TNO Informatie- en Communicatietechnologie

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek / Netherlands Organisation for Applied Scientific Research

Brassersplein 2
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 15 285 70 00
F +31 15 285 70 57
info-ict@tno.nl

TNO-whitepaper

35334

IPv6 Monitoring in Nederland: De Nulmeting

Datum	21 juni 2010
Auteur(s)	Maria Boen-Leo, Arjen Holtzer, Martin Tijmes, Rob Smets
Exemplaarnummer	
Oplage	
Aantal pagina's	27
Aantal bijlagen	
Opdrachtgever	Ministerie van Economische Zaken
Projectnaam	IPv6 Monitoring in Nederland
Projectnummer	035.33445

Inhoudsopgave

1 Managementuittreksel

Het internet is voor Nederland van vitaal belang. Het opraken van de adressen die nodig zijn voor het huidige op IPv4 gebaseerde internet wordt ondervangen door het introduceren van IPv6. IPv6 is echter niet verenigbaar met IPv4 waardoor het van belang is dat tijdige migratie plaatsvindt van IPv4 naar IPv6.

Dit document geeft het eerste inzicht (nulmeting) in de mate waarin in Nederland migratie naar IPv6 plaatsvindt in relatie tot ons omringende landen. Bij deze nulmeting wordt gekeken naar parameters die een duidelijke indicator zijn voor de voorbereidingen die getroffen kunnen worden, maar ook naar parameters die indicatief zijn voor de daadwerkelijke uitrol van IPv6.

Nederland mee in de voorhoede als het gaat om voorbereidingen voor de uitrol van IPv6. Nederland presteert gemiddeld als het gaat om de daadwerkelijke uitrol van IPv6. Het is bij deze nulmeting nog onvoldoende duidelijk of dit betekent dat organisaties voldoende actie hebben ondernomen om geen last te ondervinden van het opraken van de IPv4 adressen. Voor Nederland bestaan twee punten van zorg. Het eerste punt is de beschikbaarheid van IPv6 verbindingen voor eindgebruikers. Het zijn op dit moment vooral de kleine ISP’s die IPv6 hebben ingevoerd en aanbieden aan zakelijke klanten. Veel grotere ISP’s zijn hier nog niet klaar voor. Het tweede punt is de beschikbaarheid van content op en diensten over IPv6.

Omdat standaardisatie een belangrijke bijdrage kan leveren aan het introduceren van IPv6 is een aantal standaardisatieactiviteiten in kaart gebracht. IPv6 standaarden zijn sinds de jaren 90 beschikbaar. Door onder andere de standaardisatieorganisaties 3GPP en het Broadband Forum worden in overleg tussen leveranciers van telecommunicatieapparatuur, netwerkoperatoren en serviceproviders de juiste standaarden beschreven die in producten, netwerken en diensten geïmplementeerd moeten worden. Deze activiteiten vindt op dit moment plaats en moet er toe leiden dat IPv6 verbindingen over ongeveer een jaar op grote schaal aangeboden kunnen gaan worden aan eindgebruikers.

Wat betreft veiligheid is IPv6 niet kwetsbaarder dan IPv4. De gerapporteerde IPv6 gerelateerde kwetsbaarheden lijken meer impact te hebben dan die van IPv4 op het gebied van de ernst van de kwetsbaarheid en frequentie waarmee deze terug te vinden zijn in producten. Echter, het aantal gerapporteerde kwetsbaarheden is laag vergeleken met IPv4 en neemt jaarlijks af. Het is van belang deze trend nauwlettend in de gaten te houden omdat naar verwachting meer IPv6 apparatuur op de markt zal verschijnen.

Uitrol van IPv6 kan versneld worden door gericht te sturen op het aanbieden van IPv6 verbindingen aan eindgebruikers en het beschikbaar maken van content op het IPv6 internet.
Zowel de veiligheid van IPv6 als de implementatie van de standaarden dient bewaakt te worden om de uitrol van IPv6 niet te vertragen.

Of de ontwikkelingen in de toekomst snel genoeg gaan om goed voorbereid te zijn op de uitputting van IPv4 adressen zal in een beter perspectief geplaatst kunnen worden als over een half jaar een tweede meting is uitgevoerd inzake de uitrol van IPv6 in Nederland.

2 Inleiding

Internet is een vitaal deel van de maatschappij geworden. Het is uitgegroeid tot hét platform voor burgers, bedrijven, en de overheid zowel in Nederland als in de rest van de wereld.

De voortschrijdende groei van het Internet vraagt om de uitgifte van meer en meer IP adressen. Deze adressen raken hierdoor in een snel tempo op. Zonder IP adres is geen gebruik van het Internet mogelijk.

De opvolger van het huidige Internet Protocol versie 4 (IPv4), versie 6 (IPv6), lost dit probleem op doordat door de introductie van IPv6 veel meer IP adressen beschikbaar komen. Ter vergelijking: IPv6 ondersteunt een aantal adressen dat gelijk is aan ongeveer 1.000.000 keer het aantal liters water in alle wereld oceanen, terwijl IPv4 slechts een aantal adressen ondersteunt dat ongeveer gelijk is aan het aantal liters water in het IJsselmeer.

Het opraken van de IP adressen is een wereldwijd probleem. Doordat alle landen in de wereld uit dezelfde adresvoorraad putten, zal de overgang van IPv4 naar IPv6 voor iedereen van belang zijn, en heeft iedereen er belang bij dat deze overgang zo soepel mogelijk verloopt. Indien IPv6 niet op de juiste manier wordt geadopteerd, zullen burgers, bedrijven en overheden binnen en buiten Nederland hinder en mogelijke economische schade ondervinden. Zonder technische maatregelen is IPv6 niet verenigbaar met IPv4.

Het is van belang in kaart te brengen hoe de uitrol van IPv6 in Nederland voortschrijdt, ook in vergelijking met landen om ons heen, en in welke mate er hindernissen zijn die de adoptie van IPv6 vertragen. Dit geeft aan welke stakeholders belangrijk zijn bij IPv6 en of deze stakeholders zich voldoende met IPv6 bezighouden om te voorkomen dat Nederland nadelige gevolgen ondervindt van het opraken van de IPv4 adressen.

Dit whitepaper geeft inzicht in deze voortgang en belemmeringen op basis waarvan maatregelen genomen kunnen worden of juist achterwege kunnen blijven. Deze informatie dient niet alleen de overheid, maar is ook nuttig voor burgers en bedrijven.
Door monitoring van parameters ondergebracht in vier categorieën zal dit inzicht verkregen worden.
Deze vier monitoring categorieën zijn:

- Parameters die een maat zijn voor de wereldwijde adoptie van IPv6.
- Indicatoren van de mate waarin Nederland IPv6 heeft uitgerold in verhouding tot een aantal omringende landen.
- Ontwikkelingen op het gebied van standaardisatie en technologische ontwikkelingen.
- Veiligheid van IPv6 in relatie tot IPv4.

Er zal twee keer gemeten worden om inzicht te krijgen in de mate waarin de uitrol van IPv6 zich ontwikkeld. Dit whitepaper beschrijft de stand van zaken rond april 2010, een nulmeting. Na ongeveer een halfjaar zal een tweede whitepaper opgesteld worden.
Verschillen met de nulmeting zullen geanalyseerd worden zodat duidelijk wordt op welke onderdelen de adoptie van IPv6 veranderd is.

3 Van IPv4 naar IPv6

3.1 Inleiding

Als er geen nieuwe beschikbare IPv4 adressen meer zijn, zullen nieuwe aansluitingen alleen een IPv6 adres krijgen en geen IPv4 adres. Deze nieuwe aansluitingen zullen niet de mogelijkheid hebben om direct te communiceren met eindgebruikers die geen IPv6 adres hebben of websites kunnen bereiken die geen IPv6 ondersteunen.

De benodigde snelheid van adoptie van IPv6, ofwel de urgentie van migratie, is afhankelijk van de leegloop van de IPv4 adresvoorraden. Dit kunnen we karakteriseren als de consumptie van IPv4 adressen.

Op dit moment zijn er verscheidene initiatieven om de adoptie van IPv6 te bevorderen, zoals de IPv6 TaskForce[1]. Inmiddels zijn ook op verschillende plekken in de wereld al de eerste IPv6 netwerken uitgerold, waarbij particulieren en bedrijven een IPv6 aansluiting kunnen verkrijgen. Maar hoe staat het nu echt met de adoptie van IPv6 en dragen deze initiatieven significant bij aan de adoptie?

Om op een juiste manier inzicht te krijgen in de problematiek rondom het opraken van de IP adressen wordt in de volgende sectie enige achtergrond informatie gegeven worden om een juist kader te kunnen vormen. Vervolgens zal de nulmeting behandeld worden waarbij parameters die een indicatie zijn voor de adoptie van IPv6 worden besproken.

3.2 Achtergrond

In deze paragraaf zal allereerst ingegaan worden op het uitgifte proces van IP adressen. Vervolgens zal het belang voor Nederland besproken worden, evenals de stuwende kracht voor de alsmaar groeiende benodigde hoeveelheid IP adressen. Hierna wordt ingegaan op de opbouw van het IPv6 adres, en het verschil in uitgifte vergeleken met IPv4. Als laatste wordt de ISP als stakeholder aangehaald.

3.2.1 Het uitgifte proces van IP adressen

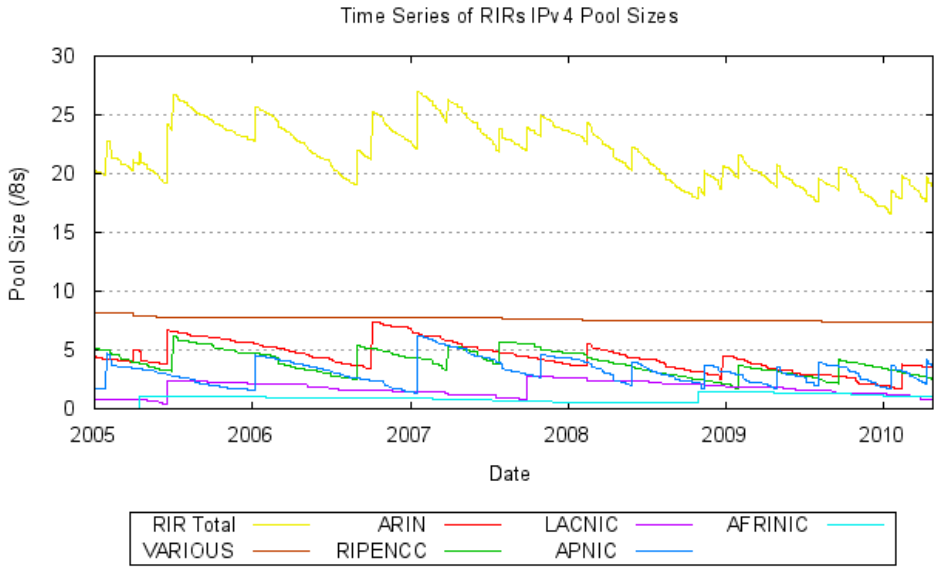
De wereldwijde coördinatie van de uitgifte van IP adressen wordt gedaan door de Internet Assigned Numbers Authority (IANA). IANA gaat zowel over de uitgifte van IPv4 als IPv6 adressen. De locale distributie van IP adressen wordt bewerkstelligd door Regional Internet Registries (RIR's), welke elk een bepaald deel van de wereld bedienen. Een overzicht van de RIR's en hun toegewezen deel van de wereld wordt gegeven in Figuur 1.

