Computernetwerken 2: Netwerkbeheer

Bert De Saffel

10 mei 2017

Inhoudsopgave

Deel I

Theorie

Hoofdstuk 1

Beheer van TCP/IP-internetwerken

1.1 Configuratie van DNS

1.2 Multicasting

Multicasting is een manier om informatie te verzenden naar specifieke toestellen die geïnteresseerd zijn in deze informatie. Multicast adressen lopen vanaf 224.x.y.z tot 239.x.y.z. Dus een bron die informatie wil versturen zal één van deze adressen moeten innemen.

1.2.1 IGMP

Wanneer een toestel een multicast receiver wil worden, zal hij dit moeten melden aan de routers op zijn subnetwerk. Hiervoor wordt het **Internet Group Management Protocol** gebruikt. Dit protocol zal aan de multicast bron zeggen of er iemand aan het luisteren is of niet.

1.2.2 Optionele optimalisaties

1.2.3 Verkiezingsprocessen

Deel II

Labo's

Hoofdstuk 2

20/02/2017 - DNS Deel 1

Hoofdstuk 3

22/02/2017 - DNS Deel 2

Hoofdstuk 4

01/03/2017 - Statische Routing

Hoofdstuk 5

13/03/2017 - RIP en OSPF

5.1 Inleiding

In dit labo werden het RIP en OSPF protocol toegepast. De volgende problematieken werden aangepakt:

1. Is er een verschil tussen RIP op windows en RIP op Unix. Is het mogelijk dat een windows en een Unix toestel, geconfigureerd met RIP, kunnen communiceren met elkaar?
2. Kan een RIP router met een OSPF router communiceren?
3. Wat is het effect als er een connectie uitvalt, zowel bij RIP als bij OSPF?

5.2 RIP configuratie op Windows

Op windows kan RIP voornamelijk geconfigureerd worden met de grafische interface. De stappen om RIP te configureren gaan als volgt:

1. Voor elke interface moeten de metrieken op nul staan met het volgende commando: *netsh int ipv4 set int ethx met=0*.
2. Open *rrasmgmt.msc*.
3. Rechtermuisklik op de naam van de huidige computer.
4. Klik op *Configure and Enable Routing and Remoute Access*.
5. Kies voor een *Custom Configuration* en selecteer alleen LAN route.
6. IPV4 -¿ General -¿ New Routing Protocol -¿ RIP.
7. Interfaces ethx toevoegen.

5.3 RIP configuratie op Unix

De RIP configuratie op Unix gebeurt via de CLI.

1. Het toestel moet als router ingesteld worden: *sysctl -w net.ipv4.ip_forward=1*
2. Interfaces instellen: *ifconfig ethx 192.168.x.y/24 up* waarbij x het getal is van de interface en y het getal van het toestel zelf. Voorbeeld voor het toestel Bach:

```
ifconfig eth1 192.168.17.125/24 up
ifconfig eth2 192.168.4.125/24 up
ifconfig eth3 192.168.2.125/24 up
```

3. In de folder */etc/quagga* moeten er drie bestanden aangepast worden: *zebra.conf*, *ripd.conf* en *ospfd.conf*. In elk van deze bestanden komt hetzelfde stukje tekst

```
hostname pcnaam
password user           //normal password
enable password root    //root password
```

4. Herstarten van de daemons:

```
/etc/rc.d/init.d/zebra restart
/etc/rc.d/init.d/ripd restart
/etc/rc.d/init.d/ospfd restart
```

5. Het commando *telnet localhost ripd* op de volgende manier overlopen

```
enable
user
|configure terminal
|root
||router rip
|||network ethx
|||redistribute connected
|||redistribute kernel
|||redistribute static
|||write
|||q
||q
|show ip rip
|show ip rip status
```

5.4 OSPF configuratie op Unix

De OSPF configuratie voor een Unix toestel verloopt analoog als de RIP configuratie. Het enige verschil is de laatste stap. Hier wordt het commando *telnet localhost ospfd* overlopen op de volgende manier.

```
enable
 user
 |configure terminal
 |root
 ||router ospf
 |||redistribute connected
 |||redistribute kernel
 |||redistribute static
 |||net 192.168.168.x.0/24 area x
 |||write
 |||q
 ||q
 |show ip ospf interface
 |show ip ospf route
```

5.5 Scenario's

In het begin van het labo draaide iedereen onder RIP Unix. Nadat alles werkende was moest de ene helft overschakelen naar RIP onder Windows. Er kon vastgesteld worden dat communicatie tussen een Windows en Unix toestellen zonder problemen kan verlopen.

Hierna werden de toestellen aan de rand van de tafels ingesteld als een OSPF router die in area 1 zitten. Op dit moment zal geen enkele RIP router met een OSPF router kunnen communiceren. Om dit op te lossen moet er een border router aangemaakt worden die zowel RIP als OSPF draait. Deze ene router moet dan een extra commando ingeven in het *telnet localhost ospfd* of *telnet localhost ripd* programma. Deze lijn komt na het ingeven van *router rip* of *router ospf*. De extra lijn die ingegeven moet worden is: *redistribute ip*. Op dit moment kunnen RIP routers met OSPF routers communiceren via deze border router.

De volgende stap is om alle overige RIP routers in te stellen als OSPF routers. Deze routers zullen in area 2 komen. Nadat dit gebeurd is kan er vastgesteld worden dat communicatie tussen area 1 and area 2 routers niet meer mogelijk is. Dit komt omdat er nog geen area 0 is die deze verbindt. Deze area kan perfect functioneren met slechts één router, maar dit mogen er ook meer zijn.

In het geval dat er een connectie uitvalt bij RIP zal het $\pm$ 2 minuten duren vooraleer er opnieuw een stabiel netwerk is. De maximum metriek bij RIP bedraagt ook maar 15. In het geval dat een bepaalde metriek hoger is dan 15 zal de routetabel dus niet correct ingevuld worden.

Hoofdstuk 6

15/03/2017 - Switches

6.1 Inleiding

In dit labo werden er verschillende toestellen ingesteld als een switch. Het begint met kleine eilandjes met één switch en wordt uitgebreid totdat elk eiland aan elkaar verbonden is.

6.2 Unix toestel instellen als switch

Om een Unix toestel in te stellen als een switch wordt er gebruik gemaakt van het *brctl* programma. De volgende commandosequentie wordt gebruikt om een toestel in te stellen als switch.

1. ifconfig ethx 0.0.0.0 up
2. /usr/sbin/brctl addbr bridgenaam
3. /usr/sbin/brctl stp bridgenaam on
4. /usr/sbin/brctl addif bridgenaam ethx
5. ifconfig bridgenaam 0.0.0.0 up

6.3 Spanning Tree Protocol

Het SPT is een algoritme dat gebruikt wordt om lussen in een topologie te vermijden. Dit algoritme gaat als volgt in zijn werk:

1. Een root bridge wordt geselecteerd aan de hand van het kleinste MAC adres
2. Hierna wordt er voor elke poort een metriek berekent. De poort met de kleinste metriek wordt de designated poort genoemd. Deze poort zal nooit geblokkeerd worden.

3. Alle andere poorten zullen geblokkeerd worden

Om de uitvoer van dit protocol te gebruiken wordt het commando */usr/sbin/-brctl showstp bridgenaam* gebruikt. Dit geeft een overzicht per interface al dan niet hij geblokkeerd wordt of niet.

Hoofdstuk 7

22/03/2017 - Multicast routing

7.1 Inleiding

In dit labo werd er gedemonstreerd hoe multicasting in elkaar zit. De opstelling zit als volgt in elkaar: Elke tafel bestaat uit 3 toestellen, waarvan 1 hiervan een normaal windows toestel is, een ander een Unix switch is en tot slot een Unix router. Het windows toestel is verbonden aan de switch via eth2. De Unix router is verbonden aan de switch via eth3. Elke tafel heeft een nummer dat van 224 tot 239 loopt.

7.2 Verspreiden van video's

Om multicasting mogelijk te maken moeten er voor de drie toestellen configuratie gebeuren.

1. De router moet het volgende commando ingeven: *ifconfig eth3 192.168.x.x.* x is in dit geval het tafelnummer waartoe de router behoort.

2. De switch moet zichzelf nog eerst configureren als switch. Zie 6.2. Het enige verschil is het laatste ifcommando. In dit geval wordt het *ifconfig bridgenaam 192.168.x.1 up.* Het volgende commando moet ook ingegeven worden: *ip r r 0.0.0.0/0 via 192.168.x.x.*

3. Tot slot moet het windows toestel ook nog geconfigureerd worden.

In dit labo willen we video's verspreiden. De switch moet hiervoor vier instanties van vlc media player openen. Dit kan met het volgende commando *vlc &.* Voor elke instantie met het volgende gebeuren:

1. Klik op *Media*, dan op *Streaming.*

2. In het tabblad *Bestand* moet er slechts één .mov bestand toegevoegd worden.

3. Klik op het pijltje dat rechts van *Stream* staat, in de dropdown klik je op Stream.

4. De bron is al ingesteld, dus klik op volgende.

5. In de dropdown van File selecteer je UDP (legacy) en klik je daarna op toevoegen.

6. In het adres schrijf je x.0.0.y, waarbij x de tafelnummer is en het laatste getal 1, 2, 3 of 4 is afhankelijk van de instantie van vlc. De poort blijft ongewijzigd.

7. In dit geval mag de transcodering ook uitegschakeld worden, aangezien dit al in het video bestand zit.

8. Tot slot moet de TTL verandert worden in 20.

Op dit ogenblik kan het windows toestel op dezelfde tafel video's ontvangen die de switch aan het streamen is. Het Windows toestel opent vier instanties van vlc media player en klikt ook op *Media* en daarna op *Streaming*. Daarna klik je op het tabblad netwerk en in het veld typ je: *udp://@:x.0.0.y*. x is de tafelnummer waarop het Windows toestel zich bevindt, terwijl y 1, 2, 3 of 4 is. Op dit moment zal het Windows toestel de filmpjes afspelen die de switch aan het streamen is.

Om nu video's van andere tafels te bekijken moet de router die zich op elke tafel bevindt, een kabel leggen naar zijn buur. Dan maakt hij een statische routetabel op. Op dit moment kan elk Windows toestel video's bekijken van andere tafels.

