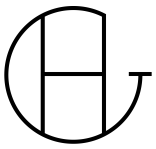


HoGent

Faculteit Bedrijf en Organisatie

De evolutie van IPv6 op globaal en Belgisch niveau

Jolan Van Impe

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Karine Van Driessche
Co-promotor:
Tim Rasschaert

Instelling: —

Academiejaar: 2017-2018

Tweede examenperiode

Faculteit Bedrijf en Organisatie

De evolutie van IPv6 op globaal en Belgisch niveau

Jolan Van Impe

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Karine Van Driessche
Co-promotor:
Tim Rasschaert

Instelling: —

Academiejaar: 2017-2018

Tweede examenperiode

Woord vooraf

Deze bachelorproef wordt beschouwd voor het afsluiten van mijn opleiding Toegepaste Informatica op HoGent. Hiermee wil ik aantonen dat ik op een zelfstandige basis een onderzoek kan voeren en afronden.

Ik heb gekozen om mijn onderwerp van mijn bachelorproef rond het nieuwere internet protocol namelijk internet protocol versie 6 te maken. Ik selecteerde dit onderwerp omdat er een grote mogelijkheid bestaat dat dit een bepaalde rol zal spelen in de toekomst van een netwerkbeheerder. Omdat dit een nieuw protocol is, heb ik hiermee zelf weinig ervaring en vond het een unieke kans om deze uitdaging aan te gaan en hierover een bachelorproef te schrijven. IPv6 is niet onbekend maar het is een protocol dat velen kennen maar weinigen volledig begrijpen, daarom wou ik onderzoeken hoe het met onze Belgische markt gesteld is en hoe deze hierop anticipeert. Ook zal dit goed aansluiten met mijn studierichting wat het nog interessanter maakt voor mezelf. Voor dit eindresultaat te kunnen leveren, stak ik er ontzettend veel tijd in. Dankzij enkele personen heb ik deze proef met succes tot zijn eind kunnen brengen en daarom wens ik hen even te bedanken voor alle steun en hulp die ik heb gekregen tijdens deze periode.

Eerst en vooral wil ik mijn promotor bedanken namelijk mevr. Karine Van Driessche, alsook mijn co-promotor Tim Rasschaert. Dankzij de hulp van hen, heb ik deze bachelorproef tot een einde kunnen volbrengen. Vervolgens zou ik mijn familie en vriendin willen bedanken die er steeds waren tijdens de moeilijke momenten tijdens deze periode. Zij gaven mij steeds weer moed om hier volop voor te gaan. Verder hoop ik dat het lezen van deze proef u een deugddoend gevoel zal geven.

Jolan Van Impe,
Academiejaar 2017-2018

Samenvatting

Dit onderzoek zal gaan over de evolutie en adoptie van IPv6 op de Belgische markt. Het nieuwe internet protocol en de opvolger van IPv4. In 2012 was al bekend gemaakt dat het einde van de beschikbare adressen er zat aan te komen en dat er hiervoor een opvolger nodig was. Daarom werd , alsook in 2012, dag van IPv6 uitgeroepen. Hiermee was de opvolger direct voorgesteld en bekroond als officiële vervanger van IPv4. Momenteel is het 6 jaar later en is er nog niet veel meer sprake geweest van IPv6 of een effective overgang naar IPv6. Daarom zal dit onderzoek zich verdiepen in de hedendaagse adoptie van IPv6.

Er zal onderzocht worden waarom IPv6 er is gekomen en wat de positieve punten zijn aan dit protocol. Wat de verschillen zijn tussen IPv4 en IPv6, specifiek gericht op de headers van beide protocollen. Verder in deze scriptie zal er onderzocht worden wat mogelijke tunneltechnieken zijn en hoe de communicatie tussen beide protcollen kan verlopen.

Om op de meeste onderzoeksvragen een antwoord te vinden, zal er aangetoond worden wat de situatie is van IPv6 en hoe de wereld, bedrijven en ISP's zich hierop aanpassen. Hoe de overschakeling al dan niet positief aan verlopen. Na het lezen van deze scriptie zal men een beter inzicht moeten hebben over de huidige situatie en waarom deze nog niet zo hoog scoort. Ook België zal nader onderzocht worden over de hoe de Belgische bedrijven zich aanpassen en wat hun ondervinden zijn en wat men kan doen om te adoptiegroei te vergroten.

Inhoudsopgave

Lijst van figuren

1. Inleiding

Dankzij de groei van het internet, internetgebruikers, Internet Of Things en aantal mensen op aarde zijn er steeds meer apparaten verbonden met het internet. Dit zorgt voor de steeds verdere uitputting van IPv4 protocol. Het tekort aan beschikbare IPv4 adressen komt steeds dichterbij en de laatste /8 blok is vrijgegeven. Dit wil zeggen dat het einde van IPv4 nadert. De reeds gelanceerde opvolger, IPv6, zal de problemen van IPv4 moeten oplossen. Hierdoor is er een onderzoek nodig naar de werking en verschillen van IPv6. Verder zal er aangetoond worden wat de huidige stand van zaken is over de adoptie van IPv6 en hoever deze al staat.

1.1 Probleemstelling

Dankzij deze scriptie krijgt men een duidelijk visueel zicht over hoe de momentele stand van zaken is op vlak van IPv6 en de adoptie ervan over heel de wereld. Deze zou een motivatie kunnen opleveren voor andere bedrijven de stap te laten nemen naar een IPv6 of een IPv4/IPv6 netwerk structuur. Sinds de lancering van IPv6 is er al een tijd verstreken. Daarom zal deze proef een update geven van waar de huidige situatie zich bevindt.

1.2 Onderzoeksvraag

Enkele onderzoeksvragen die gesteld kunnen worden is hoe IPv4 en IPv6 zich met elkaar onderschijden. Wat de huidige situatie is van IPv6 op globaal niveau. Hoe goed België scoort op de adoptie van IPv6. Hoe Belgische bedrijven zich hierop gaan aanpassen. Hoe

het komt dat België goed of slecht scoort en wat de bevindingen zijn van bedrijven. Alsook waarom de overschakeling niet zo vlot aan het verlopen is.

1.3 Onderzoeksdoelstelling

Om deze scriptie tot een succes te brengen is het noodzakelijk genoeg data en informatie te verkregen van bedrijven. Dankzij deze data is het mogelijk om de huidige stand van zaken voor te stellen en een beeld te scheppen hoe goed de adoptie van IPv6 aan het verlopen is.

1.4 Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:

In Hoofdstuk 2 wordt de methodologie toegelicht en worden de gebruikte onderzoekstechnieken besproken om een antwoord te kunnen formuleren op de onderzoeksvragen.

In Hoofdstuk 3, in het eerste hoofdstuk zal er een inleiding gegeven worden over IPv6. Dankzij dit inleidend hoofdstuk zal er al een kennis verschaft worden die interessant kan zijn voor de rest van de scriptie. Alsook worden hierin de basiselementen uitgelegd over IPv6.

In Hoofdstuk 4, het tweede hoofdstuk bevat een gedetailleerde vergelijking tussen IPv4 en IPv6. In dit hoofdstuk zal vooral de nadruk gelegd worden op de headers van beide protocollen.

In Hoofdstuk 5, nu IPv6 steeds populairder wordt is het ook nodig om communicatie te leggen tussen IPv4 clients en IPv6 clients. In dit hoofdstuk zullen dus enkele transitie en tunnel technieken uitgelegd worden.

In Hoofdstuk 6, het is nu al zeker dat er een einde zal komen aan IPv4. Hierin zal verder uitgelegd worden hoe de momentele stand van zaken is voor IPv4. Hoe lang er nog te resten valt voor IPv4 en hoe de komende maanden eruit zullen zien.

In Hoofdstuk 7, hierin zal er duidelijk de huidige adoptie grafisch voorgesteld worden op globaal niveau. Aan de hand van verschillende data en grafieken is het zeer duidelijk hierover een zicht te verkrijgen.

In Hoofdstuk 8, in dit hoofdstuk zal er dieper gegaan worden in de adoptie op de Belgische markt ne hoe sommige bedrijven ervoor staan. Dankzij opgestelde vragen krijgt men een voorbeeld hoe de Belgische bedrijven erover denken en ervoor staan.

In Hoofdstuk 9, tenslotte, wordt de conclusie gegeven en een antwoord geformuleerd op de onderzoeksvragen. Daarbij wordt ook een aanzet gegeven voor toekomstig onderzoek binnen dit domein.

2. Methodologie

In dit hoofdstuk zal er besproken worden welke methodes en manieren van werking er gehandhaafd werd voor uitschrijven van deze proef. Vervolgens zal er ook een duidelijke overzicht getoond worden wat men juist van elk hoofdstuk kan verwachten.

2.1 Gehanteerde methodiek

Het onderzoek is onderverdeeld in verschillende delen. In het eerste deel zal er eerder aangetoond worden wat IPv6 inhoud en hoe deze verschilt met zijn voorganger IPv4. Dit zal al een duidelijk overzicht moeten geven waarom er de noodzaak was om de overschakeling uit te voeren. Verder zijn er ook enkele transitie technieken die kunnen toegepast worden in een netwerk om mee te gaan in deze overgang. In het tweede grote deel van de proef zal er eerder een onderzoek gedaan worden naar de adoptie van IPv6 en hoe onze Belgische markt en bedrijven hierop anticiperen. Hoe IPv4 er momenteel voor staat en hoelang dit protocol nog zal overleven tot er niets anders meer is dan IPv6. Ook werden enkele vragen opgesteld en beantwoord door bedrijven over hun standpunt en visie over IPv6.

Om deze scriptie tot een geslaagd succes te brengen, heb ik gekozen om te onderzoeken hoe Belgische bedrijven en ISP's reageren op IPv6. Aan bedrijven zijn er enkele vragen opgesteld en beantwoord die een duidelijk overzicht geven over hoe zij erover denken, wat hun standpunt is, of er mogelijkse plannen zijn voor een uitbreiding of ze er momenteel mee aan het experimenteren zijn. Bij ISP's was het belangrijk of hun klanten al begeleid werden met IPv6 en of hun apparatuur IPv6 ondersteunend zijn.

3. Inleiding tot IPv6

In dit hoofdstuk wordt er een inleiding tot IPv6, de geschiedenis en ontstaan van IPv6 doornomen. Alsook zullen er nieuwe elementen besproken worden die gehandhaafd worden in IPv6 en de reden van bestaan en waarom we dit protocol nodig zullen hebben.

3.1 Waarom IPv6

IPv4 werd ontwikkeld in de vroege jaren ’70 voor het communiceren tussen onderzoekers en academici in Amerika. Op dat moment werd er geen rekening gehouden met enkele elementen zoals genoeg adressen, extra beveiliging en Quality of Service, QoS. Het protocol heeft meer dan 30 jaar overleefd en heeft een belangrijke rol gespeeld in het internetrevolutie. Maar zelfs de slimste systemen verjaren en raken uiteindelijke verouderd. Dit was zeker het geval met IPv4. Vandaag de dag staat alles verbonden met het internet en met elkaar. De enorme opkomst van webshops, IoT, mobiel apparatuur, sociale netwerken en zo voort zorgt voor meer geconnecteerde apparaten. Deze opkomst zorgde voor het bereiken van de limiet van IPv4 en leidde tot een opvolger namelijk IPv6. IPv6 werd ontwikkeld door het experimenteren met IPv4. Hierdoor werd al snel opgemerkt dat er geen limieten meer mochten zijn maar meer flexibiliteit en schaalbaarheid. IPv6 zorgde daarom voor de grote groei van het internetgebruik, mobiliteit en extra beveiliging op vlak van end-to-end beveiliging (**Hagen2014**).

3.2 Geschiedenis van IPv6

Internet Engineering Taks Force (IETF) begon in de jaren 1990 met het ontwikkelen van een opvolger voor IPv4. Al snel werd er een oplossing voor de gelimiteerde tekortkomingen gezocht en extra functionaliteit toegewezen. Daarom lanceerde IETF, Internet Protocol Next Generation (IPng) zone in de jaren 1993. Dit werd gebruikt voor het onderzoeken van voorstellen en aanbevelingen van verdere procedures (**Hagen2014**).

Op de Toronto IETF meeting in 1994 werd er het nieuwe protocol namelijk IPv6 voorgesteld. De bestuurders richtte een Address Lifetime Expectation (ALE) werkgroep op om na te gaan of de geschatte levenstijd van IPv4 IETF genoeg tijd gaf om een oplossing te vinden met nieuwe functionaliteit, of er enkel tijd over was om het adres probleem aan te gaan. ALE had op basis van toenmalig beschikbare statistieken geschat dat de uitputting van IPv4 plaats zou vinden tussen het jaar 2005 en 2011. Later in 1994 werd IPv6 goedgekeurd door de Internet Engineering Steering Groep (**Hagen2014**).

Eén van de grootste uitdagen maar ook opportuniteiten van IPv6 is de herontwikkeling van netwerken in de toekomst. Dit is waar bedrijven hun grootse aandacht aan zouden moeten vestigen bij het overstappen naar een IPv6 netwerk. Zodanig er geen oude concepten worden meegenomen naar een nieuw protocol. Daarom is het belangrijk om bij de integratie volledig de architectuur te herstructureren (**Hagen2014**).

3.3 Nieuwigheden in IPv6

Bij de vernieuwde apparaten zal IPv6 steeds beschikbaar zijn voor configuratie. Als dit bij oudere toestellen nog niet het geval is, dan kan dit vaak via software upgrades. Enkele nieuwigheden bij IPv6 is een uitgebreid adres lengte, autoconfiguratie, het formaat van de header is eenvoudiger opgesteld en verbeterde steun voor extra opties en extensies (**Hagen2014**).

3.3.1 Uitgebreid adres lengte

Het adresformaat bevat 128 bits, dit rekent uit op meer dan 340 biljoen verschillende adressen. Dit wil ook zeggen dat er meer adressen beschikbaar zijn dan korrels zand op de aarde. Dit zou het tekort aan adressen voor eens en voor altijd moeten oplossen (**Hagen2014**).

3.3.2 Autoconfiguratie

Een nieuwe functionaliteit is het Stateless Address Autoconfiguration (SLAAC) mechanisme. Dit mechanisme zal ervoor zorgen dat het connecteren efficiënter zal verlopen bij vooral mobiele apparaten zoals smartphones wanneer ze zich in een onbekend netwerk bevinden. Dit zou het werk van een netwerk engineer moeten vergemakkelijken

(**Hagen2014**).

3.3.3 Eenvoudiger headerformaat

De header van een IPv6 pakket is vereenvoudigd. De lengte zal een vaste lengte hebben van 40 bytes, wat het verwerken hiervan veel sneller maakt dan ervoor. De 40 bytes is onderverdeeld in twee maal 16 bytes voor het bestemmingsadres en bronadres en nog 8 bytes voor algemene header informatie (**Hagen2014**).

3.3.4 Verbeterde steun voor extra opties en extensies

IPv6 heeft de optie om extension headers toe te voegen. Deze worden enkel toegevoegd als ze nodig zijn. Dit zorgt er alweer voor om het pakket sneller te verwerken. Routingheaders, QoS en beveiliging zijn enkele headers die kunnen meegegeven worden (**Hagen2014**).

3.4 Hebben we IPv6 echt nodig?

Om hierop kort te antwoorden, ja. IPv6 is een noodzaak geworden in de internetwereld. We zijn op een moment gekomen dat het aantal beschikbare IPv4 adressen steeds dichter bij de nul komt. Dit is echter niet te vermijden met de dagelijkse groei van het internet. Daarom is er de overschakeling nodig naar IPv6. IPv4 had een limiet van 4,3 miljard adressen, waardoor deze limiet al snel werd bereikt (**Hagen2014**).

4. Vergelijking IPv4 met IPv6

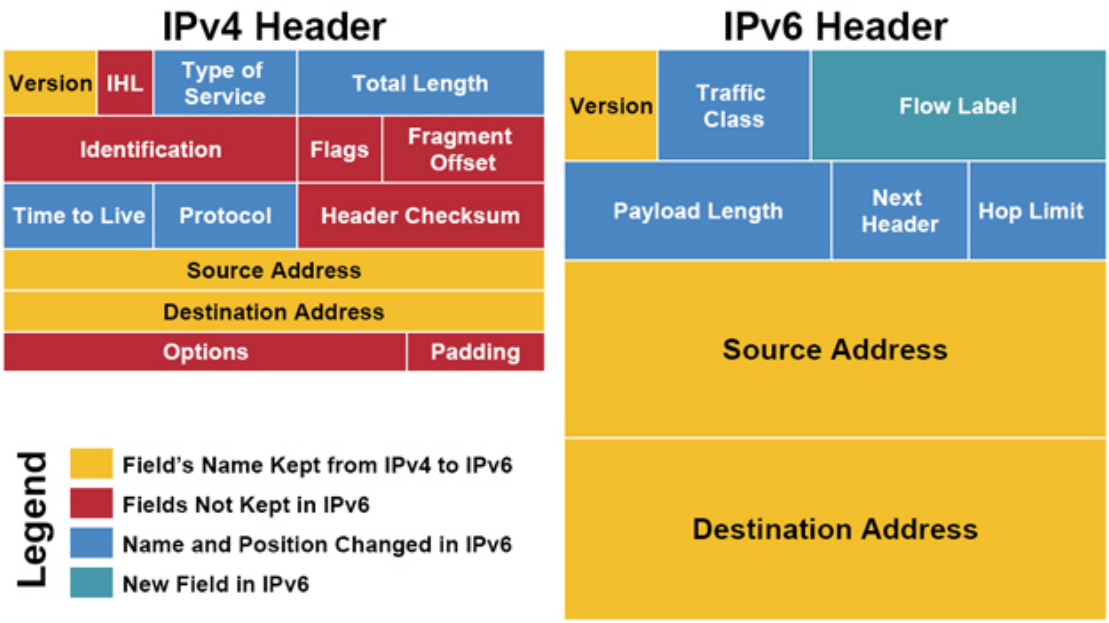
In dit hoofdstuk zal er dieper worden ingegaan op de verschillen tussen beide protocollen, specifiek de vorming van de headers. Welke aanpassingen er werden gemaakt naar aanleiding van het nieuwe internet protocol en eveneens de mogelijke effecten deze verschillen kunnen hebben. Hiermee zal er een duidelijk zicht gegeven worden waarmee er juist rekening wordt gehouden naar aanleiding van de ontwikkeling van IPv6. Dit hoofdstuk bevat dus een voorstudie naar aanleiding van de overschakeling naar IPv6.

