

Breedband IPv6 transitie

Scriptie



Dit document behoort tot het afstudeerdossier van de student Jasper Kemper bij het bedrijf Breedband.

Afstudeerdocent: Erik van der Arend
Bedrijfsbegeleider: Tom van Klinken

Datum: zondag 27 oktober 2019
Versie: 1.00
Status: Definitief

Versiebericht

Versienummering wordt ingevuld bij elke wijziging in het document. Het eerste deel ([0].01) duidt een definitieve versie aan waarin het document is opgeleverd aan alle belanghebbenden. Het tweede deel (0.[01]) duidt een wijziging aan waarin inhoud is bijgewerkt, de verandering is aangegeven in de kolom "Verandering". Een optioneel derde deel (0.01[a]) duidt een kleine aanpassing aan die de inhoud van het document niet drastisch veranderd, deze versies worden niet meegenomen in het versiebericht en worden doorgaans niet verspreidt.

Versie	Verandering	Datum	Door
0.01	Document aangemaakt.	19-06-2019	Jasper Kemper
0.02	Indeling bepaald; Probleemanalyse V0.07 ingevoegd; Behoeftanalyse V0.04 ingevoegd; Contextanalyse V0.05 ingevoegd; Aangepast tot leesbaar document.	01-07-2019	Jasper Kemper
0.03	Literatuuronderzoek V0.07 ingevoegd; Inspirerend voorbeeld V0.02 ingevoegd; Feedback ingevoegd.	20-09-2019	Jasper Kemper
0.04	Probleemanalyse bijgewerkt naar V0.08; Behoeftanalyse bijgewerkt naar V0.05; Contextanalyse bijgewerkt naar V0.06; Literatuuronderzoek bijgewerkt naar V0.08; Inspirerend voorbeeld bijgewerkt naar V0.04; Ontwerp V0.05 ingevoegd; Feedback verwerkt.	09-10-2019	Jasper Kemper
0.05	Feedback verwerkt; Kwaliteitscontrole.	14-10-2019	Jasper Kemper
0.06	Begrippenlijst bijgewerkt; Reflectie ingevoegd; Feedback verwerkt.	27-10-2019	Jasper Kemper
1.00	Kwaliteitscontrole; Definitief gemaakt.	27-10-2019	Jasper Kemper

Voorwoord

Voor u ligt de scriptie 'Breedband IPv6 transitie' geschreven door Jasper Kemper gedurende zijn afstudeerperiode van de studie IT-Service Management op het Saxion. De scriptie bevat een onderzoek naar een IPv6 transitie in opdracht van het bedrijf Breedband.

Ik wil graag mijn dank betuigen aan mijn bedrijfsbegeleider Tom van Klinken voor zijn uitmuntende kennis en bijdrage aan de scriptie. Tevens wil ik mijn afstudeerbegeleider Erik van der Arend bedanken voor zijn steun en feedback tijdens het schrijven van deze scriptie.

Samenvatting

Breedband is een bedrijf met als corebusiness het leveren van internetdiensten aan zijn klanten. Met het opraken van de IPv4-adressen kijkt Breedband naar oplossingen voor dit probleem. Het oog is gevallen op de transitie techniek 'Lightweight 4over6' (lw4o6). Deze scriptie bevat een onderzoek naar deze techniek en het achterliggende probleem waar de desbetreffende techniek de oplossing voor zou kunnen zijn. Om dit onderzoek soepel te laten verlopen is de methode uit de 'Reader Ontwerponderzoek' door Haveman, Hageraats en Van der Linden (2016) gebruikt. Om de resultaten in het onderzoek gestructureerd te verkrijgen, is gebruikgemaakt van een zestiental methodieken.

Door specifieker naar het probleem te kijken en meerdere perspectieven te combineren, is te stellen dat Breedband een oplossing nodig heeft voor het bekende probleem "IPv4-exhaustion". Dit is af te bakenen met de onderzoeksvraag:

"Hoe kan Breedband de dreiging van IPv4-exhaustion beperken totdat IPv6 de standaard wordt?"

Met een tiental deelvragen is een onderzoek opgesteld naar de eisen aan een oplossing, de randvoorwaarden vanuit de context en een theoretisch kader. Daarnaast is gekeken naar inspirerende voorbeelden. De belangrijkste conclusie van het onderzoek is dat lw4o6 daadwerkelijk de best geschikte oplossing is voor Breedband. Lw4o6 is volledig open source te implementeren en is met per-subscriber-state goed te realiseren met behulp van veelvoorkomende hardware. Andere partijen die lw4o6 hebben geïmplementeerd zijn Deutsche Telekom en OTE. Deze partijen zijn aanzienlijk groter dan Breedband en hebben daardoor voldoende financiële omvang om de lwB4 functie op maat laten maken voor een white label CPE. Dit is voor Breedband niet rendabel. Breedband moet zich daarom richten op een open source CPE die lwB4 ondersteund.

De oplossing voor het probleem is een ontwerp voor een lw4o6 implementatie. Daarbij wordt een OpenWRT CPE gebruikt als lwB4 en een Ubuntu virtuele machine als lwAFTR. In de evaluatie is echter gebleken dat OpenWRT slecht functionerende onderdelen heeft in zijn lwB4-functie waardoor het niet goed kan worden geïmplementeerd. De lwAFTR is wel in volledigheid te implementeren. Provisioning van de functies is niet compleet te realiseren wanneer er geen volledige lwB4 beschikbaar is. Provisioning dient te zijn gebaseerd op de inrichting van de lwB4, waarna deze configuratie wordt gerepliceerd naar een lwAFTR.

De conclusie van het onderzoek is dat lw4o6 veel potentie heeft, maar niet direct kan worden geïmplementeerd. Het antwoord op de hoofdvraag luidt dan ook:

Breedband dient de ontbrekende functies in OpenWRT door softwareontwikkelaars te laten aanvullen. Daarnaast dient de provisioning die daarbij komt kijken te worden gelinkt aan alle functies binnen het netwerk van lw4o6. Wanneer deze functies compleet zijn en lw4o6 in zijn volledigheid kan draaien, is lw4o6 te implementeren om zo de dreiging van IPv4-exhaustion te beperken.

Begrippenlijst

Begrip	Betekenis
464XLAT	4-6-4 Provider/Customer side Translation - Een IPv4-to-IPv6 transitie techniek (Mawatari, Kawashima, & Byrne, 2013).
4in6 tunnel	IPv4 in IPv6 tunnel - Een tunnel waarin IPv4-verkeer kan worden verzonden over een IPv6-verbinding (Conta & Deering, 1998).
ACL	Access Control List - Een lijst met regels die bepalen of pakketten worden doorgelaten tijdens routing (Cox, 2019).
ADM	Add-Drop Multiplexer - Een multiplexer die meerdere lower-bandwidth verbindingen kan toevoegen of extraheren uit een high-bandwidth stream (Zhu, 2016).
AFTR	Address Family Transition Router - Een onderdeel van DS-Lite dat NAT uitvoert op provider-niveau en pakketten decapsuleert (Durand, Droms, Woodyatt, & Lee, 2011).
Anycast	Pakketten die naar meerdere bekende leden op een netwerk worden verzonden (gebruikt voor loadbalancing, alleen op IPv6) (Hinden & Deering, IP Version 6 Addressing Architecture, 2006).
ARP	Address Resolution Protocol - Een protocol dat op basis van MAC-adressen computers in het netwerk ontdekt (Plummer, 1982).
B4	Basic Bridging BroadBand - Tunnels IPv4 pakketten zodat ze over IPv6 netwerk kunnen worden vervoerd (Durand, Droms, Woodyatt, & Lee, 2011).
BGP	Border Gateway Protocol - Het protocol dat wordt gebruikt om te routeren tussen providers (Rekhter, Li, & Hares, A Border Gateway Protocol 4 (BGP-4), 2006)
BNG	Broadband Network Gateway - Een BNG bepaald de sessies van subscribers en aggregeert daarbij het verkeer naar het netwerk van de serviceprovider (Cisco, z.d.).
Broadcast	Pakketten die naar ieder lid op een IPv4-netwerk worden verzonden (Mogul, 1984).
Bump-in-the-wire	Bump in the wire - Een netwerkkapparaat dat met twee interfaces is aangesloten op een netwerk. Data komt binnen op één interface en wordt na verwerking doorgestuurd naar de andere interface (Haletky, 2017).
CGN	Carrier-Grade NAT - Een IPv4-to-IPv6 transitie techniek, maar ook vaak gebruikt als overkoepelende term voor andere transitie technieken die gebruik maken van NAT op provider-niveau (Jiang, Guo, & Carpenter, 2011).
CIDR	Classless Inter-Domain Routing - Vervanging van het oude subnetten op basis van klassen, CIDR deelt specifiek op het aantal bits van het subnetmask (Janssen, z.d.).
CLAT	Customer-side Translator - Onderdeel van 464XLAT dat NAT uitvoert aan de kant van de consument (Bagnulo, Matthews, & van Beijnum, 2011).
COTS	Common/Commercial off the Shelf - Reguliere hardware die grootschalig verkrijgbaar is bij leveranciers, zonder handmatige aanpassingen (Rouse, COTS, MOTS, GOTS, and NOTS, 2010).
CPE	Customer Premises Equipment - De hardware op locatie van de klant; alles wat de klant met het ISP-netwerk verbindt (Rouse, CPE device, 2010)
Decapsulation	Het uitpakken van IP-pakketten die zijn ingepakt doormiddel van encapsulation (Farinacci, Li, Hanks, & Meyer, 2000).
Destination Option Header	Een optionele header in een IPv6-pakket met aanvullende informatie over de bestemming van het pakket (Deering & Hinden, 2017).
DHCP	Dynamic Host Configuration Protocol for IPv4 - Het protocol netwerkinstellingen distribueert aan apparaten op een IPv4-netwerk (Droms, 1997)
DHCPv6	Dynamic Host Configuration Protocol for IPv6 - Het protocol netwerkinstellingen distribueert aan apparaten op een IPv6-netwerk (Mrugalski, et al., 2018)
DPI	Deep Packet Inspection - Een functie die vaak op firewalls wordt gedraaid om pakketten te inspecteren op inhoud (Brook, 2018).

Tabel 1. Begrippenlijst (deel 1 van 3)

Begrip	Betekenis
DS	Dual Stack - De term voor het onderhouden van een IPv4 én IPv6 netwerk naast elkaar op dezelfde hardware (Hogg, 2007).
DS-Lite	Dual Stack lite - Een IPv4-to-IPv6 transitie techniek (Durand, Droms, Woodyatt, & Lee, 2011).
DUID	DHCP Unique Identifier - Een identificatiecode waarmee een client een IP address opvraagt bij een DHCPv6 server (Mrugalski, et al., 2018).
Encapsulation	Het inpakken van IP-pakketten in andere IP-pakketten om te versturen over een verbinding (Farinacci, Li, Hanks, & Meyer, 2000).
IANA	Internet Assigned Numbers Authority - De organisatie die distributie van IP-adressen beheert. IANA distribueert IP-adressen aan RIR's (IANA, z.d.).
ICANN	Internet Corporation for Assigned Names and Numbers - Overkoepelende organisatie die taken van IANA uitvoert (ICANN, z.d.).
IPv4 Subnet classes	Internet Protocol version 4 Subnet classes - Class A, B en C voor het verdelen van host- en netwerkbits in IP-pools (Janssen, z.d.).
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol - Een IPv4-to-IPv6 transitie techniek (Templin, Gleeson, & Thaler, 2008).
LIR	Local Internet Registry - ISP's die in direct contact staan met een RIR, deelt IP-adressen uit aan kleinere ISPs, eigen netwerk, of klanten (Richter, Allman, Bush, & Paxson, 2015).
lw4o6	Lightweight ipv4 over ipv6 - Een IPv4-to-IPv6 transitie techniek. Ook gezien als extensie op DS-Lite (Cui, et al., 2015).
lwAFTR	Lightweight Address Family Transition Router - Lichtelijk aangepaste versie van AFTR voor gebruik in lw4o6 (Cui, et al., 2015).
lwB4	Lightweight Basic Bridging BroadBand - Lichtelijk aangepaste versie van B4 voor gebruik in lw4o6 (Cui, et al., 2015).
MAC	Media Access Control - Vrijwel unieke identificatie adressering voor fysieke netwerkadapters (Eastlake 3rd & Abley, 2013)
MAP	Mapping of Address and Port - Een IPv4-to-IPv6 transitie techniek (Dec, Li, Bao, Matsushima, & Murakami, 2015).
MAP-E	Mapping of Address and Port with Encapsulation - Een IPv4-to-IPv6 transitie techniek (Dec, Li, Bao, Matsushima, & Murakami, 2015).
MAP-T	Mapping of Address and Port using Translation - Een IPv4-to-IPv6 transitie techniek (Li, Bao, Troan, Matsushima, & Murakami, 2015).
MP-BGP	Multi-Protocol Border Gateway Protocol - Een extensie op BGP die ondersteunt om meerdere protocollen tegelijk te kunnen verzenden (Ergun, 2016).
MPLS	Multi-Protocol Label Switching - Hangt een label aan pakketen zodat ze onderscheiden worden (Rosen, Viswanathan, & Callon, 2001).
NAPT	Network Address and Port Translation - Techniek die IP-adressen en poortnummers in adres-headers binnen IP-packets veranderd (Srisuresh & Egevang, 2001).
NAT	Network Address Translation - Techniek die IP-adressen in adres-headers binnen IP-packets veranderd (Srisuresh & Egevang, 2001).
NAT44	Network Address Translation IPv4 to IPv4 - Een NAT functie die specifiek alleen IPv4 naar IPv4 vertaalt (Srisuresh & Egevang, 2001).
NAT64	Network Address Translation IPv6 to IPv4 - Een NAT functie die specifiek IPv6 naar IPv4 vertaalt (Bagnulo, Matthews, & van Beijnum, 2011).
NAT-PMP	NAT Port Mapping Protocol - Een protocol dat het mogelijk maakt voor clients achter een NAT, om port-mappings aan te vragen op de NAT. NAT-PMP wordt niet meer verder ontwikkeld en wordt inmiddels overgenomen door PCP (Cheshire & Kochmal, 2013).
NFV	Network Functions Virtualization - Overkoepelende term voor VNF's (SDxCentral, 2013).

Tabel 2. Begrippenlijst (deel 2 van 3)

Begrip	Betekenis
On-a-stick	On a stick - Een netwerkkapparaat dat met één interface is aangesloten op een netwerk, verwerkte data wordt teruggestuurd over dezelfde interface als de data binnenkomt (Jensen, 2019).
PCI Device Passthrough	Een techniek waarin een hypervisor een PCI-apparaat direct toewijst aan een virtuele machine, zonder de hardware eerst te virtualiseren (VMware, 2019).
PCP	Port Control Protocol - De directe opvolger van NAT-PMP (Wing, Cheshire, Boucadair, Penno, & Selkirk, Port Control Protocol (PCP), 2013) .
PE	Provider Edge - De rand van de provider, grenzend aan het publieke internet (Rekhter, Bonica, & Rosen, Use of Provider Edge to Provider Edge (PE-PE), 2007)
PLAT	Provider-side Translator - Onderdeel van 464XLAT dat NAT uitvoert aan de kant van de provider (Li, Bao, & Baker, IP/ICMP Translation Algorithm, 2011).
Prefix Delegation	Een techniek waarmee een IPv6-subnet wordt opgevraagd en automatisch verder wordt gedelegeerd door een DHCPv6-server (Deering & Hinden, 2017).
psid	Port-set ID - Het identificatienummer van een poortreeks die wordt gebruikt in gedeelde IP-adres structuren. Vormt in combinatie met de pslen een berekening om de begin en eindpoort van een port-set te bepalen (García, Dive into Lightweight 4over6, 2017).
pslen	Port-set length - De grootte van een poortreeks die wordt gebruikt in gedeelde IP-adres structuren. Vormt in combinatie met een berekening een decimale waarde die het aantal poorten aanduidt die kan worden gebruikt (García, Dive into Lightweight 4over6, 2017).
psoffset	Port-set offset - Een waarde die bepaalt hoeveel psid's worden overgeslagen bij configuratie (García, Dive into Lightweight 4over6, 2017).
RA	Router Advertisement - Een dienst op een router die netwerkinformatie vrijgeeft voor clients in het netwerk die via SLAAC hun IP-adres willen configureren (Narten, Nordmark, Simpson, & Soliman, 2007).
RADIUS	Remote Authentication Dial-In User Service - Een authenticatie, autorisatie en accountingsysteem gebruikt voor netwerkdiensten (Rigney, Rubens, Simpson, & Willens, 2000).
RFQ	Request For Quotation - Een bedrijfsproces waarin meerdere leveranciers worden aangesproken om bepaalde producten of diensten te creëren voor een bedrijf (Mhay & Coburn, 2019)
RIR	Regional Internet Registry - Regionale IP-managers die adressen uitdelen aan LIR's (Richter, Allman, Bush, & Paxson, 2015).
SLAAC	Stateless Address AutoConfiguration - Een functie voor netwerkadapters om IPv6 automatisch te configureren op het netwerk en apparaat informatie (Donaldson, 2011).
Softwires	Mappings tussen IPv6 adressen en IPv4 public address + Port set (García, Dive into Lightweight 4over6, 2017).
SPOF	Single Point of Failure - Een onderdeel in een systeem dat enkelvoudig is uitgevoerd (Riley, 2018).
Stateful	Een eigenschap die bepaalt of een apparaat informatie moet bijhouden van sessies om te functioneren (Bhakhra, z.d.).
Stateless	Een eigenschap die bepaalt of een apparaat functioneert zonder sessies bij te houden (Bhakhra, z.d.).
Subscriber management	Het systeem dat alle subscribers (eindgebruikers) van een netwerk inricht en beheert (Sridhar, 2017).
VLAN	Virtual Local Area Network - Extra veld in een IP-packet dat VLAN aanduidt, een VLAN duidt een virtueel losstaand netwerk van andere VLAN's (Ionos, 2019).
VNF	Virtual Network Function - Een netwerkfunctie (zoals routing, of intrusion detection) die virtueel softwarematig wordt uitgevoerd, zonder afhankelijkheden van specifieke hardware (Hirotsu, 2016).
White Label	Hardware zonder merknaam, bedoelt voor bedrijven die het als eigen willen verkopen of gebruiken (Tardi, 2019).

Tabel 3. Begrippenlijst (deel 3 van 3)

Inhoudsopgave

1. Introductie	11
2. Aanpak	12
2.1. Proces	12
2.2. Methodieken	13
2.2.1. Triangulatie	13
2.2.2. Literatuuronderzoek	13
2.2.3. Interviews	14
2.2.4. Deskresearch	14
2.2.5. Stakeholderanalyse	14
2.2.6. MoSCoW analyse	14
2.2.7. Requirement categorisering	14
2.2.8. Reviewtechnieken	15
2.2.9. Aggregatieniveaus	15
2.2.10. DESTEP-analyse	15
2.2.11. GOKIT	15
2.2.12. Bronbeoordeling	15
2.2.13. Prototyping	16
2.2.14. Archimate	16
2.2.15. UML	16
2.2.16. Multicriteria-analyse	16
2.3. Afwijkingen	16
3. Probleemanalyse	17
3.1. Resultaten	17
3.1.1. Probleem	17
3.1.2. Perspectieven	17
3.2. Conclusie	19
3.2.1. Onderzoeksvraag	19
3.2.2. Deelvragen	20
4. Vooronderzoek	21
4.1. Behoefteanalyse	21
4.1.1. Resultaten	21
4.1.2. Conclusie	22
4.2. Contextanalyse	24
4.2.1. Resultaten	24
4.2.2. Conclusie	27
4.3. Literatuuronderzoek	29
4.3.1. Resultaten	29
4.3.2. Conclusie	40
4.4. Inspirerend voorbeeld	42
4.4.1. Resultaten	42
4.4.2. Conclusie	45
5. Ontwerp	46
5.1. Ontwerpbenadering	46
5.2. Functioneel	48
5.2.1. Lightweight B4	49
5.2.2. Lightweight AFTR	49

5.2.3. Provisioning	49
5.3. Technisch	50
5.3.1. Lightweight B4	50
5.3.2. Lightweight AFTR	50
5.3.3. Provisioning	51
5.4. Ontwerpevaluatie	52
5.4.1. Implementatie	52
5.4.2. CPE (Lightweight B4)	54
5.4.3. Lightweight AFTR	56
5.4.4. DHCPv6	56
5.5. Conclusie	57
6. Conclusies en aanbevelingen	59
Bibliografie	61
Bijlage A: Interview projectdefinitie	66
Bijlage B: Interview management	68
Bijlage C: Zoekstrategie	69
Bijlage D: Bronbeoordeling	70
Bijlage E: Status lwB4 OpenWRT	76
Bijlage F: Virtuele OpenWRT	77
Bijlage G: Ubuntu lwB4	78
Bijlage H: lwAFTR configuratie	81
Bijlage I: Kea DHCPv6 config	83
Bijlage J: Ontwerpprincipe gebruik	84
Bijlage K: Haalbaarheidsrapport	87
Bijlage L: Organigram Breedband	90
Bijlage M: Multicriteria-analyse transitie technieken	91
Bijlage N: Reflectie	92

Figuren

Figuur 1. Schematische weergave ontwerponderzoek.	12
Figuur 2. IPv4 prijstrends	18
Figuur 3. IPv6 adoptie op basis van IPv6 webbrowsers (Google).	19
Figuur 4. Stakeholder categorie-indeling	21
Figuur 5. Schematische weergave van klantverbindingen Breedband	25
Figuur 6. Schematische weergave infrastructuur Breedband-consumenten	26
Figuur 7. Architectuurplaat Subscriber Management	28
Figuur 8. Schema voor IP-distributie	30
Figuur 9. IPv6-adres breakdown.	31
Figuur 10. IPv6 geschiktheid in West-Europa	32
Figuur 11. DS-Lite werking - versimpelde weergave	33
Figuur 12. Lw4o6 werking - versimpelde weergave	34
Figuur 13. Lw4o6 in TeraStream	43
Figuur 14. Architectuurplaat lw4o6	47

Figuur 15. Sequence diagram van lw4o6 verkeer	48
Figuur 16. Schema prototype	53
Figuur 17. OpenWRT prototype netwerk configuratie.	55
Figuur 18. Ubuntu prototype netwerk configuratie.	55

Tabellen

Tabel 1. Begrippenlijst (deel 1 van 3)	5
Tabel 2. Begrippenlijst (deel 2 van 3)	6
Tabel 3. Begrippenlijst (deel 3 van 3)	7
Tabel 4. Stakeholdertabel	21
Tabel 5. Business requirements	22
Tabel 6. User requirements	23
Tabel 7. System requirements	23
Tabel 8. DESTEP-analyse	24
Tabel 9. Vergelijking van transitie technieken	38
Tabel 10. Ontwerpprincipes (tabel 1 van 2)	40
Tabel 11. Ontwerpprincipes (2 van 3)	41
Tabel 12. Ontwerpprincipes (tabel 3 van 3)	42
Tabel 13. Requirements uit voorbeelden	45
Tabel 14. Option_S46 eisen per transitie techniek.	51
Tabel 15. Iteraties prototype	52
Tabel 16. Prototype netwerken	54
Tabel 17. Requirements beoordeling	58
Tabel 18. Bronbeoordeling (deel 1 van 6)	70
Tabel 19. Bronbeoordeling (deel 2 van 6)	71
Tabel 20. Bronbeoordeling (deel 3 van 6)	72
Tabel 21. Bronbeoordeling (deel 4 van 6)	73
Tabel 22. Bronbeoordeling (deel 5 van 6)	74
Tabel 23. Bronbeoordeling (deel 6 van 6)	75
Tabel 24. Gebruik van ontwerpprincipes (deel 1 van 3)	84
Tabel 25. Gebruik van ontwerpprincipes (deel 2 van 3)	85
Tabel 26. Gebruik van ontwerpprincipes (deel 3 van 3)	86
Tabel 27. MCA-criteria	91

1. Introductie

Van mei 2019 tot november 2019 is een afstudeertraject gevolgd door Jasper Kemper ter afronding van de studie 'IT-Service Management' op het Saxion. Het afstudeertraject bestaat uit het onderzoeken van een probleem en het adviseren over een oplossing. Het afstudeertraject wordt uitgevoerd bij het bedrijf Breedband.

Breedband is een bedrijf gevestigd in het centrum van Arnhem en heeft als core business het leveren van internetdiensten. Het bedrijf heeft één kantoor in Arnhem en maakt gebruik van verschillende datacentra verspreid over Nederland om zijn diensten aan te bieden. Het project zal plaatsvinden op het kantoor, waar in totaal 26 personen werkzaam zijn.

Het bedrijf structureert zijn taken door splitsing van verschillende afdelingen, te zien in het organigram in bijlage L. Het onderzoek is uitgevoerd vanuit de afdeling 'Research & Development'. De opdracht is bepaald en begeleid door CTO Tom van Klinken.

Breedband heeft voornamelijk zakelijke klanten, maar biedt ook internetdiensten aan consumenten over zijn eigen glasvezelnetwerk. Voor elke klant die internetdiensten afneemt is het noodzakelijk om IPv4-adressen te gebruiken zodat zij kunnen deelnemen aan het IPv4-internet. Om het gebruik van IPv4-adressen te beperken kijkt Breedband naar oplossingen en heeft specifiek interesse in IPv6 transitie techniek 'lw4o6' (RFC7596 (Cui, et al., 2015)). De interesse is gewekt door een kort, niet gedocumenteerd, onderzoek door Tom van Klinken.

Deze scriptie bevat een onderzoek naar de techniek 'lw4o6' en het achterliggende probleem waar deze techniek de oplossing voor zou kunnen zijn.

Leeswijzer:

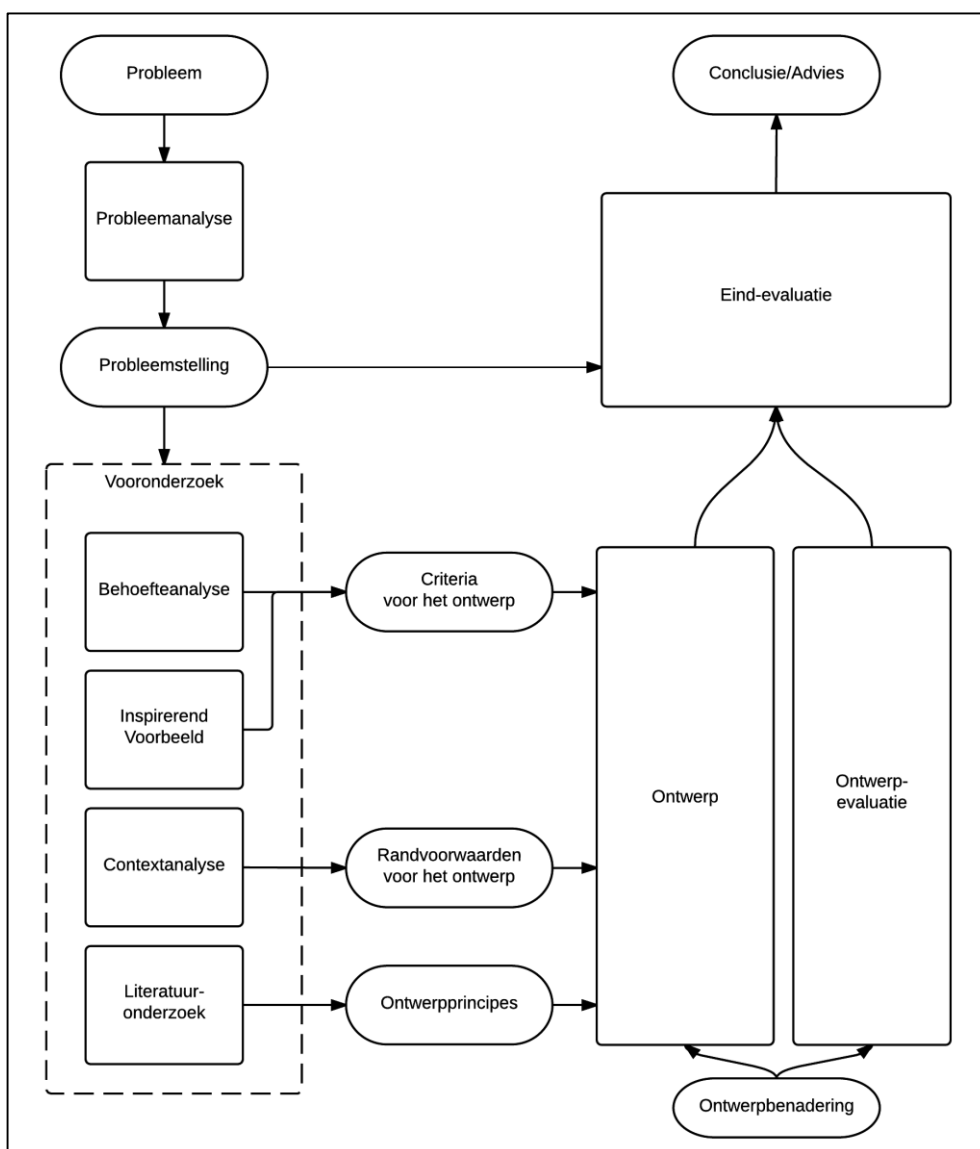
- **Aanpak;**
Het document begint met een hoofdstuk dat beschrijft hoe het afstudeertraject is aangepakt. Dit hoofdstuk maakt duidelijk welke processen en methodieken hebben geleid tot een compleet en onderbouwd resultaat.
- **Probleemanalyse;**
De opdracht wordt ontleed en het probleem wordt geanalyseerd. De uitkomst van dit hoofdstuk geeft inhoudelijke sturing voor het onderzoek en resulteert in een hoofdvraag met een set deelvragen.
- **Vooronderzoek;**
Het onderzoek bestaat uit een behoefteanalyse, contextanalyse, literatuuronderzoek en het inspirerend voorbeeld. Respectievelijk resulteren deze hoofdstukken in de requirements, randvoorwaarden, een theoretisch kader en criteria vanuit voorbeelden.
- **Ontwerp;**
Het ontwerp is gericht om te dienen als oplossing voor het probleem uit de probleemanalyse. Het wordt ontworpen aan de hand van de informatie uit het onderzoek.
- **Conclusies en aanbevelingen.**
De uitkomst van het ontwerp is geëvalueerd en resulteert in een conclusie die antwoord kan geven op de onderzoeksvraag. Aanvullend op het antwoord op de deelvraag worden aanbevelingen gegeven voor de opdrachtgever.

2. Aanpak

De aanpak van het afstudeertraject is opgebouwd uit twee onderdelen: het proces en de methodieken. In het proces wordt de basis van de loop van het afstudeertraject beschreven en zal duidelijk worden op welke manier is gewerkt. In de methodieken is dieper ingegaan op specifieke methodieken die zijn gebruikt bij bepaalde onderdelen in de scriptie.

2.1. Proces

Het belangrijkste deel van dit project is het onderzoek. Om dit onderzoek soepel te laten verlopen is er een erkende methode gebruikt voor het onderzoek binnen Saxion. Dit is de methode uit de volgende literatuur 'Reader Ontwerponderzoek' door Haveman, Hageraats en Van der Linden (2016). In deze reader wordt de structuur aangehouden uit Figuur 1.



Figuur 1. Schematische weergave ontwerponderzoek.

Noot. Herdrukt van Reader Ontwerponderzoek (p. 8) door Haveman, Hageraats & Van der Linden (2016).

In de probleemanalyse wordt het probleem uitgewerkt en wordt het vanuit meerdere perspectieven bekeken. De probleemanalyse resulteert in een probleemstelling waarmee het vooronderzoek kan worden gestart (Haveman, Hageraats, & Van der Linden, 2016).

In het vooronderzoek volgens Haveman, Hageraats en Van der Linden (2016) worden vier document opgesteld. De behoefteanalyse onderzoekt de behoefte van de klant. Het inspirerend voorbeeld kijkt naar andere partijen die voor een soortgelijk probleem hebben gestaan. De informatie uit het inspirerend voorbeeld en de behoefteanalyse resulteren in criteria voor het ontwerp. De contextanalyse onderzoekt de context en de omgeving waar de oplossing op moet worden ontworpen, dit resulteert in randvoorwaarden voor het ontwerp. Het gehele vooronderzoek is input voor een geschikt ontwerp.

Een geschikt ontwerp volgens Haveman, Hageraats en Van der Linden (2016) begint met een ontwerpbenadering die beschrijft hoe het ontwerp wordt geschreven, maar ook hoe het ontwerp wordt geëvalueerd. De uitkomst van het ontwerp en de ontwerpevaluatie maakt het mogelijk de eind-evaluatie uit te voeren die resulteert in een conclusie en advies.

2.2. Methodieken

In dit hoofdstuk is van elke gebruikte methode in het onderzoek een beschrijving gegeven van de toepassingen. Daarnaast is aangegeven waarom deze methode is gebruikt. Vervolgens wordt verwezen naar literatuur achter de theorie om zo de betrouwbaarheid van de methode aan te duiden.

2.2.1. Triangulatie

Om de validiteit van dit onderzoek te vergroten wordt gebruik gemaakt van theoretische triangulatie zoals beschreven door Staa & Evers (2010).

Voor een duidelijke beschrijving van het probleem worden verschillende perspectieven op het probleem beschreven. De verschillende perspectieven worden in de conclusie samengevoegd zodat het probleem zo onpartijdig mogelijk kan worden geformuleerd. De perspectieven die worden behandeld zijn:

- Engineering: om een beeld te vormen van de overwegingen vanuit de technische kant de oplossing;
- Management: om een beeld te vormen van de overwegingen vanuit het managementaspect van de oplossing;
- Literatuur: om een beeld te vormen van de redenen vanuit de literatuur om te kijken naar een oplossing.

2.2.2. Literatuuronderzoek

De methode literatuuronderzoek moet men niet verwarren met het product literatuuronderzoek volgens het proces uit de reader ontwerp onderzoek (Haveman, Hageraats, & Van der Linden, 2016). In deze scriptie wordt gebruik gemaakt van literatuur op verschillende plekken in dit document. Bij de methode literatuuronderzoek wordt de literatuur eerst verwerkt. Vervolgens wordt in de tekst verwezen naar de betreffende bron. De bronnen zijn uiteindelijk terug te vinden in de bibliografie, waar ze genoteerd worden volgens APA zesde editie, zoals bepaald door de American Psychological Association (2010). Hieronder wordt per onderdeel kort beschreven waarom en hoe de literatuur is gebruikt om tot een goed resultaat te komen.

Probleemanalyse

Voor het 'Perspectief vanuit de literatuur', dat bijdraagt aan de methode triangulatie, is literatuuronderzoek gebruikt om relevante informatie te verzamelen over het probleem van Breedband. Hiervoor is specifiek gezocht op informatie die een blik geeft op de probleemstelling die in paragraaf 3.1.1. wordt beschreven. Daarmee wordt een beeld gevormd op het probleem vanuit de literatuur. De bronnen zijn uiteindelijk terug te vinden in de bibliografie waar ze genoteerd worden volgens APA zesde editie zoals bepaald door de American Psychological Association (2010).

Literatuuronderzoek

In het onderzoek wordt het theoretisch kader gevormd door het product 'literatuuronderzoek' zoals beschreven in Reader ontwerp onderzoek van Haveman, Hageraats, & Van der Linden (2016). In het product literatuuronderzoek wordt gebruik gemaakt van de methode literatuuronderzoek, dit om een duidelijk beeld te vormen van alle theorie met betrekking tot het probleem en mogelijke oplossingen. Uit de literatuur worden ontwerpprincipes gehaald die als input dienen voor het ontwerp.

Inspirerend Voorbeeld

In het inspirerend voorbeeld wordt door middel van literatuuronderzoek informatie verzameld van andere partijen die voor hetzelfde probleem hebben gestaan als Breedband. Daarbij worden artikelen gebruikt om een beeld te vormen van de aanpak van het probleem door deze partijen.

Ontwerp

Ter onderbouwing van een aantal aspecten van het ontwerp die nog niet eerder zijn geïntroduceerd in het document is literatuuronderzoek gebruikt.