Elke RIR kan een aanvraag doen naar een reeks IP adressen en deze vervolgens uitgeven aan een Local Internet Registry (LIR). Een typisch voorbeeld van een LIR is een ISP, maar kan ook een bedrijf of een gemeente zijn.

[1] http://www.ipv6-taskforce.nl/

Figuur 1: De Regional Internet Registries (RIR's), en hun bedieninggebied

In Figuur 2 is voor de afgelopen vijf jaar te zien dat elk van de RIR's een eigen voorraad heeft tussen de 0 en 5 /8's[2] waaruit zij IPv4 adressen toewijzen aan LIR's. Op het moment dat hun eigen voorraad leeg dreigt te raken doen ze een aanvraag bij IANA voor nieuwe adressen.



Figuur 2: De IPv4 adresvoorraad (gemeten in /8's) van de RIR's (bron: potarooo.net)

3.2.2 Het gebruik en belang van IP adressen in Nederland

In de totale adresruimte van IPv4 adressen zitten ongeveer 4,3 miljard adressen (2^{32}). Ruim 13,5% van de adresruimte is gereserveerd, voor onder andere experimenteel en lokaal gebruik. Het restant, ongeveer 3,7 miljard adressen, is beschikbaar voor uitgifte. Nederland heeft tot 31-12-2009 in totaal 23 miljoen IPv4 adressen toegewezen gekregen en zal in de toekomst nog vele IP adressen meer gaan gebruiken.

Met de invoering van IPv4 had men niet kunnen voorzien dat het Internet in de afgelopen 25 jaar zo'n vlucht heeft genomen. Sinds begin jaren negentig speelt het

[2] Een /8 representeert een gedeelte van de adresruimte, waarbij de eerste 8 acht bits van het IPv4 adres gegeven zijn, en met de resterende 24 bits alle mogelijke combinaties gemaakt kunnen worden.

bewustzijn dat de beschikbare IPv4 adressen vroeg of laat op zullen raken. De daadwerkelijke leegloop van de IPv4 adresvoorraad is door een divers aantal methodes enigszins uitgesteld.[3]

Nederland is koploper in de Europese Unie op het gebied van computerbezit en het aantal huishoudens met internet. In 2008 beschikte 88% van de Nederlandse huishoudens[4] over een computer. Ook in Zweden, Denemarken, Luxemburg en Duitsland lag dit aandeel boven de 80%, terwijl het Europese gemiddelde 68% was. Er is een sterke samenhang tussen computerbezit en de aanwezigheid van internet. In 2008 had 86% van alle huishoudens in Nederland toegang tot internet, en is in 2009 gegroeid tot 90%. In 2009 waren er nog zo'n 900 duizend personen zonder toegang tot internet. Voor het merendeel (69%) van deze personen[5] geldt dat zij een internetaansluiting niet zinvol vindt, er geen interesse in heeft, of het eenvoudigweg niet wil.

In steeds minder huishoudens is een desktopcomputer met internettoegang aanwezig. Deze ontwikkeling is toe te schrijven aan de stormachtige opkomst van de laptop. In 2009 is in 83% van de huishoudens een desktop beschikbaar voor toegang tot internet, en in 62% van de huishoudens wordt een laptop gebruikt. Naast de laptop wordt de mobiele telefoon steeds meer gebruikt om toegang tot het internet te verkrijgen. In 2009 maakt 15% van de internetgebruikers gebruik van zijn mobiele telefoon om te internetten, waar dat in 2008 en 2007 nog respectievelijk 10% en 8% was. De huidige groei in het gebruik van IP adressen wordt voornamelijk gedreven door mobiele toepassingen, met de opkomst van internettoegang op mobiele apparaten zoals bijvoorbeeld Apple's iPhone en Google's Android platform.

Tabel 1: Overzicht met het aantal breedband internet- en mobiele telefoonaansluitingen (in miljoenen) in Nederland.

	2004	**2006**	**2008**
Breedband[6] internetaansluitingen	3,09	5,23	5,74
Mobiele telefoonaansluitingen	15,90	17,00	19,80
Totaal aantal aansluitingen	18,99	22,23	25,54

In Tabel 1 is een overzicht gegeven van de internet- en mobiele telefoonaansluitingen in Nederland. Het aantal breedbandige internetaansluitingen nadert het aantal huishoudens en is als gevolg daarvan afgenomen in groei. Het aantal mobiele aansluitingen is tussen 2004 en 2008 gestaag gegroeid. Een aantal van 19,80 miljoen mobiele aansluitingen betekent dat in 2008 elke inwoner gemiddeld 1,2 mobiele telefoonaansluitingen heeft. In 2009 gebruikte 15% van de internetgebruikers zijn telefoon om te internetten, waar dat in 2008 nog 10% was en in de toekomst zal dit nog verder zal groeien. Tezamen met de groei in mobiele aansluitingen zal het IP gebruik in de komende jaren blijven toenemen. Door de eindige schaalbaarheid van het nu nog veel gebruikte NAT zullen de mogelijkheden met IPv4 uiteindelijk niet toereikend zijn. Hierdoor is de transitie naar

[3] Met de invoering van CIDR (Classless Inter-Domain Routing) in 1993 wordt de totale adresruimte efficienter benut. Het gebruik van NAT (Network Address Translation) zorgt ervoor dat meerdere eindgebruikers met één of meerdere IP adressen toegang tot Internet verkrijgen. En de teruggave van bepaalde IP adresreeksen door bedrijven aan de IANA heeft ervoor gezorgd dat ongebruikte adresreeksen opnieuw toegewezen kunnen worden. Deze methodes zijn echter slechts een vertraging in de daadwerkelijke uitputting van de IPv4 adressen, welke uiteindelijk onvermijdelijk is.

[4] Het totaal aantal huishoudens in Nederland in 2009 is ongeveer 6,6 miljoen.

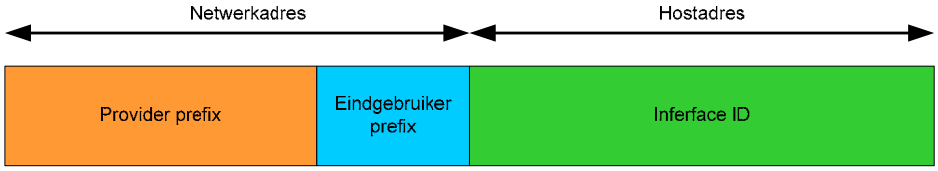
[5] Personen in de leeftijd van 12 tot 74 jaar.

[6] Breedband verbindingen zijn verbindingen met het internet met een totale transmissiecapaciteit van minstens 256 Kbps.

IPv6 zeer relevant voor Nederland en is het belangrijk om de ontwikkelingen omtrent de adoptie van IPv6 scherp in de gaten te houden

3.2.3 IPv6 adressen

Het belangrijkste voordeel van IPv6 ten opzichte van IPv4 is de grotere adresruimte. In tegenstelling tot de 32 bits van een IPv4 adres, bestaat een IPv6 adres uit 128 bits. De IPv6 adresruimte is weergegeven in Figuur 3. De eerste 64 bits worden gebruikt voor het netwerkadres en de laatste 64 bits voor het hostadres. Een eindgebruiker zal een compleet netwerkadres aangeboden krijgen, waarbij de eindgebruiker het hostadres bepaalt op basis van het MAC adres of een ander mechanisme.



Figuur 3: IPv6 adresstructuur. Het netwerkgedeelte van het IPv6 adres bestaat uit provider prefix en een eindgebruiker prefix. Het hostadres wordt ook wel aangegeven met de interface ID.

Doordat per netwerkadres nog 2^{64} hostadressen beschikbaar zijn zal de daadwerkelijke utilisatie van de totale adresruimte van IPv6 uiteindelijk laag zijn. Echter, met het kiezen voor deze opzet wordt implementatie van de automatische adresconfiguratie[7] versimpeld. Daarbij zullen door de inherente structuur van grote subnetten en subnet aggregatie het netwerkmanagement en de routering meer efficiënt zijn. Verder bouwen RIR's ruimte in bij de adresuitgifte, zodat toegewezen adresblokken in de toekomst uitgebreid kunnen worden met een aangrenzend adresblok. Hierdoor blijft het mogelijk om het nieuwe en oude adresblok gezamenlijk als één prefix richting het internet te adverteren, waardoor de omvang van BGP routeringstabel zoveel mogelijk beperkt blijft.

Normaal gesproken zal een ISP aanspraak maken op één of meerdere /32's. De ISP geeft vervolgens een /48 uit aan haar klanten met een vaste aansluiting. Deze /48 kan gezien worden als de provider prefix, zoals aangegeven in Figuur 3. Dit betekent dat hiermee de eerste 48 bits van het IPv6 adres vast staan. Met de resterende bits in het netwerkadres, de eindgebruiker prefix, kunnen door de klant nog verschillende subnetten gemaakt worden. In de praktijk kan het voorkomen dat ISP's ook /56's uitgeven in plaats van /48's. Voor mobiele telefoons worden in het normale geval /64's uitgegeven.

3.2.4 ISP's als stakeholder

Bij de adoptie van IPv6 spelen ISP's een belangrijke rol als stakeholder en worden daarom ook meegenomen in dit onderzoek. Ook in andere survey's is de adoptie van IPv6 door ISP's op bepaalde vlakken al onderzocht. In het project *IPv6 Deployment Monitoring* voor de Europese Commissie[8] heeft TNO, in samenwerking met GNKS, een enquête uitgezet via de RIR's Ripe NCC en APNIC.

