Reeks B

Vraag 1: DHCP (§2.1 & §2.1.1)

a. Geef een overzicht van de belangrijkste DHCP *concepten* en *terminologie*.
b. Waarin verschilt DHCP van BOOTP ? Beschrijf de *structuur* van DHCP berichten. Je hoeft de verschillende types berichten niet te vermelden.
c. Waarom voert DHCP *opties* in ?
d. Geef een overzicht van de *courant gebruikte* DHCP opties.
e. Beschrijf wat er gebeurt op DHCP niveau bij het heropstarten van een *Windows Server* toestel, nadat men een shutdown heeft uitgevoerd.
f. Beschrijf wat er gebeurt indien een *Windows Server* DHCP-*cliënt* geen DHCP-server kan bereiken.

A)
Concepten:
- Dynamic **H**ost **C**onfiguration **P**rotocol: DHCP werkt volgens het client-server model: er worden één of meerdere servers gebruikt die configuratie informatie bevatten voor de DHCP-clients. Een client stuurt bij het opstarten een korte DHCP-aanvraag naar alle computers op zijn subnetwerk (niet verder omdat de netwerksoftware nog niet volledig actief is), in de hoop dat er minstens 1 DHCP-server reageert. Deze stuurt de gevraagde configuratie-informatie terug.

- Een DHCP-server bevat lijst van configuratie informatie voor *specifieke geregistreerde computers*. Deze toestellen krijgen een permanente configuratie toegewezen (toestellen met nood aan vaste identificatie naar buitenwereld vb. www-servers).

- Hij kan ook dynamisch adressen uitdelen aan *niet-geregistreerde computers* (deze krijgen telkens het volgende vrije adres uit de DHCP-scope). Deze adressen hebben beperkte lease → onderhandeling cliënt-server voor verlenging.
Een DHCP-scope is een soort van reservoir van vrije IP-adressen.

- DHCP-server kan zichzelf geen ip-adres toewijzen, deze moet dus manueel geconfigureerd wordens

- DHCP-server kan ook gebruikt worden op netwerk dat meer pc's bevat dan maximum toegelaten aantal. Die pc's kunnen dan niet allemaal tegelijk actief zijn.

- DHCP koppelt IP-adres en MAC-adres. Zo onthoudt hij welk IP-adres bij welke machine hoort.

- Voordelen:
- TCP/IP instellingen cliënt automatisch opnieuw geconfigureerd indien opgestart op nieuwe locatie.
- beperking van de complexiteit en omvang van een aantal beheerstaken
- vermijden configuratiefouten en adresconflicten
- onafhankelijk van besturingssysteem.

Terminologie:
DHCP-servers: bevatten configuratie informatie voor DHCP-cliënts.
DHCP-cliënts: computers die van de diensten v/ DHCP-servers willen gebruik maken
DHCP-scope: een reservoir van vrije IP-adressen (dynamisch uitdelen adressen)
Lease: de geldigeheidsduur van een IP-adres, dynamisch toegekend.
DHCP-opties: gecodeerde gegevensitems die opgeslagen worden in de protocolberichten, uitgewisseld tussen DHCP-server en zijn cliënt.

B)

Verschil DHCP <> BOOTP:

- BOOTP: vereist op voorhand een lijst van alle MAC-adressen v/d ethernetkaarten
- BOOTP: geen mogelijkheid om tijdelijke IP-adressen ter beschikking te stellen
- DHCP = BOOTP + scopes + opties (in TLV formaat).

Structuur berichten:

1) Header: vaste lengte (300 bytes). DHCP header identiek aan BOOTP header. Het bevat oa.:

- Transactie ID: cliënt Hiermee kan de client, als hij een antwoord krijgt van de server, weten op welke vraag dit een antwoord is.
- IP (zonder subnetmasker) + MAC-adressen cliënt
- IP + naam server

De opties worden voorafgegaan door een veld van 4 vast bytes (99.130.83.99), dat het *magic cookie* genoemd wordt en het formaat van het DHCP-bericht identificeert.

