat onmiddellijk de vraag stellen aan de “root”
- Uiteindelijk wordt de DNS-server gevonden die verantwoordelijk (authoritative) is voor “research.odisee.be.”
- Daar kan de vraag gesteld worden: Wat is het IP-adres voor de host “www” binnen je domein “research.odisee.be.”



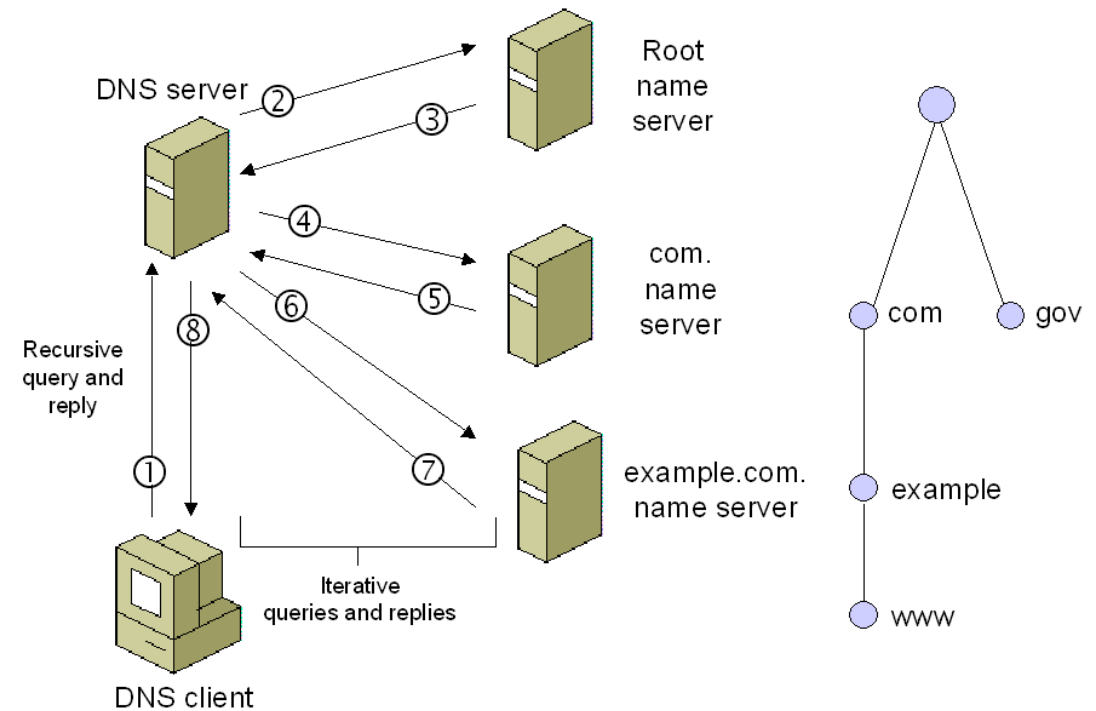
# DNS Name Resolving



# DNS Name Resolving

## Iteratief vs. Recursief

- Afhankelijk van de situatie kan een query Iteratief of Recursief uitgevoerd worden
- Bij een recursieve vraag aan de eerstvolgende DNS-server zal die DNS-server zelf de vraag verder volledig afhandelen en het antwoord sturen naar de client
- Bij een iteratieve vraag zal de client één voor één zelf alle DNS servers contacteren