Uit deze enquête blijkt dat de belangrijkste reden voor ISP's om actief IPv6 te adopteren, is het voorbereid willen zijn op het opraken van IPv4 adressen. Er zijn echter

[7] Stateless Address Autoconfiguration, in tegenstelling tot statefull address configuration waarbij een DHCP server benodigd is om een IP adres toe te wijzen aan de eindgebruiker.

[8] Meer informatie over het IPv6 Deployment Monitoring project kan gevonden worden op: http://www.ipv6monitoring.eu/

nog een groot aantal kwesties waarvan ISP's aangegeven hebben ze als bottleneck voor de uitrol te ervaren[9]. De belangrijkste bottlenecks zijn:

- Men heeft geen idee hoe te migreren van IPv4 naar IPv6.
- IPv4-IPv6 translatie mechanismes zijn nog niet gestandaardiseerd, waardoor het te vroeg is om IPv6 te adopteren.
- Doordat er geen compatibiliteit is tussen IPv6 met IPv4, weet men niet hoe het nieuwe IPv6 netwerk moet gaan communiceren met IPv4 systemen.
- Beveiligingsmaatregelen (zoals firewalls, …) voor IPv6 zijn nog niet beschikbaar of bieden nog niet dezelfde functionaliteit als IPv4 producten.
- De beveiliging in IPv6 is nog niet zo volwassen als IPv4, waardoor de betrouwbaarheid van het netwerk lager kan zijn.
- Het gebruik van zowel IPv4 als IPv6 maakt de organisatie dubbel zo kwetsbaar door problemen met beide protocollen.
- De markt van IPv6 producten is niet transparant, waardoor men niet weet welke producten benodigd zijn voor een specifieke situatie zonder te gaan experimenteren.

Ondanks dat er op dit moment nog maar weinig vraag is naar IPv6 zouden ISP's wel moeten werken aan een roadmap voor IPv6, als ze dit nog niet gedaan hebben. Men dient in het achterhoofd te houden, dat als straks de IPv4 adressen op zijn klanten een manier zullen eisen om toch toegang tot het hele internet te krijgen, ofwel ook de eindgebruikers en websites die alleen over IPv6 te bereiken zijn. Dit kan door middel van een 'native' IPv6 aansluiting, maar kan ook bereikt worden door middel van tunneling[10].

[9] IPv6 Deployment Monitoring Study Report (http://www.ipv6monitoring.eu/project-files?func=startdown&id=9)

[10] Native wil zeggen over een daadwerkelijk IPv6 netwerk en getunneld wil zeggen over een IPv4 toegangsnetwerk.

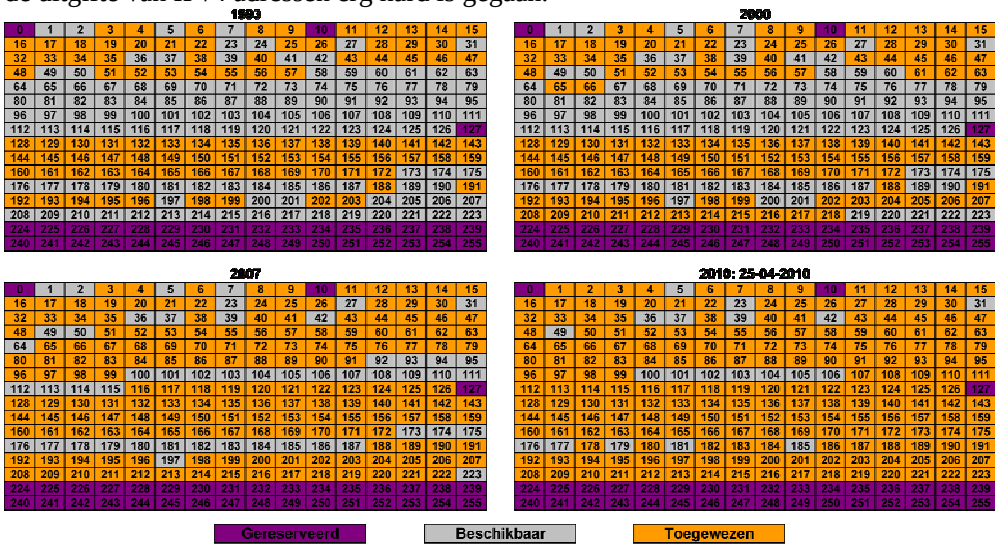
3.3 De nulmeting

Om de ontwikkelingen omtrent IPv6 goed in kaart te brengen zal tweemaal een meting worden uitgevoerd. In deze sectie zullen voor de nulmeting de parameters besproken worden die inzicht geven in de wereldwijde adoptie van IPv6 en die uitrol van IPv6 binnen Nederland. Allereerst zal gekeken worden naar de IPv4 adresvoorraad om de urgentie van IPv6 te kunnen bepalen. Daarna zal de uitrol van IPv6 besproken worden.

3.3.1 Leegloop IANA adresvoorraad en uitgifte IPv4 adressen

Wereldwijd

In de afgelopen jaren is de uitgifte van IPv4 adressen exponentieel gegroeid. In Figuur 4 zijn voor vier tijdsmomenten de toegewezen /8's weergegeven in beeldvorm (de IPv4 adresruimte kent 256 /8 adresblokken). Het is duidelijk te zien dat in de laatste tien jaar de uitgifte van IPv4 adressen erg hard is gegaan.



Figuur 4: De leegloop van de IPv4 adresvoorraad bij IANA, in vier verschillende tijdsvakken. De totale adresruimte bestaat uit 256 /8's. In elke tabel zijn de /8's grafisch weergegeven. De tabel rechtsonder geeft de stand van zaken per 25-04-2010 weer. Er nog 7% van de adressen (/8's) beschikbaar voor uitgifte.

Uit Figuur 4 valt op te maken dat er nog ongeveer 7% van de IPv4 adressen beschikbaar zijn voor uitgifte. Er zijn verschillende voorspellingen over de consumptiesnelheid van IPv4 adressen en wanneer de adressen allemaal uitgegeven zijn. De meest geaccepteerde voorspellingen zijn van Geoff Huston, een senior onderzoeker die nauw betrokken is geweest bij de ontwikkelingen van het Internet, en lid is van de uitvoeringscommissie van de RIR APNIC. Op zijn blog[11] houdt hij verschillende ontwikkelingen en statistieken bij. Hij voorspelt dat als de huidige trend van adres consumptie zich voortzet, er vanaf 30 september 2011[12] geen IPv4 adressen door IANA meer uitgegeven kunnen worden. Naar verwachting zal de eerste RIR zal ongeveer een jaar later, november 2012, al zijn adressen hebben toegewezen.

[11] http://www.potaroo.net/
[12] Gemeten op 1 april 2010

Tabel 2: Het aantal toegewezen IPv4 adressen (in miljoenen /32's)

	2005	2006	2007	2008	2009
Toegewezen adressen wereldwijd	174,5	168,5	206,4	203,8	190,1
Relatieve groei wereldwijd	8,0%	7,7%	8,8%	8,0%	6,9%
Toegewezen adressen Nederland	2,12	1,72	1,87	0,91	2,08
Relatieve groei Nederland	14,9%	10,1%	10,3%	4,6%	10,0%

Na een groei in uitgifte van IPv4 adressen in 2007, is de afgelopen twee jaar het aantal uitgegeven adressen steeds afgenomen. Zie Tabel 2. Deze afname wordt voornamelijk veroorzaakt door een lagere toewijzing aan landen die door de Ripe NCC bediend worden. Ook is er in Noord-Amerika (ARIN) in 2009 een duidelijke afname te zien. In Zuid-Oost Azië, en dan voornamelijk China, is er juist een sterke groei te zien in de consumptie van IP adressen. In 2009 werd bijna de helft (46%) van de toegewezen adressen door alle RIR's uitgegeven door de APNIC, zoals aangegeven in Tabel 3. Door deze vertraging in het uitgifte proces is de uitputtingsdatum ook wat opgeschoven. Aan het begin van 2009 was de voorspelde datum nog april 2011, en in lijn met de huidige uitgiftesnelheid is deze datum 6 maanden opgeschoven naar eind september 2011, zoals eerder genoemd.

Tabel 3: IPv4 adres uitgifte, verdeling onder de RIR's

	2005	2006	2007	2008	2009
RipeNCC	35%	33%	31%	22%	23%
ARIN	27%	28%	26%	28%	22%
APNIC	31%	31%	34%	44%	46%
LACNIC	6%	7%	7%	6%	6%
AfriNIC	1%	2%	3%	1%	3%

Nederland

Als het aantal toegewezen IPv4 adressen wereldwijd vergeleken wordt met Nederland, dan is te zien dat er binnen Nederland nog steeds een sterke behoefte is aan nieuwe IP adressen. Uit Tabel 2 blijkt dat Nederland in 2009 ongeveer 2 miljoen adressen toegewezen heeft gekregen. Het totale aantal IPv4 adressen dat Nederland t/m 2009 heeft aangevraagd komt daarmee op 23 miljoen. Ook in de toekomst zal de vraag naar IP adressen doorzetten.

3.3.2 De adoptie van IPv6

3.3.2.1 Uitgifte IPv6

Wereldwijd

De uitgifte van IPv6 adresblokken is gaande sinds 1999. Een overzicht van de huidige toewijzingen zijn te vinden in Tabel 4. In de afgelopen jaren hebben een aantal grote toewijzingen de adres allocaties gedomineerd. In 2007 werd er een enkel groot blok (2401:6000::/20) toegewezen aan het Ministerie van Defensie van Australië (268,44 miljoen /48's). In 2008 is er een grote toewijzing gedaan aan het Braziliaanse Comité Gestor da Internet no Brasil (2804::/16, 1073,74 miljoen /48's), en een grote toewijzing aan het Ministerie van Defensie van de VS.