2) *Opties:* variabele lengte. Elke optie bevat 3 velden:

1. Veld1: 1 byte, identificeert de optie
2. veld2: 1 byte, grootte in bytes van veld 3,
3. veld3: waarde v/d optie

- *Optie 255*: niet verplicht, aanduiden einde DHCP-opties, alles na deze optie wordt genegeerd. (geen lengte of waarde-veld)
- *Padding veld*: niet verplicht, om de verschillende opties in het DHCP-bericht uit te lijnen op woordgrenzen. Deze optie wordt als optie 0 geimplementeerd. (geen lengte of waarde-veld)

C)

Bij toewijzing van een adres kan meteen ook een heel pakket configuratiewaarden doorgegeven worden via deze opties. Als DHCP-server optie aanbiedt waarmee cliënt niets kan aanvangen → optie wordt genegeerd.

D)

1	duidt het subnetmasker v/h cliëntsubnet aan
3	een lijst met IP-adressen van default gateways, die door de cliënt in volgorde gebruikt worden
6	een lijst met IP-adressen van DNS nameservers, die door de cliënt in volgorde gebruikt worden
12	een naam voor de cliënt met een maximumlengte van 63 tekens
15	de DNS suffix, die door de cliënt gebruikt wordt bij het herleiden van niet-gekwalificeerde DNS namen
19	bepaalt of de cliënt de functie van router vervult
23	geeft de standaard ttl-waarde aan voor uitgaande datagrammen
28	doorgaans 255.255.255.255, maar kan gewijzigd worden in andere geldige waarden voor broadcast adressen
31	geeft aan of de cliënt routers aanvraagt via ICMP router-discovery
33	lijst met paren IP-adressen, telkens het netwerkadres en het routeradres van een route
35	geeft een time-out waarde in seconden voor vermeldingen in de ARP cache
69	een lijst met IP-adressen voor SMTP servers, in volgorde van voorkeur
70	een lijst met IP-adressen voor POP3 servers, in volgorde van voorkeur

E)
Windows DHCP-clients bewaren de DHCP-configuratie lokaal op de harde schijf in het register *hive*. Na opnieuw opstarten wordt geprobeerd de oude lease te verlengen (DHCP-Request zenden). Als DHCP-server waarvan ip verkregen niet beschikbaar is, dan probeert de client te detecteren of ze nog steeds in hetzelfde subnetwerk staan door een ping opdracht uit te voeren naar zijn default gateway. Indien dit zo is, blijven ze de oude lease stilzwijgend verder gebruiken.

F)
Indien geen DHCP-server kan bereikt worden dan kunnen Linux- en Windows-clients met een tijdelijke IP-configuratie werken (= **A**utomatic **P**rivate **IP** **A**ddressing of automatische IP-configuratie). Zeer nuttig voor cliënts in kleine netwerken.
De adressen worden automatisch toegekend uit klass-B adressen 169.254/16 (niet gebruikt op Internet). Deze toewijzingen zijn transparant voor gebruikers en ze krijgen geen waarschuwing als adreslease bij DHCP-server mislukt is.
DHCP-cliënt zal dan conflictendetectie uitvoeren door met *Gratuitous ARP aanvraag* te controleren of IP-adres gebruikt is in netwerk. Indien bezet wordt ander random IP-adres gekozen en getest (win: max 10 keer).
DHCP-cliënts blijven in de achtergrond proberen (win: elke 5min) de DHCP-server te bereiken en adreslease te verkrijgen. Indien dit lukt dan vervalt de automatische configuratie en gebruikt DHCP-cliënt configuratie door DHCP-server aangeboden.