De reden waarom we statische routing toegepast hebben is omdat we gebruik willen maken van de daemon *pimd*. Deze implementeerd een sparse protocol. Om deze daemon uit te voeren wordt het volgende commando gebruikt: */usr/local/sbin/pimd -d*. Om de uitvoer van deze daemon te bekijken gebruik je het commando *cat /proc/net/ip_mr_vif* en *cat /proc/net/ip_mr_cache*. Op dit moment zijn er verschillende Windows toestellen video's aan het bekijken van andere tafels. Dit kan worden afgeleid aan de output van deze twee bestanden.

Nu wordt de *pimd* daemon gestopt terwijl de Windows toestellen nog bezig zijn aan het kijken. Het spreekt vanzelf dat de video's zullen stoppen met spelen. Om een andere daemon te demonstreren moet eerst de statische routetabel vernietigd worden. De tweede daemon is */usr/local/xorp/sbin/xorp_rtmgr*. Deze daemon zal automatisch een routetabel maken. Na verloop van tijd zullen de video's die op de Windows toestellen aan het afspelen waren, terug afspelen.

Hoofdstuk 8

29/03/2017 - WLAN's

8.1 Inleiding

In dit labo hebben we verschillende routingprotocollen losgelaten op een WLAN.

8.2 Opvragen informatie WLAN op Windows

Vooraleer er informatie kan opgevraagt worden moet de wireless receiver aanstaan en een IP-adres hebben.

1. Open Network Connections → Rechtermuisklik op de wireless interface → Properties → Klik op Internet Protocol Version 4 → Properties → Use the following IP address
2. Open Network Connections → Rechtermuisklik op de wireless interface → Connect

Er zijn twee manieren om informatie op te vragen. De ene is oppervlakkig terwijl de tweede gedetailleerder is.

1. *netsh wlan show networks mode=bssid.* Dit toont de netwerken met hun accespoints warvoor een signaal kan ontvangen worden.
2. *netsh wlan show interface.* Dit toont de accespoint waarmee het toestel verbonden is

8.3 Opvragen informatie WLAN op Unix

Vooraleer de wireless interface kan opgestart worden moet er eerst een configuratiebestand bekeken worden, namelijk */etc/sysconfig/network-scripts/ifcfg-wlan0.* Dit bestand heeft standaard de volgende inhoud:

```
DEVICE=wlan0
BOOTPROTO=static
MODE=Managed
ESSID=tiwi
```

Als het commando *ifup wlan0* wordt ingegeven zal dit bestand uitgevoerd worden. Om nu te kijken ofdat het werkt kan eerst het commando *ifconfig wlan0* uitgevoerd worden. Om nu meer informatie te bekijken kan het commando *iwconfig wlan0* uitgevoerd worden. Hier staat er geen kanaal, maar wel de frequentie waarop hij luisterd. Hier kan het kanaal van afgeleid worden via volgende formule: $kanaalnummer = (freqentie - 2407)/5$. In het geval dat de frequentie 2422 is zal het kanaal nummer $(2422 - 2407)/5 = 15/5 = 3$ zijn. 2407 is het begin van de frequentieband en 5 is de stapnummer om naar de volgende afgebakende frequentiezone te gaan zodat er geen overlappingen zijn.

8.4 Ad Hoc modus

Tot nu toe werdt er automatisch een kanaal toegekend. Ad Hoc is een gedecentraliseerd systeem, dus wordt er geen gebruik gemaakt van routers. Elk toestel wordt gezien als een node in het netwerk, en zal data doorsturen en ontvangen van andere nodes. Om Ad Hoc modus aan te zetten moet het bestand *ifcfg-wlan0* aangepast worden met de volgende inhoud. In deze instantie stellen we ook zelf ons ESSID en CHANNEL in om te demonstreren wat er gebeurt als er overlappingen zijn op de frequentieband.

```
DEVICE=wlan0
BOOTPROTO=static
MODE=Ad-Hoc
CHANNEL=9          //Andere computers lopen van 1 tot 13
ESSID=negen
```

Als je naar toestellen met een CHANNEL die 5 stappen van uw eigen channel is, zal je merken dat het niet vlot verloopt en dat er zelfs berichten niet toekomen.

8.5 Netwerkanalyse met jperf

Er bestaat een grafische tool om het netwerk te bestuderen. Om deze tool te gebruiken moet er minstens één cliënt toestel en één server toestel de configuratie hebben uitgevoerd. Dit programma kan geopent wordt door eerst naar de folder */usr/local/jperf-2.0.2* te navigeren en daarna het commando *bash jperf.sh* uit te voeren.

In de grafische interface moet de **cliënt** de volgende zaken instellen:

- Het server adres invullen, dit is het adres van de toestel die de stappen voor de server zal uitvoeren.
- Transmit hoog genoeg zetten (10000+)

- Report interval op 3 zetten zodat er geen onnodige pieken tevoorschijn komen
- Run JPERF klikken

De **server** moet enkel het bolletje aanklikken bij server en daarna Run klikken. De cliënt zal op dit moment pakketten versturen en die worden visueel weergegeven voor zowel de cliënt als de server. Het is natuurlijk mogelijk om meerdere cliënts naar één server te laten communiceren.

8.5.1 memo

for x in 123.155; do ping -c 1 -w 1 192.168.123.$x — grep '0 received' ¿ /dev/null —— echo $x; done Alle Ip adressen pingen;

vi mesh sysctl -¡ net.ipv4.conf.wlan0.send_redirects=0 redirects uitschakelen
flushen: iptables -t mangle -F
ip r r 192.168.123.x/32 via 192.168.123.buur

8.6 Routingprotocollen voor Ad Hoc netwerken

Aangezien WLAN's meer dynamisch zijn dan normale netwerken zijn klassieke routingprotocollen zoals RIP en OSPF niet aan te raden. Voor WLAN's bestaan er twee soorten protocollen, **proactief** en **reactief**. Proactieve protocollen zullen de routetabel van alle routers op voorhand invullen. Reactieve protocollen zullen pas een route in de routetabel aanmaken op het moment dat deze nodig is. Na een tijd wordt die route terug verwijdert.

8.6.1 Proactieve aanpak

In principe hanteert OPSF een proactieve aanpak, maar deze is niet geoptimaliseerd voor WLAN's. Daarom werd er een alternatief ontwikkelt. Dit heet het **O**ptimized **L**ink **S**tate **R**outing Protocol. Elke router zal een aantal van zijn buren instellen als Multipoint Relay. Deze MR's zijn verantwoordelijk voor het forwarden van berichten. ORSL maakt ook gebruik van een multi-hop. Dit is om direct een buur over te slaan en naar één van zijn buren te gaan.

In Unix bestaat de *olsrd* daemon. Deze kan uitgevoerd worden met het commando */usr/sbin/olsrd*. Na verloop van tijd zal de routetabel aangevuld zijn en is netwerkverkeer mogelijk. Om de route te bekijken naar een bepaalde router kan het commando *ping -R x* gebruikt worden. De optie -R toont een lijst van alle routers dat het pakket voorbijgaat.

8.6.2 Reactieve aanpak

Een voorbeeld van een reactieve protocol is **O**n **D**emand **D**istance. De werking van dit protocol verloopt in twee stappen. In dit voorbeeld wil de router S data versturen naar de router D.

1. **Route Request bericht**
   Dit bericht bevat het adres van de router en een volgnummer. Dit volgnummer wordt met één verhoogd elke keer dit bericht bij een tussenligende router ontvangen wordt. Wanneer S laat weten dat hij naar D wil gaan, zal hij dit aan al zijn buren melden. De eerste keer dat de buren zo een request ontvangen zal deze buur dit bericht ook naar zijn buren doorsturen. Op dit moment weten de 2de niveau buren hoe ze naar S moeten gaan. Dit heet Reverse Pathing. Elke buur zal naar zijn buren dit bericht flooden. De nieuwe buren zullen dus ook weten langs welke router ze moeten gaan om tot S te komen. Op het moment dat de router D bereikt is, zullen eventueel andere routers nog verder flooden omdat zij niet weten dat D bereikt is.

2. **Route Reply bericht**
   Als D bereikt is, zal hij op zich een Route Reply bericht sturen naar S. Er is geen flooding meer nodig dankzij de Reverse Pathing techniek die een routetabel heeft gemaakt om naar S te gaan. Op dit moment wordt er weer aan Reverse Pathing gedaan om naar D te gaan zodat de volgende keer ook geen flooding meer nodig is. Pas nadat S het Route Reply bericht ontvangt kan er data verzonden worden naar D.

In Unix bestaat de daemon */usr/sbin/aodvd* die dit protocol implementeert. Als je dit protocol uitvoert, zal je routetabel leeg blijven totdat je data verstuurt naar een andere router. Echter als je de daemon terug sluit, kan je zien dat hij de routetabel niet volledig opkuist en is dus negatief. Ook bij het afsluiten van het Unix toestel slaagt het tilt.

Deel III

Modelvragen

Hoofdstuk 9

Reeks A

9.1 A1 - Configuratie van de netwerkinterface & multicasting op subnetwerkniveau

9.1.1 Vragen

1. Bespreek alle (ook meer recente) opdrachten, inclusief hun opties en output, die onder *Linux* voor de configuratie van de netwerkinterface kunnen gebruikt worden, zowel op de subnetwerklaag als op de internetlaag. Behandel eveneens eventuele configuratiebestanden (inclusief locatie en inhoud). Vergeet in het bijzonder de *opstartbestanden* niet.

2. Bespreek het equivalent onder Windows Server, zowel via de *Command Prompt*, als via de grafische interface.

3. Wat is de bedoeling van *multicasting op subnetwerkniveau*? Hoe wordt dit doel gerealiseerd?

4. Hoe weet een multicast bron of router dat hij verantwoordlijk is om multicast berichten af te leveren aan cliënts (*niet-routers*) op de diverse subnetwerken waarop hijzelf is aangesloten. Bespreek het protocol dat hierbij gehanteerd wordt, inclusief de bijkomende faciliteiten van meer recente versies ervan.

9.1.2 Antwoorden

1. - Commando **dmesg**.
   Dit commando wordt gebruikt om logberichten te raadplegen van de boot procedure. Hierin staan ook de netwerkinterfaces die geïnstalleerd zijn. Door *dmesg — grep eth* uit te voeren krijg je alles met betrekking tot de netwerkinterfaces. Deze informatie bevat het type, het hardwareadres (MAC), interrupt- en I/O poort bronnen.