Tabel 4: Totale aantal toegekende en geadverteerde IPv6 /48's (in miljoenen) op 31-12-2009

	Amerika	Europa	Azië	Afrika	Oceanië
Gealloceerd	5316,1	2243,1	1079,7	4,1	549,5
Geadverteerd	33,8	2132,0	773,8	1,6	272,6

Tabel 5: Aantal individuele IPv6 toewijzingen (ongeacht adresblokomvang) bij de Regional Internet Registries (RIR's)

	2005	2006	2007	2008	2009
RipeNCC	98	94	164	439	642
ARIN	59	71	218	235	396
APNIC	54	43	63	163	194
LACNIC	31	16	27	31	35
AfriNIC	3	19	20	18	14

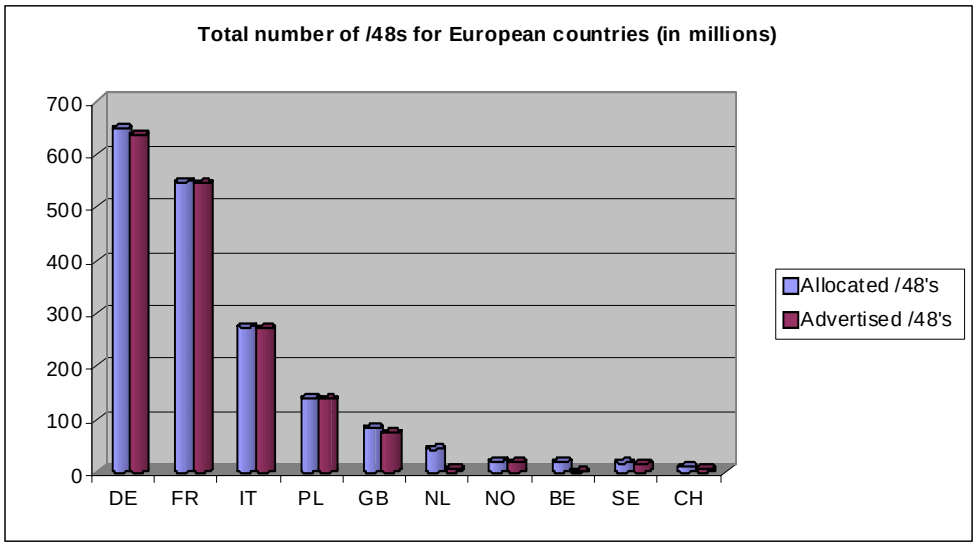
Het valt op te merken dat de huidige uitrol van IPv6 vooral plaatsvindt in de meer volwassen internetmarkten zoals West-Europa en Noord-Amerika, waar veel landen een hoge internet penetratie hebben. Dit is ook terug te zien in Tabel 5 waar een duidelijk onderscheid is te zien in het aantal aanvragen, waarbij de Ripe NCC en ARIN voorop lopen. De afname in IPv4 allocaties en toename van IPv6 allocaties in deze RIR's geven een duidelijke uitrol aan, alsmede een bewustwording van de voorbereidingen van de uitrol van IPv6 door de aanvraag van IPv6 adresreeksen om deze uit te kunnen geven aan klanten.

Nederland

In Tabel 6 is te zien dat in 2009 er door Nederland 3 miljoen IPv6 /48's zijn aangevraagd, in vergelijking tot 2 miljoen IPv4-adressen. Hierbij moet worden opgemerkt dat door de manier van toewijzing al snel zeer grote blokken worden uitgegeven, zoals eerder aangegeven. Als er vervolgens gekeken wordt naar het percentage van de adressen die worden geadverteerd in de routeringstabellen dan is dit nog maar 13,65%. Zoals weergegeven in Figuur 5, loopt Nederland hierin achter op de top 5 Europese landen. Dit geeft aan dat de eerste stap naar adoptie is gemaakt, maar de daadwerkelijke uitrol bevindt zich nog in de beginfase aangezien IPv6 adressen eerst geadverteerd moeten worden voordat ze uitgegeven kunnen worden aan klanten.

Tabel 6: Top 10 landen met de meest toegewezen IPv6 adressen (in miljoenen /48's) per jaar

2007		2008		2009	
Australië	268,89	Brazilië	4307,55	VS	15,28
Engeland	68,75	VS	948,83	Duitsland	9,44
Japan	67,44	Zweden	9,37	Engeland	4,06
VS	8,19	Frankrijk	5,37	**Nederland**	3,01
Duitsland	5,77	Duitsland	4,52	Australië	2,88
Taiwan	4,26	Engeland	2,36	Rusland	2,88
Polen	1,18	**Nederland**	2,23	Japan	2,22
Uruguay	1,05	Rusland	2,16	Frankrijk	1,64
Canada	0,85	Zwitserland	2,16	Tsjechië	1,44
Rusland	0,72	China	1,70	Zweden	1,44



Figuur 5: Het aantal toegekende (Allocated) en geadverteerde (Advertised) IPv6 adressen voor de top 10 Europese landen met de meest toegewezen IPv6 adressen (in miljoenen /48's) per 23-04-2010.

3.3.2.2 Implementatie van IPv6 in besturingssystemen

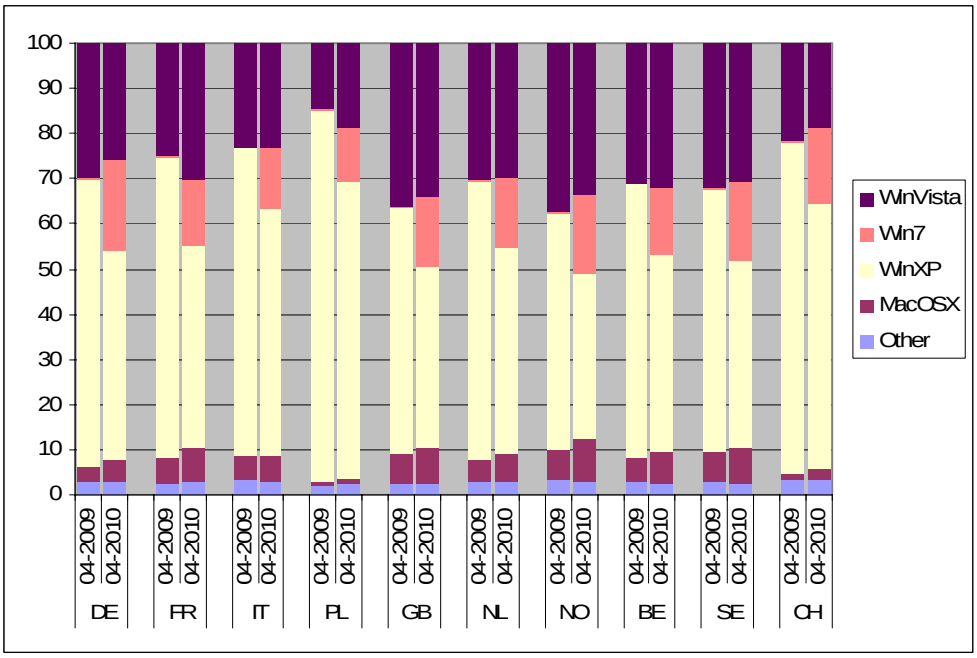
Voordat eindgebruikers daadwerkelijk gebruik kunnen maken van IPv6, zullen de besturingssystemen met IPv6 moeten kunnen omgaan. De besturingssystemen Windows Vista en Windows 7 ondersteunen IPv6 direct bij installatie, en gebruiken IPv6 ook als voorkeursprotocol boven IPv4.

Europa
In Figuur 6 is te zien dat binnen Europa een belangrijk marktaandeel wordt ingenomen door Windows XP. In Windows XP wordt IPv6 niet direct ondersteund, maar kan de IPv6 stack wel geïnstalleerd worden[13]. Daarnaast verlopen DNS requests bij Windows XP altijd over IPv4. In het afgelopen jaar is er een sterke opkomst van Windows 7 gekomen, welke voornamelijk marktaandeel van Windows XP overneemt. Deze verandering draagt zorg voor een percentage van ongeveer 50% van de gebruikte besturingssystemen die IPv6 ondersteunen. Door het doortrekken van de huidige trend kan verwacht worden dat Windows 7 in de komende jaren steeds meer marktaandeel van Windows XP over zal nemen, waardoor een stijgend percentage van alle besturingssystemen geschikt zal zijn voor IPv6.

Nederland
Ook in Nederland is de trend dat het marktaandeel IPv6 geschikte besturingssystemen groeit. Nederland loopt daarbij mee in de voorhoede van Europa.

De verschillende web-browsers die in omloop zijn, vormen geen grote bottleneck voor het gebruik van IPv6. Slecht een paar procent wat de gebruikte browsers ondersteunt nog geen IPv6, zoals oudere versies van Internet Explorer (eerder dan v4.01) en Mozilla Firefox (eerder dan v1.5). Dit is geen significante bottleneck voor de invoering van IPv6.

[13] Het is te verwachten dat de installatie van de IPv6 stack in Windows XP niet snel opgepakt zal worden door de normale thuisgebruiker vanwege de benodigde kennis.



Figuur 6: Marktaandeel besturingssystemen voor de top 10 Europese landen met de meeste IPv6 allocaties

3.3.2.3 Ondersteuning van IPv6 door ISP's

Europa

Een overzicht van ISP's die een native IPv6 verbinding aanbieden aan hun klanten (consumenten en zakelijke klanten) wordt bijgehouden door de website sixxs.net. Op deze website is een overzicht te vinden met de belangrijkste ISP's, onderverdeeld per land. In Figuur 7 zijn deze resultaten weergegeven in een staafdiagram. Het valt op dat de absolute aantallen die weergegeven zijn in de figuur vrij laag zijn en dat daarmee de adoptie van IPv6 onder ISP's nog in de beginfase zit.

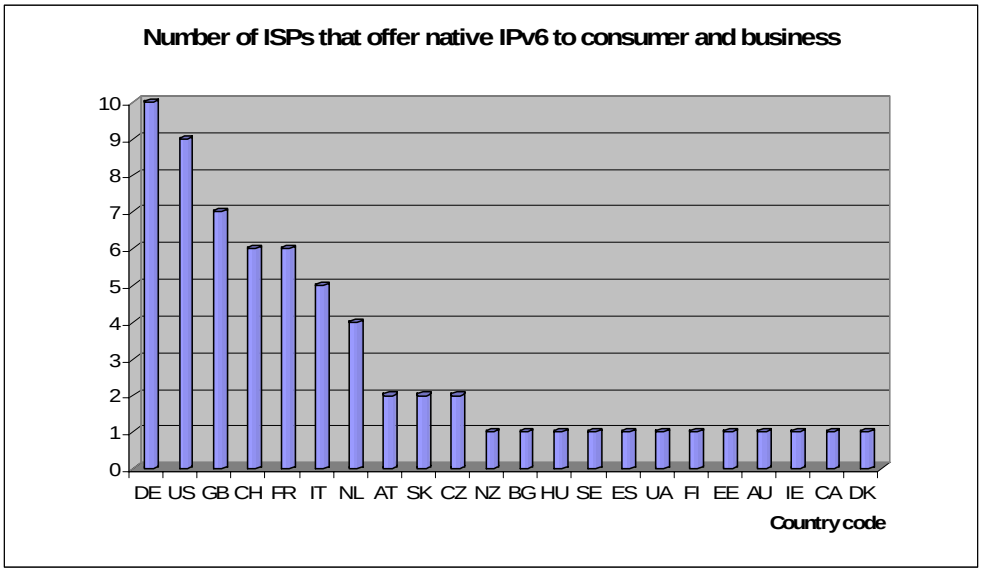
Uit de enquête genoemd in paragraaf 3.2.4 komt naar voren dat 82% van de ondervraagde 267 ISP's in Europa overweegt een IPv6 allocatie aan te vragen en/of dit actief te gaan gebruiken. Hier vallen ook ISP's onder die al een allocatie gekregen hebben. Deze intentie is nadrukkelijk aanwezig bij grotere ISP's. Tevens blijkt dat 56% van de Europese ISP's al enige vorm van IPv6 verkeer terugvindt in haar netwerk. Aannemelijk is dat dit verkeer vooral gegenereerd wordt door verbindingen tussen ISP's en nauwelijks voorkomt in het access netwerk.

