Windows Server

Systems Advanced: Les 6 DNS

HOGESCHOOL PXL

DNS

- Oorspronkelijk ontwikkeld om de groei van email op het ARPANET te ondersteunen
- Voorziet nu heel het internet van ‘name resolution’
- Omzetten van alfabetische namen naar numerieke adressen (www.google.be -> IP)
- Gebaseerd op een ‘hosts’ file voor mapping naam -> IP (RFC 226) :

  Windows: c:\Windows\System32\drivers\etc\hosts

  Linux: /etc/hosts

- Inefficient met files (meerdere kopies van hosts file... problematisch...)
- Van 1972 – 1983 : gecentraliseerd management: download de hosts file...

  -> Problematisch door groei

DNS

- Vanaf 1981 (RFC 799/819/882/883/1034/1035/...) DNS zoals we het nu kennen:

- 2 belangrijke principes: Delegatie & Authoriteit

- Authoriteit: Een zone van invloed waarover met de volledige controle heeft
In geval van dns gaat het over de zone en de subzones bv google.be met alle subdomeinen en hostnames.

- Delegatie: Het proces waarbij iemand authoriteit krijgt over zijn of haar zone.

DNS Concepts:

Resolver (deel van het OS) gaat namen omzetten in IP's

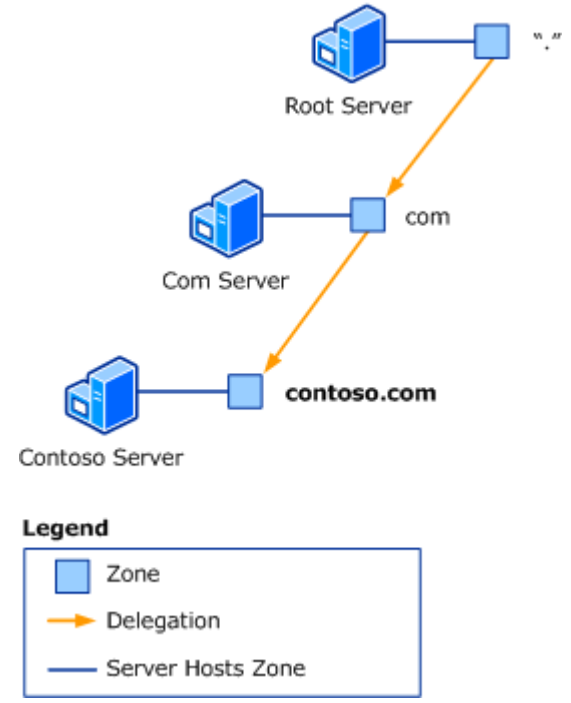
Resolving begint bovenaan bij . -> root nameservers

Hieruit komt informatie over com -> nameserver com

Hieruit komt informatie over contoso -> nameserver contoso

Binnen de contoso zone is er bv een host www
-> www.contoso.com.

https://technet.microsoft.com/en-us/library/cc731879(v=ws.10).aspx



HOGESCHOOL PXL

DNS Concepts:

DNS = database met domeinnaam informatie

DNS is ingedeeld in zones (vergelijkbaar table) en bevat records.

Zone: afgebakende blok informatie (authority): contoso.com

Via delegatie kunnen subdomeinen aparte zones op andere servers worden (delegatie van authority) en beheerd worden door andere afdelingen.

belgium.contoso.com
japan.contoso.com
germany.contoso.com

DNS Concepts:

Forward Lookup Zone: naam->IP

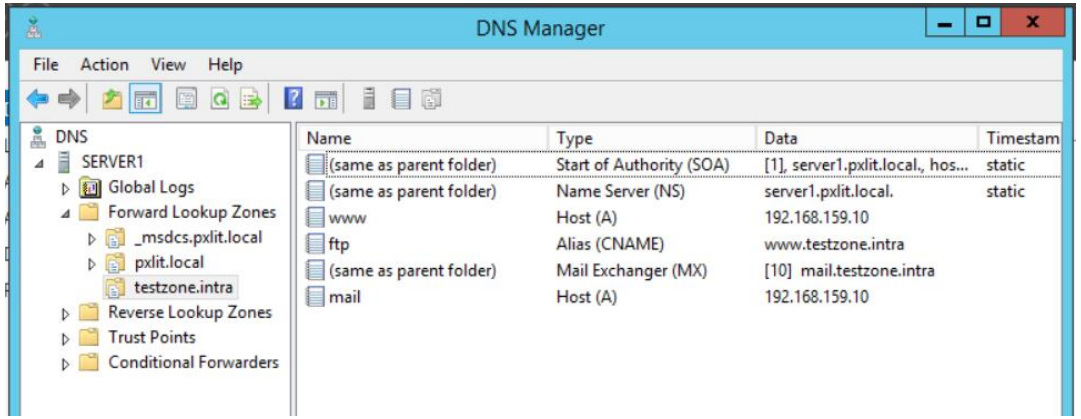
SOA record: algemene informatie over de zone