4.1 Header van IPv4 en IPv6

Onderstaande figuur geeft een duidelijke weergave van de IPv4 en IPv6 headers. Beide hebben een duidelijk verschil naar gelang de inhoud, aantal velden en aantal gebruikte bits. Op het eerste zicht is er te zien dat een IPv6 header een eenvoudiger overzicht handhaaft. Door het minder aantal velden in de header tegenover die van IPv4. Dit maakt van IPv6 een gestroomlijnder protocol en is zo efficiënter om af te handelen. Nog een voordeel hiervan is dat een IPv6 header een vaste 40 bits header bevat in vergelijking met IPv4, waarbij een IPv4 header gebruik maakt van een variabele lengte voor zijn header. Verder in dit hoofdstuk worden de verschillende velden met elkaar vergeleken.

4.1.1 Version Field

Zowel IPv4 als IPv6 begint met een versie veld. Dit veld bevat de versie van het gebruikte internet protocol. Bij IPv4 zal dit de waarde 4 opleveren en voor IPv6 zal dat de waarde 6 zijn (**Graziani2017**).



Figuur 4.1: Vergelijking IPv4 header en IPv6 header (**4vs6**)

4.1.2 IPv4 Internet Header Length (IHL) Field

IHL is de lengte van de IPv4 header in 32-bit woorden, met optionele velden. In feite toont dit het einde van de IPv4 header en het begin van de data of payload. De minimumwaarde van dit veld is 5. Dit betekent 5 keer 32-bit woorden of 160 bits, in octetten is dit 20 bytes. Dit komt dus overeen met de minimumwaarde van een IPv4 header zonder optionele velden. Deze optionele velden kunnen de lengte van het IHL tot een maximum van 60 bytes brengen. In vergelijking met IPv6, bestaat dit veld niet meer in de nieuwe header. De reden waarom dit veld in meer van noodzaak is in de header, is omdat een IPv6 header een vaste lengte gebruikt namelijk 40 bytes. Dit zorgt ervoor dat het behandelen veel efficiënter te pas kan gaan. Ook maakt IPv6 gebruik van optionele velden maar deze hebben geen invloed op de lengte, dit behoudt de vaste lengte van de header (**Graziani2017**).

4.1.3 IPv4 Type of Service (ToS) en IPv6 Traffic Class Fields

Type of Service in IPv4 en Traffic Class Fields zijn in principe dezelfde velden. Juist werd de naamgeving hiervan aangepast in IPv6. Beiden worden gebruikt om te preciseren welke soort behandeling het pakket juist zal krijgen van routers. Deze informatie zal helpen om de functies van Quality of Service (QoS) te leveren door verschillende graden van precedentie aan te bieden. Wanneer er meerdere pakketten verstuurd worden vanuit dezelfde interface dan kan de waarde in dit veld een hulp bieden voor zowel de behandeling van pakket als voor de volgorde waarin de pakketten verstuurd worden (**Graziani2017**).

4.1.4 IPv6 Flow Label Field

Het flow label field wordt gebruikt om alle pakketten binnen dezelfde stroom/flow te helpen identificeren en ervoor te zorgen dat alle pakketten dezelfde behandeling krijgen van de IPv6-routers. Routers houden de individuele pakketstromen bij. Omdat de routers niet onafhankelijk de header van elk pakket hoeven te verwerken, worden deze multipakket flows efficiënter verwerkt. Echter zijn er niet veel implementaties die rekening houden met flow label. Behalve Equal Cost Multi-Path (ECMP) en Server Load Balancing (SLB). Als een flow label de waarde 0 bevat dan betekent dit dat er met het verkeer geen rekening gehouden zal worden met een flow (**Graziani2017**).

4.1.5 IPv4 Total Length Field, IPv6 Payload Length Field en IPv6 Jumbograms

Het IPv4 Total Length Field is de totale lengte van het IPv4 pakket, dit wordt uitgemeten in bytes, en bevat zowel de header als de data. Het veld is een 16-bit veld en dus een maximum grootte van een IPv4 pakket is 65535 bytes. De meeste IPv4 pakketten zijn dus ook kleiner van grootte (**Graziani2017**).

Het IPv6 Payload Length Field is een 16-bit veld dat de lengte in bytes van het data deel van een IPv4-pakket. Echter telt de lengte van de IPv6 header hierin niet mee en bevat het enkel de data en IPv6-extensies. Als het pakket dus extensies bevat zullen deze hierin ook meegeteld worden. Extensies worden beschouwd als een deel van de payload (**Graziani2017**).

Beiden zijn met elkaar te vergelijken, behalve voor één belangrijk verschil. In het IPv4 Total Length Field bevat het de totale lengte van een IPv4-pakket, zowel data als header. Bij het IPv6 Payload Length Field is dit enkel het totaal aantal bytes van de data of payload, de header wordt hierin niet meegerekend. Daarom kan de lengte bij IPv4 verschillen door gebruik te maken van optionele velden waarbij IPv6 een vaste lengte heeft van 40 bytes (**Graziani2017**).

Zoals eerder vermeld geweest, IPv4 Total Length is een 16-bit veld dat een maximum pakket grootte van 65355 bytes heeft. Deze pakketten zullen deze grootte haast nooit halen wegens de maximum transmission unit (MTU). IPv4 heeft geen optie om deze theoretische grootte te overschrijden. Daarentegen kan IPv6 zijn maximum payload wel overschrijven. Dit type van pakket wordt dan een jumbogram genoemd. Een jumbogram is een IPv6-pakket dat een grotere payload van 65535 bytes bevat. Jumbogrammen gebruiken de Jumbo Payload optie in de Hop-by-Hop extensie header. De Jumbo payload optie gebruikt een veld van 32-bit lengte groot om het verzenden van IPv6-pakketten tussen de 65536 en 4294967295 bytes toe te laten. Deze jumbogrammen worden het vaakst gebruikt bij connecties tussen supercomputers (**Graziani2017**).

4.1.6 IPv4 en IPv6 MTU's

De meeste transmissie linken gebruiken een maximum pakketlengte gekend als een MTU (maximum transmission unit). Een MTU bij IPv4 en IPv6 is de totale lengte van een pakket inclusief de header (**Graziani2017**).

Echter is het nodig dat elke node de mogelijkheid heeft om een Ipv4 pakket te versturen van 68 bytes zonder verdere fragmentatie. Dit komt omdat een Ipv4 header de grootte van 60 bytes kan bevatten in lengte, waardoor er nog 8 bytes overblijven voor de payload. Daarom moet de payload een Ipv4 fragment zijn. Anders moet de payload header informatie toegevoegd krijgen voor een ander protocol, waardoor het groter dan 8 bytes zal worden. Elke IPv4 eindbestemming van het Ipv4 pakket moet een IPv4 pakket van 576 bytes kunnen ontvangen, dit kunnen ook alle fragmenten van een pakket zijn (**Graziani2017**).

Bij IPv6 is het nodig dat elke link een minimum MTU van 1280 bytes heeft, met een aangeraden MTU van 1500 bytes. In vergelijk met het IPv4 protocol is dit 68 bytes (**Graziani2017**).

4.1.7 IPv4 Framgmentation

Het IPv4 protocol werd eerder ontwikkeld voor een breed spectrum van transmissielinks. Als de router een IPv4 pakket ontvangt dat groter is dan de MTU van de uitgaande interface dan kan het pakket gefragmenteerd worden afhankelijk van de header van het pakket. Het kan voorvallen dat een pakket al gefragmenteerd, in meerdere pakketten, werd verzonden door de verzender. Als de finale ontvanger alle pakketten ontvangt, dan is het zijn taak om deze terug te zetten in het originele IPv4 pakket (**Graziani2017**).

Fragmentatie deelt dus IPv4 pakketten in kleinere delen zodat deze kunnen doorgestuurd worden op een link dat niet de volledige grootte van het originele pakket kon verzenden. Het bestemmende apparaat heeft als taak deze ontvangen pakketten terug om te vormen naar het originele pakket. Het IPv4 Identification, Flags en Fragment Offset velden worden gebruikt om het pakket op te delen en terug samen te voegen (**Graziani2017**).

Identification veld is 16 bits groot. Elk IPv4 pakket heeft een uniek veld in het 16 bit Identification veld. Als een IPv4 pakket wordt opgesplitst in delen dan helpt dit veld om de gefragmenteerde pakketten terug samen te voegen voor de ontvanger (**Graziani2017**).

Flags veld is een veld dat de grootte heeft van 3 bits. De eerste bit is 0, dit geeft aan of het gereserveerd is of niet. De tweede bit is bekend als de DF (don't fragment) bit. Als deze de waarde 1 heeft toont dit aan dat het pakket niet gefragmenteerd is. De laatste, derde, bit is de more fragments flag. Deze bit is gebruikt om aan te tonen of dit pakket het laatste pakket is of niet. Als deze de waarde 1 heeft dan is dit pakket niet het laatste en volgen er nog. 0 geeft aan dat dit het laatste pakket is. Als een IPv4 pakket niet gefragmenteerd is dan zal deze vlag de waarde 0 bevatten (**Graziani2017**).

Fragment Offset veld is een veld van 13 bits lang. Als een IPv4 pakket is gefragmenteerd dan toont dit veld aan waar het pakket gepositioneerd is en waar de data komt in delen

van 8 octetten, 64 bits. De ontvanger krijgt hierdoor een beeld van waar het pakket komt tussen alle andere pakketten. Als het pakket niet gefragmenteerd is zal deze de waarde 0 hebben (**Graziani2017**).

4.1.8 IPv6 Fragmentation: IPv6 Source only

Een IPv6 router zal geen fragmentering toepassen op een pakket, zoals bij IPv4 wel het geval is, enkel als het de zender is van het pakket. Zoals te zien op de afbeelding is er in de IPv6 header geen plaats gemaakt voor de velden die IPv4 gebruikt om te fragmenteren (**Graziani2017**).

Als een IPv6 router een pakket ontvangt dat groter is dan de MTU uitgaande interface, dan zal de router simpelweg het pakket droppen en zal een ICMPv6 (Internet Control Message Protocol version 6) Packet Too Big bericht terug verzenden naar de zender van het pakket. Het Packet Too Big bericht bevat de MTU grootte van de link in bytes zodanig dat de zender van het pakket zijn grootte kan aanpassen en het pakket terug kan verzenden (**Graziani2017**).

De data wordt vaak verzonden in series van pakketten, ook wel een packet train genoemd. Hoe groter deze pakketten zijn, hoe minder pakketten er zullen verstuurd moeten worden. Daarom is het aangeraden om de grootte zo hoog mogelijk te maken zodat alle links, van zender naar ontvanger, deze ondersteunen. Dit wordt ook de Path MTU (PMTU) genoemd. Hiervoor kan een apparaat een PMTU Discovery doen om de laagste MTU link te achterhalen (**Graziani2017**).

4.1.9 IPv4 Protocol en IPv6 Next Header Fields

Het IPv4 Protocol veld toont het protocol aan dat gebruikt wordt in de data portie van het IPv4 pakket. Hiervoor heeft IPv6 een gelijkaardig veld, het Next Header veld, dat aantoont welk type header er volgt achter de algemene IPv6 header. Ook al lijkt het gelijkaardig met het IPv4 veld, toch zijn er enkele verschillen tussen beiden (**Graziani2017**).

Dezelfde waarden die gebruikt worden in het IPv4 Protocol veld zijn terug te vinden in het IPv6 Next Header veld, buiten dat er bij IPv6 nog extra waarden mogelijk zijn. De meest voorkomen waarde voor beiden is voor TCP de waarde 6 en voor UDP 17 (**Graziani2017**).

Als er enkel een IPv6 header is en geen extra header meer volgt, dan zal het IPv6 Next Header veld de waarde van het protocol weergeven dat wordt gebruikt in de data portie van het IPv6 pakket. Dit is dus hetzelfde voor het IPv4 Protocol veld (**Graziani2017**).

4.1.10 IPv4 Time To Live (TTL) en IPv6 Hop Limit Fields

De IPv4 Time To Live (TTL) en IPv6 Hop Limit velden zorgen ervoor dat pakketten niet eindeloos blijven rondgaan in netwerken, zoals routingloops. Deze velden worden steeds verminderd door 1 als het pakket een router passeert. Als het veld de waarde 0 bereikt

dan wordt het pakket weggegooid en een ICMPv4 of ICMPv6 Time Exceeded bericht verstuurd naar de zender van het pakket (**Graziani2017**).

Van IPv4 naar IPv6, was het TTL veld verandert naar het Hop Limit veld. Het IPv4 TTL veld was eigenlijk bedoelt om het maximum aantal tijd dat het pakket mag ronddolen in een netwerk en niet het aantal hops met routers. Deze tijd wordt berekend in seconden. Het maximum is 255 seconden of 4.25 minuten. In plaats van deze tijd te berekenen gaan de routers het IPv4 TTL veld verminderen met 1, hierdoor worden het aantal van hops aangekaart (**Graziani2017**).

4.1.11 Checksums: IPv4, TCP en UDP

Een checksum in de IPv4 header dient ervoor om na het versturen van pakketten deze te controleren op corrupte data. Dit is een 16-bit checksum die zich focust op de IPv4 header. Elke router die dit pakket passeert zal de berekening doen van de checksum en controleren. Als deze dan gefaald of fout is zal de router het pakket verwijderen (**Graziani2017**).

In IPv6 is er geen checksum in de IPv6 header. De checksum is er bewust uitgelaten omdat layer 2 data link technologie, zoals ethernet, een eigen checksum en error controle hebben. Alsook TCP en UDP hebben hun eigen checksums. Dit maakt een extra checksum op layer 3 niveau overbodig en redundant (**Graziani2017**).

Omdat er geen checksum is toegevoegd in IPv6 zal de UDP checksum wel verplicht zijn bij IPv6, wat bij IPv4 niet het geval is. Dit veld dient er toe om de betrouwbaarheid van de UDP header en data te waarborgen. Bij het TCP protocol is zowel bij IPv6 als bij IPv4 de checksum een vereiste (**Graziani2017**).

Checksums worden gebruikt op verschillende layers door verschillende protocollen. Een checksum zal dus controleren op mogelijk fouten die zijn opgelopen tijdens het verzenden van de data. Elk transport laag of andere bovenlaag protocol dat een IPv4 adres bevat in de berekening van de checksum moet veranderd worden voor het IPv6 te kunnen gebruiken. Deze wijziging is nodig voor het 128-bit IPv6 adres (**Graziani2017**).

Wanneer TCP of UDP verzonden word over IPv6, dan bevat de checksum enkele velden namelijk IPv6 bronadres, IPv6 bestemmingsadres, de payload van de bovenlaag en de IPv6 next-header waarde (**Graziani2017**).

Een wijziging aan zowel TCP als UDP voor het transporteren van IPv6 pakketten is dus nodig. Omdat beide checksums gebruik maken van de IPv6 adressen, is het dus nodig deze te herwerken voor het langere adres. Ook al zijn de adressen langer, de werkwijzen en berekeningswijze blijven dezelfde voor zowel IPv6 als IPv4 (**Graziani2017**).

Bij IPv4 is er een checksum aanwezig in de header, dit maakt voor UDP de checksum overbodig. Bij IPv6 was de checksum vooral verwijdert om de snelheid van de verwerking te verbeteren. Daarom is het dus verplicht om bij TCP en UDP de checksum te gebruiken (**Graziani2017**).

4.1.12 IPv4 en IPv6 bronadres en bestemmingsadres velden

Eén van de grootste veranderingen van IPv4 naar IPv6 is de lengte van het bron- en bestemmingsadres. De lengte van de adressen zijn van 32-bit adressen naar 128 bit-adressen veranderd in IPv6 (**Graziani2017**). Enkele veranderingen zijn:

- Het bronadres is altijd een unicast adres, bij IPv6 kan dit een link-local unicast, unique local unicast of unspecified unicast adres zijn
- Het bestemmingsadres kan een unicast, multicast, anycast of een broadcast adres zijn. Bij IPv6 is enkel het broadcast adres niet aanwezig

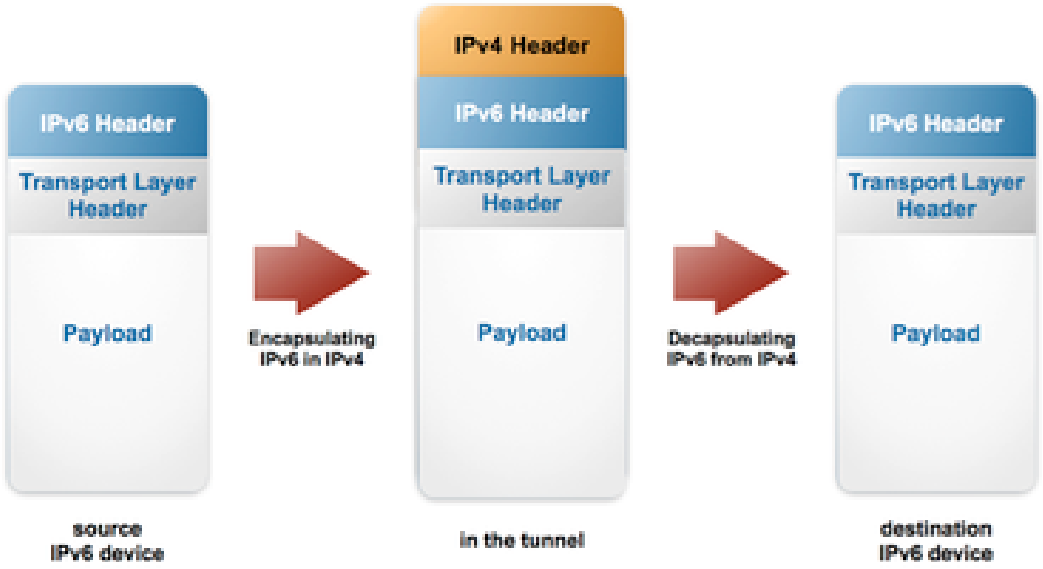
5. Transitie technieken

Als men spreekt over het overschakelen naar IPv6, dan is het niet de bedoeling IPv4 direct aan de kant te leggen en volledig niet meer te gebruiken. Alleen een IPv6 netwerk is meestal niet het beste idee omdat niet iedereen een diepe kennis hiervan heeft. Daarom zou het beter zijn om eerst kennis te maken met IPv6 door gebruik te maken van beide protocollen. Het probleem is dat een IPv6 netwerk niet direct kan communiceren met een IPv4. Daarom zullen er verder in dit hoofdstuk enkele methodes worden besproken over hoe IPv6 nodes met IPv4 nodes kunnen communiceren via tunneling en inkapseling en translatie. Daarbij gaan we ook het beste scenario aantonen die ideaal zou zijn om aan de slag mee te gaan in een lokaal netwerk.