Nederland

In vergelijking tot andere landen loopt Nederland niet heel ver achter. Buiten de gegevens van sixxs.net zijn er in Nederland nog enkele ISP's te vinden die IPv6 verbindingen aanbieden aan een beperkte klantgroep. In totaal zijn er zes ISP's te identificeren die op dit moment IPv6 aanbieden voor de zakelijke markt en één voor consumenten. De zakelijke providers zijn BIT, Breedband Delft, Interoute, Signet, Introweb en Proserve. XS4ALL biedt als enige IPv6 aan voor een beperkte groep consumenten[14]. Het grotere aanbod op de zakelijke markt wordt deels veroorzaakt door

[14] http://www.xs4all.nl/klant/ipv6/

een groter aanbod aan ISP's, alsmede de vraag vanuit bedrijven om met IPv6 te kunnen experimenteren.



Figuur 7: Aantal ISP's per land dat commercieel IPv6 verbindingen aanbiedt aan consumenten en/of zakelijke gebruikers per 18-05-2010 (bron: sixxs.net)

Uit de enquête genoemd in paragraaf 3.2.4 komt naar voren dat voor Nederland geldt dat 92% van de respondenten heeft aangegeven IPv6 verkeer terug te vinden in hun netwerk. Het aantal Nederlandse respondenten in de enquête is zo klein dat hun aandeel in de Nederlandse ISP markt niet representatief is. Dit betekent dat het gemeten percentage weinig zekerheid geeft over de aanwezigheid van IPv6 verkeer in netwerken van Nederlandse ISP's.

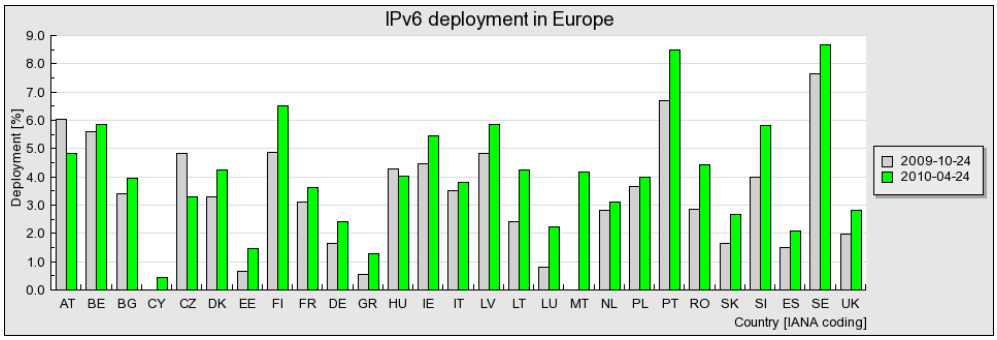
3.3.2.4 Daadwerkelijk IPv6 gebruik

Binnen het project *IPv6 Deployment Monitoring*[15], uitgevoerd door TNO en GNKS, zijn metingen gedaan naar de daadwerkelijke uitrol van IPv6 in de EU. Hierbij zijn het aantal gebruikers in kaart gebracht dat IPv6 gebruikt, en de beschikbaarheid van de meest populaire websites over zowel IPv4 als IPv6. Voor de bepaling naar IPv6 websites is voor elk Europese lidstaat de top 500 van de meest populaire websites genomen (bron: http://www.alexa.com).

Europa

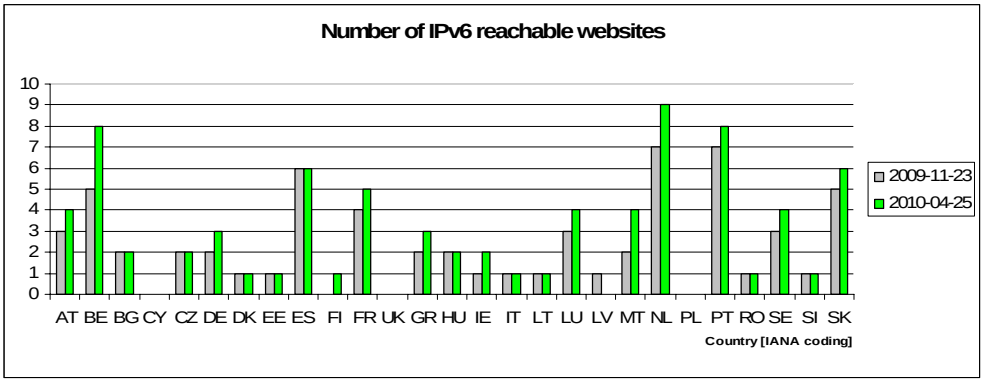
In Figuur 8 blijkt dat gemiddeld gezien de percentages IPv6 gebruikers in het afgelopen halfjaar voorzichtig gestegen zijn, maar dat de percentages nog niet boven de 10% uitkomen. Voor de landen Cyprus, Malta, Luxemburg en Estland is de steekproefgrootte niet voldoende voor een significante weergave.

[15] http://www.ipv6monitoring.eu/



Figuur 8: Percentage van internet gebruikers dat IPv6 gebruikt (bron: ipv6monitoring.eu) per 24 april 2010 en 24 oktober 2009.

Kijkend naar hoeveel websites over IPv6 bereikbaar zijn, blijkt uit Figuur 9 dat het hoogste aantal gehaald wordt door Nederland, alhoewel de absolute aantallen niet zeer hoog zijn. Hier zien we dat zelfs voor de meer populaire websites er nog geen duidelijk signaal van de oppak van IPv6 is.



Figuur 9: Aantal websites in de top 500 meest populaire websites per lidstaat van de EU, die bereikbaar zijn over zowel IPv4 als IPv6 (bron: ipv6monitoring.eu) per 25 april 2010 en 23 november 2009.

Nederland

In vergelijking met andere landen laat Nederland een gemiddelde adoptie zien van IPv6. In Figuur 7 laat zien dat ongeveer 3% van de Nederlandse internet gebruikers toegang heeft tot het IPv6 internet. In vergelijking met andere landen is dit een gemiddelde score.

Met betrekking tot het aantal populaire Nederlandse websites dat via IPv6 benaderbaar is loopt Nederland voorop in Europa. De groei in IPv6 bereikbare websites is echter heel erg klein (slechts 0,4% in een periode van 5 maanden).

4 Standaardisatie en technologische ontwikkelingen

4.1 Inleiding

Standaardisatie en technologische ontwikkelingen zijn sterk aan elkaar gerelateerd. In dit hoofdstuk wordt er een link gelegd tussen de standaardisatie en technologische ontwikkelingen aan de ene kant, en de ontwikkelingen in de uitrol van IPv6 aan de andere kant.

Drie belangrijke standaardisatieorganisaties binnen de ontwikkeling van standaarden en producten zijn de IETF, 3GPP en het Broadband Forum. Deze organisaties zijn leidend op het gebied van IPv6 protocolontwikkeling, cellulaire netwerken en toegangsnetwerken. Al deze organisaties zullen onder de loep genomen worden met betrekking tot IPv6.

4.2 IETF

De Internet Engineering Task Force (IETF) is de organisatie die internetstandaarden ontwikkelt en promoot. IPv6 is ontwikkeld door de IETF. De IETF bestaat uit een groot aantal werkgroepen, die elk een specifiek onderwerp onder de loep nemen. Elke werkgroep dient zijn taak binnen de gestelde tijd uit te voeren, en zal daarna ontbonden worden.

Elke werkgroep produceert deliverables in de vorm van Internet Drafts, die uiteindelijk RFC’s kunnen worden. Internet Drafts worden gekarakteriseerd als ‘work-in-progress’. Deze drafts zijn geldig voor 6 maanden of korter, en staan tijdens publicatie op het internet open voor discussie.

Er is een groot aantal werkgroepen dat zich bezig houdt met onderwerpen gerelateerd aan IPv6. In feite dient elke werkgroep, waarvoor dit relevant is, rekening te houden met IPv6, omdat de IETF IPv6 ziet als het belangrijkste IP protocol voor de toekomst.

In Tabel 7 zijn deze werkgroepen weergegeven, waarbij een datum aangeeft of deze al ontbonden of nog actief is. Daarnaast is de relevantie gedefinieerd, als maat van de bijdrage die de werkgroep kan leveren aan de initiële adoptie en uitrol van IPv6 in Nederland.

Tabel 7: Overzicht van IETF werkgroepen die zich met onderwerpen gerelateerd aan IPv6 bezighouden. De werkgroepen waar een datum bij staat zijn inmiddels ontbonden. De nieuwe werkgroepen zijn veelal voortborduurt op ontbonden werkgroepen. Relevantie is gedefinieerd als de (verwachte) bijdrage aan de initiële adoptie en uitrol van IPv6 in Nederland.