- Commando **insmod** of **modprobe**
  Deze commando zal een driver eenmalig laden. Voorbeelden zijn: *insmod 3c90x.o* en *modprobe 3c90x.o*.
- Commando **install**
  Dit commando zal een driver permanent laden. Hierbij zijn er echter meer parameters vereist. Het totale commando kan er zo uitzien: *install -m 644 3c90x.o /lib/modules/'uname -r'/kernel/drivers/net*
  De optie -m is gelijkaardig aan chmod. 644 staat dus voor lezen en schrijven voor de eigenaar, en lezen voor de groep en anderen. Daarna volgt de naam van de driver *(3c90x.o)* en uiteindelijk de locatie waar de driver moet komen. Het uname commando zal met de optie -r het releasenummer van de kernel teruggeven zodat je die folder niet vanbuiten moet kennen.
- Commando **lsmod**
  Geeft een lijst van alle geïnstalleerde drivers. Dient als controle van de vorige 3 commando's.
- Commando **ifconfig**
  Staat voor **i**nter**f**ace **config**ure. Hiermee woren IP-addressen geconfigureerd alsook om de status van de netwerkinterfaces te bekijken. Om een enkele interface te bekijken gebruik je bv. het commando *ifconfig eth0*. Dit geeft informatie zoals het IP-adres, het broadcast adres voor het subnet waarop de interface zich bevindt, en het subnetmasker voor dat subnet. Verder toont het ook nog het hardwareadres van de interface. Dit commando kan ook gebruikt worden om na te gaan of een bepaalde interface wordt herkend door de kernel. In plaats van informatie zal er dan een foutboodschap gegeven worden dat de interface niet herkent wordt. *ifconfig* uitvoeren zonder parameters zal een lijst geven van alle interfaces die beschikbaar zijn, elk met hun eigen informatie. De *-a* parameter zal deze lijst uitbreiden met interfaces die niet actief zijn.
  Alhoewel *ifconfig* kan gebruikt worden om informatie van interfaces op te halen, is dit niet de primaire bedoeling. *ifconfig* wordt in de eerste plaats gebruikt om IP configuratie van netwerkkaarten in te stellen. Het *ifconfig*-commando wordt steeds vervolgd door de naam van de interface en daarna door vele opties, die bijna allemaal door een sleutelwoord beginnen, de gebruikelijke UNIX-conventie voor opties wordt hier dus niet gebruikt. Een lijst van de belangrijkste opties zijn:
  (a) het IP-adres in dotted-decimal notatie.
  (b) **up** of **down**. Zet een interface respectievelijk aan of uit. Bij *down* moet je nooit het IP-adres meegeven, bij *up* moet je dit wel doen als het de eerste keer is als je deze interface instelt.
  (c) ***netmask*** *aaa.bbb.ccc.ddd* stelt het subnetmasker in. Als deze optie niet wordt meegegeven zal Linux automatisch een subnetmasker kiezen dat past bij het IP-adres. Voor een klasse C

adres zal hij 255.255.255.0 kiezen, voor een klasse B adres zal hij 255.240.0.0 kiezen, en voor een klasse A adres zal hij 255.0.0.0 kiezen.

(d) ***broadcast*** *aaa.bbb.ccc.ddd* stelt het broadcastadres in. Ook als deze optie niet wordt meegegeven zal het besturingsyssteem zelf een adres kiezen afgeleid uit het IP-adres en de subnetmasker.

(e) **multicast** en **-multicast** zetten respectievelijk het ontvangen en versturen van multicast berichten aan of uit.

(f) **promise** en **-promise** zetten respectievelijk de promiscuous mode aan of uit.

(g) Voor point-to-point verbindingen gebruik je **pointtopoint** gevolgd door het ip-adres van de andere kant van de verbinding.

- Commando **netstat**
  netstat kan dienen als alternatief voor ifconfig als de optie -i meegegeven worden. *netstat -i* zal een lijst geven van alle interfaces. Om ook een lijst van niet actieve interfaces te tonen gebruik je ook de -a parameter. Op het einde van elke interface staan er een aantal vlaggen. Deze vlaggen, B, L, R en U stellen respectievelijk het broadcast-adres, loopback interface, running en up voor.
- Commando **ip addr** Nog een alternatief van *ifconfig* en *netstat*. Deze opdracht zal een lijst geven van alle interfaces, met hun MAC en IP adressen.
- Commando **ifrename** Dit command wordt gevolgd met de huidige naam van een interface en een nieuwe naam voor deze interface.
- Commando **ifdown**
  Dit commando wordt gevolgd door de naam van een interface en zal deze uitschakelen.
- Commando **ifup**
  Dit commando wordt gevolgd door de naam van een interface en zal deze opstarten.
- Folder **/proc/modules**
  Bevat alle geladen drivers
- Folder **/etc/sysconfig/network-scripts**
  Dit bevat configuratiebestanden die vooral gebruikt worden tijdens het opstarten van het toestel.
- Bestand **/etc/modprobe.d**
  Bestand met configuratieopties om te zeggen wat voor drivers dat elke interface moet laden.

2. - Grafisch
     - Naam wijzigen van een interface
       Open de map *Network Connections* → Rechtermuisklik op de interface en vervolgens *rename*.

  - Controloren en wijzigen van hardware en software van een interface
    Open de map *Network Connections* → Rechtermuisklik op de interface → Properties → Configure → Kies één van de tabbladen *General*, *Advanced*, *Driver* of *Resources*.
  - Monitoren van het netwerkverkeer van de huidige sessie van een interface
    Open de map *Network Connections* → Rechtermuisklik op de interface → Status. Hier kan je statistieken zien zoals de duur van de sessie, het aantal pakketten dat verzonden en ontvangen zijn. Als het geen LAN is zie je ook compressie en gegevens met betrekking tot fouten.
  - Statuscontrole automatiseren
    Open de map *Network Connections* → Rechtermuisklik op de interface → Properties → Configure → Kruis het vakje *Show icon in taskbar when connected* aan. Hierdoor verschijnen er pictogrammen op de taakbalk.
  - Interface uitschakelen
    Open de map *Network Connections* → Rechtermuisklik op de interface → Disable
    OF
    Open de map *Network Connections* → Rechtermuisklik op de interface → Status → Disable
  - Instellen IP-adres en subnetmasker
    Open de map *Network Connections* → Rechtermuisklik op de interface → Properties → Dubbelklik op Internet protocol version 4 (TCP/IP) → Klik op *Use t he following IP address* → Vul het IP-adres en het subnetmasker in

- Command prompt
  - Monitoren van het netwerkverkeer van de huidige sessie van een interface
    Gebruik het **netstat** commando om informatie te verkrijgen gelijkaardig aan het grafische *Status*. Als je de optie *-e* meegeeft krijg je informatie met betrekking tot de ethernet. De optie *-s* geeft ook de statistieken voor elk van de TCP, UDP, ICMP en IP protocollen. Als je in plaats van *-s* een *-p* als optie geeft, dan kan je kiezen door een protocolnaam erachter te zetten zoals: *netstat -ep UDP*.
  - Opvragen van de TCP/IP-netwerkconfiguratie
    Het commando **ipconfig /all** wordt gebruikt om allerlei gegevens te tonen gerelateerd met het TCP/IP netwerk.
  - Instellen IP-adres en subnetmasker Het **netsh** commando kan voor vele zaken gebruikt worden. Om een IP-adres en subnetmasker van een interface te wijzigen: *netsh interface ip set address "Local Area Connection"static 193.190.170.3 255.255.255.192*

3. ?

4. Het protocol dat gebruikt wordt om communicatie tussen bronnen en ontvangers te realiseren is het Internet Group Management Protocol. Dit protocol wordt gebruikt om individuele hosts aan een multicast groep toe te voegen. Hosts identificeren computers die interesse hebben, door deze IGMP berichten naar hun lokale multicast router te laten sturen. Routers luisteren dus naar IGMP berichten en zenden periodiek berichten uit om te ontdekken welke groepen er actief of inactief zijn op een specifiek subnetwerk. Dit protocol kent drie versies:

   (a) IGMPv1
   Stuurt report berichten naar het groepadres dat bereikt moet worden. Als een host de groep wil verlaten kan hij dit op elk moment doen. Als een router na een tijd geen report berichten meer ontvangt, zal hij stoppen met te forwarden naar dit groepadres.

   (b) IGMPv2
   Stuurt ook report berichten naar het groepadres dat bereikt moet worden, maar als een host niet meer geïnteresseerd is in een groep moet hij een Leave-Group bericht sturen. De router gaat na of er nog hosts in die groep geïnteresseerd zijn. Zoniet dan stopt de router met forwarden naar dit groepadres. Dit reduceert het netwerkverkeer aangezien er sneller gestopt zal worden met forwarding.

   (c) IGMPv3 Hier kan er ook nog aangegeven worden of men pakketten wil ontvangen of filteren van specifieke adressen.

   Om nu te weten of dat een router verantwoordelijk is om multicast berichten af te leveren worden er Query berichten verstuurd naar het multicast adres 244.0.0.1 met een time to live waarde van 1. Als er meerdere routers op een subnetwerk zijn wordt de router met het kleinste IP-adres geselecteerd.

9.2 A2 - Routing

9.2.1 Vragen

1. Bespreek het *doel* van routing, de *werking*, en de belangrijkste *componenten* ervan. Behandel de *terminologie* en *problematiek* die het routing proces kenmerkt.

2. Geef de diverse (inclusief de meest eenvoudige) alternatieven om de *routingtabel van niet-routers* (o.a. toestellen die slechts op één subnetwerk zijn aangesloten) te configureren. Indien er hiertoe op Linux of Windows bijzondere componenten moeten geïnstalleerd of geconfigureerd worden, bespreek hoe dit moet gebeuren.

3. Vergelijk de *voor- en nadelen* van *statische* en *dynamische* routing, zonder in detail in te gaan op specifieke routingprotocollen.

4. Maak een *classificatie* van *routingprotocollen*, volgens twee criteria. Omschrijf de terminologie die je hierbij invoert. Geef ondermeer aan op welk niveau hetzelfde routingprotocol actief kan zijn, en hoe aan schaalbeperking kan worden gedaan. Geef van elke klasse de meest courante *vertegenwoordigers*. Het is niet de bedoeling in te gaan op een gedetailleerde vergelijking tussen de verschillende klassen en hun specifieke vertegenwoordigers.