Vraag 2: DHCP leaseprocessen en relay-agents (§2.1.2 & §2.1.3)

a. Geef een overzicht van de verschillende *types* DHCP berichten.
b. Bespreek de opeenvolgende *stappen* van beide DHCP *leaseprocessen*.
c. Bespreek doel en werking van DHCP *relay-agents*. Welke velden in DHCP berichten helpen deze functie realiseren ?
d. Indien je over een aantal DHCP servers beschikt, hoe kun je deze best configureren om een internetwerk, bestaand uit een aantal netwerken, te ondersteunen ?
e. Hoe kunnen *Linux* en *Windows 2000* toestellen als DHCP relay-agent worden geconfigureerd ?

A)
1. DHCP-Discovery bericht
2. DHCP-Offer bericht
3. DHCP-Request bericht
4. DHCP-Decline bericht
5. Positief DHCP-acknowledgment bericht
6. Negatief DHCP-acknowledgment bericht
7. DHCP-Release bericht
8. DHCP-Inform bericht

B)
<u>Initialisatieproces:</u>
→ wanneer computer voor eerst gestart wordt en zich probeert aan te melden bij het netwerk.

1. DHCP-cliënt verzendt *DHCP-discovery* broadcast bericht. In het bericht wordt onderhandeld over leasetijden en gewenste gegevens (opties 51: gewenste leasetijd, optie 55: lijst van gewenste opties). IP-adres van DHCP-cliënt in bericht is 0.0.0.0, dat van destination is 255.255.255.255.

2. Alle DHCP-servers kunnen hierop reageren met een *DHCP-Offer* bericht waarin IP-adreslease wordt aangeboden. Elke DHCP-server zal het aangeboden adres voorlopig reserveren voor de cliënt. Met optie 54 wordt de serveridentificatie (ip-adres) opgenomen → DHCP-cliënt kan onderscheid maken tussen verschillende leaseaanbiedingen. Als er geen DHCP-Offer bericht wordt ontvangen gaat de DHCP-cliënt periodiek (met wachtperiode) opnieuw DHCP-Discovery berichten zenden tot hij uiteindelijk een DHCP-Offer bericht ontvangt.

3. Zodra de DHCP-cliënt 1 of meerdere DHCP-Offer berichten ontvangen heeft, selecteert hij 1 van de aangeboden adressen door een *DHCP-Request bericht* naar de corresponderende server (met optie 54 wordt serveridentificatie ingevuld). Dit wordt gebroadcast zodat andere DHCP-servers zien dat ze niet gekozen zijn → zullen hun gereserveerde adres weer vrij maken.

4. DHCP-server zendt meestal *Positief DHCP-acknowledgment bericht* om de lease te bevestigen, vereiste DHCP-opties worden eveneens meegestuurd. Soms *Negatief DHCP-acknowledgment bericht* (wanneer de client bv een ongeldig of reeds toegekend adres aanvraagt of wanneer de DHCP-server een aanvraag ontvangt voor een subnet waarvoor hij geen DHCP-scope ter beschikking heeft) → initialisatie mislukt → opnieuw vanaf stap 1 beginnen.

5. Als de client een Positief DHCP-acknowledgment bericht is ontvangt worden de TCP/IP eigenschappen van de DHCP-cliënt worden *geconfigureerd* en wordt die client aangemeld op het netwerk.
   Als de client merkt dat er één van configuratieparameters foutief is, dan stuurt deze een *DHCP-Decline bericht* naar de DHCP-server. De client begint opnieuw vanaf stap1.
   DHCP-cliënt wil aanvullende informatie → hij zendt *DHCP-Inform bericht*
   DHCP-cliënt heeft lease niet meer nodig en doet vrijwillig afstand van de lease → hij zendt *DHCP-Release bericht*

<u>Vernieuwingsproces:</u>
→ Als helft van leasetijd is verlopen (T1), dan gaat DHCP-cliënt vernieuwsproces starten om lease te verlengen. Met optie 58 kan afgeweken worden van (T1).