5.1 Tunneling en inkapseling

Om het connecteren van IPv6 hosts over een IPv4 netwerk, zal er gebruik gemaakt worden van een IPv6 tunnel over het IPv4 netwerk.

Het IPv6 pakket dat afkomstig is van het IPv6 apparaat van de verzender zal ingekapseld worden bij het toegangspunt van de tunnel, waar het een extra IPv4 header krijgt en vervolgens als IPv4 pakket zal verstuurd worden door het IPv4 netwerk. Bij het einde van de tunnel zal de IPv4 header verwijderd worden en het pakket zal nadien als een IPv6 pakket toekomen bij het IPv6 bestemmingsapparaat. Enkele methodes die verder worden uitgelegd zijn 6in4, 6to4, 6rd, GRE, ISATAP en DS-Lite (**RIPE2016**).



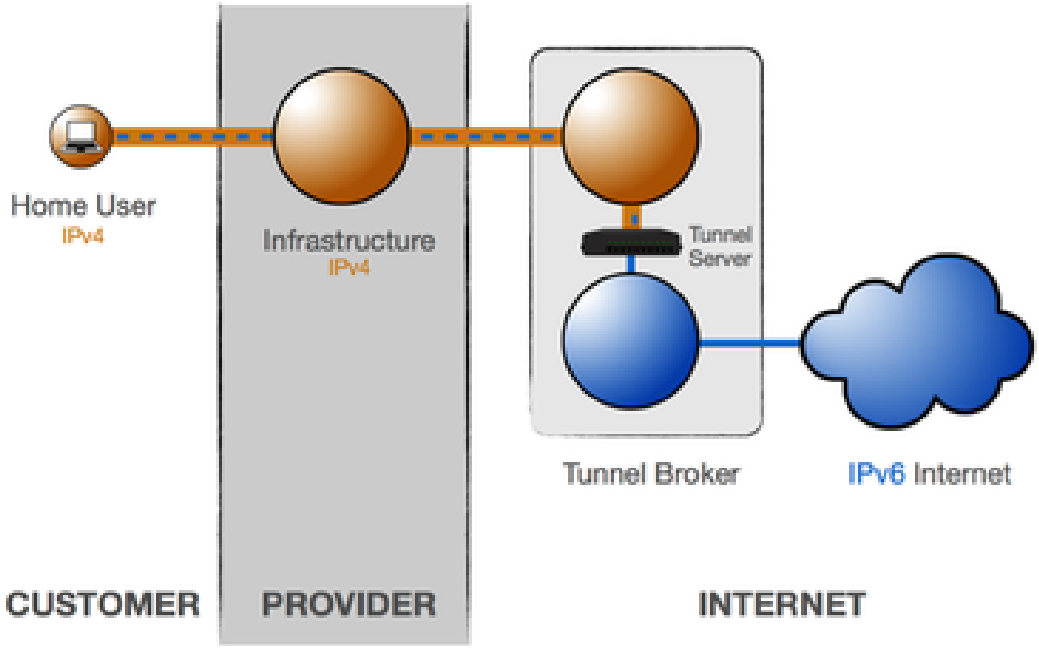
Figuur 5.1: Tunneling en inkapseling (**RIPE2016**)

5.1.1 6in4

Als een IPv4 host, een IPv6 wilt bereiken maar geen ipv6 connectiviteit heeft thuis , is er de mogelijkheid een 6in4 tunnel op te zetten. Op het moment dat een IPv4 host een webserver via IPv6 wil bereiken is dit echter niet mogelijk. Hiervoor kan er gebruik gemaakt worden van een 6in4 tunnel. De host dient een tunnel op te zetten en gebruik te maken van een tunnelbroker. Via de tunnelbroker zal er een IPv6 adres beschikbaar zijn waarnaar de IPv6 pakketten verstuurd zullen worden. Een 6in4 tunnel zal een verzonden IPv6 pakket van de host omzetten naar een IPv4 pakket. Men zal een nieuwe IPv4 header toevoegen over de IPv6 header. Hierdoor kan het pakket verzonden worden over het IPv4 internet. Als het pakket de tunnelbroker bereikt dan zal hij op zijn moment het pakket uitpakken en de IPv4 header verwijderen. Nadien blijft enkel het oorspronkelijke IPv6 pakket over en wordt deze over het IPv6 internet verstuurd naar de webserver. Dit mechanisme is een stabiele en voorspelbare manier omdat men steeds weet naar waar het pakket zal verzonden worden. Voor een ISP is dit echter geen gangbare methode. Als een ISP gebruik zal maken van een 6in4 tunnel, dan zal deze voor iedere klant manueel een tunnel moeten aanmaken (**RIPE2016**).

5.1.2 6to4

Doorgaans wordt 6to4 tunneling niet meer gebruikt. 6to4 is een tunneltechniek die het nadeel van de vorige mechaniek oplost, 6in4. Deze techniek is, in vergelijking met 6in4, beter schaalbaar op grotere vlakken. Hiermee zou een ISP voor al zijn klanten de techniek kunnen hanteren. Echter heeft deze methode enkele nadelen. Er kunnen zich op onverwachte momenten een lange latency veroorzaken met zeer negatieve gebruikservaringen tot gevolg. 6to4 gebruikt overal in de wereld dezelfde IPv6 en IPv4 prefix voor het be-



Figuur 5.2: 6in4 visualisatie (**RIPE2016**)

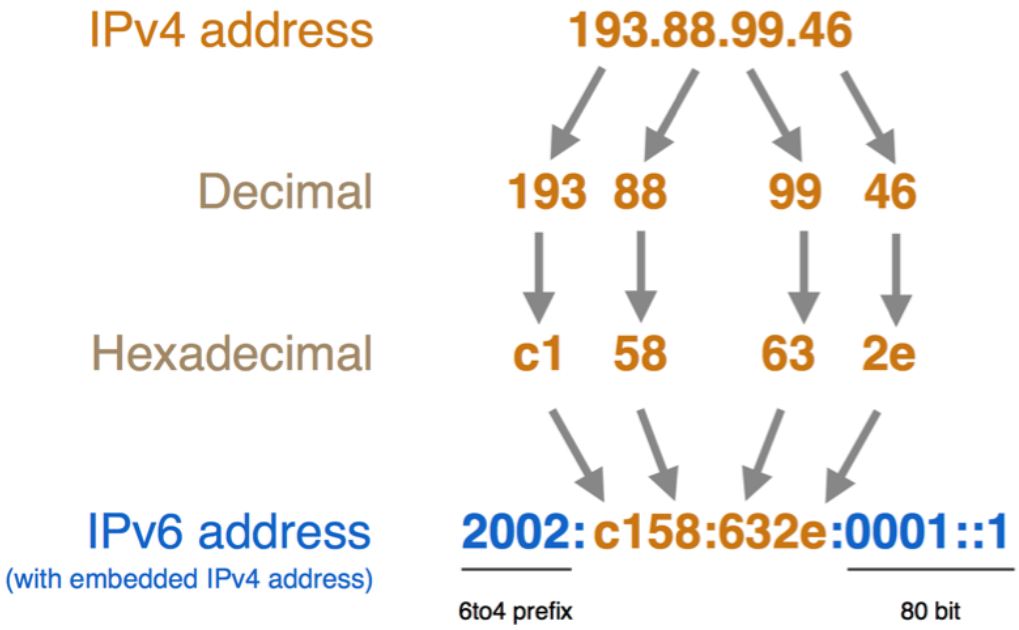
gin en einde van de tunnel. Namelijk 2002::/16 voor IPv6 en 192.88.99.0/24 voor IPv4. Wanneer IPv6 bronapparaat met 6to4 tunnel een connectie wilt aangaan met een ander IPv6 apparaat over IPv4 internet, dan zal de tunnel automatisch een einde vinden zonder dat er configuratie nodig is aan de tunnel zelf. Hierdoor is de schaalbaarheid groot en dient er geen manuele configuratie meer te gebeuren. Echter heeft de eindgebruiker wel een publiek IPv4 adres nodig om de connectie succesvol tot stand te brengen. Het IPv4 tunneluitgangspunt is geïntegreerd in de bitnummers 17-48 van het 6to4 IPv6-adres. Dus het tunnelingangspunt neemt automatisch het IPv4-adres van het tunneluitgangspunt van de tunnel over van het IPv6-aders van de bestemming (**RIPE2016**).

Een schematische voorstelling van de verschillende delen van een 6to4 IPv6 adres is als volgt.

Omdat de eindpunten van de tunnel anycasted zijn, wilt dit zeggen dat de gebruiker geen controle heeft over welke tunnel effectief gebruikt zal worden. Het terugkerende verkeer kan hierdoor ook een ander ingangspunt van een tunnel nemen wat kan leiden tot asymmetrische routes, lange latencies en onaanvaardbare wachttijden voor de gebruikers hiervan (**RIPE2016**).

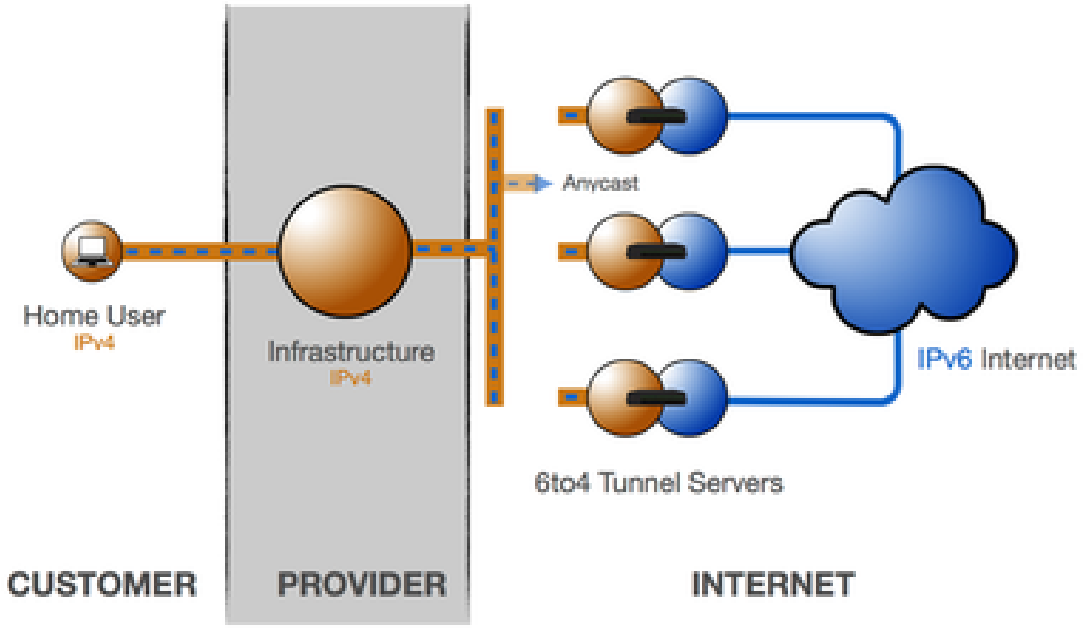
5.1.3 6rd

De derde methode namelijk 6rd, werd ontwikkeld om de problemen zoals lange latencies, die eigenaardig waren bij de tunneltechniek 6to4, op te lossen. Ook zal 6rd de schaalbaarheid behouden die te vinden was bij 6to4. Ondertussen is 6rd al ingevoerd bij enkele



Figuur 5.3: 6to4 omzetting (**RIPE2016**)

Figuur 5.4: 6to4 schematische voorstelling (**RIPE2016**)



Figuur 5.5: 6to4 visualisatie (**RIPE2016**)

miljoenen personen (**RIPE2016**).

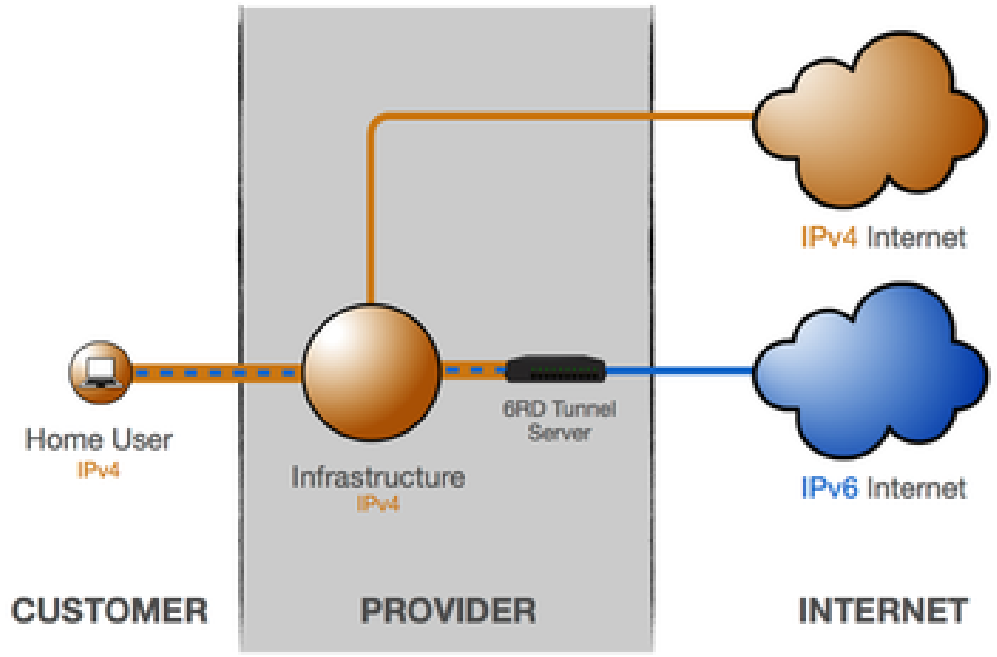
Het principe achter deze techniek is zeer eigenaardig aan die van 6to4. Eén van de belangrijkste verschillen is dat de IPv4 en IPv6 adresruimte van de ISP nu gebruikt zal worden voor de eindpunten van de tunnels. Dit betekent dat anycast niet langer meer gebruikt zal worden. Het verkeer wordt hierdoor symmetrisch en wordt door de ISP beheerd (**RIPE2016**).

Net zoals bij 6to4 moeten de IPv4-adressen van de tunneleindpunten in het IPv6-adres van de eindgebruiker worden geïntegreerd. Aangezien de eerste 32 bits van het IPv6-adres van het eindapparaat opgenomen zal worden door de prefix van de ISP en de tweede 32 bits gebruikt zal worden voor de IPv4 adressen van de tunneleindes. Slechts één /64 IPv6 range zal beschikbaar zijn voor elk apparaat (**RIPE2016**).

Het aanvragen van een grotere toewijzing van adresruimte, /29 in plaats van een /32, zou drie extra bits betekenen. Dit komt overeen met acht IPv6-subnetten die aan elk eindapparaat kan toegewezen worden in plaats van slechts één (**RIPE2016**).

Er is ook de mogelijkheid om te kiezen voor alleen het variabele deel van een IPv4-adres in het 6rd IPv6-adres te integreren. Als er een /21 IPv4-allocatie gebruikt wordt, dan betekent dat, dat de variabele bits, de laatste 11 bits, worden geïntegreerd in plaats van alle 32 bits van het IPv4-adres (**RIPE2016**).

Het combineren van beide methodes, zowel het gebruik maken van een /29 IPv6-toewijzing en het gebruik maken van de variabele bits van het IPv4 adres, geeft ons het volgende weer (**RIPE2016**).



Figuur 5.6: 6rd visualisatie (**RIPE2016**)

Figuur 5.7: 6rd schematische voorstelling deel 1 (**RIPE2016**)

Figuur 5.8: 6rd schematische voorstelling deel 2 (**RIPE2016**)

Figuur 5.9: 6rd schematische voorstelling deel 3 (**RIPE2016**)

Figuur 5.10: 6rd schematische voorstelling deel 4 (**RIPE2016**)

5.1.4 DS-Lite

DS-Lite staat voor Dual Stack Lite en is vooral gebaseerd op native IPv6, tunneling en NAT (Network Address Translation).

In tegenstelling tot alle andere transitietechnieken die reeds besproken zijn, gaat DS-Lite zijn IPv4-pakketten inkapselen in IPv6-pakketten. Wat resulteert in het tunnelen van IPv4 over IPv6. Dit is precies de tegenovergestelde werking van alle vorige besproken methodes (**RIPE2016**).