# DIRECTORY SYSTEMEN

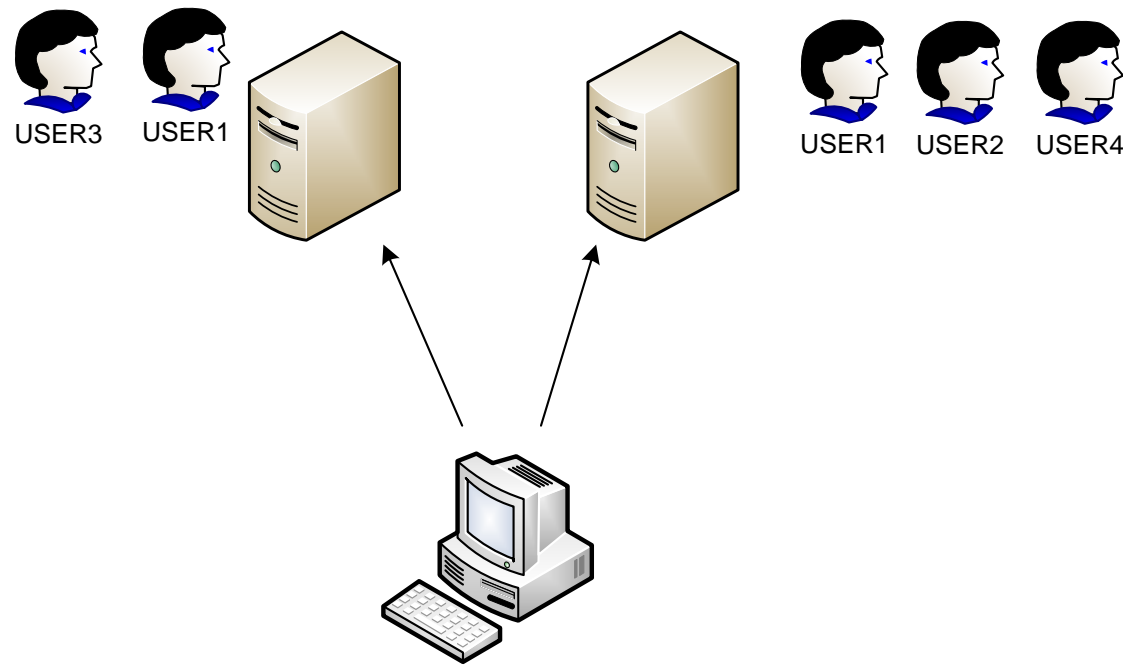
# Directory Service

- Software voor het bijhouden, beheren en toegankelijk maken van informatie in een 'Directory'
- Bij ons meer concreet:  
gebruiker- en computer accounts, groepen, printers en andere gedeelde bronnen in ons netwerk

# Vroeger

Doel: beheren wie wat mag doen op het netwerk

Oplossing:



# Vroeger

Doel: beheren wie wat mag doen op het netwerk

Oplossing:

- Elke server regelt dit zelf voor zichzelf
- Nadelen:
  - Elke gebruiker had gebruikersnaam + wachtwoord per server
  - Moeilijk te beheren door administrators

# X.500

- Verzameling van standaarden ontworpen door ISO/ITU
- Model voor protocollen en informatie in een directory service die onafhankelijk is van een applicatie of netwerkplatform
- Oorspronkelijk uit 1988
- Nadien verschillende aanpassingen/uitbreidingen (=verbeteringen)
- Definieert specificaties voor gedistribueerde directory gebaseerd op hiërarchie
- Men noemt het geheel een **DIT** (Directory Information Tree)

# X.500

- Gebruikt model voor *Directory Server Agents* (DSA's)
- DSA's bewaren elk een stuk van de "Directory Information Base" (DIB)
- DSA's werken samen => transparantie voor gebruikers
- X.500 bepaalt:
  - **Hoe** informatie opgeslagen wordt in DS
  - De nodige **protocollen** om data op te vragen
- In X.500 1988 vooral aandacht voor protocollen voor **gedistribueerde DS**



# X.500

2 belangrijke protocollen:

- **DAP** (Directory Access Protocol): laat toe dat gebruikers en applicaties de DS kunnen bevragen
- **DSP** (Directory Service Protocol): zorgt voor doorgeven van aanvragen aan andere DSA's (indien geen antwoord gevonden wordt op de lokale DSA)

=> DAP = server<->client , DSP = server<->server

# X.500

## Belangrijke aanpassingen (1993)

- **Access control:** beveiligingsmechanisme op basis van “Strong Authentication” met Public/Private key en digitale handtekeningen => veilige en flexibele DS (X.509 PKI)
- **Schema Management:** bepaalt wat én hoe informatie opgeslagen wordt
- **Collective Attributes:** zorgt voor 1 locatie voor bepaalde data en die toch te integreren op verschillende plaatsen in DS (bv adres vd werkgever bij de arbeiders)
- **DSA information Model:** Bepaalt de manier waarop DSA data opslaat (eventueel zelfde data delen via replicatie)
- **Internationalisation:** Ondersteunt multi-byte karakters

# X.500

## DISP

- Directory Information Shadowing Protocol
- Zorgt ervoor dat kopieën van verschillende directory onderdelen kunnen gebruikt worden op verschillende servers (**Replicatie**)

# X.500

## Conclusie:

- X.500 zorgt voor veilige gedistribueerde of gecentraliseerde DS  
==> interessant voor de grote spelers op de NOS-markt.

Heel wat van de principes hier uitgelegd zullen herkenbaar zijn bij Active Directory!!

# LDAP

## Lightweight Directory Access Protocol

- Is een internet standaard
- LDAP v2 en v3
- Is een open standaard voor DS
- Ideaal voor client-applications en (web)-servers vanwege LDAP over TCP/IP
- Bedoeling: **gebruikers in DS laten zoeken**
- Gemaakt voor DS, gebaseerd op X.500
- Is dus zéér aantrekkelijk alternatief voor DAP

# ACTIVE DIRECTORY

# Active Directory Objecten

Bepaalde objecten in Active Directory liggen voor de hand:

- Gebruikers
- Computers
- Groepen

Andere niet:

- Organisational Units
- Sites
- Shares
- ....