9.2.2 Antwoorden

1. Het doel van routing is om verschillende subnetwerken aan elkaar te hangen, zodat het lijkt dat ze op één en hetzelfde internetwerk zitten, ook al zijn ze fysiek aangesloten op subnetwerken die van verscheidene technologieën gebruik maken. Het is de taak van een router om ervoor te zorgen dat een bericht naar het juiste subnetwerk verzonden wordt. Voor berichten te versturen in hetzelfde subnetwerk is er geen router nodig. Als een router een bericht krijgt heeft hij twee mogelijkheden. De eerste mogelijkheid komt voor in het geval dat de ontvanger in hetzelfde subnetwerk zit. De router zal dan onmiddelijk dit bericht afleveren aan de ontvanger. De tweede mogelijkheid komt voor wanneer de ontvanger niet in het subnetwerk van de router zit. Dan zal de router dit bericht doorsturen naar een andere router. Het proces van berichten door te sturen naar andere routers heet routing.

   Vooraleer een router naar een andere router kan doorsturen moet de router een routetabel hebben. Dit is een lijst die voor elk netwerk in het internetwerk waarvan de router zelf geen deel uitmaakt, aangeeft naar welke volgende router hij het bericht moet versturen. Per regel in de routingtabel staat er het netwerkadres, forwarding adres, de interface, metriek en de lifetime. Het netwerkadres moet uniek zijn voor elk toestel op het internetwerk en duidt een specifiek toestel aan. Het forwarding adres is

het adres van de router. De interface bepaalt welke interface de router moet gebruiken. De metriek is een getal dat de kost aanduidt om tot het netwerkadres te komen. Voor de metriek wordt vaak de hop afstand gebruikt. Dit is een getal dat aanduidt hoeveel routers er overbrugt moeten worden om tot een eindbestemming te komen. Het lifetime veld houdt de tijd bij hoelang de route als geldig beschouwd kan worden.

Om nu te weten naar welke route en via welke interface berichten moeten doorgestuurd worden, wordt er een mechanisme gebruikt.

- De router moet op zoek gaan naar alle regels in de routingtabel waar het IP-adres van de bestemming deel uitmaakt van het netwerkadres. Dit gebeurt door bits van het IP-adres en het netwerkadres te vergelijken over de prefixlengte.
- De meest specifieke van het bovenstaande resultaat wordt gekozen.
- In het geval er meerdere gekozen zijn, wordt de regel met de kleinste metriek genomen.
- Als er geen regel gekozen werd, zal een ICMP-Destination Unreachable bericht verstuurd worden naar de afzender.

Het routingproces kent twee problematieken:

(a) Routing loops komt voor wanneer een routingtabel voor een bepaalde eindbestemming een pad construuert dat terugverwijst naar één van de intermediaire routers. De berichten zullen dus in een lus blijven circuleren totdat de levensduur verstreken is. Het bericht zal nooit aangekomen zijn.

(b) Black holes komen voor wanneer een router niet meer functioneert. De aanpassingen in de routetabel gebeuren niet onmiddelijk waardoor het versturen van het bericht kan vastlopen.

2. De simpelste manier is om een default gateway in te stellen. Alle berichten zullen aan deze router worden overgedragen en de router zal dan in zijn routetabel kijken en verder versturen. Dit vereenvoudigt de configuratie van niet-routers aanzienlijk. Dit is niet optimaal in het geval er subnetwerken bestaan die meerdere routers hebben, want dan wordt niet altijd het optimale pad gekozen. Om dit op te lossen wordt er aan host routing gedaan. Dit geeft de mogelijkheid om een intermediaire router in te stellen afhankelijk ofdat het sneller zou zijn of niet. Je kan ook statisch de juiste default gateway instellen.

   Er bestaan ook een aantal technieken die deze routetabellen dynamisch kunnen invullen. Het eerste mechanisme is route discovery met ICMP. Er wordt gebruik gemaakt van twee ICMP-berichten: ICMP-Router Sollicitation en ICMP-Router Advertisement. Sollicitation berichten worden naar het multicastadres 244.0.0.2 verzonden om de routers in het internetwerk te ontdekken. Routers die hiervoor geconfigureerd waren sturen een

Advertisement bericht als reactie. Dit gebeurt periodiek om te laten weten dat de router nog steeds beschikbaar is. Route discovery met ICMP is standaard ingeschakeld op Windows toestellen. Als Routing and Remote Access Service ingeschakeld is zal het echter geen Advertisement berichten versturen.

De tweede techniek maakt gebruik van ICMP-redirect berichten. Als een router merkt dat het verkeer afkomstig is van een computer die de volgende hop rechtstreeks kon bereiken zal de router een ICMP-redirect bericht terugsturen naar de afzender. De afzender kan dan zijn routetabel aapassen. Deze techniek wordt afgeraden om te gebruiken aangezien het onmogelijk is om de authenticiteit van deze berichten te verifiëren. De informatie in een IP-datagram kunnen zeer eenvoudig vervalst worden. Windows en Linux houden rekening met een ICMP-redirect bericht, maar voegen enkele routes naar individuele toestellen toe. De lifetime van zo een route is ook beperkt tot enkele minuten.

De derde techniek is door berichten tussen routers op een subnetwerk te broadcasten. Hierdoor kunnen andere toestellen passief luisteren naar deze berichten. Niet-routers kunnen over dezelfde informatie beschikken als de routers. Dit proces heet eavesdropping. Als RIP wordt gebruikt wordt dit Silent RIP genoemd en wordt enkel toegepast op niet-routers. Op Linux kan Silent RIP geactiveerd worden met routed -q. Op windows toestellen moet de service RIP Listener geïnstalleerd worden. Om dit de installeren moet je volgende stappen ondernemen:

(a) Add/Remove Programs

(b) Networking Services

(c) Rip Listener aanzetten

Zowel Linux als Windows luisteren alleen naar RIPv1 berichten.

3. - Statische routing betekent dat de netwerkbeheerder zelf alle routingtabellen voor elke router zal invullen. Hier zijn heel wat nadelen aan verbonden. Het neemt veel tijd in beslag om voor elke router een routetabel op te stellen en is het bovendien zeer foutgevoelig. In het geval dat er een topologiewijziging plaatsvindt moeten alle routetabellen opnieuw ingesteld worden. Als dit nit gebeurt kunnen routing loops en black holes voorkomen. Het voordeel is dat het sneller is als het internetwerk een zeer beperkt aantal routers en subnetwerken heeft, en ook wanneer de topologie nauwelijks verandert.
   - Dynamische routing betekent dat routers met elkaar zullen communiceren door middel van routingprotocollen. Alle routers melden aan andere routers met welke netwerken zij verbonden zijn en welke zij onrechtstreeks kunnen bereiken. Elke router zal zijn routingtabel dus zelf aanmaken. Het voordeel is dat de routetabel aangepast wordt, ook in geval van topologiewijzigingen. Als een router uitvalt zullen

andere routers berichten naar elkaar versturen om een nieuwe routingtabel op te stellen. Als de router terug aanstaat, kan er terug naar de oorspronkelijke situatie gegaan worden, eveneens door het uitwisselen van berichten. Dit heet route flapping. Het nadeel van dynamische routing is het extra netwerkverkeer door het constant uitwisselen van berichten.

4. Routingprotocollen kunnen geclassificeerd worden op basis van methode en de technologie.

   - Methode
     Er wordt een onderscheid gemaakt tussen interior en exterior gateway protocollen. Interior gateway protocollen worden ingezet om de routingtabellen binnen een autonoom systeem in te vullen. Een IGP heeft als doel de beste route te berekenen naar om het even welke eindbestemming en het verspreiden van deze informatie naar elke router op het autonoom systeem. Vertegenwoordigers van deze methode zijn RIP, EIGRP, OSPF en IS-IS. EGPs dienen dan om routing informatie uit te wisselen tussen autonome systemen, meer bepaald enkel de border router van het autonoom systeem. Een EGP moet met meer factoren rekening houden zoals overeenkomsten tussen verschillende internet service providers. Vertegenwoordigers van deze methode zijn EGP, GGP en BGPv4.
   - Technologie
     Er wordt een onderscheid gemaakt tussen twee klassen. De eerste is distance vector. Deze techniek zorgt ervoor dat een router enkel zijn buren zal informeren over topologische veranderingen. Vertegenwoordigers van deze technologie zijn RIP en EIGRP. De tweede klasse is link state. Hier zal elke router een lijst hebben van elle connecties in het netwerk en berekent de beste naar elke mogelijke bestemming. De verzameling van de beste paden worden dan opgesteld in de routetabel. Vertegenwoordigers van deze technologie zijn OSPF en IS-IS.

9.3 A3 - RIP

9.3.1 Vragen

1. Geef een gedetailleerde beschrijving van de *werking* van RIP. Bespreek de *mogelijkheden*, *beperkingen* en *problemen*. Bespreek in het bijzonder de gehanteerde metriek, en hoe RIP berichten verpakt worden (cfr. het OSI 7-lagen model).

2. Wat wordt er bedoeld met *reductie van de convergentieperiode* (inclusief oorzaken) ? Bespreek de verschillende technieken om dit te verwezenlijken.

3. Bespreek de verschillende verbeteringen van RIPv2 ten opzichte van RIPV1.

9.3.2 Antwoorden

1. Een RIP router zal periodiek alle route vectoren van zijn routingtabel naar alle routers die hij op subnetwerk-niveau rechtstreeks kan bereiken. Dit wordt een advertisement genoemd en elke router zal zijn routetabel aanvullen met de informatie die in deze advertisement staat. Uiteindelijk heeft elke routers informatie over het hele internetwerk. Het verzenden van zo een advertisement is niet gesynchroniseerd met andere routers. Elke router zal op zijn eigen tijdstip een advertisement verzenden. Een router zal nooit bevestigen of hij zo een advertisement heeft ontvangen of juist niet. Deze berichten zijn dan ook slechts ingekapseld in UDP segmenten met poortnummers 520, zowel voor het zender als voor het ontvanger veld.