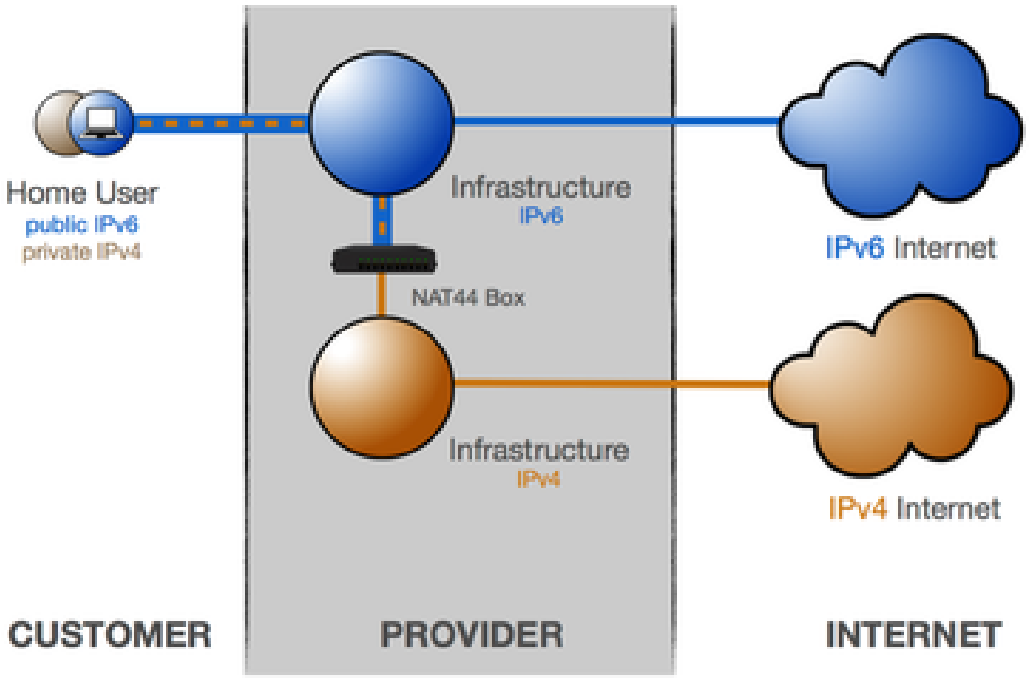
DS-Lite kan een IPv6-apparaat verbinding laten maken met een IPv4-apparaat en het IPv4-internet. Het voornaamste doel van DS-Lite is dat een ISP geen publiek IPv4 adres maar moet toewijzen aan een klant. In plaats daarvan worden alleen globale IPv6-adressen toegewezen (**RIPE2016**).

De CPE verdeelt, hetzelfde als een NAT-apparaat, private IPv4-adressen aan klanten. In plaats van de NAT zelf laten uit te voeren gaat de CPE het IPv4-pakket inkapselen in een IPv6-pakket. De CPE maakt hierbij gebruik van zijn wereldwijde IPv6-verbinding om het pakket op een correcte manier af te leveren aan de CGN van de ISP (carrier-grade NAT) dat een openbaar IPv4-adres heeft. Het IPv6 pakket wordt op zijn beurt uitgepakt waardoor het IPv6 pakket terug naar het oorspronkelijke IPv4 pakket wordt hersteld. NAT zal nadien uitgevoerd worden op het IPv4-pakket en het pakket zal zo door het openbare IPv4-internet gestuurd worden naar zijn bestemming (**RIPE2016**).

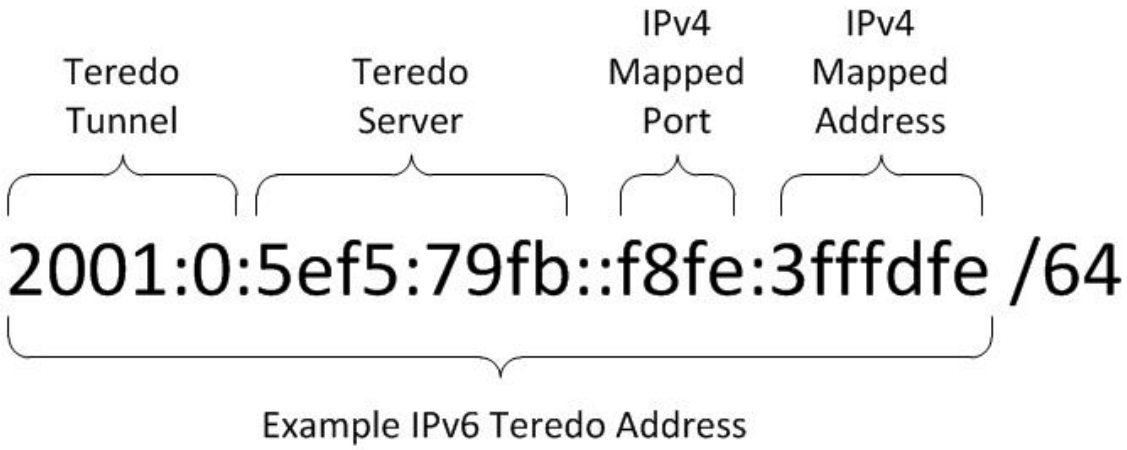
5.1.5 Teredo

Teredo is een per-host tunneltechniek voor het verzenden van IPv6 pakketten achter NAT apparaten via IPv4. De IPv6-pakketten worden ingepakt als een IPv4-pakket met een UDP header van het bestemmingsadres van een Teredo server met een welbekend UDP poort 3544. De algemene Teredo server voor windows is teredo.ipv6.microsoft.com. Alle tunnels naar Teredo gebruikers delen dezelfde IPv6 prefix namelijk 2001:0::/32 gevolgd door het IPv4 adres van de gebruikte Teredo Server. In het geval van Microsoft is dit 94.245.121.251 en omgezet in hexadecimaal is het 5ef5:79fb. Het adres met beide prefixen ziet er als volgt uit, 2001:0:5ef5:79fb::/64 (**Vinciguerra2013**).

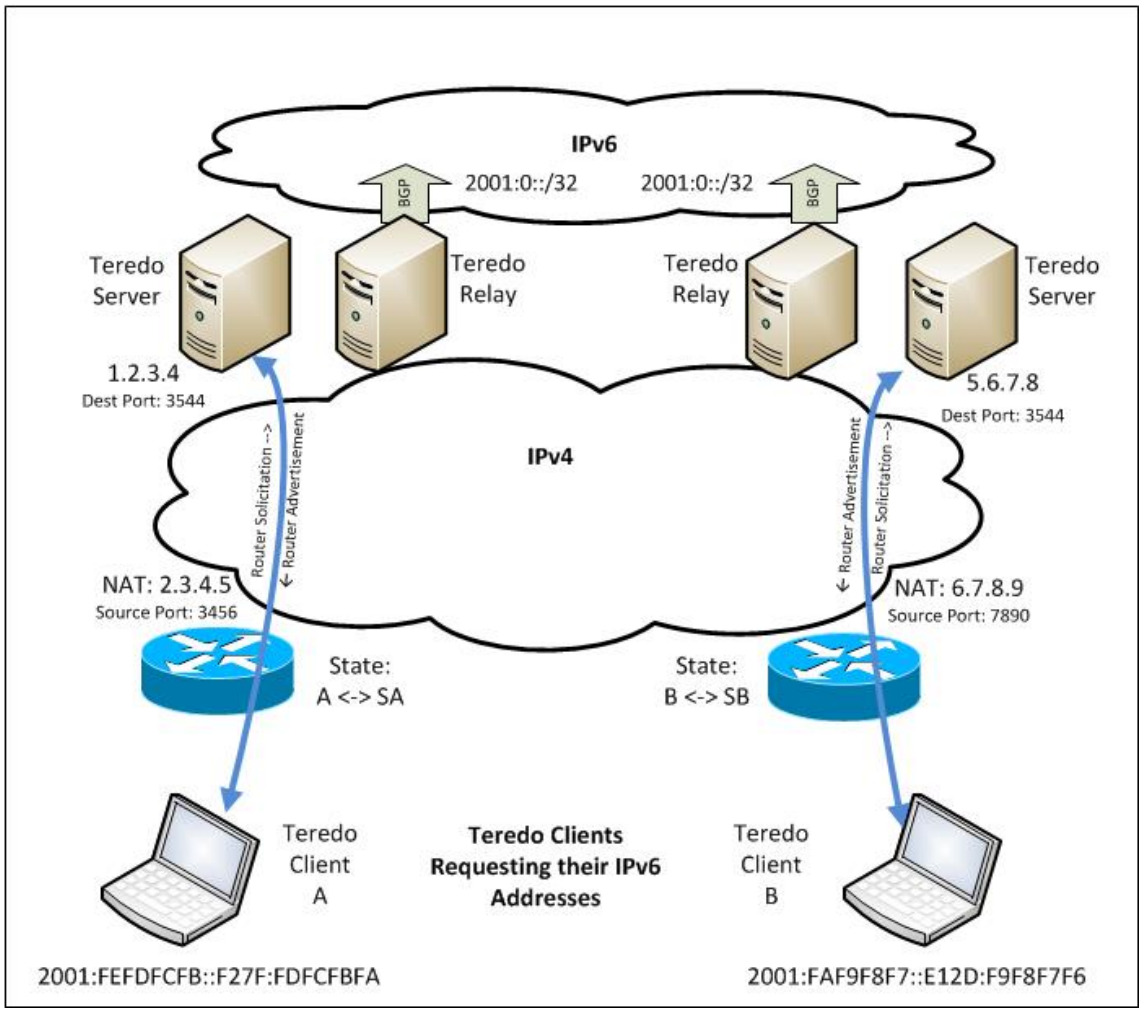
De Teredo gebruiker zal een IPv4 router soliciation versturen naar de Teredo server. Nadien zal de server de gebruiker voorzien van zijn IPv6-adres door het versleutelen van zijn IPv6-adres door het NATed bron IPv4-adres en de UDP-bronpoort naar het einde van het



Figuur 5.11: DS-Lite visualisatie (**RIPE2016**)



Figuur 5.12: Teredo schematische voorstelling (**Vinciguerra2013**)



Figuur 5.13: Teredo visualisatie (**Vinciguerra2013**)

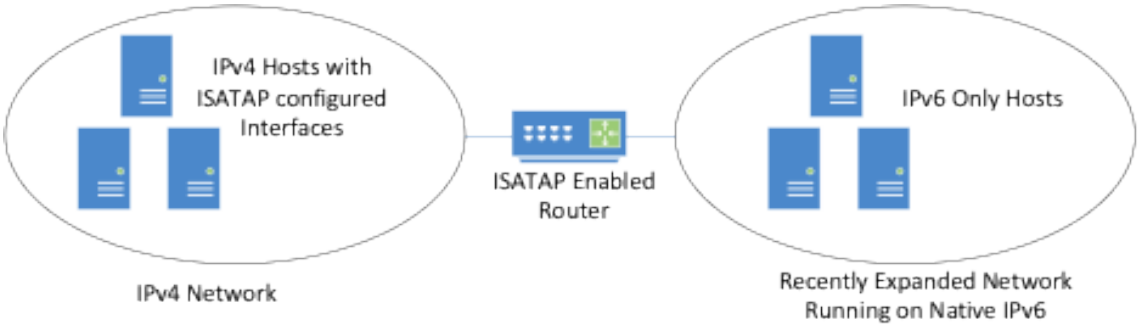
IPv6-adres (**Vinciguerra2013**).

Het Teredo protocol is gebaseerd op een speciaal IPv6-pakket zonder payload dat een luchtbeld wordt genoemd, om door NAT apparaten te geraken. Er zijn twee soorten bubbels. Als eerst zijn er de directe bubbels, die van Teredo peer naar Teredo peer worden verstuurd. Als tweede zijn er de indirecte bubbels die door de Teredo server van de peer verstuurd worden (**teredo**).

5.1.6 ISATAP

ISATAP (Intra Site Automatic Tunneling Address Protocol) is een interface die hosts kunnen gebruiken om IPv6 verkeer over een IPv4 netwerk te laten verzenden. Door het toevoegen van headers met IPv4 netwerk informatie aan het IPv6 pakket kan de gebruiker pakketten verzenden over het netwerk naar een IPv6 bestemming. Nadien kan de ontvanger van het pakket deze uitpakken tot zijn originele staat (**RIPE2016**).

ISATAP is vrij eenvoudig om te herkennen. De adressen die dit protocol hanteert zijn zeer



Figuur 5.14: ISATAP visualisatie (**RIPE2016**)

uniek geformatteerd. Een voorbeeld van een ISATAP adres is 2002:9D36:1:2:0:5EFE:192:168:12:9 (**RIPE2016**).

Bij nader inzien zijn er twee opvallende delen aan het adres. Het eerste deel, 2002:9D36:1:2:0:5EFE: is geformatteerd als een typisch IPv6 adres. Het tweede deel, 192.168.12.9, is het formaat van een IPv4 adres. Het formaat hiervan bevat essentiële informatie. Ten eerste is het adres een geldig IPv6 adres waarmee IPv6 connectie mogelijk is. Vervolgens geeft de aanwezigheid van het IPv4-adres, de IPv4-informatie aan die zal gebruikt worden om het IPv6-verkeer over het IPv4-netwerk te leiden (**RIPE2016**).

Met een ISATAP router en het configureren van ISATAP bij hosts in het IPv4 netwerk, is het mogelijk om IPv6 only hosts te laten communiceren met het IPv4 netwerk (**RIPE2016**).

5.2 Translatie

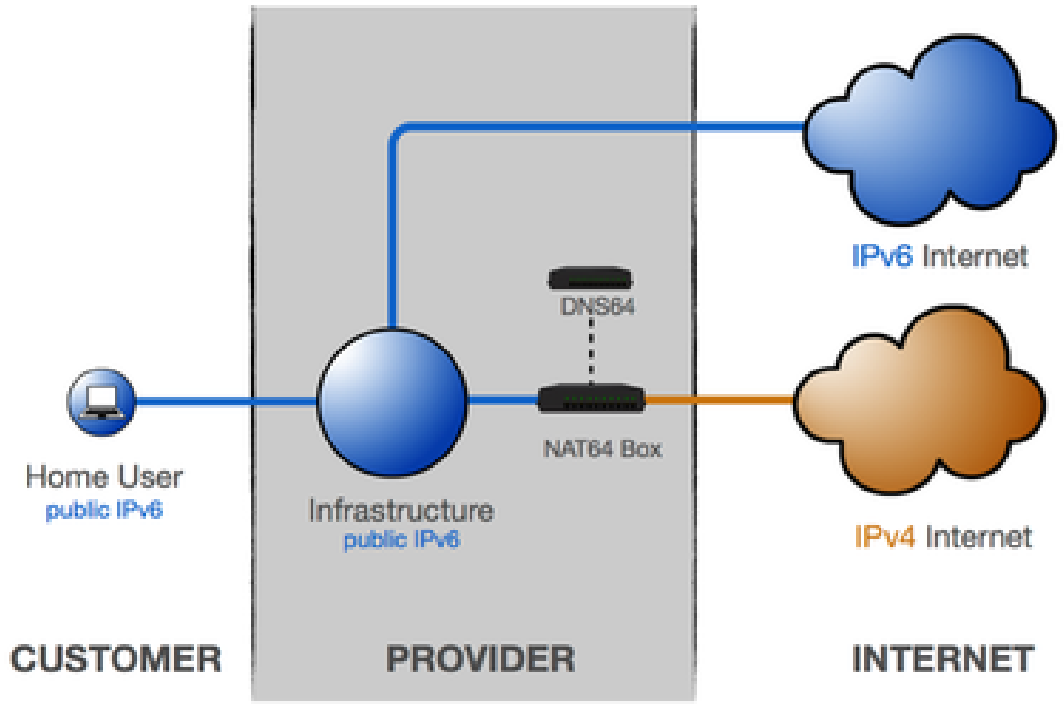
In het geval van een translatie zal het pakket niet worden ingepakt als een IPv4 pakket. In dit geval zal de IPv6 header van het pakket vervangen worden door een IPv4 header. Hierdoor zal het IPv6 pakket vertaald en omgezet worden naar een IPv4. Enkele technieken die hiervoor worden uitgelegd zijn NAT64/DNS64 en 464XLAT (**RIPE2016**).

5.2.1 NAT64/DNS64

NAT64/DNS64 is een methode die het mogelijk maakt om voor IPv6 klanten connecties te laten maken naar IPv4-apparaten.

In het netwerk van de ISP is er een translator box aanwezig (NAT64 server) die de headers van een IPv6-pakket verwijderen en vervangen met een IPv4-header. De NAT64 server is het eindpunt voor op tenminste één IPv4 adres en een IPv6 netwerk segment van 32 bits (**RIPE2016**).

Het meest centrale deel van dit mechanisme is DNS64. In het geval van DNS64 zet de DNS-server IPv6 DNS queries om naar IPv4 DNS queries. Achteraf zullen de ontvangen pakketten omgezet worden van IPv4 DNS records naar IPv6 records (**RIPE2016**).



Figuur 5.15: NAT64 visualisatie (**RIPE2016**)

NAT64/DNS64 wordt hoofdzakelijk gebruikt bij grote mobiele providers.

5.2.2 464XLAT

Een mogelijk probleem bij sommige mobile apps is dat deze enkel IPv4 connecties ondersteunend zijn en dus niet functioneel zijn met IPv6.

Om dit probleem te verhelpen is een extra transitie methode nodig namelijk 464XLAT. Dit wordt in gebruikt in combinatie met NAT64/DNS64 (**RIPE2016**).

464XLAT wordt geactiveerd via het installeren van software op het IPv6 mobiele apparaat, CLAT demon (**RIPE2016**).

464XLAT zal het mobiele apparaat een dummy IPv4 geven. Op deze manier kunnen de applicaties die enkel IPv4 ondersteunen gebruik maken van deze dummy. Achteraf zal CLAT demon een lokale vertaling doen naar IPv6 op het apparaat (**RIPE2016**).

5.3 Besluit

Bij het gebruiken van deze methodes komt er ook een extra complexiteit bij te pas. Dit zal het netwerk niet vergemakkelijken en hecht een zeker kennis en onderhoud van het

netwerk. Deze methodes zouden op elk ogenblik vermeden moeten worden waar mogelijk. Een betere oplossing voor dit probleem zou het toepassen van DS-Lite kunnen zijn. Deze mechaniek heeft een lagere complexiteit en brengt minder nadelen met zich mee.

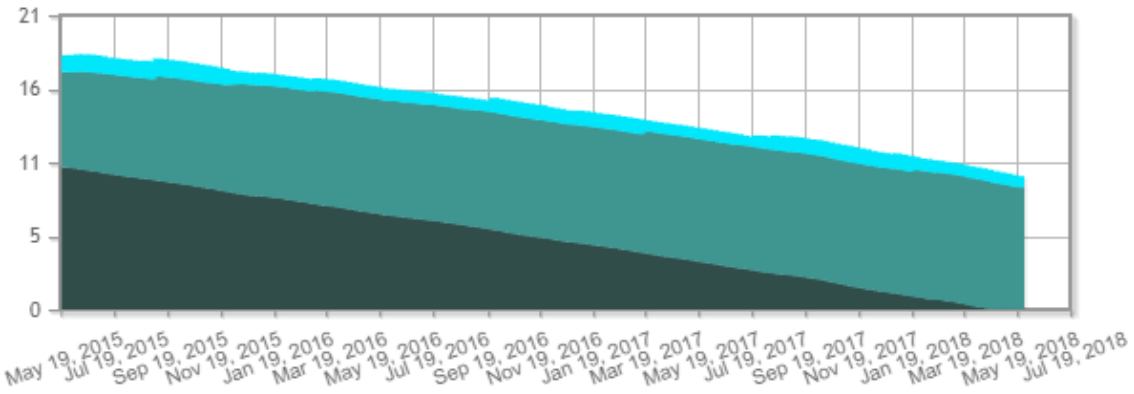
6. Aftellen van IPv4

Dit hoofdstuk bespreekt wat de uitputting van IPv4 juist inhoudt, hoe deze tot zover is kunnen komen en wat een oplossing is om hiermee om te gaan. Ook zal er visueel aangetoond worden hoe we er vandaag de dag tegenover staan en wat er de komende maanden zal gebeuren rond IPv4 uitputting en IPv6.