- default TTL: hoe lang blijven records in cache

MX record: mail exchanger record -> geeft aan wie de mailserver is

A record: mapping naam -> IP adres

CNAME record: naam -> naam

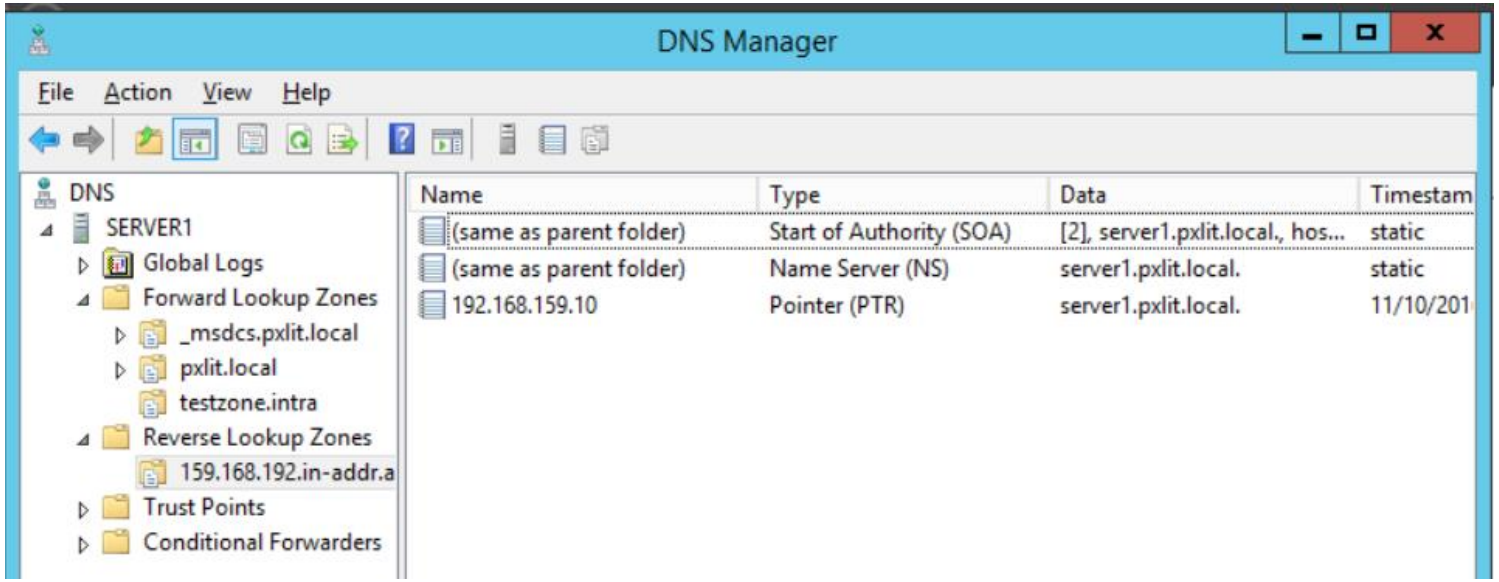


DNS Concepts:

Reverse Lookup Zone: IP -> naam

PTR record: IP -> naam

Zo krijgen je logs ook namen van toestel ipv enkel ip adressen



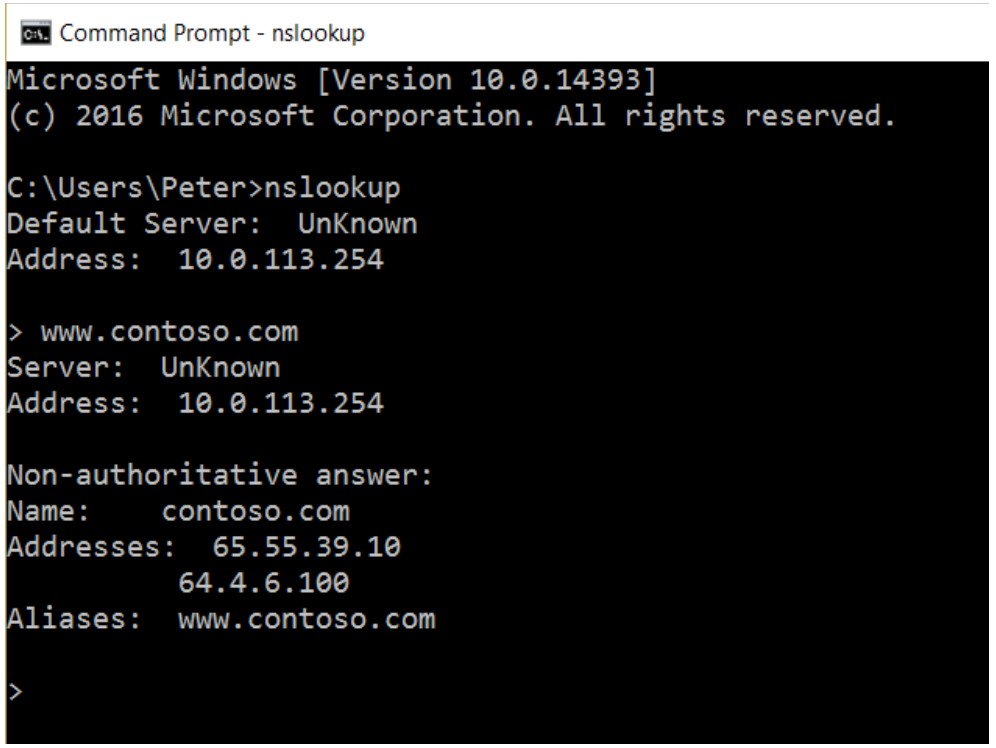
NSLOOKUP

Nslookup om dns query te testen:

Default Server: reverse lookup van de huidige nameserver, geeft weer wie je nameserver is.

Non-authorative answer:

Uit de cache van de dns-server komt het antwoord: www.contoso.com = 65.55.39.10 & 64.4.6.100



NSLOOKUP

set type='type' kan binnen nslookup gebruikt worden om het specifieke type van een record op te vragen

set type=any
set type=a
set type=soa
set type=mx

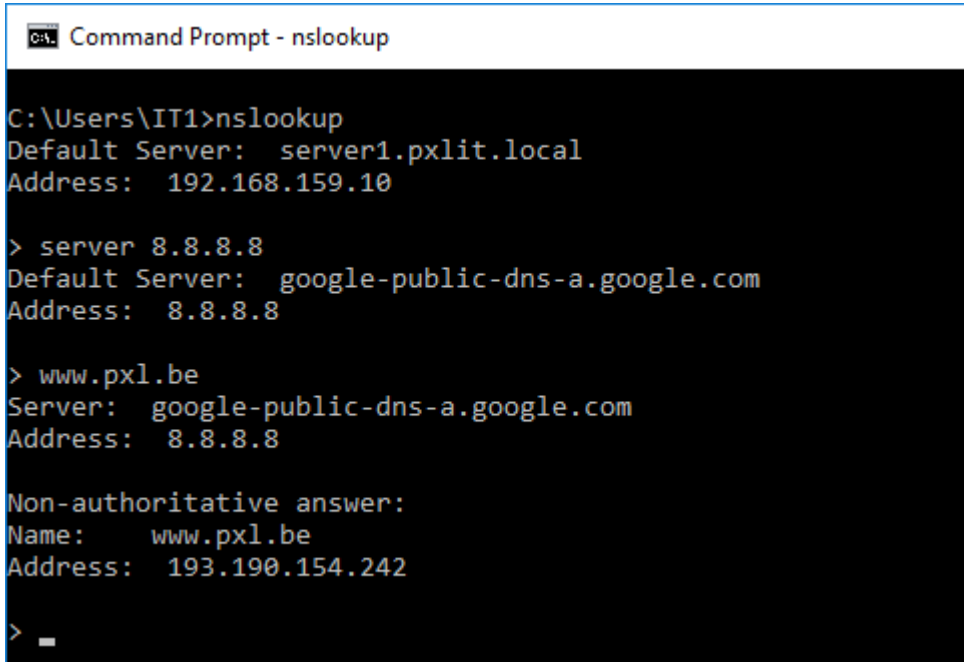
```
> set type=soa
> contoso.com
Server:  UnKnown
Address:  10.0.113.254

Non-authoritative answer:
contoso.com
        primary name server = ns1.msft.net
        responsible mail addr = msnhst.microsoft.com
        serial  = 2015071001
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 7200000 (83 days 8 hours)
        default TTL = 3600 (1 hour)
> set type=mx
> contoso.com
Server:  UnKnown
Address:  10.0.113.254

Non-authoritative answer:
contoso.com     MX preference = 10, mail exchanger = mail.global.frontbridge.com

mail.global.frontbridge.com     internet address = 207.46.163.170
mail.global.frontbridge.com     internet address = 207.46.163.138
mail.global.frontbridge.com     internet address = 207.46.163.247
```

NSLOOKUP

De nameserver waar je de vraag aan gaat stellen kan je veranderen met:

server IP-van-de-andere-nameserver

Nslookup gaat de vraag rechtstreeks stellen aan de nameserver in kwestie en je het antwoord rapporteren.