Werkgroep	Datum	Relevantie
IPv6 Management Information Base	1997-10	+
IP Next Generation	2001-12	+
Next Generation Translation	2003-02	+
IP Version 6	2008-03	+
IPv6 Backbone	2008-03	+
Network Mobility	2008-03	-
Mobility for IPv6	2008-03	-
Mobile Nodes and Multiple Interfaces in IPv6	2008-03	-
Site Multihoming in IPv6	2008-03	-
Site Multihoming by IPv6 Intermediation	active	-
IPv6 Operations	active	++
IPv6 over Low power WPAN	active	-
IPv6 Maintenance	active	0
Mobility EXTensions for IPv6	active	-
Inter-Domain Routing	active	0
Behavior Engineering for Hindrance Avoidance	active	++
Mobile Ad-hoc Networks	active	-

Aan de data van de afgesloten werkgroepen is te zien dat de standaardisatie van IPv6 al lange tijd gaande is. In de werkgroep ‘IP Version 6’, die enkele jaren geleden is ontbonden, zijn de belangrijkste specificaties omtrent IPv6 vastgelegd. Ook het gebruik van IPv6 in het core netwerk, is gespecificeerd in de werkgroep ‘IPv6 Backbone’ (6bone), wat een internet-brede routering van IPv6 pakketten mogelijk maakt. Bij de uitrol van IPv6 spelen deze specificaties een belangrijke rol.

Van de actieve werkgroepen zijn ‘IPv6 Operations’ en ‘Behavior Engineering for Hindrance Avoidance’ (behave) veruit de belangrijkste. In ‘IPv6 Operations’ worden richtlijnen opgesteld voor het operationeel gebruik van IPv6 en hoe IPv6 uitgerold kan worden in bestaande IPv4-only netwerken. Hierbij wordt vooral gekeken naar kwesties die op dit moment spelen in de uitrol. De huidige Internet Drafts van ‘IPv6 Operations’ zijn:

- (2010-01-24) Requirements for IPv6 customer edge routers
- (2010-02-08) IPv6 deployment in internet exchange points
- (2010-03-08) Security concerns with IP tunneling
- (2010-04-15) Emerging Service Provider Scenarios for IPv6 Deployment
- (2010-04-17) Mobile Network Considerations for IPv6 Deployment
- (2010-04-24) Simple security capabilities in CPE for residential IPv6 services

Onderwerpen die naar voren komen in de genoemde drafts zijn beveiliging en producten die IPv6 moeten gaan ondersteunen. In hoofdstuk 3 zijn dit ook de onderwerpen die ISP’s als bottleneck ervaren bij de uitrol van IPv6. Het werken aan deze drafts zal daardoor een goede stimulans zijn voor de uitrol van IPv6 door ISP’s. Daarbij worden scenario’s ontwikkeld voor de uitrol van IPv6, voor zowel de vaste als de mobiele netwerken.

In de werkgroep ‘behave’ wordt voornamelijk gekeken naar oplossingen van verschillende translatie scenario’s, waardoor IPv4 gebruikers met IPv6 gebruikers kunnen communiceren en andersom. Deze oplossingen zullen steeds belangrijker gaan worden in de transitiefase.

De twee werkgroepen met een gemiddelde relevantie zijn ‘IPv6 Maintenance en Inter-Domain Routing’. De eerste werkgroep is langlopend en verantwoordelijk voor het bijhouden van de voortgang van de IPv6 protocol specificaties en de architectuur van netwerken. De werkgroep ‘Inter-Domain Routing’ houdt zich zijdelings bezig met IPv6, en specificeert bijvoorbeeld de routering voor de verbinding van IPv6-eilanden over IPv4 MPLS door het gebruik van IPv6 Provider Edge Routers. Dit soort ontwikkelingen kunnen bijdragen aan de transitie mogelijkheden van ISP’s.

4.3 3GPP

Het 3rd Generation Partnership Project (3GPP) is een samenwerkingsverband tussen verschillende telecommunicatiestandaarden en is erg belangrijk voor de ontwikkeling van specificaties, netwerkprotocollen en infrastructuur van mobiele netwerken. De 3GPP specificaties zijn gebaseerd op de GSM standaard, en geëvolueerd naar de standaarden met betrekking tot UMTS, HDPA, IMS en LTE.

De standaarden van 3GPP worden gestructureerd in zogenaamde releases. De huidige release waaraan gewerkt wordt in Release 10. Onderdeel van deze release is een migratie studie naar IPv6, waaruit richtlijnen naar voren zullen komen welke erg belangrijk zijn voor mobiele operators.

Inmiddels zijn er wereldwijd al enkele operators die IPv6 ondersteunen, door middel van een dual-stack implementatie of IPv6-only. De specificaties hiervoor zijn al beschreven in Release 8, welke eind 2008 is uitgekomen. Er is echter nog geen studie gedaan naar de transitie van IPv4 naar dual-stack IPv4/IPv6 of IPv6-only. Met behulp van de IETF transitiemechanismes (welke onder andere in de IPv6 Operations werkgroep naar voren komen) zal 3GPP verschillende migratiescenario’s analyseren.

In het eerste kwartaal van dit jaar zijn tijdens een workshop drie migratiescenario’s vastgesteld die brede steun kregen:

1 Dual-stack connectiviteit met een beperkte publieke adresruimte
  In dit scenario krijgt de gebruiker zowel een IPv4 als IPv6 adres. Geleidelijk zal het IPv4 verkeer naar IPv6 migreren. Een risico is dat de publieke IPv4 adresvoorraad te klein is. Overwogen kan worden om privé adresruimte[16] te gebruiken achter een NAT.
2 Dual-stack connectiviteit met een beperkte privé-adresruimte
  Net als in het vorige scenario krijgt de gebruiker hier zowel een IPv4 en een IPv6 adres. De gebruikte IPv4 adressen komen echter allemaal uit de privé adresruimte. De uitdaging in dit scenario komt naar voren als er meer dan 16 miljoen gebruikers (klasse A adresruimte) tegelijkertijd op het netwerk zitten.
3 Aansluiting d.m.v. IPv6-only en toepassingen die IPv6 ondersteunen

[16] Privé adressen zijn adressen die niet routeerbaar zijn op het internet. Door deze beperking wordt het mogelijk de adressen opnieuw te gebruiken, ofwel verschillende netwerken kunnen binnen het eigen netwerk dezelfde IP adressen gebruiken.

In dit scenario krijgt de gebruiker alleen een IPv6 adres door het tekort aan IPv4 adressen of omdat het anderzijds voordelig kan zijn. Gebruikers met IPv6 connectiviteit die IPv6 ondersteunde toepassingen gebruiken dienen nog steeds in staat te zijn om zowel IPv4 als IPv6 diensten te gebruiken.

Deze scenario's worden verder uitgewerkt in samenwerking met veel internationale partijen en mobiele operators. De transitiescenario's zullen gepubliceerd worden in Release 10, welke begin 2011 wordt verwacht. De uitwerking zal niet bestaan uit verplichte specificaties, maar uit richtlijnen die mobiele operators ten harte kunnen nemen in voorbereiding naar en tijdens de transitiefase van IPv4 naar dual-stack IPv4/IPv6 en IPv6-only.

4.4 Broadband Forum

Het Broadband Forum heeft als doel het opstellen van specificaties waarmee netwerk operatoren en serviceproviders leveranciers kunnen benaderen. Door afstemming tussen klant en leverancier over de te volgen roadmap wordt een snellere adoptie van technologie en diensten gerealiseerd. Het Broadband Forum put uit standaarden van o.a. de IETF, ITU-T, en IEEE.

In het Broadband Forum worden standaarden aangepast aan de specifieke uitdagingen en problemen die een rol spelen bij het uitrollen van telecommunicatiediensten en daarmee afwijken van het uitrollen van netwerken en diensten in een bedrijfsomgeving.

In het eerste kwartaal van 2009 werd een lijst opgesteld met issues die een rol spelen in de introductie van IPv6 in thuis- , access- en corenetwerken. Hierin werd een diversiteit aan issues in kaart gebracht op zowel techno-economisch vlak als puur technisch. Om diensten gebaseerd op IPv6 uit te kunnen rollen zal zowel het thuisnetwerk, het accessnetwerk als het corenetwerk de juiste technologische IPv6 specificaties moeten bezitten. Tevens zal er onder serviceproviders in grote lijnen overeenstemming moeten zijn hoe de IPv6 features passen in commerciële migratie trajecten.

De Broadband Forum roadmap voor IPv6 in huis- en accessnetwerken bestaat uit o.a. de volgende activiteiten:

- WT-124, beschrijft Residential Gateway IPv6 eisen (vernieuwd de huidige TR-124).
- WT-187, beschrijft IPv6 over PPP tunnels. (In Nederland wordt veel met PPP gewerkt.)
- WT-177 (TR101), beschrijft hoe IPv6 in een Ethernet omgeving door access multiplexers (AM's) moet worden verwerkt.
- WT-242, beschrijft hoe IPv4 en IPv6 co-existeren.
- WT-243, beschrijft procedures hoe IPv4 zal uitfaseren.

In mei 2010 stemmen de aan deze *working texts* deelnemende organisaties over WT-124 en WT-187. Daarmee worden deze door de deelnemende organisaties definitief bekrachtigd. WT-177 is op dit moment kandidaat voor stemming. WT-242 en WT-243 moeten nog invulling krijgen. In deze working texts zullen o.a. onderwerpen aan bod komen die vanwege de tijdsplanning bewust uit WT-177 zijn weggelaten.

De uiteindelijke beschikbaarheid van producten voor netwerkoperatoren en serviceproviders komt hierdoor enkele stappen dichterbij met als belangrijkste resultaat

dat een migratie naar IPv6 kosten efficiënter zal kunnen verlopen en minder riskant is. Indien zowel fabrikanten als netwerkoperatoren en service providers niet geremd worden door politieke of economische factoren kan beschikbaarheid (of in ieder geval de mogelijkheid) van op IPv6 gebaseerde diensten in 2011 een feit zijn.

4.5 Conclusie

De standaard voor IPv6 is in de jaren 90 ontwikkeld door de IETF. Hiermee zijn onder andere de specificaties van het protocol, de adresstructuur en adresruimte gedefinieerd. Dit geeft aan dat de standaardisatie van IPv6 geen bottleneck meer vormt voor de uitrol van IPv6.

Binnen de verschillende standaardisatieorganisaties wordt echter nog steeds werk verricht en geïnitieerd dat gerelateerd is aan IPv6. Dit gaat niet zo zeer over de specificatie van IPv6, maar over ontwikkelingen gerelateerd aan IPv6, zoals technologieën ten behoeve van transitiescenario’s en IPv6 functionaliteiteisen aan producten.

In de werkgroepen van de verschillende standaardisatieorganisaties is een duidelijke aansluiting te zien bij de praktische problemen die op dit moment ervaren worden bij de uitrol van IPv6.