Op 3 februari 2011 had IANA (Internet Assigned numbers Authority) aangekondigd dat hun vrije IPv4 pool volledig uitgeput was. De IPv4 uitputting betekent niet dat het einde van het internet is aangebroken. Deze term wordt gebruikt om aan te tonen dat er geen niet-toegewezen IPv4 adressen beschikbaar zijn om uit te delen. Door de grote groei aan IoT, mobiele apparaten en andere geconnecteerde apparaten zijn de beschikbare adressen op een zeer snelle en korte tijd uitgedeeld. Dit werd nooit verwacht tijdens de bouw van IPv4 en werd ook niet gemaakt om heel de wereld in contact te brengen met het internet. Als gevolg was er dus het IPv6 protocol ontwikkeld die de uitputting van IPv4 zou wegnemen.

RIPE NCC, die verantwoordelijk is voor Europa, is begonnen op 14 september 2012 met het uitdelen van zijn laatste /8 blok. De /8 blok bevat de laatste beschikbare IPv4 adressen om uit te delen en bevat 16777216 (2 tot de 24) adressen. Volgens de policy van RIPE NCC is het voor de leden enkel mogelijk om een /22 (1024 adressen) blok aan te vragen, ook al kunnen ze grondig aantonen dat er een grotere blok nodig is krijgen ze maar een /22. Ook zal er geen nieuwe PI (Provider Independent) aangesteld worden.

Voor het bereiken van de laatste /8 blok zijn er verschillende fases ondernomen. Fase 0 was het uitdelen van de IPv4 adressen. Op dat moment was er nog geen sprake van een totale uitputting. Tijdens deze fase werden adressen enkel toegewezen als de evaluatie ook volledig afgerond was. Er werden dus ook geen adressen gereserveerd of aan de kant



Figuur 6.1: IPv4 uitputting (**RIPE2014**)

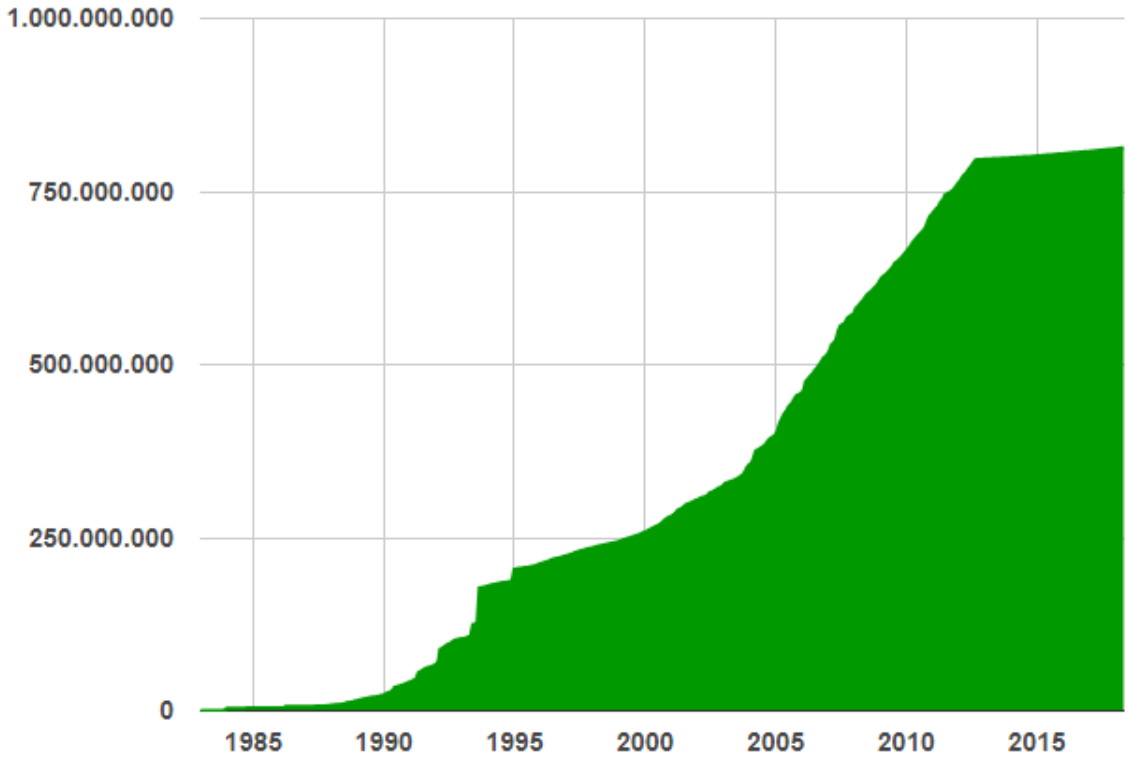
gehouden tijdens deze evaluatie. Verzoeken naar adressen werden grondig gecontroleerd door een IPRA (IP resource Analyst) en voerde interne controle uit (**RIPE2016Fases**).

Het bereiken van fase 1 vond plaats op 4 september 2012. Deze fase werd geactiveerd als er een kritieke toestand plaats vond bij de beschikbare adressen. Op dit moment was er nog een voorraad van één maand of één /10 blok naast /8 om uit te delen. Verder werden de controles zwaarder en grondiger behandeld (**RIPE2016Fases**).

Momenteel situeren we onszelf in fase 2. Deze fase ging van start op 14 september 2012, enkele dagen nadat fase 1 werd bereikt. Bij het begin van deze fase werden alle verzoeken die in de wachtrij stonden bevroren. Zij werden op de hoogte gebracht dat de laatste /8 blok en werd ingezet en verdeeld. Enkel de LIRs die in aamerking komen zullen eenmalig een /22 toegewezen krijgen (**RIPE2016Fases**).

Op 10 april 2018 waren er nog 0.12 miljoen adressen over of 0.01 /8s. Vandaag zijn er geen beschikbare adressen meer over in de blok, dit werd bereikt vanaf 17 april 2018. Nu de laatste blok volledig op is wil dit niet zeggen dat er geen beschikbare adressen meer over zijn. RIPE NCC is momenteel bezig met het herstellen van andere adressen. Deze kunnen gaan van het terugnemen van adressen als een bepaalde LIR is gestopt en van gerecupereerde adressen van IANA's pool. Maar vooraleer deze adressen worden uitgedeeld en toegewezen blijven ze in quarantaine. Momenteel is er ook geen exacte datum of tijdstip vastgelegd wanneer adressen uit de quarantaine worden gehaald klaar om uitgedeeld te worden (**RIPE2014**).

Deze grafiek geeft een evolutie aan van beschikbare IPv4 adressen. In bovenstaande grafiek is er duidelijk te zien dat naar gelang de tijd de beschikbare adressen dalen. De donkere kleur staat voor de laatste /8 blok die vrijgegeven is. De licht groene kleur heeft dan meer een stijgende evolutie gekend. Dit zijn de adressen die gerecupereerd zijn van IANA en van LIRs die gestopt zijn. In dit deel komen er dus meer adressen vrij maar blijven ze wel in quarantaine. de blauwe kleur bovenaan toont de gereserveerde adressen aan. Deze worden ingedeeld in een /13 voor tijdelijke toewijzingen, /16 voor IXPs (Internet Exchange Point) en nog een /16 voor onvoorziene omstandigheden die kunnen plaatsvinden. Ook hierin zitten enkele gerecupereerde adressen in quarantaine (**RIPE2014**).



Figuur 6.2: IPv4 evolutie (**RIR2018**)

Op 8 mei 2018 zijn er in totaal nog 9.70 miljoen adressen over waarvan er maar 8.89 miljoen ter beschikking zijn. Zoals we al eerder vernomen hadden, is het aantal in de laatste 185 /8 blok enorm klein. Het aantal beschikbare adressen staat op 0.04 miljoen adressen. Al de gerecupereerde adressen komen samen neer op een 8.85 miljoen adressen. Maar deze zijn dus nog steeds in quarantaine en komen nog niet vrij. De gereserveerde adressen zijn niet beschikbaar en tellen mee voor 0.81 miljoen (**RIPE2014**).

De grafiek hierboven toont de evolutie van IPv4 in de RIPE NCC zone, ook wel verantwoordelijke voor Europa. De groei dat er is gekomen vanaf de jaren 2000 is immens. Als we verder kijken naar het jaartal 2012, wanneer de laatste 185 /8 blok was aangekondigd, zien we een sterke verandering in de groei. De groei die het tussen het jaar 2012 en heden heeft een zeer kleine stijgingsfactor. Dit komt voornamelijk door de policies die zijn opgesteld door RIPE om met de laatst beschikbare blok voorzichtig overweg te gaan. Hierbij werd er grondig gekeken en in kleinere maten adressen toegewezen waardoor ze zo lang mogelijk de volledige uitputting wilden tegengaan.

6.1 Besluit

Enkele conclusies die er kunnen gemaakt worden zijn, dat komende maanden een hoogtepunt zullen zijn voor zowel IPv4 als voor IPv6. Voor IPv4 kan dit het volledig einde betekenen van de blok wat voor IPv6 een goede zaak kan betekenen. Nu het moeilijker is

om nog een range van IPv4 adressen te krijgen gaat er meer overschakelen naar een IPv6 range. Hierdoor zal de vraag naar IPv6 stijgen en de ontwikkeling en overgang sneller in gang gezet worden.

7. IPv6 op globaal niveau

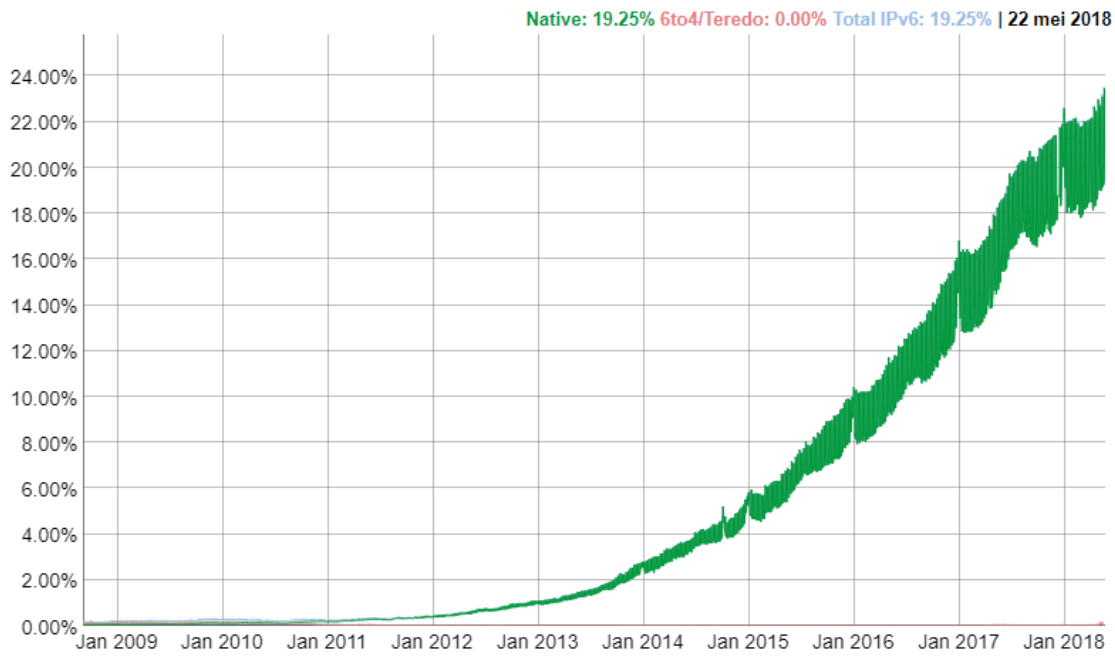
In dit hoofdstuk zal er dieper worden ingegaan op de adoptie van IPv6 op verschillende niveaus. Er zal bekeken worden hoe deze overgang loopt op zowel globaal niveau als een klein deel op Europees en Belgisch niveau. Dit zou een goede schets moeten geven over hoe het er in België momenteel aan toe gaat en of we al dan niet een betere verhouding hebben dan andere landen.

7.1 Hoe staat IPv6 er tegenover

Het is ook al eerder geweten dan vandaag dat de uitputting van IPv4 tot zijn einde is gekomen. De beschikbare adressen zijn bijna volledig uitgedeeld en het einde is nabij. Als gevolg hiervan was er IPv6 ontwikkeld om IPv4 over te nemen na zijn uitputting. Dankzij de 'World IPv6 Day' is de groei en het aantal gebruikers van IPv6 zeker gestegen. Vanaf deze dag is IPv6 officieel aangekondigd als opvolger van IPv4.

7.2 IPv6 op globaal niveau

IPv6 is wereldwijd bekend, het nieuwe internet protocol. Hier zal er verder onderzocht worden wat de huidige status is over het internationale gebruik van IPv6. Hoe bedrijven, landen en gebruikers zich hieraan gaan aanpassen en of dit wel effectief bekend is en gebruikt wordt. Het globaal bekijken van het gebruik van IPv6 kan op verschillende manieren gebeuren. Er zal gebruik gemaakt worden van grafieken die geanalyseerde data grafisch zal voorstellen. Verschillende grafieken zullen vergelijkingen weergeven op



Figuur 7.1: IPv6 evolutie van Google (**GoogleIPv6**)

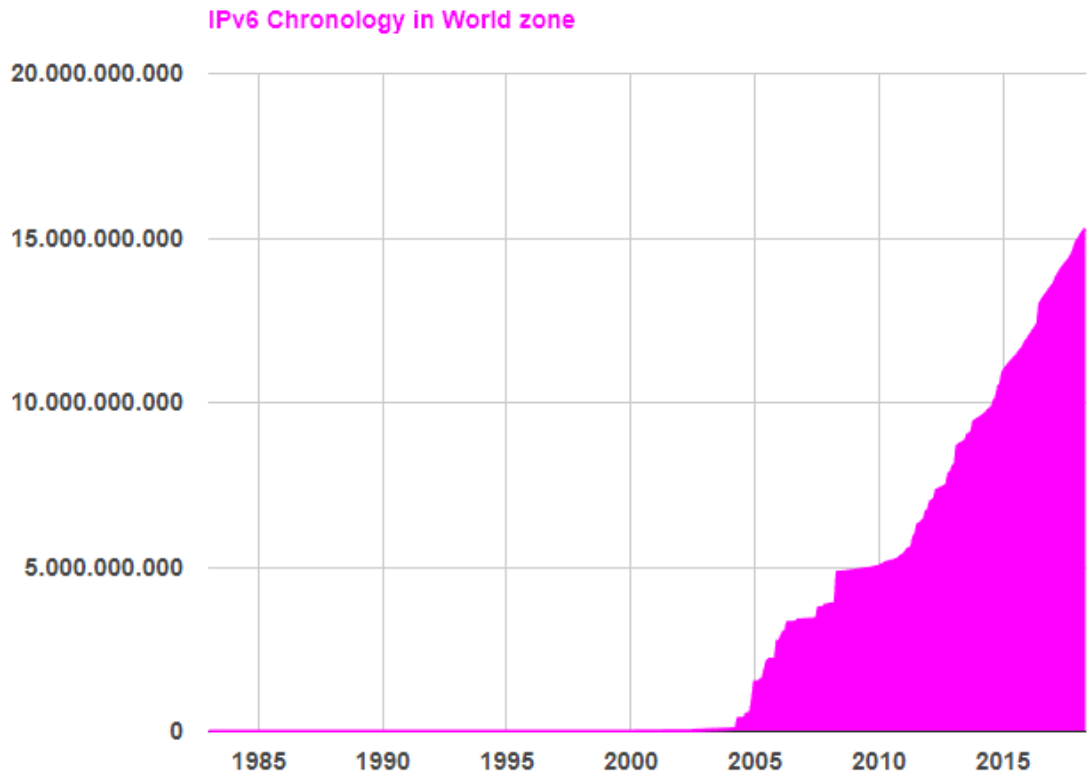
verschillende aspecten die onderzocht kunnen worden. Alsook het analyseren van globale enquêtes.

Een eerste grafiek zal aantonen hoeveel gebruikers er zijn, die Google bereiken over IPv6. Deze grafiek geeft een duidelijke weergave van de groei die afgelopen jaren volgde en vooral vanaf 2011, de dag waarop IPv6, begon met evolueren. De laatste meting was op 22 mei 2018 en bevatte een totaal van 19.25% IPv6 gebruikers. Dit wilt verder zeggen dat bijna 1 op de 5 personen Google bereikt via IPv6.