DNS & Cache

De resolver van windows zal standaard reeds gestelde dns vragen cachen.
(van applicaties, niet van nslookup, want hierbij stel je de vraag rechtstreeks aan de nameserver ZONDER OS resolver)

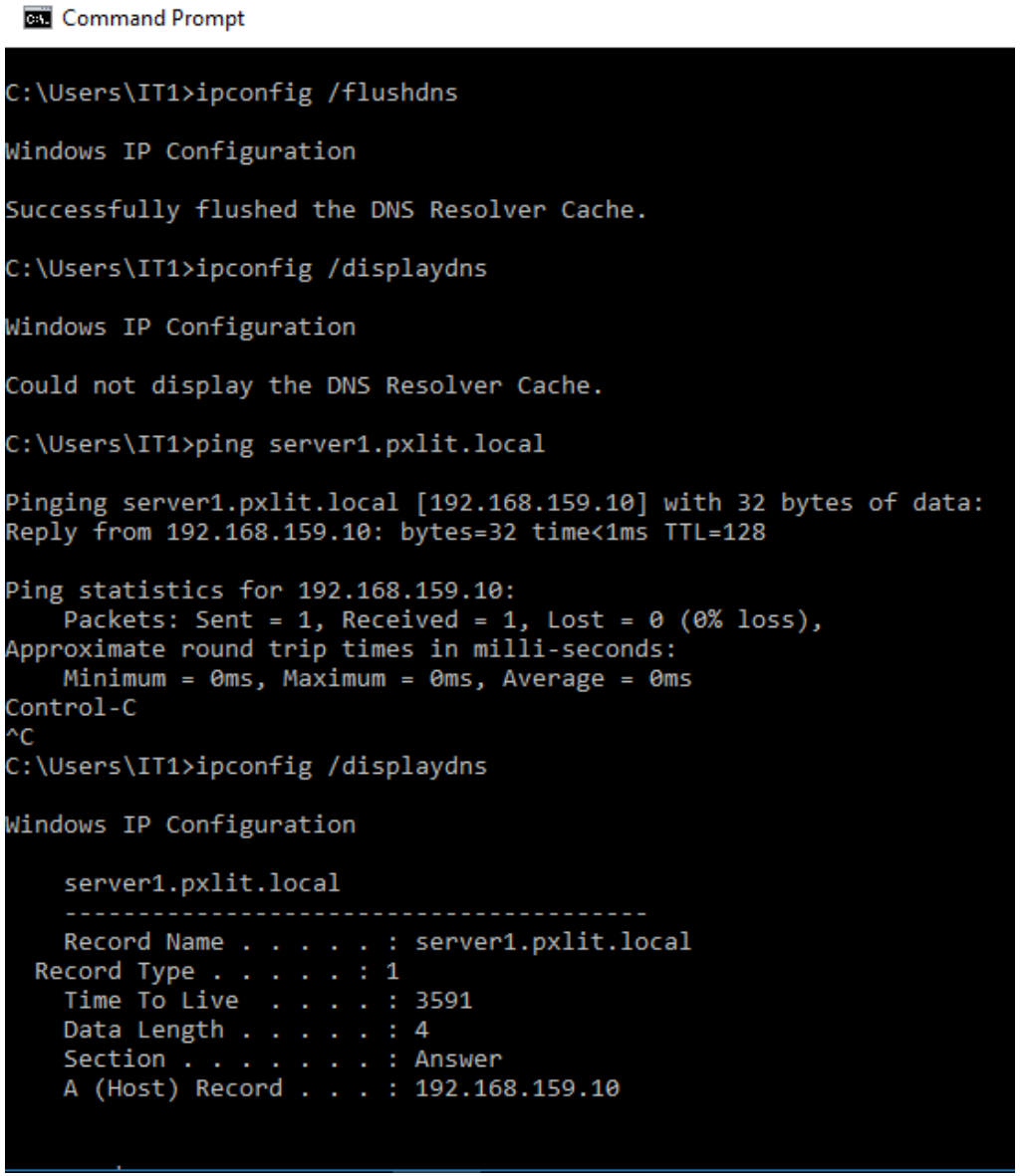
ipconfig /flushdns

ping client1.pxlit.local

ipconfig /displaydns

Let op met de TTL -> cache blijft hangen

Hier nog 3591 seconden!



HOGESCHOOL PXL

DNS Concepts:

Client: recursieve query

Mogelijke Antwoorden:

IP

geen antwoord

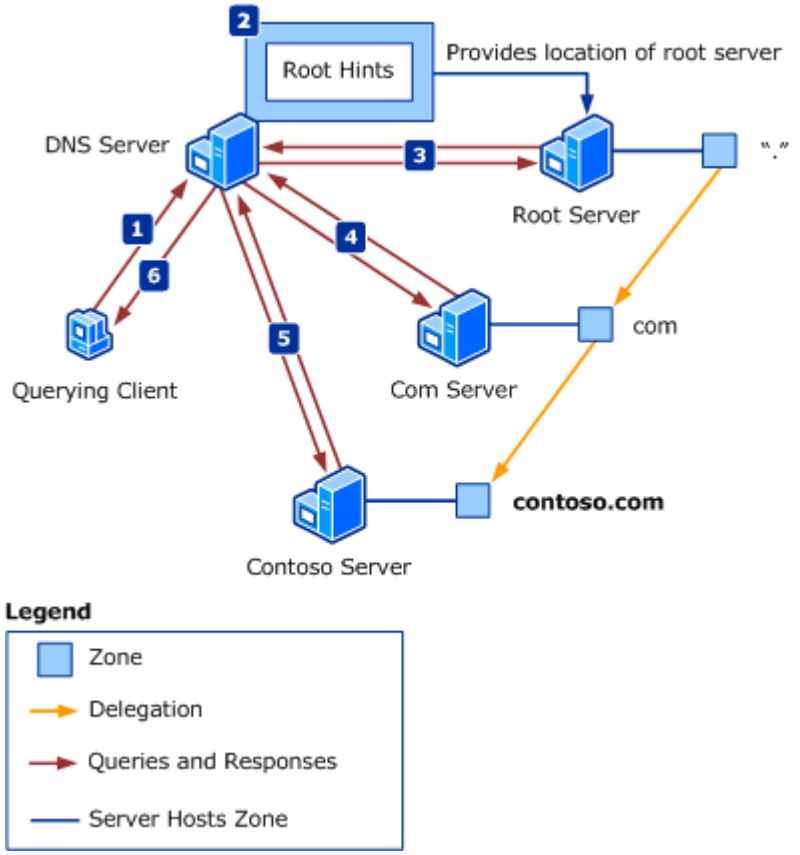
Server: iteratieve query

Mogelijke Antwoorden:

IP

geen antwoord

ik weet het niet maar ga kijken bij nameserver X

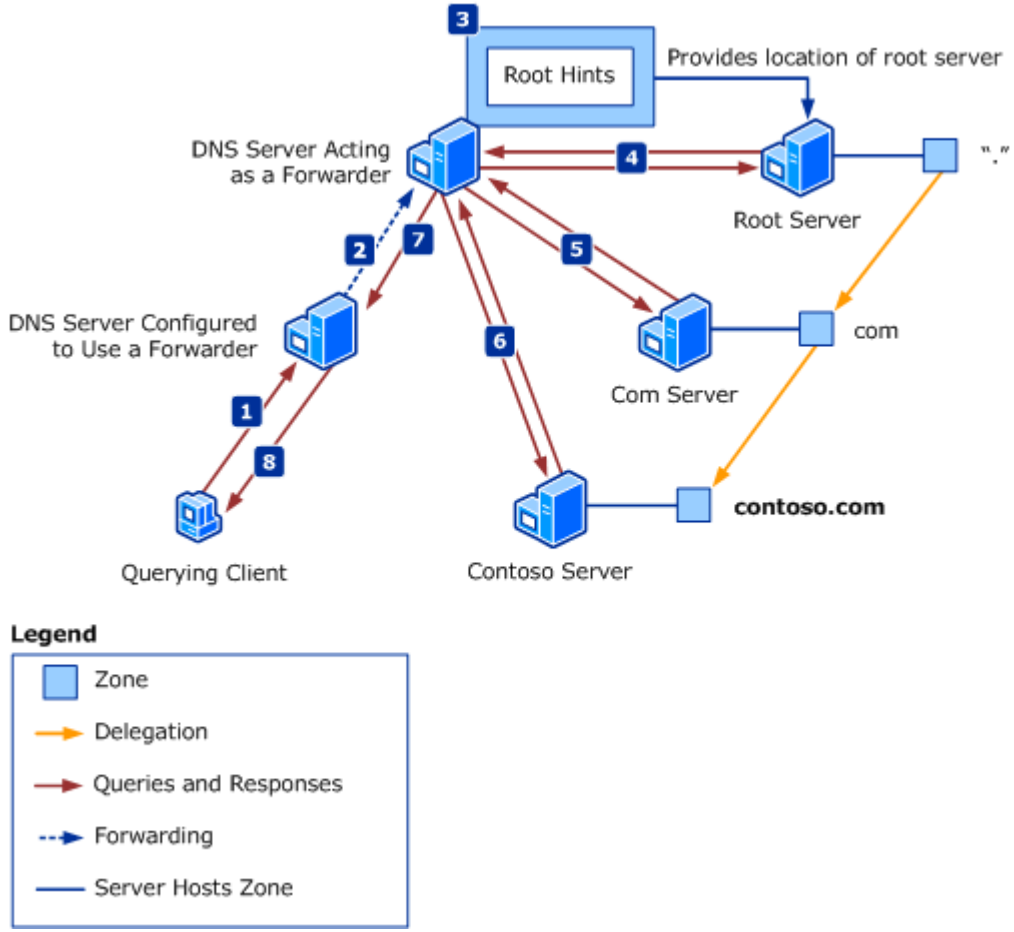


DNS Concepts:

DNS Forwarding:

Als je server geen vragen kan stellen op het internet zal de vraag geforwarded worden naar een hogerliggende dns-server met wel toegang tot het internet

Verder afhandeling, idem server



DNS & Active Directory

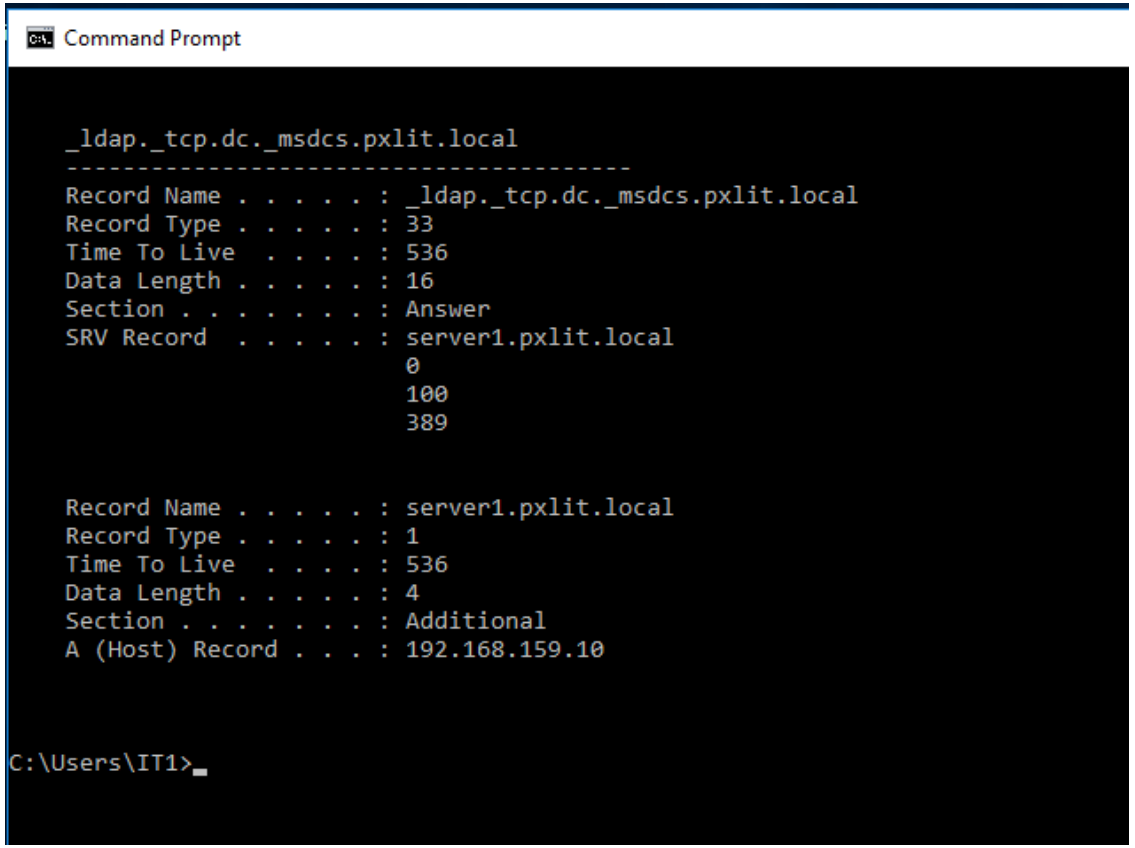
Active Directory kan NIET zonder DNS:

AD: bevat objecten die users,computers,... Voorstellen

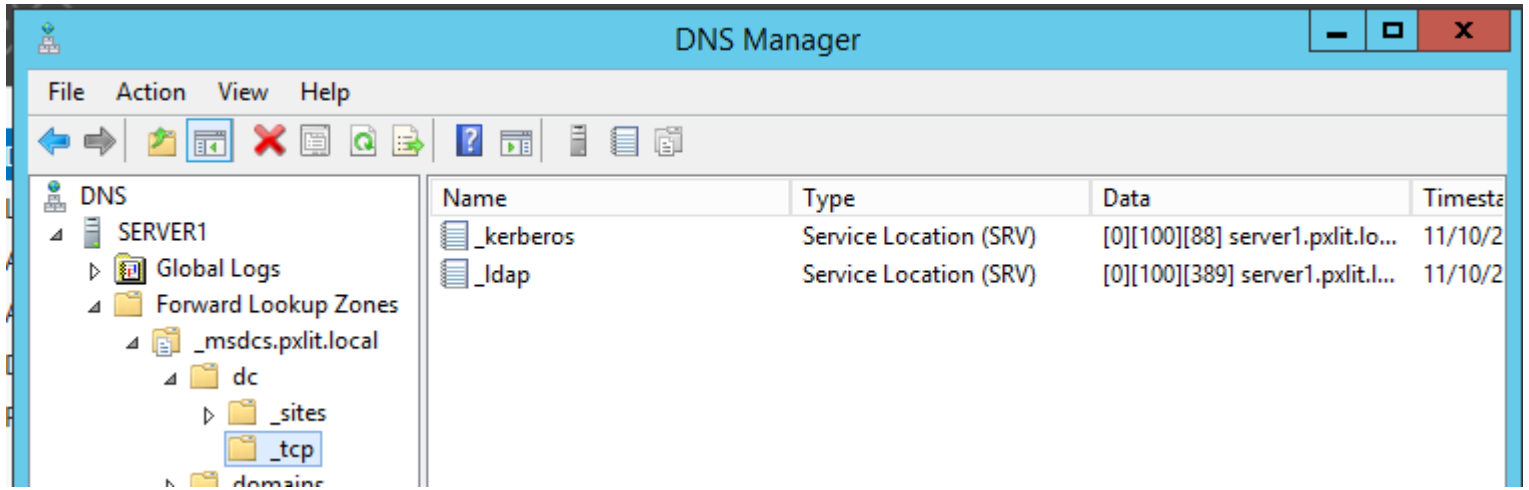
DNS: zorgt voor de koppeling van deze objecten naar IP's en afficheren van services.

Reboot de Client en kijk in dnscache
ipconfig /displaydns

Je hebt nooit ingegeven in de client waar de server te vinden is, enkel de nameserver ingesteld -> de client vraagt via dns op waar de server te vinden is (ldap).



DNS & AD



Deze gegevens kan je terugvinden in je DNS van je Domaincontroller en geven de LDAP service aan.
Je ziet hier ook records voor kerberos, de global catalog en bijkomende services.

DNS is onlosmakelijk verbonden met AD!

DNS.be

DNS.be is een vzw die in België verantwoordelijk is voor dns.

Via een DNS agent huur/koop je een domeinnaam voor een periode van standaard 1 jaar.

Je krijgt dan het recht deze domeinnaam te laten verwijzen naar de nameservers van jou keuze.

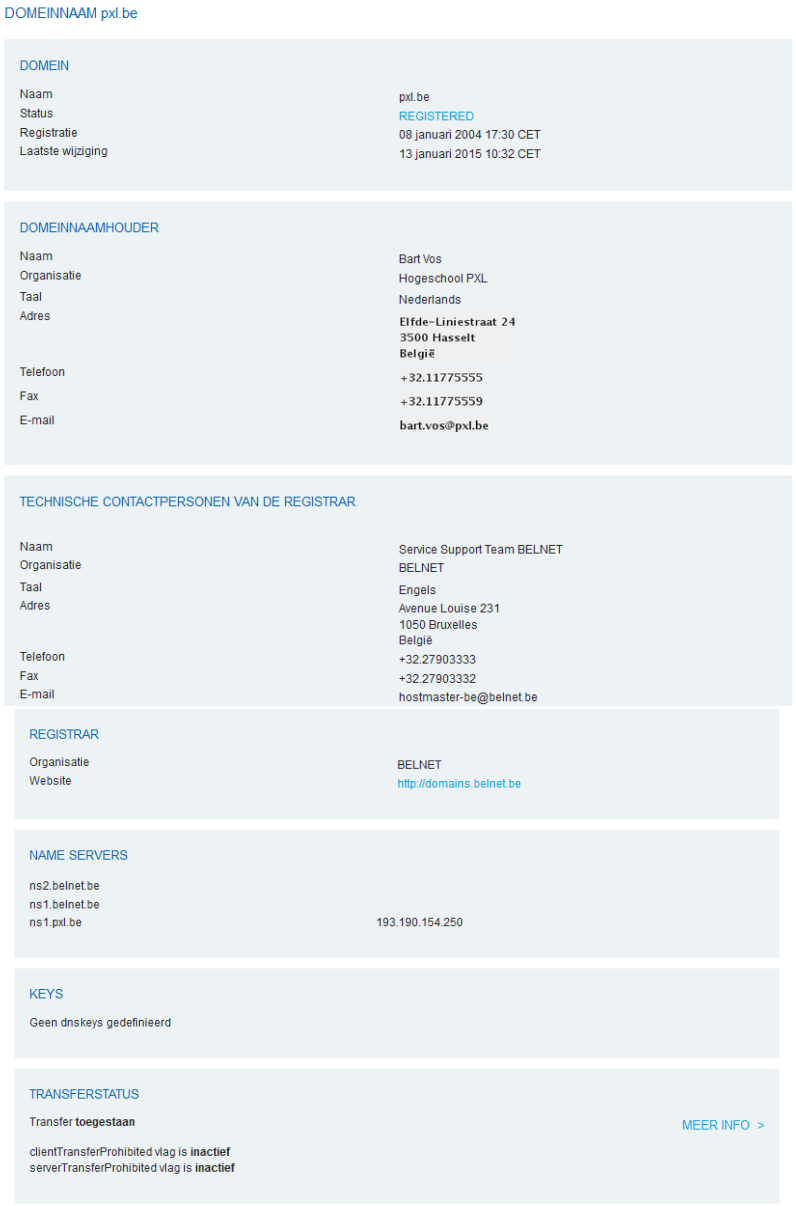
Zoek de nameservers van pxl.be eens op via whois op de site van dns.be