5 Veiligheid van IPv6 in relatie tot IPv4

5.1 Inleiding

Als organisaties IPv6 gaan toepassen is het van belang dat deze technologie volwassen genoeg is om betrouwbaar te kunnen gebruiken. Indien bij burgers, bedrijven en overheden de perceptie leeft dat diensten die gebruikmaken van IPv6 minder veilig zijn dan wanneer deze diensten over IPv4 zouden worden afgenomen, dan kan dit een remmend effect hebben op de adoptie van IPv6. Om deze reden is gekeken naar veiligheid van het gebruik van IPv6 ten opzichte van het gebruik van IPv4.

Als het aankomt op de veiligheid van een dienst, dan is deze zo sterk als de zwakste schakel. De afhankelijkheid van IP verbindingen is slechts één van deze schakels. Migratie van een veilig en uitontwikkeld IPv4 netwerk naar IPv6 kan een dienst alsnog kwetsbaar maken indien het IPv6 netwerk kwetsbaarheden bevat.

5.2 Methode

In deze monitor wordt gebruik gemaakt van gerapporteerde kwetsbaarheden[17,18]. Wanneer kwetsbaarheden gerapporteerd worden (middels een diversiteit aan mailing lijsten die gemonitored worden) en als kwetsbaarheden geaccepteerd zijn, dan worden zij toegevoegd in een databestand en wordt het *Common Vulnerability Scoring System* (CVSS) gebruikt om een objectieve indicatie te geven van de impact van een kwetsbaarheid[19]. In dit systeem wordt een cijfer tussen de 0 en 10 toegekend door security analisten, producenten van beveiligingssystemen en door leveranciers van software applicaties. Op deze manier wordt een groot deel van een dienstketen vertegenwoordigd en wordt een betrouwbare score verkregen. Een “0” betekent dat de kwetsbaarheid gering is, terwijl een “10” betekent dat de kwetsbaarheid groot is. Om tot een inschatting te komen van een basis kwetsbaarheid wordt beoordeeld naar een aantal criteria:

- Toegangseisen voor de aanvaller (de afstand waarop een aanval moet worden ingezet)
- Toegangscomplexiteit (de mate waarin een aanvaller moet zien binnen te komen in een systeem)
- Authenticatie (de frequentie waarmee een aanvaller gevraagd wordt zich te legitimeren)
- Confidentiële impact (de gevoeligheid van de informatie die de aanvaller in handen kan krijgen)
- Integriteit impact (de mate waarin een aanvaller informatie kan veranderen/vernietigen)
- Beschikbaarheid impact (de uitval van het aangevallen systeem)

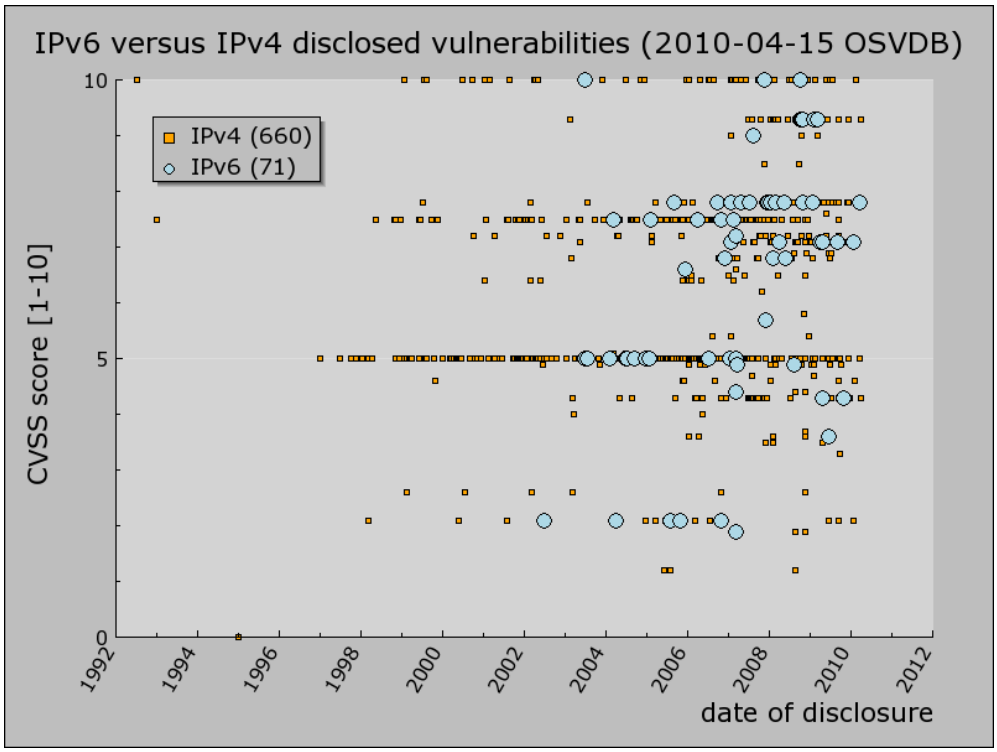
[17] Deze methode heeft als nadeel dat niet alle kwetsbaarheden bekend gemaakt worden. Er zal dan ook nooit een 100% compleet en actueel overzicht zijn van alle kwetsbaarheden. Om een vergelijking tussen IPv6 en IPv4 te maken is een compleet en actueel overzicht niet perse nodig als aangenomen wordt dat de fractie IPv6 kwetsbaarheden dat gerapporteerd wordt gelijk is aan de fractie IPv4 kwetsbaarheden dat gerapporteerd wordt.
[18] www.osvdb.org
[19] www.first.org/cvss

Door middel van een verdeelsleutel wordt het uiteindelijke CVSS cijfer bepaald dat een maat is voor de ernst van de kwetsbaarheid.

Omdat de impact van individu tot individu, van bedrijf tot bedrijf en ook binnen overheidsinstellingen erg wisselend is wordt deze niet meegenomen in de rapportage. Dit vraagt namelijk om een zeer gedetailleerde studie per geval naar specifieke dreigingen en vaak zeer specifieke gevolgen.

Het CVSS cijfer dient voor al deze gevallen als een belangrijke parameter. Mochten er voor IPv6 gerelateerde kwetsbaarheden andere cijfers gelden dan voor IPv4, dan treden zeker ook verschillen op in de impact binnen eenzelfde organisatie. Echter, voor verschillende organisaties en diensten zal dit resulteren in een diversiteit aan mogelijke impact.

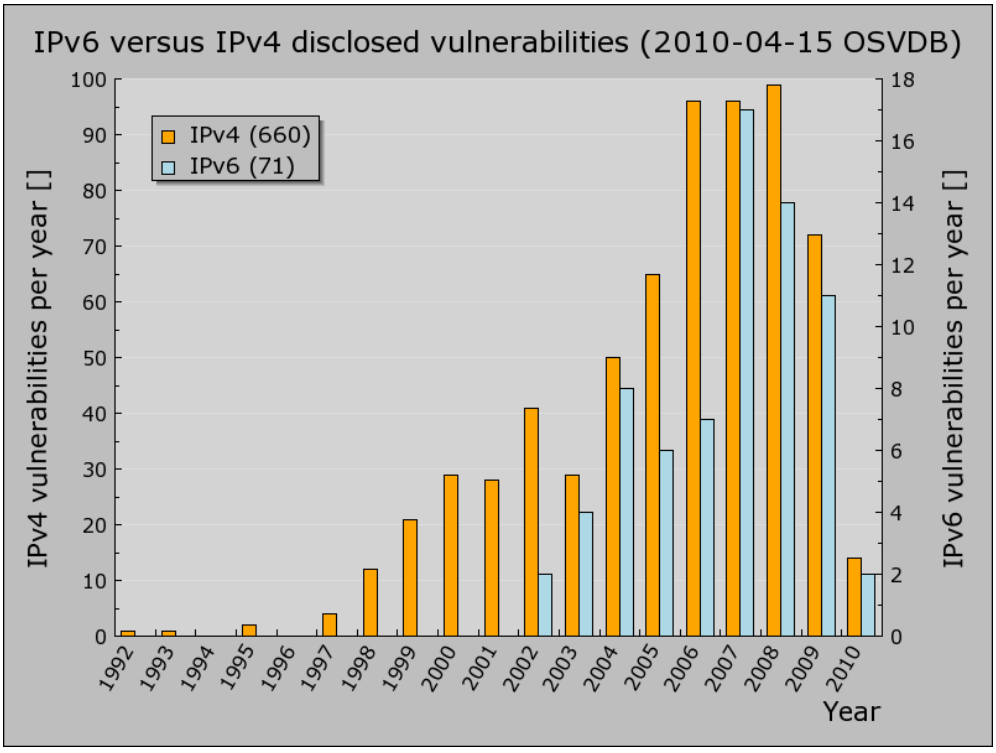
5.3 Monitoring van kwetsbaarheden



Figuur 10: Gerapporteerde kwetsbaarheden[18] van IPv6 en van IPv4, tot 15 april 2010 en de CVSS scores. De datum is de datum waarop de kwetsbaarheid openbaar werd gemaakt.

Figuur 10 laat zien waar de kwetsbaarheden voor IPv4 en IPv6 liggen in de tijd en wat de kwetsbaarheidscore is. Ieder meetpunt stelt een gerapporteerde en bevestigde kwetsbaarheid[18] voor. De kwetsbaarheden hebben betrekking op het IPv4 en IPv6 protocol en de ondersteunende protocollen. (Voor IPv4 zijn dit o.a. ICMP, DHCP, IGMP, etc...). Niet meegenomen zijn kwetsbaarheden die onafhankelijk zijn van de IP protocolversie zijn zoals bijvoorbeeld mechanismen voor authenticatie, autorisatie en accounting.