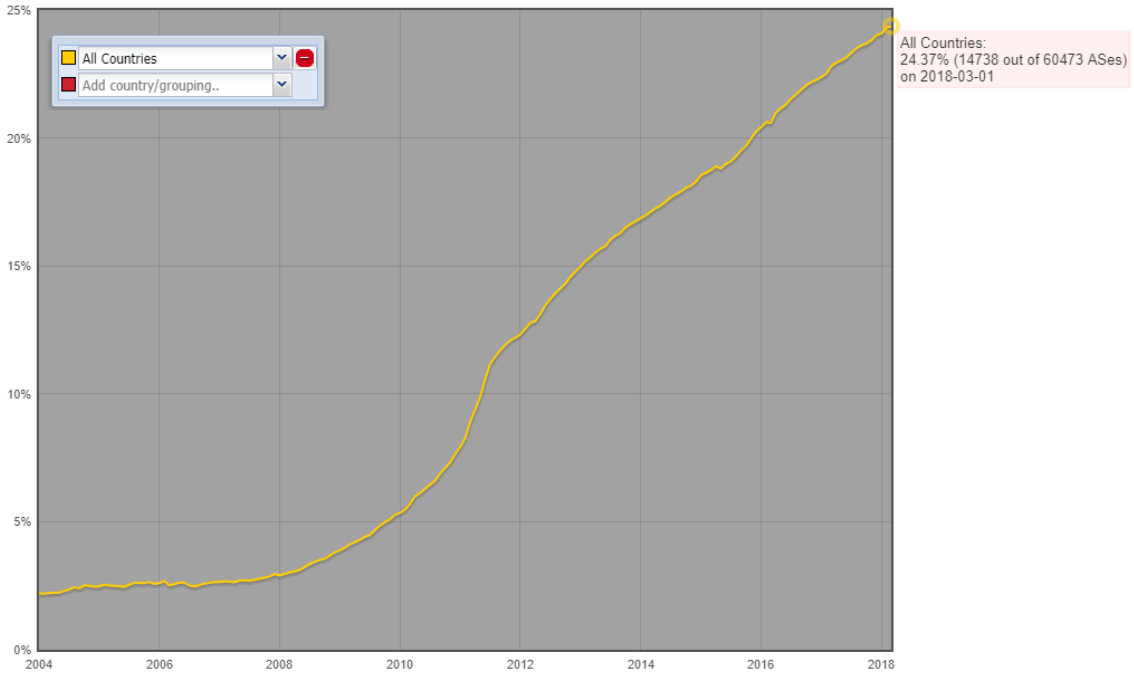
Een volgende grafiek geeft weer hoeveel /48 blokken er uitgedeeld zijn van IPv6. Als we deze grafiek dieper gaan onderzoeken, zijn er twee stijgingen te zien. De eerste stijging vond plaats vanaf 2004 tot en met 2006. Deze evolutie is vooral te danken aan de eerste opkomst van IPv6. De tweede groei, waarbij deze nog niet is gestopt en dus nog steeds aan het doorgroeien is, is begonnen in 2011. Hier kunnen we zeggen dat dit gekomen is door de dag van IPv6 dat was uitgeroepen in 2011. Ook is er te zien dat vanaf het jaar 2011 een blijvende stijging is wat het zeer goed maakt voor de populatiegroei van IPv6. De laatste meting, op 1 mei 2018, telt 15.281.735.778 /48 blokken wereldwijd.

Onderstaande grafiek geeft ons een breder beeld over het percentage netwerken, autonome systemen, dat een IPv6 prefix aankondigd. Globaal gezien is er een gemiddelde van 24.37%, waarvan 14738 van de 60473 Ases, IPv6 geactiveerde netwerken. Deze laatste meting werd genomen op 1 maart 2018.

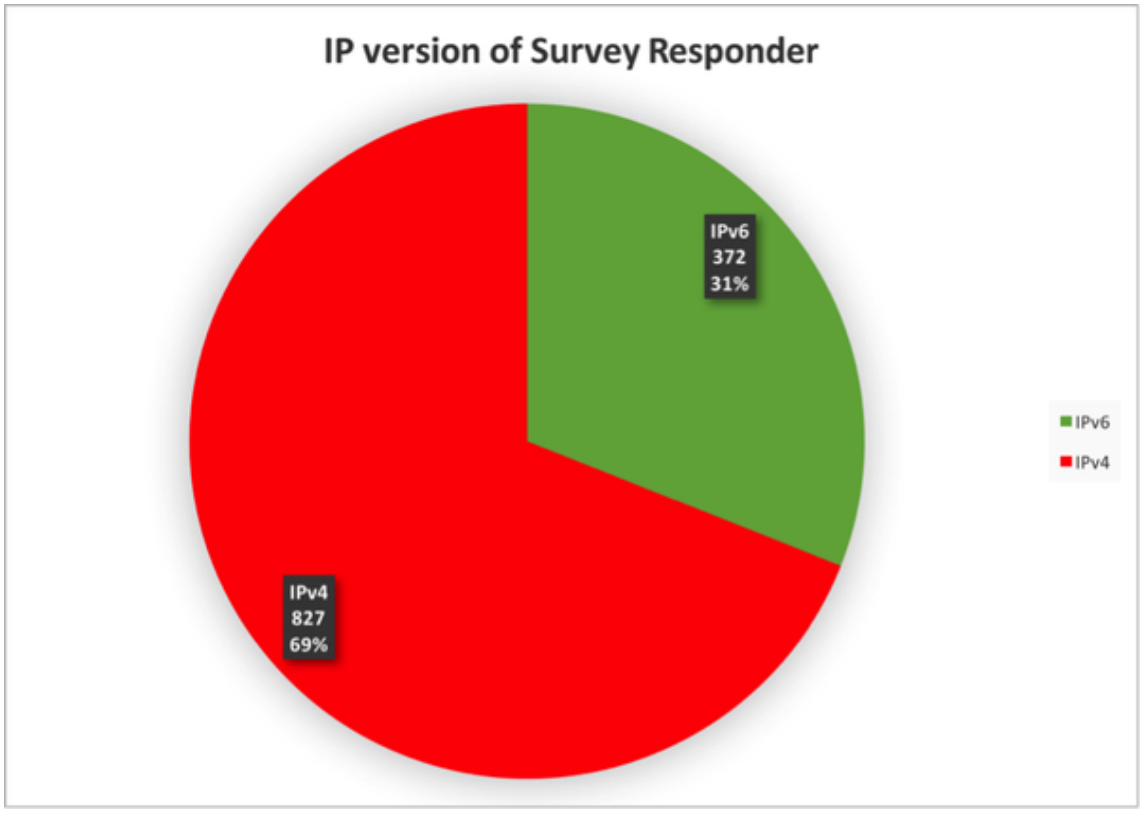
Er is ook een duidelijk overzicht van welk land het beste scoort op verschillende onderdelen van IPv6 gebruik. Dit gebruik kan onderverdeeld worden in 4 verschillende categorieën namelijk, Web, Email, DNS en IPv6 actieve gebruikers.



Figuur 7.2: IPv6 /48 blok visueel (**RIR2018**)



Figuur 7.3: IPv6 autonome systemen (**RIPE2016**)



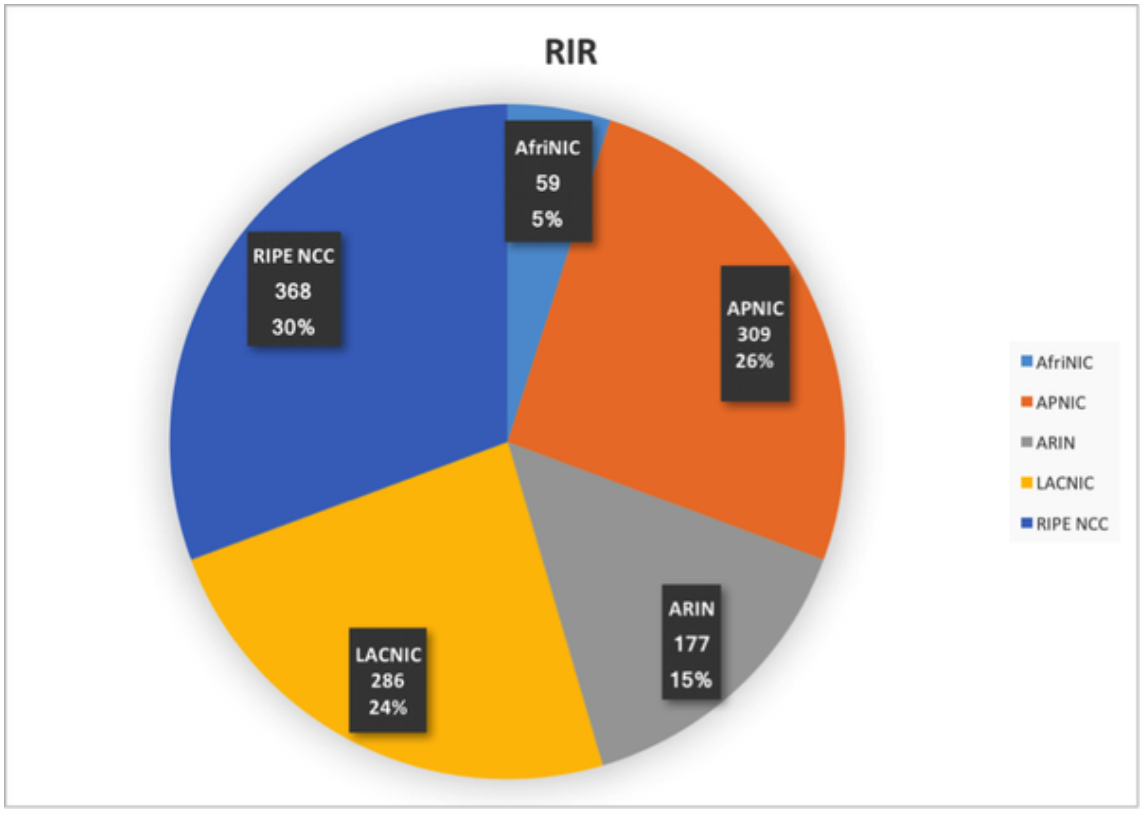
Figuur 7.4: IPv6 survey 2016 respons (**Martinez2016**)

Vervolgens heeft RIPE enkele enquêtes opgesteld om te meten wat de ondervindingen zijn en hoe het zit met het uitrollen van IPv6. Hiermee kan er onderzocht worden hoe de aanpak, adoptie en aanvaardingen zijn van IPv6. Verder gaan er enkele enquêtes aangekaart worden en met elkaar vergeleken worden. Deze zullen een duidelijk overzicht geven van de overgang van IPv6 op jaarniveau. Hiermee kan er onderzocht worden hoe groot de evolutie is op de voorbije jaren.

De eerste enquête die werd opgesteld dateert van 14 November 2016, de intentie hiermee was om een breder beeld te creëren over de huidige uitrolling van IPv6 was, specifiek gericht op ISP's.

De eerste grafiek geeft een zeer informatief beeld terug. Hierop is beter te zien dat de respons op de enquête uit twee soorten gebruikers bestaat. De eerste groep heeft IPv4 gebruikt, de andere groep gebruikte IPv6 om deze enquête te beantwoorden. Dit geeft ons dus al een beter beeld van hoeveel percent van de gebruikers het IPv6 protocol hanteren. In 2016 was dit maar liefst 31%, 372 van de 1199 deelnemers, hebben over IPv6 beantwoord.

Een volgende grafiek geeft beter aan van waar deze deelnemers komen en onder welke instantie ze vallen. Met instanties wordt er bedoeld onder welke regio de deelnemers vallen. Op onderstaande grafiek is er dus duidelijk te zien dat de meeste uit de regio RIPE NCC komen. Deze instantie is verantwoordelijk voor de Europese kant. Waaronder ARIN verantwoordelijke is voor de Amerikaanse regio, AfriNIC voor de Afrikaanse, APNIC voor de Aziatische en de LACNIC voor de Latijns-Amerikaanse regio.



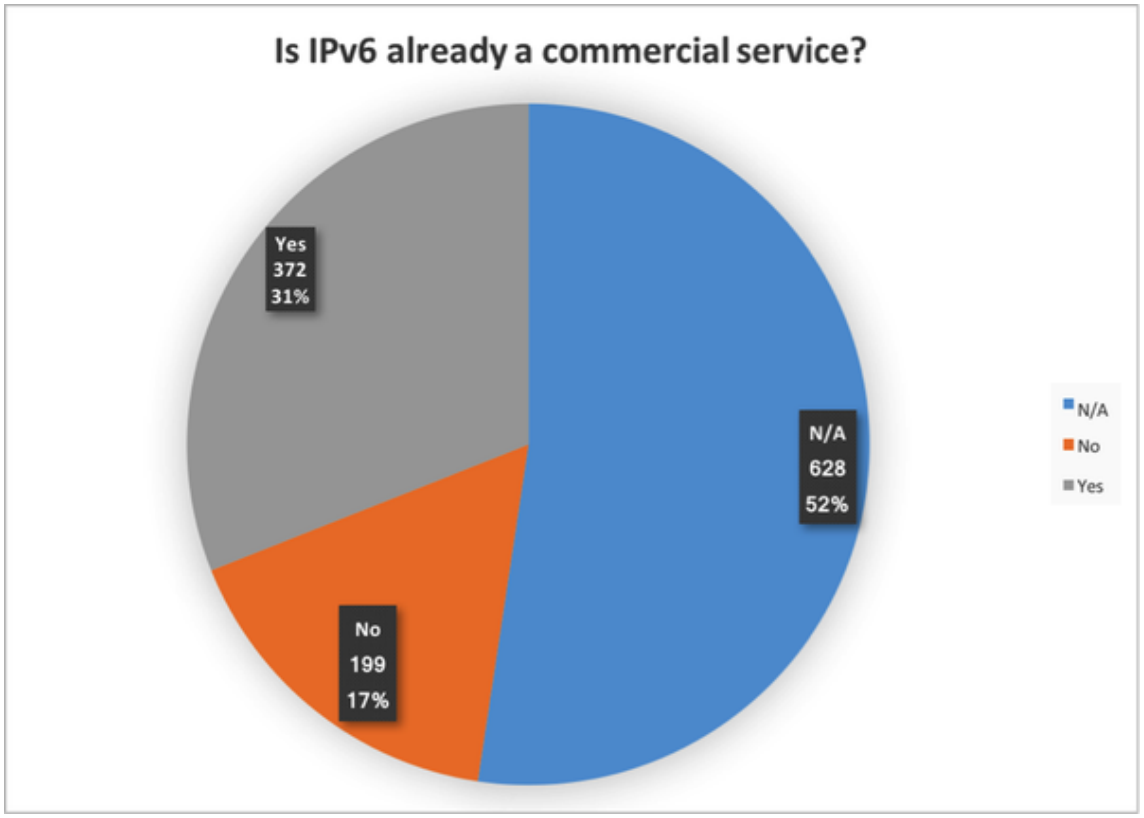
Figuur 7.5: IPv6 survey 2016 RIR (**Martinez2016**)

Hoe gecommercialiseerd is IPv6 binnen de ISP's nu? Wel, volgende grafiek geeft hierop een duidelijker beeld. Er wordt aangetoond dat 31% van de ISP's gebruik maken van IPv6 en commercieel actief mee bezig zijn. 17% van de ISP's is nog niet actief en dus ook nog niet commercieel actief, of zit momenteel in de test fase voor verdere stappen te ondernemen. De overige 52% heeft deze vraag niet beantwoord. Daardoor kunnen we besluiten dat van alle deelnemers er 64% van de ISP's actief bezig is.

Op vlak van technologie is er veel keuze om klanten gebruik te laten maken van IPv6. Om een beter beeld te geven van de geprefereerde technologie keuzes van ISP's is hieronder een grafiek die deze vraag beantwoord. Op het eerste zicht is er een groot deel dat gebruik maakt van FTTH, 35%, xDSL, 22%, en via kabel of DOCSIS, 20%.

De laatste grafiek zal een verduidelijking weergeven op de gebruikte transitie mechanismen van een ISP. Bij transitie mechanisme zijn er veel verschillende methodes, maar welke het meest gebruikt worden onder de ISP's is belangrijk om te weten. Op onderstaande grafiek is er een duidelijke winnaar. De methode die het meeste gehanteerd wordt is Dual-stack met een publiek IPv4 en Global unicast adres, GUA. In hoofdstuk 3 werd er dieper ingegaan op enkele methodes en uit de conclusie blijkt dat er een voorkeur was naar Dual-stack, wat hier ook bewezen is.

Om de evolutie op een jaar tijd te bekijken, gaan we deze resultaten vergelijken met de enquête die dateert van 13 oktober 2017. Met deze update is er een beter zicht mogelijk op de evolutie van IPv6 op een jaar tijd. Hierbij zullen de uitslagen vergeleken worden met de



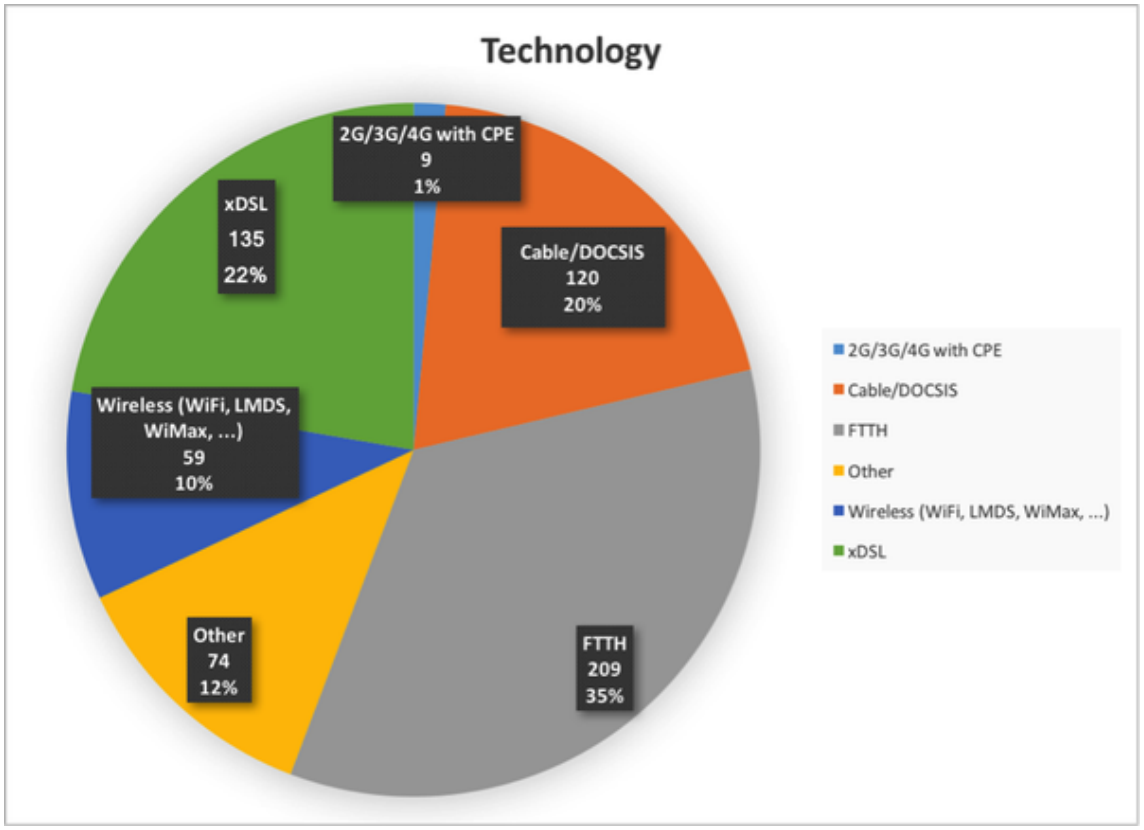
Figuur 7.6: IPv6 survey 2016 commercieel (**Martinez2016**)

enquête van 2016.