2.2.3. Interviews

In deze scriptie wordt op verschillende plekken gebruik gemaakt van informatie die is verkregen uit interviews. De interviews zijn gehouden volgens de theorie die Grit (2011) beschrijft in zijn boek Projectmanagement. Hieronder is per interview beschreven hoe deze is gehouden en hoe de verkregen informatie is gebruikt.

Om een duidelijk beeld te krijgen van het perspectief "Engineering" en daarbij ook extra informatie over de opdracht te krijgen, is een semi-gestandaardiseerd interview afgenomen bij innovatie-expert Tom van Klinken van Breedband. Het interview is opgesteld met een aantal vragen en onderwerpen waarop is doorgevraagd. De resultaten van dit interview zijn te lezen in 'bijlage A' en verwerkt in paragraaf 'Perspectief vanuit Breedband engineering' van de probleemanalyse. Informatie uit dit interview is ook gebruikt om requirements in te vullen in de Behoeftanalyse.

Om een duidelijk beeld te krijgen van het perspectief "Directie" is een semi-gestandaardiseerd interview afgenomen bij de eigenaar en directeur van Breedband, Dave Aaldering. Het interview is, net als het eerdergenoemde interview, opgesteld met een aantal vragen en onderwerpen waarop vervolgens kon worden doorgevraagd. De resultaten van dit interview zijn te lezen in 'bijlage B' en verwerkt in paragraaf 'Perspectief vanuit Breedband management' van de probleemanalyse.

2.2.4. Deskresearch

Om praktische informatie te vinden die van toepassing is voor Breedband wordt gebruik gemaakt van deskresearch zoals Poortinga (z.d.) beschrijft. In de onderdelen waar deskresearch wordt gebruikt, is in de tekst een verwijzing gegeven naar de betreffende informatie. De informatie die is gebruikt wordt hieronder opgesomd.

- Persoonlijke communicatie;
- Documentatie uit het intranet:
 - Technische informatie over infrastructuur;
 - Informatie over bedrijfsprocessen.

2.2.5. Stakeholderanalyse

Om de stakeholders te bepalen wordt gebruik gemaakt van een stakeholderanalyse beschreven door Schuurmans (2016). Door de stappen van de stakeholderanalyse te doorlopen worden de stakeholders duidelijk en wordt daarbij ook hun rol in het onderzoek bepaald. Resultaten hiervan zijn verwerkt in de behoeftanalyse in paragraaf 'Stakeholdersanalyse'.

2.2.6. MoSCoW analyse

In de Behoeftanalyse worden de behoeftes van stakeholders geprioriteerd volgens de MoSCoW-analyse. De MoSCoW-analyse wordt uitgevoerd volgens de beschrijving van Tamminga (2015). Dit betekent dat requirements worden gelabeld met "Must have", "Should have", "Could have" en "Won't have".

2.2.7. Requirement categorisering

Om requirements in de Behoeftanalyse goed te kunnen behandelen worden ze gecategoriseerd in business-, user- en systeemrequirements zoals Parker (2012) beschrijft. Businessrequirements doelen op behoeftes vanuit de organisatie en geven duidelijkheid omtrent de 'waarom'-vraag. User requirements doelen op de doeleinden van een oplossing en geven duidelijkheid omtrent de 'wat'-vraag. Tot slot zijn er systeemrequirements die beschrijven hoe een oplossing moet worden ingericht en beantwoordt daarom de 'hoe'-vraag.

2.2.8. Reviewtechnieken

Verskillende reviewtechnieken dragen bij aan de kwaliteit van een document zoals Zijlstra (2011) beschrijft in zijn artikel "een kwaliteitsreview verhoogt de kwaliteit meetbaar". Voor deze scriptie is gebruik gemaakt van twee verschillende reviewtechnieken: distributie voor commentaar en kwaliteitsreview.

Voor elke definitieve oplevering is er een distributie voor commentaar geweest. Het document is gedistribueerd naar bedrijfsbegeleider 'Tom van Klinken' en afstudeerbegeleider 'Erik van der Arend'. Zij hebben het document inhoudelijk beoordeeld en voorzien van feedback, die vervolgens is verwerkt tot een verbeterde versie.

Tijdens het opstellen van de probleemanalyse is meerdere keren een kwaliteitsreview uitgevoerd met focus op spel- en grammaticale fouten. De review is uitgevoerd door de onderzoeker zelf.

2.2.9. Aggregatieniveaus

Voor een duidelijk beeld van de context waarin het project zich afspeelt, is het verstandig om vanuit verschillende aggregatieniveaus naar de context te kijken. Om dit toe te passen op het huidige project wordt een drietal aggregaties gebruikt met de bekende naamgevingen. Hieronder zijn de aggregaties opgesomd met een korte beschrijving in welk niveau ze zich bevinden.

- **Macro:** de omgeving op landelijk niveau;
- **Meso:** de omgeving buiten het bedrijf, klanten en leveranciers;
- **Micro:** directe omgeving waarin het project zich afspeelt en waar de interventie plaatsvindt.

In paragraaf 4.2.1 van de contextanalyse wordt elke aggregatie uitgewerkt en worden de invloeden daarvan op het project bepaald.

2.2.10. DESTEP-analyse

Om Macro-omgeving in paragraaf 4.2.1 van de contextanalyse te kunnen analyseren wordt gebruik gemaakt van de DESTEP-analyse zoals de IMU (2016) dit beschrijft. De DESTEP-analyse is gericht op marketingplannen, maar kan voor dit onderzoek meer informatie bieden over de externe omgeving van het onderzoek. Om de informatie relevant te houden zijn niet categorieën van factoren benoemd, maar slechts de categorieën die daadwerkelijk impact kunnen hebben op het onderzoek.

2.2.11. GOKIT

Het GOKIT-model (ook wel TGKIO genoemd) wordt gebruikt om aspecten van projecten in te delen in gerichte categorieën. Die categorieën zijn: Geld, Organisatie, Kwaliteit, Informatie en Tijd. In de Contextanalyse worden randvoorwaarden ingedeeld volgens deze categorieën op basis van de beschrijving van Grit (2016).

2.2.12. Bronbeoordeling

Om de betrouwbaarheid van de literatuur vast te stellen, wordt gebruik gemaakt van een vorm van bronbeoordeling wat is afgeleid uit een artikel van de Rijksuniversiteit Groningen (2018). In deze methode worden bronnen beoordeeld op de onderstaande punten, om zo een mate van betrouwbaarheid te bepalen.

- Auteur: wat is de achtergrond van de auteur omtrent het onderwerp?
- Doel: is de bron objectief, of is het reclame?
- Actualiteit: is de informatie nog steeds relevant?
- Versie: is de bron herzien of geredigeerd?
- Referenties: wordt de informatie herleid uit andere bronnen?
- Overeenkomsten: komt de informatie overeen met soortgelijke bronnen?
- Satire: is de bron als waarheid bedoeld, of als satire?

Bronnen die zijn gebruikt in het literatuuronderzoek zijn door deze methodiek beoordeeld. De beoordeling van de eerste zes punten wordt per bron weergegeven in bijlage D. Alle bronnen die op punt 7 (satire) afvallen, worden bij voorbaat niet in het document meegenomen. De tabel in de bijlage dient als onderbouwing voor de betrouwbaarheid van gebruikte bronnen. Ongeschikte bronnen zijn op basis van deze methode buiten het document gehouden.

2.2.13. Prototyping

Om de literatuur omtrent een onderwerp te kunnen zoeken en analyseren, is het van belang dat het onderwerp wordt begrepen. Dit is zeker het geval bij technische toepassingen waar het niet compleet duidelijk is welke componenten benodigd zijn. Om de werking van technische componenten te analyseren is het daarom interessant om deze door middel van prototyping beter te begrijpen. In dit literatuuronderzoek is prototyping toegepast zoals beschreven door Dam & Siang (2019), met als doel om lw4o6 beter te begrijpen. Door de beschreven componenten in een prototype op te zetten, is meer duidelijkheid gekomen over extra benodigdheden. Deze extra benodigdheden zijn in het literatuuronderzoek beschreven om meer onderbouwing te bieden voor het ontwerp.

2.2.14. Archimate

Archimate is een breed ondersteunde modelleertool voor het beschrijven van IT-omgevingen. De specificaties van Archimate zijn beschreven door The Open Group (2017) in meest recente versie 3.0. Archimate is gebruikt om de technische informatie van de huidige infrastructuur in kaart te brengen in de contextanalyse. In het ontwerp worden vervolgens de gewenste aanpassingen gedaan en verwerkt in de architectuurplaat.

2.2.15. UML

Om een duidelijk beeld te krijgen van de functies van de uiteindelijke oplossing is een sequence diagram gebruikt aan de hand van UML, de modelleertaal beschreven door Open Management Group (2017). De sequence diagram wordt in het ontwerp gebruikt om de functies en hun taken te weergeven. Op basis van de duidelijk weergegeven functies en taken is het ontwerp van deze functies beschreven.

2.2.16. Multicriteria-analyse

Voor het vergelijken van verschillende IPv6 transitie technieken is een multicriteria-analyse uitgevoerd zoals beschreven door Janse (2018). De analyse is uitgevoerd met criteria relevant voor transitie technieken. De uitwerking van de analyse is te lezen in bijlage M. De resultaten zijn verwerkt in het literatuuronderzoek (4.3.1).

2.3. Afwijkingen

Gedurende het onderzoek is gebleken dat praktische informatie over lw4o6 slecht vindbaar is. Dit resulteerde in een moeizame start van het literatuuronderzoek. Om dit proces te verbeteren is een afwijking toegevoegd op de aanpak, waarin prototyping is gebruikt om de praktische informatie over lw4o6 in kaart te brengen. Dit is gedaan door vroeger te beginnen met het prototype voor het ontwerp, waardoor het prototype parallel loopt aan het opstellen van het literatuuronderzoek, inspirerend voorbeeld en het ontwerp zelf. Dit heeft gezorgd voor het iteratieve aspect van het prototype en hiermee is meer sturing gegeven aan het onderzoek.

3. Probleemanalyse

De probleemanalyse definieert het probleem voor het onderzoek. In de probleemanalyse worden de resultaten benoemd, die vervolgens worden verwerkt tot een conclusie.

3.1. Resultaten

Op basis van verschillende methodieken is informatie gewonnen. In dit hoofdstuk wordt de gewonnen informatie gestructureerd weergegeven om een goed beeld te creëren van het probleem. Allereerst wordt het probleem kort beschreven op basis van literatuuronderzoek, vervolgens worden meerdere perspectieven op dit probleem beschreven. Per perspectief wordt de blik op het probleem, en de overwegingen voor een potentiële oplossing, beschreven.

3.1.1. Probleem

Breedband is een Internet Service Provider (ISP) en heeft daarom als corebusiness het leveren van internetdiensten. Dit doen ze door een eigen netwerk te onderhouden en klanten hierop aan te sluiten. Over het netwerk, net als de rest van het wereldwijde internet, wordt veelal gewerkt met internetprotocol versie 4 (IPv4). Het is al langer bekend dat het aantal bruikbare adressen binnen IPv4 opraken. Hiervoor is een oplossing nodig. Het antwoord op dit probleem is al bekend, namelijk internetprotocol versie 6 (IPv6). IPv6 en IPv4 kunnen standaard niet met elkaar samenwerken en worden daarom vaak naast elkaar gebruikt, dit wordt 'Dual stack' genoemd. Het probleem daarbij blijft dat er IPv4 adressen worden gebruikt en het grootste deel van het verkeer via IPv4 gaat. In een gesprek stelt Tom van Klinken dat, "om het gebruik van IPv4 adressen te beperken, Breedband op zoek is naar een oplossing voor een IPv6-transitie" (persoonlijke communicatie, 10 april 2019). Door een eerder niet-gedocumenteerd kort onderzoek door Breedband is interesse gewekt in de techniek 'lw4over6' (RFC7596) (Cui, et al., 2015). Breedband heeft daarom gericht gevraagd naar een haalbaarheidsrapport van de toepassing van de transitie techniek 'lw4over6'.

3.1.2. Perspectieven

Voor een objectieve beschrijving van het probleem wordt de probleemstelling bekeken vanuit verschillende perspectieven volgens de methode 'triangulatie' beschreven in paragraaf 2.2.1. Een drietal perspectieven zijn gevonden: engineering, management en literatuur. De eerste twee worden bepaald aan de hand van interviews en deskresearch, waar het perspectief uit de literatuur wordt onderbouwd door literatuuronderzoek.

Perspectief vanuit Breedband engineering

Volgens Tom van Klinken (bijlage A) worden vanuit engineering twee problemen gezien: het schaarser en daardoor steeds duurder worden van de IPv4 adressen en de wens om meer IPv6 uit te rollen. Op dit moment worden deze problemen alleen aangepakt met Dual Stack en het gebruik van een voorraad IPv4 adressen. Een oplossing zoals 'lw4over6' pakt beide problemen aan door het opsplitsen van IPv4 adressen voor effectiever gebruik van de adressen, terwijl IPv6 native wordt ondersteund.

Perspectief vanuit Breedband management

Volgens Dave Aaldering uit een interview (bijlage B) is het niet belangrijk vanuit het management welke oplossing wordt gebruikt. Het is vooral belangrijk dat klanten volop gebruik kunnen blijven maken van de diensten. IPv4-exhaustion betekent voor een ISP dat het minder IPv4 adressen kan leveren aan klanten. Met onvoldoende adressen zou het betekenen dat bestaande klanten niet kunnen worden bediend bij groei, en nieuwe klanten überhaupt niet kunnen worden bediend. In commercieel opzicht betekent dit dat IPv4-exhaustion de groei van Breedband belemmert.

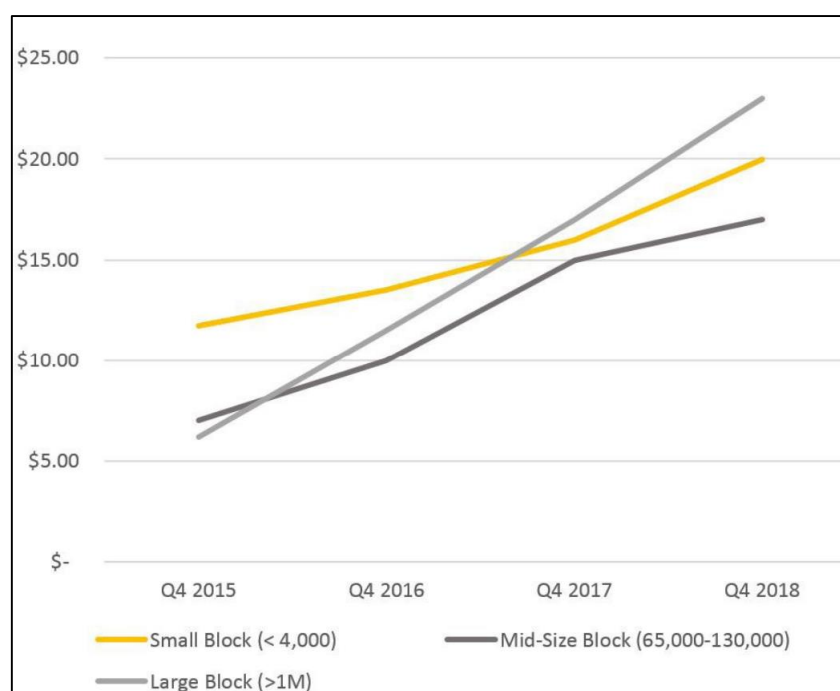
Er is geen beleid om klanten naar IPv6 te pushen. IPv6 wordt nu alleen op aanvraag geboden. Dit is vooral omdat klanten het nog niet helemaal begrijpen. De pijn van IPv4-exhaustion wordt nu opgevangen door de ISP's, de klanten zelf merken hier nog niet veel van. Klanten zullen hier zelf ook niet zomaar wat aan doen omdat zij zelf de pijn niet voelen. "Als het niet kapot is, gaan ze het niet repareren", aldus Dave Aaldering in het interview (bijlage B). Dit is vooral gericht op consumenten en Mkb'ers. Grote organisaties die zelf verantwoordelijk zijn voor de inkoop van IP-adressen, hebben de implementatie van IPv6 vaak wel op orde.

Als ISP moet je zuinig omgaan met IPv4-adressen. De kosten van IPv4-adressen stijgen, waardoor bedrijven met diepe zakken meer macht hebben in de IPv4 markt. Het is daarom van belang om hier een oplossing voor te hebben zodat je ook als kleinere ISP kunt blijven concurreren in de markt.

IPv6-transitie-technieken worden soms als tijdelijk gezien, totdat IPv6 volledig geïmplementeerd is. Alleen zoals Aaldering quote in zijn interview (bijlage B): "niets is zo permanent als een tijdelijke oplossing". Er moet dus een oplossing worden gevonden die op lange termijn mee kan.

Perspectief vanuit de literatuur

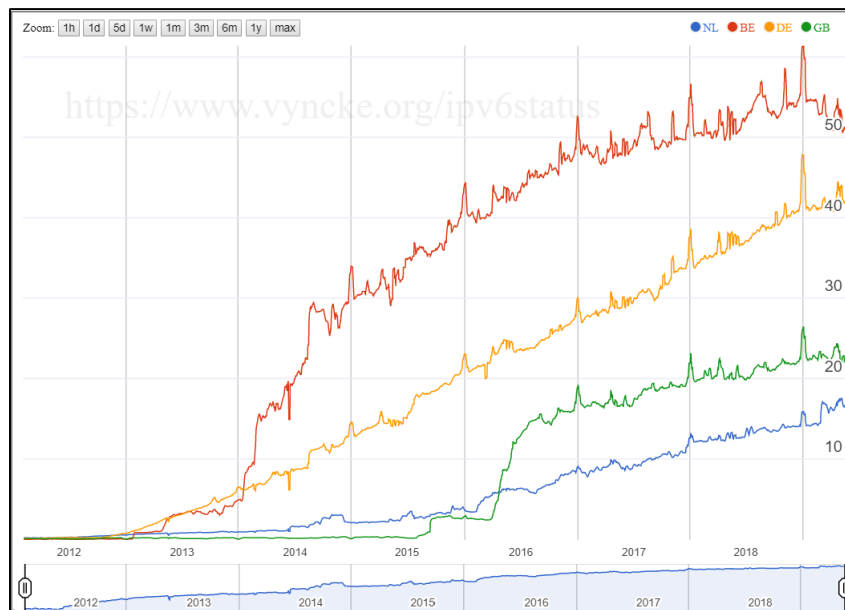
Vanuit de literatuur is het probleem al jaren breed bekend. "IPv4-exhaustion" is al een bekende term sinds 1992 (NFWare, 2018). Sindsdien zijn er al verschillende methodes toegepast om het verbruik van IPv4 adressen te verminderen. In 1994 is al begonnen met een vervanger voor IPv4, wat later IPv6 werd genoemd. De meest recente versie van IPv6 is in 2006 gepubliceerd (RFC4291) (Hinden & Deering, IP Version 6 Addressing Architecture, 2006). Ondertussen zijn Regional Internet Registries (RIR's) aangesteld om de verdeling van IPv4 adressen te reguleren. Sinds 2005 zijn er vijf RIR's: RIPE, APNIC, ARIN, LACNIC en AFRINIC. In 2011 hebben zij allen een laatste IPv4 "/8-block" toegewezen gekregen (McCarthy, 2018). Door het gebrek aan vrije publieke IP-adressen stijgt de prijs van een IPv4-adres aanzienlijk, zoals te zien in Figuur 2 (Avenue4 LLC, 2019).



Figuur 2. IPv4 prijstrends

Noot. Herdrukt van "2018 State of the IPv4 Market" van Avenue4 LLC, (2019, 22 maart), p. 5. Geraadpleegd van: <http://avenue4llc.com/wp-content/uploads/2019/03/Avenue4-2018-State-of-the-IPv4-Market.pdf>

IPv6 wordt gezien als de oplossing voor IPv4-exhaustion. IPv6 is echter niet zomaar wereldwijd geïmplementeerd. Een apparaat dat via IPv6 communiceert kan (native) niet communiceren met een ander apparaat dat via IPv4 communiceert. Dit wordt gezien als een gebrek aan "Backwards compatibility" van IPv6, maar volgens het rapport "State of IPv6 Deployment" van Internet Society (2017), een gebrek aan "Forwards compatibility" van IPv4. Voordat het internet IPv6 als standaard krijgt, moet dus de hele wereld over zijn op IPv6. Dit kan dus alleen door zo langzamerhand IPv6 te implementeren, naast IPv4. Dit lost echter niks op binnen afzienbare tijd, omdat nieuwe gebruikers ook IPv4 nodig gaan hebben. De voortgang van IPv6 deployment van Nederland en verschillende buurlanden is in de grafiek in Figuur 3 te zien. Waar de X-as het tijdsverloop weergeeft, en de Y-as het percentage van browsers die IPv6-enabled zijn laat zien.



Figuur 3. IPv6 adoptie op basis van IPv6 webbrowsers (Google).

Noot. Herdrukt van "Comparison of IPv6 IPv6-Enabled Web Browsers (courtesy Google) in Different Countries", door Vyncke. 2019, 21 mei. Geraadpleegd van <https://www.vyncke.org/ipv6status/compare.php?metric=p&countries=nl,be,de,gb>

Niet iedereen ziet IPv6 als een oplossing. Bernstein (z.d.) beschrijft in zijn artikel 'The IPv6 mess' over de problemen die IPv6 met zich mee brengt en waarom IPv6 daarom geen geschikte oplossing is voor IPv4-exhaustion. Zo worden drie onderdelen aangestipt: incompatibiliteit, onsamenhangendheid en de afleiding. Met incompatibiliteit wordt bedoeld dat IPv4 en IPv6 niet samen kunnen werken. Dit omdat IPv6 is ontwikkeld als 'alternatief' op IPv4, in plaats van 'extensie' op IPv4. De onsamenhangendheid betekent dat er geen samenhang is in de systemen die IPv6 moeten gaan gebruiken. Er wordt in steeds meer systemen aangeraden om IPv6 te implementeren, maar het wordt niet verplicht. Zolang er nog een gedeelte op IPv4 werkt, kan nooit succesvol worden overgegaan op IPv6. De afleiding doelt op de focus. De focus op uitbreiding van IPv6 sites is niet de oplossing. Zolang niet alles op IPv6 bereikbaar is, zal het nooit IPv4 vervangen.

3.2. Conclusie

Wanneer de perspectieven op het probleem worden gecombineerd kan worden gesteld dat Breedband een oplossing nodig heeft voor het bekende probleem "IPv4-exhaustion". Een oplossing is vanuit meerdere afdelingen binnen Breedband gewenst. De afdeling "Engineering" is hier natuurlijk het meest bij gebaat. De belangrijkste knelpunten zijn het gebruik van IPv4-adressen, de daarbij horende kosten en het beheer van een IPv4- én een IPv6-netwerk. De bekende "oplossing" die wordt gesteld vanuit de literatuur is "IPv6", daarom wordt in het onderzoek de aanname aangehouden dat IPv6 de vervangende standaard wordt van IPv4. De weg naar wereldwijd gebruik van IPv6 is niet zomaar afgelegd. Er is een manier nodig om de uitfasering van IPv4 te overbruggen. Om het probleem af te bakenen, zodat het zo veel mogelijk sturing kan geven aan het onderzoek, is een onderzoeksvraag opgesteld. Er zijn vervolgens een aantal deelvragen opgesteld die de informatie verzamelen die nodig is om de onderzoeksvraag te kunnen beantwoorden.

3.2.1. Onderzoeksvraag

De strekking van het onderzoek is het bepalen hoe Breedband de dreiging van IPv4-exhaustion kan beperken en wat daarvan de haalbaarheid is. Dit is het best af te bakenen met de volgende onderzoeksvraag:

"Hoe kan Breedband de dreiging van IPv4-exhaustion beperken totdat IPv6 de standaard wordt?"

3.2.2. Deelvragen

Hieronder zijn de deelvragen weergegeven. Per deelvraag is beschreven op welke manier de deelvraag zal worden onderzocht en welke vorm het resultaat van de deelvraag zal hebben.

1. Wat is het probleem met IPv4 voor Breedband?

Deze deelvraag is gericht op het duidelijk maken van het probleem wat Breedband op dit moment heeft en waarom de oplossing nodig is. Dit is onderzocht in de probleemanalyse en is dan ook beantwoord in deze conclusie.

2. Welke eisen moeten worden gesteld aan een oplossing voor het probleem?

Deze deelvraag kijkt naar de eisen en wensen van Breedband zelf. De vraag is welke eisen worden precies gesteld vanuit het bedrijf zelf en misschien ook vanuit de klant. De deelvraag wordt beantwoord in een behoeftanalyse en zal resulteren in een lijst requirements voor een oplossing.

3. Hoe ziet de huidige infrastructuur eruit waarop de oplossing moet worden geïmplementeerd?

Deze deelvraag wil duidelijk maken wat de omgeving is waar het probleem zich bevindt en waar rekening mee moet worden gehouden bij het bedenken van een oplossing voor dit probleem. De deelvraag zal worden beantwoord met een contextanalyse en resulteren in een aantal randvoorwaarden die worden meegenomen in het ontwerp.

4. Hoe biedt IPv6 een oplossing voor de gebreken van IPv4?

Deze deelvraag richt zich op het duidelijk maken van de IPv6 transitietechniek die misschien de oplossing kan zijn voor het probleem. Deze deelvraag wordt beantwoord in de vorm van een literatuuronderzoek dat resulteert in ontwerpprincipes die worden meegenomen in het ontwerp.

5. Hoe kan IPv6 worden bereikt door middel van 'lw4over6'?

Deze deelvraag richt zich op de transitietechniek die het bedrijf voor ogen heeft. De manier waarop de techniek werkt en hoe deze in theorie wordt toegepast. Deze deelvraag wordt beantwoord in de vorm van een literatuuronderzoek dat resulteert in ontwerpprincipes die worden meegenomen in het ontwerp.

6. Welke alternatieve manieren zijn er om van IPv4 naar IPv6 te migreren?

Deze deelvraag kijkt naar de alternatieve strategieën die kunnen worden gebruikt om van IPv4 te migreren naar IPv6. Hiermee kan de strategie die gewenst is vanuit de opdrachtgever, worden vergeleken met alternatieven. Deze deelvraag wordt beantwoord in de vorm van een literatuuronderzoek dat resulteert in ontwerpprincipes die worden meegenomen in het ontwerp.

7. Welke eventuele risico's zijn er tijdens of na een migratie?

Deze deelvraag kijkt naar de risico's van een migratie naar IPv6. Op basis van risico's die bekend zijn in de literatuur kunnen problemen worden herkend en eventuele oplossingen worden gevonden. De deelvraag wordt behandeld in het literatuuronderzoek en zal resulteren in een beschrijving van de risico's en hoe deze kunnen worden ontweken. Dit resulteert in ontwerpprincipes die worden meegenomen in het ontwerp.

8. Hoe wordt lw4over6 toegepast door andere partijen?

Deze deelvraag kijkt naar andere partijen die voor hetzelfde probleem hebben gestaan. Wellicht wordt hier kennis gewonnen om sturing te geven aan de oplossing voor Breedband. De deelvraag wordt beantwoord in het onderzoek als inspirerend voorbeeld en zal resulteren in aanvullende randvoorwaarden voor het ontwerp.

9. Wat is nodig om de nieuwe oplossing technisch te implementeren?

Deze deelvraag wordt beantwoord in de vorm van een ontwerp. Het ontwerp wordt opgesteld op basis van de transitie techniek die uit het literatuuronderzoek als beste komt. Alle kennis die is opgedaan bij voorgaande vragen en het onderzoek kan worden gebundeld tot een ontwerp als potentiële oplossing.

10. Hoe kan de werking van de nieuwe oplossing worden bewezen?

Deze deelvraag is gericht op het bewijzen dat het ontwerp doet wat het belooft. Dit wordt gedaan in de vorm van een prototype dat zich kan meten met requirements uit de behoeftanalyse.

4. Vooronderzoek

Om de juiste informatie te vinden voor een succesvol antwoord op alle onderzoeksvragen, is het onderzoek opgedeeld in vier onderdelen. Deze opdeling is gebaseerd op de procesaanpak beschreven in hoofdstuk 2.1.

4.1. Behoeftanalyse

De behoefteanalyse is een onderdeel van het onderzoek dat de eisen en behoeften duidelijk maakt voor de oplossing. In de behoefteanalyse worden de resultaten benoemd, die vervolgens worden verwerkt tot een conclusie.

4.1.1. Resultaten

De behoefteanalyse doelt op het beantwoorden van deelvraag 2:

“Welke eisen moeten worden gesteld aan een oplossing voor het probleem?”

Om hier antwoord op te geven, zijn eerst alle stakeholders bepaald. Uit informatie verkregen van deze stakeholders zijn vervolgens de relevante requirements gefilterd. De stakeholderanalyse wordt uitgevoerd aan de hand van de methodiek beschreven in paragraaf 2.2.5.

Stakeholdersanalyse

De relevante stakeholders zijn bepaald door een initiële lijst met alle betrokkenen op te stellen. De betrokkenen zijn vervolgens geverifieerd in een gesprek met opdrachtgever Tom van Klinken (Persoonlijke communicatie, 3 juni 2019). Vervolgens zijn de betrokkenen gefilterd tot een lijst met stakeholders.

Stakeholder	G/I	Positie	Belang	Invloed	Categorie
Tom van Klinken	Individu	Primair	Zeër hoog	Zeër hoog	Belangrijke speler
Senior Engineers	Groep	Primair	Zeër hoog	Hoog	Belangrijke speler
Directie	Groep	Primair	Hoog	Hoog	Belangrijke speler
Engineers	Groep	Secundair	Hoog	Matig	Belanghebbende
Servicedesk	Groep	Secundair	Hoog	Matig	Belanghebbende
Bedrijven (klanten)	Groep	Secundair	Matig	Matig	Toeschouwer
Consumenten (klanten)	Groep	Secundair	Matig	Laag	Toeschouwer

Tabel 4. Stakeholdertabel

Voor een duidelijk overzicht zijn de stakeholders hieronder ingedeeld in een schematische weergave.



Figuur 4. Stakeholder categorie-indeling

Met de belangrijke spelers uit de stakeholderanalyse is een interview gehouden over de wensen voor een oplossing. Interview met Dave Aldering, de vertegenwoordiger van de stakeholdergroep 'Directie', is te lezen in bijlage B. Interview met Tom van Klinken is te lezen in bijlage A. Tom van Klinken is naast opdrachtgever ook vertegenwoordiger voor de groep 'Senior Engineers'.

4.1.2. Conclusie

De behoefteanalyse geeft focus aan het project door duidelijk te maken wie de belanghebbenden zijn en wat zij verwachten van dit onderzoek. Om dit zo duidelijk mogelijk te maken zijn in dit hoofdstuk eerst de belangrijkste stakeholders opgesomd met een korte beschrijving van wat hun belangen zijn in het project. De duidelijke vertaling van al hun belangen in een lijst met requirements is een afsluitende paragraaf. In deze lijst zijn de requirements onderverdeeld in business- user- en systemrequirements, en zijn ze geprioriteerd aan de hand van MoSCoW.

Stakeholders

In dit hoofdstuk zijn de stakeholders gefilterd tot een lijst van de belangrijkste drie, op basis van hun niveau van belang en invloed uit de stakeholderanalyse. De stakeholders zijn hieronder opgesomd met een korte beschrijving van hun uitgangspunten.

- **Tom van Klinken;**
Als opdrachtgever heeft Tom van Klinken het meeste belang bij en invloed op het onderzoek. Zijn doel is om het IPv4-gebruik te verminderen en het beheer van het netwerk te beperken door een native IPv6 netwerk te ontwerpen waar IPv4 alleen als service wordt aangeboden.
- **Senior engineers;**
De senior engineers zijn de personen die uiteindelijk het netwerk gaan beheren. Wanneer problemen ontstaan met het netwerk moeten zij dit gaan oplossen. Hun belang is voornamelijk gericht op het technische aspect waarin beheerbaarheid centraal staat.
- **Directie.**
De directie van Breedband heeft de focus liggen op het beperken van de kosten van IPv4 zonder dat dit impact heeft op de klanten en de service. Behalve het beperken van de kosten, is het ook van groot belang dat de oplossing de groei van het bedrijf en ook van klanten, kan stimuleren.

Requirements

Vanuit de probleemanalyse is een deelvraag gesteld die is gekoppeld aan de behoefteanalyse. De deelvraag wordt beantwoord met de onderstaande requirements.

“Welke eisen moeten worden gesteld aan een oplossing voor het probleem?”

Voor het bepalen van de eisen, worden de wensen van stakeholders vertaald naar een lijst met requirements. De wensen van de stakeholders zijn duidelijk gemaakt in de interviews (bijlage A en bijlage B). De requirements zijn vervolgens gefilterd, S.M.A.R.T.-geformuleerd, geprioriteerd en ingedeeld in drie tabellen om scheiding te maken tussen de categorieën. Deze indeling van de requirements gebeurt aan de hand van de methodieken beschreven in 2.2.6 en 2.2.7.

#	Requirement (S.M.A.R.T.)	Prioriteit	Stakeholder
B01	Er komt een ontwerp dat de toepassing van de gewenste oplossing beschrijft.	Must have	Tom van Klinken
B02	Er komt een prototype dat de werkzaamheid van het ontwerp kan weergeven.	Must have	Tom van Klinken
B03	Er komt een haalbaarheidsrapport dat de haalbaarheid van de toepassing van lw4o6 binnen Breedband aantoont.	Must have	Tom van Klinken
B04	De oplossing beperkt de groeibelemming van IPv4-exhaustion.	Must have	Directie
B05	De klant ondervindt geen last van een implementatie van de oplossing.	Should have	Directie
B06	De oplossing is open source.	Could have	Tom van Klinken

Tabel 5. Business requirements

#	Requirement (S.M.A.R.T.)	Prioriteit	Stakeholder
U01	De oplossing is volledig compatible met het IPv4-internet.	Must have	Tom van Klinken
U02	De oplossing beperkt het gebruik van IPv4 adressen.	Must have	Tom van Klinken
U03	De CPE van de oplossing ondersteunt IPv6 in het LAN-netwerk.	Could have	Tom van Klinken
U04	De CPE van de oplossing ondersteunt IPv4 in het LAN-netwerk.	Must have	Tom van Klinken
U05	De CPE van de oplossing is benaderbaar via een public IPv4 adres.	Must have	Tom van Klinken
U06	De werking van de oplossing is inzichtelijk met monitoring-tools.	Could have	Engineering
U07	In het onderzoek worden alternatieven transitie-technieken vergeleken.	Should have	Tom van Klinken
U08	Het prototype toont het ontwerp aan met minimaal vier (virtuele) CPE's.	Should have	Tom van Klinken
U09	De oplossing ondersteunt telefonie via de CPE.	Should have	Tom van Klinken

Tabel 6. User requirements

#	Requirement (S.M.A.R.T.)	Prioriteit	Stakeholder
S01	Het ISP-netwerk is IPv6-gebaseerd.	Should have	Tom van Klinken
S02	De oplossing werkt in combinatie met Cisco-routers.	Could have	Tom van Klinken
S03	De CPE ondersteunt UPnP.	Should have	Tom van Klinken
S04	Er is geen SPOF in het access netwerk.	Should have	Tom van Klinken

Tabel 7. System requirements

4.2. Contextanalyse

De contextanalyse beschrijft de context waarin het onderzoek wordt uitgevoerd. Daarbij worden randvoorwaarden duidelijk ten behoeve van de oplossing. In de contextanalyse worden de resultaten benoemd, die vervolgens worden verwerkt in een conclusie.

4.2.1. Resultaten

De contextanalyse doelt op het beantwoorden van deelvraag 3:

"Hoe ziet de huidige infrastructuur waarop de oplossing moet worden geïmplementeerd eruit?"

Voor een methodische beschrijving van de context wordt gekeken naar drie aggregatieniveaus zoals beschreven in paragraaf 2.2.9.