HOGESCHOOL PXL

DNS.be

Een domeinnaam heeft

- Domeinnaamhouder (eigenaar)
- Technical Contact (technische ondersteuning)
- Registrar (agent)
- Nameservers
- Keys (dynamische updates/wijzigingen)
- Transferstatus



DOMEINNAAM pxl.be

DOMEIN

Naam	pxl.be
Status	REGISTERED
Registratie	08 januari 2004 17:30 CET
Laatste wijziging	13 januari 2015 10:32 CET

DOMEINNAAMHOUDER

Naam	Bart Vos
Organisatie	Hogeschool PXL
Taal	Nederlands
Adres	Elfde-Liniestraat 24 3500 Hasselt België
Telefoon	+32.11775555
Fax	+32.11775559
E-mail	bart.vos@pxl.be

TECHNISCHE CONTACTPERSONEN VAN DE REGISTRAR

Naam	Service Support Team BELNET
Organisatie	BELNET
Taal	Engels
Adres	Avenue Louise 231 1050 Bruxelles België
Telefoon	+32.27903333
Fax	+32.27903332
E-mail	hostmaster-be@belnet.be

REGISTRAR

Organisatie	BELNET
Website	http://domains.belnet.be

NAME SERVERS

ns2.belnet.be	
ns1.belnet.be	
ns1.pxl.be	193.190.154.250

KEYS

Geen dnskeys gedefinieerd

TRANSFERSTATUS

Transfer **toegestaan** MEER INFO >

clientTransferProhibited vlag is **inactief**
serverTransferProhibited vlag is **inactief**

HOGESCHOOL PXL

Split DNS:

Andere DNS realiteit binnen/buiten

1)Vraag www.pxl.be op in nslookup

Verzet je nameserver naar 8.8.8.8 (google dns)

2)Vraag www.pxl.be opnieuw op in nslookup

1) Geeft je een adres uit de private range

2) Geeft je een internet adres, publieke range

Afhankelijk van waar je gaat inpluggen kan de DNS reply verschillen.
Zo kan je makkelijker een onderscheid maken of een user ‘intern’ of ‘extern’ is.

DNS Zones

Primary zone: eerste originele zone binnen je dns. Is read/write en bevat alle records van je domein. Tussen primary zones wordt continu gerepliceerd.

Secondary zone: kopie van de primary zone en is enkel read-only. De records worden niet weggeschreven. Ze worden ook enkel geupdate na een zone transfer.

Active directory integrated zone: een DNS zone waarbinnen alle records ook naar de AD worden geschreven.

Forward lookup zone: zone waarbij de records een dns naam bevatten en het corresponderend ip wordt opgeslagen.

Reverse lookup zone: zone waarbij de records een ip adres bevatten en de corresponderende naam wordt opgeslagen.

Stub zone: bevat enkel de dns zone records zodat aangevraagde records kunnen worden doorgestuurd naar een master zone (primary zone bv).

Soorten dns records

Resource Records Type	Name	Function
A	Host record	Contains the IP address of a specific host, and maps the FQDN to this 32-bit IPv4 addresses.
AAAA	IPv6 address record	Ties a FQDN to an IPv6 128-bit address.
CNAME	Canonical Name / Alias name	Ties an alias to its associated domain name.
MX	Mail exchange record	Provides routing for messages to mail servers and backup servers.
NS	Name server record	Provides a list of the authoritative servers for a domain. Also provides the authoritative DNS server for delegated subdomains.
PTR	Pointer resource record	Points to a different resource record, and is used for reverse lookups to point to A type resource records.
SOA	Start of Authority resource record	This resource record contains zone information for determining the name of the primary DNS server for the zone. The SOA record stores other zone property information, such as version information.
SRV	Service locator record	Used by Active directory to locate domain controllers, LDAP servers, and global catalog servers.

Lab

Maak een nieuwe primary forward lookup zone pxl.be

Maak een nieuwe cname www in de FLZ pxl.be en koppel deze aan de A-host record van server1.pxlit.local.

Ping naar www.pxl.be. Welk ipadres krijg je? Waarom?

Maak een nieuwe primary forward lookup zone voetbal.be

Maak een nieuwe cname intranet in de FLZ voetbal.be en koppel deze aan de A-host record van server1.pxlit.local.