Opnieuw werd er gekeken hoever de commercialisatie stond van IPv6 bij ISP's. Bij het opnieuw stellen van deze vraag is er een duidelijk verschil van resultaten ten opzichte van het vorige jaar. Het grootste verschil is het aantal deelnemers die deze vraag niet beantwoord hadden. Bij de laatste update werd deze vraag volledig beantwoord en gaf dit een beter beeld van de effectieve commerciële diensten. Er waren maar liefst voor 65%, 438 van de 673 deelnemers, van de antwoorden een ja-stem. Dit wil zeggen dat 65% van de deelnemers actief bezig is met het aanbieden van IPv6 aan klanten. Waaronder het jaar ervoor maar 199 ISP's bezig waren met het verdelen van IPv6.

Op vlak van de gebruikte technologieën zijn er weinig veranderingen gebeurt op jaarbasis. De meest gehanteerde methodes blijven FTTH, xDSL en 3G broadband als bijkomende methode. Deze zijn voorlopig de meeste populaire technologieën. Hoewel in het jaar 2016 DOCSIS populair was, is deze verminderd naar gebruik toe.

Ook is er een overgang van gebruikte transitie mechanieken. Hierdoor blijkt dat nieuwere en recentere methodes worden gehanteerd in plaats van de oudere technieken. Het is zo dat er een groei is in het gebruik van 464XLAT en dual-stack met publieke IPv4 adressen. Verder is het zeker belangrijk om een nieuw evolutie-onderzoek op te stellen van het jaar 2017 tot 2018. Dit zou een nog beter zicht moeten geven over wat er echt aan het doorgroeien is naar een standaardoplossing voor dergelijke methodieken om met IPv6 te werken.

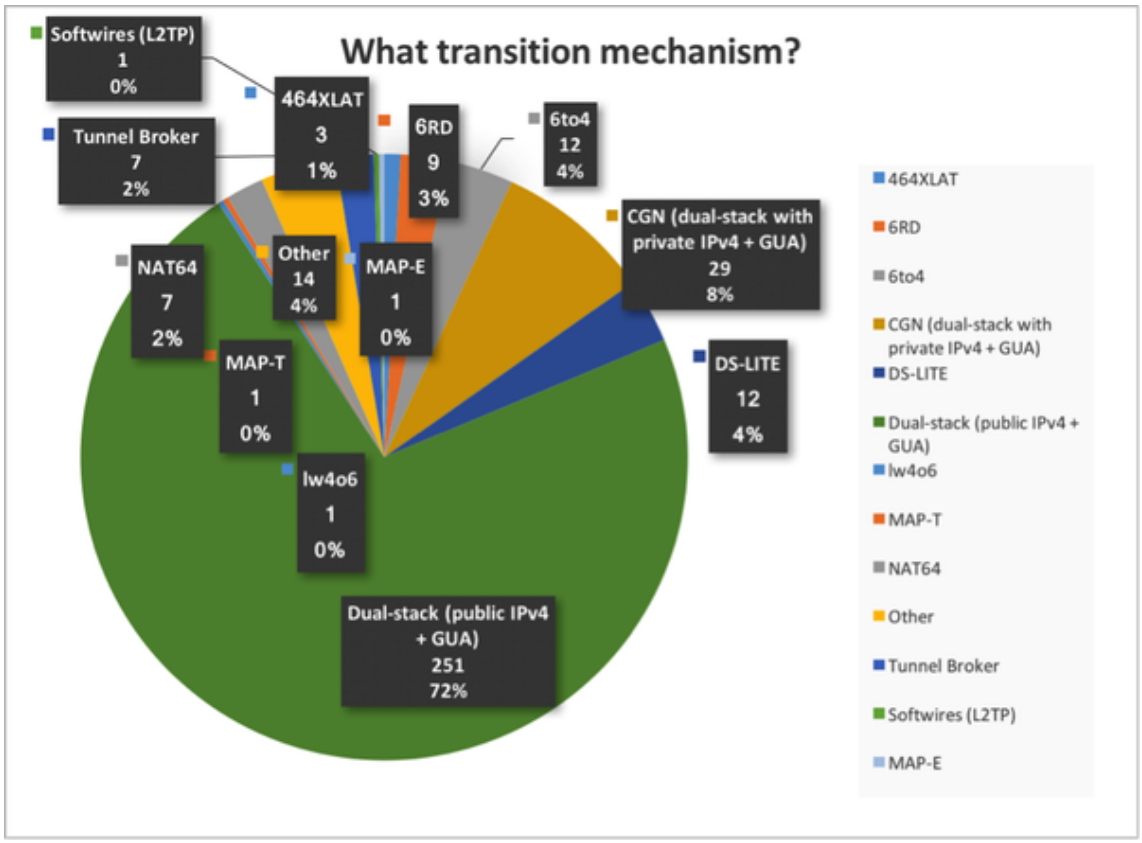


Figuur 7.7: IPv6 survey 2016 technologie (**Martinez2016**)

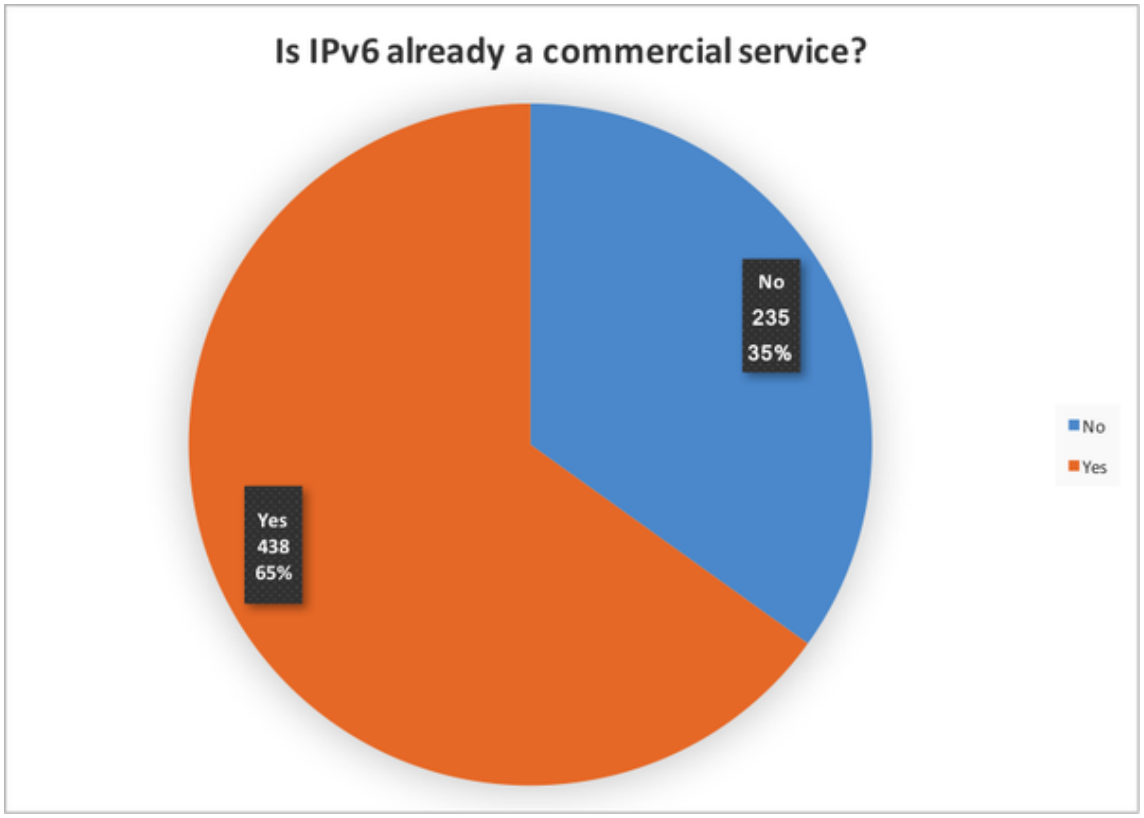
In 2018 werd er een interessante update van een bepaalde enquête uitgevoerd. Deze ging eerder over de adoptie wereldwijd en niet zozeer gefocust op ISP's. Deze enquête werd uitgevoerd in verschillende jaren zoals 2008, 2009, 2011, 2012 en het laatste jaar 2013. Nu in 2018 werd er een update gemaakt voor de evolutie om de afgelopen 5 jaar te weerspiegelen en opnieuw informatie te verzamelen. RIPE heeft deze uitgevoerd en de eerste resultaten werden voorgesteld op het RIPE76 evenement in Marseille op 14-18 mei 2018. De uitgebreide resultaten zullen worden voorgesteld op 6 juni op het Educa evenement. Daarom zullen de eerste resultaten al onderzocht worden in deze scriptie.

In de verkregen resultaten is er te zien dat er ongeveer een 50% van de antwoorden vooral uit grote ISP's is gekomen, voor 30% aan educatieve instellingen en ICT instellingen en voor 20% aan overheid, onderzoekers en andere instellingen. Deze indelingen komen overeen met de jaren ervoor wat het zeer goed maakt omdat het over dezelfde aantal soorten instellingen gaat. Het probleem bij deze enquête was dat deze niet bereikbaar zijn vanaf IPv6. Waardoor er enkele resultaten wegvielen maar volgens RIPE was dit de bedoeling omdat deze hetzelfde moest opgesteld zijn als de jaren er voorheen.

Opvallende data die was geanalyseerd was de IPv6 allocatie. IPv6 allocatie betekent het toewijzen van adresruimte naar IR (Internet Registry) om op hun beurt terug die adresruimte door te verdelen. Momenteel staat het op 85% IPv6 allocatie. Dit komt neer op een groei van 20% met het jaar 2012 en een groei van 10% met 2013. Het is logisch dat deze momenteel minder en minder zal groeien. Het is dus nog niet de bedoeling om 100%



Figuur 7.8: IPv6 survey 2016 transitie (**Martinez2016**)



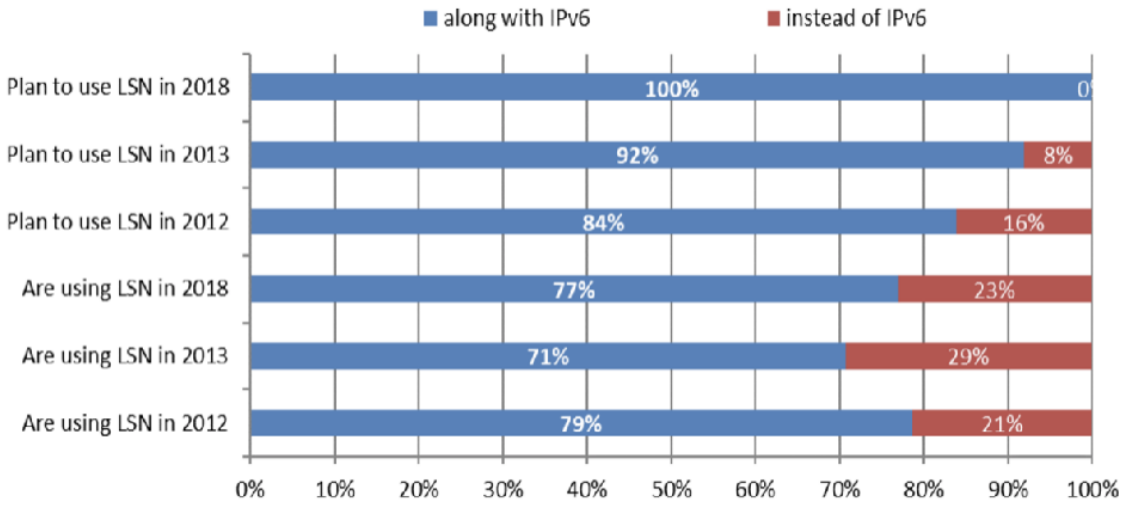
Figuur 7.9: IPv6 survey 2017 commercieel (**Martinez2017**)

al toe te wijzen en te verdelen.

Alweer zijn de transitie technieken onderzocht en geanalyseerd naar welke het meeste aanvaard en gebruikt worden. Volgens deze data gebruikt meer dan 50% geen transitie methode. Van diegene die wel deze technologie gebruiken kan er het volgende worden afgeleid. Op deze grafiek is er duidelijk te zien dat NAT64 een groot deel in beslag neemt en de populairste methode is. Daarnaast hebben DS-Lite en 6RD ook hun gebruikers maar bevatten deze een kleinere populariteit.

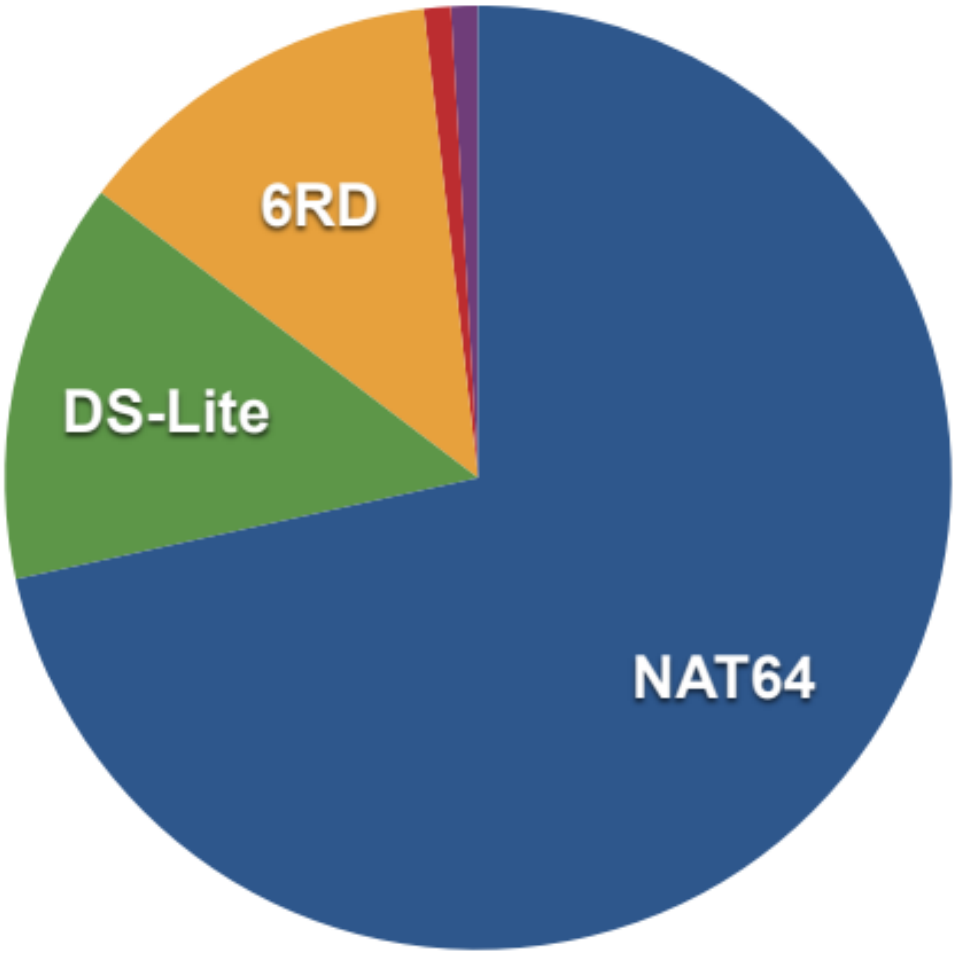
Ook is er iets interessant uitgehaald uit de verkregen data. Het gebruik maken van CGN (Carrier Grade NAT) of LSN (Large Scale NAT) samen of in plaats van IPv6. Met deze grafiek is er een zeer goed zicht op de toekomst van IPv6. In het jaar 2012 was er 16% dat koos om deze technologie, CGN/LSN, te gebruiken in de plaats van IPv6. Het jaar daarop was dit met de helft verminderd en momenteel in 2018 staat het aantal geplande op 0%. Dit is goed omdat men op deze manier gaat samenwerken met het IPv6 protocol en niet proberen deze te vervangen. Momenteel gebruiken er wel nog 23% van deelnemers CGN/LSN als vervanger van IPv6. Als we dit vergelijken met het jaar 2013 zien we een kleine daling wat het overschakelen van vervangen naar samen met verbeterd. De komende jaren mogen we dus zeker verwachten dat deze enkel maar gaat afnemen omdat de geplande vervanging 0% bevat.

Nu we weten hoe het al gaat met IPv6, blijven er toch velen achter en durven ze vaak de stap niet te zetten naar IPv6. Daarom was er een bepaalde vraag gesteld om te achterhalen



Figuur 7.10: IPv6 survey 2018 CGN/LSN (**Massimiliano2018**)

Figuur 7.11: IPv6 survey 2018 verdeling (**Massimiliano2018**)



Figuur 7.12: IPv6 survey 2018 transitie (**Massimiliano2018**)

waarom het ondersteunen van IPv6 niet direct gebruikt wordt. Hier kwam er als duidelijk antwoord dat de kennis, bijkomende kosten en het overbrengen naar niet technische afdelingen het moeilijk maakt om dit te volbrengen. Als deze antwoorden werden vergeleken met de jaren voordien dan ziet men dezelfde antwoorden steeds terugkomen. Daarom blijft er vaak de vraag waarom er nog steeds geen verandering volgde en wat men daaraan kan doen.

In het volgende hoofdstuk zal er vooral dieper ingegaan worden op de adoptie in België en hoe deze daar aan het evolueren is. Aan de hand van grafieken zal er een duidelijk overzicht gegeven worden over de huidige aanpak van IPv6 op de Belgische markt.