Macro

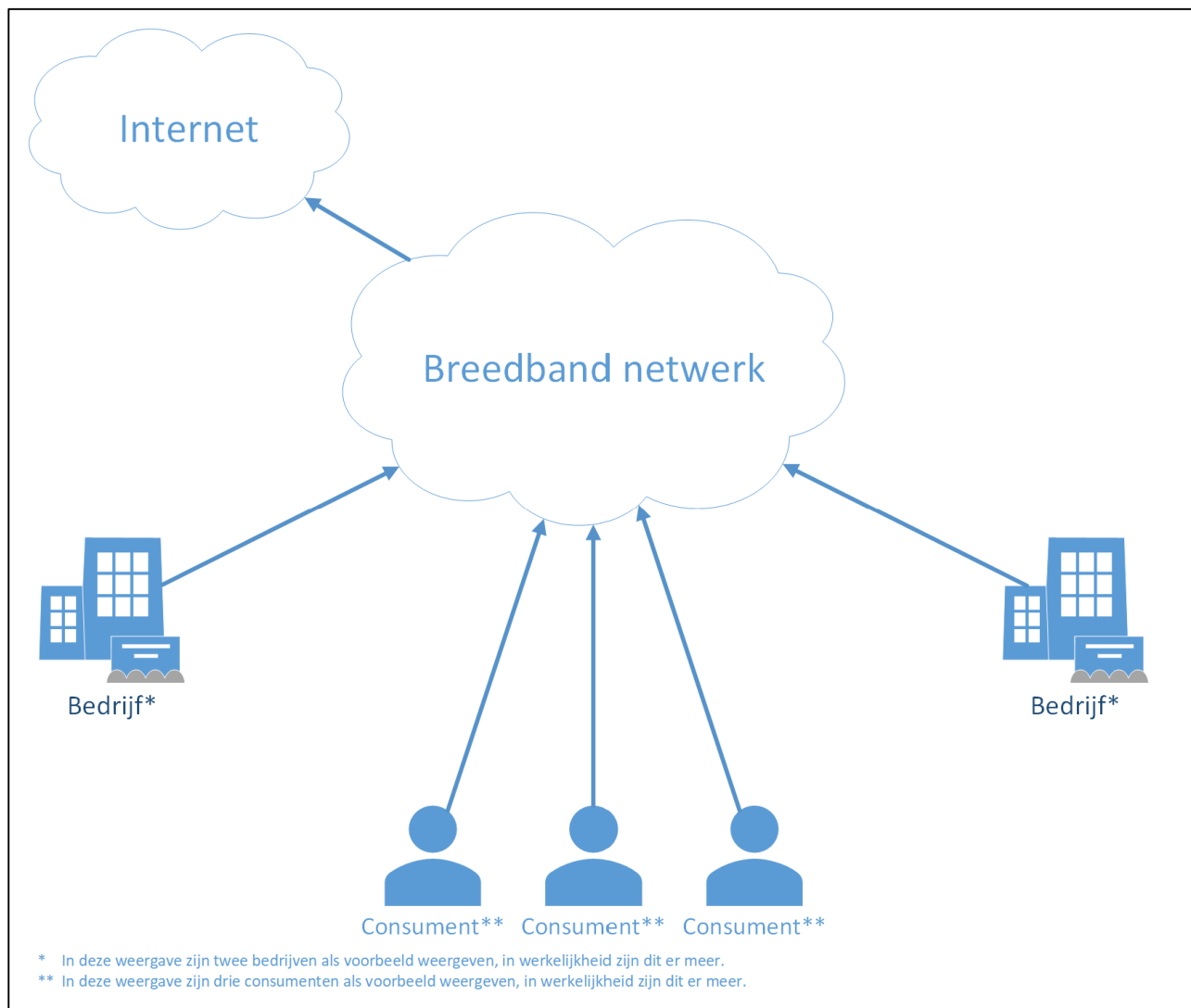
Voor een duidelijke beschrijving van de macro-omgeving worden verschillende factoren beschreven door middel van de DESTEP-methode zoals beschreven in paragraaf 2.2.10. Niet alle factoren resulteren in relevante gegevens. Daarom zijn hieronder alleen de relevante factoren uitgewerkt.

DESTEP	Omschrijving
Demografische factoren	Er zijn geen relevante demografische factoren gevonden voor dit onderzoek.
Economische factoren	De blijvend stijgende kosten van IPv4-adressen zijn een bedreiging voor Breedband. De gemiddelde kosten van een IPv4-adres liggen nu rond de \$20 (Howard, 2019). Met de verwachting dat het blijft stijgen, is dit een aanzienlijke bedreiging voor een ISP.
Sociaal-maatschappelijke factoren	Er zijn geen relevante sociaal-maatschappelijke factoren gevonden voor dit onderzoek.
Technologische factoren	In Nederland loopt de implementatie van IPv6 nog achter op buurlanden. Dit komt voornamelijk doordat de grootste ISP's in Nederland IPv6 niet goed ondersteunen (Offerman, Boerman, Davids, & van Duijnhoven, 2018). Dit gat kan worden gevuld door andere ISP's. Dit biedt kansen voor Breedband.
Ecologische factoren	Er zijn geen relevante ecologische factoren gevonden voor dit onderzoek.
Politiek-juridische factoren	De GDPR bepaalt dat IP-adressen worden behandeld als persoonlijke data. Dat betekent dat deze niet zomaar gedeeld kunnen worden. Er is een uitzondering voor alle partijen die betrokken zijn bij het routeren van pakketten van een betreffend IP-adres (Cormack, 2018). Dit is niet van grote impact omdat IPv6 hierin niet afwijkt van de regelgeving omtrent IPv4.
	Vanuit de Europese Unie is een Data Retention Regulation gesteld (Europese Commissie, 2006). Het gebruik van CGN en andere technieken die gebruik maken van het delen van IP-adressen onder meerdere abonnees maken het lastig om aan de regulatie te voldoen (Europol, 2017). Dit vormt een bedreiging voor het project. Er moet rekening worden gehouden met de Data Retention Regulation, zodat hieraan wordt voldaan.

Tabel 8. DESTEP-analyse

Meso

De meso-omgeving van Breedband is een combinatie van de leveranciers en klanten. De leveranciers worden niet bij dit project betrokken, omdat de wijzigingen aan het interne netwerk van Breedband geen impact heeft op de wijze van handelen met de leveranciers volgens Tom van Klinken (persoonlijke communicatie, 11 juni 2019). Tevens zijn eventuele aanpassingen in de infrastructuur niet gebonden aan leveranciers. In de schematische weergave in Figuur 5 is een korte schets gegeven, waarin duidelijk wordt dat bedrijven en consumenten worden aangesloten op het netwerk van Breedband. Breedband faciliteert daarbij een verbinding tussen de klant en het internet. In de beschrijving in paragraaf Micro wordt het Breedband netwerk uitgebreider beschreven.



Figuur 5. Schematische weergave van klantverbindingen Breedband

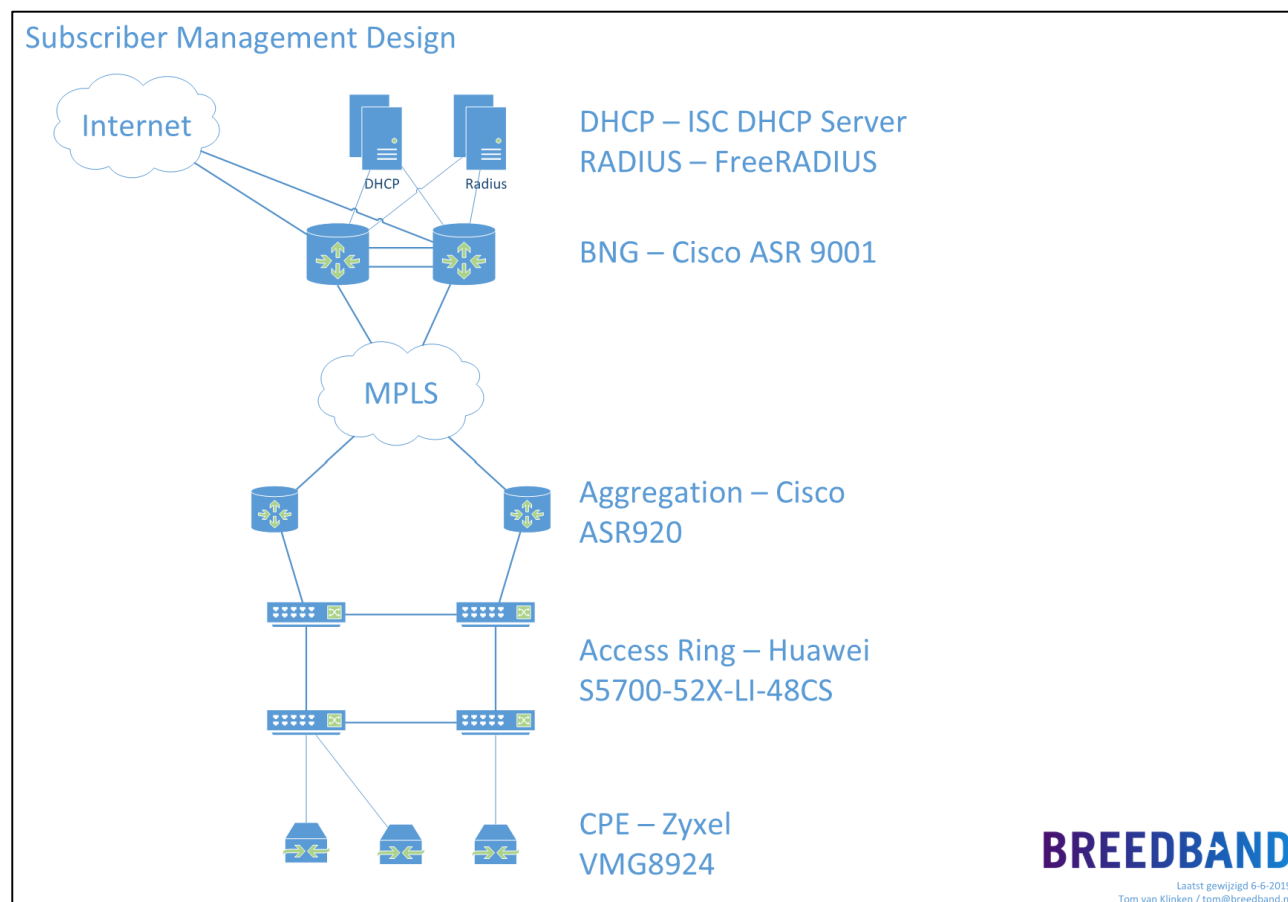
Micro

Breedband bedient met zijn medewerkers en complete netwerk-infrastructuur zijn klanten. Voor het leveren van internetdiensten is het bedrijf ingedeeld in een aantal afdelingen om taken efficiënt te verdelen. De verdeling is te zien in bijlage L. De afdelingen met betrekking tot de opdracht zijn:

- Engineering;
- Research & Development.

Dit omdat deze afdelingen verantwoordelijk zijn voor het inrichten en onderhouden van de technische infrastructuur.

Het belangrijkste praktische aspect van het onderzoek is de infrastructuur van Breedband waarop mogelijk een aanpassing nodig is om de gewenste oplossing te realiseren. De infrastructuur bepaalt het gebruik van IPv4-adressen en daarom de impact van IPv4-exhaustion. De huidige omgeving is weergegeven in Figuur 6.



Figuur 6. Schematische weergave infrastructuur Breedband-consumenten

Noot. Herdrukt van "Subscriber management" door Tom van Klinken¹.

Klanten beschikken over CPE (Customer Premises Equipment), bestaande uit een media-converter en een Zyxel router, die in verbinding staan met de Access Ring van Breedband. De Access Ring wordt door de Aggregation-laag doorgestuurd over een MPLS-netwerk naar de BNG (Broadband Network Gateway). Op de BNG wordt een DHCP-server en een RADIUS-Server beheerd. De BNG voorziet het netwerk van toegang tot het internet (van Klinken, 2019). Een ISP beheert de CPE van consumenten en hierdoor ook het thuisnetwerk van de consument. Consumenten zijn daardoor gemakkelijker te migreren naar een nieuwe oplossing dan zakelijke klanten, die veelal eigen equipment hebben.

¹ Bron afkomstig uit persoonlijke communicatie (6 juni 2019) (niet publiekelijk toegankelijk) met Tom van Klinken.

4.2.2. Conclusie

Met betrekking tot de context is het belangrijkste aspect waarmee rekening moet worden gehouden de technische infrastructuur. De technische infrastructuur is de basis voor het leveren van internetdiensten en moet daarom optimaal blijven draaien. Met deze contextanalyse is de volgende deelvraag te beantwoorden:

“Hoe ziet de huidige infrastructuur waarop de oplossing moet worden geïmplementeerd eruit?”

De directe infrastructuur waarop de oplossing moet worden geïmplementeerd is schematisch weergegeven in Figuur 6. Dit schema is methodisch gemaakt volgens Archimate (beschreven in paragraaf 2.2.14), resulterend in Figuur 7. Er zijn echter weinig harde randvoorwaarden voor de infrastructuur die uit de context zijn bepaald. Het bedrijf bekijkt liever de opties om hun infrastructuur (in de toekomst) aan te passen indien dit voor een betere oplossing kan zorgen. Toch is uit de context een aantal randvoorwaarden te filteren waaraan het ontwerp moet voldoen om succesvol te integreren in de bestaande situatie. De randvoorwaarden zijn ingedeeld volgens het GOKIT-model en hieronder opgesomd:

Geld

- De oplossing moet de stijgende kosten voor de aanschaf van IPv4-adressen beperken.

Organisatie

Er zijn geen randvoorwaarden gesteld in deze categorie.

Kwaliteit

- De oplossing moet over MPLS kunnen worden gekoppeld tussen verschillende fysieke locaties;
- De oplossing moet blijven voldoen aan de Data Retention Policy;
- De oplossing moet blijven voldoen aan de GDPR.

Informatie

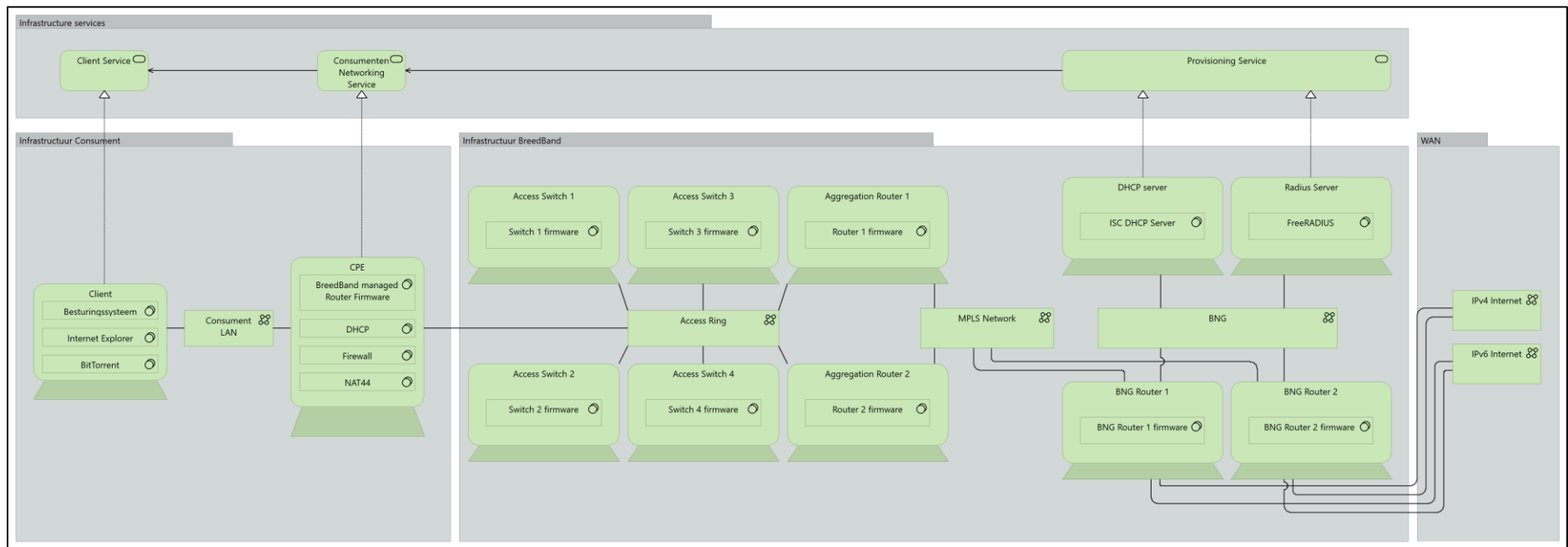
- Alle documentatie gerelateerd aan de oplossing moet worden opgeleverd aan Tom van Klinken.

Tijd

- Het haalbaarheidsonderzoek dient uiterlijk 11 november te worden opgeleverd;
- Het ontwerp dient uiterlijk 11 november te worden opgeleverd;
- De scriptie dient uiterlijk 11 november te worden opgeleverd.

Op basis van het schema van de subscriber management (Figuur 6) door Tom van Klinken (persoonlijke communicatie, 6 juni 2019) is een architectuurplaat opgesteld aan de hand van de Archimate methodiek (paragraaf 2.2.14). De plaat is weergegeven in Figuur 7.

De *Client Service* representeert de infrastructurele service die wordt gerealiseerd door een apparaat van een eindgebruiker. Deze *Client Service* maakt gebruik van de *Consumenten Networking Service* gerealiseerd door de *CPE*. De *CPE* maakt gebruik van de *Provisioning Service* om zijn configuratie te bepalen. De *Provisioning Service* wordt gerealiseerd door de *DHCP* en *Radius server* in de *BNG*. Daardoor kan de *CPE* zijn verkeer over het netwerk van de *Access Ring*, *MPLS* en de *BNG* versturen naar het internet.



Figuur 7. Architectuurplaat Subscriber Management

4.3. Literatuuronderzoek

Het literatuuronderzoek is een onderdeel van het onderzoek dat het theoretisch kader definieert. Het literatuuronderzoek richt zich op ontwerpprincipes die worden meegenomen in het ontwerp van de oplossing. In het literatuuronderzoek worden de resultaten benoemd, die vervolgens worden verwerkt tot een conclusie. Voor het vinden van resultaten is gebruikt gemaakt van een zoekstrategie die is bijgevoegd als bijlage C.

4.3.1. Resultaten

'Lightweight IPv4 over IPv6' (lw4o6) (RFC7596 (Cui, et al., 2015)) is een transitie techniek om het gebruik van IPv6 te stimuleren en het gebruik van IPv4 te beperken. Het is niet de enige oplossing. In het literatuuronderzoek wordt onderzocht wat het einddoel IPv6 precies is. Vervolgens wordt de beoogde oplossing, lw4o6, onder de loep genomen. Tevens wordt er gekeken welke alternatieven er beschikbaar zijn. Tot slot worden de risico's bij een transitie bekeken.

IPv6

Eén van de technische doelen van het onderzoek is het bereiken van een netwerk waarin zo veel mogelijk met IPv6 wordt gewerkt. Maar om duidelijk te krijgen waarom dit relevant is, is het belangrijk om eerst te weten wat IPv6 nou precies is en waarom het zo belangrijk is om zoveel mogelijk IPv6 toe te passen. Deze paragraaf doelt op het beantwoorden van deelvraag 4.

"Hoe biedt IPv6 een oplossing voor de gebreken van IPv4?"

Aanleiding

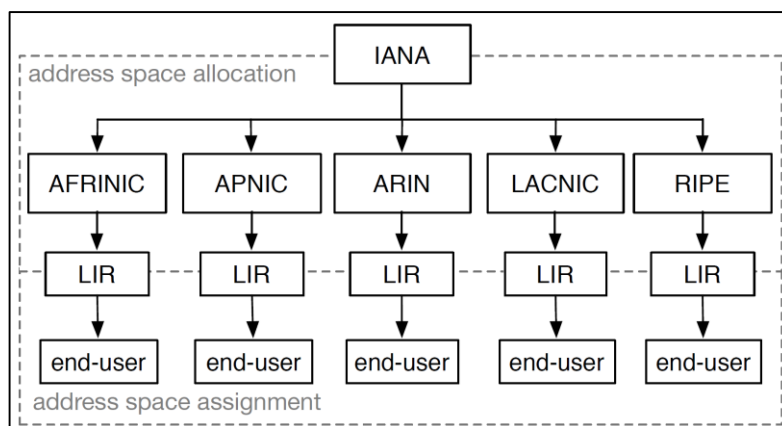
De aanleiding voor het ontwikkelen van IPv6 is het schaarser worden van IPv4 adressen en de problemen die hierdoor ontstaan. IPv4 is ontwikkeld met een 32-bits adresindeling in 4 octetten van 8 bits, genoteerd in decimale waarde (maximale notatie: 255.255.255.255). De 32-bits adresindeling betekent dat in totaal 'slechts' 2^{32} adressen beschikbaar zijn (4,3 miljard) (RFC791 (Postel, 1981)).

IPv4 subnetting

Om de IP-adressen efficiënt te kunnen uitgeven zijn ze ingedeeld in subnetten. Deze subnetten delen een IP-adres op in een netwerk-gedeelte en host-gedeelte. Net als een IPv4-adres, is een IPv4-subnetmask (de notatie voor een subnet) ingedeeld met een 32-bits notatie. Een subnet kan in tegenstelling tot een IPv4-adres alleen bestaan uit een set van opvolgende enen (netwerk-gedeelte) en een set van opvolgende nullen (host-gedeelte). Om IP-adressen efficiënt te verdelen is het van belang om subnetten efficiënt in te delen. Subnetten bevatten van origine drie klassen: klasse A (/8), klasse B (/16) en klasse C (/24). Classless Inter-Domain Routing (CIDR) maakt het mogelijk om af te wijken van de reguliere klassen door bits uit te wisselen tussen het netwerk en host gedeelte, op die manier kunnen subnetten specifiekier worden ingericht om efficiënter om te gaan met adressen (Janssen, z.d.). Het subnetten heeft als gevolg dat IP-adressen worden opgedeeld in groepen. Het inefficiënt indelen van subnets en het creëren van veel kleine subnets resulteert in onnodig IP-gebruik. Te grote subnets hebben vaak ongebruikte IP-adressen die niet worden benut.

IPv4 distributie

Het verdelen van IP-adressen wordt geregeld door de Internet Assigned Numbers Authority (IANA), een organisatie onder Internet Corporation for Assigned Names and Numbers (ICANN). In de begintijd van het internet werden /8-blokken vrij uitgedeeld. IANA kwam er in 1990 al achter dat IPv4-adressen uitputbaar zijn en dat beter toezicht noodzakelijk is om uitputting op korte termijn te voorkomen. Tussen 1990 en 1993 werd beleid RFC1466 (Gerich, 1993) opgesteld voor het beheren van IP-adres uitgave. Tussen 1992 en 2005 zijn verschillende Regional Internet Registries (RIR's) opgericht (RIPE voor Europa) die de uitgave van IP-adressen regionaal beheren onder eigen beleid. RIR's ontvingen van IANA /8-blokken wanneer hun bestaande blok onder een specifiek aantal adressen kwam. De ontvangen adressen verdelen zij onder Local Internet Registries (LIR's) die het uiteindelijk naar eindgebruikers distribueren. LIR's krijgen IP-adressen op basis van het beleid van de RIR waar zij onder vallen. Figuur 8 toont een schematische weergave van de distributie. (Richter, Allman, Bush, & Paxson, 2015)



Figuur 8. Schema voor IP-distributie

Noot. Herdrukt van "A primer on IPv4 scarcity", door Richter, P., Allman, M., Bush, R., & Paxson, V., 2015, *ACM SIGCOMM Computer Communication Review*, 45(2), p. 22.

IPv4 exhaustion

De georganiseerde distributie van IP-adressen heeft de uitputting misschien vertraagd, maar uiteindelijk lost het niks op. De NRO (2011) laat weten dat in februari 2011 IANA haar laatste vijf /8-blokken heeft uitgedeeld (één aan elke RIR). Vanuit een globaal perspectief zijn IP-adressen nu uitgeput. RIRs zijn zuiniger met hun laatste /8-blok door een strakker beleid te voeren. Meer dan het vertragen van de uitputting doet dit niet.

De oplossing

Al in 1990 werd ingezien dat IPv4-adressen uiteindelijk op zouden raken. Er is daarom gelijk gewerkt aan een opvolger; Internet Protocol versie 6 (IPv6), dat beschikbaar is sinds 1996 (Tadayoni & Henten, 2015). De tussenstap, versie 5, is overgeslagen omdat deze versie dezelfde limieten had als IPv4 en niet als doelstelling had om de IP-Adresruimte te vergroten. (Mitchell, 2019).

Werking

IPv6 werkt op veel vlakken hetzelfde als IPv4. Natuurlijk zijn er aanpassingen die het een verbetering maken ten opzichte van IPv4. IPv6 maakt gebruik van een nieuwe address space. Daarnaast worden subnets anders behandeld en is het inrichten van IPv6 adressen versimpeld door de toevoeging van SLAAC.

Address space

Zoals al eerder is benoemd is IPv6 de opvolger van IPv4. IPv6 heeft als focus het vergroten van de address space in het internetprotocol. Hiervoor was te lezen hoe IPv4 was ingedeeld in een 32-bits adresindeling met 4 octetten van 8 bits. IPv6 is ingedeeld in een 128-bits indeling met 8 hexatetten van 16 bits (SolidBE, 2017). De hexatetten worden in adresnotaties weergegeven als een viertal hexadecimale waarden (waar een octet in IPv4 een drietal decimale waarden is). Doordat IPv6 een 128-bits adresindeling heeft, is het mogelijk om 2^{128} adressen op te stellen, dat komt neer op ruim 3,4 sextiljoen adressen (één sextiljoen is een '1' met 36 nullen). Ter illustratie: genoeg om elk persoon op aarde ruim 45 quadriljard IP-adressen te geven, of elke zandkorrel op aarde ruim 3 triljoen IP-adressen.

Subnetting

Net als bij IPv4 wordt bij IPv6 gebruik gemaakt van subnetting. Ten opzichte van IPv4 wordt bij IPv6 alleen de 49^e tot en met de 64^e bit gebruikt voor het verdelen van subnetten (Mukherjee, z.d.). Het 1^e t/m 23^e bit bepaalt de RIR waar het adres van afkomstig is, de 24^e t/m 32^e bepaalt de ISP en de 33^e t/m 48^e bepaalt de site. Alles achter het subnet, de 65^e t/m 128^e bit, is bedoeld voor het host-gedeelte (ook wel interface-ID genoemd) (Deering & Hinden, 2017). In Figuur 9 wordt dit schematisch weergegeven.

Binaire waarde adres	0010101000000011	0100111100000000	0000000000000001	0000000000000000	1001110000100110	0001000101010001	0011101100101000	0101101101000011
Hexadecimale waarde adres	2A03	4F00	0001	0000	9C27	1151	3B28	5B43
Binaire waarde subnet	1111111111111111	1111111111111111	1111111111111111	1111111111111111	0000000000000000	0000000000000000	0000000000000000	0000000000000000
Selectie van bits	1 t/m 23	24 t/m 32	33 t/m 48	49 t/m 64	65 t/m 128			
Doel van bits	Registry	ISP	Site	Subnet	Interface ID			

Figuur 9. IPv6-adres breakdown.

SLAAC & DHCP

Een apparaat dat wil deelnemen aan een IPv4-netwerk moet een IP-adres configureren dat matcht met het IPv4-netwerk. Dat kan handmatig, maar voor gebruiksvriendelijkheid wordt dit ingesteld via een DHCP-server. Een DHCP-server deelt IP-adressen en netwerkinformatie uit aan gebruikers op dat netwerk. In IPv6 is er een extra optie toegevoegd: Stateless Address AutoConfiguration (SLAAC). SLAAC maakt het mogelijk voor een apparaat om zelf een uniek IPv6-adres te genereren. Voor het netwerkgedeelte hiervan wordt gebruikt gemaakt van Router Advertisements (RA) en voor de interface ID wordt het lokale MAC-adres gebruikt. DHCP voor IPv6 (DHCPv6) is dan optioneel om het beheer van adressering alsnog centraal te houden (White, 2017)?

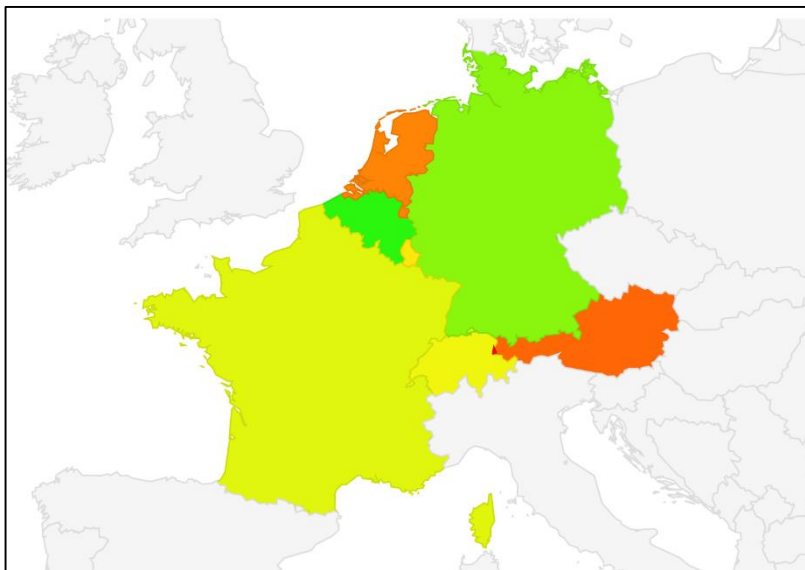
Mate van toepassing

Doordat IPv6 niet kan samenwerken met IPv4 is het noodzakelijk om zoveel mogelijk netwerken ook IPv6-compatible te maken. Het gebruik van IPv4 zal pas afnemen wanneer IPv6 de overhand neemt en dusdanig veel geïmplementeerd is dat het 'de standaard' genoemd kan worden. Dit kan nog lang duren omdat er altijd personen of bedrijven zijn die nog géén IPv6-ondersteuning hebben. Wanneer dan bijvoorbeeld een nieuwe website wordt gelanceerd zonder IPv4-adres, zou die site niet voor iedereen bereikbaar zijn.

IPv6 geschiktheid in West-Europa

Voor de transitie naar IPv6 is het van belang dat zoveel mogelijk netwerken IPv6 ondersteunen. In Figuur 10 is daarvan de voortgang te zien in West-Europa. Het valt op dat Nederland een laag percentage van IPv6-geschiktheid heeft, waar België erg hoog scoort.

- België: 56,22%
- Duitsland: 43,74%
- Frankrijk: 32,41%
- Zwitserland: 30,47%
- Luxemburg: 26,92%
- Nederland: 15,40%
- Oostenrijk: 11,76%



Figuur 10. IPv6 geschiktheid in West-Europa

Noot. Herdukt van "Use of IPv6 for Western Europe (QO)", door APNIC, (2019, 4 juli). Geraadpleegd van <https://stats.labs.apnic.net/ipv6/QO>

België

Vyncke (in McNamara, 2016), co-voorzitter van de IPv6 raad in België, beschrijft een aantal redenen waarom België zo hoog uitvalt. De belangrijkste redenen zijn: IPv4-adressen van nagenoeg alle ISPs in België raakten op. De drie grootste ISPs in België hebben om tafel gezeten met de raad van IPv6 en deelden daar hun status en plannen omtrent IPv6. "Een andere belangrijke reden is dat er een (niet publiekelijke) memorandum van overeenstemming is opgesteld tussen de ISP Association, cyber politie en het ministerie van economische zaken" (Vyncke, in McNamara, 2016). Hierin wordt gesteld dat één IPv4-adres maar onder een maximum van 16 gebruikers kan worden gedeeld. Dit laatste beperkt de toepassing van een groot aantal transitie-technieken waardoor ISP's sneller over willen naar een definitieve IPv6 oplossing.

Nederland

Onderaan de lijst in West-Europa, net boven Oostenrijk, staat Nederland. CEO van Digitale Infrastructuur Nederland (DINL) Michiel Steltman stelt dat dit komt omdat "Nederland al vroeg is begonnen met het opzetten van een sterke IT-infrastructuur" (in Offerman, Boerman, Davids, & van Duijnhoven, 2018). Dit resulteert erin dat er relatief weinig nieuwe systemen bijkomen en de het IPv4-gebruik dus relatief weinig stijgt. Om deze reden zijn de grootste ISP's in Nederland weinig bezig met het uitrollen van IPv6 (Emerce, 2018).

Lightweight 4over6

Door de sturing van de opdrachtgever wordt in het onderzoek vooral gekeken naar de IPv6-transitie techniek "Lightweight 4over6" (RFC7596 (Cui, et al., 2015)). Naast lw4o6 zijn er ook andere transitie-technieken. Doordat lw4o6 ook door andere partijen is toegepast heeft Breedband specifiek interesse in deze techniek. Alternatieve transitie technieken worden alsnog beschreven onder de paragraaf 'Alternatieven'. Deze paragraaf doelt op het beantwoorden van deelvraag 5.

"Hoe kan IPv6 worden bereikt door middel van 'lw4over6'?"

Wat is lightweight 4over6?

Lw4o6 is een extensie op een andere techniek, Dual Stack Lite (DS-Lite) (RFC6333 (Durand, Droms, Woodyatt, & Lee, 2011)). Om lw4o6 duidelijk te beschrijven moet dus eerst worden gekeken naar DS-Lite en hoe deze techniek werkt.

Dual Stack Lite

DS-Lite is een transitie techniek die zich focust op het beschikbaar houden van IPv4-verkeer op een IPv6-netwerk. De techniek is gericht op providers die tegen het probleem aanlopen waarin zowel een IPv4- als een IPv6-netwerk moet worden onderhouden. Hiervoor is een oplossing ontwikkeld die door middel van tunneling IPv4-verkeer van een eindgebruiker kan transporteren over een IPv6 netwerk. Deze techniek stuurt het pakket naar de 'edge' van dit netwerk waar de tunnel eindigt en het pakketje wordt doorgestuurd naar het IPv4 internet (Durand, Droms, Woodyatt, & Lee, 2011).

Om dit te realiseren worden meerdere componenten gebruikt, namelijk B4 (Basic Bridging BroadBand) en een AFTR (Address Family Transition Router), uitgesproken als de Engelse termen 'before' en 'after'.

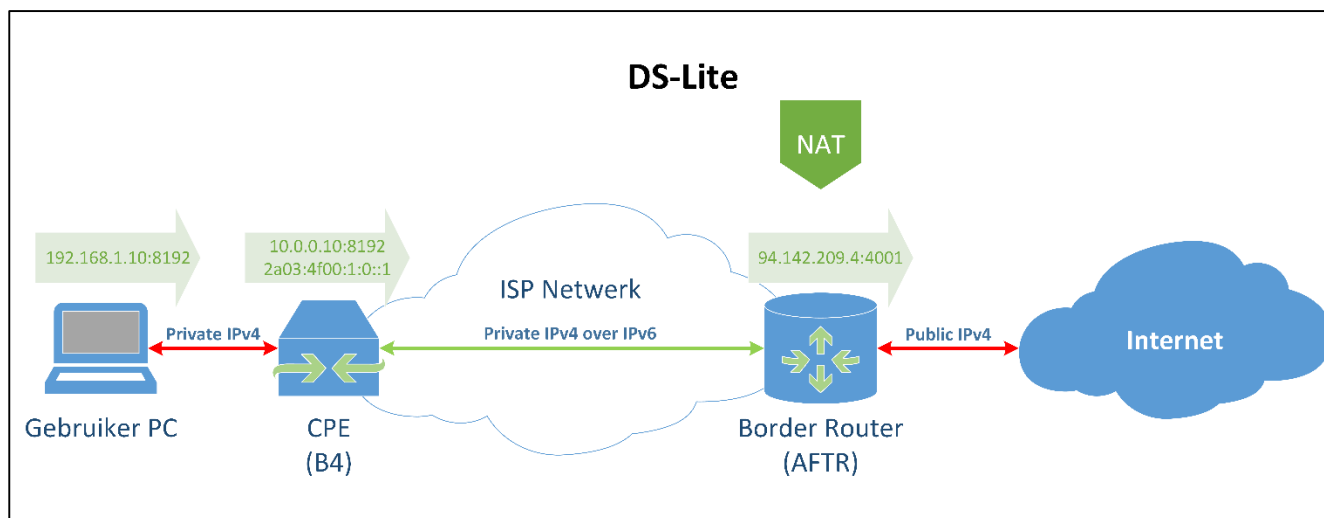
B4

De B4 is een functie die wordt uitgevoerd op de CPE. De B4 pakt IPv4-pakketjes in uit het netwerk van de eindgebruiker en stuurt dit over het IPv6-netwerk van de ISP naar de AFTR.