   Voor de metriek wordt er standaard de hop afstand gebruikt. Dit wil zeggen dat als een router een advertisement ontvangt, dat hij de metriek van de ontvangen routers verhoogt met 1 en pas daarna zal hij deze informatie opnemen in zijn routingtabel, met de aangepaste metriek. Als de metriek groter dan 16 bedraagt zal RIP dit aanschouwen als onbereikbaar. Het is daarom ook niet interessant om iets anders te nemen als metriek. De maximum diameter van een internetwerk bedraagt dan ook 15 op voorwaarde dat de hop afstand als metriek gebruikt wordt. In het geval dat een eindbestemming langs meerdere paden kan bereikt worden, zou via de RIP standaarden elk pad moeten opgenomen worden in de routetabel, maar dit zou veel te grote routetabellen opleveren en daarom houden de meeste implementaties alleen de kleinste metriek over. Grote routetabellen hebben immers impact op het RIP verkeer aangezien elk RIP bericht ten hoogste 25 routes kan adverteren.

   RIP berichten worden niet gericht naar specifieke buren, maar gebroadcast. Deze broadcast wordt elke 30 seconden uitgevoerd ook al is internetwerk in een stabiele configuratie. Dit zort voor een trage convergentieperiode. Aan de basis van dit probleem liggen drie principes. Zoals vermeld houden de meeste RIP implementaties de kleinste metriek bij in het geval er meerdere paden naar een eindbestemming zijn. Advertisements waarin

een pad een hogere metriek heeft zal worden genegeerd, maar de metriek van de beste route wordt wel verhoogd. Het tweede probleem is de lifetime parameter. Dit is een parameter die bepaalt hoelang de levensduur is van RIP aangeleerde routes. Standaard bedraagt deze drie minuten. Tot slot is het uitwisselingsproces niet synchroon tussen de verschillende routers. Hierdoor wordt het eindresultaat beïnvloed van de volgorde van verzending.

Aangezien er een trage convergentieperiode is door deze drie principes ontstaan er twee problemen. Het eerste probleem is het count-to-infinity probleem. Dit komt voor als een router, die merkt dat een verbinding onbeschikbaar TODOTODO

2. De reductie van de convergentieperiode betekent het verkleinen van de tijd om bij wijzigingen in het internetwerk, opnieuw tot een stabiele toestan te komen. Oorzaken zie vorige vraag.

   Om dit op te lossen bestaan er vier technieken. Bij het kiezen van een techniek wordt die best toegepast op alle routers van het internetwerk voor de beste kans op slagen.

   (a) **split horizon**
   Routers zullen niet meer routes adverteren op het subnetwerk waarlangs ze deze routers vernomen hebben. Dit vermijdt het count-to-infinity en het routing-loop probleem. Beschermt niet tegen alle vormen van lussen, maar reduceerd wel de kans en bovendien wordt de belasting van het RIP protocol op het netwerk beperkt.

   (b) **poison reverse**
   Dit is een variant van de split horizon techniek. Deze blijft wel adverteren naar alle subnetwerken, maar vermeldt de routers op het subnetwerk langs waar ze de routes vernomen hebben met een metriek van 16. Hierdoor is poison reverse beter dan split horizon om count-to-infinity te voorkomen, maar heeft niet hetzelfde gunstig effect op de netwerkbelasting.

   (c) **triggered updates**
   Routers die deze techniek ondersteunen zullen ook adverteren wanneer er een metriek van een route wijzigt. De router zal alleen de wijziging adverteren en niet de volledige routetabel. Als de lifetime parameter 0 is, wordt deze route bijna onmiddelijk met een metriek van 16 gebroadcast. Dit verkleint ook weer de kans op het count-to-infinity probleem. Deze techniek zorgt voor een aanzienlijke vermindering in de convergentieperiode, maar er wordt aanzienlijk meer broadcast-berichten verstuurd, wat in sommige netwerken niet aanvaardbaar is.

   (d) **general RIP request**
   Bij het opstarten van een router kan hij een general RIP request broadcasten. Andere routers die dit ondersteunen kunnen hierop

antwoorden met hun volledige routetabel. Dit vermijdt dat een router 30 seconden moet wachten vooraleer hij een advertisement ontvangt.

3. RIPv2 kent vier verbeteringen ten opzichte van RIPv1.

   (a) RIPv1 berichten worden gebroadcast. Elk toestel op een internetwerk zal deze RIP berichten dus ontvangen, ook de niet-routers. Dit zorgt dus voor veel onnodige broadcastverkeer. RIPv2 biedt de mogelijkheid om de advertisements te richten naar het multicast adres 244.0.0.9

   (b) RIPv1 houdt geen rekening met subnetmaskers aangezien in die tijd gebruikt werd gemaakt van zelfidentificerende adressen van klasse A, B en C. Tegenwoordig zorgt dit voor problemen om routers naar subnetten op te nemen. RIPv2 neemt expliciet het subnetmasker op.

   (c) RIPv2 maakt gebruikt van het *next hop* veld om het adres van de eerstevolgende hop aan te duiden. Op deze manier kunnen routers bij ontvangst van een route-vector eerst kijken of de hop niet rechtstreeks te bereiken is en worden dubbele hops vermeden. Verder laat het ook toe om routers die op een andere routing domein zit te refereren.

   (d) RIPv1 heeft geen beveiliging om de correctheid van een bericht te controleren. Alle UDP berichten die verzonden worden via poort 520, worden als geldig aanschouwd. Dit laat toe om berichten te versturen via poort 520 die foutieve informatie bevatten. RIPv2 ondersteunt eenvoudige authentificatie met wachtwoorden alsook MD5.

9.4 A4 - OSPF

9.4.1 Vragen

1. Geef een gedetailleerde beschrijving van de *werking van OSPF*, inclusief de diverse mechanismen van berichtenuitwisseling en de OSPF routers met een bijzondere functie, maar zonder in te gaan op de uitwerking van het *algoritme van Dijkstra* en het concept van *OSPF* area's.

2. Beschrijf, o.a. aan de hand van een figuur, wat er precies gebeurt indien er een nieuwe router in een door OSPF gestuurd internetwerk wordt opgenomen.

3. Hoe worden OSPF berichten verpakt (cfr. het OSI 7-lagen model)?

9.4.2 Antwoorden

1. Alle routers verzamelen Link State Advertisements en compileren die in een Link State Database. Doordat elke LSA een timestamp (lolly nummer) heeft kan een router weten ofdat het om nieuwe of oude informatie gaat. Elke LSA refereereert naar één router met info van de subnetwerken waarop hij aangesloten is, en een metriek die de kost weergeeft. Een LSDB bevat en volledige inventaris van alle routers en van alle subnetwerken waarop deze een aansluiting hebben. Vooraleer er netwerkverkeer mogelijk is moeten deze LSDB gesynchroniseerd zijn met alle routers en vooraleer dat er gesynchroniseerd kan worden moeten een router alle LSAs ontvangen hebben van alle andere routers op het internetwerk.

   De synchronisatie verloopt efficiënt en vraagt weinig tijd. Het is niet de bedoeling dat een router met alle andere routers op het internetwerk moet controleren ofdat hun LSDB gesynchroniseerd is. Er worden groepen van naburige routers samengesteld, zo een eenheid noemt een adjacancy. Een adjacancy wordt gevormd wanneer een een groep routers dezelfde LSDB hebben. Initieël moet een router dus vergelijken met zijn buren die hij rechtstreeks op zijn interface kan bereiken. Adjacencies worden dus dynamisch gevormd. Tijdens de initialisatie van een OSPF Router stuurt hij een hello bericht om andere routers op de hoogte te brengen van zijn bestaan. Een hello bericht bevat de router ID van de verzender, alsook de router IDs van de naburige routers waarvan hij zelf reeds een hello bericht heeft ontvangen. Initieël bevat zo een hello bericht alleen het ID van de router. Tijdens het verzenden van hello berichten zal dit bericht aangevuld worden met router IDs van nabije buren. Een OSPF router beschouwt de router IDs als rechtstreekse buren, ook al zijn ze dit niet.

   De volgende fase is het database exchange proces. Dit proces zal voor elk koppel routers van een te construeren adjacency een master/slave verhouding aannemen en wisselt hierna database description pakketten uit. In dit bericht staan de LSAs van een LSBD van een bepaalde router. Elke router

van het koppel vergelijkt aan de hand van deze pakketten de inhoud van zijn LSBD en van zijn partner. Als er blijkt dat er informatie veroudert is, moet de router een Link State Request aanvragen aan zijn partner. Zijn partner zal dan reageren met een Link State Update pakkeet. Wanneer alle koppels bevestigd hebben wordt uiteindelijk de adjacancy gevormd. Na dit proces blijven leden van een adjacancy hello pakketten versturen naar leden van deze adjacancy. Default is dit om de 10 seconden. Als er na 40 seconden geen hello pakket ontvangt, beschouwen de leden van de adjacency de router als uitgevallen.

Eens de synchronisatie verlopen is, kan de LSDB voor elke router gecompileerd worden en bekomt elke router een routingtabel. Deze routingtabel wordt opgesteld aan de hand van vier componenten

(a) Het kortste pad naar een eindbestemming wordt berekent via het algoritme van dijkstra

(b) Elke router kent het pad naar de eindbestemming aangezien ze de hele LSBD hebben

(c) Elke router berekent een Shortest Path Tree met zichzelf als root

(d) Hieruit berekent elke router zijn routingtabel.

Om het aantal adjacencies te beperken wordt er een Designated Router verkozen voor elk subnetwerk. Er worden dan enkel adjacencies gevormd tussen DRs. Alle routers die niet DR zijn hoeven geen adjacent te zijn, bij een wijzigiging moeten zij dit vermelden aan de DR via het multicast adres 224.0.0.6, die er dan voor zorgt dat de wijziging naar de andere routers moet doorsturen via het multicast adres 244.0.0.5. Het gebruik van dit mechanisme zorgt ervoor dat de netwerkbelasting linear toe en niet kwadratisch. Een DR is een eigenschap van de interface van de router en dus niet de router zelf. Het is mogelijk dat een router voor een aantal subnetwerken DR is en voor andere subnetwerken juist niet. Er is ook een Backup Designated Router voorzien, die gebruikt zal worden indien een DR uitvalt of verbinding verliest. Op die manier moeten er geen nieuwe adjacenies gemaakt worden. Een DR en een BDR worden verkozen tijdens de uitwisseling van hello pakketten. De keuze wordt uiteindelijk gemaakt op de router met de hoogste prioriteit. Als er routers zijn met dezelfde prioriteit wordt de router met de hoogste router ID verkozen als DR. Dit geldt hetzelfde voor een BDR maar met tweede hoogste prioriteit en router ID. Als een router prioriteit 0 heeft zal deze nooit verkozen worden tot DR.