# Objecten

Alles ( bestanden, mappen, gebruikers, printers, Active Directory onderdelen,...) kan eigenlijk aanzien worden als een object

- Maakt het eenvoudig voor het besturingssysteem om beveiliging te voorzien want 'alles' wordt op eenzelfde manier bekeken
- Objecten kunnen we bekijken als containers:  
een object bevat altijd iets
  - Bestand bevat data
  - Groep bevat andere gebruikers
  - Printers bevatten een plaats in de AD
  - Gebruikers bevatten een plaats in de AD

} Leaf objects



# Beheer

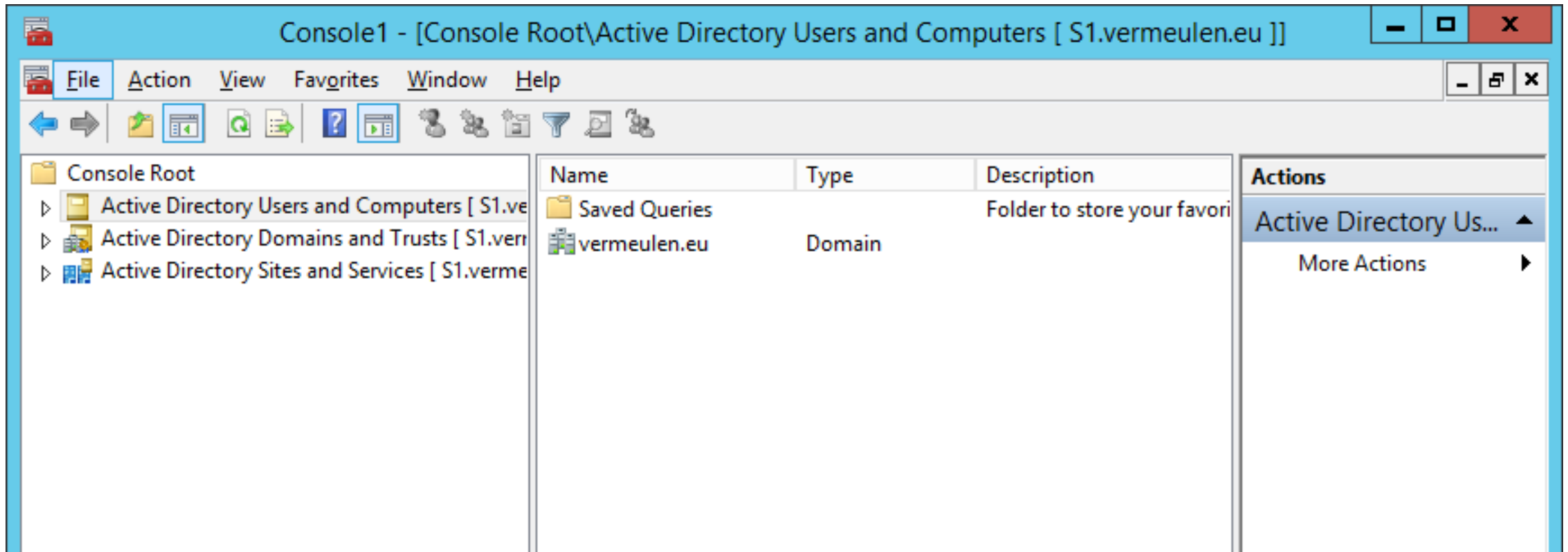
Beheer in windows 2003/2008/2012:

3 belangrijke tools om delen van de Active Directory te beheren

- Active Directory Users and Computers
- Active Directory Domains and Trusts
- Active Directory Sites and Services

# Beheer

- Toevoegen aan management console



# Bronnen

- Windows Server: [www.microsoft.com/microsoft/Servers](http://www.microsoft.com/microsoft/Servers)
- DNS root server: [https://en.wikipedia.org/wiki/Root\\_name\\_server](https://en.wikipedia.org/wiki/Root_name_server), <http://www.root-servers.org>
- Name resolution in Linux: <https://debian-handbook.info/browse/stable/sect.hostname-name-service.html>
- Name resolving volgorde in Windows: <https://support.microsoft.com/en-us/kb/172218>
- NetBIOS in Linux: <https://www.zulius.com/how-to/resolve-windows-netbios-names-from-linux/>
- Voor de andere onderwerpen is meestal een voldoende uitleg te vinden op de engelstalige versie van Wikipedia
- Op DNS en Active Directory komen we volgende weken nog terug