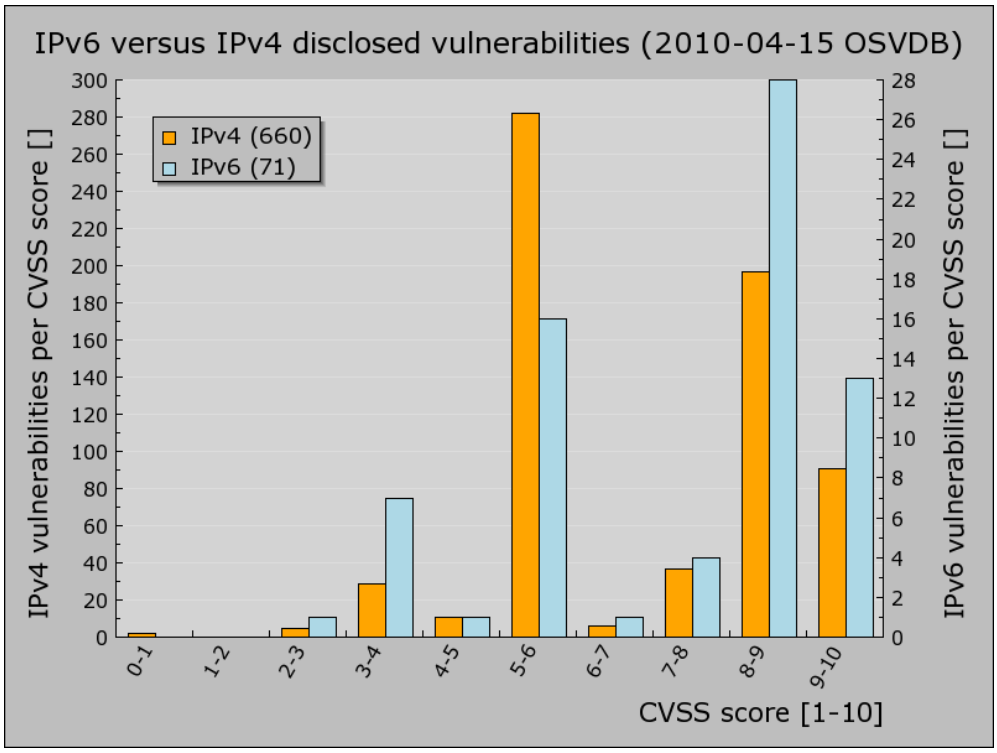
Figuur 11 laat zien hoe de kwetsbaarheden tot 15 april 2010 verdeeld zijn over de tijd. Hierin zijn alle kwetsbaarheden, ongeacht CVSS score, meegenomen. Op 15 november 2009 waren er 632 gerapporteerde kwetsbaarheden voor IPv4 en 69 meldingen voor IPv6. Gedurende vijf maanden is het aantal kwetsbaarheden voor zowel IPv4 als IPv6 toegenomen met ongeveer 4%. Verder valt op te merken dat de verdeling van gevonden kwetsbaarheden zowel voor IPv4 als IPv6 piekt rond 2007 en 2008. Dit kan betekenen dat er toen daadwerkelijk veel kwetsbaarheden in producten zaten, of dat er sindsdien gewoonweg minder incidenten zijn gemeld.



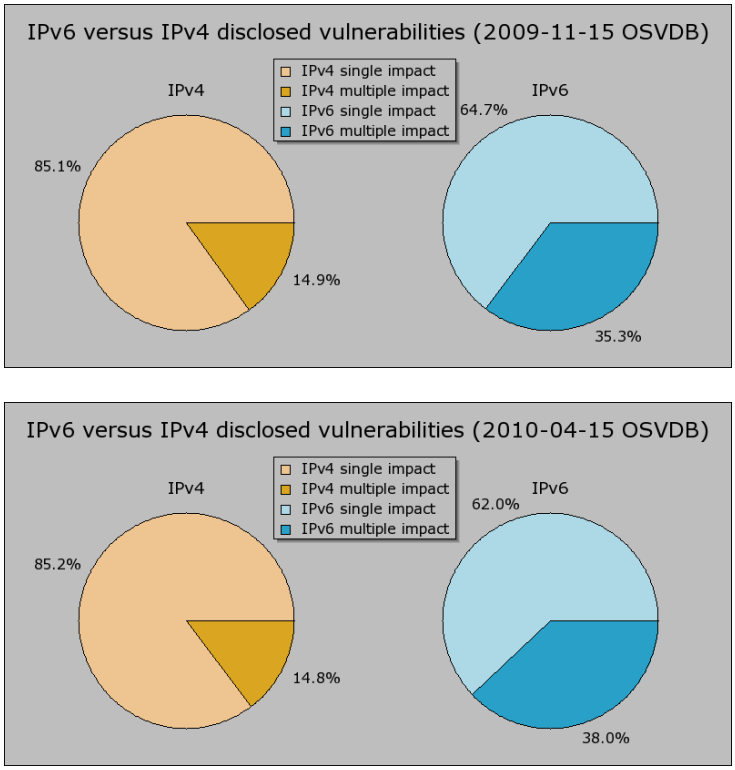
Figuur 11: Aantallen gerapporteerde[18] IPv4 en IPv6 kwetsbaarheden per jaar, tot 15 april 2010.

Figuur 12 laat zien dat wat betreft CVSS score het aantal gerapporteerde IPv6 kwetsbaarheden onderling anders verdeeld is dan de IPv4 kwetsbaarheden. IPv6 kent relatief veel ernstige kwetsbaarheden (CVSS scores groter dan acht) in tegenstelling tot IPv4, waar de helft van de kwetsbaarheden als middelmatig kan worden aangemerkt (CVSS score tussen de vijf en zes).

Voor de adoptie van IPv6 is het van belang dat burgers en bedrijven zich niet gehinderd voelen door kwetsbaarheden die kunnen leiden tot veiligheidsincidenten zoals verlies van data, diefstal van data en verminking van data. Het is van belang dat er voldoende uitwijkmogelijkheden zijn met betrekking tot alternatieve apparatuur en software. Om deze reden is het van belang te onderzoeken in welke mate kwetsbaarheden zich manifesteren in een enkele implementatie van een apparaat of programma, of dat kwetsbaarheden terug te vinden zijn in meerdere implementaties en daardoor in een diversiteit van apparatuur en programmatuur kunnen voorkomen. Hiertoe is per kwetsbaarheid gekeken of deze impact enkelvoudig of meervoudig is.



Figuur 12: Aantallen gerapporteerde[18] IPv4 en IPv6 kwetsbaarheden ingedeeld naar kwetsbaarheidscore, tot 15 april 2010.



Figuur 13: Impact van kwetsbaarheden op producten en software. Boven: situatie tot 15 november 2009, onder: situatie tot 15 april 2010.

Figuur 13 laat zien hoe zich deze impact verhoudt. De figuur geeft voor IPv4 en voor IPv6 aan wat de verhouding is tussen kwetsbaarheden die impact hebben op meerdere producten of software (multiple impact) en een enkel product of software (single impact).

Voor IPv4 ligt dit percentage ongeveer op 15% en is constant te noemen tussen de periode 15 november 2009 en 15 april 2010. Voor IPv6 heeft meer dan een derde van de kwetsbaarheden impact op meerdere producten of software. Dit is zorgelijk omdat deze kwetsbaarheden niet opgelost kunnen worden door over te stappen naar andere apparatuur of software. Hier komt bovendien nog bij dat in de vijf maanden tijd tussen de meetmomenten uitsluitend kwetsbaarheden met meervoudige impact zijn gerapporteerd.

Uit Figuur 12 en Figuur 13 blijkt dat IPv6 relatief veel kwetsbaarheden kent met een hoge CVSS score en dat een percentage van bijna 40% van deze kwetsbaarheden impact hebben op producten van verschillend fabricaat. Dit is zorgelijk omdat het moeilijk wordt voor ernstige kwetsbaarheden uit te wijken naar alternatieve producten. Indien de trend zoals zichtbaar in Figuur 11 zich doorzet en de rapportage van kwetsbaarheden verder afneemt (het is dan te verwachten dat er ook daadwerkelijk minder kwetsbaarheden in producten aanwezig zijn), dan zou het nemen van maatregelen niet noodzakelijk hoeven te zijn. Een vervolgmeting over ongeveer een halfjaar zal hernieuwd inzicht hierin geven.

5.4 Conclusie

Er is op basis van gerapporteerde kwetsbaarheden reden aan te nemen dat het met de veiligheid van IPv6 in vergelijking met IPv4 niet slecht gesteld is. Kwetsbaarheden in IPv6 kunnen vaker een grotere impact hebben dan kwetsbaarheden in IPv4, maar de frequentie waarmee IPv6 gerelateerde kwetsbaarheden gerapporteerd wordt is laag in vergelijking met IPv4 en bovendien dalende.

Het verdient de aanbeveling kwetsbaarheden te blijven monitoren totdat een grootschalige adoptie van IPv6 feit is. Plotselinge toetreding van fabrikanten van IPv6 apparatuur en software en de te verwachten stijging van adoptie van IPv6 door consumenten en bedrijven kan alsnog leiden tot groei in de toename in gerapporteerde kwetsbaarheden.

6 Conclusies en aanbevelingen

De status van de uitrol van IPv6 in Nederland ten opzichte van ons omringende landen is door middel van een nulmeting in kaart gebracht. In vergelijking met ons omringende landen loopt Nederland mee in de voorhoede als het gaat om voorbereidingen voor de uitrol van IPv6. Nederland presteert gemiddeld als het gaat om de daadwerkelijke uitrol van IPv6.

Indien aangenomen wordt dat de IPv4 adressen opraken tussen september 2011 en november 2012 dan is de voornaamste zorg het kunnen bieden van een IPv6 verbinding aan eindgebruikers. Standaardisatieactiviteiten die bijdragen aan het beschikbaar maken van hiervoor benodigde telecommunicatieapparatuur zijn geïnitieerd en bevinden zich in een vergevorderd stadium. De industrie zal op dit punt naar verwachting nog geen hinder ondervinden van het uitblijven van consensus tussen toeleveranciers van telecommunicatieapparatuur en netwerkoperatoren en internetaanbieders.

Het uitblijven van beschikbaarheid van content (o.a. websites) en diensten op IPv6 is een tweede zorg die een serieuze belemmering kan vormen voor de uitrol van IPv6 in Nederland.

IPv6 gerelateerde kwetsbaarheden worden relatief vaker teruggevonden in meerdere producten en fabricaten tegelijk, in vergelijking met IPv4. Tevens blijkt dat in vergelijking met IPv4 de IPv6 kwetsbaarheden vaker potentieel grote impact kunnen hebben. Het aantal gerapporteerde IPv6 kwetsbaarheden in apparatuur en software is echter laag en dalende in vergelijking met IPv4 gerelateerde kwetsbaarheden. Vervolg metingen zullen moeten uitwijzen of deze daling zich in de toekomst doorzet wanneer meer producten op de markt komen en IPv6 gebruik toeneemt.

Uitrol van IPv6 kan versneld worden door gericht te sturen op het aanbieden van IPv6 verbindingen aan eindgebruikers en het beschikbaar maken van content op IPv6. Zowel de veiligheid van IPv6 als de implementatie van de standaarden dient bewaakt te worden om de uitrol van IPv6 niet te vertragen.