1. DHCP-cliënt zendt (rechtstreeks) *DHCP-Request bericht* naar DHCP-server om adreslease te vernieuwen en te verlengen.

2. DHCP-server zendt meestal (indien bereikbaar) *Positief DHCP-Acknowledgment bericht* naar DHCP-cliënt. Ook worden DHCP-opties meegezonden en automatisch geconfigureerd indien nodig → dynamische aanpassing lease instellingen. Indien geen DHCP-Acknowledgment bericht ontvangen → periodiek (met wachtperiode) DHCP-Request bericht opnieuw verzenden.

3. Indien de client niet in staat is te communiceren met de oorspronkelijke DHCP-server, dan wacht deze totdat ook T_2 (meestal 7/8 van de volledige leasetijd, tenzij optie 59 geconfigureerd is), de tijd voor *rebinding* van de lease, is verstreken. Op dat ogenblik wordt de rebinding-status geactiveerd. De client probeert dan de huidige lease te verlengen bij gelijk welke DHCP-server.

4. Als er een DHCP-server reageert met DHCP-Acknowledgment om cliëntlease bij te werken → DHCP-cliënt zal lease bij deze DHCP-server verlengen. Indien dit bericht niet wordt ontvangen → DHCP-Request bericht wordt 3 maal herhaald (4+,8+ en 16+ seconden).

5. Als lease verloopt en DHCP-cliënt heeft geen verlenging kunnen bekomen → adreslease onmiddellijk beëindigen = TCP/IP op DHCP-cliënt deactiveren. DHCP-cliënt moet van voorafaan herbeginnen (initialisatieproces).

C)
Doel: Dit is een klein programmatje dat DHCP-berichten doorgeeft tussen cliënts en servers in verschillende subnetten. Dit is nodig omdat routers geen broadcastberichten (vb: DHCP-Discovery) doorzenden. Hierdoor zou men anders op elk lokaal subnetwerk een afzonderlijke DHCP-server moeten voorzien.

Opm: De meeste harwdware routers ondersteunen de functionaliteit van *BOOTP-relay agent* en kunnen dus BOOTP-berichten herkennen en doorgeven. Omdat DHCP bercihten via dezelfde UDP-poorten worden verzonden als BOOTP-berichten en precies dezelfde berichtstructuur hebben, geeft de router met de functionaliteit van een BOOTP-relay agent ook alle DHCP-berichten door. Als router deze functionaliteit niet aankan dan moet elk subnet een DHCP-server hebben of op elk subnet moet een *computer* functioneren *als relay-agent*.

Werking: relay-agent ontvangt DHCP-berichten die als broadcast berichten binnenkomen op één van zijn interfaces, hij geeft deze berichten rechtstreeks, point-to-point door aan gekende DHCP-servers of hij broadcast ze opnieuw naar alle externe subnetten via zijn interfaces bereikbaar. Aantal opeenvolgende broadcasts is beperkt: win max 4. BOOTP-header van DHCP-bericht bevat hop-veld dat telkens verhoogd wordt.

Velden:

- Veld met gateway ip-adres in de header v/h DHCP-bericht. Als de relay agent een DHCP-bericht ontvangt en dit veld staat op 0.0.0.0 dan vult hij hierin het adres van de router in.
- A.d.h.v dit ip-adres kan de DHCP-server beslissen als hij beschikt over een scope voor het subnet waarop de DHCP-cliënt zich bevindt.
- Hop-veld → max aantal broadcasts.

D)
Het is raadzaam de DHCP-servers in verschillende subnetten plaatsen, om een hogere mate van fouttolerantie te bereiken. Er is echter geen enkel mechanisme voor communicatie tussen DHCP-servers en ze samen te laten werken. Deze servers mogen dan ook geen gemeenchappelijke ip-adressen in hun scopes hebben. Elke server moet over een unieke groep ip-adressen beschikken.
Dikwijls wordt volgende vuistregel gehanteerd: 80% van het adresbereik van een subnet laten beheren door een DHCP-server van dat subnet en 20% laten beheren door DHCP-servers op externe subnetten. Zo kunnen de DHCP-aanvragen doorgestuurd worden naar een extern subnet wanneer een server wordt afgesloten.