AFTR

De AFTR is de functie die het pakketje weer uitpakt. Door middel van NAT44 wordt het lokale IPv4-adres vertaald naar een publiek IPv4-adres en wordt het IPv4-verkeer doorgestuurd naar de IPv4-gateway. Daarnaast wordt het IPv6-adres genoteerd in de NAT-binding-table voor het omgekeerde proces.

Een schematische weergave van de functies in DS-Lite is weergegeven in Figuur 11.



Figuur 11. DS-Lite werking - versimpelde weergave

Van DS-Lite naar lw4o6

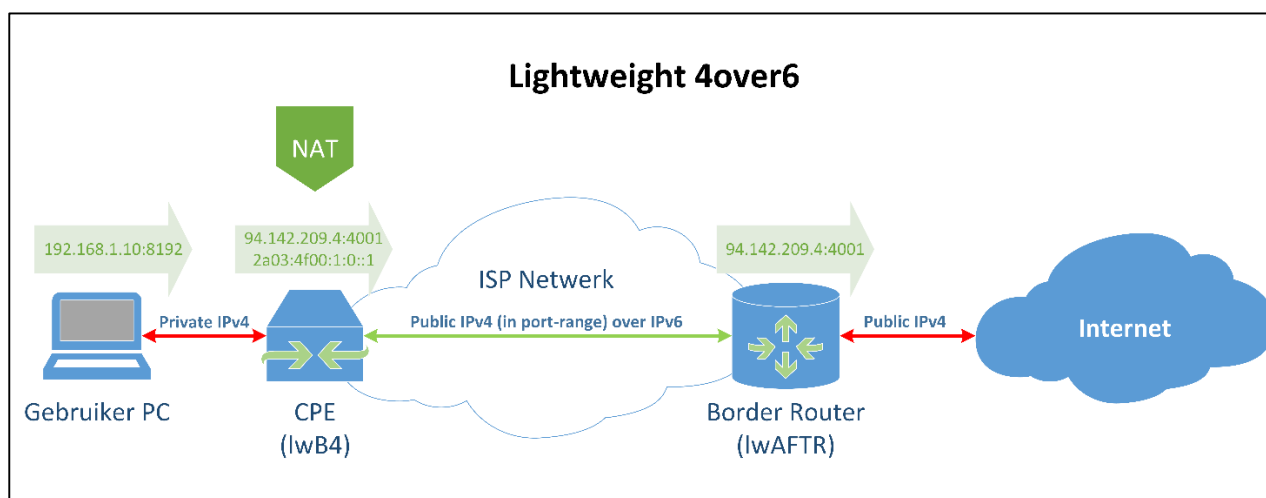
Lw4o6 is een extensie op DS-Lite. Bij lw4o6 wordt de CGN-functie, die bij DS-Lite in de AFTR plaatsvindt, verplaatst naar de CPE waar ook de B4 draait. In lw4o6 worden deze functies hernoemd naar 'Lightweight Basic Bridging BroadBand' (lwB4) en 'Lightweight Address Family Transition Router' (lwAFTR) (Cui, et al., 2015).

LwB4

Op de lwB4 wordt nu naast de tunneling ook de NAT uitgevoerd. Doordat de NAT op de CPE kan worden uitgevoerd, wordt de werkdruk van een lwAFTR per CPE verlaagd. Hierdoor wordt de schaalbaarheid aanzienlijk verhoogd. Verdere werking van de lwB4-functie is uitgelegd in Component: Lightweight B4.

LwAFTR

Op de lwAFTR wordt nu alleen het pakket gecontroleerd in de binding-table. Wanneer deze wordt geaccepteerd, wordt het IPv4 pakket uitgepakt zodat het naar de IPv4-gateway kan worden gestuurd. Verdere werking van de lwAFTR-functie is uitgelegd in Component: Lightweight AFTR.



Figuur 12. Lw4o6 werking - versimpelde weergave

Component: Lightweight B4

De lwB4 is de eerste functie in een lw4o6 setup die de eindgebruiker tegenkomt. De lwB4, zoals beschreven in RFC7596 (Cui, et al., 2015), is een functie die kan worden gedraaid op verschillende manieren maar voornamelijk als een soort routing-functie dient en daardoor het best kan worden gedraaid op een router. De meest voor de hand liggende optie is om de lwB4 te draaien op de gateway tussen klant-netwerk en ISP-netwerk, de CPE. García (García, Dive into Lightweight 4over6, 2017) beschrijft dat hiervoor enkel een tunnel en NAT nodig is en dat dit haalbaar is op OpenWRT, een open source router besturingssysteem (OpenWRT, 2019). Op de lwB4 worden twee functies uitgevoerd ten behoeve van lw4o6, de NAT en encapsulatie van IPv4 in IPv6. Om dit te realiseren heeft de lwB4 een configuratie met de volgende gegevens:

- Een (gedeeld) publiek IPv4 adres;
- Port-set informatie;
- lwAFTR adres.

Gedeeld publiek IPv4 adres

Om uiteindelijk pakketten het IPv4-internet op te kunnen sturen is een publiek IPv4 adres nodig. In lw4o6 worden IPv4-adressen echter gedeeld op basis van poortnummers. Het gedeelde publieke IPv4 adres wordt wel in de router ingesteld. Het gedeelte dat mag worden gebruikt wordt aangeduid in de port-set informatie.

Port-set informatie

Port-set informatie bestaat uit minimaal twee waarden: pslen (Port-set length) en psid (Port-set ID). Het totaal aantal poorten op een IP-adres is 16-bits lang. Dat betekent in decimale weergave 2^{16} , oftewel 65.536. De pslen is vervolgens een waarde tussen 0 en 16 wat het aantal poorten berekend van wat wordt gebruikt in het shared IP-adres. Dat wordt als volgt berekend met voorbeeld pslen = 6:

$$2^{(Max\ bits - pslen)} = 2^{(16 - 6)} = 2^{10} = 1024$$

Het aantal poorten dat wordt gebruikt met een pslen van 6 is dus 1024. Het psid bepaald vervolgens welke poorten tussen 0 en 65536 worden gebruikt.

psid 0	=	Port-set 0-1023
psid 1	=	Port-set 1024-2047
...		...
psid 63	=	Port-set 64512 - 65535

In een reguliere lw4o6 configuratie wordt de eerste psid (0) altijd overgeslagen (García, Dive into Lightweight 4over6, 2017).

LwAFTR adres

Het lwAFTR adres is het IPv6-adres van de lwAFTR waar de lwB4 al zijn IPv4 verkeer, vertaald en verpakt in IPv6, heen stuurt. De lwAFTR is daarna verantwoordelijk voor verdere afhandeling.

Werking

Wanneer een lwB4 een IPv6-pakket ontvangt, wordt deze direct geforward naar de IPv6 gateway. IPv6-pakketten volgen standaard geen route in de lw4o6-setup. Wanneer een lwB4 een IPv4-pakket ontvangt, wordt dit pakket eerst vertaald door middel van NAT44, waarvoor NAPT wordt gebruikt. Het lokale IP-adres met zijn source-port wordt vertaald naar het (gedeelde) publieke IP-adres met een poort uit de port-set als source-port. Dit pakket wordt vervolgens ingepakt in een IPv6-pakket met als destination-adres de lwAFTR die het pakket verder afhandelt (Cui, et al., 2015).

Component: Lightweight AFTR

De lwAFTR, zoals beschreven in RFC7596 (Cui, et al., 2015), is de functie in het netwerk van de ISP die pakketten van de lwB4 ontvangt en omzet naar het IPv4 internet, en vice versa. Om dit te doen voert de lwAFTR twee processen uit: softwire-controle en tunneling.

Softwires

De lwAFTR is een bestemming voor één of meerdere lwB4 apparaten. De lwAFTR heeft als verantwoordelijkheid om alle ingekomen pakketten te controleren of deze daadwerkelijk in de lw4o6 setup zijn meegenomen. Dit doet de lwAFTR door hun source-IPv6-adres te controleren in de softwire-tabel. De softwire-tabel is een tabel met een notatie voor elke lwB4 in de lw4o6 setup. Daarbij zijn de volgende gegevens genoteerd:

- lwB4 IPv6-adres;
- (Gedeelde) publieke IPv4-adres;
- Port-set.

De gegevens in de softwire-tabel zijn hetzelfde als de gegevens in de lwB4 zelf. Wanneer de lwAFTR de gegevens uit het pakket herkent, is het pakket goedgekeurd voor decapsulatie.

Decapsulatie

Tijdens decapsulatie wordt het IPv4 pakket weer uit het IPv6 pakket gehaald, zodat het IPv4 pakket naar de Provider Edge (PE) kan worden gestuurd en zo de server van bestemming kan bereiken.

De lwAFTR functie is nagenoeg stateless, op een softwire-tabel na. De softwire-tabel kan worden ingericht op basis van een provisioning service. Dit resulteert erin dat een lwAFTR gemakkelijk vervangbaar en schaalbaar is.

De lwAFTR functie is momenteel beschikbaar op de open source netwerk toolkit Snabb (Snabbco, 2018).

Component: Provisioning

Om lw4o6 goed te kunnen managen en zo stateless mogelijk in te richten, is provisioning van belang. Het doel van provisioning is:

- lwB4-configuraties distribueren;
- lwAFTR-configuraties bijwerken met een nieuwe software-tabel op basis van lwB4-configuraties.

Softwires

Software is een term waarmee een virtuele draad beschreven wordt. Het vertegenwoordigt een tunnel van een border relay naar een CPE. De term software wordt breder gebruikt in IPv6 transitie-technieken en is dus niet exclusief voor lw4o6. Softwires worden beschreven in RFC8026 (Boucadair & Farrer, Unified IPv4-in-IPv6 Software Customer Premises Equipment (CPE), 2016). Een software bevat de informatie die voor zowel de CPE (in het geval van lw4o6: de lwB4) als de border relay (lwAFTR) nodig is om een tunnel op te zetten. Elke software is geconfigureerd op één CPE en wordt collectief in een tabel gezet, de tabel wordt geconfigureerd op elke border relay. Bij een provisioning service in een lw4o6-omgeving is het van belang dat softwires vanuit een centraal punt worden geconfigureerd en automatisch worden gedistribueerd naar de betrokken functies.

DHCPv6

In een beheerde netwerkomgeving is DHCP vaak nodig voor de configuratie van netwerkadressen. DHCPv6 biedt behalve de standaardfuncties voor het regelen van adressen in een netwerk, ook DHCP-options die specifiek informatie voor lw4o6 configureren. IANA heeft een aantal DHCP-options toegewezen voor transitie-technieken in RFC7598 (Mrugalski, et al., 2015). Voldoende automatisering in provisioning maakt het tevens mogelijk om lwAFTR functies redundant uit te voeren omdat de software-tables tegelijk kunnen worden geüpdatet.

Alternatieven

Lw4o6 is niet de enige manier om de impact van IPv4-exhaustion te beperken en een transitie naar IPv6 te starten. Andere mogelijkheden kunnen de keuze voor lw4o6 onderbouwen, of misschien zelfs een beter alternatief bieden. Deze paragraaf doelt op het beantwoorden van deelvraag 6:

“Welke alternatieve manieren zijn er om van IPv4 naar IPv6 te migreren?”

Mogelijkheden

Naast lw4o6 zijn er een hoop andere IPv6 transitie technieken. Hieronder is een lijst weergegeven met de erkende alternatieve transitie technieken en een korte beschrijving hoe deze werken. Technieken met potentie voor Breedband worden uitgelicht en later in de vergelijking meegenomen.

DS-Lite

DS-Lite is een techniek dat het meest overeenkomt met lw4o6. Dit heeft als reden dat lw4o6 gebaseerd is op de techniek van DS-Lite. DS-Lite is eerder in dit document uitgebreid beschreven (Dual Stack Lite) als basis voor de uitleg van lw4o6. Om die reden wordt dit niet nogmaals beschreven.

4over6

Transit Solution Using IP Encapsulation and MP-BGP Extensions (4over6) is een techniek die zich focust op IPv4-verkeer over een IPv6-verbinding te vervoeren. De taken van 4over6 wordt opgesplitst in de control plane die zich focust op het configureren van de apparaten die een tunnel moeten opzetten, en de data plane die zich focust op het verpakken en transporteren van het netwerkverkeer. Net als de eerdergenoemde technieken DS-Lite en lw4o6 richt 4over6 zich op een tunnel tussen edge-routers, waarin IPv4-verkeer wordt ingepakt in IPv6-verkeer. 4over6 is een voorganger op technieken zoals lw4o6 en DS-Lite, maar is op zichzelf niet verder ontwikkeld en niet geadopteerd voor grootschalig gebruik. De techniek 4over6 is uitgebreid beschreven in RFC5747 (Wu, Cui, Li, & Metz, 2010).

MAP-E/MAP-T

MAP (Mapping of Address and Port) heeft een tweetal varianten, MAP-E (MAP met encapsulation) en MAP-T (MAP met translation). MAP maakt gebruik van NAT op CPE om lokaal IPv4 verkeer om te zetten naar publiek IPv4 met een specifieke port-set. Deze IPv4-packet met port-set informatie wordt verpakt naar een IPv6 adres binnen een MAP-domain zodat het over een IPv6-netwerk kan worden gerouteerd. De border relay van een MAP-implementatie verwerkt dit packet zodat het kan worden doorgestuurd naar het internet. MAP-E wordt beschreven in RFC7597 (Dec, Li, Bao, Matsushima, & Murakami, 2015), MAP-T wordt beschreven in RFC7599 (Li, Bao, Troan, Matsushima, & Murakami, 2015).

4rd

IPv4 Residual Deployment (4rd) is een transitie-techniek die nagenoeg hetzelfde is als MAP. In additie op MAP biedt 4rd transparantie in de IPv4-fragmentatie zodat RFC4821 (Mathis & Heffner, 2007) beschikbaar blijft. Bij 4rd blijven pakket-inspectie functies als DPI of ACLs beschikbaar. 4rd is beschreven in RFC7600 (Despres, Penno, Lee, Chen, & Chen, 2015).

CGN

Carrier Grade NAT (CGN) is een NAT-oplossing die op ISP-niveau wordt toegepast. Door middel van CGN kunnen grote aantallen eindgebruikers achter een enkel IP-adres worden geplaatst. CGN is gericht op het delen van IPv4-adressen onder eindgebruikers. De manier waarop CGN wordt toegepast bepaald of IPv6 wordt ondersteund. Algemene toepassing van een CGN is beschreven in RFC6264 (Jiang, Guo, & Carpenter, 2011).

CGN heeft last van de standaard problemen die komen kijken bij het delen van IP-adressen. Deze problemen staan beschreven in RFC6269 (Boucadair, Durand, Levis, & Roberts, 2011).

464XLAT

464XLAT is een techniek die werkt met twee NAT64 systemen. Op de CPE van een consument wordt CLAT, RFC6146 (Bagnulo, Matthews, & van Beijnum, 2011), toegepast zodat pakketten kunnen worden vervoerd over een IPv6 netwerk. Op de edge van de provider wordt vervolgens weer PLAT, RFC6145 (Li, Bao, & Baker, IP/ICMP Translation Algorithm, 2011), uitgevoerd om het pakket naar het IPv4 internet te kunnen versturen. 464XLAT wordt beschreven in RFC6877 (Mawatari, Kawashima, & Byrne, 2013).

Stateful NAT, dat bij 464XLAT wordt uitgevoerd op de PLAT, is bij grote implementatie een zware functie om uit te voeren. Dit kan de schaalbaarheid van het systeem beperken.

Overig

Er worden in de wereld van transitie-technieken nog veel meer technieken benoemd. Niet alle technieken zijn bedoeld om IPv4 over IPv6 beschikbaar te houden, maar veel zijn ook gericht op het uitrollen van IPv6 over IPv4 netwerken. Deze technieken vallen daardoor buiten de scope, maar worden kort benoemd zodat geen verwarring ontstaat:

- 6in4 (Basic Transition Mechanism for IPv6 Hosts and Routers), RFC4213 door Nordmark & Gilligan (2005);
- 6to4 (Connection of IPv6 Domains via IPv4 Cloud), RFC3056 door Carpenter & Moore (2001);
- 6rd (IPv6 Rapid Deployment), RFC5969 door Townsley & Troan (2010);
- 6over4 (Transmission of IPv6 over IPv4 Domains without Explicit Tunnels), RFC2529 door Carpenter & Jung (1999);
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), RFC5214 door Templin, Gleeson & Thaler (2008).

Vergelijking

Op basis van de informatie van de transitie technieken is een vergelijking in Tabel 9 weergegeven. Ter onderbouwing is informatie gewonnen uit een artikel over tunneling technieken door Chuangchunsong, Kamolphiwong, Kamolphiwong, Elz, & Pongpaibool (2014). Daarnaast is een performance analyse meegenomen van Singalar en Banakar (2018).

De vergelijking is gebaseerd op een multicriteria-analyse beschreven in paragraaf 2.2.16. De uitwerking en onderbouwing van de waardes in de analyse zijn toegelicht in bijlage M.

Techniek	Manier	Address sharing	State management	Transparancy	Scalability	NAT	Status	Software beschikbaarheid	Open Source	Kosten	Score
Iw4o6	Tunneling	NAPT	Per subscriber	Limited	High	On CPE	Standard	++	+++	€	27
DS-Lite	Tunneling	NAPT	Per session	Limited	Medium	On BR	Standard	+++	+++	€€€	23
4over6	Tunneling	Geen	Per subscriber	Limited	Medium	On BR	Experimental	-	-	-	13
MAP-E	Tunneling	NAPT	Stateless	Limited	High	On CPE	Standard	++	+	€€	25
MAP-T	Translation	NAPT	Stateless	Limited	High	On CPE	Standard	++	+	€€	24
4rd	Tunneling	NAPT	Stateless	Not limited	High	On CPE	Experimental	-	-	-	19
CGN	Translation	NAT	Per subscriber	Not limited	Medium	On BR	Standard	+++	++	€€€	22
464XLAT	Translation	Geen	Per subscriber	Not limited	Medium	Double NAT	Standard	++	++	€€	20

Tabel 9. Vergelijking van transitie technieken.

Op basis van de vergelijking is te zien dat Iw4o6 de hoogste score behaald. Dit bevestigt dat Iw4o6 op moment van schrijven de beste transitie techniek is voor Breedband.

Risico's

Bij een implementatie van een nieuw systeem zijn altijd risico's. Ook bij lw4o6 moet er rekening worden gehouden met mogelijke risico's. De literatuur beschrijft al een aantal risico's die bekend zijn bij lw4o6 en welke impact deze kunnen hebben op de implementatie. Hieronder zijn de risico's ingedeeld in risico's aan de kant van de klant en risico's voor de ISP zelf. Deze paragraaf doelt op het beantwoorden van deelvraag 7:

"Welke eventuele risico's zijn er tijdens of na een migratie?"

Klant

Bij een implementatie van lw4o6 is het van belang dat de klant zo min mogelijk impact ondervindt van de transitie. Toch zal er nieuwe CPE aan te pas komen en kan er impact zijn voor de klant, afhankelijk van de gebruiksdoelen van de klant. Het meest voor de hand liggende risico is dus het vervangen van de CPE. Dit heeft impact heeft bij bestaande klanten, omdat met een nieuwe router het netwerk opnieuw moet worden geconfigureerd.

Beperkte poortreeks

In een lw4o6 omgeving heeft elke eindgebruiker een beperkte reeks aan poorten op een IP-adres, wat risico's met zich mee brengt zoals beschreven in RFC6269 (Ford, Boucadair, Durand, Levis, & Roberts, 2011). Al het uitgaande verkeer kan worden vertaald naar poorten binnen die reeks. Daarnaast komen alle sessies ook terug binnen die reeks. Wanneer een eindgebruiker echter diensten binnen zijn netwerk heeft, zoals een webserver of een camera, moet dit worden opgezet op de router door middel van 'port forwarding'. De klant kan echter alleen gebruikmaken van zijn toegewezen poortreeks en kan dus meestal geen gebruikmaken van de poorten die specifieke services als 'standaard' herkennen.

UPnP is een techniek die 'port forwards' automatisch aanvraagt bij een router. Een apparaat dat gebruik maakt van UPnP zal een verzoek doen voor een specifieke poort, waarop de router antwoordt of die beschikbaar is. Is dit niet het geval, dan wordt vaak een nieuw verzoek voor een andere (meestal opvolgende) poort gestuurd, na een vastgesteld aantal (verschillend per apparaat) geweigerde verzoeken stopt het apparaat. Bij UPnP IGD 1.0 (een oudere versie) is er geen manier om het apparaat te sturen naar een beschikbare poort. Dit betekent dat UPnP vaak zal mislukken wanneer het verzoek buiten de beschikbare poortreeks ligt. UPnP IGD 2.0 (een nieuwere versie) kan het apparaat duidelijk maken welke poorten beschikbaar zijn zodat dit proces sneller werkt en een hogere slagingskans heeft. Bij apparaten met UPnP IGD 1.0 zal het proces dus vaak mislukken (Ford, Boucadair, Durand, Levis, & Roberts, 2011). NAT-PMP (PCP) (RFC6887) is een protocol dat dit probleem verhelpt, maar wordt nog niet door alle apparaten ondersteund (Wing, Cheshire, Boucadair, Penno, & Selkirk, Port Control Protocol (PCP), 2013).

Een ander probleem dat de beperkte poortreeks met zich mee brengt, is dat deze kunnen conflicteren met diensten die draaien op bekende poortreeksen. Sommige applicaties hebben namelijk geen flexibiliteit omtrent poortgebruik en zijn dus niet bereikbaar bij gebruikers met een beperkte poortreeks buiten de standaard.

ISP

Voor het gebruik en de implementatie van lw4o6 zijn de bijbehorende risico's voor de ISP als volgt.

CPE

Bij de provider wordt de implementatie uitgevoerd. Daarbij moeten aanpassingen worden aangebracht in de infrastructuur die het mogelijk maken om de nieuwe techniek grootschalig te gebruiken. Zoals eerder genoemd moet de CPE bij de klant worden vervangen om een lwB4 functie te ondersteunen. De ISP is verantwoordelijk voor het vervangen van de CPE (Martínez, 2017).

Data regulation

In een lw4o6-oplossing worden IP-adressen gedeeld onder meerdere gebruikers. In een artikel van Europol (2017) wordt gesteld dat het delen van IP-adressen niet gewenst is voor partijen als Europol omdat dit het opsporen van mogelijk crimineel internetgebruik kan bemoeilijken. Bij het gebruik van een CGN worden meerdere consumenten onder een enkel publiek IP-adres gehouden. Hierdoor strandt het traceren van criminele activiteiten altijd bij een IP-adres in beheer van de provider. Europol is daardoor afhankelijk van medewerking en logging van de provider om criminele activiteit op te sporen. Tijdens een presentatie (García, Lightweight 4-over-6: One step further Dual-Stack Lite Networks (RIPE 76), 2018) laat een Blake Willis, een partij uit het publiek, weten dat hun contact bij Europol heeft verzocht niet meer dan 8 tot 16 consumenten achter één IP-adres te houden. Dit risico is ook beschreven in RFC6269 (Ford, Boucadair, Durand, Levis, & Roberts, 2011) onder 'Traceability', maar is nog niet wettelijk vastgelegd.

Scaling & Provisioning

Het succesvol beheer van een lw4o6-oplossing betekent dat de lwAFTR en lwB4 functies moeten worden ingericht. Dit wordt provisionen genoemd. Om redundantie in te bouwen of de oplossing te schalen is het noodzakelijk om gebruik te maken van meerdere lwAFTR-oplossingen. Omdat een lwAFTR niet compleet stateless is, maar een per-subscriber state houdt, is het noodzakelijk dat alle lwAFTR appliances een volledige (gelijke) configuratie hebben van de software-tabel.

Blacklisting

Door het gebruik van één IP-adres bij meerdere eindgebruikers wordt het gevolg van blacklisting-methodes, die gebruik maken van IP-adres herkenning, problematisch voor meerdere eindgebruikers. Niet alleen het gevolg van de blacklisting wordt aangetast, ook de kans op blacklisting is verhoogd per gebruiker. Bijvoorbeeld applicaties die meerdere gelijktijdige verbindingen weigeren, kunnen problemen vertonen wanneer meerdere eindgebruikers achter eenzelfde IP-adres de applicatie gelijktijdig willen gebruiken (Ford, Boucadair, Durand, Levis, & Roberts, 2011).

4.3.2. Conclusie

Het literatuuronderzoek biedt meer inzicht in de belangrijke onderdelen omtrent de oplossing waar Breedband naar op zoek is. Het bevestigt dat lw4o6 de beste oplossing is voor Breedband om IPv4-exhaustion tegen te gaan.

De informatie uit het literatuuronderzoek biedt in de resultaten al antwoord op deelvragen en vormt in de conclusie een lijst met ontwerpprincipes. De ontwerpprincipes dienen als richtlijn voor een ontwerp. De ontwerpprincipes zijn hieronder in opgesomd.

#	Ontwerp principe
OP1	Als IPv4 onvoldoende IPv4-adressen biedt, dan moet IPv6 worden gebruikt, omdat IPv6 ruim voldoende adressen kan aanbieden voor de toekomst (Tadayoni & Henten, 2015).
OP2	Als IPv4 uitputting op distributie-niveau moet worden aangepakt, dan is het van belang om algemene richtlijnen voor distributie te volgen, omdat de richtlijnen onnodige uitgave van IPv4-adressen beperken (Gerich, 1993).
OP3	Als IPv4-exhaustion een probleem is voor een organisatie, dan moet er een netwerk-transitie plaatsvinden naar IPv6-only met IPv4-as-a-service, omdat IPv6 voldoende adresruimte heeft en met de juiste transitie-techniek is IPv4 alsnog mogelijk te maken als een service (Boucadair, et al., 2012).
OP4	Als IPv6-netwerken moeten worden ingericht, dan moet zoveel mogelijk gebruik worden gemaakt van SLAAC, omdat dit het netwerk flexibeler maakt en er minder stateful-configuraties nodig zijn (White, 2017).
OP5	Als IPv6-adressen structureel moeten worden beheerd, dan moet DHCPv6 in het netwerk worden geïmplementeerd, omdat DHCPv6 de IPv6-adressering kan beheeren binnen een netwerk en daarbij gewenste DHCPv6-options kan meegeven (White, 2017).
OP6	Als een IPv6-transitie grootschalig wordt toegepast, dan is het van belang de oplossing zo stateless mogelijk te maken, omdat stateful functies de schaalbaarheid en beheerbaarheid aanzienlijk verslechteren (Boucadair, et al., 2012).
OP7	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van lw4o6, omdat lw4o6 een transitie biedt met per-subscriber-state en schaalbare netwerkfuncties en mogelijkheid tot het delen van IP-adressen (Cui, et al., 2015).
OP8	Als men lw4o6 wil implementeren, dan moeten minimaal de functies lwB4 en lwAFTR worden gerealiseerd, omdat deze twee functies de basis vormen voor lw4o6 en het verkeer van IPv4 over het IPv6-netwerk mogelijk maken (Cui, et al., 2015).
OP9	Als een lwAFTR wordt geconfigureerd, dan moet er gebruik worden gemaakt van de open source Snabb toolkit, omdat dit de enige succesvolle open source implementatie is van deze netwerkfunctie (García, 2017).

Tabel 10. Ontwerpprincipes (tabel 1 van 2)

#	Ontwerpprincipe
OP10	Als een lwB4 moet worden geconfigureerd, dan moet OpenWRT worden gebruikt met enige handmatige aanpassingen, omdat OpenWRT ondersteuning biedt voor de lwB4 functie, maar door gebreken nog niet 100% inzetbaar is (García, 2017).
OP11	Als een softwire wordt opgesteld, dan moet PSID '0' altijd worden overgeslagen, omdat dit conflicten oplevert met standaard services op standaard poortnummers (García, 2017).
OP12	Als een softwire-tabel moet worden opgesteld, dan moet hiervoor een provisioning service worden ingericht, omdat de service alle functies gelijktijdig zou kunnen updaten zodat schaling gemakkelijker is toe te passen (Cui, et al., 2015).
OP13	Als een provisioning-service wordt ingericht voor lw4o6, dan moet deze service een lwB4 kunnen voorzien van configuratie, omdat handmatige configuratie van de lwB4-functies de beheerbaarheid van het systeem verhoogt (Cui, et al., 2015).
OP14	Als een provisioning-service wordt ingericht voor lw4o6, dan moet deze service een lwAFTR kunnen voorzien van configuratie, omdat elke lwAFTR op de hoogte moet zijn van alle softwires om de omgeving foutloos te laten draaien (Cui, et al., 2015).
OP15	Als een lwB4 op afstand moet worden ingericht, dan moet gebruik worden gemaakt van DHCPv6-options, omdat IANA een specifieke set aan DHCPv6-options heeft gedefinieerd voor softwire-configuratie (Mrugalski, et al., 2015).
OP16	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van MAP-E, omdat MAP-E een volledig stateless transitie-techniek biedt met mogelijkheid tot het delen van IP-adressen (Dec, Li, Bao, Matsushima, & Murakami).
OP17	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van MAP-T, omdat MAP-T een volledig stateless transitie-techniek biedt met mogelijkheid tot het delen van IP-adressen (Li, Bao, Troan, Matsushima, & Murakami, 2015).
OP18	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van DS-Lite, omdat DS-Lite een transitie-techniek met per-flow state en goed beheerbaar is en mogelijkheid biedt tot het delen van IP-adressen (Durand, Droms, Woodyatt, & Lee, 2011).
OP19	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van 4over6, omdat 4over6 een stateless transitie-techniek is met gebruik van tunneling (Wu, Cui, Li, & Metz, 2010).
OP20	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van 4rd, omdat 4rd een volledig stateless transitie-techniek biedt met transparantie in IP-pakketten en het de mogelijkheid om IP-adressen te delen (Despres, Penno, Lee, Chen, & Chen, 2015).
OP21	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van CGN, omdat CGN een beheerbare NAT-oplossing toepast op het ISP-netwerk om IP-adressen te delen (Boucadair, Durand, Levis, & Roberts, 2011).
OP22	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van 464XLAT, omdat 464XLAT het mogelijk maakt om IPv4-adres te versturen over een IPv6-netwerk door middel van dubbele NAT (Mawatari, Kawashima, & Byrne, 2013).
OP23	Als een beperkte poortreeks beschikbaar is voor een eindgebruiker, dan moeten voldoende port-forwarding instructies aanwezig zijn voor correct gebruik van de beperkte poort-reeks, omdat poorten buiten de reeks niet bruikbaar zijn en dit voor gebruikers zonder voldoende kennis ingewikkeld is (Ford, Boucadair, Durand, Levis, & Roberts, 2011).
OP24	Als UPnP beschikbaar moet zijn binnen een beperkte poortreeks, dan moet UPnP IGD 2.0 in combinatie met NAT-PMP (PCP) worden toegepast, omdat oudere versies geen port-negotiation uitvoeren en daardoor falen op verzoeken buiten de poortreeks (Ford, Boucadair, Durand, Levis, & Roberts, 2011).

Tabel 11. Ontwerpprincipes (2 van 3)

#	Ontwerpprincipe
OP25	Als een lw4o6 wordt geïmplementeerd, dan moet de CPE worden vervangen door CPE met voldoende ondersteuning, omdat de lwB4 functie ondersteunt dient te worden de CPE (Martínez, 2017).
OP26	Als IP-adressen worden gedeeld, dan dienen er niet meer dan 16 gebruikers achter een enkel IP-adres te zitten, omdat het delen onder meer gebruikers het opsporen van criminele activiteiten slecht mogelijk maakt (García, Lightweight 4-over-6: One step further Dual-Stack Lite Networks (RIPE 76), 2018).

Tabel 12. Ontwerpprincipes (tabel 3 van 3)

4.4. Inspirerend voorbeeld

Het inspirerend voorbeeld is een onderdeel dat kijkt naar andere partijen die een soortgelijk probleem hebben moeten aanpakken. Er wordt daarbij gekeken welke oplossingen worden gebruikt en hoe deze functioneren. Het inspirerend voorbeeld is opgesteld volgens de aanpak zoals beschreven in Proces.

4.4.1. Resultaten

In de praktijk zijn er in elk geval twee partijen in Europa bekend die lw4o6 hebben toegepast binnen hun productieomgeving. Hieronder worden de twee voorbeelden genoemd en de toepassing ervan beschreven op basis van literatuuronderzoek en deskresearch. Deze paragraaf doelt op het beantwoorden van deelvraag 8:

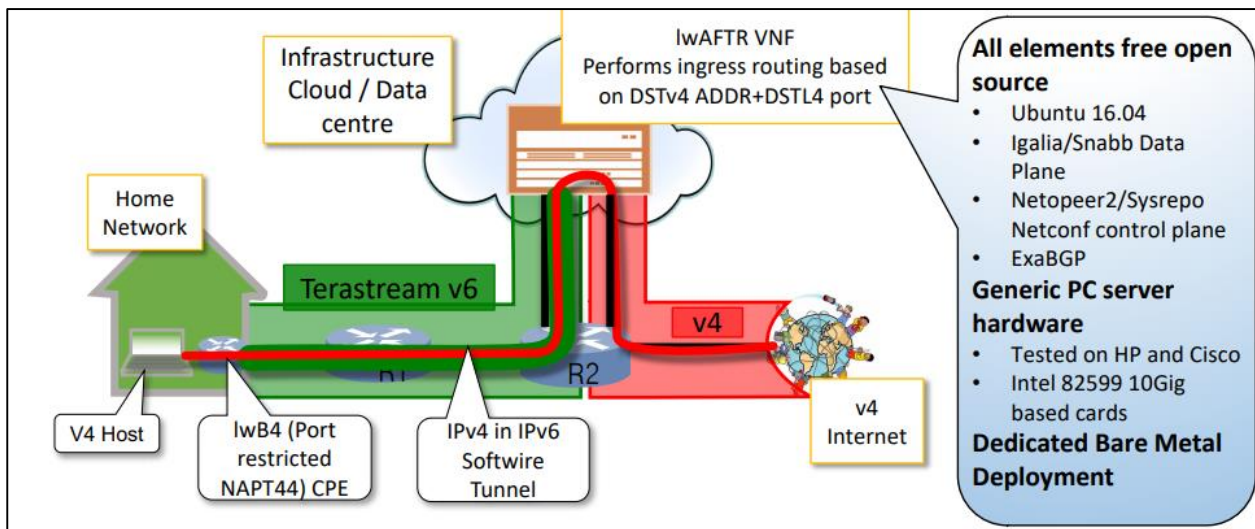
“Hoe wordt lw4over6 toegepast door andere partijen?”

Inspirerend voorbeeld: DT Terastream

Deutsche Telekom is een bedrijf uit Duitsland dat zich focust op het leveren van internetdiensten en is, net als Breedband, een ISP. Deutsche Telekom, met een jaaromzet van 75 miljard euro in 2018, is iets grootschaliger dan Breedband (Deutsche Telekom, 2018).

Om het netwerk van Deutsche Telekom in Duitsland te verbeteren en daarbij ook IPv4 uitputting tegen te gaan, is Deutsche Telekom gestart met het project 'Terastream'. Bij het opstellen van het nieuwe netwerk wordt een gebroken ring gebruikt, ook wel 'hoefijzer' structuur. In de gebroken ring worden meerdere PE-routers verbonden met twee core routers door middel van ADM op verschillende golflengtes (ook wel lambda genoemd). Vanwege de complexiteit en beheersbaarheid van dual stack, wordt het nieuwe access-netwerk als IPv6-only uitgerold (Pepelnjak, Deutsche Telekom TeraStream: Designed for Simplicity, 2013).

Op het IPv6-only netwerk kan standaard geen IPv4-verkeer worden vervoerd. Daarvoor maakt Deutsche Telekom gebruik van de IPv6 transitie techniek: lw4o6. De IPv6 transitie techniek biedt een aantal uitdagingen, namelijk: CPE, AFTR en Orchestration (Pepelnjak, Terastream Part 2: Lightweight 4over6 and Network Function Virtualization (NFV), 2013).