2. Router 1 komt op het netwerk en wisselt hello-pakketen uit aan Router 2. Nadat ze op de hoogte zijn van elkaars bestaan vormen Rotuer 1 en Router 2 een adjacancy en wisselen ze Database Description pakketten uit. De DD pakketten van Router 1 bevat alleen de LSA van zichzelf en de pakketten van Router 2 bevat alle LSAs behalve van Router 1. Hierna vraagt Router 1 een Link State Request aan Router 2 om alle LSAs van de routers in het

internetwerk. Router 2 stuurt Link State Update pakketten naar Router 1 met deze informatie. Router 2 vraagt analoog aan Router 1 om zijn LSA. Op dit moment bevatten Router 1 en Router 2 een gesynchroniseerde LSDB. Op basis hiervan wordt er voor Router 1 en Router 2 een nieuwe routingtabel en een SPF tree berekent. Router 2 stuurt Link State Update pakketten naar alle routers waarmee hij een adjacancy vormt. Dit pakket bevat enkel de LSA van Router 1. Router 3 en 4 bevestigen na onvangst en kunnen ook een nieuwe routingtabel berekenen. Router 3 en 4 sturen op hun beurt ook een LSU pakkeet met de LSA van Router 1 naar Router 5 en 6. Router 5 en 6 berekenen dan ook een nieuwe routingtabel.

3. OSPF pakketten worden rechtstreeks verpakt in IP-datagrammen. Er wordt gewacht op een ontvangsbevestiging. Bij het tekortkomen van een antwoord zal dit geïnterpreteerd worden als het falen van een verbinding.

9.5 A5 - Multicastrouting

9.5.1 Vragen

1. Geef de basisprincipes van *multicastrouting*.
2. Omschrijf de twee fundamenteel verschillende manieren om deze basisprincipes te realiseren, inclusief hun relatieve voor- en nadelen.
3. Bespreek in detail de diverse facetten van het momenteel meest gebruikte *multicastroutingprotocol*.
4. Omschrijf de optionele technieken om de werking van dit protocol nog meer te optimaliseren.
5. Hoe kan men een *Linux* toestel als multicastrouter laten werken? Geef twee concrete voorbeelden. Geef aan hoe men de diverse *multicastverkeerstromen* kan opvolgen.
6. Sommige routers verzorgen in het multicastproces *bijzondere* rollen, die ze pas na specifieke *verkiezingsprocessen* toebedeeld krijgen. Geef een overzicht van deze bijzondere functies, en de overeenkomstige verkiezingsprocessen.

9.5.2 Antwoorden

1. Een multicast adres gebruikt gebruikt een klasse D IP-adres. Deze klasse heeft een bereik van 224.0.0.0 tot 239.255.255.255. Deze adressen hebben geen prefixlengte, deze is echter altijd /32. Een multicast bron is een toestel dat pakketten zal versturen naar een bepaald multicast adres. Toestellen die geïnteresseerd zijn zullen naar ditzelfde adres luisteren. Alle toestellen die naar hetzelfde adres luisteren worden ook een multicast groep genoemd.

   Aangezien er verschillende receivers zijn, kunnen de pakketten via meerdere wegen hun doel bereiken. De verzameling van al deze wegen wordt een distributieboom genoemd. Deze boom kan zowel opwaards als neerwaarts genavigeerd worden. Opwaards of 'upstream' navigatie gebeurt via een incoming interface, neerwaarts of 'downstream' navigatie gebeurt via een outgoing interface

   Routers houden een lijst bij van alle incoming en outgoing interfaces. Dit wordt het multicast forwarding state genoemd. Het aantal outgoing interfaces kan maximum gelijk zijn aan het aantal interfaces op de router. Zo een forward state van een router wordt bijgehouden in de koppels (S, G) en (*, G). S staat voor het IP-adres van de bron en G staat voor een specifiek multicast groep adres. Wanneer een een * staat in plaats van S, staat dit voor eender welke bron dat verzend naar G.

In multicast routing zal de router het pakket verzenden doorheen de distributieboom en weg van de bron om routing loops te vermijden en de afstand tussen de bron en de ontvanger zo klein mogelijk te houden. Dit mechanisme kan op twee manieren gebeuren.

De eerste mogelijkheid is door gebruik te maken van het Shortest Path Tree. Elke bron van een multicast groep is de root van hun eigen boom. Als een router ontdekt dat er een receiver, die rechtstreeks op zijn interface zit, geïnteresseerd is in een bepaalde groep, zullen deze twee bomen aan elkaar gekoppeld worden. Er wordt hier aan RPF gedaan om te achterhalen hoe er naar de bron moet gegaan worden. De router verstuurd een Join bericht via de RPF interface om de volgende router te laten weten dat hij pakketten wil ontvangen van een bepaalde groep met een bepaalde bron. Dit blijft gebeuren totdat de router bereikt wordt die direct aan de bron is verbonden, of een router bereikt werd die al aan het forwarden is voor deze bron en groep. De boom van de bron is nu uitgebreid en de geïnteresseerde receiver hoort hier nu bij. Het versturen van pakketten is nu mogelijk.

De twede mogelijkheid is het Rendezvouz Point Tree. Deze boomstructuur stelt één router aan als Rendevouz Point. Deze router kent alle adressen van elke multicastgroep. Al het verkeer zal door deze Rendevouz Point moeten doorstromen. Hier wordt er ook aan RPF gedaan.

2. - Dense protocols
   Een dense protocol gaat er van uit dat er veel receivers zijn op het domain en dat elk subnet minsten één receiver heeft voor elke multicast groep. Dit type van protocollen gebruiken het flood-and-prune model. Dit zal initieël het verkeer van multicast bronnen broadcasten naar routers. Als een router verkeer ontvangt van een groep op zijn interface die het dichtst bij zijn bron ligt zal hij dit doorsturen naar al zijn interfaces behalve de interface waarop hij het verkeer gekregen heeft. Bij het ontvangen van verkeer op een niet RPF interface, zal hij dit bericht discarden en een prune bericht sturen naar de upstream.

   Het beste voordeel van Dense protocollen is simpliciteit. Het laat toe om makkelijk een distributieboom te maken dat als top de multicast bron heeft. Een boom die op deze manier gegenereerd wordt garandeerd het kortste en efficiëntste pad van bron naar ontvanger.

   Een negatief punt is schaalbaarheid. Aangezien dat dense protocollen flooden over het hele network, is het niet toepasselijk om te gebruiken op aanzienlijk grote netwerken.

   - Sparse protocols
     Een sparse protocol gaat er van uit dat er maar een kleine hoeveelheid receivers, maar minstens één, aanwezig zijn voor elke multicast groep. Sparse protocols gaan een kernrouter aanduiden die alle actieve sources in een domein gaat tracken en zal daarom niet het hele netwerk

flooden zoals bij een dense protocol. Sparse protocollen volgen het explicit join model. Bij dit model zal multicast data maar geforward worden naar routers die dit opvragen. De distributieboom heeft als top de aangeduide kernrouter. Als een host een groep wilt joinen, dan gaan de rechtstreekse verbonden routers de distributieboom joinen richting de kernrouter. Verkeer wordt ontvangen door deze kernrouter over de Shortest Path Tree en geforwaard naar geïnteresseerde ontvangers via de kernrouter.

Voordelen van dit soort protocollen is dat er geen flooding noodzakelijk is en dat er geen forwarding states moeten bijgehouden worden in routers die niet de kernrouter zijn. De kernrouter is de enige router die op de hoogte moet zijn van alle actieve bronnen.

Het nadeel is dat het niet altijd het kortste pad zal nemen. Multicast data moet eerst door de kernrouter gaan, ook al is de ontvanger dichter bij de bron dan de kernrouter.

3. Het meest gebruikte multicastroutingprotocol is Protocol Independent Multicast-Sparse Mode. Dit protocol verloopt in drie stappen.

   (a) De eerste stap is het opbouwen van de Rendevouz Point Tree.

4. Optimalisatie enz

5. Er bestaan twee verschillende daemons op Linux. De eerste is pimd. Deze daemon kan uitgevoerd worden met het commando /usr/local/sbin/pimd -d. pimd vereist echter wel dat er al een routetabel aanwezig is. De tweede variant is xorp_rtmgr en kan uitgevoerd worden met /usr/local/xorp/sbin/xorp_rtmgr. In tegenstelling tot pimd zal xorp_rtmgr zelf een routetabel aanmaken. Om het multicast verkeer te bekijken gebruiken we iperf. Om dit programma te kunnen gebruiken zijn er twee toestellen nodig. Een server toestel en een cliënt toestel. De server moet alleen aanduiden dat hij als server zal draaien. De cliënt moet het IP-adres van de server ingeven en de TTL waarde verhogen. Als beide toestellen op Run klikken zal er verkeer gegenereerd worden en kan deze bekeken worden op

6. Er bestaan drie verkiezingsprocessen.

   (a) Het eerste verkiezingsproces is gelijkaardig aan OSPF. Er wordt een Designated Router bron verkozen per subnetwerk en gebeurt via hello berichten. Hello berichten worden verstuurt naar het multicastadres 224.0.0.13. De router met de hoogste DR priority wordt geselecteerd als DR. Als alle routers geen DR priority functionaliteit hebben wordt de router met het hoogste IP adres gekozen. Elke router zal dus zelf de Designated Router selecteren aan de hand van deze informatie. Dit vormt geen probleem als alle routers hetzelfde algoritme gebruiken om de DR te selecteren. De taak van de DR is om het PIM-join bericht door te sturen van de receiver naar het Rendevouz Point en om data te forwarden naar de receivers.

(b) Het tweede verkiezingsproces is het selecteren van de active querier. De router wordt geselecteerd aan de hand van het kleinste ip adres. De active querier is verantwoordelijk voor het verzenden van IGMP-group berichten en om de status bij te houden van elke actieve multicast groep.