E)
Linux: commando **dhcrelay** met als argumenten ip-adressen van één of meerdere DHCP-servers aan dewelke DHCP-berichten moeten doorgestuurd worden.
Windows:Analoog als RIP en OSPF wordt DHCP Relay Agent als nieuw routingprotocol toegevoegd m.b.v. **rrasmgmt.msc** MMC Console. Minstens één interface toevoegen via de controlestructuur en General tabpagina invullen (max waarde hop-veld, vertragingsinterval). Locatie van DHCP-servers inbrengen door rechtermuisknop op DHCP Relay Agent controlestructuur > properties > General tabpagina invullen.

Vraag 3: Configuratie van DNS servers onder Linux (§3.3.2)
De figuur in bijlage stelt een intranet bestaand uit een aantal *Linux* computers voor, met corresponderend IP-adres, van de vorm 192.168.16.*z* . Het getal *z* lees je af links van de naam van de computer. De getallen rechts van de naam van de computer moet je negeren. De computers staan gegroepeerd in een tabel met als header de naam van het domein waarin ze zich bevinden. De rechthoeken die domeinen groeperen stellen dan weer een zone voor. Stippellijnen duiden op een domein/subdomein relatie. De pijlen laten toe om de primaire nameserver van elke zone te achterhalen. Geen enkele zone heeft een secundaire nameserver. Je hoeft geen reverse DNS te configureren.

a. Stel het *configuratiebestand* en alle *zonebestanden* op van volgende DNS servers, waarbij je er rekening moet mee houden dat elk van deze servers ook *secundaire nameserver* is voor alle zones van de andere server: ... . Gebruik **relatieve DNS namen** waar mogelijk. Gebruik noch *forwarders*, noch de $ORIGIN opdracht !
b. Bespreek in detail het begrip *secundaire nameserver*, inclusief voordelen, beperkingen en problemen. (§3.1 & §3.3.3)

A) *niet gevonden... is blijkbaar niet opgelost in de originele versies ?Die komt nog 2 keer terug in de volgende vragen dus is vrij belangrijk ☺*

B)
Naast primaire bestaan er ook secundaire nameservers, deze houden precies dezelfde informatie bij als de primaire nameservers.
Doel: Verlichten van de taak van primaire nameservers en zorgen voor verhoogde fouttolerantie. Als primaire uitvalt kan secundaire gepromoveerd worden (door netwerkbeheerder).
Beperkingen:
Wijzigingen van gegevens v/d zone worden enkel doorgevoerd bij de primaire nameserver. De secundaire nameserver moet dus regelmatig contact opnemen met de primaire om een kopie van de nieuwe zone-informatie te verkrijgen.
Opm:

- In het configuratiebestand van named is voor een secundaire nameserver de lijn allow-transfer { ip-adressen; }; verplicht bij options sleutelwoord.
- Als men bij zone sleutelwoord als type **slave** gebruikt: named is secundaire nameserver voor opgegeven zone. **masters** lijn bevat één of meerdere ip-adressen van nameservers voor dit domein. **file** lijn bevat naam zonebestand, relatieve padnaam altijd t.o.v. dir opgegeven in options. Dit bestand wordt door server automatisch aangemaakt en bevat kopie van de zone-informatie v/h opgegeven domein → sec nameserv kan dus blijven werken als prim nameserv uitvalt. Daarom aanbevolen minimaal 2 nameservers te gebruiken voor elke zone.