Figuur 13. Lw4o6 in Terastream

Noot. Herdrukt van "DT Terastream 2018", door Abrahamsson, M. 2018. Geraadpleegd van <https://www.ripe.net/support/training/ripe-ncc-educa/presentations/mikael-abrahamsson-dtag.pdf>

CPE

Om IPv4 te gebruiken via een IPv6 transitie techniek is het van belang dat de Customer Premises Equipment (CPE) de techniek volledig adopteert. Lw4o6 vereist dat op de CPE een lwB4 wordt gerealiseerd. Een lwB4 functie wordt niet standaard in router-software geleverd, waardoor een kant-en-klare router niet bruikbaar is. Deutsche Telekom kan door de omvang van de onderneming CPE op maat laten maken. Er is een CPE op maat ontwikkeld gebaseerd op OpenWRT, die een 4in6 tunnel (RFC2473 (Conta & Deering, 1998)) opzet naar een lwAFTR en daarbij NAT44 uitvoert.

AFT R

De 4in6 tunnels vanaf de lwB4 moeten worden verwerkt naar het IPv4 internet. Daarvoor is een lwAFTR benodigd. Deutsche Telekom maakt gebruik van de open source software Snabb waarin een lwAFTR programma beschikbaar is. Omdat een lwAFTR alleen per-subscriber state bewaard, is inkomend verkeer niet gebonden aan één lwAFTR instantie. Hierdoor is het schalen van het systeem gemakkelijk. Deutsche Telekom draait daarom meerdere lwAFTR instanties grenzend aan een core-router. Dit houdt het systeem schaalbaar.

Provisioning

Voor schaalbaarheid is het van belang dat configuratie van het systeem geautomatiseerd is. Daarvoor is het van belang dat provisioning van de functies lwB4 en lwAFTR wordt geregeld vanuit een centraal punt. Deutsche Telekom combineert hiervoor twee methodes (Abrahamsson, 2018):

- DHCPv6 voor het inrichten van een lwB4;
- Netconf/YANG voor het inrichten van een lwAFTR.

Bijzonderheden

Ondanks dat Iw4o6 gericht is op het delen van IPv4 adressen, is dit niet vereist. Het voordeel van een IPv6-only access netwerk blijft ook bestaan wanneer volledige IPv4 adressen worden toegewezen aan consumenten. Hoewel Deutsche Telekom wel heeft geëxperimenteerd met gedeelde IPv4 adressen met een port-set van 1024, worden op dit moment nog volledige IPv4 adressen uitgedeeld in het Terastream netwerk (Abrahamsson, 2018).

Inspirerend voorbeeld: OTE

OTE, voluit draagt het de naam "Hellenic Telecommunications Organisation S.A., OTE Group", is de grootste ISP in Griekenland. Sinds 2009 is Deutsche Telekom de grootste aandeelhouder in OTE, waardoor invloeden van Terastream ook zijn doorgestroomd naar beslissingen binnen OTE (Papachristou, 2009).

Net als Deutsche Telekom maakt OTE gebruik van lightweight 4over6 voor consumenten op hun access netwerk (Zorbadelos & Nikolopoulos, A Large-scale lw4o6 Deployment for Broadband Users in Greece, 2018).

CPE

De CPE is in een lw4o6 deployment verantwoordelijk voor de lwB4 functie. In het geval van OTE is dat ook zo. OTE heeft zich bij het ontwikkelen van hun transitie techniek gericht op een CPE die zij al grootschalig intern toepassen. De CPE is ontwikkeld door een leverancier van OTE (OTE geeft de naam van de leverancier niet vrij) en de CPE is dus op maat gemaakt (Zorbadelos, Towards IPv6 Only: A large scale lw4o6 deployment, 2018).

AFTR

Om de lwAFTR in het lw4o6 netwerk te realiseren is een RFQ opgesteld. Een aantal leveranciers (niet publiekelijk gemaakt) hebben deelgenomen aan de RFQ. OTE heeft op basis van interne beslissingen de keuze gemaakt voor de lwAFTR op hardware van Juniper, die het open source Snabb systeem implementeert in combinatie met hun eigen VMX Control Plane. De lwAFTR draait als VNF on-a-stick, waardoor extra lwAFTR instances gemakkelijk kunnen worden toegevoegd. Door gebruik van anycast wordt verkeer verdeeld over lwAFTR instances (Zorbadelos, Towards IPv6 Only: A large scale lw4o6 deployment, 2018).

Provisioning

Om de lw4o6-omgeving van OTE te managen beschrijft Zorbadelos (2018) verschillende technieken toegepast voor de provisioning.

Radius

Om consumenten te managen is een Radius server ingesteld op basis van FreeRadius. De Radius heeft een handmatige configuratie om te kunnen matchen met lw4o6.

DHCP

Om de CPE's te voorzien van IP-adressen en voor overige configuratie wordt een DHCPv6 server gebruikt. OTE heeft daarbij gekozen voor de open source DHCP-server 'ISC-DHCP', omdat op het moment van de presentatie dit de enige DHCP-server was die DHCPv6 option S46 ondersteunt (ISC, z.d.). DHCPv6 option S46 kan de benodigde informatie pushen naar de CPE om een lwB4 te configureren.

Bijzonderheden

OTE heeft lw4o6 uitgerold in hun netwerk en noemde dit een multi-year-effort (Zorbadelos, Towards IPv6 Only: A large scale lw4o6 deployment, 2018). Tijdens de implementatie werd nog steeds doorontwikkeld aan de technieken, waardoor sommige aspecten van de implementatie achterlopen op de nieuwste mogelijkheden. Een voorbeeld hiervan is de DHCP-server van ISC. In de huidige configuratie ondersteunt OTE geen IPv6 Prefix Delegation door het gebrek aan ondersteuning in ISC-DHCP. ISC heeft inmiddels een nieuwe variant van zijn DHCP-server uitgebracht, ISC-KEA-DHCP, die meer ondersteuning biedt voor DHCPv6 functies en standaard Option S46 en statische IPv6 Prefix Delegation ondersteunt. De schaalbaarheid van de DHCP-server met betrekking tot lw4o6 is nog onduidelijk, het bedrijf ISC liet Zorbadelos (2018) weten dat zij hier zelf ook nog geen ervaring mee hebben.

Voor het configureren van lwB4 functies wordt de eerder benoemde DHCPv6 gebruikt, daarbij wordt een IPv6 en IPv4 adres (onafhankelijk van elkaar) uitgegeven in combinatie met het (anycast) adres van de lwAFTR en de benodigde port-set informatie. Elke consument krijgt 1024 poorten op een gedeeld IPv4 adres. De keuze voor 1024 is niet onderbouwd en is als een 'educated guess' te zien, de keuze voor deze poort-hoeveelheid heeft nog niet tot directe problemen geleid in productie. Het gebruik van 1024 poorten betekent dat in de totale port-range van 65536 er 63 port-sets (64-1, omdat de eerste port-set-id wordt genegeerd) kunnen worden gebruikt. Tijdens de presentatie van Zorbadelos (2018) meldt Blake Willis uit het publiek dat Europol uitspraken heeft gedaan met het dringende verzoek om bij IP-sharing maximaal 16 consumenten (bij voorkeur zelfs maar 8) achter één IP-adres te zetten. Deze uitspraak is echter niet gedocumenteerd en dus niet bindend.

In de huidige setup wordt lw4o6 parallel gedraaid aan Dual-Stack. Dat betekent dat bij problemen bij de consument, deze wordt teruggezet naar het Dual-Stack netwerk waarop zij een volledig IPv4 adres krijgen. Problemen hebben meestal te maken met port-forwarding, zoals bij gebruik van camera's of een NAS, omdat de huidige CPE nog geen UPnP of port-forwarding ondersteunt op het gedeelde IPv4 adres.

Om de status van het lw4o6 gebruik te monitoren is het van belang dat de handelingen van de lwAFTR worden gemonitord. OTE maakt gebruik van Juniper VMX met de Snabb lwAFTR en wordt Juniper OpenNTI gebruikt voor monitoring. Daarbij worden lwAFTR counters in een InfluxDB gezet (open source database software (InfluxData, z.d.)), waarna duidelijke statusgrafieken kunnen worden gemaakt in Grafana (visualisatiesoftware (GrafanaLabs, z.d.)).

4.4.2. Conclusie

Op basis van de resultaten van het inspirerend voorbeeld is de volgende deelvraag 8 te beantwoorden:

"Hoe wordt lw4over6 toegepast door andere partijen?"

Er zijn wel degelijk partijen die lw4o6 als oplossing toepassen om IPv4-uitputting tegen te gaan. Twee grote ISPs spreken hier openlijk over op verschillende meet-ups en in artikelen. Deutsche Telekom is de eerste partij die hiermee is gaan werken. De toepassing van lw4o6 rust vooral op de functies lwB4 en lwAFTR. Deutsche Telekom heeft hierover veel informatie en open source applicaties teruggegeven aan de community. Door mee te werken aan de RFC7596 (Cui, et al., 2015) voor lw4o6 en de ontwikkeling van een lwAFTR functie in de open source Snabb-toolkit, is lw4o6 toegankelijker geworden voor andere partijen. Voor de lwB4 functie is een softwarematige aanpassing op het open source OpenWRT-systeem geschreven en in gebruik genomen op hun CPE's.

OTE heeft net als Deutsche Telekom de transitie techniek toegepast in zijn netwerk. De keuze is voornamelijk gevallen op lw4o6 omdat Deutsche Telekom grootaandeelhouder is en daarom invloed heeft op de keuzes binnen het bedrijf. Net als Deutsche Telekom wordt voor de lwAFTR een Snabb-implementatie gebruikt, voor de lwB4 is een leverancier van hun CPE's benaderd waarvoor zij een software-implementatie op maat hebben gemaakt.

Op basis van de informatie van de implementaties van beide partijen is het mogelijk om een lijst met aanvullende eisen op te stellen voor het gebruik van lw4o6. De lijst is methodisch gecategoriseerd en geprioriteerd volgens de MoSCoW-analyse.

#	Requirement (S.M.A.R.T.)	Prioriteit
S06	Voor provisioning van CPE's moeten DHCPv6-options worden gebruikt.	Should have
S07	Voor loadbalancing van lwAFTR's moet een anycast-adres worden gebruikt.	Could have

Tabel 13. Requirements uit voorbeelden

5. Ontwerp

Het ontwerp dient als oplossing voor het probleem. In dit hoofdstuk is de ontwerpbenadering beschreven en vervolgens is het ontwerp zowel functioneel als technisch uitgewerkt. Het ontwerp is selectief geëvalueerd met een ontwerpevaluatie.

5.1. Ontwerpbenadering

Het ontwerp voor een lw4o6 oplossing wordt opgesteld met behulp van de Prototyping-methode, zoals beschreven door Haveman, Hageraats & Van der Linden (2016) in de Reader Ontwerponderzoek. Prototyping is een cyclische aanpak van het ontwerp waarbij herhaaldelijk onderdelen worden ontworpen en getest voordat verder wordt gewerkt. Er is gekozen voor prototyping, omdat lw4o6 geen kant-en-klaar product is en bij de toepassing ervan veel handmatig moet worden ingesteld. Met deze aanpak worden verschillende onderdelen aangepakt en onafhankelijk van elkaar getest. De onderdelen die worden behandeld zijn:

- lwB4 (CPE-gedeelte van lw4o6);
- lwAFTR (ISP-gedeelte van lw4o6);
- Provisioning van CPE.

Door het cyclisch ontwerpen en testen van de onderdelen wordt bepaald welke onderdelen geschikt zijn en waar verdere ontwikkeling nodig is. Het ontwerp wordt beschreven in paragraaf 5.2 en 5.3. Het testontwerp en de resultaten daarvan worden beschreven in paragraaf 5.4.

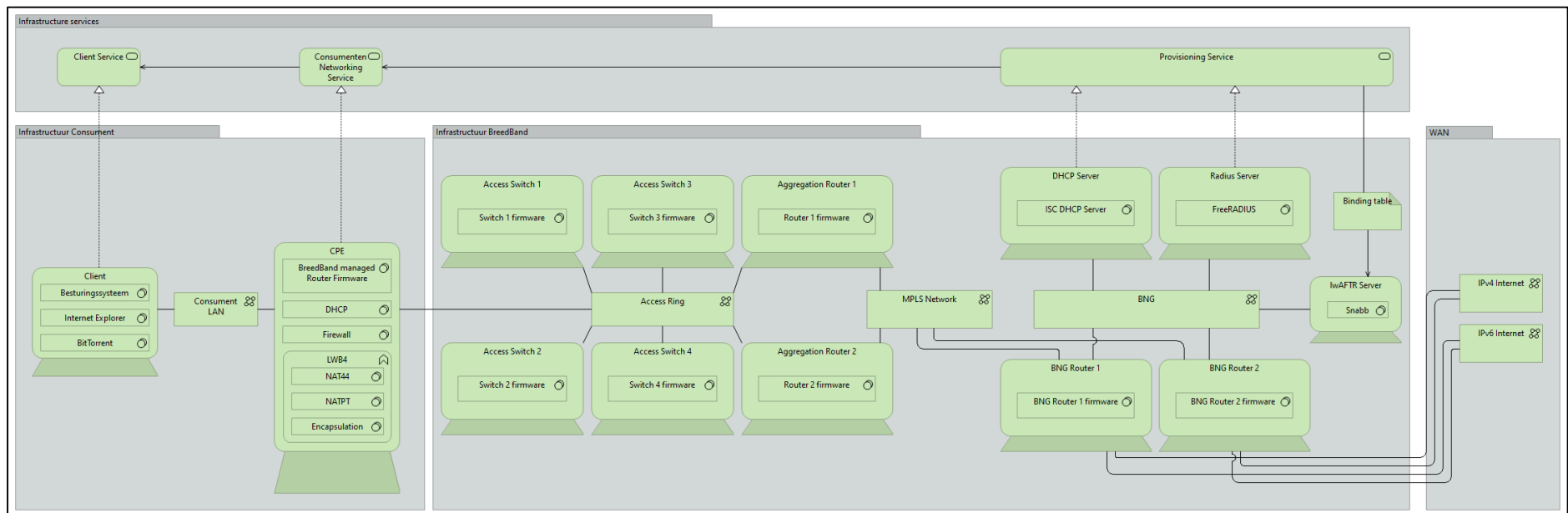
Om prototyping te kunnen hanteren wordt gebruik gemaakt van het Agile-framework 'Kanban'. Kanban is een methode waarbij losse taken voor elk onderdeel worden geformuleerd (Brown, 2018). Elke taak doorloopt dan onafhankelijk van andere taken de stadia: 'To-do', 'Testing' en 'Done'. Deze methode is tijdens dit project gebruikt met de online notitie-tool Google Keep.

Het ontwerp pakt de conclusies uit het onderzoek en zet deze om tot het beantwoorden van deelvraag 9:

“Wat is nodig om de nieuwe oplossing technisch te implementeren?”

Lw4o6 is een transitie techniek die afhankelijk is van twee belangrijke functies, de lwB4 op de CPE en de lwAFTR op de PE. Een optioneel onderdeel voor lw4o6, zeker aan te raden voor een succesvollere implementatie, is de provisioning. In het literatuuronderzoek is de werking van lw4o6 al beschreven. In dit hoofdstuk wordt de toepassing van de functies beschreven, zodat lw4o6 toepasbaar wordt voor Breedband.

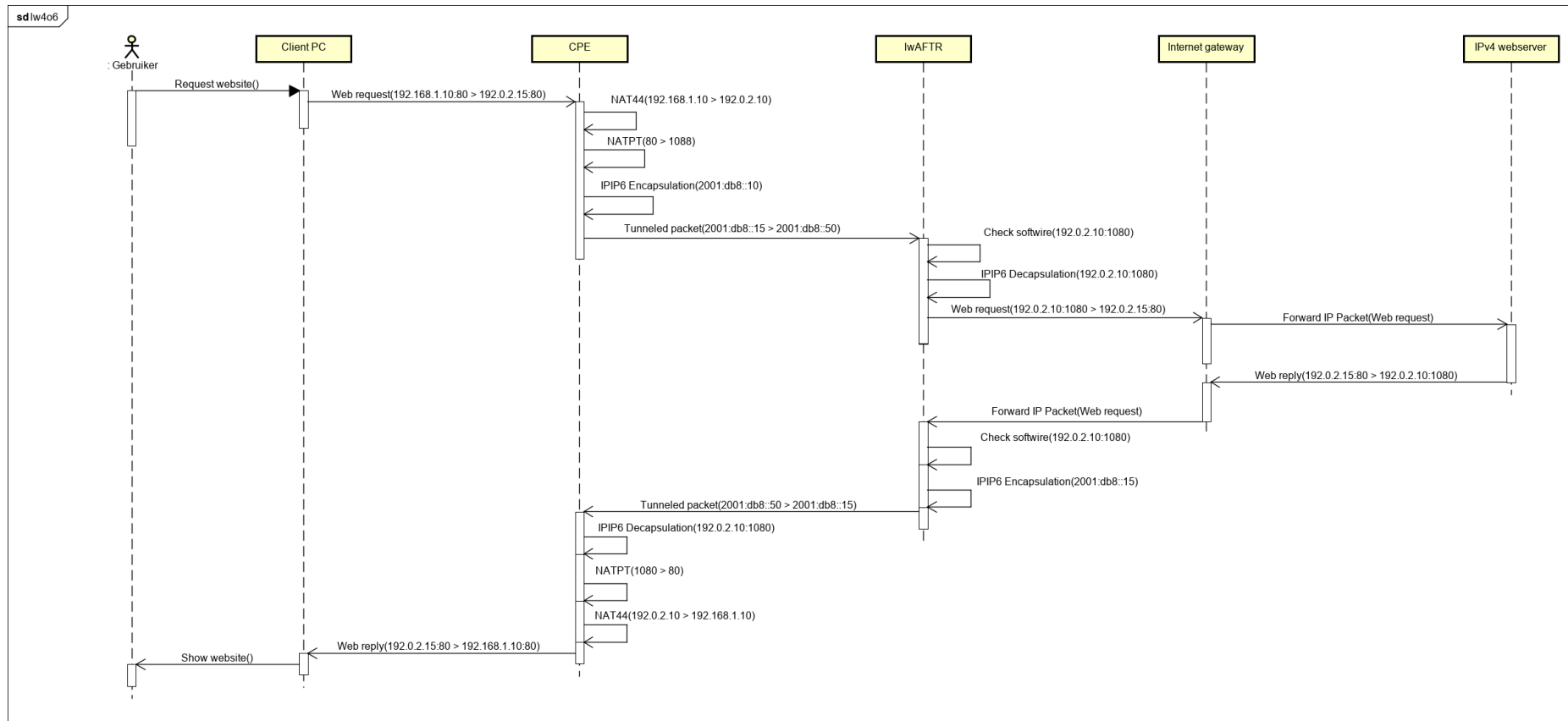
Het ontwerp voor Breedband richt zich op een scenario waarin de lwAFTR zich in hetzelfde netwerk bevindt als de lwB4 clients. Dit is technisch niet noodzakelijk, maar maakt de provisioning makkelijker en het geheel overzichtelijker. Het ontwerp is gebaseerd op de toepassing van lw4o6 zoals beschreven in het literatuuronderzoek. Dit ontwerp wordt beschreven volgens de onderstaande schematische weergave op basis van Archimate zoals beschreven in paragraaf 2.2.14. De architectuurplaat is gebaseerd op de architectuurplaat van Figuur 7 en bevat aanpassingen om lw4o6 te ondersteunen. De CPE in het nieuwe ontwerp bevat nu ook de *lwB4-functie* om lw4o6 te ondersteunen. Bij de provider wordt in de BNG een *lwAFTR* geplaatst (on-a-stick). Daarbij wordt een *binding table* toegevoegd aan de *provisioning service* waarin softwires worden onderhouden.



Figuur 14. Architectuurplaat lw4o6

5.2. Functioneel

Om te begrijpen hoe de nieuwe functies het gebruik van internet voor een eindgebruiker veranderen op de achtergrond, is hieronder een sequence diagram weergegeven. In de sequence diagram is weergegeven hoe de lwB4 het IPv4-verkeer vertaalt naar een shared public IP-adres in een specifieke poortreeks. Vervolgens wordt het pakketje verpakt en over een IPv6-netwerk naar de lwAFTR verstuurd. De lwAFTR controleert het pakketje van de lwB4 op de software, waarna de lwAFTR het uitpakt en doorstuurt naar een webserver. De lwAFTR ontvangt en verstuurd pakketten stateless, waardoor hetzelfde proces in tegenovergestelde richting wordt uitgevoerd met inkomend IPv4-verkeer.



Figuur 15. Sequence diagram van lw4o6 verkeer

5.2.1. Lightweight B4

De lwB4 functie in het lw4o6 ontwerp wordt gerealiseerd op de CPE van de consument. Er zijn op het moment van schrijven geen Commercial Off The Shelf (COTS) CPE's die de lwB4 functie ondersteunen. Dit betekent dat er handmatige aanpassingen moeten worden gedaan aan software van routers die dit ondersteunen.

De functionele eisen aan een router om lwB4 te ondersteunen zijn:

- IPv4 in IPv6 encapsulation (4in6 tunneling);
- NAT44 & NATPT.

Om de functie goed te kunnen beheren (Provisioning) is het volgende benodigd:

- DHCPv6 client met Option S46 ondersteuning.

5.2.2. Lightweight AFTR

De lwAFTR functie in het lw4o6 ontwerp wordt gerealiseerd in het ISP-netwerk. De lwAFTR dient in het netwerk geplaatst te worden waar deze kan beschikken over verbindingen met een IPv6 én IPv4 netwerk.

Software

lwAFTR wordt momenteel alleen aangeboden als kant-en-klare VNF in de software Snabb. De software kan draaien op elke moderne x86-64 Linux distributie en kan worden gedraaid in een Docker container. De software wordt onderhouden door een community en is te verkrijgen via GitHub. De branch met de meeste vorderingen in de ondersteuning van lwAFTR is op het moment 'Max-next'². Dit is bepaald door het testen van de branch en door directe communicatie met een ontwikkelaar van deze branch. In de communicatie stond de basis van de problemen die zijn ondervonden tijdens het testen centraal (verder toegelicht in paragraaf 5.4.1).

5.2.3. Provisioning

De hiervoor genoemde functies, lwB4 en lwAFTR kunnen beide statisch worden ingericht voor succesvolle werking. Dat beperkt echter de schaalbaarheid en betrouwbaarheid van de omgeving. Voor een betrouwbare en schaalbare oplossing is een provisioning functie benodigd om beide functies te voorzien van juiste informatie.

Om de IP-adressering in het netwerk te kunnen beheren is een DHCP-server van belang. Standaard IP-configuratie kan via een DHCP-server worden gedistribueerd. Dit betekent dat de DHCPv6 alle lwB4 functies gaat voorzien van:

- IPv6-adres;
- IPv6 delegated prefix;
- IPv6 domainname servers.
- Gedeeld IPv4-adres;
- Port-set informatie (psid, pslen en psoffset);
- lwAFTR IPv6-adres.

Bij elke wijziging in de software-tabel voor nieuwe gebruikers moeten alle lwAFTR's worden geüpdatet. Dit kan op meerdere manieren worden gedaan. Er is echter nog geen vaste erkende oplossing. De beste methode is om de distributie van de software-tabel te laten matchen met huidige systemen. Aan de hand van handgeschreven scripts kunnen de tabellen gerepliceerd en geactiveerd worden op de lwAFTR's.

² <https://github.com/snabbco/snabb/tree/max-next>

5.3. Technisch

Om de functies technisch te implementeren, wordt in dit hoofdstuk beschreven wat hiervoor nodig is.

5.3.1. Lightweight B4

Uit het literatuuronderzoek (paragraaf 4.3.1 – onder Component: Lightweight B4) is gebleken dat de functie in theorie haalbaar is op OpenWRT router-firmware. OpenWRT is een open source systeem dat packages bevat die bedoeld zijn voor MAP-E en lw4o6 configuratie. De package 'map' die dat realiseert bevat echter een aantal bugs waardoor de package niet bruikbaar is als functionerende lwB4 (zie bijlage E).

Waar andere partijen, zoals DT en OTE, op maat geschreven software op white-label hardware zetten, is dit voor Breedband niet rendabel. Breedband heeft te weinig afname van CPE's om deze optie te benutten. Daardoor is de beste oplossing om de opensource package in OpenWRT bij te werken zodat deze de lwB4 functie wel volledig kan uitvoeren.

Hardwarematig zijn er geen speciale eisen voor een lwB4. De functie kan op elk apparaat fungeren dat de Basic Requirements for IPv6 Customer Edge Routers ondersteunt. Deze requirements zijn gedefinieerd in RFC7084 (Singh, BeeBee, Donley, & Stark, 2013).

5.3.2. Lightweight AFTR

Technisch heeft de lwAFTR de meest belangrijke functie. De lwAFTR handelt namelijk van meerdere CPE's de pakketten af en heeft dus een centrale rol. Om deze functie goed te laten draaien zijn bepaalde specificaties nodig.

Hardware

De software Snabb lwAFTR kan worden gedraaid op alle hardware die de moderne x86-64 Linux distributies ondersteunen. Om de functie lwAFTR te kunnen gebruiken dient er echter directe toegang te zijn tot een netwerkkaart (NIC) als PCI-device. Huidige drivers ondersteunen de volgende NIC's (Takikawa, Bristow, Wingo, & Rottenkolber, 2017):

- Intel 82599 10Gb adapter;
- Intel i350 1Gb adapter;
- Intel i210 1Gb adapter.

Virtualisatie

Het systeem waarop Snabb wordt gedraaid kan volledig worden gevirtualiseerd, met uitzondering van de NIC. De eis die de Snabb lwAFTR directe toegang heeft tot de NIC, zorgt ervoor dat er geen gevirtualiseerde netwerkadapter kan worden gebruikt. De NIC moet direct worden aangesproken. De ondersteuning voor gevirtualiseerde NIC's is in ontwikkeling, maar nog niet volwassen genoeg om te implementeren.

Schaalbaarheid en redundantie

Snabb ondersteunt het draaien van meerdere lwAFTR instances. Dit betekent dat wanneer een machine meerdere NIC's bevat, meerdere instances tegelijk op één machine kunnen worden gedraaid. Deze functie maakt het mogelijk om op een enkele Snabb-machine de lwAFTR-capaciteit te kunnen verhogen wanneer voldoende CPU's en NIC's aanwezig zijn.

De lwAFTR kan worden uitgevoerd als bump-in-the-wire configuratie of als on-a-stick configuratie. Bij een bump-in-the-wire worden twee NIC's gekoppeld aan één lwAFTR instance, hierbij is er een dedicated NIC voor inkomend verkeer (IPv6) en een dedicated NIC voor uitgaand verkeer (IPv4). Bij een on-a-stick configuratie wordt zowel inkomend als uitgaand verkeer op dezelfde NIC behandeld. Door het gebruik van een enkele NIC wordt een on-a-stick configuratie gebruikt in het ontwerp. Dit omdat het de uitrol van extra instances versimpeld.

Door de stateless aard van de lwAFTR is redundantie gemakkelijk te implementeren, omdat voor elk pakket het niet uitmaakt welke lwAFTR instance het behandelt. Door een anycast-adres te gebruiken voor meerdere lwAFTR instances, wordt het verkeer verdeeld over deze instances. Om redundantie te bereiken moet op minimaal twee verschillende fysieke locaties een lwAFTR instance draaien.

5.3.3. Provisioning

DHCP biedt ook mogelijkheden om extra opties te versturen naar clients. IANA heeft voor software-configuraties vaste DHCP-options vastgelegd in de DHCPv6-space (Cui, et al., 2015). Met deze opties kunnen parameters worden meegegeven voor lwB4 configuratie. Daarmee wordt beschikbaar:

- Gedeeld IPv4-adres;
- Port-set informatie (psid, pslen en psoffset);
- lwAFTR IPv6-adres.

Om een lwB4 correct in te richten zijn de hiervoor bestemde DHCPv6-options nodig. De opties voor software-provisioning zijn hieronder weergegeven met daarbij de betrokkenheid per IPv6-transitie techniek.

#	Option	MAP-E	MAP-T	Lw4o6
89	OPTION_S46_RULE	Mandatory	Mandatory	Not permitted
90	OPTION_S46_BR	Mandatory	Not permitted	Mandatory
91	OPTION_S46_DMR	Not permitted	Mandatory	Not permitted
92	OPTION_S46_V4V6BIND	Not permitted	Not permitted	Optional
93	OPTION_S46_PORTPARAMS	Optional	Optional	Optional

Tabel 14. Option_S46 eisen per transitie techniek.

De opties relevant voor lw4o6 zijn de opties voor Border Relay (OPTION_S46_BR), port parameters (OPTION_S46_PORTPARAMS) en de IPv4 en IPv6 koppeling (OPTION_S46_V4V6BIND). Deze opties worden verpakt in de containeroptie: OPTION_S46_CONT_LW. De optie voor port parameters is geen op zichzelf staande optie, deze is verpakt bij de optie voor IPv4 en IPv6 koppeling. Dit omschrijft de volgende DHCP-option structuur:

```
OPTION_S46_CONT_LW
{
  OPTION_S46_BR
  OPTION_S46_V4V6BIND
  {
    OPTION_S46_PORTPARAMS
  }
}
```

Er is gekozen voor de DHCP-server van ISC-KEA omdat deze als enige open-source software de benodigde DHCPv6-options ondersteunt (ISC, z.d.). Breedband maakt al gebruik van ISC-DHCP, wat een voorloper is van ISC-KEA. Een upgrade naar KEA biedt ondersteuning voor het inrichten van lwB4 apparaten.

5.4. Ontwerpevaluatie

De ontwerpevaluatie doelt op het beantwoorden van deelvraag 10:

"Hoe kan de werking van de nieuwe oplossing worden bewezen?"

5.4.1. Implementatie

Om het ontwerp te evalueren is een prototype opgesteld op basis van een eerder prototype dat gedurende het onderzoek is gebruikt in de methode 'Prototyping'. Dit prototype is iteratief uitgebouwd en getest. Elke functie is daarbij getest op de bijbehorende user requirement en de beoogde functionaliteit waarvoor het is ontworpen. Daarin zijn bepaalde onderdelen niet tot het definitieve prototype gekomen. Ter onderbouwing van de totstandkoming van het huidige prototype is in Tabel 15 te zien welke stappen zijn genomen.

Onderdeel	Software	Handeling	Geslaagd
Provisioning	DHCPv6	Installatie ISC-KEA	Ja
Provisioning	DHCPv6	Configuratie DHCPv6	Ja
Provisioning	DHCPv6	Configuratie DHCPv6 Prefix Delegation	Ja
lwb4	OpenWRT	Installatie OpenWRT	Ja
lwb4	OpenWRT	Configuratie LAN4	Ja
lwb4	OpenWRT	Configuratie LAN6	Ja
lwb4	OpenWRT	Configuratie WAN6	Ja
lwb4	OpenWRT	Prefix Delegation	Ja
lwb4	OpenWRT	DHCPv6 client voor WAN	Ja
lwb4	OpenWRT	Installatie lwb4-tool	Ja
lwb4	OpenWRT	Configuratie lwb4-tool	Nee
lwaFTR	Snabb	Installatie Snabb	Ja
lwaFTR	Snabb	Configuratie VMNet adapter	Nee
lwaFTR	Snabb	Configuratie i350 adapter	Ja
lwaFTR	Snabb	Draaien van lwaFTR programma	Ja*
lwb4	Ubuntu	Configuratie lwb4 tunnel	Ja
lwb4	Ubuntu	Configuratie lwb4 NAPT	Ja
lwb4	Ubuntu	Configuratie LAN4	Ja

Tabel 15. Iteraties prototype

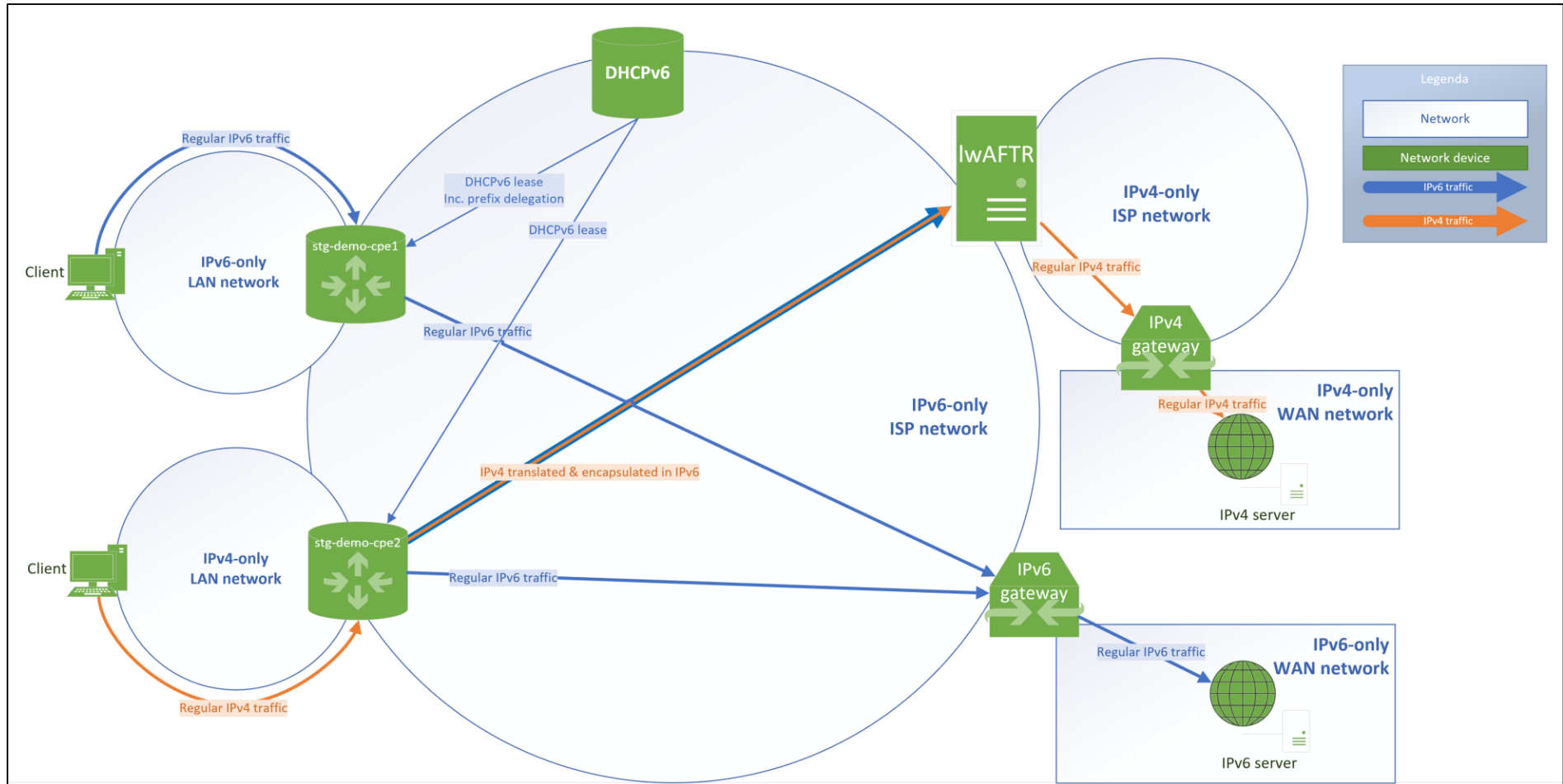
*Voor voltooiën van deze actie is een developer benaderd waardoor een update aan Snabb is toegevoegd om dit werkend te krijgen. Interactie over het probleem en de oplossing is te lezen op GitHub (<https://github.com/snabbco/snabb/issues/1440>).

De handelingen uit Tabel 15 zijn elk uitvoerig getest om tot een geslaagd resultaat te komen. Bij een niet geslaagde handeling is gezocht naar een alternatief.

De configuratie van lwb4 op OpenWRT is niet gelukt door cruciale fouten in de huidige software. De parameters voor configuratie van de 4in6 tunnel en de portreeks worden niet goed verwerkt (toegelicht in bijlage E). Als alternatief op de lwb4-functie in OpenWRT is de lwb4-functie gerealiseerd op een Ubuntu-server.

De configuratie van een VMNet adapter op de lwaFTR is niet gelukt omdat er geen werkende drivers zijn voor deze virtuele adapter. Als alternatief op de configuratie van een VMNet-adapter is een Intel i350 adapter geconfigureerd.