(c) Het derde verkiezingsproces is een Rendevouz Point verkiezen in functie van een multicastgroep.

Hoofdstuk 10

Reeks B

10.1 B1 - Draadloze netwerken

10.1.1 Vragen

1. Met welke opdrachten kan men op *Windows* toestellen nagaan welke de karakteristieken zijn van de eigen *Wifi* interface en van de *Wifi* zenders in de buurt. Geef aan welke karakteristieken vermeld worden.

2. In welk opzicht zijn *Ad Hoc routingprotocollen* (in *wireless meshes*) anders dan de meer traditionele routingprotocollen (bedoeld voor internetwerken die uit bekabelde subnetwerken bestaan)?

3. Geef de twee fundamenteel verschillende manieren om *Ad Hoc routingprotocollen* te realiseren, inclusief hun relatieve voor- en nadelen en hun optimaal toepassingsgebied.

4. Bespreek een concreet voorbeeld van een implementatie die tot één van deze categorieën behoort, met vooral aandacht voor de verschillen met het traditionele routingprotocol (voor bekabelde internetwerken), waarvan het is afgeleid.

5. Bespreek een concreet voorbeeld van een implementatie die tot de andere categorie behoort, nu met een gedetailleerde beschrijving van hoe de routingtabellen door specifieke berichtuitwisselingen ingevuld worden.

10.1.2 Antwoorden

1. Om alle netwerken met hun accespoints te tonen wordt het commando **netsh wlan show networks mode=bssid** gebruikt. Met dit commando wordt een lijst verkregen van alle netwerken met hun accespoints. Per accespoints kan ook de signaalsterkte en het kanaal gevonden worden. Om de accespoint te bekijken waarmee een toestel verbonden is gebruik

je **netsh wlan show interface**. Ook hier wordt de signaalsterkte en het kanaal getoond. Bijkomende informatie zoals upload- en downloadrate zijn ook aanwezig.

2. Ad Hoc modus is een gedecentraliseerd systeem waarbij er geen routers aanwezig zijn. Elk toestel wordt gezien als een node in het netwerk, en zal data doorsturen en ontvangen van andere nodes. WLANS zijn te variabel aangezien toestellen op elk moment verbonden kunnen zijn met het internetwerk. Traditionele routingprotocollen zijn hier niet op voorbereid en hebben daarom geen nut in een WLAN.

3. Er bestaan twee soorten Ad Hoc routing protocollen: proactief en reactief.

   - Proactief
     Een proactief protocol zal voor elke potentiële router een route maken in de routetabel. Deze routetabel wordt dan verdeeld over het hele netwerk. Het nadeel hiervan is dat het een nieuwe routetabel moet opstellen als er een topologische wijziging plaatsvindt. Het voordeel is dat er snel een connectie kan vastgelegd worden.
   - Reactief
     Een reactief protocol daarentegen zal pas een route aanmaken op het moment dat dit nodig is. Na een tijd zal deze route terug verwijdert worden. Als een toestel een pakket wil versturen naar ander toestel dat zich niet op hetzelfde subnetwerk bevindt, moet hij dit via zijn gateway versturen. Deze router zal dit dan doorspelen naar alle directe buren. Die buren zullen op hun beurt dit ook melden aan hun directe buren. Dit wordt gedaan totdat het doeladres bereikt is. Let wel op dat andere routers niet weten wanneer het doeladres bereikt is, en zullen verder flooden tot het niet meer mogelijk is. Het nadeel is hier dus dat het soms lang kan duren eens een pakket verstuurd kan worden.

4. Het protocol dat hier zal besproken worden heet het Optimized Link State Routing Protocol. Dit is een proactief protocol en werd geïnspireerd door OSPF. In principepe is OSPF ook een proactief protocol, maar is niet geschikt voor WLANs aangezien OSPF werkt met adjacencies. In WLANs treden overlapping vaak voor. OLSR zorgt ervoor dat elke router een aantal van zijn buren instelt als Multipoint Relay. Deze MR's zijn verantwoordelijk voor het forwarden van berichten zoals designated routers verantwoordelijk zijn in OSPF. Dit zorgt voor selectieve flooding

5. Het protocol dat hier zal besproken worden heet het On Demand Distance Protocol en is een voorbeeld van een reactief protocol. Dit protocol werkt in twee fasen. Fase 1 is het versturen van een Route Request bericht. Dit bericht bevat het adres van het toestel dat je wil bereiken en een volgnummer. Dit volgnummer wordt met 1 verhoogd per request aan een router. De bron stuurt naar de router waarmee hij verbonden is dat hij een

bericht wil versturen naar een bepaald doeladres. De router zal dit melden aan alle directe buren. Als het de eerste keer is dat deze request verstuurd wordt zal elke buur deze request doorsturen naar hun directe buren. Op dit moment weten deze buren hoe zij naar S moeten gaan, namelijk via de router waarvan ze de request ontvangen hebben. Dit proces heet reverse pathing en wordt zolang toegepast totdat het doeladres bereikt is. Alleen het doeladres zal weten dat hij bereikt is. De andere routers zullen blijven flooden. De tweede fase is het Route Reply bericht van het doeladres terugsturen naar de bron. Er is geen flooding meer mogelijk aangezien er aan reverse pathing gedaan werd. Het doeladres weet perfect hoe hij naar het bronadres moet navigeren. Terwijl het doeladres naar het bronadres gaat, wordt er terug aan reverse pathing gedaan. Als het Route Reply bericht toekomt op het bronadres, zal elke router weten hoe hij van het bronadres naar het doeladres moet navigeren. Pas hierna kan er data uitgewisseld worden tussen het bron- en doeladres.

10.2 B2 - Configuratie van DNS servers onder Linux

10.2.1 Vragen

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. Je hoeft geen reverse DNS te configureren.

1. 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 *forwaders*, noch de $ORIGIN opdracht!

2. Bespreek in detail het begrip *secundaire nameserver*, inclusief voordelen, beperkingen en problemen.

10.2.2 Antwoorden

1. **Configuratiebestand: /etc/named.conf**

```
options {
        directory "/var/named";
        allow-transfer { 192.168.1.126; };
};

zone "XX.us.zone" IN {
        type slave;
        file "XX.us.zone";
        masters { 192.168.1.126 }
}

zone "." {
        type hint;
        file "named.ca";
}
```

Zonebestand: /var/named/XX.us.zone

```
$TTL 60
@       IN      SOA     corelli.sonatas.XVII.it. email.provider.be. (
                                        1       ; serial
```

```
                                        1       ; refresh
                                        1       ; retry
                                        1       ; expire
                                        1 )     ; minimum
                IN      NS      corelli.sonatas.XVII.it.
vocal           IN      NS              gershwin.vocal
barber          IN      A               192.168.1.4
bernstein       IN      A               192.168.1.17
cage            IN      A               192.168.1.58
copland         IN      A               192.168.1.73
glass           IN      A               192.168.1.99
```

2. Secundaire DNS servers houden dezelfde informatie bij als primaire DNS servers maar hebben het voordeel dat ze de taak van de primaire servers verlichten. Ook in het geval dat een primaire DNS server uitvalt kan de secundaire DNS server nog steeds informatie uitwisselen. Een nadeel is dat wijzigingen enkel doorgevoerd worden op de primaire nameserver. De secundaire nameserver moet dus controleren of dat de primaire nameserver gewijzigd is.

10.3 B3 - Configuratie van DNS servers onder Linux

10.3.1 Vragen

De figuur in bijlage stelt een intranet bestaand uit een aantal *Linux* ...(crf.vraag B2) ... achterhalen. Geen enkele zone heeft een secundaire nameserver. Je hoeft geen reverse DNS te configureren.

1. Stel het *configuratiebestand* en alle *zonebestanden* op van volgende DNS servers. Gebruik **relatieve DNS namen** waar mogelijk. Gebruik noch *forwaders*, noch de $ORIGIN opdracht!

2. 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.

10.3.2 Antwoorden

1. **Configuratiebestand : /etc/named.conf**

```
options {
        directory "/var/named";
};
```

```
zone "x" IN {
        type master;
        file "x";
}

...
```

Zonebestand cfr vraag B2

2. Het eerste record van een zonebestand is altijd een Start Of Authority record en wordt altijd voorafgegaan door een @. Dit is een speciale naam dat staat voor de huidige oorsprong. Een SOA record bevat de primaire nameserver, een e-mailadres van de verantwoordelijke en een aantal getallen. Het eerste getal is een serial nummer. Dit moet verhoogd worden wanneer er iets aan het configuratiebestand gewijzigd wordt. De vier andere getallen zijn tijdsduren in seconden. Het refresh interval zegt aan de secundaire nameserver wanneer hij zijn database moet vernieuwen met de data van de primaire server. Het retry interval zegt aan de secundaire server hoelang hij moet wachten om opnieuw de primaire nameserver te contacteren in het geval dat een refresh mislukt is. Het expire interval zegt hoelang de gegevens bewaard blijven en het laatste getal is de default TTL waarde. Na de SOA records komen er één of meerdere NS records. Deze records bevatten de namen van alle primaire en secundaire DNS servers van dit domei en al zijn gedelegeerde domeinen. Een MX record bevat een nummertje dat de prioriteit aangeeft en de naam van de nameserver. Indien er meerdere MX records bestaan zullen deze afgelopen worden volgens prioriteit. Een CNAME record laat toe om aliases te gebruiken. Zo kan je een naam naar een andere naam mappen. Tot slot is er nog de A record. Dit zal een naam naar een IP-adres mappen.

10.4 B4 - Configuratie van DNS servers onder Linux

De figuur in bijlage stelt een intranet bestaand uit een aantal *Linux* ...(crf.vraag B2) ... achterhalen. Geen enkele zone heeft een secundaire nameserver. Je hoeft geen reverse DNS te configureren.

10.4.1 Vragen

1. Stel het *configuratiebestand* en alle *zonebestanden* op van volgende DNS servers. Gebruik **relatieve DNS namen** waar mogelijk. Gebruik noch *forwaders*, noch de $ORIGIN opdracht!

2. 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 al-

ternatieve records en formaten beschrijven, die je niet noodzakelijk hebt gebruikt.