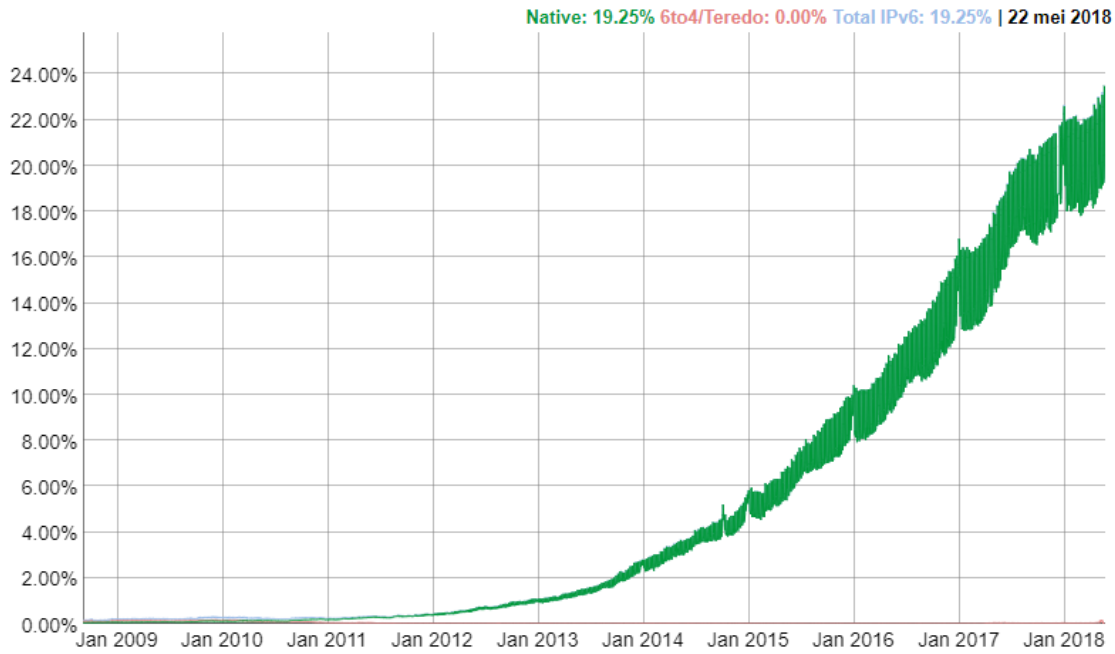
8. Belgische bedrijven en IPv6

8.1 IPv6 Adoptie

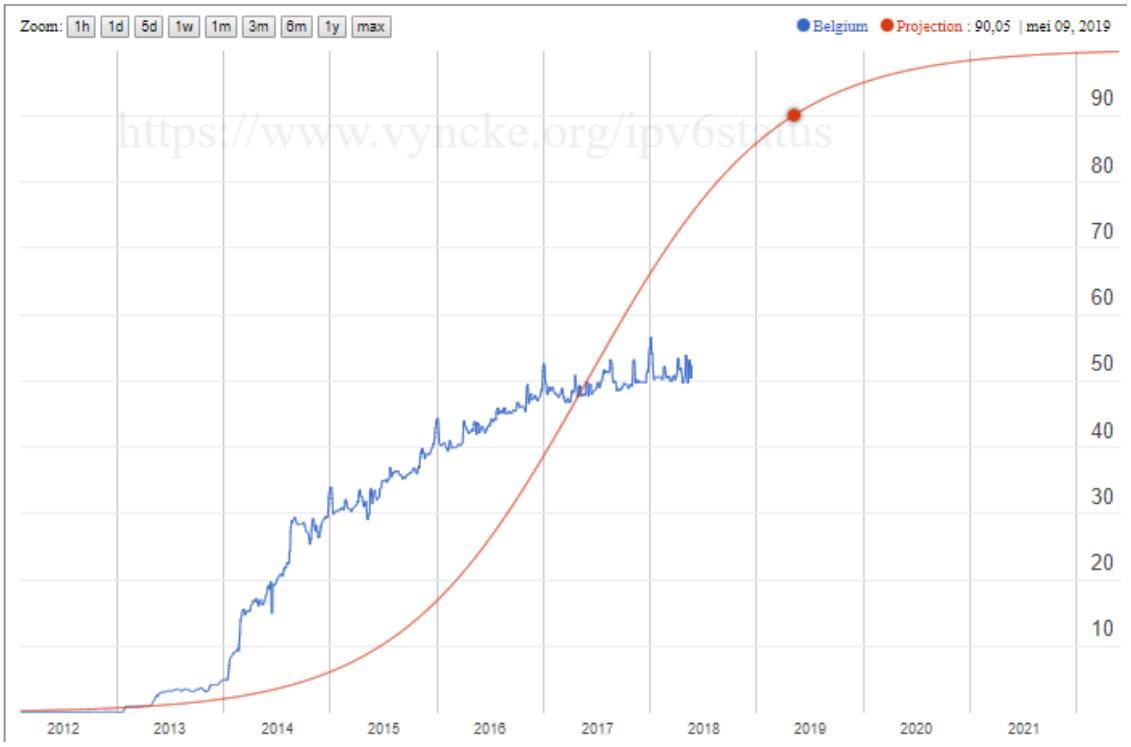
Op onderstaande afbeelding van Google is er te zien dat België momenteel een IPv6 adoptie heeft van 52.22%. Dit wil zeggen dat 52.22% van de gebruikers IPv6 connectie gebruikt om over Google te surfen. Dus meer dan de helft van het verkeer gaat over IPv6. Volgens de statistieken van Google is België het hoogste land met zoveel IPv6 connectiviteit. Hoe groener het land, hoe groter de adoptie. Terwijl het wereldwijde aantal maar 20.74% bevat. Dan heeft België meer dan het dubbele aantal dan het wereldwijde gebruik. Dit maakt België het land met het hoogste aantal IPv6 gebruikers van de wereld.

Nog belangrijk om na te gaan zijn de webbrowsers die IPv6 bereikbaar maken. Dit is een zeer belangrijk element en zeker voor de Belgische bedrijven. Omdat meer en meer gebruik wordt gemaakt van IPv6 en er vaak nog alleen IPv6 gebruikt wordt, is het belangrijk dat bedrijven zich hieraan gaan aanpassen. Als een website van een webshop enkel via IPv4 bereikbaar is dan kunnen de IPv6 klanten geen online shoppingen doen bij deze winkel. Hiervoor is het belangrijk dat bedrijven er zich van bewust zijn dat de webbrowsers zowel IPv4 als IPv6 toegankelijk moeten maken. In onderstaande grafiek is er te zien wat de status is van IPv6 toegankelijke webbrowsers en hoe de evolutie hiervan in de toekomst geschat kan worden. Om de evolutie hiervan te berekenen is er gebruik gemaakt van een logistische s-curve en een voorspelling op de komende 4 jaar of 1460 dagen. Op 26 mei waren er 52.27% van de sites IPv6 toegankelijk. Volgens de berekeningen zal de 90% behaald worden op 9 mei 2019, of minder dan 1 jaar zou er 90% van de Belgische webbrowsers IPv6 actief moeten zijn.

Het is alvast zeker dat België het beste presteert op het aantal gebruikers over IPv6. Nu rest er enkel nog de vraag waarom België meer gebruikers heeft dan eender welk land.



Figuur 8.1: IPv6 status IPv6 in België (**GoogleIPv6Belgie**)



Figuur 8.2: IPv6 vervolg op 4 jaar (**Vyncke2018**)

Voor deze vraag heeft Eric Vyncke, mede-eigenaar van de Belgische IPv6 Council, een mogelijk antwoord. Het biedt enkele mogelijkheden die een rol kunnen spelen waarom België zo'n hoog percentage behaald. De eerste mogelijkheid is er omdat België een vrij klein land is en dicht bevolkt. Omdat het land vrij klein is, is de afstand dus ook klein. Daarom wordt er ook vaak gebruik gemaakt van kabel of xDSL aansluitingen. Ook omdat veel van de Belgische ISP's een tekort hadden aan IPv4 adressen, was er snel een oplossing door gebruik te maken van IPv6. Ook is er een soort van geheim tussen de verschillende ISP's, cyberpolitie, regelgevers en de minister van economische zaken om het delen van 1 IPv4 adres maximum te beperken tot 16 abonnees. Dit had een grote invloed op het gebruik van NAT/CGN. Als de cultuur van België nader wordt bekeken dan is het een mix van zowel een Duitse als Latijnse cultuur. Dit wil ook zeggen dat er vaak gekeken wordt op een langere termijn en dat er niet veel wordt aangetrokken rond de processen. Ook hebben de drie grote ISP's van België samengezeten om het gebruik van IPv6 te verduidelijken. Hierbij hebben ze vooral ervaring en een routekaart met elkaar gedeeld om de evolutie te vergemakkelijken. Dit zijn enkele redenen volgens Eric Vyncke, waarbij hijzelf zegt dat er geen duidelijke reden hiervoor is en dit enkel maar veronderstellingen zijn.

8.2 Enquête aan Belgische bedrijven

Voor een breder beeld te krijgen over hoe het er in sommige bedrijven aan toe zijn, is er een enquête opgestuurd naar verschillende experten. De enquête en opgestelde vragen kan u terugvinden in de bijlagen om de corpus van de scriptie te bewaren. Deze vragen zijn vooral gericht op hoe het bedrijf er tegenover staat, IPv6. Het intern netwerk draaiende op IPv4, IPv6 of beiden. Hoe het zit met de kennis over IPv6, advies geven hiervan, begrippen herkennen en meer. Om de resultaten samen te vatten is er te merken dat er nog geen geval is van een IPv6 only intern netwerk. Zowel IPv4 als een IPv4/IPv6 structuur is al te vinden in een intern netwerk van bedrijven. Als er dan eerder de vraag werd gesteld of er toekomst plannen waren voor een mogelijke implementatie dan kwam er ook de respons dat ze er nog niet mee bezig waren en nog niet aan dachten om dit te implementeren in hun netwerk. Met de vraag of ze zouden kiezen voor een IPv4/IPv6 of een IPv6 structuur, dan kwam er een duidelijk antwoord dat ze allemaal voor gemengd kozen. Dit omdat men de overgang in een langzame beweging zouden volbrengen en omdat IPv4 nog steeds populair blijft. Alsook omdat niet al het apparatuur IPv6 compatibel is in vele gevallen. Er werd ook een bedrijf ondervraagd dat niet hoofdzakelijk met ICT diensten bezig is maar wel hun eigen afdeling heeft. Zij zouden voor deze overschakeling grotendeels gebruik maken van hun interne werkkracht maar zouden toch nog extra externe expertise raadplegen terwijl bij een IT consultancy bedrijf genoeg interne werkkracht heeft met de kennis van IPv6. Als er werd nagegaan over de kennis van IPv6, door het ondervragen van een begrip namelijk SLAAC, dan had niemand daar een probleem mee deze ook te beantwoorden. Wat wil leiden tot een beginkennis van IPv6. De voornaamste redenen om de overschakeling nog niet te beginnen is vooral door de complexiteit van de overgang en kennis van de engineers. Maar ook omdat sommige infrastructuren er nog niet klaar voor of nog niet compatibel hiermee zijn. Wat ook een reden was dat klanten geen nieuwe investeringen willen doen in de ICT infrastructuur en zeker nog niet met de start van GDPR (General Data Protection Regulation). Als ze zichzelf een score op 5 moeten geven dan scoort deze maximaal 2.5/5

voor kennis in IPv6. Dit toont nogmaals aan dat er te weinig opleidingen en opvolging is van het nieuwe internet protocol. Hierin zal in de toekomst meer geïnvesteerd moeten worden als men hiermee meer te maken zal hebben. Ook is er gevraagd geweest naar de toegankelijkheid van hun webbrowsers. We hebben zowel het antwoord ja als nee gekregen. Dit toont erop aan dat men toch rekening aan het houden is met de toegankelijkheid van hun sites. Ook bij degenen waarbij ze nog niet IPv6 actief zijn, blijft het antwoord dat het momenteel nog niet zo is, wat wil duiden op toekomstige plannen. De laatste vraag die besproken zal worden gaat over hoe ze in aanraking gekomen zijn met IPv6. We zien hierbij vooral dat er toch al trainingen en seminaries worden gevolgd. Alsook het behalen van certificaten en in contact komen met partners en datacenters. Ook bij de twee grootste Belgische IPS's, Telenet en Proximus, is het mogelijk om als klant gebruikt te maken van IPv6. Als men thuis een IPv6 verbinding wilt hebben dan bieden ze beiden ook een zeer goede ondersteuning hiervoor aan.

Een besluit die we hieruit kunnen trekken is dat er toch al bedrijven actief met IPv6 aan het werken zijn maar eerder gedeeld met IPv4. Dit maakt het ook beter om al een ruimere kennis op te doen. Ook is eruit af te leiden dat de kennis totaal nog niet op een hoog punt staat, maar dat er gezegd kan worden dat er trainingen gevolgd worden.

9. Conclusie

De conclusie die uit deze scriptie kan gehaald worden is dat men zowel op globaal als op Belgische vlak zeer sterk bezig is met de adoptie van IPv6. De meeste bedrijven, vooral ISP's, zijn er zich van bewust dat het werken met IPv6 een vereiste zal worden. Ook de afgelopen jaren was er een toenemende groei van het gebruik hiervan en zal de komende maanden en jaren alleen maar verbeteren. Hiervoor is het ook zeker belangrijk om de groei op een jaarlijkse basis goed bij te houden zodanig men dit als motivatie voor bedrijven kan gebruiken. Ook is België het beste land met het aantal gebruikers die IPv6 hanteren wat een totale verrassing is voor vele Belgen.

Alsook biedt deze scriptie enkele antwoorden op de onderzoeksvragen. Er is een duidelijk overzicht van hoe de adoptie en aanvaarding van IPv6 staat op globaal niveau. Volgens Google stond deze op 23.33% op 26 mei 2018. Wat het toch al meer dan 1/5 van al het verkeer maakt. Na 7 jaar sinds de eerste IPv6 wereld dag kan men dit zeker niet slecht noemen. Als er nog een duidelijker zicht wilt gegeven worden is het nodig om per land zijn evolutie te gaan bekijken.

Om enkele antwoorden te bieden op de onderzoeksvragen omtrent de evolutie op Belgisch niveau, dan kunnen we zeggen dat België het beter doet dan verwacht. Zoals eerder vernoemd, scoort België het beste op vlak van IPv6 gebruikers over heel de wereld wat het zeer interessant maakt. Om hierover een duidelijke verklaring te geven is moeilijk maar de gegeven veronderstellingen van Eric Vyncke kunnen hier zeker een invloed op hebben. Er kan ook afgeleid worden uit de enquêtes dat er toch al aan IPv6 gedacht wordt en dat hiermee al effectief in een werkomgeving mee geëxperimenteerd wordt. Alsook kan er geconcludeerd worden dat er nog veel groeipotentieel is naargelang het gebruik maken van IPv6 en dan niet zo gericht op de implementatie. Enkele hoofdredenen waarom bij de meeste bedrijven nog niet een implementatie is doorgekomen is vooral het gebrek aan

kennis van het protocol. De noodzaak is dat bedrijven extra investeringen moeten doen omtrent trainingen, cursussen, certificatie en seminaries. Er kan ook gezegd worden dat de overgang van IPv4 naar IPv6 niet op één dag kan gebeuren maar dat dit vooral veel tijd, werk en planning in beslag neemt. Er wordt dus ook een IPv4/IPv6 verkozen in plaats van een IPv6 only netwerk. Wat vooral te maken kan hebben met de comptabiliteit van de apparaten in de infrastuur als met de kennis die engineers momenteel hebben over het protocol.

Er wacht IPv6 een veelbelovende toekomst te wachten waaraan bedrijven zich meer en meer bewust van beginnen te worden dat het hoe dan ook een vereiste is om hiermee in aanraking te komen.

A. Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

A.1 Introductie

Mijn onderzoek zal gaan naar hoe de overschakeling binnen bedrijven van IPv4 (Internet Protocol version 4) naar IPv6 (Internet Protocol version 6) verloopt. Zijn de bedrijven in hun netwerk bezig naar het overschakelen naar het vernieuwde internet protocol, die noodzakelijk was binnen het internet, of ze het van plan of hebben ze er helemaal nog niet bij stilgestaan. Om dit onderzoek tot een succes uit te voeren, zal ik gebruik maken van een enquête en de antwoorden doorgronden of deze al dan niet terechte opmerkingen zijn.

A.2 State-of-the-art

Deze scriptie zal gaan over de huidige stand van zaken van de adoptie van IPv6 op zowel globaal niveau als op Belgisch niveau. Er zal een studie uitgevoerd worden en enquêtes onderzocht worden. Dit dient ervoor om het standpunt van een bedrijf naar boven te brengen en de verkregen resultaten te doorgronden.

A.3 Methodologie

Om mijn onderzoek uit te voeren zal ik gebruik maken van vragenlijsten. Hierdoor zullen mijn onderzoeksvragen beantwoord worden en is er een duidelijk overzicht over het gebeuren binnen een netwerk van een bedrijf. Aan de hand van deze antwoorden kan er gekeken worden of deze al dan niet doorgrond zijn en of deze terechte antwoorden zijn. Ook zullen er veel data van enquêtes overlopen worden en geanalyseerd. Deze zullen steeds grafisch voorgesteld worden in grafieken.

A.4 Verwachte resultaten

De verwachte resultaten zijn dat men ziet dat enkele bedrijven al rekening houden met de overstapping naar het vernieuwde internet protocol IPv6. Ook zal het aantal niet immens groot zijn en zeker onder de helft van het aantal ondervragen bedrijven zitten. Alsook dat nog niemand de grootste stap richting de overgang heeft gemaakt en zeker niet volledig het IPv6 protocol zal hanteren maar eerder samen met IPv4.

A.5 Verwachte conclusies

Mijn verwachtingen zijn dus dat er van geen enkel van de ondervraagde bedrijven een bedrijf is waarin ze volledig IPv6 zullen hanteren. Ik vermoed ook dat uit het onderzoek zal blijken dat er toch enkele bedrijven er zich van bewust zijn en toch de stap aan het maken zijn voor eerder een gemengde oplossing te gebruiken, dus IPv4 en IPv6 samen. Maar het grootste deel zal zeker nog niet in de richting gaan van een mogelijke implementatie van het protocol.