Door het gebrek aan een complete lwB4 oplossing, is het prototype van een CPE opgesplitst in twee delen, namelijk de router op OpenWRT en de lwB4 op Ubuntu. De lwAFTR is volledig geïmplementeerd en de provisioning is gericht op het router-gedeelte door middel van een DHCPv6-server. In Figuur 16 is een schema weergegeven dat duidelijk maakt hoe het prototype eruitziet.



Figuur 16. Schema prototype

Om de functionaliteit van lw4o6 te bewijzen is een systeemtest uitgevoerd op de CPE met werkende lwB4 (stg-demo-cpe2) en lwAFTR. De hiervoor ingerichte CPE wordt toegelicht onder de kop lwB4 in paragraaf 5.4.2. De lwAFTR is toegelicht in paragraaf 5.4.3.

In het prototype is de CPE opgesplitst en zijn verschillende functies apart van elkaar bewezen. De eerste CPE, stg-demo-cpe1, realiseert de standaard routingsfuncties met focus op IPv6 ondersteuning en daarbij de prefix delegation. Stg-demo-cpe1 is gebaseerd op OpenWRT, omdat OpenWRT de meeste potentie heeft om een definitieve oplossing te bieden. Het ontbrekende deel in OpenWRT, een correct functionerende lwB4, is op een Ubuntu systeem nagebootst om de werking van lw4o6 te bewijzen. In een definitieve implementatie worden de onderdelen samengevoegd tot één werkend geheel. Hieronder worden alle onderdelen per functie en hoe ze zijn opgesteld in het prototype beschreven.

Het gehele prototype wordt gerealiseerd op een enkelvoudige fysieke machine met ESXi 6.7.0 (update 2) als virtualisatieplatform (VMware, z.d.). Het platform is verbonden aan een netwerk met een gateway (rtr1-kantoor-bbni) naar het internet. Om aan de eisen van een lwAFTR te voldoen bevat het platform de mogelijkheid om een NIC direct toe te wijzen aan een virtuele machine aan door middel van PCI Device Passthrough. De server heeft daarvoor een Intel i350 1Gb NIC ter beschikking.

Voor het prototype zijn de volgende netwerken gebruikt. De grijs gemarkeerde netwerken zijn reeds bestaande netwerken en apparaten van Breedband, waar ook gebruik van is gemaakt.

Doel	VLAN	Router	Netwerk
ISP-netwerk IPv4	3400_innovatie_wan4	rtr1-kantoor-bbni	31.3.10.112/29
ISP-netwerk IPv6	3401_innovatie_wan6	rtr1-kantoor-bbni	2a00:c080:1:12::/64
Consumenten LAN1	0111_stg-demo-csmlan1	stg-demo-cpe1	192.168.1.0/24
Consumenten LAN2	0112_stg-demo-csmlan2	stg-demo-cpe2	192.168.2.0/24

Tabel 16. Prototype netwerken

Over het gehele prototype worden de volgende DNS-servers van Breedband gebruikt:

- 2a00:c080:1:1::2 (IPv6 preferred);
- 2a00:c080:1:2::2 (IPv6 alternative);
- 46.225.56.6 (IPv4 preferred);
- 46.226.57.6 (IPv4 alternative).

Voor IPv6 prefix delegation zijn de volgende statische routes geconfigureerd op rtr1-kantoor-bbni:

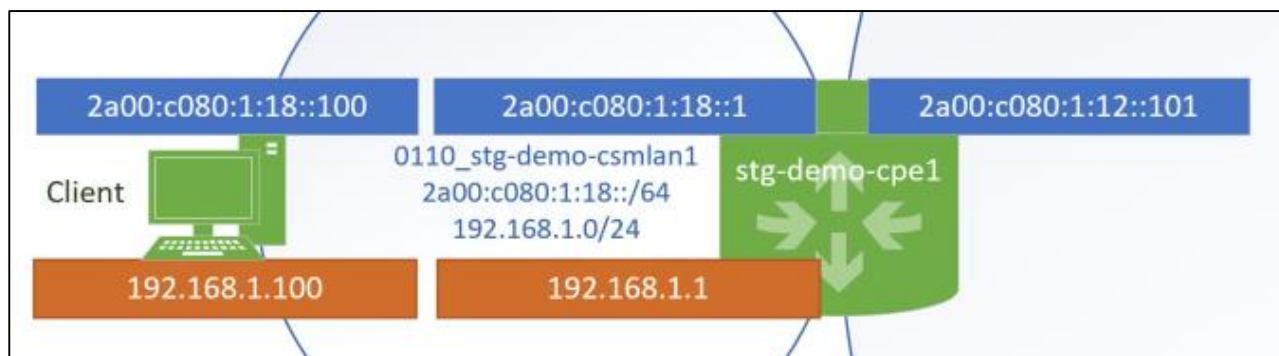
- 2a00:c080:1:18::/64 -> 2a00:c080:1:12::101
- 2a00:c080:1:19::/64 -> 2a00:c080:1:12::102
- 2a00:c080:1:1a::/64 -> 2a00:c080:1:12::103
- 2a00:c080:1:1b::/64 -> 2a00:c080:1:12::104
- 2a00:c080:1:1c::/64 -> 2a00:c080:1:12::105
- 2a00:c080:1:1d::/64 -> 2a00:c080:1:12::106
- 2a00:c080:1:1e::/64 -> 2a00:c080:1:12::107
- 2a00:c080:1:1f::/64 -> 2a00:c080:1:12::108

5.4.2. CPE (Lightweight B4)

De CPE in het ontwerp bedient de reguliere routingsfuncties, zoals elke router die voldoet aan RFC8026 (Boucadair & Farrer, Unified IPv4-in-IPv6 Software Customer Premises Equipment (CPE), 2016). Buiten de standaardfuncties biedt de CPE ook een lwB4 functie. Omdat er geen CPE-software beschikbaar is die zonder programmeerwerk beide functie vlekkeloos kan uitvoeren, worden beide functies in een apart systeem bewezen.

Router

Om de CPE naar wens op te stellen met de ondersteuning van een lwB4-functie, is een OpenWRT systeem gebruikt. Voor het prototype is gebruik gemaakt van OpenWRT 18.06.4 op een virtuele machine met twee NIC's. Eén van de NIC's dient de LAN-zijde (0111_stg-demo-csmlan1), de andere NIC dient als WAN voor de CPE en is gekoppeld aan het ISP-netwerk IPv6 (3401_innovatie_wan6). De installatie van OpenWRT in een virtuele omgeving gaat volgens bijlage F.

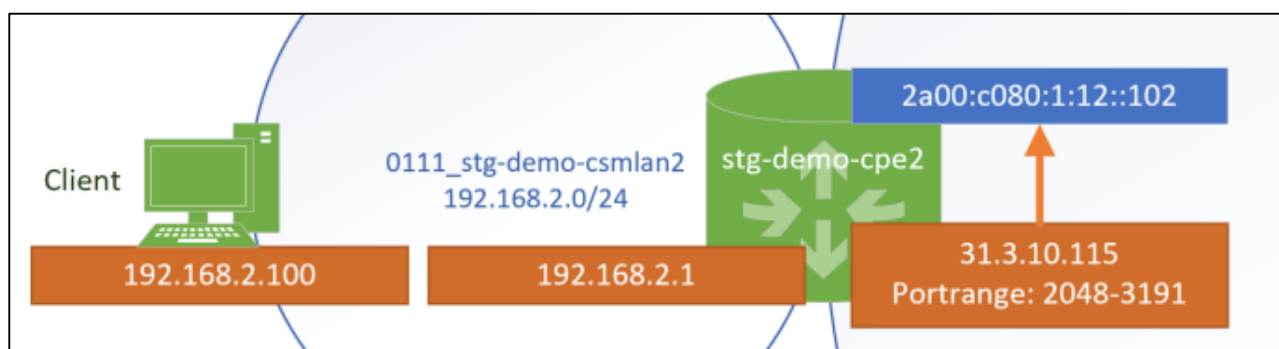


Figuur 17. OpenWRT prototype netwerk configuratie.

Met een correct geconfigureerde DHCPv6 wordt de bovenstaande OpenWRT automatisch geconfigureerd. Dit echter alleen wanneer de LAN-interface correct is aangegeven en de WAN-interface is ingesteld met een DHCPv6-client.

lwB4

Om de lwB4 functie alsnog te testen, is een virtuele machine opgezet met dezelfde netwerkinstellingen als de bovenstaande OpenWRT machine. Gezien de focus op de lwB4-functie is het IPv6-LAN met prefix delegation niet meegenomen op de Ubuntu machine. Er is gebruik gemaakt van Ubuntu Server 18.04.3 LTS volgens de reguliere installatiemethode via de installatiewizard.



Figuur 18. Ubuntu prototype netwerk configuratie.

Om Ubuntu te laten dienen als router met ondersteuning voor een statisch lwB4 functie wordt gebruikt gemaakt van de volgende programma's:

- iproute2 – voor configuratie van een 4in6-tunnel en standaard routing;
- iptables – voor configuratie van NAT44 en NAPT;
- isc-dhcp-server – voor het vormen van het LAN-netwerk door middel van DHCPv4.

Om vervolgens de lwB4 te configureren is het volgende ingesteld:

- 4in6 (ipip6) tunnel van eigen IPv6-adres (peer) naar lwAFTR-IPv6-adres (remote) **zonder** encapsulation-limit;
- WAN-interface met:
 - IPv6-adres van de lwB4;
 - Shared IPv4-adres.
- LAN-interface met IPv4 in een subnet in de private IPv4-range;
- isc-dhcp-server met een DHCP4-server op de LAN-interface om het bovenstaande IPv4-subnet uit te delen aan verbonden LAN-clients;
- Forward-rules die al het IPv4-verkeer naar de WAN-interface sturen;
- NAT-rules die al het IPv4-verkeer vertalen de beperkte port-set.

De commando's voor configuratie zijn weergegeven in bijlage G.

5.4.3. Lightweight AFTR

De lwAFTR wordt gerealiseerd op een virtuele machine die draait op Ubuntu Server 18.04.3 LTS. Snabb is geïnstalleerd volgens de README van het Github-kanaal (Gorrie, Wingo, Rottenkolber, Wiget, & Hartlage, 2018). Er wordt gebruik gemaakt van de max-next branch³.

Op de virtuele machine is een enkele Intel i350 NIC direct toegewezen als PCI-device, zodat de lwAFTR instance on-a-stick kan draaien. Ubuntu herkent de PCI-device als "0b:00.0".

De Snabb lwAFTR functie is kant-en-klaar en kan met een juiste configuratie worden gestart. Voor het prototype is de configuratie gebruikt in bijlage H. De configuratie is geplaatst in de "src"-folder van de Snabb-installatie met de naam "lwaftr.conf". De lwAFTR wordt gestart met het volgende commando:

```
./snabb lwaftr run --conf lwaftr.conf --on-a-stick 0b:00.0
```

Om verkeer vanaf WAN te kunnen routeren naar een shared IPv4-adres dient een ARP-entry in de ARP-tabel van de gateway (rtr1-kantoor-bbni) te worden gezet. De lwAFTR publiceert het gedeelde IP-adres niet automatisch via ARP, hierdoor dient dit statisch te worden geconfigureerd.

5.4.4. DHCPv6

Omdat nog geen lwB4 beschikbaar is die overweg kan met de DHCPv6-options, is de DHCPv6 enkel ingericht om IPv6-adressen inclusief prefix delegation uit te delen aan de CPE's. De DHCPv6 draait op een Ubuntu Server 18.04.3 LTS met één netwerkadapter in 3401_innovatie_wan6.

Om DHCPv6 te realiseren is gebruikgemaakt van ISC-KEA 1.5.0. De DHCP-server draait enkel DHCPv6 op de WAN-interface met de configuratie in bijlage I.

De DHCP voorziet de DHCPv6-client in het netwerk van:

- DNS-Servers 2a00:c080:1:1::2 en 2a00:c080:1:2::2
- Een IPv6-adres in de range 2a00:c080:1:12::/64

De geconfigureerde CPE's krijgen een statische toewijzing op basis van hun DUID. Daarbij wordt een IPv6-prefix toegewezen die de CPE kan delegeren naar zijn LAN-netwerk.

³ <https://github.com/snabbco/snabb/tree/max-next>

5.5. Conclusie

Het ontwerp beschrijft een lw4o6 implementatie die binnen het netwerk van Breedband kan worden gebruikt. Het is duidelijk dat niet alle onderdelen in het ontwerp gereed zijn voor gebruik in productie. Verdere ontwikkeling van het geheel is noodzakelijk. Hieronder zijn de onderdelen benoemd die nog niet volwassen genoeg zijn voor implementatie. Bij de onderdelen zijn de acties beschreven die moeten worden ondernomen om deze wel te kunnen implementeren.

CPE met geïntegreerde lwB4 ondersteuning.

Er is een CPE nodig die aan de eisen voldoet van RFC8585. Op moment van schrijven zijn er geen COTS-routers beschikbaar die alle benodigde functies ondersteunen. Waar andere grote partijen ervoor kiezen om op maat gemaakte software te (laten) schrijven voor hun eigen white label routers, is het voor Breedband verstandig te kijken naar open source oplossingen. OpenWRT biedt potentie voor het ondersteunen van lw4o6, maar vereist de nodige verbeteringen voordat dit kan worden gerealiseerd. OpenWRT bevat de package 'map' voor het configureren van een lw4o6-verbinding. De volgende onderdelen werken daarin niet:

- Een tunnel wordt automatisch opgezet met een encapsulation-limit. Dat resulteert erin dat de destination option header wordt toevoegt aan het IPv6-pakket. De lwAFTR van Snabb ondersteunt geen IPv6-pakketten met extra headers (Snabbco, 2016), waardoor alle pakketten met deze header worden genegeerd.
- Configuratie van NAT-vertalingen werkt niet correct. De berekening van de poortreeks komt niet overeen met de opgegeven variabelen. Tevens wordt het geconfigureerde gedeelde IPv4-adres genegeerd en wordt in de plaats daarvan een gegenereerd foutief IPv4-adres gebruikt. De configuratie scripts van de 'map' package moeten in het geheel worden herzien.

Lw4o6 provisioning.

Provisioning hangt samen met het inrichten van de lwB4- en de lwAFTR-functies.

- Het gebrek aan een werkende lwB4-functie betekent dat het automatisch inrichten daarvan nog niet mogelijk is. Het is van belang de lwB4-functie werkend te krijgen en op basis van die oplossing de provisioning in te richten. DHCPv6 wordt aangeraden op basis van werkend bewijs bij partijen als OTE en DT.
- Het automatisch inrichten van lwAFTR-functies bevat verschillende opties. Er is geen standaard optie. Andere partijen gebruiken hier handmatige oplossingen voor die niet open source zijn gemaakt. Het is belangrijk om dit proces samen te laten lopen met de provisioning van de lwB4 en hangt dus samen met het punt hierboven.

Het ontwerp heeft als input veel ontwerpprincipes uit het literatuuronderzoek gebruikt. De gebruikte ontwerpprincipes zijn hieronder opgesomd. De onderbouwing hiervoor is te vinden in bijlage J.

- | | | | | |
|--------|--------|--------|---------|---------|
| • OP1; | • OP4; | • OP7; | • OP10; | • OP25; |
| • OP2; | • OP5; | • OP8; | • OP11; | • OP26. |
| • OP3; | • OP6; | • OP9; | • OP15; | |

Het succes van het ontwerp is te spiegelen aan de requirements uit de paragrafen 4.1.2, 4.4.2 en aan de randvoorwaarden. Aan de randvoorwaarden wordt volledig voldaan. Uit de ontwerpevaluatie blijkt dat niet alle functies mogelijk zijn zoals gewenst. Hierdoor zijn bij het testen aanpassingen gemaakt op het gewenste ontwerp. Hoewel het gewenste ontwerp met genoeg doorontwikkeling mogelijk is, is het op dit moment nog niet haalbaar. De requirements zijn daarom dubbel beoordeeld, zowel op de status van nu, als op de potentie van het ontwerp. De beoordeling is te vinden in Tabel 17 op de volgende pagina.

#	Requirement (S.M.A.R.T.)	Prioriteit	Status	Potentie
B01	Er komt een ontwerp dat de toepassing van de gewenste oplossing beschrijft.	Must	Ja	Ja
B02	Er komt een prototype dat de werkzaamheid van het ontwerp kan weergeven.	Must	Ja	Ja
B03	Er komt een haalbaarheidsrapport die de haalbaarheid van de toepassing van lw4o6 binnen Breedband aantoon.	Must	Ja	Ja
B04	De oplossing beperkt de groei belemmering van IPv4-exhaustion.	Should	Ja	Ja
B05	De klant ondervindt geen last van een implementatie van de oplossing.	Should	Ja	Ja
B06	De oplossing is open source.	Could	Ja	Ja
U01	De oplossing is volledig compatible met het IPv4-internet.	Must	Ja	Ja
U02	De oplossing beperkt het gebruik van IPv4 adressen.	Must	Ja	Ja
U03	De CPE van de oplossing ondersteunt IPv6 in het LAN-netwerk.	Could	Nee	Ja
Op dit moment is er geen COTS-CPE beschikbaar die lwB4 in zijn totaliteit ondersteunt. Zonder CPE kan deze requirement niet worden behaald. Het is echter wel haalbaar, maar vereist verdere ontwikkeling van de software.				
U04	De CPE van de oplossing ondersteunt IPv4 in het LAN-netwerk.	Must	Nee	Ja
Op dit moment is er geen COTS-CPE beschikbaar die lwB4 in zijn totaliteit ondersteunt. Zonder CPE kan deze requirement niet worden behaald. Het is echter wel haalbaar, maar vereist verdere ontwikkeling van de software.				
U05	De CPE van de oplossing is benaderbaar via een public IPv4 adres.	Must	Nee	Ja
Op dit moment is er geen COTS-CPE beschikbaar die lwB4 in zijn totaliteit ondersteunt. Zonder CPE kan deze requirement niet worden behaald. Het is echter wel haalbaar, maar vereist verdere ontwikkeling van de software.				
U06	De werking van de oplossing is inzichtelijk met monitoring-tools.	Could	Nee	Ja
Op dit moment is het nog niet geïmplementeerd in het ontwerp omdat de focus is gebleven bij de cruciale functies. Geschikte monitoring is slecht te realiseren wanneer de eindproducten nog niet definitief zijn.				
U07	In het onderzoek worden alternatieven transitie-technieken vergeleken.	Should	Ja	Ja
U08	Het prototype toont het ontwerp aan met minimaal vier (virtuele) CPE's.	Should	Nee	Ja
Het prototype toont er geen vier omdat de functie niet in één geheel kan worden getoond.				
U09	De oplossing ondersteunt telefonie via de CPE.	Should	Ja	Ja
S01	Het ISP-netwerk is IPv6-gebaseerd.	Should	Ja	Ja
S03	De oplossing werkt in combinatie met Cisco-routers.	Could	Ja	Ja
S04	De CPE ondersteunt UPnP.	Should	Nee	Ja
Op dit moment is er geen COTS-CPE beschikbaar die lwB4 in zijn totaliteit ondersteunt. Zonder CPE kan deze requirement niet worden behaald. Het is echter wel haalbaar, maar vereist verdere ontwikkeling van de software.				
S05	Er is geen SPOF in het access netwerk.	Should	Ja	Ja
S06	Voor provisioning van CPE's moeten DHCPv6-options worden gebruikt.	Should	Ja	Ja
S07	Voor loadbalancing van lwAFTR's moet een anycast-adres worden gebruikt.	Could	Ja	Ja

Tabel 17. Requirements beoordeling

6. Conclusies en aanbevelingen

In deze scriptie is onderzoek gedaan naar het antwoord op de onderzoeksvraag. Het antwoord hierop vormt een conclusie van waaruit een advies kan worden uitgebracht.

“Hoe kan Breedband de dreiging van IPv4-exhaustion beperken totdat IPv6 de standaard wordt?”

De impact die Breedband ondervindt van IPv4-exhaustion is groot. Het kost veel tijd en geld om voldoende voorraad IPv4-adressen aan te houden om klanten te kunnen voorzien van diensten. De oplossing voor de gebrekkige IPv4-adresruimte is IPv6. Breedband moet hier efficiënter gebruik van maken. Om het gebruik van IPv4-adressen te beperken, zijn verschillende IPv6 transitie technieken beschikbaar. Breedband heeft interesse in lw4o6, wat op het moment van schrijven de meest interessante transitie techniek is voor het bedrijf.

Lw4o6 is een transitie techniek die in de theorie compleet is, maar voor praktische toepassing een systeem in ontwikkeling is. Het voordeel van lw4o6 is de open source beschikbaarheid en de behulpzame community voor de benodigde functies om de techniek te realiseren. Lw4o6 heeft zich bewezen bij verschillende partijen zoals Deutsche Telekom en OTE. Het implementeren van lw4o6 vereist de realisatie van drie functies, waarbij op bepaalde vlakken handmatig werk vereist is.

- **lwb4;**
De lwb4 vereist een CPE die deze functie ondersteunt. Er is geen COTS CPE die dit mogelijk maakt. OpenWRT is open source routersoftware die op veel hardware wordt ondersteunt. OpenWRT heeft potentie om een lwb4 functie te realiseren. Op het moment van schrijven bevat de software een programma met als doel om onder andere lwb4 te ondersteunen. Het programma voor lwb4 werkt echter niet goed en vereist veel werk van een programmeur om werkend te krijgen. De gebreken zijn te vinden in bijlage E.
- **lwaftr;**
De lwaftr is beschikbaar in open source netwerksoftwarepakket 'Snabb'. De functie is gemakkelijk en virtueel inzetbaar. Hieraan hoeven geen handmatige wijzigingen te worden aangebracht, met uitzondering van de configuratie voor samenwerking met de andere functies van lw4o6.
- **Provisioning.**
Voor het dynamisch inrichten en beheren van lw4o6 speelt provisioning een belangrijke rol. Er zijn verschillende systemen die hieraan kunnen bijdragen, maar er is geen vaste oplossing voor. De partijen uit het inspirerend voorbeeld maken gebruik van DHCPv6 voor het inrichten van de lwb4. Zij maken daarnaast gebruik van handmatige scripts (met onbeschreven backbone) voor het inrichten van de lwaftr.

Een samenvattende beschrijving van de haalbaarheid van een transitie naar lw4o6 voor Breedband, is opgesteld en bijgevoegd in bijlage K.

Discussie

In het onderzoek is duidelijk geworden hoe belangrijk de IPv6 transitie is voor de ontwikkeling van het internet. Ook laat het onderzoek zien hoe weinig dit bij de eindgebruiker speelt. De transitie naar IPv6 moet dus volledig worden uitgevoerd vanuit de ISP's. Er zijn verschillende technieken beschikbaar voor een transitie. Lw4o6 is een techniek met de meeste raakvlakken voor kleine en middelgrote ISP's. De open source beschikbaarheid en stateless-aard van lw4o6 maakt de techniek makkelijk te verantwoorden als oplossing. Maar hoe verstandig is het implementeren en wat doet de techniek in de toekomst? Over de toekomst is lastig iets te zeggen, maar als onderzoeker wel over te speculeren. Lw4o6 is een schaalbare methode om IPv4 te kunnen uitfasen. Doordat lw4o6 naast het delen van IPv4-adressen ook volledige IPv4-adressen kan verwerken, is het mogelijk om alle soorten klanten te dienen over een lw4o6 netwerk. De lwaftr-functie in lw4o6 is door grote partijen, zoals DT en OTE, gerealiseerd met een open source toolkit, Snabb, waardoor de ontwikkeling van het systeem levendig blijft. De lwb4-functie wordt minder breed opgepakt in de open source community, omdat deze door grote partijen handmatig wordt toegevoegd aan white label hardware. De vraag naar een open source lwb4 oplossing is dus niet groot. Met aanvullende ontwikkeling aan OpenWRT is lwb4 werkend te krijgen op deze open source router software. Als dit beschikbaar komt in de community wordt lw4o6 toegankelijker voor kleine ISP's en kan de transitie techniek op den duur meer draagvlak krijgen.

Advies

Op basis van de conclusie is het volgende advies bepaald. Breedband moet voor efficiënt gebruik van de beperkte IPv4-adressen zo veel mogelijk overgaan op IPv6. Om dat te realiseren is lw4o6 een goede oplossing. De techniek is echter niet direct te implementeren. Om dit wel mogelijk te maken moeten de volgende punten nog worden aangepakt:

- De software voor de lwB4-functie in OpenWRT herschrijven en terugkoppelen aan de community zodat dit onderhouden wordt;
- Een provisioning-oplossing inrichten met DHCPv6 voor lwB4. Ook moet een efficiënte manier gevonden worden om deze provisioning te repliceren naar de lwAFTR.

De bovenstaande punten vereisen uitgebreide kennis van programmeren. Het kan interessant zijn om hiervoor een softwareontwikkelaar in te schakelen. Met dit onderzoek als basis kan de vervolgonwikkeling een interessante afstudeeropdracht vormen voor een student met meer achtergrond in softwareontwikkeling.

Bibliografie

- Abrahamsson, M. (2018). *DT Terastream 2018*. Opgehaald van Ripe.net: <https://www.ripe.net/support/training/ripe-ncc-educa/presentations/mikael-abrahamsson-dtag.pdf>
- Abrahamsson, M. (2018, juni 14). *Session 4 - RIPE NCC::Educa - IPv6 Day - IPv6 Implementations*. Opgehaald van Youtube: <https://www.youtube.com/watch?v=6IN5mvidPnw&feature=youtu.be&t=43>
- American Psychological Association. (2010). *Publication manual of the American Psychological Association*, (6e ed.). Washington, DC.
- APNIC. (2019, juli 4). *Use of IPv6 for Western Europe (QO)*. Opgehaald van APNIC Labs: <https://stats.labs.apnic.net/ipv6/QO>
- Avenue4 LLC. (2019, maart 22). *2018 State of the IPv4 Market*. Opgehaald van Avenue4 LLC: <http://avenue4llc.com/wp-content/uploads/2019/03/Avenue4-2018-State-of-the-IPv4-Market.pdf>
- Bagnulo, M., Matthews, P., & van Beijnum, I. (2011). Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. doi:10.17487/RFC6146
- Bernstein, D. J. (z.d.). *The IPv6 mess*. Opgehaald van Crypto: <https://cr.yp.to/djbdns/ipv6mess.html>
- Bhakhra, S. (z.d.). *Difference between Stateless and Stateful Protocol*. Opgehaald van GeeksforGeeks: <https://www.geeksforgeeks.org/difference-between-stateless-and-stateful-protocol/>
- Boucadair, M., & Farrer, I. (2016, november). *Unified IPv4-in-IPv6 Softwire Customer Premises Equipment (CPE)*. doi:10.17487/RFC8026
- Boucadair, M., Durand, A., Levis, P., & Roberts, P. (2011). Issues with IP Address Sharing. doi:10.17487/RFC6269
- Brook, C. (2018, december 5). *What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More*. Opgehaald van Digital Guardian: <https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more>
- Brown, T. (2018, augustus 8). *Scrum vs. kanban: Which agile framework is better?* Opgehaald van OpenSource: <https://opensource.com/article/19/8/scrum-vs-kanban>
- Carpenter, B. E., & Jung, C. (1999). Transmission of IPv6 over IPv4 Domains without Explicit Tunnels. doi:10.17487/RFC2529
- Carpenter, B. E., & Moore, K. (2001). Connection of IPv6 Domains via IPv4 Clouds. doi:10.17487/RFC3056
- Cheshire, S., & Kochmal, M. (2013, april). *NAT Port Mapping Protocol (NAT-PMP)*. doi:10.17487/RFC6886
- Chuangchunsong, N., Kamolphiwong, S., Kamolphiwong, T., Elz, R., & Pongpaibool, P. (2014). Performance evaluation of IPv4/IPv6 transition mechanisms: IPv4-in-IPv6 tunneling techniques. *The International Conference on Information Networking 2014 (ICOIN2014)*, 238-243. doi:10.1109/ICOIN.2014.6799698
- Cisco. (z.d.). *Broadband Network Gateway Overview*. Opgehaald van Cisco: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/bng/configuration/guide/b-bng-cg52xasr9k/b-bng-cg52xasr9k_chapter_010.pdf
- Conta, A., & Deering, S. (1998, december). *Generic Packet Tunneling in IPv6 Specification*. doi:10.17487/RFC2473
- Cormack, A. (2018, april 4). *IP Addresses, Privacy and the GDPR*. Opgehaald van Jisc: <https://community.jisc.ac.uk/blogs/regulatory-developments/article/ip-addresses-privacy-and-gdpr>
- Cox, J. (2019, juni 5). *Access Control List (ACL) – What are They and How to Configure Them!* Opgehaald van ITT Systems: <https://www.ittsystems.com/access-control-list-acl/>
- Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y. L., & Farrer, I. (2015, juli). *Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture*. doi:10.17487/RFC7596
- Dam, R., & Siang, T. (2019, januari). *Design Thinking: Get Started with Prototyping*. Opgehaald van Interaction Design Foundation: <https://www.interaction-design.org/literature/article/design-thinking-get-started-with-prototyping>
- Dec, W., Li, X., Bao, C., Matsushima, S., & Murakami, T. (2015). Mapping of Address and Port with Encapsulation (MAP-E). doi:10.17487/RFC7597
- Deering, S. E., & Hinden, R. M. (2017, juli). *Internet Protocol, Version 6 (IPv6) Specification*. doi:10.17487/RFC8200
- Despres, R., Penno, R., Lee, Y., Chen, G., & Chen, M. (2015). IPv4 Residual Deployment via IPv6 - A Stateless Solution (4rd). doi:10.17487/RFC7600
- Deutsche Telekom. (2018). *Deutsche Telekom - The 2018 financial year*. Opgehaald van Deutsche Telekom: http://report.telekom.com/annual-report-2018/servicepages/downloads/files/entire_dtag_ar18.pdf?pk_campaign=lp_pdf
- Donaldson, R. (2011, juni 2). *DHCP for IPv4 vs. IPv6 - What You Need to Know*. Opgehaald van CircleID: http://www.circleid.com/posts/dhcp_for_ipv4_vs_ipv6_what_you_need_to_know/
- Droms, R. (1997, maart). *Dynamic Host Configuration Protocol*. doi:10.17487/RFC2131

- Durand, A., Droms, R., Woodyatt, J., & Lee, Y. L. (2011, augustus). *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*. doi:10.17487/RFC6333
- Eastlake 3rd, D. E., & Abley, J. (2013, oktober). *IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters*. doi:10.17487/RFC7042
- Emerce. (2018, september 25). *KPN en Ziggo traag met invoering IPv6*. Opgehaald van Emerce: <https://www.emerce.nl/nieuws/kpn-ziggo-traag-invoering-ipv6>
- Ergun, O. (2016, mei 27). *What is MP-BGP – Multiprotocol BGP*. Opgehaald van OrhanErgun: <https://orhanergun.net/2016/05/mp-bgp-multiprotocol-bgp/>
- Europese Commissie. (2006, april 13). Parliament and Council directive of data retention. *Directive 2006/24/EC of the European Parliament and of the Council*. Opgehaald van <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>
- Europol. (2017, februari 2). *Closing the online crime attribution gap; European law enforcement tackles carrier-grade NAT (CGN)*. Opgehaald van Europol: <https://www.europol.europa.eu/newsroom/news/closing-online-crime-attribution-gap-european-law-enforcement-tackles-carrier-grade-nat-cgn>
- Farinacci, D., Li, T., Hanks, S., & Meyer, D. (2000, maart). *Generic Routing Encapsulation*. doi:10.17487/RFC2784
- Ford, M., Boucadair, M., Durand, A., Levis, P., & Roberts, P. (2011, juni). *Issues with IP Address Sharing*. doi:10.17487/RFC6269
- García, D. P. (2017, juni 5). *Dive into Lightweight 4over6*. Opgehaald van Igalia: <https://blogs.igalia.com/dpino/2017/06/05/dive-into-lw4o6/>
- García, D. P. (2018, mei 22). *Lightweight 4-over-6: One step further Dual-Stack Lite Networks (RIPE 76)*. Opgehaald van YouTube: <https://youtu.be/CF9S11RXJlk?t=1590>
- Gerich, E. (1993, mei). *Guidelines for Management of IP Address Space*. doi:10.17487/RFC1466
- Gorrie, L., Wingo, A., Rottenkolber, M., Wiget, M., & Hartlage, R. (2018, april 13). *Snabb*. Opgehaald van GitHub: <https://github.com/snabbco/snabb/blob/max-next/README.md>
- GrafanaLabs. (z.d.). *The analytics platform for all your metrics*. Opgehaald van GrafanaLabs: <https://grafana.com/grafana/>
- Grit, R. (2011). Een interview afnemen. In R. Grit, *Projectmanagement* (6e ed., pp. 155-158). Houten, Groningen, Nederland: Noordhoff Uitgevers. Opgeroepen op mei 16, 2019
- Grit, R. (2016). Beheersaspecten TGKIO en risico's. In R. Grit, *P6-Methode* (2e ed., pp. 21-24). Houten, Groningen, Nederland: Noordhoff Uitgevers.
- Haletky, E. L. (2017, april 17). *Things That Go Bump in the Wire*. Opgehaald van AstroArch: https://www.astroarch.com/tvp_strategy/things-that-go-bump-in-the-wire-40059/
- Haveman, K., Hageraats, E., & Van der Linden, S. (2016, september). Ontwerponderzoek. *Reader Ontwerponderzoek, v2*.
- Hinden, R. M., & Deering, S. E. (2006, februari). *IP Version 6 Addressing Architecture*. Opgeroepen op mei 20, 2019, van Internet Engineering Task Force: <https://tools.ietf.org/html/rfc4291>
- Hinden, R. M., & Deering, S. E. (2006, februari). *IP Version 6 Addressing Architecture*. doi:10.17487/RFC4291
- Hirotsu, D. (2016, oktober). *NFV vs. VNF: What's the difference?* Opgehaald van TechTarget: <https://searchnetworking.techtarget.com/answer/NFV-vs-VNF-Whats-the-difference>
- Hogg, S. (2007, september 5). *IPv6: Dual stack where you can; tunnel where you must*. Opgehaald van NetworkWorld: <https://www.networkworld.com/article/2285078/ipv6-dual-stack-where-you-can-tunnel-where-you-must.html>
- Howard, L. (2019, februari 10). *Address Pricing: 2019 and Beyond*. Opgehaald van Retevia: <https://www.retevia.net/address-pricing-2019-and-beyond/>
- IANA. (z.d.). *About us*. Opgehaald van IANA: <https://www.iana.org/about>
- ICANN. (z.d.). *ICANN History Project*. Opgehaald van ICANN: <https://www.icann.org/history>
- IMU. (2016, mei 10). *DESTEP analyse*. Opgehaald van Internet Marketing Unie: <https://imu.nl/internet-marketing-kennisbank/begrippen/destep-analyse/>
- InfluxData. (z.d.). *InfluxDB*. Opgehaald van InfluxData: <https://www.influxdata.com/products/influxdb-overview/>
- Internet Society. (2017). *State of IPv6 Deployment*. Opgeroepen op mei 20, 2019, van Internet Society: https://www.internetsociety.org/wp-content/uploads/2017/08/IPv6_report_2017-0606.pdf
- Ionos. (2019, maart 26). *VLAN | What is a virtual local area network?* Opgehaald van Ionos: <https://www.ionos.com/digitalguide/server/know-how/vlan-basics/>
- ISC. (z.d.). *ISC DHCP*. Opgehaald van ISC: <https://www.isc.org/dhcp/>
- ISC. (z.d.). *KEA*. Opgehaald van ISC: <https://kea.isc.org/>
- Janse, B. (2018). *Multicriteria-analyse (MCA)*. Opgehaald van Toolshero: <https://www.toolshero.nl/besluitvorming/multicriteria-analyse-mca/>
- Janssen, D. (z.d.). *8 Steps to Understanding IP Subnetting*. Opgehaald van Technopedia: <https://www.techopedia.com/6/28587/internet/8-steps-to-understanding-ip-subnetting>