Vraag 4: Configuratie van DNS servers onder Linux

De figuur in bijlage stelt een intranet bestaand uit een aantal *Linux* computers voor, met corresponderend IP-adres, van de vorm 192.168.16.*z* . Het getal *z* lees je af links van de naam van de computer. De getallen rechts van de naam van de computer moet je negeren. De computers staan gegroepeerd in een tabel met als header de naam van het domein waarin ze zich bevinden. De rechthoeken die domeinen groeperen stellen dan weer een zone voor. Stippellijnen duiden op een domein/subdomein relatie. De pijlen laten toe om de primaire nameserver van elke zone te achterhalen. Geen enkele zone heeft een secundaire nameserver. Je hoeft geen reverse DNS te configureren.

a. Stel het *configuratiebestand* en alle *zonebestanden* op van volgende DNS servers: ... . Gebruik **relatieve DNS namen** waar mogelijk. Gebruik noch *forwarders*, noch de $ORIGIN opdracht !
b. Bespreek in detail het formaat van een *zonebestand* en zijn *records*. Je mag dit doen op basis van één van de oplossingen in a), doch je moet ook alternatieve records en formaten beschrijven, die je niet noodzakelijk hebt gebruikt. (§3.3.1 & §3.3.4)

B)
Doorgaans correspondeert elke lijn van het zonebestand met een afzonderlijke DNS-record. Meerdere lijnen als 1 record groeperen kan mbv ronde haakjes.

Elke DNS-record bestaat uit 5 velden: naam ttl **IN** recordtype waarde

Veld1:
- naam van een machine of een domein (mag ook spatie of tab zijn, dan wordt de naam van het vorige record in het bestand gebruikt).
- Namen kunnen op verschillende manieren genoteerd worden:
  - Een niet-gekwalificeerde alfanumerieke naam: dit is een naam die relatief is t.o.v. domein waarvoor dit een zonebestand is.
  - Naam eindigt op punt: dit is een absolute domeinnaam
  - Speciale naam @: verwijst naar huidige oorsprong, wordt doorgaans enkel gebruikt bij SOA record bovenaan het bestand → oorsprong = huidige domein, $ORIGIN: oorsprong wijzigen

Veld2:
- Time-to-Live (ttl): mag weggelaten worden, geeft aan hoelang DNS-record geldig is (en hoelang het door andere computer gecached mag worden), weinig gebruikt omdat in een SOA-record een default ttl-waarde opgegeven wordt.

Veld3:
- IN (afkorting voor Internet): ook nog andere maar niet veel gebruikt

Veld4:
- Type DNS-record: A, PTR, MX, SOA, NS, CNAME

Veld5:
- Waarde DNS-record: ip-adres opgegeven naam(A), ip-adres mailserver (MX)

Commentaarlijnen worden voorafgegaan door ';'.

Het eerste record is een SOA-record (**S**tart **o**f **A**uthority) → geeft begin aan van de records van bepaalde zone, in elk bestand maar één SOA-record als we per zone één zonebestand gebruiken.
Formaat:
@ IN SOA dns-naam email (
volgnummer
refresh interval
retry interval
expire interval
default ttl
)

- *DNS-naam primaire nameserver* (absoluut) gevolgd door *e-mailadres* v/ persoon verantwoordelijk voor server ('@' vervangen door '.').
- *Volgnummer*: dit nummer wordt gebruikt door de secundaire DNS-server om na te gaan of de informatie die zij hebben nog wel recent is. Nummer telkens verhogen bij wijziging configuratiebestand. Conventie: 8 eerste cijfers = jaartal,maand,dag; laatste 2 = hoeveelste wijziging.
- *4 tijdsduren*: in seconden
    - *refresh interval:* geeft aan om de hoeveel tijd de secundaire nameserver voor deze zone zijn database moet veranderen (1 à 2 keer per dag = voldoende).
    - *Retry interval:* hoelang sec. nameserv moet wachten om prim. nameserv opnieuw te contacteren na mislukte refresh
    - *Expire interval:* hoelang gegevens bewaren als refresh mislukt
    - *Default ttl:* mag grote waarde hebben (week of maand)

Na SOA-record meestal een aantal NS-records. Deze sommen de namen op van alle primaire en secundaire nameservers van dit domein en al zijn gedelegeerde domeinen. Ook nameservers vermelden die zich buiten het domein bevinden!
Formaat: **IN NS** naam