10.4.2 Antwoorden

1. **Configuratiebestand : /etc/named.conf**

```
options {
        directory "/var/named";
};

zone "x" IN {
        type master;
        file "x";
}

...
```

   Zonebestand cfr vraag B2

2. Het configuratiebestand bevat de instellingen voor de serverdaemon en vermeldt de namen van de zonebestanden. Dit bestand is onderverdeeld in een aantal opdrachten. De structuur van een opdracht hangt af van het sleutelwoord waarmee ze beginnen. De twee belangrijkste sleutelwoorden zijn **options** en **zone**.

   Het options sleutelwoord bevat een aantal opties voor de serverdaemon. De eerste optie is is directory. Dit wordt direct gevolgd door de naam van de directory waarin de zonebestanden zich vinden. De tweede optie is forwarders. Dit wordt gevolgd door een lijst van IP-adressen in accolades. Als er bepaalde DNS-info niet bereikbaar is zal hij deze lijst van IP-adressen bevragen voor deze informatie. Als deze IP-adressen ook geen antwoord bieden zullen de DNS-aanvragen naar de rootservers gestuurd worden. De derde en laatste optie is allow-transfer. Dit wordt zoals forwards ook gevolgd door een lijst van IP-adressen omringd in accolades. De IP-adressen zijn van toestellen die een zone transfer kunnen uitvoeren en is een verplichte optie als er secundaire nameservers gebruikt worden.

   Het zone sleutelwoord geeft informatie voor een bepaalde zone.

10.5 B5 - Configuratie van reverse DNS onder Linux

10.5.1 Vragen

1.

10.5.2 Antwoorden

1.

Hoofdstuk 11

Reeks C

11.1 C1 - DHCP leaseprocessen en relay-agents

11.1.1 Vragen

1. Geef een overzicht van de verschillende *types* DHCP berichten. Hoe wordt in het bericht het type aangeduid?
2. Bespreek in detail de opeenvolgende *stappen* van beide DHCP *leaseprocessen*.
3. Bespreek het doel en (in detail) de werking van DHCP relay-agents. Welke velden in DHCP berichten helpen deze functie realiseren.

11.1.2 Antwoorden

1. Er bestaan 8 berichttypen
   - DHCP-Discovery bericht
   - DHCP-Offer bericht
   - DHCP-Request bericht
   - DHCP-Decline bericht
   - Positief DHCP-Acknowledgment bericht
   - Negatief DHCP-Acknowledgment bericht
   - DHCP-Release bericht
   - DHCP-Inform bericht

   Het type van het bericht wordt wordt door een waarde van 1 tot en met 8 meegegeven aan de optie 53 of 'dhcp-message type' van het bericht
2. Het initialisatieproces komt voor wanneer een DHCP-cliënt zich meldt aan een network waar hij nog geen deel van uitmaakte.

(a) De DHCP-cliënt broadcast een DHCP-Discovery bericht naar het lokale subnet. In dit bericht wordt de leasetijden en een aantal opties vastgelegd. Voor de leasetijden wordt optie 51 gebruikt en voor de lijst van opties wordt optie 55 gebruikt. Het IP-adres van de DHCP-cliënt wordt in een DHCP-Discovery bericht ingevuld met 0.0.0.0

(b) Alle DHCP-servers kunnen hierop reageren met een DHCP-offer bericht. In dit bericht zal een IP-adreslease aangeboden worden en ook de aangevraagde opties van de cliënt. Elke server zal dit IP-adres reserveren voor de cliënt. Door middel van optie 54 kan een cliënt onderscheid maken tussen verschillende servers aangezien hier het IP-adres van de server bewaard wordt. In het geval dat er geen server gevonden is zal de cliënt een nieuw DHCP-discovery bericht versturen. De wachtperiode vergroot altijd van 2, 4, 8, tot 16 seconden. na deze 4 pogingen wordt de wachttijd ingezet op 5 minuten totdat een DHCP-offer bericht ontvangen wordt van een server.

(c) Als er één of meerdere DHCP-offers zijn selecteert de cliënt de eerste offer die aan alle verlangens voldoet. Naar deze server stuurt de cliënt dan een DHCP-Request bericht. In dit request bericht wordt de server ook geïdentificeerd met een IP-adres met optie 54

(d) De geselecteerde server stuurt doorgaans een positief DHCP-Acknowledgment bericht naar de cliënt om de lease te bevestigen. De aangevraagde opties door de cliënt worden hier ook mee verzonden. De DHCP-Servers die niet geselecteerd werden zullen stoppen met het IP-adres voor deze cliënt te reserveren. In het geval dat de cliënt een ongeldig of reeds een toegekend IP-adres heeft zal elke DHCP-server een negatief DHCP-Acknowledgment bericht naar de cliënt sturen. Hierdoor mislukt het hele initialisatieproces en moet er terug vanaf stap 1 begonnen worden.

(e) Uiteindelijk worden de TCP/IP eigenschappen geconfigureerd aan de hand van de gegevens die de cliënt van de server ontvangen heeft. Als de cliënt merkt dat er één van de parameters ongelgid zijn stuurt hij een DHCP-Decline bericht naar de geselecteerde server en moet het initialisatieproces opnieuw gestart worden. Als de cliënt meer informatie wil kan hij een DHCP-Inform bericht sturen naar de server. Als de cliënt de lease niet meer nodig heeft kan hij een DHCP-Release bericht sturen.

Het vernieuwingsproces vindt plaats wanneer een cliënt al over een lease beschikt, maar deze lease langer wil laten gelden.

(a) De cliënt stuurt een DHCP-Request bericht naar de server met als melding om de adreslease te vernieuwen en verlengen.

(b) Als de server beschikbaar is stuurt deze een positief DHCP-Acknowledgment bericht naar de cliënt. Op deze manier wordt de lease van elke DHCP-cliënt telkens opnieuw verlengd. Hierbij worden er ook DHCP-opties

meegestuurd. Als er opties zijn die gewijzigd zijn, zal de DHCP-cliënt dit automatisch bijwerken. Indien de cliënt geen DHCP-Acknowledgment bericht ontvangt zal hij een periodiek een DHCP-Request bericht versturen naar de server.

(c) In het geval dat de oorspronkelijke DHCP-Server niet beschikbaar is zal de cliënt wachten totdat de tijd voor rebinding van de lease is verstreken. Wanneer dit gebeurd zal de cliënt een willekeurige DHCP-Server aanspreken om zijn adreslease te vernieuwen.

(d) Als deze server reageert met een positief DHCP-Acknowledgment bericht, kan de cliënt zijn adreslease bij deze server vernieuwen. Indien dit niet is zal de cliënt terug periodiek DHCP-Request berichten versturen.

(e) Als de lease verloopt en de cliënt kan geen server bereiken, of als een server heeft geantwoord met een negatief DHCP-Acknowledgment bericht, moet de cliënt zijn adreslease onmiddelijk stoppen met als gevolg dat de TCP/IP configuratie ongedaan wordt. De cliënt moet nu het initialisatieproces overlopen.

3. Aangezien dat een DHCP-Server zijn berichten broadcast, en dat een router geen broadcastberichten doorlaat, kan een DHCP-Server enkel werken op subnetniveau. Een relay agent maakt het mogelijk om DHCP broadcastberichten door te sturen naar andere subnetten. Een relay agent is een programma dat DHCP berichten doorgeeft tussen cliënts en servers in verschillende subnetten. Sommige hardware routers ondersteunen de functionaliteit van een BOOTP relay-agent. Deze routers kunnen dan BOOTP berichten herkennen, en aangezien dat DHCP berichten via dezelfde UDP poorten verzonden worden als BOOTP berichten en bovendien dezelfde structuur hebben, kan een BOOTP relay-agent perfect DHCP pakketten door het internetwerk verzenden. Indien er zo geen router beschikbaar is moet ofwel de DHCP-Server, ofwel een andere computer in het subnet als relay-agent fungeren. Dit toestel zal DCHP-berichten ontvangen die als broadcast op één van zijn interfaces, en geeft deze berichten door aan gekende DHCP servers of als broadcast naar alle externe subnetten waarmee hij via zijn fysieke interfaces verbonden is. Het aantal broadcasts wordt doorgaans beperkt. Bij een Windows relay-agent is dit maximumaal vier. Hierom wordt er een *hop* veld bijgehouden dat met één verhoogd wordt telkens het bericht opnieuw gebroadcast wordt. Door een relag-agent verloopt het leaseproces anders:

   (a) Een cliënt stuurt een DHCP-Discovery bericht in zijn subnet.

   (b) De relay-agent ontvangt dit bericht en controleert het veld met het gateway IP-adres in de header van het DHCP-bericht. Als dit veld de waarde 0.0.0.0 bevat, zal de relay-agent dit vervangen door zijn eigen IP-adres en doorsturen naar ofwel een specifiek DHCP-Server ofwel broadcasten naar subnetten waarop de relay-agent fysiek is aangesloten.

(c) De DHCP-Server die dit bericht ontvangt zal nagaan uit welke scope een adreslease moet verleend worden, afhankelijk van het gateway veld dat ingevuld werd met het IP-adres van de relay-agent. De server kiest uit deze scope een IP-adres en stuurt dit via een DHCP-Offer bericht naar de relay-agent.

(d) De relay-agent geeft de adreslease aan de cliënt. Aangezien het client IP-adres onbekend is moet deze nog gebroadcast worden in het lokale subnet.

11.2 C2 - IPv6 Adressering

11.2.1 Vragen

1. Bespreek de *structuur* en *numerieke voorstelling* van IPv6 adressen.

2. Geef en bespreek de verschillende *types* IPv6 adressen. Geef onder andere van elk van deze types de structuur, hun interpretatie, relevante voorbeelden en eventuele subtypes.

11.2.2 Antwoorden

1. IPv6 adressen zijn samengesteld uit 128 bits. De basisstructuur van een IPv6 structuur heeft de vorm `P:Q:R:S:T:U:V:W` waarbij elke letter een hexadecimaal getal van vier cijfers voorstelt. Een IPv6 kan meerdere notaties hebben:

   - 2001:410:1:: = 2001:410:0001:0000:0000:0000:0000:0000
   - :: = 0:0:0:0:0:0:0:0
   - ::1 = equivalent 127.0.0.1 IPv4
   - FE80::5EFE:192.168.41.30 = FE80:0:0:0:0:5EFE:C0A8:291E
   - 2001:410:1::/48

2.