- Jensen, B. (2019, juli 11). *For Networking Geeks Only: Why Router-on-a-Stick is Good*. Opgehaald van CEPro: https://www.cepro.com/news/networking_geeks_why_router_on_a_stick_is_good/
- Jiang, S., Guo, D., & Carpenter, B. (2011). An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition. doi:10.17487/RFC6264
- Krul, A. (2017, april 20). *Zo doe je een literatuuronderzoek of literatuurstudie*. Opgehaald van Scribbr: <https://www.scribbr.nl/scriptie-structuur/hoe-doe-je-literatuuronderzoek/>
- Li, X., Bao, C., & Baker, F. (2011). IP/ICMP Translation Algorithm. doi:10.17487/RFC6145
- Li, X., Bao, C., Troan, O., Matsushima, S., & Murakami, T. (2015). Mapping of Address and Port using Translation (MAP-T). doi:10.17487/RFC7599
- Martínez, J. P. (2017, november 9). *CE vendors share their thoughts on IPv6 support*. Opgehaald van APNIC: <https://blog.apnic.net/2017/11/09/ce-vendors-share-thoughts-ipv6-support/>
- Mathis, M., & Heffner, J. W. (2007). Packetization Layer Path MTU Discovery. doi:10.17487/RFC4821
- Mawatari, M., Kawashima, M., & Byrne, C. (2013). 464XLAT: Combination of Stateful and Stateless Translation. doi:10.17487/RFC6877
- McCarthy, K. (2018, april 18). *OK, this time it's for real: The last available IPv4 address block has gone*. Opgeroepen op mei 2019, 2019, van The Register: https://www.theregister.co.uk/2018/04/18/last_ipv4_address/
- McNamara, P. (2016, juli 27). *Why Belgium leads the world in IPv6 adoption*. Opgehaald van Network World: <https://www.networkworld.com/article/3100968/why-belgium-leads-the-world-in-ipv6-adoption.html>
- Mhay, S., & Coburn, C. (2019, september 15). *What's The Difference Between Contract RFT RFQ RFP RFI?* Opgehaald van Negotiations: <https://www.negotiations.com/articles/procurement-terms/>
- Mitchell, B. (2019, mei 22). *What Happened to IPv5?* Opgehaald van Lifewire: <https://www.lifewire.com/what-happened-to-ipv5-3971327>
- Mogul, J. (1984, oktober). *Broadcasting internet datagrams*. doi:10.17487/RFC0919
- Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M. C., Jiang, S., . . . Winters, T. (2018, november). *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. doi:10.17487/RFC8145
- Mrugalski, T., Troan, O., Farrer, I., Perreault, S., Dec, W., Boa, C., . . . Deng, X. (2015, juli). *DHCPv6 for Software 46 CEs*. doi:10.17487/RFC7598
- Mukherjee, A. (z.d.). *IPv6 subnetting - how and why to subnet IPv6*. Opgehaald van Firewall: <http://www.firewall.cx/networking-topics/protocols/877-ipv6-subnetting-how-to-subnet-ipv6.html>
- Narten, T., Nordmark, E., Simpson, W. A., & Soliman, H. (2007, september). *Neighbor Discovery for IP version 6 (IPv6)*. doi:10.17487/RFC4861
- NFWare. (2018, november 6). *How bad is IPv4 address exhaustion?* Opgeroepen op mei 20, 2019, van NFWare: <https://nfware.com/blog-ipv4-limitations>
- Nordmark, E., & Gilligan, R. E. (2005). Basic Transition Mechanisms for IPv6 Hosts and Routers. doi:10.17487/RFC4213
- NRO. (2011, februari 3). *Free Pool of IPv4 Address Space Depleted*. Opgehaald van NPO: <https://www.nro.net/ipv4-free-pool-depleted>
- Object Management Group. (2017, december 5). *OMG Unified Modeling Language*. Opgehaald van Object Management Group: <https://www.omg.org/spec/UML/2.5.1/PDF>
- Offerman, A., Boerman, N., Davids, M., & van Duijnhoven, M. (2018, september). *Slow IPv6 migration and industry's short-sighted outlook represent problem for The Netherlands Inc.* Opgehaald van SIDN: https://assets.ctfassets.net/yj8364fopk6s/YWwjAY5yRXW0e3hTiGRqfQ/6195a3f343ce33c32852ad1f7929f467/IPv6_Inventory_2018_021118.pdf
- OpenWRT. (2019, juli 2). *Welcome to the OpenWrt Project*. Opgehaald van OpenWRT: <https://openwrt.org/>
- Papachristou, H. (2009, juni 18). *UPDATE 2-Greece to sell 5 pct OTE stake to Deutsche Telekom*. Opgehaald van Reuters: <https://www.reuters.com/article/greece-ote/update-2-greece-to-sell-5-pct-ote-stake-to-deutsche-telekom-idUSLI45104020090618>
- Parker, J. (2012, februari 18). *Business, User, and System Requirements*. Opgehaald van Enfocuss Solutions: <http://enfocussolutions.com/business-user-and-system-requirements/>
- Pepelnjak, I. (2013, november 18). *Deutsche Telekom TeraStream: Designed for Simplicity*. Opgehaald van ipSpace.net: <https://blog.ipspace.net/2013/11/deutsche-telekom-terastream-designed.html>
- Pepelnjak, I. (2013, november 27). *Terastream Part 2: Lightweight 4over6 and Network Function Virtualization (NFV)*. Opgehaald van ipSpace.net: <https://blog.ipspace.net/2013/11/terastream-part-2-lightweight-4over6.html>
- Plummer, D. C. (1982, november). *An Ethernet Address Resolution Protocol*. doi:10.17487/RFC0826
- Poortinga, E. (z.d.). *Deskresearch en literatuuronderzoek: het verschil*. Opgehaald van Studiemeesters: <https://www.studiemeesters.nl/studietips/verschil-tussen-deskresearch-literatuuronderzoek-theorie/>

- Postel, J. (1981, september). *Internet Protocol*. doi:10.17487/RFC0791
- Rekhter, Y., Bonica, R. P., & Rosen, E. C. (2007, januari). *Use of Provider Edge to Provider Edge (PE-PE)*. doi:10.17487/RFC4797
- Rekhter, Y., Li, T., & Hares, S. (2006, januari). *A Border Gateway Protocol 4 (BGP-4)*. doi:10.17487/RFC4271
- Richter, P., Allman, M., Bush, R., & Paxson, V. (2015). A Primer on IPv4 Scarcity. *ACM SIGCOMM Computer Communication Review*, 45(2), 21-31. doi:10.1145/2766330.2766335
- Rigney, C., Rubens, A. C., Simpson, W. A., & Willens, S. (2000, juni). *Remote Authentication Dial In User Service (RADIUS)*. doi:10.17487/RFC2865
- Rijksuniversiteit Groningen. (2018, december 21). *Wat is goede literatuur?* Opgehaald van Rijksuniversiteit Groningen: <https://www.rug.nl/sciencelinx/betasteunpunt/pwsmaken/betrouwbareliteratuur/betrouwbareliteratuur>
- Riley, P. (2018, augustus 31). *Understanding Single Points of Failure (SPOF)*. Opgehaald van Gigamon: <https://blog.gigamon.com/2018/08/31/understanding-single-points-of-failure/>
- Rosen, E. C., Viswanathan, A., & Callon, R. (2001, januari). *Multiprotocol Label Switching Architecture*. doi:10.17487/RFC3031
- Rouse, M. (2010, april). *COTS, MOTS, GOTS, and NOTS*. Opgehaald van TechTarget: <https://searchdatacenter.techtarget.com/definition/COTS-MOTS-GOTS-and-NOTS>
- Rouse, M. (2010, oktober). *CPE device*. Opgehaald van TechTarget: <https://whatis.techtarget.com/definition/CPE-device>
- Schuurmans, E. (2016, augustus 29). *In 5 stappen een praktische stakeholderanalyse*. Opgehaald van Lean en Kwaliteit: <https://www.leanenkwaliteit.nl/blog/5-stappen-praktische-stakeholderanalyse/>
- SDxCentral. (2013, augustus 26). *What is NFV - Network Functions Virtualization - Definition?* Opgehaald van SDxCentral: <https://www.sdxcentral.com/networking/nfv/definitions/whats-network-functions-virtualization-nfv/>
- Singalar, S., & Banakar, R. M. (2018). Performance Analysis of IPv4 to IPv6 Transition Mechanisms. *Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*. doi:10.1109/ICCUBEA.2018.8697539
- Singh, H., BeeBee, W., Donley, C., & Stark, B. (2013, november). *Basic Requirements for IPv6 Customer Edge Routers*. doi:10.17487/RFC7084
- Snabbco. (2016, december 9). *RFC 7596 compliance*. Opgehaald van GitHub: <https://github.com/snabbco/snabb/blob/master/src/program/lwaftr/doc/rfccompliance.md>
- Snabbco. (2018, april 13). *Snabb*. Opgehaald van GitHub: <https://github.com/snabbco/snabb>
- SolidBE. (2017, juni 6). *IPv6 in een notendop*. Opgehaald van SolidBE: <https://solidbe.nl/nl/tech/networking/ipv6-in-een-notendop/>
- Sridhar. (2017, mei 15). *What is Subscriber Management System?* Opgehaald van Quora: <https://www.quora.com/What-is-Subscriber-Management-System>
- Srisuresh, P., & Egevang, K. B. (2001, januari). *Traditional IP Network Address Translator (Traditional NAT)*. doi:10.17487/RFC3022
- Tadayoni, R., & Henten, A. (2015, november 7). From IPv4 to IPv6: Lost in translation? *Telematics and Informatics*, pp. 650-659. doi:10.1016/j.tele.2015.10.004
- Takikawa, A., Bristow, P., Wingo, A., & Rottenkolber, M. (2017, september 26). *Intel i210 / i350 / 82599 Ethernet Controller apps*. Opgehaald van GitHub: https://github.com/snabbco/snabb/tree/master/src/apps/intel_mp
- Tamminga, E. (2015, september). *Mijn ervaringen als ICT deskundige*. Opgehaald van Ernst Peter Tamminga: <https://www.ernstpeter tamminga.nl/Blog/articleType/ArticleView/articleId/55/MoSCoW-Prioriteiten-in-een-IT-project>
- Tardi, C. (2019, april 10). *White Label Product*. Opgehaald van Investopedia: <https://www.investopedia.com/terms/w/white-label-product.asp>
- Templin, F. L., Gleeson, T., & Thaler, D. (2008). Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). doi:10.17487/RFC5214
- The Open Group. (2017, augustus). *Welcome to the ArchiMate® 3.0.1 Specification, an Open Group Standard*. Opgehaald van The Open Group: <https://pubs.opengroup.org/architecture/archimate3-doc/>
- Townsley, M., & Troan, O. (2010). IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification. doi:10.17487/RFC5969
- van Klinken, T. (2019, juni 6). Subscriber Management.
- van Staa, A., & Evers, J. (2010). 'Thick analysis': strategie om de kwaliteit van kwalitatieve data-analyse te verhogen. *KWALON*(43), 5-12.
- VMware. (2019, mei 31). *Add a PCI Device*. Opgehaald van VMware Docs: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-

- 5B3CAB26-5D06-4A99-92A0-3A04C69CE64B.html?hWord=N4IghgNiBcICYEsBOBTaxgFwAQIPQHsQBfIA
- VMware. (z.d.). *VMware ESXi: The Purpose-Built Bare Metal Hypervisor*. Opgehaald van VMware: <https://www.vmware.com/products/esxi-and-esx.html>
- Vyncke. (2019, mei 21). *Comparison of IPv6 IPv6-Enabled Web Browsers (courtesy Google) in Different Countries*. Opgehaald van Vyncke: <https://www.vyncke.org/ipv6status/compare.php?metric=p&countries=nl,be,de,gb>
- White, R. (2017, december 5). *SLAAC and DHCPv6*. Opgehaald van Rule11: <https://rule11.tech/slaac-and-dhcpv6/>
- Wing, D., Cheshire, S., Boucadair, M., Penno, R., & Selkirk, P. (2013, april). *Port Control Protocol (PCP)*. doi:10.17487/RFC6887
- Wing, D., Cheshire, S., Boucadair, M., Penno, R., & Selkirk, P. (2013, April). *Port Control Protocol (PCP)*. doi:10.17487/RFC6887
- Wu, J., Cui, Y., Li, X., & Metz, C. (2010). 4over6 Transit Solution Using IP Encapsulation and MP-BGP Extensions. doi:10.17487/RFC5747
- Zhu, A. (2016, juni 25). *Introduction to Optical Add-Drop Multiplexer (OADM)*. Opgehaald van Medium: <https://medium.com/@AriaZhu/introduction-to-optical-add-drop-multiplexer-oadm-4c161b90fad3>
- Zijlstra, W. (2011, maart 3). *Een kwaliteitsreview verhoogt de kwaliteit meetbaar*. Opgeroepen op mei 16, 2019, van ZBC Kennisbank: <https://zbc.nu/management/kwaliteitsmanagement-systemen-en-iso-9001/een-kwaliteitsreview-verhoogt-de-kwaliteit-meetbaar/>
- Zorbadelos, K. (2018, mei 12). *Towards IPv6 Only: A large scale lw4o6 deployment*. Opgehaald van Ripe: <https://ripe76.ripe.net/archives/video/30/>
- Zorbadelos, K., & Nikolopoulos, Y. (2018, juli 4). *A Large-scale lw4o6 Deployment for Broadband Users in Greece*. Opgehaald van Ripe NCC: <https://labs.ripe.net/Members/kzorba/a-large-scale-lw4o6-deployment-for-broadband-users-in-greece>

Bijlage A: Interview projectdefinitie

Algemeen

Wat is het probleem waar Breedband nu tegenaan kijkt omtrent het komende onderzoek?

IPv4 adressen worden schaarser en daardoor steeds kostbaarder. Daarnaast is er een steeds grotere wens van (vooral Power Users) om ook IPv6 connectiviteit te krijgen.

Hoe wordt er nu omgegaan met het probleem?

Op dit moment hebben we nog een kleine voorraad IPv4 adressen. Deze gebruiken we op dit moment. Op het moment dat deze "op" zijn kunnen we gaan investeren in nieuwe adressen of zorgen dat we een beter schaalbare oplossing hebben.

Waarom is er gekeken naar 'lw4over6'?

Deze oplossing lost beide issues op. Doordat een IPv4 adres opgesplitst kan worden kunnen IPv4 adressen gedeeld tussen meerdere klanten waardoor we deze effectiever kunnen gebruiken. Tevens heb je native IPv6 support.

Is er ook gekeken naar alternatieven?

Zo ja, waarom is dat niet onderdeel van dit onderzoek?

We zijn al jaren naar het kijken naar oplossingen, maar er is er geen die beide uitdagingen tegelijk oplost en vaak lost het maar 1 van beide problemen op. Vele oplossingen voegen daardoor vooral complexiteit toe of worden snel heel kostbaar. Technieken zoals DS-Lite vertrouwen namelijk op CGN (Carrier Grade NAT) wat een zeer dure en slecht schaalbare oplossing is. De andere techniek die erg veel belovend is, is MAP (Mapping of Address and Port). Deze techniek heeft echter weinig draagkracht.

Zo nee, waarom is er niet verder gekeken, maar gelijk gekozen voor 'lw4over6'?

Lw4over6 is een van de nieuwste technieken, maar heeft in korte tijd veel draagkracht gekregen. Er duiken steeds meer implementaties op en wordt ook in de praktijk gebruikt.

Wat is het doel dat moet worden bereikt met een oplossing?

Bijvoorbeeld: Kostenbesparing, Directe vraag van een klant, beheer-technische verbeteringen?

We moeten werken naar een toekomst vaste oplossing waarbij we een voor de klant goed werkende oplossing leveren en hierbij de nieuwe vorm van connectiviteit leveren (IPv6) en ondertussen zorgen dat IPv4 diensten probleemloos te benaderen zijn en dat zonder de kostprijs van het product explosief te moeten laten stijgen.

Welke producten verwacht u aan het einde van het onderzoek te ontvangen?

Bijvoorbeeld: Haalbaarheidsonderzoek, Ontwerp voor implementatie, Proof of Concept

Mijn vermoeden is dat er veel componenten beschikbaar zijn, maar dat er nog een aantal onderdelen missen. Ik zou graag weten wat deze zijn om dit weer als uitgangspunt te kunnen gebruiken voor een volgende afstudeerder.

Wat is de scope van het onderzoek?

Bijvoorbeeld: Welk gedeelte van de infrastructuur (wel of niet op locatie bij klanten). Dit onderzoek zal intern plaatsvinden. Belangen liggen vooral bij techniek en management.

Zijn er randvoorwaarden waaraan het onderzoek moet voldoen?

Zo ja, welke randvoorwaarden zijn er?

Bijvoorbeeld: Alleen onderzoeken naar Open-Source oplossingen

Er is een voorkeur voor Open-Source en het moet werken in combinatie met ons bestaande Cisco IOS XR gebaseerde netwerk. Het is wel van belang dat de Open Source pakketten actief onderhouden worden, mocht dit niet beschikbaar zijn dan kan closed-source ook overwogen worden. Keuze voor CPE is vrij.

Haalbaarheidsonderzoek

Welke informatie omtrent is precies gewenst in het haalbaarheidsonderzoek?

Bijvoorbeeld: Alleen een oordeel of 'lw4over6' mogelijk is. (of meer?)

Het moet duidelijk zijn hoe volwassen deze techniek is en welke gaten er op dit moment nog zijn in de beschikbare implementaties.

Proof of Concept

Met wat voor hardware kan een Proof of Concept worden gemaakt?

Bijvoorbeeld: Een specifieke fysieke server met virtualisatie mogelijkheden.

Er is een VMWare ESX server beschikbaar om VM's te draaien. Op deze server is tevens een aan ons netwerk gekoppelde IOS XRv router beschikbaar die van dezelfde software voorzien is als de rest van ons netwerk.

Zijn er strikte randvoorwaarden waaraan het Proof of Concept moet voldoen?

Bijvoorbeeld: Mag alleen open-source zijn.

Nee.

Wat is de scope van een Proof of Concept?

Hoeveel netwerken moeten er minimaal kunnen werken met het prototype?

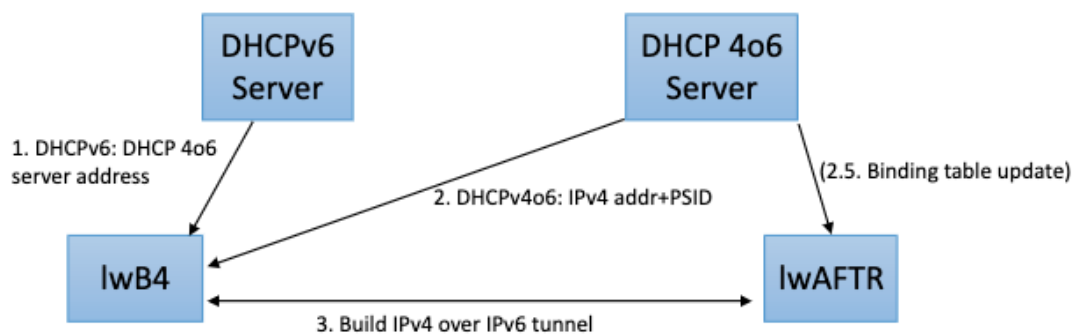
Bijvoorbeeld: Een aantal netwerken als demo, of een specifieke range.

Minimaal 4 CPE's

Welke systemen moeten werkend worden aangetoond in het prototype?

Bijvoorbeeld: Een lijst met specifieke hardware die in realiteit ook wordt gebruikt (maar dan in grote aantallen).

Dit plaatje werkend op een aantal VM's met in totaal 4 lwB4 CPE's met daarachter een test-pc die zowel met IPv4 als IPv6 het internet op kan:



Verder is er een wens dat UPNP gaat werken op de lwB4 gateway.

Slotvraag

Heeft u nog iets toe te voegen wat u vindt dat ook besproken had moeten worden?

Nee.

Bijlage B: Interview management

Vragen

Bent u bekend met het project dat onderzoek doet naar 'lw4over6'?

Nee, toelichting is gegeven.

Heeft IPv4-exhaustion impact op managementvlak?

IPv4 is nodig om klanten te belevaren als ISP. Onvoldoende IPv4-adressen zou betekenen dat je je bestaande klanten niet kan dienen bij groei en nieuwe klanten zonder eigen IP-adressen überhaupt niet kan dienen. In commercieel opzicht betekent IPv4-exhaustion dat de groei wordt belemmerd.

Hebben jullie manieren om klanten te overtuigen om iets aan IPv4-exhaustion te doen?

Er is geen beleid om klanten naar IPv6 te pushen. IPv6 wordt nu alleen op aanvraag geboden. Dit is vooral omdat klanten het nog niet helemaal begrijpen. De pijn van IPv4-exhaustion wordt nu opgevangen door de ISP's, de klanten zelf nog niet. Klanten zullen hier zelf ook niet zomaar wat aan doen omdat zij zelf de pijn niet voelen. "Als het niet kapot is, gaan ze het niet repareren". Dit is vooral gericht op consumenten en MKB'ers. Grote organisaties hebben dit vaak wel op orde.

Wat zijn management overwegingen om een oplossing te vinden voor IPv4-exhaustion?

Als ISP moet je zuinig omgaan met IPv4-adressen. De kosten van IPv4-adressen stijgen, waardoor bedrijven met diepe zakken meer macht hebben in de IPv4 markt. Het is daarom van belang om hier een oplossing voor te hebben zodat je ook als kleinere ISP kunt blijven concurreren in de markt.

Heeft management specifiek belang bij 'lw4over6', of meer voor een algemene oplossing voor IPv4-exhaustion?

Er is geen voorkeur voor oplossing. Het gaat er vooral om dat er een oplossing komt. IPv6 transitie technieken worden soms als tijdelijk gezien, tot dat IPv6 volledig geïmplementeerd is. Alleen "niets is zo permanent als een tijdelijke oplossing". Er moet dus een oplossing worden gevonden die op lange termijn mee kan.

Bijlage C: Zoekstrategie

Om structureel antwoord te vinden op de deelvragen die aan bod komen in het literatuuronderzoek, wordt gebruik gemaakt van zoekvragen. Per deelvraag zijn één of meer zoekvragen gedefinieerd waar specifiek op kan worden gezocht. Het collectieve antwoord op de zoekvragen biedt een antwoord op de deelvraag. Hieronder zijn de zoekvragen per deelvraag weergegeven.

4. Hoe biedt IPv6 een oplossing voor de gebreken van IPv4?

- 4.1 Wat is de aanleiding voor het ontwikkelen van IPv6?
- 4.2 Waarvoor wordt IPv6 gebruikt?
- 4.3 Hoe werkt IPv6?
- 4.4 In welke mate wordt IPv6 al toegepast?

5. Hoe kan IPv6 worden bereikt door middel van 'lw4over6'?

- 5.1 Wat is lw4o6?
- 5.2 Uit welke componenten bestaat lw4o6?

6. Welke alternatieve manieren zijn er om van IPv4 naar IPv6 te migreren?

- 6.1 Welke alternatieve transitie-technieken zijn beschikbaar?
- 6.2 Hoe staan alternatieve transitie-technieken tegenover lw4o6?

7. Welke eventuele risico's zijn er tijdens of na een migratie?

- 7.1 Welke risico's ontstaan bij gebruik van lw4o6 bij de klant (ontvangende kant)?
- 7.2 Welke risico's ontstaan bij gebruik van lw4o6 bij de aanbieder (ISP)?

Om tot geschikte bronnen te komen wordt op basis van de bovenstaande zoekvragen, of vervoegingen ervan, gezocht in de volgende databanken:

- Google
- Google Scholar
- IEEEExplore
- HBO Kennisbank
- Web of Science
- IETF (RFC Databank)

Bijlage D: Bronbeoordeling

Bron	Auteur	Doel	Actuali- teit	Versie	Referenties	Overeenkomsten	Gevonden via
(Tadayoni & Henten, 2015)	Geen opmerkingen over auteur	Informeren over de status van IPv6	2015	Officieel gepubliceerde versie	Er worden methodisch referenties gebruikt en genoteerd	Informatie komt overeen met soortgelijke bronnen	Web of Science
(Richter, Allman, Bush, & Paxson, 2015)	Geen opmerkingen over auteur	Informeren over de exhaustion van IPv4	2015	Officieel gepubliceerde versie	Er worden methodisch referenties gebruikt en genoteerd	Informatie komt overeen met soortgelijke bronnen	Web of Science
(Janssen, z.d.)	Onderbouwde achtergrond in netwerken	Informeren over de werking van subnets	Geen datum beschikbaar	Artikel zonder versienotering	Referenties worden gegeven met URLs	Informatie komt overeen met soortgelijke bronnen	Google
(Postel, 1981)	Erkend door IETF	Informeren over IPv4	1981	RFC: Internet Standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(NRO, 2011)	Erkende bron op netwerkgebied	Informeren over IPv4 depletion	2011	Artikel zonder versienotering	Geen referenties gebruikt	Informatie komt overeen met soortgelijke bronnen	Google
(Mitchell, 2019)	Geen opmerkingen over auteur	Informeren over IPv5	2019	Artikel zonder versienotering	Referenties worden gegeven met URLs	Informatie komt overeen met soortgelijke bronnen	Google
(Solidbe, 2017)	Bedrijf met duidelijke kennis in netwerken	Informeren over IPv6	2017	Artikel zonder versienotering	Geen referenties gebruikt	Informatie komt overeen met soortgelijke bronnen	Google

Tabel 18. Bronbeoordeling (deel 1 van 6)

BREEDBAND

Bron	Auteur	Doel	Actualiteit	Versie	Referenties	Overeenkomsten	Gevonden via
(Mukherjee, z.d.)	Bedrijf met duidelijke kennis in netwerken	Informeren over IPv6 subnetten	Geen datum beschikbaar	Artikel zonder versienotering	Geen referenties gebruikt	Informatie komt overeen met soortgelijke bronnen	Google
(Deering & Hinden, 2017)	Erkend door IETF	Informeren over IPv6	2017	RFC: Internet Standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(White, 2017)	Auteur met meerdere artikelen in netwerken	Informeren over SLAAC en DHCP	2017	Artikel zonder versienotering	Geen referenties gebruikt	Informatie komt overeen met soortgelijke bronnen	Google
(McNamara, 2016)	Auteur van bedrijf met achtergrond in netwerken	Informeren over IPv6 status in België	2016	Artikel zonder versienotering	Als referentie een interview met erkende expert op het gebied van netwerken	Informatie komt overeen met soortgelijke bronnen	Google
(Offerman, Boerman, Davids, & van Duijnhoven, 2018)	Auteurs van erkende Nederlandse organisatie in netwerken	Informeren over IPv6 status in Nederland	2018	Officieel gepubliceerde versie	In tekst gebruikte referenties	Orginele afkomst van informatie	Google
(Emerce, 2018)	Erkende nieuwssite voor technieuws	Informeren over IPv6 status in Nederland	2018	Artikel zonder versienotering	In tekst gebruikte referenties	Informatie komt overeen met soortgelijke bronnen	Google
(Cui, et al., 2015)	Erkend door IETF	Informeren over transitie techniek lw4o6	2015	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF

Tabel 19. Bronbeoordeling (deel 2 van 6)

BREEDBAND

Bron	Auteur	Doel	Actuali-teit	Versie	Referenties	Overeenkomsten	Gevonden via
(Durand, Droms, Woodyatt, & Lee, 2011)	Erkend door IETF	Informereren over transitie techniek ds-lite	2011	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(García, Dive into Lightweight 4over6, 2017)	Erkende expert op gebied van lw4o6	Informereren over lw4o6	2017	Artikel zonder versienotering	Referenties worden gegevens met URLs	Informatie komt overeen met soortgelijke bronnen	Google
(Mrugalski, et al., 2015)	Erkend door IETF	Informereren over DHCPv6 options voor softwires	2015	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Boucadair & Farrer, Unified IPv4-in-IPv6 Softwire Customer Premises Equipment (CPE), 2016)	Erkend door IETF	Informereren over softwire eisen aan CPE's	2016	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Ford, Boucadair, Durand, Levis, & Roberts, 2011)	Erkend door IETF	Informereren over risico's van IP-sharing	2011	RFC: Informational	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Europol, 2017)	Erkende partij voor	Informereren over de gevaren van CGN	2017	Officiële persbericht	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	Google

Tabel 20. Bronbeoordeling (deel 3 van 6)

Bron	Auteur	Doel	Actuali- teit	Versie	Referenties	Overeenkomsten	Gevonden via
(García, Lightweight 4-over-6: One step further Dual-Stack Lite Networks (RIPE 76), 2018)	Erkende expert op gebied van lw4o6	Informeren over de implementatie van lw4o6	2018	Eenmalig optreden	In de presentatie zijn referentie gegeven.	Informatie komt overeen met soortgelijke bronnen	Google
(Martínez, 2017)	Erkende auteur in gebied van netwerken	Informeren over de risico's van CPE veranderingen	2017	Artikel zonder versienotering	Referenties worden gegevens met URLs	Informatie komt overeen met soortgelijke bronnen	Google
(Wu, Cui, Li, & Metz, 2010)	Erkend door IETF	Informeren over transitie techniek 4over6	2015	RFC: Experimental	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Dec, Li, Bao, Matsushima, & Murakami)	Erkend door IETF	Informeren over transitie techniek MAP-E	2015	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Li, Bao, Troan, Matsushima, & Murakami, 2015)	Erkend door IETF	Informeren over transitie techniek MAP-T	2015	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Mathis & Heffner, 2007)	Erkend door IETF	Informeren over MTU	2007	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF

Tabel 21. Bronbeoordeling (deel 4 van 6)

BREEDBAND

Bron	Auteur	Doel	Actuali-teit	Versie	Referenties	Overeenkomsten	Gevonden via
(Despres, Penno, Lee, Chen, & Chen, 2015)	Erkend door IETF	Informereren over transitie techniek 4rd	2015	RFC: Experimental	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Jiang, Guo, & Carpenter, 2011)	Erkend door IETF	Informereren over transitie techniek CGN	2011	RFC: Informational	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Bagnulo, Matthews, & van Beijnum, 2011)	Erkend door IETF	Informereren over de functie CLAT	2011	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Li, Bao, & Baker, IP/ICMP Translation Algorithm, 2011)	Erkend door IETF	Informereren over de functie PLAT	2011	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Mawatari, Kawashima, & Byrne, 2013)	Erkend door IETF	Informereren over transitie techniek 464XLAT	2013	RFC: Informational	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Nordmark & Gilligan, 2005)	Erkend door IETF	Informereren over transitie techniek Overig - 6in4	2005	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF

Tabel 22. Bronbeoordeling (deel 5 van 6)

BREEDBAND

Bron	Auteur	Doel	Actuali- teit	Versie	Referenties	Overeenkomsten	Gevonden via
(Carpenter & Moore, 2001)	Erkend door IETF	Informereren over transitie techniek Overig - 6to4	2001	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Townesley & Troan, 2010)	Erkend door IETF	Informereren over transitie techniek Overig - 6rd	2010	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Carpenter & Jung 1999)	Erkend door IETF	Informereren over transitie techniek Overig - 6over4	1999	RFC: Proposed standard	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Templin, Gleeson & Thaler, 2008)	Erkend door IETF	Informereren over transitie techniek Overig - ISATAP	2008	RFC: Informational	Er worden methodisch referenties gebruikt en genoteerd	Officiële bron van informatie	IETF
(Singalar en Banakar, 2018)	Erkend door ICCUBEA	Informereren over verschillen van IPv6 transitie technieken	2018	Officieel gepubliceerde versie	Er worden methodisch referenties gebruikt en genoteerd	Informatie komt overeen met soortgelijke bronnen	IEEXPLORE
(Chuangchunson g, Kamolphiwong, Kamolphiwong, Elz, & Pongpaibool, 2014)	Erkend door ICOIN	Informereren over verschillen van IPv6 transitie technieken	2014	Officieel gepubliceerde versie	Er worden methodisch referenties gebruikt en genoteerd	Informatie komt overeen met soortgelijke bronnen	IEEXPLORE

Tabel 23. Bronbeoordeling (deel 6 van 6)

Bijlage E: Status lwB4 OpenWRT

Om duidelijk te krijgen wat nodig is om lwB4 werkend te krijgen op OpenWRT is opgesomd wat de status is van de verschillende eisen:

- **IPv4 in IPv6 encapsulation**
 - De MAP-package is in staat om een IPIP6-tunnel op te zetten, echter is de tunnel standaard geconfigureerd met een encapsulation-limit dat ervoor zorgt dat er een destination options header (DSTOPT) wordt toegevoegd. De destination options header wordt niet ondersteund door de Snabb lwAFTR en dropt alle packets met deze header. De functie beschrijft dat deze optie is uit te schakelen, maar een bug in de software zorgt ervoor dat dit vooralsnog niet mogelijk is.
 - De tunnel wordt opgezet met een gegenereerd IPv6-adres waardoor configuratie moeilijk te matchen is met de configuratie in de software-tabel.
- **NAT44 & NATPT**
 - De MAP-package is in staat om IPv4-verkeer te vertalen naar een gedeeld IPv4-adres en een beperkte poortreeks. Door fouten in de software is deze functie echter nog niet betrouwbaar. Zowel de berekening van het gedeelde IPv4-adres als de berekening voor de beperkte poortreeks is niet betrouwbaar.
- **DHCPv6 client**
 - De client ondersteunt de configuratie van standaard IPv6 diensten zoals statische IPv6-adressen en prefix-delegation. De router is in staat de prefix automatisch te delegeren naar het LAN-netwerk zodat clients achter de router over global IPv6-adressen beschikken.
 - De client is in staat om option S46 op te vragen. Echter kan deze nog niet worden verwerkt, omdat de lwB4 functie nog niet werkend is.

Bijlage F: Virtuele OpenWRT

Deze bijlage bevat een handleiding voor het opstellen van een OpenWRT router in een ESXi-omgeving.

1. Creëer een nieuwe virtuele machine in ESXi met:
 - a. 1 CPU
 - b. 2GB RAM (initieel benodigd)
 - c. Minimale aanbevolen opslag
 - d. 1 netwerkadapter in het 0100_innovatie-mgmt netwerk
 - e. Guest OS: Ubuntu Linux (32-bit)
2. Download een Live-CD om te kunnen booten. Voor dit voorbeeld wordt 4MLinux gebruikt:
<http://4mlinux.com/index.php?page=home>
3. Mount de Live-CD op de VM en start de VM via deze CD.
4. Configureer handmatig de netwerkadapter:
 - a. IP-adres: 192.168.240.149
 - b. Netmask: 255.255.255.224
 - c. Gateway: 192.168.240.129
 - d. DNS: 46.226.57.6 en 46.226.57.6
5. Start de CLI en voer de volgende commando's uit:
Let op: [tab] duidt het gebruik van de tab-toets aan zodat de bestandsnaam wordt aangevuld.

```
wget https://downloads.openwrt.org/releases/18.06.4/targets/x86/generic/openwrt-18.06.4-x86-generic-combined-ext4.img.gz
gunzip openwrt-[tab]
dd if=openwrt-[tab] of=/dev/sda
poweroff
```

Vervang de URL wanneer een andere versie van OpenWRT is gewenst.

6. Pas de instellingen van de VM aan:
 - a. Zet RAM naar 256mb
 - b. Verander het netwerk van de netwerkadapter naar 3401_innovatie_wan6
 - c. Voeg netwerkadapter toe voor de LAN-interface (0112-stg-csmlan2)
 - d. Verwijder de CD/DVD-drive.

Wanneer de VM nu wordt gestart wordt een schone installatie van OpenWRT gestart.

Bijlage G: Ubuntu lwB4

Deze bijlage bevat de specifieke configuratie van de lwB4 op stg-demo-cpe2 in het prototype.