Bij MX-record wordt voor de naam een prioriteit opgegeven → indien meerdere MX-records voor zelfde naam wordt laagste prioriteit gekozen.
Formaat: **IN MX** prioriteit naam

Een CNAME-record wordt gebruikt om een alias op te geven voor een bepaalde DNS-naam. Alias mag enkel aan linkerkant van CNAME-definitie staan en niet aan linkerkant van andere definitie! → CNAME-records zoveel mogelijk vermijden en door A-records vervangen.
Het is mogelijk ip-adres aan meerdere namen te koppelen of meerdere ip-adressen aan zelfde naam te koppelen → cyclisch volgorde gebruikt → belastingdaling.

Vraag 5: Configuratie van DNS servers onder Linux

De figuur in bijlage stelt een intranet bestaand uit een aantal *Linux* ...(cfr.vraag B5)...

achterhalen. Geen enkele zone heeft een secundaire nameserver. Je hoeft geen reverse DNS te configureren.

a. Stel het *configuratiebestand* en alle *zonebestanden* op van volgende DNS servers: ... . Gebruik **relatieve DNS namen** waar mogelijk. Gebruik noch *forwarders*, noch de $ORIGIN opdracht !
b. Bespreek in detail het formaat van een *configuratiebestand*. Je mag dit doen op basis van één van de oplossingen in a), doch je moet ook alternatieve opdrachten en sleutelwoorden beschrijven, die je niet noodzakelijk hebt gebruikt. (§3.3.3)

B) Het bestand is onderverdeeld in een aantal opdrachten bepaald door sleutelwoorden (zone en options zijn belangrijkste).

options groepeert een aantal opties; elke optie bestaat uit sleutelwoord, eventueel een aantal parameters, afsluitende kommapunt.

- **directory *padnaam*;** : dir waar zonebestanden zich bevinden
- **forwarders { *ip-adressen;* };** : lijst van ip-adressen waarnaar named zijn vraag zal richten als hij DNS-informatie niet in eigen cache vindt, als deze servers ook geen antwoord hebben → aanvraag aan root-servers. Is belastingverlagend voor root-servers.
- **allow-transfer { ip-adressen; };** : lijst van ip-adressen van computers die zone-transfer kunnen uitvoeren, bij ontbreken kunnen alle computers dit. Noodzakelijk voor secundaire nameservers en ls commando van nslookup. Ook netwarkadressen met prefixlengtesyntax kunnen opgegeven worden.

zone–opdrachten geven informatie over verschillende zones waarvoor de geconfigureerde DNS-server moet instaan (primair of secundair). Na zone volgt naam zone tussen "" en eventueel gevolgd door in, tussen accolades bevindt zich de zone-specifieke configuratie-informatie.

- **type**: geeft functie van de nameserver aan
  - **master**: named is primaire nameserver voor opgegeven zone. **file** lijn bevat naam zonebestand, relatieve padnaam altijd t.o.v. dir opgegeven in options. **allow-update** lijn (optioneel, ip-adres of netwerkadres/prefix) vermeldt computers die dynamische updates mogen uitvoeren. **allow-transfer** lijn hier heeft voorrang op deze bij options.
  - **slave**: named is secundaire nameserver voor opgegeven zone. **masters** lijn bevat één of meerdere ip-adressen van nameservers voor dit domein. **file** lijn is analoog. Dit bestand wordt door server automatisch aangemaakt en bevat kopie van de zone-informatie v/h opgegeven domein → sec nameserv kan dus blijven werken als prim nameserv uitvalt. Daarom aanbevolen minimaal 2 nameservers te gebruiken voor elke zone. Meerdere prim nameservs per zone kan maar afgeraden → inconsistentie.
  - **stub**: stub nameserver gedraagt zich zoals sec. nameserv maar dupliceert enkel NS records v/d opgegeven master servers.
  - **forward**: stuurt alle aanvragen door naar andere nameservers, ip-adressen vermeld in forwarders-lijn → in options (globaal voor server) of in zone (specifiek voor zone).
  - **hint**: altijd met zonenaam ".", opgegeven bestand bevat lijst van root-servers die gebruikt worden door nameserver bij opstarten en slechts geraadpleegd wordt om namen van echte root-servers te vinden.

Vraag 6: Configuratie van reverse DNS onder Linux

a. Wat wordt beoogd met *reverse DNS* ? Hoe wordt dit gerealiseerd ? (§3.3.2)
b. De figuur in bijlage stelt een intranet voor bestaand uit een aantal *Linux* computers. Alle computers hebben een interface op het gemeenschappelijke 192.168.16/24 netwerk, met corresponderend IP-adres, van de vorm 192.168.16.*z* . Het getal *z* lees je af links van de naam van de computer. Alle computers hebben eveneens een interface op een 10.*x.y*/24 netwerk, met corresponderend IP-adres van de vorm 10.*x.y.z* . De getallen *x* en *y* lees je af rechts van de naam van de computer. De computers staan gegroepeerd in een tabel met als header de naam van het domein waarin ze zich bevinden. De rechthoeken die domeinen groeperen stellen dan weer een zone voor. Stippellijnen duiden op een domein/subdomein relatie. De pijlen laten toe om de primaire nameserver van elke *forward DNS* zone te achterhalen. De *reverse DNS* van het 10/8 internetwerk wordt gedelegeerd aan ... . De *reverse DNS* van de 10.*x*/16 internetwerken ($x \neq 0$) wordt gedelegeerd aan: ... . De *reverse DNS* van de 10.*x.y*/24 netwerken ($x \neq 0, y \neq 0$) tenslotte wordt gedelegeerd aan de computers met IP-adres van de vorm 10.*x.y.z*, die reeds nameserver van meerdere *forward DNS* zones zijn: ... . Geen enkele zone heeft een secundaire nameserver. Stel het *configuratiebestand* en de *zonebestanden* op van alle servers die een rol spelen bij de reverse DNS resolving van IP-adressen behorend tot netwerken ... en ... . Je hoeft hierbij enkel de configuratie informatie te vermelden die noodzakelijk is voor reverse DNS. Gebruik **relatieve DNS namen** waar mogelijk. Het gebruik van *forwarders* is hier niet toegelaten !

A)Reverse DNS = domeinnaam opzoeken voor een gegeven IP-adres. Meestal om beviligingscontrole uit te voeren. De DNS-records die deze omgekeerde informatie bevatten zijn van het type PTR.

Om de naam van de machine met adres w.x.y.z op te zoeken, moet je het PTR-record opvragen van autoritaire server die deze informatie bevat. Omdat we het domeinnaam van die machine niet kennen kunnen we niet zomaar weten waar deze server te zoeken. Om dit op te lossen bestaat er een pseudo-domein met de naam *in-addr.arpa*. Elk netwerkadres heeft een geassocieerde naam in dit speciale domein, naam = z.y.x.w.in-addr.arpa. Wanneer we met behulp van reverse DNS de domeinnaam van de machine met dit ip-adres willen opzoeken, vragen we eigenlijk naar het PTR-record van de naam z.y.x.w.in-addr.arpa. Hiërachische structuur van domein in-addr.arpa komt ongeveer overeen met die v/h netwerk.
Om reverse DNS toe te laten op machines in je eigen netwerk, moet je dus een primaire nameserver configureren voor overeenkomstige subdomein in-addr.arpa domein.

In zonebestand:
- SOA-record hetzelfde (behalve serienummer)
- Verder enkel maar PTR records.
- Alle namen in bestand zijn relatief t.o.v. 16.168.192.in-addr.arpa
- Getallen in linkerkolom PTR records duiden op ip-adressen (relatief), namen rechterkant zijn absoluut.

B) *niet gevonden*