Configuratie routing

Voor configuratie van de routing worden eerst de network-interfaces ingesteld:

```
nano /etc/netplan/50-cloud-init.yaml
```

Daarvoor worden de adapters ens192 (WAN) en ens224 (LAN) als volgt geconfigureerd:

```
network:
  ethernets:
    ens192:
      dhcp6: true
    ens224:
      addresses:
        - 192.168.2.1/24
      dhcp4: false
      nameservers:
        addresses:
          - 46.226.56.6
          - 46.226.57.6
        search: []
      mtu: 1460
  version: 2
```

Om forwarding mogelijk te maken dient dit te worden toegestaan in de ufw:

```
ufw enable
nano /etc/ufw/sysctl.conf
```

Uncomment de onderstaande regel in deze configuratie:

```
net/ipv4/ip_forward=1
```

Daarna worden de volgende forward regels ingesteld in iptables:

```
#Default rules
iptables -P INPUT DROP
iptables -P FORWARD DROP

#Accept LAN & LO traffic
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i ens224 -j ACCEPT

#Accept incoming established WAN
iptables -A INPUT -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT

#Forward LAN to WAN
iptables -A FORWARD -I ens224 -o mytun -j ACCEPT

#Forward WAN to LAN on established connections
iptables -A FORWARD -i ens192 -o ens224 -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i mytun -o ens224 -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT
```

Om het LAN-netwerk in te delen dient er een DHCP-server te draaien, daarvoor wordt het volgende geïnstalleerd:

```
apt install isc-dhcp-server
nano /etc/dhcp/dhcpd.conf
```

Voor de DHCP worden de volgende handmatige aanpassingen in de configuratie gebruikt:

```
option domain-name-servers 46.226.56.6, 46.226.57.6

subnet 192.168.2.0 netmask 255.255.255.0 {
  range 192.168.2.100 192.168.2.199;
  option subnet-mask 255.255.255.0;
  option routers 192.168.2.1;
  option broadcast-address 192.168.2.255;
  option interface-mtu 0x05B4;
}
```

Configuratie lwB4

Voor configuratie van een lwB4 wordt het onderstaande script gebruikt, deze is opgeslagen op `"/home/user/lwb4_deploy.sh"`.

```
#!/bin/bash
#Let op: voer uit met bash, de standaard shell in Ubuntu is dash, die ondersteunt geen <<<

#Set variables
INT=ens192                                #Interface (e.g.: eth0)
LWB4IP4="31.3.10.115"                    #Shared IP address for lwB4 (e.g.: 192.0.2.10)
LWB4IP4SUF="29"                          #Shared IP address suffix (e.g.: 24)
LWB4IP6="2a00:c080:1:12::102"            #IPv6 address for lwB4 (e.g.: 2001:db8::1)
LWAFTRIP6="2a00:c080:1:12::150"          #IPv6 address for lwAFTR (e.g.: 2001:db8::9)
PCIDEV="0000:0b:00.0"                    #PCIDevice for networkadapter (e.g.: 000:0b:00.0)
DNS1="46.226.56.6"                      #DNS-Server1 (e.g.: 8.8.8.8)
DNS2="46.226.57.6"                      #DNS-Server2 (e.g.: 8.8.4.4)
PSIDLEN=6                                #Port-set length (e.g.: 6)
PSID=2                                    #Port-set ID (e.g.: 1)

#Calculate IP Network
IFS=. read -r i1 i2 i3 i4 <<< $LWB4IP4
IFS=. read -r xx m1 m2 m3 m4 <<< $(for a in $(seq 1 32); do if [ $((a - 1) % 8)) -eq 0 ]; then echo -n .; fi;
if [ $a -le $LWB4IP4SUF ]; then echo -n 1; else echo -n 0; fi; done)
LWB4IP4PRE=$(printf "%d.%d.%d.%d\n" "$((i1 & (2#$m1)))" "$((i2 & (2#$m2)))" "$((i3 & (2#$m3)))" "$((i4 & (2#$m4)))")

#Calculate port-set
psidlenrevert=$((2 ^ $PSIDLEN) - 1)
portstart=$((psidlenrevert * $PSID) | bc)
portend=$((psidlenrevert * ($PSID + 1)) - 1 | bc)
PORTRANGE="$portstart-$portend"

ip addr flush dev $INT
ip -6 addr flush dev $INT
ip -6 tunnel del mytun mode ipip6
iptables -t nat --flush
ip r del default via 192.168.240.129

sh -c "echo -n $PCIDEV > /sys/bus/pci/drivers/ixgbe/bind" 2>/dev/null

ip link set dev $INT up
ip addr add $LWB4IP4/$LWB4IP4SUF dev $INT
ip -6 addr add fc00::1/64 dev $INT
ip -6 tunnel add mytun mode ipip6 remote $LWAFTRIP6 local $LWB4IP6 dev $INT encaplimit none
ip link set dev mytun up
ip -6 addr add $LWB4IP6 dev mytun
ip -6 addr add $LWB4IP6 dev $INT
ip route add default dev mytun
iptables -t nat -A POSTROUTING -p tcp -o mytun -j SNAT --to $LWB4IP4:$PORTRANGE
iptables -t nat -A POSTROUTING -p udp -o mytun -j SNAT --to $LWB4IP4:$PORTRANGE
iptables -t nat -A POSTROUTING -p icmp -o mytun -j SNAT --to $LWB4IP4:$PORTRANGE
ip r add default via $LWB4IP4PRE dev $INT

sudo echo "nameserver $DNS1" >> /etc/resolv.conf
sudo echo "nameserver $DNS2" >> /etc/resolv.conf
```

Om de configuratie automatisch te starten wordt het onderstaande geplaatst in /etc/rc.local

```
#!/bin/bash

#Execute lwB4-script
bash /home/user/lwb4_deploy.sh

#Default rules
iptables -P INPUT DROP
iptables -P FORWARD DROP

#Accept LAN & LO traffic
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i ens224 -j ACCEPT

#Accept incoming established WAN
iptables -A INPUT -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT

#Forward LAN to WAN
iptables -A FORWARD -I ens224 -o mytun -j ACCEPT

#Forward WAN to LAN on established connections
iptables -A FORWARD -i ens192 -o ens224 -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i mytun -o ens224 -m conntrack -ctstate ESTABLISHED,RELATED -j ACCEPT

#Confirm NAT rules
iptables -t nat -A POSTROUTING -p tcp -o mytun -j SNAT --to 31.3.10.115:2048-3191
iptables -t nat -A POSTROUTING -p udp -o mytun -j SNAT --to 31.3.10.115:2048-3191
iptables -t nat -A POSTROUTING -p icmp -o mytun -j SNAT --to 31.3.10.115:2048-3191

exit 0
```

Bijlage H: IwAFTR configuratie

```
software-config {
  instance {
    device "0b:00.0";
    queue {
      id 0;
      external-interface {
        ip 31.3.10.114;
        // mac ac:f2:c5:ed:c9:98;
        mac ac:f2:c5:ed:c9:9a;
        vlan-tag 3400;
        next-hop {
          mac 08:96:ad:91:c2:3f;
          //ip 31.3.10.113;
        }
      }
      internal-interface {
        ip 2a00:c080:1:12::150;
        mac ac:f2:c5:ed:c9:99;
        vlan-tag 3401;
        next-hop {
          mac 08:96:ad:91:c2:3f;
          //ip 2a00:c080:1:12::1;
        }
      }
    }
  }
}
external-interface {
  allow-incoming-icmp true;
  error-rate-limiting {
    packets 600000;
    period 2;
  }
  generate-icmp-errors true;
  mtu 1460;
  reassembly {
    max-fragments-per-packet 40;
    max-packets 20000;
  }
}
internal-interface {
  allow-incoming-icmp true;
  error-rate-limiting {
    packets 600000;
    period 2;
  }
  generate-icmp-errors true;
  hairpinning true;
  mtu 1500;
  reassembly {
    max-fragments-per-packet 40;
    max-packets 20000;
  }
}
binding-table {
  software {
    ipv4 31.3.10.115;
    psid 1;
    b4-ipv6 2a00:c080:1:12::101;
    br-address 2a00:c080:1:12::150;
    port-set {
      psid-length 6;
    }
  }
}
software {
  ipv4 31.3.10.115;
  psid 2;
  b4-ipv6 2a00:c080:1:12::102;
  br-address 2a00:c080:1:12::150;
  port-set {
    psid-length 6;
  }
}
```

}
}
}
}

Bijlage I: Kea DHCPv6 config

```
{
  "Dhcp6": {
    "interfaces-config": {
      "interfaces": ["ens256"]
    },
    "lease-database": {
      "type": "memfile",
      "persist": false,
      "name": "/var/lib/kea/leases6.csv"
    },
    "expired-leases-processing": {
      "reclaim-timer-wait-time": 10,
      "flush-reclaimed-timer-wait-time": 25,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 250,
      "unwarned-reclaim-cycles": 5
    },
    "renew-timer": 1000,
    "rebind-timer": 2000,
    "preferred-lifetime": 86400,
    "valid-lifetime": 172800,
    "option-data": [
      {
        "name": "dns-servers",
        "data": "2a00:c080:1:1::2, 2a00:c080:1:2::2"
      }
    ],
    "subnet6": [
      {
        "subnet": "2a00:c080:1:12::/64",
        "interface": "ens256",
        "pools": [ { "pool": "2a00:c080:1:12::200/120" } ],
        "reservations": [
          {
            "duid": "00:01:00:01:24:e9:36:45:00:0c:29:08:4e:b9",
            "ip-addresses": [ "2a00:c080:1:12::101" ],
            "prefixes": [ "2a00:c080:1:18::/64" ]
          },
          {
            "duid": "00:04:cb:c0:79:8e:af:e7:95:2a:f6:76:25:5d:67:40:c6:ff",
            "ip-addresses": [ "2a00:c080:1:12::102" ],
            "prefixes": [ "2a00:c080:1:19::/64" ]
          }
        ]
      }
    ]
  }
}
```

Bijlage J: Ontwerpprincipe gebruik

OP#	Ontwerpprincipe	Gebruikt	Reden
OP1	Als IPv4 onvoldoende IPv4-adressen biedt, dan moet IPv6 worden gebruikt, omdat IPv6 ruim voldoende adressen kan aanbieden voor de toekomst (Tadayoni & Henten, 2015).	Ja	IPv6 wordt gebruikt als basis, zodat IPv4 gebruikt kan worden beperkt.
OP2	Als IPv4 uitputting op distributie-niveau moet worden aangepakt, dan is het van belang om algemene richtlijnen voor distributie te volgen, omdat de richtlijnen onnodige uitgave van IPv4-adressen beperken (Gerich, 1993).	Ja	Er zijn geen aanpassingen in distributie, er wordt alleen beperkt op de uitgave dus heeft dit een positieve impact.
OP3	Als IPv4-exhaustion een probleem is voor een organisatie, dan moet er een netwerk-transitie plaatsvinden naar IPv6-only met IPv4-as-a-service, omdat IPv6 voldoende adresruimte heeft en met de juiste transitie-techniek is IPv4 alsnog mogelijk te maken als een service (Boucadair, et al., 2012).	Ja	Lw4o6 wordt geïmplementeerd.
OP4	Als IPv6-netwerken moeten worden ingericht, dan moet zoveel mogelijk gebruik worden gemaakt van SLAAC, omdat dit het netwerk flexibeler maakt en er minder stateful-configuraties nodig zijn (White, 2017).	Ja	In het LAN-netwerk wordt SLAAC automatisch geïmplementeerd zodat er geen complexe configuraties met betrekking tot IPv6 LAN op de CPE.
OP5	Als IPv6-adressen structureel moeten worden beheerd, dan moet DHCPv6 in het netwerk worden geïmplementeerd, omdat DHCPv6 de IPv6-adressering kan beheren binnen een netwerk en daarbij gewenste DHCPv6-options kan meegeven (White, 2017).	Ja	In het ISP-netwerk wordt DHCPv6 gebruikt voor configuratie van CPE's.
OP6	Als een IPv6-transitie grootschalig wordt toegepast, dan is het van belang de oplossing zo stateless mogelijk te maken, omdat stateful functies de schaalbaarheid en beheerbaarheid aanzienlijk verslechteren (Boucadair, et al., 2012).	Ja	lw4o6 biedt een per-subscriber-state, wat nagenoeg stateless is te implementeren.
OP7	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van lw4o6, omdat lw4o6 een transitie biedt met per-subscriber-state en schaalbare netwerkfuncties en mogelijkheid tot het delen van IP-adressen (Cui, et al., 2015).	Ja	Lw4o6 wordt geïmplementeerd.
OP8	Als men lw4o6 wil implementeren, dan moeten minimaal de functies lwB4 en lwAFTR worden gerealiseerd, omdat deze twee functies de basis vormen voor lw4o6 en het verkeer van IPv4 over het IPv6-netwerk mogelijk maken (Cui, et al., 2015).	Ja	Beide functies worden meegenomen in het ontwerp.
OP9	Als een lwAFTR wordt geconfigureerd, dan moet er gebruik worden gemaakt van de open source Snabb toolkit, omdat dit de enige succesvolle open source implementatie is van deze netwerkfunctie (García, 2017).	Ja	Snabb lwAFTR wordt gebruikt.

Tabel 24. Gebruik van ontwerpprincipes (deel 1 van 3)

OP#	Ontwerpprincipe	Gebruikt	Reden
OP10	Als een lwB4 moet worden geconfigureerd, dan moet OpenWRT worden gebruikt met enige handmatige aanpassingen, omdat OpenWRT ondersteuning biedt voor de lwB4 functie, maar door gebreken nog niet 100% inzetbaar is (García, 2017).	Ja	Het ontwerp is gericht op OpenWRT, het advies onderbouwt de verdere aanpassingen die nodig zijn voor complete ondersteuning.
OP11	Als een software wordt opgesteld, dan moet PSID '0' altijd worden overgeslagen, omdat dit conflicten oplevert met standaard services op standaard poortnummers (García, 2017).	Ja	Dit is een standaard in de implementatie van Snabb lwAFTR.
OP12	Als een software-tabel moet worden opgesteld, dan moet hiervoor een provisioning service worden ingericht, omdat de service alle functies gelijktijdig zou kunnen updaten zodat schaling gemakkelijker is toe te passen (Cui, et al., 2015).	Nee	In het ontwerp is nog geen oplossing gevonden voor provisioning omdat het van belang is dat dit wordt afgestemd op provisioning van lwB4. Omdat de lwB4 nog niet is vastgesteld is dit niet mogelijk.
OP13	Als een provisioning-service wordt ingericht voor lw4o6, dan moet deze service een lwB4 kunnen voorzien van configuratie, omdat handmatige configuratie van de lwB4-functies de beheerbaarheid van het systeem verhoogt (Cui, et al., 2015).	Nee	In het ontwerp is nog geen oplossing gevonden voor provisioning omdat het van belang is dat dit wordt afgestemd op provisioning van lwB4. Omdat de lwB4 nog niet is vastgesteld is dit niet mogelijk.
OP14	Als een provisioning-service wordt ingericht voor lw4o6, dan moet deze service een lwAFTR kunnen voorzien van configuratie, omdat elke lwAFTR op de hoogte moet zijn van alle softwares om de omgeving foutloos te laten draaien (Cui, et al., 2015).	Nee	In het ontwerp is nog geen oplossing gevonden voor provisioning omdat het van belang is dat dit wordt afgestemd op provisioning van lwB4. Omdat de lwB4 nog niet is vastgesteld is dit niet mogelijk.
OP15	Als een lwB4 op afstand moet worden ingericht, dan moet gebruik worden gemaakt van DHCPv6-options, omdat IANA een specifieke set aan DHCPv6-options heeft gedefinieerd voor software-configuratie (Mrugalski, et al., 2015).	Ja	Het ontwerp bevat DHCPv6 met S46-options. Het is echter nog niet geïmplementeerd in het prototype door gebrek aan lwB4 ondersteuning.
OP16	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van MAP-E, omdat MAP-E een volledig stateless transitie-techniek biedt met mogelijkheid tot het delen van IP-adressen (Dec, Li, Bao, Matsushima, & Murakami).	Nee	Er is gekozen voor lw4o6, waardoor dit ontwerpprincipe komt te vervallen.
OP17	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van MAP-T, omdat MAP-T een volledig stateless transitie-techniek biedt met mogelijkheid tot het delen van IP-adressen (Li, Bao, Troan, Matsushima, & Murakami, 2015).	Nee	Er is gekozen voor lw4o6, waardoor dit ontwerpprincipe komt te vervallen.
OP18	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van DS-Lite, omdat DS-Lite een transitie-techniek met per-flow state en goed beheerbaar is en mogelijkheid biedt tot het delen van IP-adressen (Durand, Droms, Woodyatt, & Lee, 2011).	Nee	Er is gekozen voor lw4o6, waardoor dit ontwerpprincipe komt te vervallen.

Tabel 25. Gebruik van ontwerpprincipes (deel 2 van 3)

OP#	Ontwerpprincipe	Gebruikt	Reden
OP19	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van 4over6, omdat 4over6 een stateless transitie-techniek is met gebruik van tunneling (Wu, Cui, Li, & Metz, 2010).	Nee	Er is gekozen voor lw4o6, waardoor dit ontwerpprincipe komt te vervallen.
OP20	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van 4rd, omdat 4rd een volledig stateless transitie-techniek biedt met transparantie in IP-pakketten en het de mogelijkheid om IP-adressen te delen (Despres, Penno, Lee, Chen, & Chen, 2015).	Nee	Er is gekozen voor lw4o6, waardoor dit ontwerpprincipe komt te vervallen.
OP21	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van CGN, omdat CGN een beheerbare NAT-oplossing toepast op het ISP-netwerk om IP-adressen te delen (Boucadair, Durand, Levis, & Roberts, 2011).	Nee	Er is gekozen voor lw4o6, waardoor dit ontwerpprincipe komt te vervallen.
OP22	Als een IPv6-transitie wordt toegepast, dan kan gebruik worden gemaakt van 464XLAT, omdat 464XLAT het mogelijk maakt om IPv4-adres te versturen over een IPv6-netwerk door middel van dubbele NAT (Mawatari, Kawashima, & Byrne, 2013).	Nee	Er is gekozen voor lw4o6, waardoor dit ontwerpprincipe komt te vervallen.
OP23	Als een beperkte poortreeks beschikbaar is voor een eindgebruiker, dan moeten voldoende port-forwarding instructies aanwezig zijn voor correct gebruik van de beperkte poort-reeks, omdat poorten buiten de reeks niet bruikbaar zijn en dit voor gebruikers zonder voldoende kennis ingewikkeld is (Ford, Boucadair, Durand, Levis, & Roberts, 2011).	Nee	Er is nog geen geschikte lwB4 waarop dit kan worden toegepast.
OP24	Als UPnP beschikbaar moet zijn binnen een beperkte poortreeks, dan moet UPnP IGD 2. 0 in combinatie met NAT-PMP (PCP) worden toegepast, omdat oudere versies geen port-negotiation uitvoeren en daardoor falen op verzoeken buiten de poortreeks (Ford, Boucadair, Durand, Levis, & Roberts, 2011).	Nee	Er is nog geen geschikte lwB4 waarop dit kan worden toegepast.
OP25	Als een lw4o6 wordt geïmplementeerd, dan moet de CPE worden vervangen door CPE met voldoende ondersteuning, omdat de lwB4 functie ondersteunt dient te worden de CPE (Martínez, 2017).	Ja	Er is een advies voor vervangen van de CPE, dit vereist wel de nodige verdere ontwikkeling.
OP26	Als IP-adressen worden gedeeld, dan dienen er niet meer dan 16 gebruikers achter een enkel IP-adres te zitten, omdat het delen onder meer gebruikers het opsporen van criminele activiteiten slecht mogelijk maakt (García, Lightweight 4-over-6: One step further Dual-Stack Lite Networks (RIPE 76), 2018).	Ja	Het inrichten van een softwire-tabel is vrij, waardoor gelimiteerd kan worden op het aantal gebruikers op één IP-adres.

Tabel 26. Gebruik van ontwerpprincipes (deel 3 van 3)

Bijlage K: Haalbaarheidsrapport

Inleiding

Dit haalbaarheidsrapport is een product van het onderzoek naar IPv6 transitie technieken en bevat een samenvatting van de resultaten die relevant zijn voor Breedband. In dit document wordt eerst kort de aanleiding voor het onderzoek beschreven, gevolgd door de relevante resultaten van het onderzoek. Daarna wordt een advies gegeven voor vervolgstappen voor Breedband.

Aanleiding

Breedband is een Internet Service Provider (ISP) en heeft daarom als corebusiness het leveren van internetdiensten. Dit doen ze door een eigen netwerk te onderhouden en klanten hierop aan te sluiten. Over het netwerk, net als de rest van het wereldwijde internet, wordt vooral gewerkt met internetprotocol versie 4 (IPv4). Het is al langer bekend dat het aantal bruikbare adressen binnen IPv4 op raken. Hiervoor is een oplossing nodig. Het antwoord op dit probleem is al bekend, namelijk internetprotocol versie 6 (IPv6). IPv6 en IPv4 kunnen standaard niet met elkaar samenwerken en worden daarom vaak naast elkaar gebruikt, dit wordt 'Dual stack' genoemd. Het probleem daarbij blijft dat er IPv4 adressen worden gebruikt en het grootste deel van het verkeer via IPv4 gaat. In een gesprek stelt Tom van Klinken dat, "om het gebruik van IPv4 adressen te beperken, Breedband op zoek is naar een oplossing voor een IPv6-transitie" (persoonlijke communicatie, 10 april 2019). Door een eerder niet-gedocumenteerd kort onderzoek door Breedband is interesse gewekt in de techniek 'lw4over6' (RFC7596) (Cui, et al., 2015). Breedband heeft daarom gericht gevraagd naar een haalbaarheidsrapport van de toepassing van de transitie techniek 'lw4over6'.

Resultaten

Uit uitgebreid onderzoek is gebleken dat de transitie techniek lw4o6 inderdaad de meest geschikte techniek is voor Breedband. De alternatieven met de meeste potentie zijn hieronder opgesomd, met redenen waarom deze minder geschikt zijn dan lw4o6.

- **DS-Lite;**
Lw4o6 is een directe opvolger van DS-Lite waardoor deze techniek niet meer interessant is om uit te rollen. Het belangrijkste verschil is dat lw4o6 de NAT heeft verplaatst naar de CPE, waar DS-Lite dit op provider-niveau uitvoert. Zonder NAT op provider-niveau kan de border-relay nagenoeg stateless worden gerealiseerd.
- **MAP-E/MAP-T;**
MAP is een volwaardig alternatief met een volledig stateless implementatie. Het nadeel van MAP is de open source beschikbaarheid. Bij MAP-E is het vrijwel verplicht om gebruik te maken van Cisco-apparatuur.
- **4rd.**
4rd is een verbeterde variant van MAP met voordelen op gebied van packet-transparancy. 4rd is op dit moment nog experimenteel en niet volwassen genoeg voor implementatie.

Lightweight 4over6

Lw4o6 is een transitie techniek die in de theorie compleet is, maar voor praktische toepassing een systeem in ontwikkeling is. Het voordeel van lw4o6 is de open source beschikbaarheid en de behulpzame community voor de benodigde functies om de techniek te realiseren. Lw4o6 heeft zich bewezen bij verschillende partijen zoals Deutsche Telekom en OTE. Het implementeren van lw4o6 vereist de realisatie van drie functies, waarbij op bepaalde vlakken handmatig werk vereist is.

lwB4

De lwB4 vereist een CPE die deze functie ondersteunt. Er is geen COTS CPE die dit mogelijk maakt. OpenWRT is open source routersoftware die op veel hardware wordt ondersteunt. OpenWRT heeft potentie om een lwB4 functie te realiseren. Op het moment van schrijven bevat de software een programma met als doel om onder andere lwB4 te ondersteunen. Het programma voor lwB4 werkt echter niet goed en vereist veel werk van een programmeur om werkend te krijgen.

De gebreken:

- Een tunnel wordt opgezet met een encapsulation-limit, hierdoor wordt ook de destination option header toevoegt aan het IPv6-pakket. De lwAFTR van Snabb ondersteunt geen IPv6-pakketten met extra headers, waardoor deze standaard worden genegeerd.
- Configuratie van NAT-vertalingen werkt niet correct. De berekening van de poort-set komt niet overeen met de opgegeven variabelen. Tevens wordt het geconfigureerde gedeelde IPv4-adres genegeerd en wordt in de plaats daarvan een gegenereerd foutief IPv4-adres gebruikt. De configuratie scripts van de 'map' package moeten in het geheel worden herzien.

lwAFTR

De lwAFTR is beschikbaar in open source netwerksoftwarepakket 'Snabb'. De functie is gemakkelijk en virtueel inzetbaar. Hieraan hoeven geen handmatige wijzigingen te worden aangebracht, met uitzondering van de configuratie voor samenwerking met de andere functies van lw4o6. De lwAFTR is te configureren op de meeste Linux-gebaseerde x86-64 systemen. Werkend getest op Ubuntu Server 18.04 LTS. Het is van belang dat deze machine directe toegang heeft tot een geschikte NIC.

Provisioning

Voor het dynamisch inrichten en beheren van lw4o6 speelt provisioning een belangrijke rol. Er zijn verschillende systemen die hieraan kunnen bijdragen, maar er is geen vaste oplossing voor. De partijen uit het inspirerend voorbeeld maken gebruik van DHCPv6 voor het inrichten van de lwB4. Daarnaast maken zij gebruik van handmatige scripts (met onbeschreven backbone) voor het inrichten van de lwAFTR. DHCPv6 heeft een set DHCPv6-options die IANA heeft vastgesteld voor Softwire 4-to-6 technieken (S46).

Conclusie en advies

De transitie techniek lw4o6 is een goede oplossing voor Breedband om te besparen op IPv4-adressen. Op het moment van schrijven is de oplossing nog niet volwassen genoeg voor directe implementatie, maar met voldoende verdere ontwikkeling zou dit in de toekomst zeker mogelijk moeten zijn.

Om dit lw4o6 te realiseren zijn de volgende stappen nodig:

- Verbeteren of creëren van een OpenWRT-package voor de lwB4-functie;
- Opstellen van een provisioning-service voor:
 - lwB4;
 - lwAFTR.

Ik adviseer een programmeur of afstudeerder met programmeerachtergrond in te schakelen om de ontbrekende factoren op te stellen. Daarvoor is de volgende opdracht omschrijving te gebruiken.

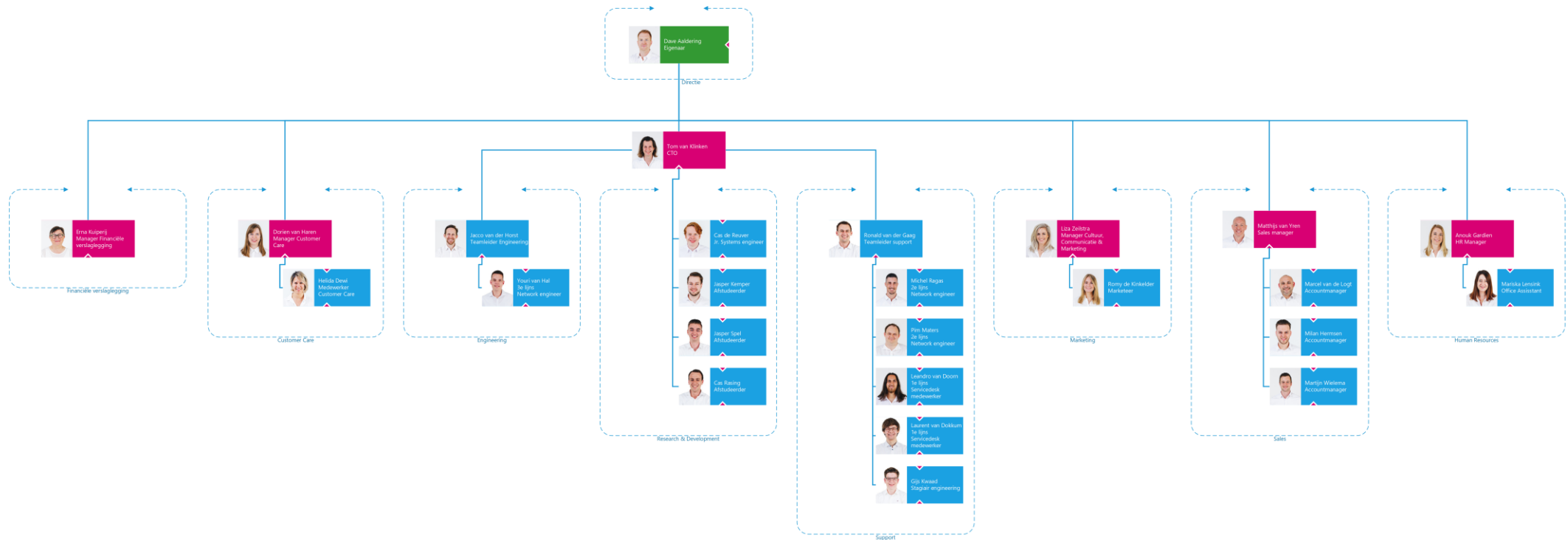
Breedband erkent de dreiging van IPv4-exhaustion en kijkt daarom naar oplossingen. Een voorgaand onderzoek heeft bepaald dat de transitie techniek Lightweight 4over6 (RFC7596) de meest interessante en rendabele oplossing kan bieden. De techniek is volledig open source te realiseren, maar op dit moment nog niet geheel functionerend. Eén van de belangrijkste functies, de lwB4, heeft een package in OpenWRT die ideaal zou zijn voor open source deployment van deze functie. Echter zit deze functie vol fouten.

De opdracht is om de lwB4 package in OpenWRT grondig te analyseren op fouten en deze te corrigeren of herschrijven. Daarbij is het van belang dat deze package kan worden ingericht met een provisioning service zoals DHCPv6. Aanvullend op de lwB4, dient de provisioning hiervan ook te worden geregistreerd in de andere functie, de lwAFTR.

De technieken die hierbij (kunnen) worden gebruikt zijn:

BASH (OpenWRT) – C/C++ (OpenWRT) – YANG (lwAFTR provisioning) – NETCONF (lwAFTR provisioning)
– DHCPv6 (lwB4 provisioning) – IPv6 transitie (netwerk)

Bijlage L: Organigram Breedband



Bijlage M: Multicriteria-analyse transitie technieken

Voor de multicriteria-analyse wordt gekeken naar verschillende criteria van IPv6 transitie technieken. Alle technieken zijn gericht om IPv4 te faciliteren over een IPv6 netwerk. Daarvoor zijn criteria gebruikt die bepalend zijn voor de geschiktheid van de IPv6 transitie techniek. De eerste vijf criteria zijn gekozen aan de hand van de relevantie in de analyse van Chuangchunsong, Kamolphiwong, Kamolphiwong, Elz, & Pongpaibool (2014) en de analyse van Singalar en Banakar (2018). De laatste drie criteria zijn bepaald op basis van de wens van opdrachtgever Tom van Klinken (persoonlijke communicatie, 25 september 2019).

- **Manier:** de manier waarop IPv4 wordt aangeboden over IPv6;
Bepaald aan de hand van informatie uit de officiële RFC van de transitie techniek.
- **Address sharing:** de manier waarop IPv4-adressen worden gedeeld;
Bepaald aan de hand van informatie uit de officiële RFC van de transitie techniek.
- **State management:** de state die op een border relay wordt bijgehouden;
Bepaald aan de hand van informatie uit de officiële RFC van de transitie techniek.
- **Transparency:** de mate van transparantie van het IPv4-pakket;
Bepaald aan de hand van informatie uit de officiële RFC van de transitie techniek.
- **Scalability:** de mate van schaalbaarheid van de oplossing;
Een schatting bepaald door de zwaarte van de benodigdheden aan de provider-kant van de transitie techniek.
- **NAT:** de locatie waar NAT wordt uitgevoerd;
Bepaald aan de hand van informatie uit de officiële RFC van de transitie techniek.
- **Status:** de theoretische status van de techniek, gebaseerd op RFC's;
De status van de RFC van de transitie techniek, bepaald door IETF, opgehaald op 25-10-2019.
- **Software beschikbaarheid:** de mate waarin software beschikbaar is om de transitie techniek uit te rollen;
Een schatting bepaald op basis van een korte
- **Open Source:** de mate waarin de software open source beschikbaar is;
Een schatting bepaald door een kort zoektocht naar software
- **Kosten:** de geschatte kosten van de implementatie en onderhoud van de techniek.
Een schatting bepaald op basis van hardware- en softwarematige eisen van de techniek.

Voor elk van de bovengenoemde criteria zijn een aantal waardes beschikbaar met daarin een numerieke score. Voor de gebruikte criteria zijn geen criteria met een afwijkende weging. Alle punten hebben volledige weging. De opties en scores zijn weergegeven in de onderstaande tabel.

Score	Manier	Address sharing	State management	Transparency	Scalability	NAT	Status	Software beschikbaarheid	Open Source	Kosten
3	Tunneling	NAPT	Stateless	Not limited	High	On CPE	Standard	+++	+++	€
2	Translation	NAT	Per subscriber	Limited	Medium	On BR	Informational	++	++	€€
1	Geen	Geen	Per session		Low	Both	Experimental	+	+	€€€
0								-	-	-

Tabel 27. MCA-criteria

Bijlage N: Reflectie

Begin 2019 ben ik begonnen met het zoeken naar een afstudeerbedrijf in de omgeving Arnhem-Nijmegen. Na contact met verschillende bedrijven, heb ik de keuze gemaakt voor het bedrijf Breedband. Bepalend hiervoor is de open sfeer van het bedrijf en de opdrachten die het bedrijf ter beschikking had.

De opdracht

Uit een lijst potentiële opdrachten van Breedband heb ik gekozen voor een onderzoek naar lw4o6, een IPv6 transitie techniek. In de studie ITSM is weinig aandacht gegeven aan IPv6 en ik was daarom geïnteresseerd in de techniek en de achtergrond daarvan. Met het kiezen van deze opdracht kon ik me volledig verdiepen in IPv6 en daarbij direct de transitie van IPv4 naar IPv6 aanpakken.

De aanpak

Bij de start van mijn afstudeerperiode ben ik direct begonnen met het plan van aanpak. Op basis van Prince2 heb ik een uitgebreid plan van aanpak geschreven met een gedetailleerde planning. In het plan is al aangegeven dat Prince2 selectief wordt toegepast. In praktijk bleek dat enkel de gedetailleerde planning een toegevoegde waarde is geweest voor het project. Het onderzoek is uitgevoerd aan de hand van de 'Reader Ontwerponderzoek' door Haveman, Hageraats en Van der Linden (2016). De planning is ingedeeld aan de hand van de reader en daardoor voornamelijk chronologisch. Tijdens het literatuuronderzoek bleek dat het onduidelijk werd welke informatie echt relevant was voor de technische aspecten van lw4o6, waardoor ik een aanpassing heb gemaakt in de planning. Het prototype is vooruit gehaald in de planning waardoor dit parallel aan het literatuuronderzoek werd opgesteld. Daardoor kon door middel van iteratief ontwikkelen van het prototype, het literatuuronderzoek beter worden aangevuld met relevante gegevens.

Begeleiding

Gedurende mijn afstudeerperiode heb ik begeleiding gehad van twee partijen: Tom van Klinken van Breedband en Erik van der Arend van Saxion.

Ik heb bij Breedband een wekelijks overleg gepland met Tom van Klinken om de voortgang te bespreken en vragen te stellen. Dit was prettig omdat ik wist dat ik was ingepland en geen verstoring ben in Tom's planning. Ik merk namelijk dat ik moeite heb om mensen in hun werk te onderbreken, waardoor ik vragen soms onnodig lang laat liggen. Ik heb ontzettend veel aan Tom gehad omdat hij door zijn vakkennis veel duidelijkheid kon verschaffen over de problemen waar ik tegen aanliep.

Voor de begeleiding vanuit Saxion heb ik een vijftal afspraken gehad met Erik van der Arend. Naast de afspraken heb ik regelmatig mijn voortgang via mail verstuurd. Ik heb het meest gehad aan de afspraken op locatie Saxion omdat ik daar met gerichte vragen kon komen, waarop ik antwoord kreeg en de discussie kon aangaan. Dit was erg behulpzaam.

Terugblik

Als ik terugkijk op de afstudeerperiode heeft het technische aspect de meeste indruk op mij gehad. Ik ben het traject ingegaan met, wat ik dacht, redelijke kennis van netwerken. Eenmaal in de netwerkwereld waarin ISP's zich bevinden, blijkt dat deze wereld veel dieper gaat dan wat ik dusver had geleerd. Ik heb ontzettend veel research moeten doen om mijn kennis omtrent IPv6 op niveau te krijgen, voordat ik verschillende transitie technieken kon begrijpen. Door dit onderzoek, maar ook door de directe informatie van collega's en alles wat zich afspeelde op de afdeling, is mijn kennis omtrent netwerken ontzettend gestegen.